



# Configuring Protocol Independent Multicast (PIM)

---

- [Finding Feature Information, on page 1](#)
- [Prerequisites for Configuring PIM, on page 1](#)
- [Restrictions for Configuring PIM, on page 2](#)
- [Restrictions for Configuring Auto-RP, on page 2](#)
- [Restrictions for Configuring Auto-RP and BSR, on page 3](#)
- [Information About PIM, on page 3](#)
- [How to Configure PIM, on page 14](#)
- [Monitoring PIM Information, on page 42](#)
- [Troubleshooting PIMv1 and PIMv2 Interoperability Problems, on page 44](#)
- [Configuration Examples for PIM, on page 44](#)
- [Where to Go Next for PIM , on page 47](#)
- [Additional References, on page 48](#)
- [Feature History and Information for PIM, on page 49](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Prerequisites for Configuring PIM

The following are the prerequisites for configuring PIM and PIM stub routing:

- Before configuring PIM stub routing, you must have IP multicast routing configured on both the stub router and the central router. You must also have PIM mode (dense-mode, sparse-mode, or sparse-dense-mode) configured on the uplink interface of the stub router.

- Before configuring PIM stub routing, you must also configure either Enhanced Interior Gateway Routing Protocol (EIGRP) stub routing or Open Shortest Path First (OSPF) stub routing on the device. The PIM stub router does not route the transit traffic between the distribution routers. Unicast (EIGRP) stub routing enforces this behavior. You must configure unicast stub routing to assist the PIM stub router behavior.

**Note**

For information about EIGRP or OSPF configurations, see the *Catalyst 3650 Routing Configuration Guide, Release 3SE*.

## Restrictions for Configuring PIM

The following are the restrictions for configuring PIM:

- PIM
  - PIM is not supported when running the LAN Base feature set.
- PIM stub routing
  - The IP Services image contains complete multicast routing.
  - In a network using PIM stub routing, the only allowable route for IP traffic to the user is through a device that is configured with PIM stub routing.
  - The redundant PIM stub router topology is not supported. Only the nonredundant access router topology is supported by the PIM stub feature.
  - Only directly connected multicast (IGMP) receivers and sources are allowed in the Layer 2 access domains. The PIM protocol is not supported in access domains.

## Restrictions for Configuring Auto-RP

The following are restrictions for configuring Auto-RP (if used in your network configuration):

- Auto-RP is not supported when running the LAN Base feature set.
- If you configure PIM in sparse mode or sparse-dense mode and do not configure Auto-RP, you must manually configure an RP.
- If routed interfaces are configured in sparse mode, Auto-RP can still be used if all devices are configured with a manual RP address for the Auto-RP groups.
- If routed interfaces are configured in sparse mode and you enter the **ip pim autorp listener** global configuration command, Auto-RP can still be used even if all devices are not configured with a manual RP address for the Auto-RP groups.

## Restrictions for Auto-RP Enhancement

The simultaneous deployment of Auto-RP and bootstrap router (BSR) is not supported.

## Restrictions for Configuring Auto-RP and BSR

The following are restrictions for configuring Auto-RP and BSR (if used in your network configuration):

- If your network is all Cisco routers and multilayer devices, you can use either Auto-RP or BSR.
- If you have non-Cisco routers in your network, you must use BSR.
- If you have Cisco PIMv1 and PIMv2 routers and multilayer devices and non-Cisco routers, you must use both Auto-RP and BSR. If your network includes routers from other vendors, configure the Auto-RP mapping agent and the BSR on a Cisco PIMv2 device. Ensure that no PIMv1 device is located in the path a between the BSR and a non-Cisco PIMv2 device.



---

**Note** There are two approaches to using PIMv2. You can use Version 2 exclusively in your network or migrate to Version 2 by employing a mixed PIM version environment.

---

- Because bootstrap messages are sent hop-by-hop, a PIMv1 device prevents these messages from reaching all routers and multilayer devices in your network. Therefore, if your network has a PIMv1 device in it and only Cisco routers and multilayer devices, it is best to use Auto-RP.
- If you have a network that includes non-Cisco routers, configure the Auto-RP mapping agent and the BSR on a Cisco PIMv2 router or multilayer device. Ensure that no PIMv1 device is on the path between the BSR and a non-Cisco PIMv2 router.
- If you have non-Cisco PIMv2 routers that need to interoperate with Cisco PIMv1 routers and multilayer devices, both Auto-RP and a BSR are required. We recommend that a Cisco PIMv2 device be both the Auto-RP mapping agent and the BSR.

## Information About PIM

Protocol-Independent Multicast (PIM) is called protocol-independent because regardless of the unicast routing protocols used to populate the unicast routing table, PIM uses this information to perform multicast forwarding instead of maintaining a separate multicast routing table.

PIM can leverage whichever unicast routing protocols are used to populate the unicast routing table, including EIGRP, OSPF, BGP, or static routes. PIM uses this unicast routing information to perform the multicast forwarding function, so it is IP protocol independent. Although PIM is called a multicast routing protocol, it actually uses the unicast routing table to perform the reverse path forwarding (RPF) check function instead of building up a completely independent multicast routing table. PIM does not send and receive multicast routing updates between routers as the other routing protocols do.

PIM is defined in RFC 4601, *Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*. PIM is defined in these Internet Engineering Task Force (IETF) Internet drafts:

- *Protocol Independent Multicast (PIM): Motivation and Architecture*
- *Protocol Independent Multicast (PIM), Dense Mode Protocol Specification*
- *Protocol Independent Multicast (PIM), Sparse Mode Protocol Specification*
- *draft-ietf-idmr-igmp-v2-06.txt, Internet Group Management Protocol, Version 2*
- *draft-ietf-pim-v2-dm-03.txt, PIM Version 2 Dense Mode*

## PIM Versions

PIMv2 includes these improvements over PIMv1:

- A single, active rendezvous point (RP) exists per multicast group, with multiple backup RPs. This single RP compares to multiple active RPs for the same group in PIMv1.
- A bootstrap router (BSR) provides a fault-tolerant, automated RP discovery and distribution function that enables routers and multilayer devices to dynamically learn the group-to-RP mappings.
- Sparse mode and dense mode are properties of a group, as opposed to an interface.



---

**Note** We strongly recommend using sparse-dense mode as opposed to either sparse mode or dense mode only.

---

- PIM join and prune messages have more flexible encoding for multiple address families.
- A more flexible hello packet format replaces the query packet to encode current and future capability options.
- Register messages sent to an RP specify whether they are sent by a border router or a designated router.
- PIM packets are no longer inside IGMP packets; they are standalone packets.

## PIMv1 and PIMv2 Interoperability

To avoid misconfiguring multicast routing on your device, review the information in this section.

The Cisco PIMv2 implementation provides interoperability and transition between Version 1 and Version 2, although there might be some minor problems.

You can upgrade to PIMv2 incrementally. PIM Versions 1 and 2 can be configured on different routers and multilayer devices within one network. Internally, all routers and multilayer devices on a shared media network must run the same PIM version. Therefore, if a PIMv2 device detects a PIMv1 device, the Version 2 device downgrades itself to Version 1 until all Version 1 devices have been shut down or upgraded.

PIMv2 uses the BSR to discover and announce RP-set information for each group prefix to all the routers and multilayer devices in a PIM domain. PIMv1, together with the Auto-RP feature, can perform the same tasks as the PIMv2 BSR. However, Auto-RP is a standalone protocol, separate from PIMv1, and is a proprietary Cisco protocol. PIMv2 is a standards track protocol in the IETF.



**Note** We recommend that you use PIMv2. The BSR function interoperates with Auto-RP on Cisco routers and multilayer devices.

When PIMv2 devices interoperate with PIMv1 devices, Auto-RP should have already been deployed. A PIMv2 BSR that is also an Auto-RP mapping agent automatically advertises the RP elected by Auto-RP. That is, Auto-RP sets its single RP on every router or multilayer device in the group. Not all routers and devices in the domain use the PIMv2 hash function to select multiple RPs.

Sparse-mode groups in a mixed PIMv1 and PIMv2 region are possible because the Auto-RP feature in PIMv1 interoperates with the PIMv2 RP feature. Although all PIMv2 devices can also use PIMv1, we recommend that the RPs be upgraded to PIMv2. To ease the transition to PIMv2, we recommend:

- Using Auto-RP throughout the region.
- Configuring sparse-dense mode throughout the region.

If Auto-RP is not already configured in the PIMv1 regions, configure Auto-RP.

## PIM Modes

PIM can operate in dense mode (DM), sparse mode (SM), or in sparse-dense mode (PIM DM-SM), which handles both sparse groups and dense groups at the same time.

### PIM DM

PIM DM builds source-based multicast distribution trees. In dense mode, a PIM DM router or multilayer device assumes that all other routers or multilayer devices forward multicast packets for a group. If a PIM DM device receives a multicast packet and has no directly connected members or PIM neighbors present, a prune message is sent back to the source to stop unwanted multicast traffic. Subsequent multicast packets are not flooded to this router or device on this pruned branch because branches without receivers are pruned from the distribution tree, leaving only branches that contain receivers.

When a new receiver on a previously pruned branch of the tree joins a multicast group, the PIM DM device detects the new receiver and immediately sends a graft message up the distribution tree toward the source. When the upstream PIM DM device receives the graft message, it immediately puts the interface on which the graft was received into the forwarding state so that the multicast traffic begins flowing to the receiver.

### PIM-SM

PIM-SM uses shared trees and shortest-path-trees (SPTs) to distribute multicast traffic to multicast receivers in the network. In PIM-SM, a router or multilayer device assumes that other routers or devices do not forward multicast packets for a group, unless there is an explicit request for the traffic (join message). When a host joins a multicast group using IGMP, its directly connected PIM-SM device sends PIM join messages toward the root, also known as the rendezvous point (RP). This join message travels router-by-router toward the root, constructing a branch of the shared tree as it goes.

The RP keeps track of multicast receivers. It also registers sources through register messages received from the source's first-hop router (designated router [DR]) to complete the shared tree path from the source to the receiver. When using a shared tree, sources must send their traffic to the RP so that the traffic reaches all receivers.

Prune messages are sent up the distribution tree to prune multicast group traffic. This action permits branches of the shared tree or SPT that were created with explicit join messages to be torn down when they are no longer needed.

When the number of PIM-enabled interfaces exceeds the hardware capacity and PIM-SM is enabled with the SPT threshold is set to **infinity**, the device does not create (source, group (S, G) ) entries in the multicast routing table for the some directly connected interfaces if they are not already in the table. The device might not correctly forward traffic from these interfaces.

## Multicast Source Discovery Protocol (MSDP)

Multicast Source Discovery Protocol (MSDP) is used for inter-domain source discovery when PIM SM is used. Each PIM administrative domain has its own RP. In order for the RP in one domain to signal new sources to the RP in the other domain, MSDP is used.

When RP in a domain receives a PIM register message for a new source, with MSDP configured it sends a new source-active (SA) message to all its MSDP peers in other domains. Each intermediate MSDP peer floods this SA message away from the originating RP. The MSDP peers install this SA message in their MSDP sa-cache. If the RPs in other domains have any join requests for the group in the SA message (indicated by the presence of a (\*,G) entry with non empty outgoing interface list), the domain is interested in the group, and the RP triggers an (S,G) join toward the source.

## PIM Stub Routing

The PIM stub routing feature, available in all of the device software images, reduces resource usage by moving routed traffic closer to the end user.

The PIM stub routing feature supports multicast routing between the distribution layer and the access layer. It supports two types of PIM interfaces: uplink PIM interfaces and PIM passive interfaces. A routed interface configured with the PIM passive mode does not pass or forward PIM control traffic, it only passes and forwards IGMP traffic.

In a network using PIM stub routing, the only allowable route for IP traffic to the user is through a device that is configured with PIM stub routing. PIM passive interfaces are connected to Layer 2 access domains, such as VLANs, or to interfaces that are connected to other Layer 2 devices. Only directly connected multicast (IGMP) receivers and sources are allowed in the Layer 2 access domains. The PIM passive interfaces do not send or process any received PIM control packets.

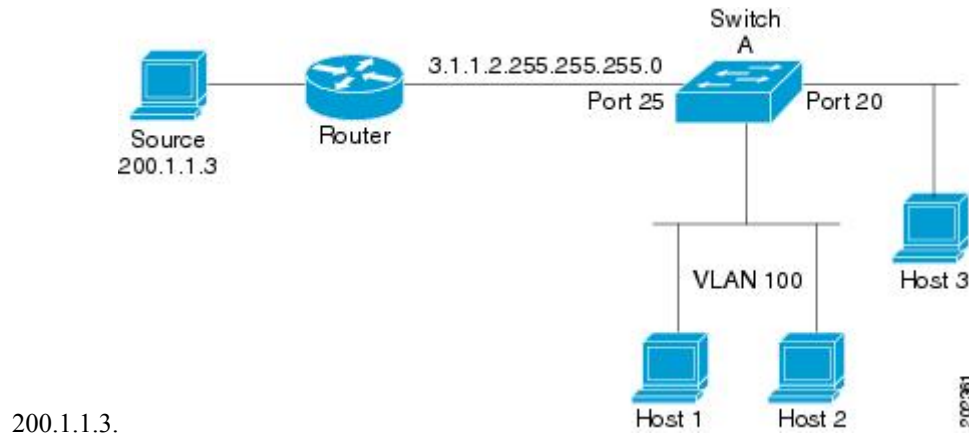
When using PIM stub routing, you should configure the distribution and remote routers to use IP multicast routing and configure only the device as a PIM stub router. The device does not route transit traffic between distribution routers. You also need to configure a routed uplink port on the device. The device uplink port cannot be used with SVIs. If you need PIM for an SVI uplink port, you should upgrade to the IP Services feature set.

You must also configure EIGRP stub routing when configuring PIM stub routing on the device. For information about this procedure, refer to the *Catalyst 3850 IP Routing Configuration Guide*.

The redundant PIM stub router topology is not supported. The redundant topology exists when there is more than one PIM router forwarding multicast traffic to a single access domain. PIM messages are blocked, and the PIM asset and designated router election mechanisms are not supported on the PIM passive interfaces. Only the nonredundant access router topology is supported by the PIM stub feature. By using a nonredundant topology, the PIM passive interface assumes that it is the only interface and designated router on that access domain.

**Figure 1: PIM Stub Router Configuration**

In the following figure, Device A routed uplink port 25 is connected to the router and PIM stub routing is enabled on the VLAN 100 interfaces and on Host 3. This configuration allows the directly connected hosts to receive traffic from multicast source



### Related Topics

[Enabling PIM Stub Routing \(CLI\)](#), on page 14

[Example: Enabling PIM Stub Routing](#), on page 44

## IGMP Helper

PIM stub routing moves routed traffic closer to the end user and reduces network traffic. You can also reduce traffic by configuring a stub router (device) with the IGMP helper feature.

You can configure a stub router (device) with the **ip igmp helper help-address** interface configuration command to enable the device to send reports to the next-hop interface. Hosts that are not directly connected to a downstream router can then join a multicast group sourced from an upstream network. The IGMP packets from a host wanting to join a multicast stream are forwarded upstream to the next-hop device when this feature is configured. When the upstream central router receives the helper IGMP reports or leaves, it adds or removes the interfaces from its outgoing interface list for that group.

For complete syntax and usage information for the **ip igmp helper-address** command, see the *IP Multicast Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*.

## Auto-RP

The PIM-SM protocols require the presence of a rendezvous point (RP) in the network. An RP acts as the meeting place for sources and receivers of multicast data. If a static RP configuration is used, then the configuration needs to be applied on all the routers in the multicast network. To automate this process, the Auto-RP protocol was devised.

This Cisco proprietary feature eliminates the need to manually configure the RP information in every router and multilayer device in the network. For Auto-RP to work, you configure a Cisco router or multilayer device as the mapping agent. It uses IP multicast to learn which routers or devices in the network are possible candidate RPs to receive candidate RP announcements. Candidate RPs periodically send multicast RP-announce messages to a particular group or group range to announce their availability.

Mapping agents listen to these candidate RP announcements and use the information to create entries in their group-to-RP mapping caches. Only one mapping cache entry is created for any group-to-RP range received, even if multiple candidate RPs are sending RP announcements for the same range. As the RP-announce messages arrive, the mapping agent selects the router or device with the highest IP address as the active RP and stores this RP address in the group-to-RP mapping cache.

Mapping agents periodically multicast the contents of their group-to-RP mapping caches. Thus, all routers and devices automatically discover which RP to use for the groups that they support. If a router or device fails to receive RP-discovery messages and the group-to-RP mapping information expires, it changes to a statically configured RP that was defined with the **ip pim rp-address** global configuration command. If no statically configured RP exists, the router or device changes the group to dense-mode operation.

Multiple RPs serve different group ranges or serve as hot backups of each other.

#### Related Topics

[Setting Up Auto-RP in a New Internetwork \(CLI\)](#), on page 19

[Example: Configuring Auto-RP](#), on page 45

## The Role of Auto-RP in a PIM Network

Auto-RP automates the distribution of group-to-rendezvous point (RP) mappings in a PIM network. To make Auto-RP work, a device must be designated as an RP mapping agent, which receives the RP announcement messages from the RPs and arbitrates conflicts. The RP mapping agent then sends the consistent group-to-RP mappings to all other devices by way of dense mode flooding.

Thus, all routers automatically discover which RP to use for the groups they support. The Internet Assigned Numbers Authority (IANA) has assigned two group addresses, 224.0.1.39 and 224.0.1.40, for Auto-RP.

The mapping agent receives announcements of intention to become the RP from Candidate-RPs. The mapping agent then announces the winner of the RP election. This announcement is made independently of the decisions by the other mapping agents.

#### Related Topics

[Configuring Sparse Mode with Auto-RP\(CLI\)](#), on page 34

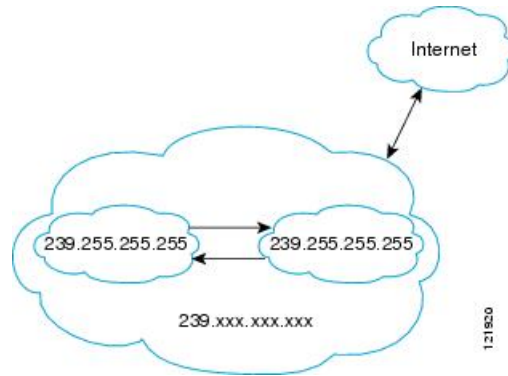
[Example: Sparse Mode with Auto-RP](#), on page 45

## IP Multicast Boundary

As shown in the figure, address scoping defines domain boundaries so that domains with RPs that have the same IP address do not leak into each other. Scoping is performed on the subnet boundaries within large domains and on the boundaries between the domain and the Internet.



Figure 2: Address Scoping at Boundaries



You can set up an administratively scoped boundary on an interface for multicast group addresses using the **ip multicast boundary** command with the *access-list* argument. A standard access list defines the range of addresses affected. When a boundary is set up, no multicast data packets are allowed to flow across the boundary from either direction. The boundary allows the same multicast group address to be reused in different administrative domains.

The Internet Assigned Numbers Authority (IANA) has designated the multicast address range 239.0.0.0 to 239.255.255.255 as the administratively scoped addresses. This range of addresses can be reused in domains administered by different organizations. They would be considered local, not globally unique.

You can configure the **filter-autorp** keyword to examine and filter Auto-RP discovery and announcement messages at the administratively scoped boundary. Any Auto-RP group range announcements from the Auto-RP packets that are denied by the boundary access control list (ACL) are removed. An Auto-RP group range announcement is permitted and passed by the boundary only if all addresses in the Auto-RP group range are permitted by the boundary ACL. If any address is not permitted, the entire group range is filtered and removed from the Auto-RP message before the Auto-RP message is forwarded.

## Auto-RP Benefits

Auto-RP uses IP multicast to automate the distribution of group-to-RP mappings to all Cisco routers and multilayer devices in a PIM network. Auto-RP has these benefits:

- Easy to use multiple RPs within a network to serve different group ranges.
- Provides load splitting among different RPs and arrangement of RPs according to the location of group participants.
- Avoids inconsistent, manual RP configurations on every router and multilayer device in a PIM network, which can cause connectivity problems.

### Benefits of Auto-RP in a PIM Network

- Auto-RP allows any change to the RP designation to be configured only on the devices that are RPs, not on the leaf routers.
- Auto-RP offers the ability to scope the RP address within a domain.

## PIMv2 Bootstrap Router

PIMv2 Bootstrap Router (BSR) is another method to distribute group-to-RP mapping information to all PIM routers and multilayer devices in the network. It eliminates the need to manually configure RP information in every router and device in the network. However, instead of using IP multicast to distribute group-to-RP mapping information, BSR uses hop-by-hop flooding of special BSR messages to distribute the mapping information.

The BSR is elected from a set of candidate routers and devices in the domain that have been configured to function as BSRs. The election mechanism is similar to the root-bridge election mechanism used in bridged LANs. The BSR election is based on the BSR priority of the device contained in the BSR messages that are sent hop-by-hop through the network. Each BSR device examines the message and forwards out all interfaces only the message that has either a higher BSR priority than its BSR priority or the same BSR priority, but with a higher BSR IP address. Using this method, the BSR is elected.

The elected BSR sends BSR messages with a TTL of 1. Neighboring PIMv2 routers or multilayer devices receive the BSR message and multicast it out all other interfaces (except the one on which it was received) with a TTL of 1. In this way, BSR messages travel hop-by-hop throughout the PIM domain. Because BSR messages contain the IP address of the current BSR, the flooding mechanism enables candidate RPs to automatically learn which device is the elected BSR.

Candidate RPs send candidate RP advertisements showing the group range for which they are responsible to the BSR, which stores this information in its local candidate-RP cache. The BSR periodically advertises the contents of this cache in BSR messages to all other PIM devices in the domain. These messages travel hop-by-hop through the network to all routers and devices, which store the RP information in the BSR message in their local RP cache. The routers and devices select the same RP for a given group because they all use a common RP hashing algorithm.

### Related Topics

[Configuring Candidate BSRs \(CLI\)](#), on page 30

[Example: Configuring Candidate BSRs](#), on page 47

## PIM Domain Border

As IP multicast becomes more widespread, the chance of one PIMv2 domain bordering another PIMv2 domain increases. Because two domains probably do not share the same set of RPs, BSR, candidate RPs, and candidate BSRs, you need to constrain PIMv2 BSR messages from flowing into or out of the domain. Allowing messages to leak across the domain borders could adversely affect the normal BSR election mechanism and elect a single BSR across all bordering domains and coningle candidate RP advertisements, resulting in the election of RPs in the wrong domain.

## Multicast Forwarding and Reverse Path Check

With unicast routing, routers and multilayer devices forward traffic through the network along a single path from the source to the destination host whose IP address appears in the destination address field of the IP packet. Each router and device along the way makes a unicast forwarding decision, using the destination IP address in the packet, by looking up the destination address in the unicast routing table and forwarding the packet through the specified interface to the next hop toward the destination.

With multicasting, the source is sending traffic to an arbitrary group of hosts represented by a multicast group address in the destination address field of the IP packet. To decide whether to forward or drop an incoming

multicast packet, the router or multilayer device uses a reverse path forwarding (RPF) check on the packet as follows:

1. The router or multilayer device examines the source address of the arriving multicast packet to decide whether the packet arrived on an interface that is on the reverse path back to the source.
2. If the packet arrives on the interface leading back to the source, the RPF check is successful and the packet is forwarded to all interfaces in the outgoing interface list (which might not be all interfaces on the router).
3. If the RPF check fails, the packet is discarded.

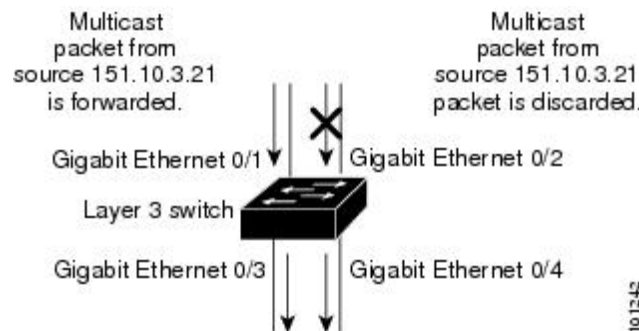
Some multicast routing protocols, such as DVMRP, maintain a separate multicast routing table and use it for the RPF check. However, PIM uses the unicast routing table to perform the RPF check.



**Note** DVMRP is not supported on the device.

**Figure 3: RPF Check**

The following figure shows port 2 receiving a multicast packet from source 151.10.3.21. The following table shows that the port on the reverse path to the source is port 1, not port 2. Because the RPF check fails, the multilayer device discards the packet. Another multicast packet from source 151.10.3.21 is received on port 1, and the routing table shows this port is on the reverse path to the source. Because the RPF check passes, the device forwards the packet to all port in the outgoing port list



**Table 1: Routing Table Example for an RPF Check**

Network	Port
151.10.0.0/16	Gigabit Ethernet 1/0/1
198.14.32.0/32	Gigabit Ethernet 1/0/3
204.1.16.0/24	Gigabit Ethernet 1/0/4

PIM uses both source trees and RP-rooted shared trees to forward datagrams. The RPF check is performed differently for each:

- If a PIM router or multilayer device has a source-tree state (that is, an (S, G) entry is present in the multicast routing table), it performs the RPF check against the IP address of the source of the multicast packet.

- If a PIM router or multilayer device has a shared-tree state (and no explicit source-tree state), it performs the RPF check on the RP address (which is known when members join the group).

Sparse-mode PIM uses the RPF lookup function to decide where it needs to send joins and prunes:

- (S, G) joins (which are source-tree states) are sent toward the source.
- (\*, G) joins (which are shared-tree states) are sent toward the RP.



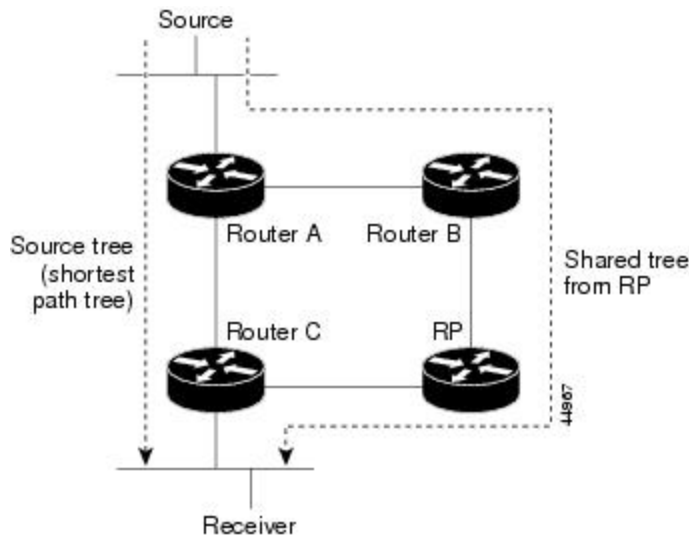
**Note** DVMRP is not supported on the device.

## PIM Shared Tree and Source Tree

By default, members of a group receive data from senders to the group across a single data-distribution tree rooted at the RP.

**Figure 4: Shared Tree and Source Tree (Shortest-Path Tree)**

The following figure shows this type of shared-distribution tree. Data from senders is delivered to the RP for distribution to group members joined to the shared tree.



If the data rate warrants, leaf routers (routers without any downstream connections) on the shared tree can use the data distribution tree rooted at the source. This type of distribution tree is called a shortest-path tree or source tree. By default, the software devices to a source tree upon receiving the first data packet from a source.

This process describes the move from a shared tree to a source tree:

1. A receiver joins a group; leaf Router C sends a join message toward the RP.
2. The RP puts a link to Router C in its outgoing interface list.
3. A source sends data; Router A encapsulates the data in a register message and sends it to the RP.

4. The RP forwards the data down the shared tree to Router C and sends a join message toward the source. At this point, data might arrive twice at Router C, once encapsulated and once natively.
5. When data arrives natively (unencapsulated) at the RP, it sends a register-stop message to Router A.
6. By default, reception of the first data packet prompts Router C to send a join message toward the source.
7. When Router C receives data on (S, G), it sends a prune message for the source up the shared tree.
8. The RP deletes the link to Router C from the outgoing interface of (S, G). The RP triggers a prune message toward the source.

Join and prune messages are sent for sources and RPs. They are sent hop-by-hop and are processed by each PIM device along the path to the source or RP. Register and register-stop messages are not sent hop-by-hop. They are sent by the designated router that is directly connected to a source and are received by the RP for the group.

Multiple sources sending to groups use the shared tree. You can configure the PIM device to stay on the shared tree.

The change from shared to source tree happens when the first data packet arrives at the last-hop router. This change depends upon the threshold that is configured by using the **ip pim spt-threshold** global configuration command.

The shortest-path tree requires more memory than the shared tree but reduces delay. You may want to postpone its use. Instead of allowing the leaf router to immediately move to the shortest-path tree, you can specify that the traffic must first reach a threshold.

You can configure when a PIM leaf router should join the shortest-path tree for a specified group. If a source sends at a rate greater than or equal to the specified kbps rate, the multilayer switch triggers a PIM join message toward the source to construct a source tree (shortest-path tree). If the traffic rate from the source drops below the threshold value, the leaf router switches back to the shared tree and sends a prune message toward the source.

You can specify to which groups the shortest-path tree threshold applies by using a group list (a standard access list). If a value of 0 is specified or if the group list is not used, the threshold applies to all groups.

## Default PIM Routing Configuration

This table displays the default PIM routing configuration for the device.

**Table 2: Default Multicast Routing Configuration**

Feature	Default Setting
Multicast routing	Disabled on all interfaces.
PIM version	Version 2.
PIM mode	No mode is defined.
PIM stub routing	None configured.
PIM RP address	None configured.
PIM domain border	Disabled.

Feature	Default Setting
PIM multicast boundary	None.
Candidate BSRs	Disabled.
Candidate RPs	Disabled.
Shortest-path tree threshold rate	0 kb/s.
PIM router query message interval	30 seconds.

# How to Configure PIM

## Enabling PIM Stub Routing (CLI)

This procedure is optional.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip pim passive**
5. **end**
6. **show ip pim interface**
7. **show ip igmp groups detail**
8. **show ip mroute**
9. **show running-config**
10. **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Device&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Device# configure terminal</pre>	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>interface</b> <i>interface-id</i> <b>Example:</b> <pre>Device(config)# interface gigabitethernet 1/0/1</pre>	<p>Specifies the interface on which you want to enable PIM stub routing, and enters interface configuration mode.</p> <p>The specified interface must be one of the following:</p> <ul style="list-style-type: none"> <li>• A routed port—A physical port that has been configured as a Layer 3 port by entering the <b>no switchport</b> interface configuration command.</li> </ul> <p>You will also need to enable IP PIM sparse-dense-mode on the interface, and join the interface as a statically connected member to an IGMP static group.</p> <ul style="list-style-type: none"> <li>• An SVI—A VLAN interface created by using the <b>interface vlan</b> <i>vlan-id</i> global configuration command.</li> </ul> <p>You will also need to enable IP PIM sparse-dense-mode on the VLAN, join the VLAN as a statically connected member to an IGMP static group, and then enable IGMP snooping on the VLAN, the IGMP static group, and physical interface.</p> <p>These interfaces must have IP addresses assigned to them.</p>
<b>Step 4</b>	<b>ip pim passive</b> <b>Example:</b> <pre>Device(config-if)# ip pim passive</pre>	Configures the PIM stub feature on the interface.
<b>Step 5</b>	<b>end</b> <b>Example:</b> <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 6</b>	<b>show ip pim interface</b> <b>Example:</b> <pre>Device# show ip pim interface</pre>	(Optional) Displays the PIM stub that is enabled on each interface.
<b>Step 7</b>	<b>show ip igmp groups detail</b> <b>Example:</b> <pre>Device# show ip igmp groups detail</pre>	(Optional) Displays the interested clients that have joined the specific multicast source group.
<b>Step 8</b>	<b>show ip mroute</b> <b>Example:</b>	(Optional) Displays the IP multicast routing table.

	Command or Action	Purpose
	Device# <code>show ip mroute</code>	
<b>Step 9</b>	<b>show running-config</b> <b>Example:</b> Device# <code>show running-config</code>	Verifies your entries.
<b>Step 10</b>	<b>copy running-config startup-config</b> <b>Example:</b> Device# <code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

**Related Topics**

[PIM Stub Routing](#), on page 6

[Example: Enabling PIM Stub Routing](#), on page 44

## Configuring a Rendezvous Point

You must have a rendezvous point (RP), if the interface is in sparse-dense mode and if you want to handle the group as a sparse group. You can use these methods:

- By manually assigning an RP to multicast groups.
- As a standalone, Cisco-proprietary protocol separate from PIMv1, which includes:
  - Setting up Auto-RP in a new internetwork
  - Adding Auto-RP to an existing sparse-mode cloud
  - Preventing join messages to false RPs
  - Filtering incoming RP announcement messages
- By using a standards track protocol in the Internet Engineering Task Force (IETF), which includes configuring PIMv2 BSR .

**Note**

You can use Auto-RP, BSR, or a combination of both, depending on the PIM version that you are running and the types of routers in your network. For information about working with different PIM versions in your network, see the PIMv1 and PIMv2 Interoperability section.

### Manually Assigning an RP to Multicast Groups (CLI)

If the rendezvous point (RP) for a group is learned through a dynamic mechanism (such as Auto-RP or BSR), you need not perform this task for that RP.



Senders of multicast traffic announce their existence through register messages received from the source first-hop router (designated router) and forwarded to the RP. Receivers of multicast packets use RPs to join a multicast group by using explicit join messages.



**Note** RPs are not members of the multicast group; they serve as a *meeting place* for multicast sources and group members.

You can configure a single RP for multiple groups defined by an access list. If there is no RP configured for a group, the multilayer device responds to the group as dense and uses the dense-mode PIM techniques.

This procedure is optional.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip pim rp-address *ip-address* [*access-list-number*] [*override*]**
4. **access-list *access-list-number* {deny | permit} *source* [*source-wildcard*]**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> <pre>Device&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b> <b>Example:</b> <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	<b>ip pim rp-address <i>ip-address</i> [<i>access-list-number</i>] [<i>override</i>]</b> <b>Example:</b> <pre>Device(config)# ip pim rp-address 10.1.1.1 20 override</pre>	Configures the address of a PIM RP. By default, no PIM RP address is configured. You must configure the IP address of RPs on all routers and multilayer devices (including the RP). <b>Note</b> If there is no RP configured for a group, the device treats the group as dense, using the dense-mode PIM techniques. A PIM device can be an RP for more than one group. Only one RP address can be used at a time within a PIM domain.

	Command or Action	Purpose
		<p>The access list conditions specify for which groups the device is an RP.</p> <ul style="list-style-type: none"> <li>For <i>ip-address</i>, enter the unicast address of the RP in dotted-decimal notation.</li> <li>(Optional) For <i>access-list-number</i>, enter an IP standard access list number from 1 to 99. If no access list is configured, the RP is used for all groups.</li> <li>(Optional) The <b>override</b> keyword indicates that if there is a conflict between the RP configured with this command and one learned by Auto-RP or BSR, the RP configured with this command prevails.</li> </ul>
<b>Step 4</b>	<p><b>access-list</b> <i>access-list-number</i> {<b>deny</b>   <b>permit</b>} <i>source</i> [<i>source-wildcard</i>]</p> <p><b>Example:</b></p> <pre>Device(config)# access-list 25 permit 10.5.0.1 255.224.0.0</pre>	<p>Creates a standard access list, repeating the command as many times as necessary.</p> <ul style="list-style-type: none"> <li>For <i>access-list-number</i>, enter the access list number specified in Step 2.</li> <li>The <b>deny</b> keyword denies access if the conditions are matched.</li> <li>The <b>permit</b> keyword permits access if the conditions are matched.</li> <li>For <i>source</i>, enter the multicast group address for which the RP should be used.</li> <li>(Optional) For <i>source-wildcard</i>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</li> </ul> <p>The access list is always terminated by an implicit deny statement for everything.</p>
<b>Step 5</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 6</b>	<p><b>show running-config</b></p> <p><b>Example:</b></p> <pre>Device# show running-config</pre>	Verifies your entries.
<b>Step 7</b>	<p><b>copy running-config startup-config</b></p> <p><b>Example:</b></p>	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	Device# <code>copy running-config startup-config</code>	

## Setting Up Auto-RP in a New Internetwork (CLI)

If you are setting up Auto-RP in a new internetwork, you do not need a default RP because you configure all the interfaces for sparse-dense mode.



**Note** Omit Step 3 in the following procedure, if you want to configure a PIM router as the RP for the local group.

### SUMMARY STEPS

1. `enable`
2. `show running-config`
3. `configure terminal`
4. `ip pim send-rp-announce interface-id scope ttl group-list access-list-number interval seconds`
5. `access-list access-list-number {deny | permit} source [source-wildcard]`
6. `ip pim send-rp-discovery scope ttl`
7. `end`
8. `show running-config`
9. `show ip pim rp mapping`
10. `show ip pim rp`
11. `copy running-config startup-config`

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b>  Device> <code>enable</code>	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>show running-config</b>  <b>Example:</b>  Device# <code>show running-config</code>	Verifies that a default RP is already configured on all PIM devices and the RP in the sparse-mode network. It was previously configured with the <code>ip pim rp-address</code> global configuration command.  <b>Note</b> This step is not required for sparse-dense-mode environments.  The selected RP should have good connectivity and be available across the network. Use this RP for the global groups (for example, 224.x.x.x and other global groups). Do not reconfigure the group address range that this RP

	Command or Action	Purpose
		serves. RPs dynamically discovered through Auto-RP take precedence over statically configured RPs. Assume that it is desirable to use a second RP for the local groups.
<b>Step 3</b>	<b>configure terminal</b> <b>Example:</b> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 4</b>	<b>ip pim send-rp-announce interface-id scope ttl group-list access-list-number interval seconds</b> <b>Example:</b> <pre>Device(config)# ip pim send-rp-announce gigabitethernet 1/0/5 scope 20 group-list 10 interval 120</pre>	<p>Configures another PIM device to be the candidate RP for local groups.</p> <ul style="list-style-type: none"> <li>For <i>interface-id</i>, enter the interface type and number that identifies the RP address. Valid interfaces include physical ports, port channels, and VLANs.</li> <li>For <b>scope ttl</b>, specify the time-to-live value in hops. Enter a hop count that is high enough so that the RP-announce messages reach all mapping agents in the network. There is no default setting. The range is 1 to 255.</li> <li>For <b>group-list access-list-number</b>, enter an IP standard access list number from 1 to 99. If no access list is configured, the RP is used for all groups.</li> <li>For <b>interval seconds</b>, specify how often the announcement messages must be sent. The default is 60 seconds. The range is 1 to 16383.</li> </ul>
<b>Step 5</b>	<b>access-list access-list-number {deny   permit} source [source-wildcard]</b> <b>Example:</b> <pre>Device(config)# access-list 10 permit 10.10.0.0</pre>	<p>Creates a standard access list, repeating the command as many times as necessary.</p> <ul style="list-style-type: none"> <li>For <i>access-list-number</i>, enter the access list number specified in Step 3.</li> <li>The <b>deny</b> keyword denies access if the conditions are matched.</li> <li>The <b>permit</b> keyword permits access if the conditions are matched.</li> <li>For <i>source</i>, enter the multicast group address range for which the RP should be used.</li> <li>(Optional) For <i>source-wildcard</i>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</li> </ul> <p><b>Note</b> Recall that the access list is always terminated by an implicit deny statement for everything.</p>

	Command or Action	Purpose
<b>Step 6</b>	<b>ip pim send-rp-discovery scope <i>t</i></b> <b>Example:</b> <pre>Device(config)# ip pim send-rp-discovery scope 50</pre>	<p>Finds a device whose connectivity is not likely to be interrupted, and assign it the role of RP-mapping agent.</p> <p>For <b>scope <i>t</i></b>, specify the time-to-live value in hops to limit the RP discovery packets. All devices within the hop count from the source device receive the Auto-RP discovery messages. These messages tell other devices which group-to-RP mapping to use to avoid conflicts (such as overlapping group-to-RP ranges). There is no default setting. The range is 1 to 255.</p>
<b>Step 7</b>	<b>end</b> <b>Example:</b> <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 8</b>	<b>show running-config</b> <b>Example:</b> <pre>Device# show running-config</pre>	Verifies your entries.
<b>Step 9</b>	<b>show ip pim rp mapping</b> <b>Example:</b> <pre>Device# show ip pim rp mapping</pre>	Displays active RPs that are cached with associated multicast routing entries.
<b>Step 10</b>	<b>show ip pim rp</b> <b>Example:</b> <pre>Device# show ip pim rp</pre>	Displays the information cached in the routing table.
<b>Step 11</b>	<b>copy running-config startup-config</b> <b>Example:</b> <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

#### Related Topics

[Auto-RP](#), on page 7

[Example: Configuring Auto-RP](#), on page 45

## Adding Auto-RP to an Existing Sparse-Mode Cloud (CLI)

This section contains suggestions for the initial deployment of Auto-RP into an existing sparse-mode cloud to minimize disruption of the existing multicast infrastructure.

This procedure is optional.

## SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **configure terminal**
4. **ip pim send-rp-announce** *interface-id* **scope** *tvl* **group-list** *access-list-number* **interval** *seconds*
5. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
6. **ip pim send-rp-discovery** *scope* *tvl*
7. **end**
8. **show running-config**
9. **show ip pim rp mapping**
10. **show ip pim rp**
11. **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Device&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>show running-config</b> <b>Example:</b> <pre>Device# show running-config</pre>	Verifies that a default RP is already configured on all PIM devices and the RP in the sparse-mode network. It was previously configured with the <b>ip pim rp-address</b> global configuration command. <b>Note</b> This step is not required for sparse-dense-mode environments. The selected RP should have good connectivity and be available across the network. Use this RP for the global groups (for example, 224.x.x.x and other global groups). Do not reconfigure the group address range that this RP serves. RPs dynamically discovered through Auto-RP take precedence over statically configured RPs. Assume that it is desirable to use a second RP for the local groups.
<b>Step 3</b>	<b>configure terminal</b> <b>Example:</b> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 4</b>	<b>ip pim send-rp-announce</b> <i>interface-id</i> <b>scope</b> <i>tvl</i> <b>group-list</b> <i>access-list-number</i> <b>interval</b> <i>seconds</i>	Configures another PIM device to be the candidate RP for local groups.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device(config)# ip pim send-rp-announce gigabitethernet 1/0/5 scope 20 group-list 10 interval 120</pre>	<ul style="list-style-type: none"> <li>For <i>interface-id</i>, enter the interface type and number that identifies the RP address. Valid interfaces include physical ports, port channels, and VLANs.</li> <li>For <b>scope</b> <i>tvl</i>, specify the time-to-live value in hops. Enter a hop count that is high enough so that the RP-announce messages reach all mapping agents in the network. There is no default setting. The range is 1 to 255.</li> <li>For <b>group-list</b> <i>access-list-number</i>, enter an IP standard access list number from 1 to 99. If no access list is configured, the RP is used for all groups.</li> <li>For <b>interval</b> <i>seconds</i>, specify how often the announcement messages must be sent. The default is 60 seconds. The range is 1 to 16383.</li> </ul>
<b>Step 5</b>	<p><b>access-list</b> <i>access-list-number</i> {<b>deny</b>   <b>permit</b>} <i>source</i> [<i>source-wildcard</i>]</p> <p><b>Example:</b></p> <pre>Device(config)# access-list 10 permit 224.0.0.0 15.255.255.255</pre>	<p>Creates a standard access list, repeating the command as many times as necessary.</p> <ul style="list-style-type: none"> <li>For <i>access-list-number</i>, enter the access list number specified in Step 3.</li> <li>The <b>deny</b> keyword denies access if the conditions are matched.</li> <li>The <b>permit</b> keyword permits access if the conditions are matched.</li> <li>For <i>source</i>, enter the multicast group address range for which the RP should be used.</li> <li>(Optional) For <i>source-wildcard</i>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</li> </ul> <p>Recall that the access list is always terminated by an implicit deny statement for everything.</p>
<b>Step 6</b>	<p><b>ip pim send-rp-discovery scope</b> <i>tvl</i></p> <p><b>Example:</b></p> <pre>Device(config)# ip pim send-rp-discovery scope 50</pre>	<p>Finds a device whose connectivity is not likely to be interrupted, and assigns it the role of RP-mapping agent.</p> <p>For <b>scope</b> <i>tvl</i>, specify the time-to-live value in hops to limit the RP discovery packets. All devices within the hop count from the source device receive the Auto-RP discovery messages. These messages tell other devices which group-to-RP mapping to use to avoid conflicts (such as overlapping group-to-RP ranges). There is no default setting. The range is 1 to 255.</p>

	Command or Action	Purpose
		<b>Note</b> To remove the device as the RP-mapping agent, use the <b>no ip pim send-rp-discovery</b> global configuration command.
<b>Step 7</b>	<b>end</b>  <b>Example:</b>  Device(config)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 8</b>	<b>show running-config</b>  <b>Example:</b>  Device# <b>show running-config</b>	Verifies your entries.
<b>Step 9</b>	<b>show ip pim rp mapping</b>  <b>Example:</b>  Device# <b>show ip pim rp mapping</b>	Displays active RPs that are cached with associated multicast routing entries.
<b>Step 10</b>	<b>show ip pim rp</b>  <b>Example:</b>  Device# <b>show ip pim rp</b>	Displays the information cached in the routing table.
<b>Step 11</b>	<b>copy running-config startup-config</b>  <b>Example:</b>  Device# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

## Preventing Join Messages to False RPs (CLI)

Determine whether the **ip pim accept-rp** command was previously configured throughout the network by using the **show running-config** privileged EXEC command. If the **ip pim accept-rp** command is not configured on any device, this problem can be addressed later. In those routers or multilayer devices already configured with the **ip pim accept-rp** command, you must enter the command again to accept the newly advertised RP.

To accept all RPs advertised with Auto-RP and reject all other RPs by default, use the **ip pim accept-rp auto-rp** global configuration command.

This procedure is optional.

### Related Topics

[Example: Preventing Join Messages to False RPs](#), on page 46



## Filtering Incoming RP Announcement Messages (CLI)

You can add configuration commands to the mapping agents to prevent a maliciously configured router from masquerading as a candidate RP and causing problems.

This procedure is optional.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip pim rp-announce-filter rp-list *access-list-number* group-list *access-list-number***
4. **access-list *access-list-number* {deny | permit} source [*source-wildcard*]**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> <pre>Device&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b> <b>Example:</b> <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	<b>ip pim rp-announce-filter rp-list <i>access-list-number</i> group-list <i>access-list-number</i></b> <b>Example:</b> <pre>Device(config)# ip pim rp-announce-filter rp-list 10 group-list 14</pre>	Filters incoming RP announcement messages. Enter this command on each mapping agent in the network. Without this command, all incoming RP-announce messages are accepted by default. For <b>rp-list <i>access-list-number</i></b> , configure an access list of candidate RP addresses that, if permitted, is accepted for the group ranges supplied in the <b>group-list <i>access-list-number</i></b> variable. If this variable is omitted, the filter applies to all multicast groups. If more than one mapping agent is used, the filters must be consistent across all mapping agents to ensure that no conflicts occur in the group-to-RP mapping information.
Step 4	<b>access-list <i>access-list-number</i> {deny   permit} source [<i>source-wildcard</i>]</b> <b>Example:</b>	Creates a standard access list, repeating the command as many times as necessary. <ul style="list-style-type: none"> <li>• For <i>access-list-number</i>, enter the access list number specified in Step 2.</li> </ul>

	Command or Action	Purpose
	<pre>Device(config)# access-list 10 permit 10.8.1.0 255.255.224.0</pre>	<ul style="list-style-type: none"> <li>• The <b>deny</b> keyword denies access if the conditions are matched.</li> <li>• The <b>permit</b> keyword permits access if the conditions are matched.</li> <li>• Create an access list that specifies from which routers and multilayer devices the mapping agent accepts candidate RP announcements (rp-list ACL).</li> <li>• Create an access list that specifies the range of multicast groups from which to accept or deny (group-list ACL).</li> <li>• For <i>source</i>, enter the multicast group address range for which the RP should be used.</li> <li>• (Optional) For <i>source-wildcard</i>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</li> </ul> <p>The access list is always terminated by an implicit deny statement for everything.</p>
<b>Step 5</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 6</b>	<p><b>show running-config</b></p> <p><b>Example:</b></p> <pre>Device# show running-config</pre>	Verifies your entries.
<b>Step 7</b>	<p><b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

### Related Topics

[Example: Filtering Incoming RP Announcement Messages](#), on page 46

## Configuring PIMv2 BSR

The process for configuring PIMv2 BSR may involve the following optional tasks:

- Defining the PIM domain border

- Defining the IP multicast boundary
- Configuring candidate BSRs
- Configuring candidate RPs

## Defining the PIM Domain Border (CLI)

Perform the following steps to configure the PIM domain border. This procedure is optional.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip pim bsr-border**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Device&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>interface</b> <i>interface-id</i> <b>Example:</b> <pre>Device(config)# interface gigabitethernet 1/0/1</pre>	Specifies the interface to be configured, and enters interface configuration mode. The specified interface must be one of the following: <ul style="list-style-type: none"> <li>• A routed port—A physical port that has been configured as a Layer 3 port by entering the <b>no switchport</b> interface configuration command.                You will also need to enable IP PIM sparse-dense-mode on the interface, and join the interface as a statically connected member to an IGMP static group.</li> <li>• An SVI—A VLAN interface created by using the <b>interface vlan</b> <i>vlan-id</i> global configuration command.</li> </ul>

	Command or Action	Purpose
		<p>You will also need to enable IP PIM sparse-dense-mode on the VLAN, join the VLAN as a statically connected member to an IGMP static group, and then enable IGMP snooping on the VLAN, the IGMP static group, and physical interface.</p> <p>These interfaces must have IP addresses assigned to them.</p>
<b>Step 4</b>	<b>ip pim bsr-border</b> <b>Example:</b> <pre>Device(config-if)# ip pim bsr-border</pre>	<p>Defines a PIM bootstrap message boundary for the PIM domain.</p> <p>Enter this command on each interface that connects to other bordering PIM domains. This command instructs the device to neither send nor receive PIMv2 BSR messages on this interface.</p> <p><b>Note</b> To remove the PIM border, use the <b>no ip pim bsr-border</b> interface configuration command.</p>
<b>Step 5</b>	<b>end</b> <b>Example:</b> <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 6</b>	<b>show running-config</b> <b>Example:</b> <pre>Device# show running-config</pre>	Verifies your entries.
<b>Step 7</b>	<b>copy running-config startup-config</b> <b>Example:</b> <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## Defining the IP Multicast Boundary (CLI)

You define a multicast boundary to prevent Auto-RP messages from entering the PIM domain. You create an access list to deny packets destined for 224.0.1.39 and 224.0.1.40, which carry Auto-RP information.

This procedure is optional.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **deny** *source* [*source-wildcard*]
4. **interface** *interface-id*

5. **ip multicast boundary** *access-list-number*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Device&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>access-list</b> <i>access-list-number</i> <b>deny</b> <i>source</i> [ <i>source-wildcard</i> ] <b>Example:</b> <pre>Device(config)# access-list 12 deny 224.0.1.39 access-list 12 deny 224.0.1.40</pre>	Creates a standard access list, repeating the command as many times as necessary. <ul style="list-style-type: none"> <li>• For <i>access-list-number</i>, the range is 1 to 99.</li> <li>• The <b>deny</b> keyword denies access if the conditions are matched.</li> <li>• For <i>source</i>, enter multicast addresses 224.0.1.39 and 224.0.1.40, which carry Auto-RP information.</li> <li>• (Optional) For <i>source-wildcard</i>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</li> </ul> <p>The access list is always terminated by an implicit deny statement for everything.</p>
<b>Step 4</b>	<b>interface</b> <i>interface-id</i> <b>Example:</b> <pre>Device(config)# interface gigabitethernet 1/0/1</pre>	Specifies the interface to be configured, and enters interface configuration mode. <p>The specified interface must be one of the following:</p> <ul style="list-style-type: none"> <li>• A routed port—A physical port that has been configured as a Layer 3 port by entering the <b>no switchport</b> interface configuration command.</li> </ul> <p>You will also need to enable IP PIM sparse-dense-mode on the interface, and join the interface as a statically connected member to an IGMP static group.</p>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>An SVI—A VLAN interface created by using the <b>interface vlan</b> <i>vlan-id</i> global configuration command.</li> </ul> <p>You will also need to enable IP PIM sparse-dense-mode on the VLAN, join the VLAN as a statically connected member to an IGMP static group, and then enable IGMP snooping on the VLAN, the IGMP static group, and physical interface.</p> <p>These interfaces must have IP addresses assigned to them.</p>
<b>Step 5</b>	<b>ip multicast boundary</b> <i>access-list-number</i> <b>Example:</b> <pre>Device(config-if)# ip multicast boundary 12</pre>	Configures the boundary, specifying the access list you created in Step 2.
<b>Step 6</b>	<b>end</b> <b>Example:</b> <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 7</b>	<b>show running-config</b> <b>Example:</b> <pre>Device# show running-config</pre>	Verifies your entries.
<b>Step 8</b>	<b>copy running-config startup-config</b> <b>Example:</b> <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

**Related Topics**

[Example: Defining the IP Multicast Boundary to Deny Auto-RP Information](#), on page 46

**Configuring Candidate BSRs (CLI)**

You can configure one or more candidate BSRs. The devices serving as candidate BSRs should have good connectivity to other devices and be in the backbone portion of the network.

This procedure is optional.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **ip pim bsr-candidate** *interface-id* *hash-mask-length* [*priority*]

4. **end**
5. **show running-config**
6. **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Device&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>ip pim bsr-candidate <i>interface-id</i> <i>hash-mask-length</i> [<i>priority</i>]</b> <b>Example:</b> <pre>Device(config)# ip pim bsr-candidate gigabitethernet 1/0/3 28 100</pre>	Configures your device to be a candidate BSR. <ul style="list-style-type: none"> <li>• For <i>interface-id</i>, enter the interface on this device from which the BSR address is derived to make it a candidate. This interface must be enabled with PIM. Valid interfaces include physical ports, port channels, and VLANs.</li> <li>• For <i>hash-mask-length</i>, specify the mask length (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.</li> <li>• (Optional) For <i>priority</i>, enter a number from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the device with the highest IP address is selected as the BSR. The default is 0.</li> </ul>
<b>Step 4</b>	<b>end</b> <b>Example:</b> <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show running-config</b> <b>Example:</b> <pre>Device# show running-config</pre>	Verifies your entries.

	Command or Action	Purpose
<b>Step 6</b>	<b>copy running-config startup-config</b> <b>Example:</b>  Device# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

**Related Topics**

[PIMv2 Bootstrap Router](#), on page 10

[Example: Configuring Candidate BSRs](#), on page 47

**Configuring the Candidate RPs (CLI)**

You can configure one or more candidate RPs. Similar to BSRs, the RPs should also have good connectivity to other devices and be in the backbone portion of the network. An RP can serve the entire IP multicast address space or a portion of it. Candidate RPs send candidate RP advertisements to the BSR.

This procedure is optional.

**Before you begin**

When deciding which devices should be RPs, consider these options:

- In a network of Cisco routers and multilayer devices where only Auto-RP is used, any device can be configured as an RP.
- In a network that includes only Cisco PIMv2 routers and multilayer devices and with routers from other vendors, any device can be used as an RP.
- In a network of Cisco PIMv1 routers, Cisco PIMv2 routers, and routers from other vendors, configure only Cisco PIMv2 routers and multilayer devices as RPs.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **ip pim rp-candidate interface-id [group-list access-list-number]**
4. **access-list access-list-number {deny | permit} source [source-wildcard]**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b>  Device> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>



	Command or Action	Purpose
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>ip pim rp-candidate interface-id [group-list access-list-number]</b> <b>Example:</b> <pre>Device(config)# ip pim rp-candidate gigabitethernet 1/0/5 group-list 10</pre>	<p>Configures your device to be a candidate RP.</p> <ul style="list-style-type: none"> <li>For <i>interface-id</i>, specify the interface whose associated IP address is advertised as a candidate RP address. Valid interfaces include physical ports, port channels, and VLANs.</li> <li>(Optional) For <b>group-list access-list-number</b>, enter an IP standard access list number from 1 to 99. If no group-list is specified, the device is a candidate RP for all groups.</li> </ul>
<b>Step 4</b>	<b>access-list access-list-number {deny   permit} source [source-wildcard]</b> <b>Example:</b> <pre>Device(config)# access-list 10 permit 239.0.0.0 0.255.255.255</pre>	<p>Creates a standard access list, repeating the command as many times as necessary.</p> <ul style="list-style-type: none"> <li>For <i>access-list-number</i>, enter the access list number specified in Step 2.</li> <li>The <b>deny</b> keyword denies access if the conditions are matched. The <b>permit</b> keyword permits access if the conditions are matched.</li> <li>For <i>source</i>, enter the number of the network or host from which the packet is being sent.</li> <li>(Optional) For <i>source-wildcard</i>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</li> </ul> <p>The access list is always terminated by an implicit deny statement for everything.</p>
<b>Step 5</b>	<b>end</b> <b>Example:</b> <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 6</b>	<b>show running-config</b> <b>Example:</b> <pre>Device# show running-config</pre>	Verifies your entries.

	Command or Action	Purpose
<b>Step 7</b>	<b>copy running-config startup-config</b> <b>Example:</b>  Device# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

**Related Topics**

[Example: Configuring Candidate RPs](#), on page 47

## Configuring Sparse Mode with Auto-RP(CLI)

**Before you begin**

- An interface configured in sparse-dense mode is treated in either sparse mode or dense mode of operation, depending on the mode in which the multicast group operates. You must decide how to configure your interfaces.
- All access lists that are needed when Auto-RP is configured should be configured prior to beginning the configuration task.

**Note**

- If a group has no known RP and the interface is configured to be sparse-dense mode, the interface is treated as if it were in dense mode, and data is flooded over the interface. To avoid this data flooding, configure the Auto-RP listener and then configure the interface as sparse mode.
- When configuring Auto-RP, you must either configure the Auto-RP listener feature (Step 5) and specify sparse mode (Step 7) or specify sparse-dense mode (Step 8) .
- When you configure sparse-dense mode, dense mode failover may result in a network dense-mode flood. To avoid this condition, use PIM sparse mode with the Auto-RP listener feature.

Follow this procedure to configure auto-rendezvous point (Auto-RP). Auto-RP can also be optionally used with anycast RP.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **ip multicast-routing [distributed]**
4. Either perform Steps 5 through 7 or perform Steps 6 and 8.
5. **ip pim autorp listener**
6. **interface** *type number*
7. **ip pim sparse-mode**
8. **ip pim sparse-dense-mode**
9. **exit**
10. Repeat Steps 1 through 9 on all PIM interfaces.

11. **ip pim send-rp-announce** {*interface-type interface-number* | *ip-address*} **scope** *tvl-value* [**group-list** *access-list*] [**interval** *seconds*] [**bidir**]
12. **ip pim send-rp-discovery** [*interface-type interface-number*] **scope** *tvl-value* [**interval** *seconds*]
13. **ip pim rp-announce-filter** **rp-list** *access-list* **group-list** *access-list*
14. **no ip pim dm-fallback**
15. **interface** *type number*
16. **ip multicast boundary** *access-list* [**filter-autorp**]
17. **end**
18. **show ip pim autorp**
19. **show ip pim rp** [**mapping**] [*rp-address*]
20. **show ip igmp groups** [*group-name* | *group-address*] [*interface-type interface-number*] [**detail**]
21. **show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kpps*]

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Device&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>ip multicast-routing</b> [ <b>distributed</b> ] <b>Example:</b> <pre>Device(config)# ip multicast-routing</pre>	Enables IP multicast routing. <ul style="list-style-type: none"> <li>• Use the <b>distributed</b> keyword to enabled Multicast Distributed Switching.</li> </ul>
<b>Step 4</b>	Either perform Steps 5 through 7 or perform Steps 6 and 8.	--
<b>Step 5</b>	<b>ip pim autorp listener</b> <b>Example:</b> <pre>Device(config)# ip pim autorp listener</pre>	Causes IP multicast traffic for the two Auto-RP groups 209.165.201.1 and 209.165.201.22 to be PIM dense mode flooded across interfaces operating in PIM sparse mode. <ul style="list-style-type: none"> <li>• Skip this step if you are configuring sparse-dense mode in Step 8.</li> </ul>
<b>Step 6</b>	<b>interface</b> <i>type number</i> <b>Example:</b> <pre>Device(config)# interface GigabitEthernet 1/0/0</pre>	Selects an interface that is connected to hosts on which PIM can be enabled.

	Command or Action	Purpose
<b>Step 7</b>	<b>ip pim sparse-mode</b> <b>Example:</b> <pre>Device(config-if)# ip pim sparse-mode</pre>	Enables PIM sparse mode on an interface. When configuring Auto-RP in sparse mode, you must also configure the Auto-RP listener in the next step. <ul style="list-style-type: none"> <li>• Skip this step if you are configuring sparse-dense mode in Step 8.</li> </ul>
<b>Step 8</b>	<b>ip pim sparse-dense-mode</b> <b>Example:</b> <pre>Device(config-if)# ip pim sparse-dense-mode</pre>	Enables PIM sparse-dense mode on an interface. <ul style="list-style-type: none"> <li>• Skip this step if you configured sparse mode in Step 7.</li> </ul>
<b>Step 9</b>	<b>exit</b> <b>Example:</b> <pre>Device(config-if)# exit</pre>	Exits interface configuration mode and returns to global configuration mode.
<b>Step 10</b>	Repeat Steps 1 through 9 on all PIM interfaces.	--
<b>Step 11</b>	<b>ip pim send-rp-announce</b> <i>{interface-type interface-number   ip-address}</i> <b>scope</b> <i>ttl-value</i> [ <b>group-list</b> <i>access-list</i> ] [ <b>interval</b> <i>seconds</i> ] [ <b>bidir</b> ] <b>Example:</b> <pre>Device(config)# ip pim send-rp-announce loopback0 scope 31 group-list 5</pre>	Sends RP announcements out all PIM-enabled interfaces. <ul style="list-style-type: none"> <li>• Perform this step on the RP device only.</li> <li>• Use the <i>interface-type</i> and <i>interface-number</i> arguments to define which IP address is to be used as the RP address.</li> <li>• Use the <i>ip-address</i> argument to specify a directly connected IP address as the RP address.</li> </ul> <p><b>Note</b> If the <i>ip-address</i> argument is configured for this command, 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).</p> <ul style="list-style-type: none"> <li>• This example shows that the interface is enabled with a maximum of 31 hops. The IP address by which the device wants to be identified as RP is the IP address associated with loopback interface 0. Access list 5 describes the groups for which this device serves as RP.</li> </ul>
<b>Step 12</b>	<b>ip pim send-rp-discovery</b> [ <i>interface-type interface-number</i> ] <b>scope</b> <i>ttl-value</i> [ <b>interval</b> <i>seconds</i> ] <b>Example:</b> <pre>Device(config)# ip pim send-rp-discovery loopback1 scope 31</pre>	Configures the device to be an RP mapping agent. <ul style="list-style-type: none"> <li>• Perform this step on RP mapping agent devices or on combined RP/RP mapping agent devices.</li> </ul>

	Command or Action	Purpose
		<p><b>Note</b> Auto-RP allows the RP function to run separately on one device and the RP mapping agent to run on one or multiple devices. It is possible to deploy the RP and the RP mapping agent on a combined RP/RP mapping agent device.</p> <ul style="list-style-type: none"> <li>• Use the optional <i>interface-type</i> and <i>interface-number</i> arguments to define which IP address is to be used as the source address of the RP mapping agent.</li> <li>• Use the <b>scope</b> keyword and <i>ttl-value</i> argument to specify the Time-to-Live (TTL) value in the IP header of Auto-RP discovery messages.</li> <li>• Use the optional <b>interval</b> keyword and <i>seconds</i> argument to specify the interval at which Auto-RP discovery messages are sent.</li> </ul> <p><b>Note</b> Lowering the interval at which Auto-RP discovery messages are sent from the default value of 60 seconds results in more frequent floodings of the group-to-RP mappings. In some network environments, the disadvantages of lowering the interval (more control packet overhead) may outweigh the advantages (more frequent group-to-RP mapping updates).</p> <ul style="list-style-type: none"> <li>• The example shows limiting the Auto-RP discovery messages to 31 hops on loopback interface 1.</li> </ul>
<b>Step 13</b>	<p><b>ip pim rp-announce-filter rp-list <i>access-list</i> group-list <i>access-list</i></b></p> <p><b>Example:</b></p> <pre>Device(config)# ip pim rp-announce-filter rp-list 1 group-list 2</pre>	<p>Filters incoming RP announcement messages sent from candidate RPs (C-RPs) to the RP mapping agent.</p> <ul style="list-style-type: none"> <li>• Perform this step on the RP mapping agent only.</li> </ul>
<b>Step 14</b>	<p><b>no ip pim dm-fallback</b></p> <p><b>Example:</b></p> <pre>Device(config)# no ip pim dm-fallback</pre>	<p>(Optional) Prevents PIM dense mode fallback.</p> <ul style="list-style-type: none"> <li>• Skip this step if all interfaces have been configured to operate in PIM sparse mode.</li> </ul> <p><b>Note</b> The <b>no ip pim dm-fallback</b> command behavior is enabled by default if all the interfaces are configured to operate in PIM sparse mode (using the <b>ip pim sparse-mode</b> command).</p>
<b>Step 15</b>	<p><b>interface <i>type number</i></b></p> <p><b>Example:</b></p>	<p>Selects an interface that is connected to hosts on which PIM can be enabled.</p>

	Command or Action	Purpose
	Device(config)# interface gigabitethernet 1/0/0	
<b>Step 16</b>	<b>ip multicast boundary</b> <i>access-list</i> [ <b>filter-autorp</b> ] <b>Example:</b> Device(config-if)# ip multicast boundary 10 filter-autorp	Configures an administratively scoped boundary. <ul style="list-style-type: none"> <li>• Perform this step on the interfaces that are boundaries to other devices.</li> <li>• The access list is not shown in this task.</li> <li>• An access list entry that uses the <b>deny</b> keyword creates a multicast boundary for packets that match that entry.</li> </ul>
<b>Step 17</b>	<b>end</b> <b>Example:</b> Device(config-if)# end	Returns to global configuration mode.
<b>Step 18</b>	<b>show ip pim autorp</b> <b>Example:</b> Device# show ip pim autorp	(Optional) Displays the Auto-RP information.
<b>Step 19</b>	<b>show ip pim rp</b> [ <b>mapping</b> ] [ <i>rp-address</i> ] <b>Example:</b> Device# show ip pim rp mapping	(Optional) Displays RPs known in the network and shows how the device learned about each RP.
<b>Step 20</b>	<b>show ip igmp groups</b> [ <i>group-name</i>   <i>group-address</i>   <i>interface-type interface-number</i> ] [ <b>detail</b> ] <b>Example:</b> Device# show ip igmp groups	(Optional) Displays the multicast groups having receivers that are directly connected to the device and that were learned through Internet Group Management Protocol (IGMP). <ul style="list-style-type: none"> <li>• A receiver must be active on the network at the time that this command is issued in order for receiver information to be present on the resulting display.</li> </ul>
<b>Step 21</b>	<b>show ip mroute</b> [ <i>group-address</i>   <i>group-name</i> ] [ <i>source-address</i>   <i>source-name</i> ] [ <i>interface-type interface-number</i> ] [ <b>summary</b> ] [ <b>count</b> ] [ <b>active kbps</b> ] <b>Example:</b> Device# show ip mroute cbone-audio	(Optional) Displays the contents of the IP multicast routing (mroute) table.

### Related Topics

[The Role of Auto-RP in a PIM Network](#), on page 8

[Example: Sparse Mode with Auto-RP](#) , on page 45

## Delaying the Use of PIM Shortest-Path Tree (CLI)

Perform these steps to configure a traffic rate threshold that must be reached before multicast routing is switched from the source tree to the shortest-path tree.

This procedure is optional.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
4. **ip pim spt-threshold** {*kbits* | **infinity**} [**group-list** *access-list-number*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b>  Device> <b>enable</b>	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b>  Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>access-list</b> <i>access-list-number</i> { <b>deny</b>   <b>permit</b> } <i>source</i> [ <i>source-wildcard</i> ]  <b>Example:</b>  Device(config)# <b>access-list 16 permit 225.0.0.0 0.255.255.255</b>	Creates a standard access list.  <ul style="list-style-type: none"> <li>• For <i>access-list-number</i>, the range is 1 to 99.</li> <li>• The <b>deny</b> keyword denies access if the conditions are matched.</li> <li>• The <b>permit</b> keyword permits access if the conditions are matched.</li> <li>• For <i>source</i>, specify the multicast group to which the threshold will apply.</li> <li>• (Optional) For <i>source-wildcard</i>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</li> </ul> The access list is always terminated by an implicit deny statement for everything.

	Command or Action	Purpose
<b>Step 4</b>	<b>ip pim spt-threshold</b> { <i>kbits</i>   <b>infinity</b> } [ <b>group-list</b> <i>access-list-number</i> ]  <b>Example:</b>  <pre>Device(config)# ip pim spt-threshold infinity group-list 16</pre>	<p>Specifies the threshold that must be reached before moving to shortest-path tree (spt).</p> <ul style="list-style-type: none"> <li>For <i>kbits</i>, specify the traffic rate in kilobits per second. The default is 0 kbps.</li> </ul> <p><b>Note</b> Because of device hardware limitations, 0 kbps is the only valid entry even though the range is 0 to 4294967.</p> <ul style="list-style-type: none"> <li>Specify <b>infinity</b> if you want all sources for the specified group to use the shared tree, never switching to the source tree.</li> <li>(Optional) For <b>group-list</b> <i>access-list-number</i>, specify the access list created in Step 2. If the value is 0 or if the group list is not used, the threshold applies to all groups.</li> </ul>
<b>Step 5</b>	<b>end</b>  <b>Example:</b>  <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 6</b>	<b>show running-config</b>  <b>Example:</b>  <pre>Device# show running-config</pre>	Verifies your entries.
<b>Step 7</b>	<b>copy running-config startup-config</b>  <b>Example:</b>  <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## Modifying the PIM Router-Query Message Interval (CLI)

PIM routers and multilayer devices send PIM router-query messages to find which device will be the designated router (DR) for each LAN segment (subnet). The DR is responsible for sending IGMP host-query messages to all hosts on the directly connected LAN.

With PIM DM operation, the DR has meaning only if IGMPv1 is in use. IGMPv1 does not have an IGMP querier election process, so the elected DR functions as the IGMP querier. With PIM-SM operation, the DR is the device that is directly connected to the multicast source. It sends PIM register messages to notify the RP that multicast traffic from a source needs to be forwarded down the shared tree. In this case, the DR is the device with the highest IP address.

This procedure is optional.



## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip pim query-interval** *seconds*
5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Device&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>interface</b> <i>interface-id</i> <b>Example:</b> <pre>Device(config)# interface gigabitethernet 1/0/1</pre>	Specifies the interface to be configured, and enters interface configuration mode. The specified interface must be one of the following: <ul style="list-style-type: none"> <li>• A routed port—A physical port that has been configured as a Layer 3 port by entering the <b>no switchport</b> interface configuration command.                You will also need to enable IP PIM sparse-dense-mode on the interface, and join the interface as a statically connected member to an IGMP static group.</li> <li>• An SVI—A VLAN interface created by using the <b>interface vlan</b> <i>vlan-id</i> global configuration command.                You will also need to enable IP PIM sparse-dense-mode on the VLAN, join the VLAN as a statically connected member to an IGMP static group, and then enable IGMP snooping on the VLAN, the IGMP static group, and physical interface.</li> </ul> These interfaces must have IP addresses assigned to them.
<b>Step 4</b>	<b>ip pim query-interval</b> <i>seconds</i> <b>Example:</b>	Configures the frequency at which the device sends PIM router-query messages.

	Command or Action	Purpose
	Device(config-if)# <b>ip pim query-interval 45</b>	The default is 30 seconds. The range is 1 to 65535.
<b>Step 5</b>	<b>end</b>  <b>Example:</b>  Device(config)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 6</b>	<b>show ip igmp interface</b> [ <i>interface-id</i> ]  <b>Example:</b>  Device# <b>show ip igmp interface</b>	Verifies your entries.
<b>Step 7</b>	<b>copy running-config startup-config</b>  <b>Example:</b>  Device# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

## Monitoring PIM Information

Use the privileged EXEC commands in the following table to monitor your PIM configurations.

*Table 3: PIM Monitoring Commands*

Command	Purpose
<b>show ip pim all-vrfs tunnel</b> [ <i>tunnel tunnel_number</i>   <i>verbose</i> ]	Displays all VRFs.
<b>show ip pim autorp</b>	Displays global auto-RP information.
<b>show ip pim boundary</b>	Displays information about mroutes filtered by administratively scoped IPv4 multicast boundaries configured on an interface.
<b>show ip pim interface</b>	Displays information about interfaces configured for Protocol Independent Multicast (PIM).
<b>show ip pim neighbor</b>	Displays the PIM neighbor information.
<b>show ip pim rp</b> [ <i>group-name</i>   <i>group-address</i> ]	Displays RP routers associated with a sparse-mode multicast group. This command is available in all software images.

Command	Purpose
<b>show ip pim tunnel</b> [tunnel   verbose]	Displays information about Protocol Independent Multicast (PIM) tunnel interfaces
<b>show ip pim vrf</b> { word { all-vrfs   autorp   boundary   bsr-router   interface   mdt   neighbor   rp   rp-hash   tunnel } }	Displays the VPN routing/forwarding instance.
<b>show ip igmp groups detail</b>	Displays the interested clients that have joined the specific multicast source group.

## Monitoring the RP Mapping and BSR Information

Use the privileged EXEC mode in the following table to verify the consistency of group-to-RP mappings:

**Table 4: RP Mapping Monitoring Commands**

Command	Purpose
<b>show ip pim rp</b> [ hostname or IP address   <b>mapping</b> [ hostname or IP address   <b>elected</b>   <b>in-use</b> ]   <b>metric</b> [ hostname or IP address ] ]	<p>Displays all available RP mappings and metrics. This tells you how the device learns of the RP (through the BSR or the Auto-RP mechanism).</p> <ul style="list-style-type: none"> <li>• (Optional) For the <i>hostname</i>, specify the IP name of the group about which to display RPs.</li> <li>• (Optional) For the <i>IP address</i>, specify the IP address of the group about which to display RPs.</li> <li>• (Optional) Use the <b>mapping</b> keyword to display all group-to-RP mappings of which the Cisco device is aware (either configured or learned from Auto-RP).</li> <li>• (Optional) Use the <b>metric</b> keyword to display the RP RPF metric.</li> </ul>
<b>show ip pim rp-hash</b> group	Displays the RP that was selected for the specified group. That is, on a PIMv2 router or multilayer device, confirms that the same RP is the one that a PIMv1 system chooses. For <i>group</i> , enter the group address for which to display RP information.

Use the privileged EXEC commands in the following table to monitor BSR information:

**Table 5: BSR Monitoring Commands**

Command	Purpose
<b>show ip pim bsr</b>	Displays information about the elected BSR.
<b>show ip pim bsr-router</b>	Displays information about the BSRv2.

# Troubleshooting PIMv1 and PIMv2 Interoperability Problems

When debugging interoperability problems between PIMv1 and PIMv2, check these in the order shown:

1. Verify RP mapping with the **show ip pim rp-hash** privileged EXEC command, making sure that all systems agree on the same RP for the same group.
2. Verify interoperability between different versions of DRs and RPs. Make sure that the RPs are interacting with the DRs properly (by responding with register-stops and forwarding decapsulated data packets from registers).

## Configuration Examples for PIM

### Example: Enabling PIM Stub Routing

In this example, IP multicast routing is enabled, Switch A PIM uplink port 25 is configured as a routed uplink port with **sparse-dense-mode** enabled. PIM stub routing is enabled on the VLAN 100 interfaces and on Gigabit Ethernet port 20.

```
Device(config)# ip multicast-routing distributed
Device(config)# interface GigabitEthernet3/0/25
Device(config-if)# no switchport
Device(config-if)# ip address 3.1.1.2 255.255.255.0
Device(config-if)# ip pim sparse-dense-mode
Device(config-if)# exit
Device(config)# interface vlan100
Device(config-if)# ip pim passive
Device(config-if)# exit
Device(config)# interface GigabitEthernet3/0/20
Device(config-if)# ip pim passive
Device(config-if)# exit
Device(config)# interface vlan100
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# ip pim passive
Device(config-if)# exit
Device(config)# interface GigabitEthernet3/0/20
Device(config-if)# no switchport
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# ip pim passive
Device(config-if)# end
```

#### Related Topics

[Enabling PIM Stub Routing \(CLI\)](#), on page 14

[PIM Stub Routing](#), on page 6

### Example: Verifying PIM Stub Routing

To verify that PIM stub is enabled for each interface, use the **show ip pim interface** privileged EXEC command:

```

Device# show ip pim interface
Address Interface Ver/ Nbr Query DR DR
Mode Count Intvl Prior
3.1.1.2 GigabitEthernet3/0/25 v2/SD 1 30 1 3.1.1.2
100.1.1.1 Vlan100 v2/P 0 30 1 100.1.1.1
10.1.1.1 GigabitEthernet3/0/20 v2/P 0 30 1 10.1.1.1

```

## Example: Manually Assigning an RP to Multicast Groups

This example shows how to configure the address of the RP to 147.106.6.22 for multicast group 225.2.2.2 only:

```

Device(config)# access-list 1 permit 225.2.2.2 0.0.0.0
Device(config)# ip pim rp-address 147.106.6.22 1

```

## Example: Configuring Auto-RP

This example shows how to send RP announcements out all PIM-enabled interfaces for a maximum of 31 hops. The IP address of port 1 is the RP. Access list 5 describes the group for which this device serves as RP:

```

Device(config)# ip pim send-rp-announce gigabitethernet1/0/1 scope 31 group-list 5
Device(config)# access-list 5 permit 224.0.0.0 15.255.255.255

```

### Related Topics

[Setting Up Auto-RP in a New Internetwork \(CLI\)](#), on page 19

[Auto-RP](#), on page 7

## Example: Sparse Mode with Auto-RP

The following example configures sparse mode with Auto-RP:

```

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
no ip pim dm-fallback
access-list 1 permit 239.254.2.0 0.0.0.255
access-list 1 permit 239.254.3.0 0.0.0.255
.
.
.
access-list 10 permit 224.0.1.39
access-list 10 permit 224.0.1.40
access-list 10 permit 239.254.2.0 0.0.0.255
access-list 10 permit 239.254.3.0 0.0.0.255

```

### Related Topics

[The Role of Auto-RP in a PIM Network](#), on page 8

[Configuring Sparse Mode with Auto-RP\(CLI\)](#), on page 34

## Example: Defining the IP Multicast Boundary to Deny Auto-RP Information

This example shows a portion of an IP multicast boundary configuration that denies Auto-RP information:

```
Device(config)# access-list 1 deny 224.0.1.39
Device(config)# access-list 1 deny 224.0.1.40
Device(config)# access-list 1 permit all
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip multicast boundary 1
```

### Related Topics

[Defining the IP Multicast Boundary \(CLI\)](#), on page 28

## Example: Filtering Incoming RP Announcement Messages

This example shows a sample configuration on an Auto-RP mapping agent that is used to prevent candidate RP announcements from being accepted from unauthorized candidate RPs:

```
Device(config)# ip pim rp-announce-filter rp-list 10 group-list 20
Device(config)# access-list 10 permit host 172.16.5.1
Device(config)# access-list 10 permit host 172.16.2.1
Device(config)# access-list 20 deny 239.0.0.0 0.0.255.255
Device(config)# access-list 20 permit 224.0.0.0 15.255.255.255
```

The mapping agent accepts candidate RP announcements from only two devices, 172.16.5.1 and 172.16.2.1. The mapping agent accepts candidate RP announcements from these two devices only for multicast groups that fall in the group range of 224.0.0.0 to 239.255.255.255. The mapping agent does not accept candidate RP announcements from any other devices in the network. Furthermore, the mapping agent does not accept candidate RP announcements from 172.16.5.1 or 172.16.2.1 if the announcements are for any groups in the 239.0.0.0 through 239.255.255.255 range. This range is the administratively scoped address range.

### Related Topics

[Filtering Incoming RP Announcement Messages \(CLI\)](#), on page 25

## Example: Preventing Join Messages to False RPs

If all interfaces are in sparse mode, use a default-configured RP to support the two well-known groups 224.0.1.39 and 224.0.1.40. Auto-RP uses these two well-known groups to collect and distribute RP-mapping information. When this is the case and the **ip pim accept-rp auto-rp** command is configured, another **ip pim accept-rp** command accepting the RP must be configured as follows:

```
Device(config)# ip pim accept-rp 172.10.20.1 1
Device(config)# access-list 1 permit 224.0.1.39
Device(config)# access-list 1 permit 224.0.1.40
```

### Related Topics

[Preventing Join Messages to False RPs \(CLI\)](#), on page 24

## Example: Configuring Candidate BSRs

This example shows how to configure a candidate BSR, which uses the IP address 172.21.24.18 on a port as the advertised BSR address, uses 30 bits as the hash-mask-length, and has a priority of 10.

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# ip address 172.21.24.18 255.255.255.0
Device(config-if)# ip pim sparse-mode
Device(config-if)# ip pim bsr-candidate gigabitethernet1/0/2 30 10
```

### Related Topics

[Configuring Candidate BSRs \(CLI\)](#), on page 30

[PIMv2 Bootstrap Router](#), on page 10

## Example: Configuring Candidate RPs

This example shows how to configure the device 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 a port. That RP is responsible for the groups with the prefix 239.

```
Device(config)# ip pim rp-candidate gigabitethernet1/0/2 group-list 4
Device(config)# access-list 4 permit 239.0.0.0 0.255.255.255
```

### Related Topics

[Configuring the Candidate RPs \(CLI\)](#), on page 32

## Where to Go Next for PIM

You can configure the following:

- IGMP
- Wireless Multicast
- SSM
- IP Multicast Routing
- Service Discovery Gateway

You can also review the following IP Multicast Optimization processes for your configuration:

- Optimizing PIM Sparse Mode in a Large IP Multicast Deployment
- Multicast Subsecond Convergence
- IP Multicast Load Splitting across Equal-Cost Paths
- SSM Channel Based Filtering for Multicast
- PIM Dense Mode State Refresh
- IGMP State Limit

# Additional References

## Related Documents

Related Topic	Document Title
PIM is defined in RFC 4601 and in these Internet Engineering Task Force (IETF) Internet drafts.	<ul style="list-style-type: none"> <li>• <i>Protocol Independent Multicast (PIM): Motivation and Architecture</i></li> <li>• <i>Protocol Independent Multicast (PIM), Dense Mode Protocol Specification</i></li> <li>• <i>Protocol Independent Multicast (PIM), Sparse Mode Protocol Specification</i></li> <li>• <i>draft-ietf-idmr-igmp-v2-06.txt, Internet Group Management Protocol, Version 2</i></li> <li>• <i>draft-ietf-pim-v2-dm-03.txt, PIM Version 2 Dense Mode</i></li> </ul>
For complete syntax and usage information for the commands used in this chapter.	<i>IP Multicast Routing Command Reference (Catalyst 3650 Switches) Command Reference (Catalyst 9500 Series Switches) Command Reference (Catalyst 9300 Series Switches)</i>
IGMP Helper command syntax and usage information.	<i>IP Multicast Routing Command Reference (Catalyst 3650 Switches)</i>
Multicast Source Discovery Protocol (MSDP)	<i>IP Routing: Protocol-Independent Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)</i>
Enhanced Interior Gateway Routing Protocol (EIGRP) stub routing	<i>IP Routing: EIGRP Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)</i>
Open Shortest Path First (OSPF) stub routing	<i>IP Routing: OSPF Configuration Guide, Cisco IOS XE 3SE (Catalyst 3650 Switches)</i>
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
Cisco IOS IP SLAs commands	<a href="#">Cisco IOS IP Multicast Command Reference</a>
Overview of the IP multicast technology area	“ IP Multicast Technology Overview ” module
Concepts, tasks, and examples for configuring an IP multicast network using PIM	“ Configuring a Basic IP Multicast Network ” module

## Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	<a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a>



**Standards and RFCs**

Standard/RFC	Title
RFC 4601	<i>Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification</i>

**MIBs**

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**Technical Assistance**

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## Feature History and Information for PIM

Release	Modification
Cisco IOS XE 3.3SE	This feature was introduced.

