# Configuring PIM



## 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.

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

## Prerequisites for PIM

- Before you begin the PIM configuration process, decide which PIM mode to use. This is based on the applications you intend to support on your network. Use the following guidelines:
  - In general, if the application is one-to-many or many-to-many in nature, then PIM-SM can be used successfully.
  - For optimal one-to-many application performance, SSM is appropriate but requires IGMP version 3 support.
- Before you configure PIM stub routing, check that you have met these conditions:

- 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.
- You must also configure Enhanced Interior Gateway Routing Protocol (EIGRP) stub routing on the switch.
- 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.

# Restrictions for PIM

## PIMv1 and PIMv2 Interoperability

To avoid misconfiguring multicast routing on your switch, 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 switches within one network. Internally, all routers and multilayer switches 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 switches 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 switches.

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 switch in the group. Not all routers and switches in the domain use the PIMv2 hash function to select multiple RPs.

Dense-mode groups in a mixed PIMv1 and PIMv2 region need no special configuration; they automatically interoperate.

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.

### Related Topics

PIM Versions, on page 7

# Restrictions for Configuring PIM Stub Routing

- To use the PIM stub routing feature, the switch or stack master or active switch can be running the IP base image. The IP base image contains only PIM stub routing.The IP services image contains complete multicast routing.
- 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.
- In a network using PIM stub routing, the only allowable route for IP traffic to the user is through a switch 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.

### Related Topics

Enabling PIM Stub Routing , on page 22
PIM Stub Routing, on page 7

# Restrictions for Configuring Auto-RP and BSR

Take into consideration your network configuration, and the following restrictions when configuring Auto-RP and BSR:

### Restrictions for Configuring Auto-RP

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

- 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 Configuring BSR

The following are the restrictions for configuring BSR (if used in your network configuration):

- Configure the candidate BSRs as the RP-mapping agents for Auto-RP.
- For group prefixes advertised through Auto-RP, the PIMv2 BSR mechanism should not advertise a subrange of these group prefixes served by a different set of RPs. In a mixed PIMv1 and PIMv2 domain, have backup RPs serve the same group prefixes. This prevents the PIMv2 DRs from selecting a different RP from those PIMv1 DRs, due to the longest match lookup in the RP-mapping database.

### Restrictions and Guidelines 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 switches, 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 switches 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 switches in your network. Therefore, if your network has a PIMv1 device in it and only Cisco routers and multilayer switches, 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 switch. 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 switches, 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.

### Related Topics

Setting Up Auto-RP in a New Internetwork , on page 26
Auto-RP, on page 9
Configuring Candidate BSRs , on page 40
Bootstrap Router, on page 10

# Information About PIM

## Protocol Independent Multicast Overview

The Protocol Independent Multicast (PIM) protocol maintains the current IP multicast service mode of receiver-initiated membership. PIM is not dependent on a specific unicast routing protocol; it is IP routing protocol independent and can leverage whichever unicast routing protocols are used to populate the unicast routing table, including Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and static routes. PIM uses unicast routing information to perform the multicast forwarding function.

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. Unlike other routing protocols, PIM does not send and receive routing updates between routers.

PIM is defined in RFC 4601, Protocol Independent Multicast - Sparse Mode (PIM-SM)

PIM can operate in dense mode or sparse mode. The router can also handle both sparse groups and dense groups at the same time (sparse-dense mode). The mode determines how the router populates its multicast routing table and how the router forwards multicast packets it receives from its directly connected LANs.

For information about PIM forwarding (interface) modes, see the following sections:

## PIM Dense Mode

PIM dense mode (PIM-DM) uses a push model to flood multicast traffic to every corner of the network. This push model is a method for delivering data to the receivers without the receivers requesting the data. This method is efficient in certain deployments in which there are active receivers on every subnet in the network.

In dense mode, a router assumes that all other routers want to forward multicast packets for a group. If a router receives a multicast packet and has no directly connected members or PIM neighbors present, a prune message is sent back to the source. Subsequent multicast packets are not flooded to this router on this pruned branch. PIM builds source-based multicast distribution trees.

PIM-DM initially floods multicast traffic throughout the network. Routers that have no downstream neighbors prune back the unwanted traffic. This process repeats every 3 minutes.

Routers accumulate state information by receiving data streams through the flood and prune mechanism. These data streams contain the source and group information so that downstream routers can build up their multicast forwarding table. PIM-DM supports only source trees--that is, (S,G) entries--and cannot be used to build a shared distribution tree.

**Note** Dense mode is not often used and its use is not recommended. For this reason it is not specified in the configuration tasks in related modules.

## PIM Sparse Mode

PIM sparse mode (PIM-SM) uses a pull model to deliver multicast traffic. Only network segments with active receivers that have explicitly requested the data will receive the traffic.

Unlike dense mode interfaces, sparse mode interfaces are added to the multicast routing table only when periodic Join messages are received from downstream routers, or when a directly connected member is on the interface. When forwarding from a LAN, sparse mode operation occurs if an RP is known for the group. If so, the packets are encapsulated and sent toward the RP. When no RP is known, the packet is flooded in a dense mode fashion. If the multicast traffic from a specific source is sufficient, the first hop router of the receiver may send Join messages toward the source to build a source-based distribution tree.

PIM-SM distributes information about active sources by forwarding data packets on the shared tree. Because PIM-SM uses shared trees (at least, initially), it requires the use of a rendezvous point (RP). The RP must be administratively configured in the network. See the Rendezvous Points, on page 9 section for more information.

In sparse mode, a router assumes that other routers do not want to forward multicast packets for a group, unless there is an explicit request for the traffic. When hosts join a multicast group, the directly connected routers send PIM Join messages toward the RP. The RP keeps track of multicast groups. Hosts that send multicast packets are registered with the RP by the first hop router of that host. The RP then sends Join messages toward the source. At this point, packets are forwarded on a shared distribution tree. If the multicast

traffic from a specific source is sufficient, the first hop router of the host may send Join messages toward the source to build a source-based distribution tree.

Sources register with the RP and then data is forwarded down the shared tree to the receivers. The edge routers learn about a particular source when they receive data packets on the shared tree from that source through the RP. The edge router then sends PIM (S,G) Join messages toward that source. Each router along the reverse path compares the unicast routing metric of the RP address to the metric of the source address. If the metric for the source address is better, it will forward a PIM (S,G) Join message toward the source. If the metric for the RP is the same or better, then the PIM (S,G) Join message will be sent in the same direction as the RP. In this case, the shared tree and the source tree would be considered congruent.

If the shared tree is not an optimal path between the source and the receiver, the routers dynamically create a source tree and stop traffic from flowing down the shared tree. This behavior is the default behavior in software. Network administrators can force traffic to stay on the shared tree by using the **ip pim spt-threshold infinity** command.

PIM-SM scales well to a network of any size, including those with WAN links. The explicit join mechanism prevents unwanted traffic from flooding the WAN links.

### Related Topics

Adding Auto-RP to an Existing Sparse-Mode Cloud , on page 29

Configuring Sparse Mode with a Single Static RP, on page 31

## Sparse-Dense Mode

If you configure either sparse mode or dense mode on an interface, then sparseness or denseness is applied to the interface as a whole. However, some environments might require PIM to run in a single region in sparse mode for some groups and in dense mode for other groups.

An alternative to enabling only dense mode or only sparse mode is to enable sparse-dense mode. In this case, the interface is treated as dense mode if the group is in dense mode; the interface is treated in sparse mode if the group is in sparse mode. You must have an RP if the interface is in sparse-dense mode and you want to treat the group as a sparse group.

If you configure sparse-dense mode, the idea of sparseness or denseness is applied to the groups for which the router is a member.

Another benefit of sparse-dense mode is that Auto-RP information can be distributed in a dense mode; yet, multicast groups for user groups can be used in a sparse mode manner. Therefore there is no need to configure a default RP at the leaf routers.

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

- Members or DVMRP neighbors are on the interface.
- There are PIM neighbors and the group has not been pruned.

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

- Members or DVMRP neighbors are on the interface.
- An explicit Join message has been received by a PIM neighbor on the interface.

## 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 switches 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.

### Related Topics

PIMv1 and PIMv2 Interoperability, on page 2

Troubleshooting PIMv1 and PIMv2 Interoperability Problems, on page 57

# PIM Stub Routing

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

**Note** The IP Base image contains only PIM stub routing. The IP Services image contains complete multicast routing. On a switch running the IP Base image, if you try to configure a VLAN interface with PIM dense-mode, sparse-mode, or dense-sparse-mode, the configuration is not allowed.

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 switch 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 switch as a PIM stub router. The switch does not route transit traffic between distribution routers. You also need to configure a routed uplink port on the switch. The switch 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.

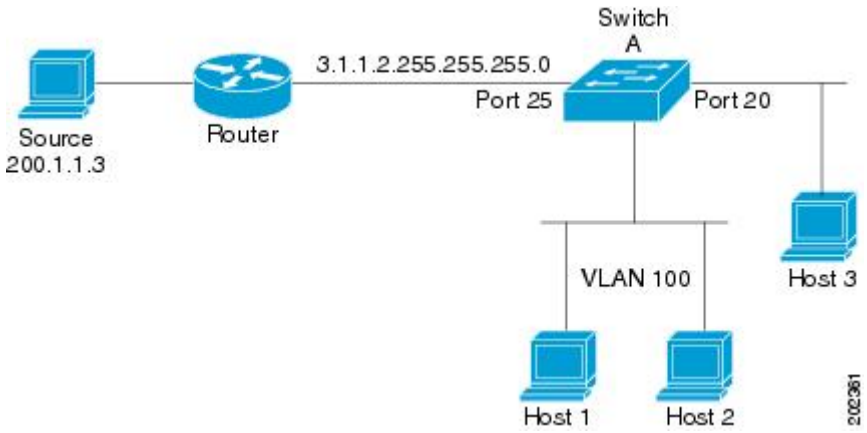
**Note** You must also configure EIGRP stub routing when configuring PIM stub routing on the switch

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.

The PIM stub feature is enforced in the IP Base image. If you upgrade to a higher software version, the PIM stub configuration remains until you reconfigure the interfaces.

In the following figure, the Switch 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 200.1.1.3.

***Figure 1: PIM Stub Router Configuration***




### Related Topics

Enabling PIM Stub Routing , on page 22
Example: Enabling PIM Stub Routing, on page 58
Example: Verifying PIM Stub Routing, on page 58
Restrictions for Configuring PIM Stub Routing, on page 3

# 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 (switch) with the IGMP helper feature.

You can configure a stub router (switch) with the **ip igmp helper-address** *ip-address* interface configuration command to enable the switch 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.

# Rendezvous Points

A rendezvous point (RP) is a role that a device performs when operating in Protocol Independent Multicast (PIM) Sparse Mode (SM). An RP is required only in networks running PIM SM. In the PIM-SM model, only network segments with active receivers that have explicitly requested multicast data will be forwarded the traffic. This method of delivering multicast data is in contrast to PIM Dense Mode (PIM DM). In PIM DM, multicast traffic is initially flooded to all segments of the network. Routers that have no downstream neighbors or directly connected receivers prune back the unwanted traffic.

An RP acts as the meeting place for sources and receivers of multicast data. In a PIM-SM network, sources must send their traffic to the RP. This traffic is then forwarded to receivers down a shared distribution tree. By default, when the first hop device of the receiver learns about the source, it will send a Join message directly to the source, creating a source-based distribution tree from the source to the receiver. This source tree does not include the RP unless the RP is located within the shortest path between the source and receiver.

In most cases, the placement of the RP in the network is not a complex decision. By default, the RP is needed only to start new sessions with sources and receivers. Consequently, the RP experiences little overhead from traffic flow or processing. In PIM version 2, the RP performs less processing than in PIM version 1 because sources must only periodically register with the RP to create state.

### Related Topics

Configuring a Rendezvous Point, on page 23

## Auto-RP

In the first version of PIM-SM, all leaf routers (routers directly connected to sources or receivers) were required to be manually configured with the IP address of the RP. This type of configuration is also known as static RP configuration. Configuring static RPs is relatively easy in a small network, but it can be laborious in a large, complex network.

Following the introduction of PIM-SM version 1, Cisco implemented a version of PIM-SM with the Auto-RP feature. Auto-RP automates the distribution of group-to-RP mappings in a PIM network. Auto-RP has the following benefits:

- Configuring the use of multiple RPs within a network to serve different groups is easy.
- Auto-RP allows load splitting among different RPs and arrangement of RPs according to the location of group participants.
- Auto-RP avoids inconsistent, manual RP configurations that can cause connectivity problems.

Multiple RPs can be used to serve different group ranges or serve as backups to each other. For Auto-RP to work, a router 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 routers. Thus, all routers automatically discover which RP to use for the groups they support.

**Note** If you configure PIM in sparse mode or sparse-dense mode and do not configure Auto-RP, you must statically configure an RP.

**Note** If router interfaces are configured in sparse mode, Auto-RP can still be used if all routers are configured with a static RP address for the Auto-RP groups.

To make Auto-RP work, a router 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 routers by 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. One advantage of Auto-RP is that any change to the RP designation must be configured only on the routers that are RPs and not on the leaf routers. Another advantage of Auto-RP is that it offers the ability to scope the RP address within a domain. Scoping can be achieved by defining the time-to-live (TTL) value allowed for the Auto-RP advertisements.

Each method for configuring an RP has its own strengths, weaknesses, and level of complexity. In conventional IP multicast network scenarios, we recommend using Auto-RP to configure RPs because it is easy to configure, well-tested, and stable. The alternative ways to configure an RP are static RP, Auto-RP, and bootstrap router.

### Related Topics

Setting Up Auto-RP in a New Internetwork , on page 26
Example: Configuring Auto-RP, on page 59
Restrictions for Configuring Auto-RP and BSR, on page 3

## Sparse-Dense Mode for Auto-RP

A prerequisite of Auto-RP is that all interfaces must be configured in sparse-dense mode using the **ip pim sparse-dense-mode** interface configuration command. An interface configured in sparse-dense mode is treated in either sparse mode or dense mode of operation, depending on which mode the multicast group operates. If a multicast group has a known RP, the interface is treated in sparse mode. If a group has no known RP, by default the interface is treated in dense mode and data will be flooded over this interface. (You can prevent dense-mode fallback; see the module “Configuring Basic IP Multicast.”)

To successfully implement Auto-RP and prevent any groups other than 224.0.1.39 and 224.0.1.40 from operating in dense mode, we recommend configuring a “sink RP” (also known as “RP of last resort”). A sink RP is a statically configured RP that may or may not actually exist in the network. Configuring a sink RP does not interfere with Auto-RP operation because, by default, Auto-RP messages supersede static RP configurations. We recommend configuring a sink RP for all possible multicast groups in your network, because it is possible for an unknown or unexpected source to become active. If no RP is configured to limit source registration, the group may revert to dense mode operation and be flooded with data.

## Bootstrap Router

Another RP selection model called bootstrap router (BSR) was introduced after Auto-RP in PIM-SM version 2. BSR performs similarly to Auto-RP in that it uses candidate routers for the RP function and for relaying the RP information for a group. RP information is distributed through BSR messages, which are carried within

PIM messages. PIM messages are link-local multicast messages that travel from PIM router to PIM router. Because of this single hop method of disseminating RP information, TTL scoping cannot be used with BSR. A BSR performs similarly as an RP, except that it does not run the risk of reverting to dense mode operation, and it does not offer the ability to scope within a domain.

### Related Topics

Configuring Candidate BSRs , on page 40

Example: Configuring Candidate BSRs, on page 60

Restrictions for Configuring Auto-RP and BSR, on page 3

## 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 comingle candidate RP advertisements, resulting in the election of RPs in the wrong domain.

### Related Topics

Defining the PIM Domain Border , on page 36

# Multicast Forwarding

Forwarding of multicast traffic is accomplished by multicast-capable routers. These routers create distribution trees that control the path that IP multicast traffic takes through the network in order to deliver traffic to all receivers.

Multicast traffic flows from the source to the multicast group over a distribution tree that connects all of the sources to all of the receivers in the group. This tree may be shared by all sources (a shared tree) or a separate distribution tree can be built for each source (a source tree). The shared tree may be one-way or bidirectional.

Before describing the structure of source and shared trees, it is helpful to explain the notations that are used in multicast routing tables. These notations include the following:

- (S,G) = (unicast source for the multicast group G, multicast group G)
- (*,G) = (any source for the multicast group G, multicast group G)

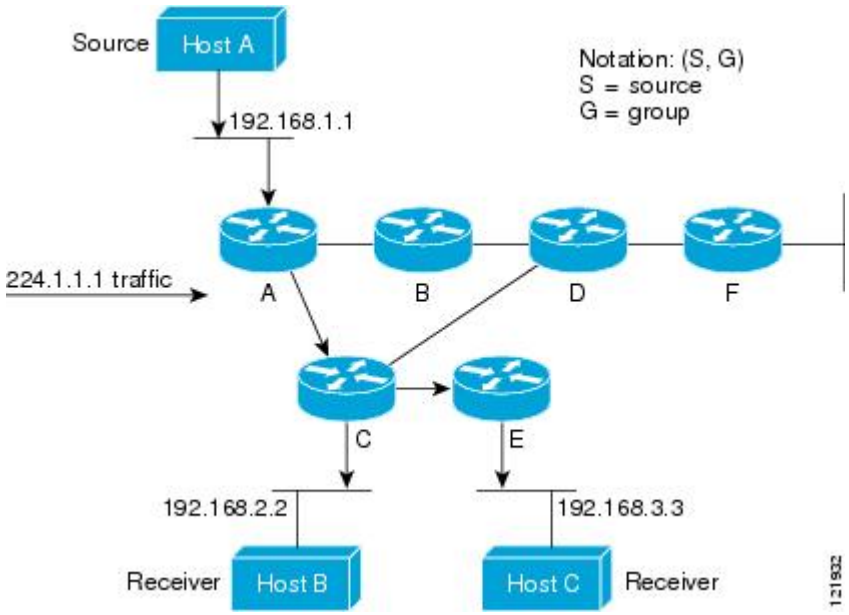
The notation of (S,G), pronounced “S comma G,” enumerates a shortest path tree where S is the IP address of the source and G is the multicast group address.

Shared trees are (*,G) and the source trees are (S,G) and always routed at the sources.

## Multicast Distribution Source Tree

The simplest form of a multicast distribution tree is a source tree. A source tree has its root at the source host and has branches forming a spanning tree through the network to the receivers. Because this tree uses the shortest path through the network, it is also referred to as a shortest path tree (SPT).

The figure shows an example of an SPT for group 224.1.1.1 rooted at the source, Host A, and connecting two receivers, Hosts B and C.



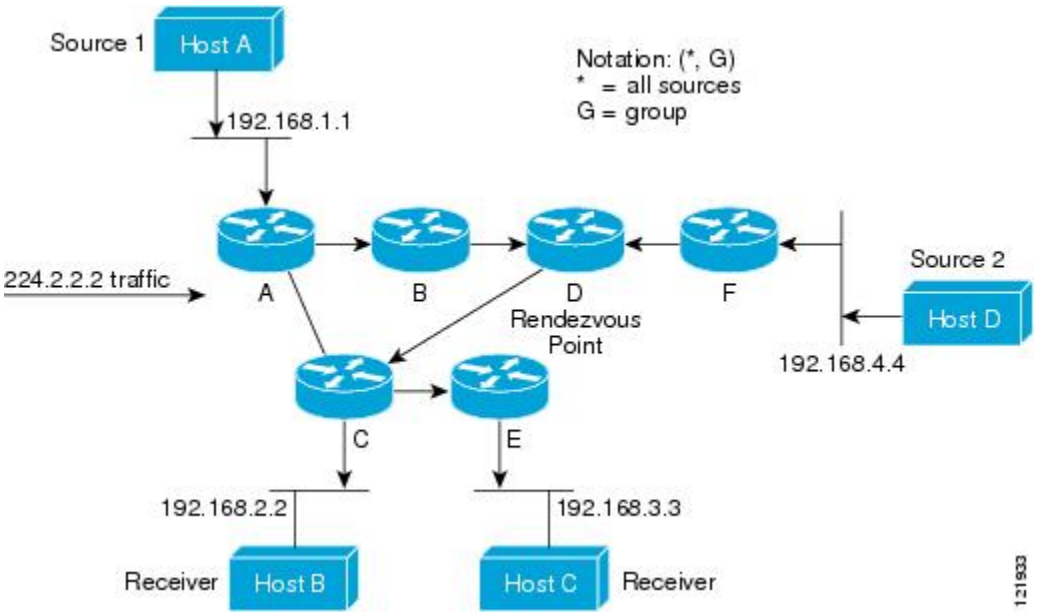

Using standard notation, the SPT for the example shown in the figure would be (192.168.1.1, 224.1.1.1).

The (S,G) notation implies that a separate SPT exists for each individual source sending to each group--which is correct.

## Multicast Distribution Shared Tree

Unlike source trees that have their root at the source, shared trees use a single common root placed at some chosen point in the network. This shared root is called a rendezvous point (RP).

Figure 5 shows a shared tree for the group 224.2.2.2 with the root located at Router D. This shared tree is unidirectional. Source traffic is sent towards the RP on a source tree. The traffic is then forwarded down the shared tree from the RP to reach all of the receivers (unless the receiver is located between the source and the RP, in which case it will be serviced directly).




In this example, multicast traffic from the sources, Hosts A and D, travels to the root (Router D) and then down the shared tree to the two receivers, Hosts B and C. Because all sources in the multicast group use a common shared tree, a wildcard notation written as (*, G), pronounced “star comma G,” represents the tree. In this case, * means all sources, and G represents the multicast group. Therefore, the shared tree shown in Figure 5 would be written as (*, 224.2.2.2).

Both source trees and shared trees are loop-free. Messages are replicated only where the tree branches. Members of multicast groups can join or leave at any time; therefore the distribution trees must be dynamically updated. When all the active receivers on a particular branch stop requesting the traffic for a particular multicast group, the routers prune that branch from the distribution tree and stop forwarding traffic down that branch. If one receiver on that branch becomes active and requests the multicast traffic, the router will dynamically modify the distribution tree and start forwarding traffic again.

## Source Tree Advantage

Source trees have the advantage of creating the optimal path between the source and the receivers. This advantage guarantees the minimum amount of network latency for forwarding multicast traffic. However, this optimization comes at a cost. The routers must maintain path information for each source. In a network that has thousands of sources and thousands of groups, this overhead can quickly become a resource issue on the routers. Memory consumption from the size of the multicast routing table is a factor that network designers must take into consideration.

## Shared Tree Advantage

Shared trees have the advantage of requiring the minimum amount of state in each router. This advantage lowers the overall memory requirements for a network that only allows shared trees. The disadvantage of shared trees is that under certain circumstances the paths between the source and receivers might not be the optimal paths, which might introduce some latency in packet delivery. For example, in the figure above the shortest path between Host A (source 1) and Host B (a receiver) would be Router A and Router C. Because we are using Router D as the root for a shared tree, the traffic must traverse Routers A, B, D and then C.

Network designers must carefully consider the placement of the rendezvous point (RP) when implementing a shared tree-only environment.

In unicast routing, traffic is routed through the network along a single path from the source to the destination host. A unicast router does not consider the source address; it considers only the destination address and how to forward the traffic toward that destination. The router scans through its routing table for the destination address and then forwards a single copy of the unicast packet out the correct interface in the direction of the destination.

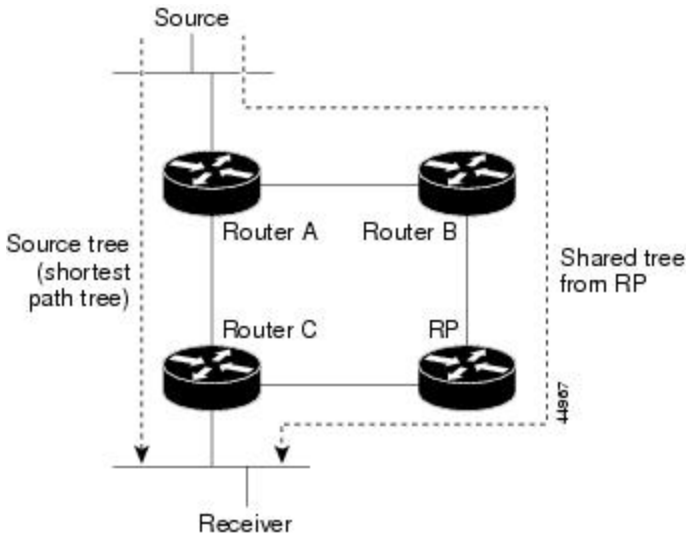
In multicast forwarding, the source is sending traffic to an arbitrary group of hosts that are represented by a multicast group address. The multicast router must determine which direction is the upstream direction (toward the source) and which one is the downstream direction (or directions) toward the receivers. If there are multiple downstream paths, the router replicates the packet and forwards it down the appropriate downstream paths (best unicast route metric)--which is not necessarily all paths. Forwarding multicast traffic away from the source, rather than to the receiver, is called Reverse Path Forwarding (RPF). RPF is described in the following section.

## 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.

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.

***Figure 2: Shared Tree and Source Tree (Shortest-Path 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 switches 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.

### Related Topics

Delaying the Use of PIM Shortest-Path Tree , on page 43

## Reverse Path Forwarding

In unicast routing, traffic is routed through the network along a single path from the source to the destination host. A unicast router does not consider the source address; it considers only the destination address and how to forward the traffic toward that destination. The router scans through its routing table for the destination network and then forwards a single copy of the unicast packet out the correct interface in the direction of the destination.

In multicast forwarding, the source is sending traffic to an arbitrary group of hosts that are represented by a multicast group address. The multicast router must determine which direction is the upstream direction (toward the source) and which one is the downstream direction (or directions) toward the receivers. If there are multiple downstream paths, the router replicates the packet and forwards it down the appropriate downstream paths (best unicast route metric)--which is not necessarily all paths. Forwarding multicast traffic away from the

source, rather than to the receiver, is called Reverse Path Forwarding (RPF). RPF is an algorithm used for forwarding multicast datagrams.

Protocol Independent Multicast (PIM) uses the unicast routing information to create a distribution tree along the reverse path from the receivers towards the source. The multicast routers then forward packets along the distribution tree from the source to the receivers. RPF is a key concept in multicast forwarding. It enables routers to correctly forward multicast traffic down the distribution tree. RPF makes use of the existing unicast routing table to determine the upstream and downstream neighbors. A router will forward a multicast packet only if it is received on the upstream interface. This RPF check helps to guarantee that the distribution tree will be loop-free.

## RPF Check

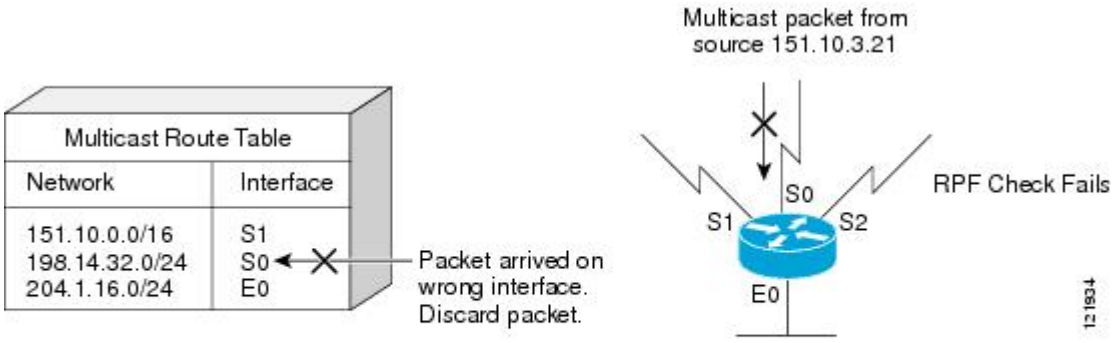
When a multicast packet arrives at a router, the router performs an RPF check on the packet. If the RPF check succeeds, the packet is forwarded. Otherwise, it is dropped.

For traffic flowing down a source tree, the RPF check procedure works as follows:

1. The router looks up the source address in the unicast routing table to determine if the packet has arrived on the interface that is on the reverse path back to the source.
2. If the packet has arrived on the interface leading back to the source, the RPF check succeeds and the packet is forwarded out the interfaces present in the outgoing interface list of a multicast routing table entry.
3. If the RPF check in Step 2 fails, the packet is dropped.

The figure shows an example of an unsuccessful RPF check.

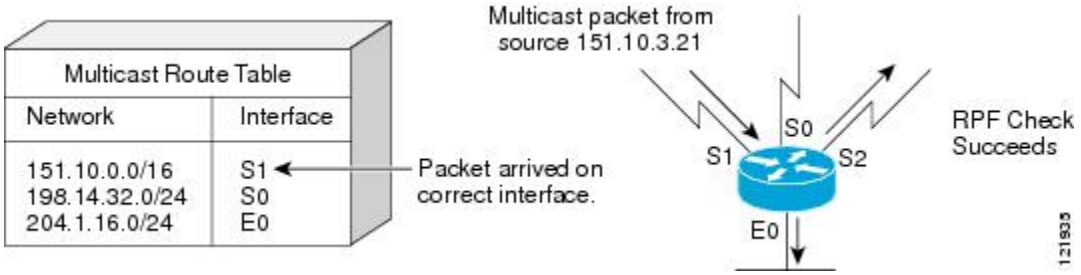
***Figure 3: RPF Check Fails***




As the figure illustrates, a multicast packet from source 151.10.3.21 is received on serial interface 0 (S0). A check of the unicast route table shows that S1 is the interface this router would use to forward unicast data to 151.10.3.21. Because the packet has arrived on interface S0, the packet is discarded.

The figure shows an example of a successful RPF check.

***Figure 4: RPF Check Succeeds***




In this example, the multicast packet has arrived on interface S1. The router refers to the unicast routing table and finds that S1 is the correct interface. The RPF check passes, and the packet is forwarded.

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 switch 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 switch 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).

DVMRP and dense-mode PIM use only source trees and use RPF.

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

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.

# Bidir-PIM Overview

Bidir-PIM shares many of its shortest path tree (SPT) operations with PIM-SM. Bidir-PIM also has unconditional forwarding of source traffic toward the RP upstream on the shared tree, but has no registering process for sources as in PIM-SM. These modifications allow forwarding of traffic in all routers based solely on the (*, G) multicast routing entries. This form of forwarding eliminates any source-specific state and allows scaling capability to an arbitrary number of sources.

### Related Topics

Configuring Bidirectional PIM , on page 47

## Multicast Group Modes

In PIM, packet traffic for a multicast group is routed according to the rules of the mode configured for that multicast group. The Cisco implementation of PIM supports four modes for a multicast group:

- PIM bidirectional mode
- PIM dense mode
- PIM sparse mode
- PIM Source Specific Mode (SSM)

A router can simultaneously support all four modes or any combination of them for different multicast groups.

## Bidirectional Shared Tree

In bidirectional mode, traffic is routed only along a bidirectional shared tree that is rooted at the rendezvous point (RP) for the group. In bidir-PIM, the IP address of the RP acts as the key to having all routers establish a loop-free spanning tree topology rooted in that IP address. This IP address need not be a router, but can be any unassigned IP address on a network that is reachable throughout the PIM domain. This technique is the preferred configuration method for establishing a redundant RP configuration for bidir-PIM.

Membership in a bidirectional group is signaled by way of explicit Join messages. Traffic from sources is unconditionally sent up the shared tree toward the RP and passed down the tree toward the receivers on each branch of the tree.

The figures below show the difference in state created per router for a unidirectional shared tree and source tree versus a bidirectional shared tree.

***Figure 5: Unidirectional Shared Tree and Source Tree***

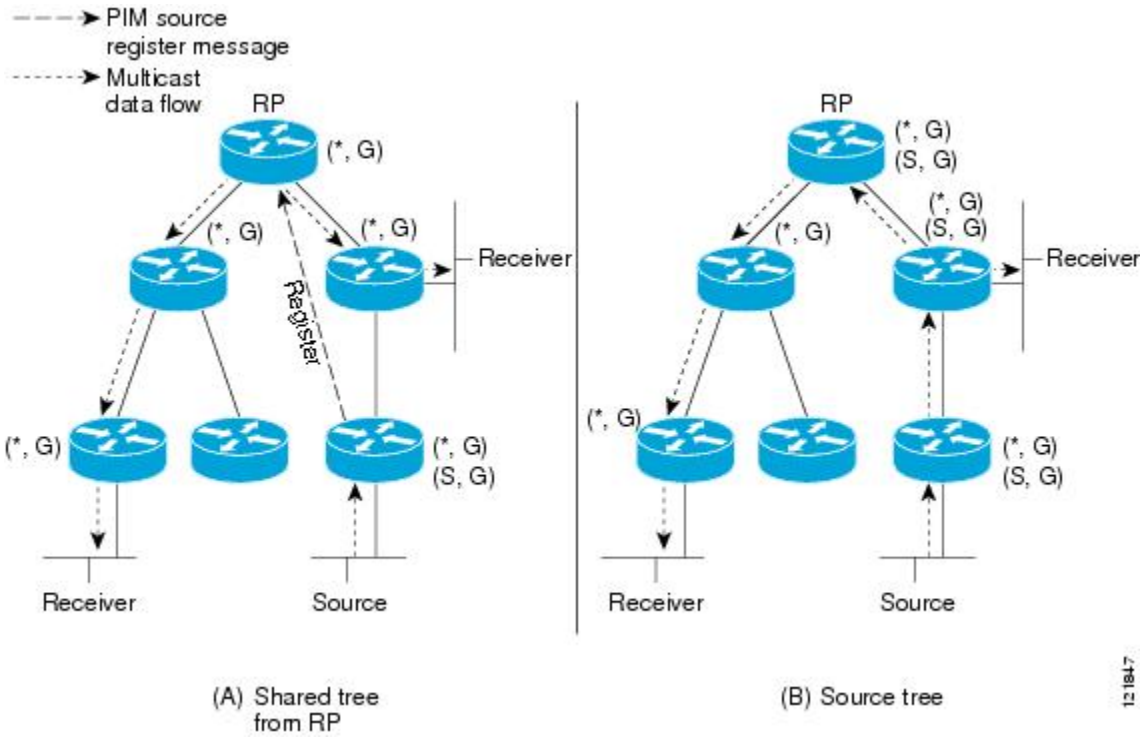
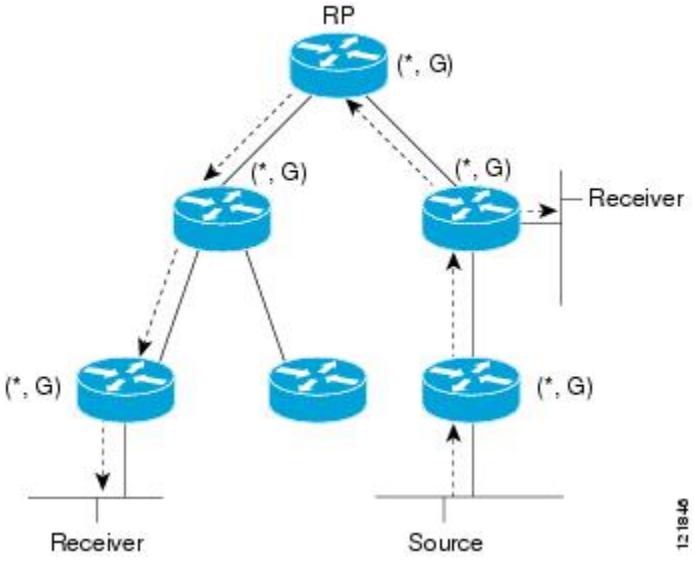



***Figure 6: Bidirectional Shared Tree***



For packets that are forwarded downstream from the RP toward receivers, there are no fundamental differences between bidir-PIM and PIM-SM. Bidir-PIM deviates substantially from PIM-SM for traffic that is passed from sources upstream toward the RP.

PIM-SM cannot forward traffic in the upstream direction of a tree because it accepts traffic from only one Reverse Path Forwarding (RPF) interface. This interface (for the shared tree) points toward the RP, thus allowing only downstream traffic flow. Upstream traffic is first encapsulated into unicast register messages, which are passed from the designated router (DR) of the source toward the RP. Second, the RP joins an SPT that is rooted at the source. Therefore, in PIM-SM, traffic from sources destined for the RP does not flow upstream in the shared tree, but downstream along the SPT of the source until it reaches the RP. From the RP, traffic flows along the shared tree toward all receivers.

In bidir-PIM, the packet-forwarding rules have been improved over PIM-SM, allowing traffic to be passed up the shared tree toward the RP. To avoid multicast packet looping, bidir-PIM introduces a new mechanism called designated forwarder (DF) election, which establishes a loop-free SPT rooted at the RP.

## DF Election

On every network segment and point-to-point link, all PIM routers participate in a procedure called designated forwarder (DF) election. The procedure selects one router as the DF for every RP of bidirectional groups. This router is responsible for forwarding multicast packets received on that network.

The DF election is based on unicast routing metrics. The router with the most preferred unicast routing metric to the RP becomes the DF. Use of this method ensures that only one copy of every packet will be sent to the RP, even if there are parallel equal-cost paths to the RP.

A DF is selected for every RP of bidirectional groups. As a result, multiple routers may be elected as DF on any network segment, one for each RP. Any particular router may be elected as DF on more than one interface.

## Bidirectional Group Tree Building

The procedure for joining the shared tree of a bidirectional group is almost identical to that used in PIM-SM. One main difference is that, for bidirectional groups, the role of the DR is assumed by the DF for the RP.

On a network that has local receivers, only the router elected as the DF populates the outgoing interface list (olist) upon receiving Internet Group Management Protocol (IGMP) Join messages, and sends (*, G) Join and Leave messages upstream toward the RP. When a downstream router wishes to join the shared tree, the RPF neighbor in the PIM Join and Leave messages is always the DF elected for the interface that lead to the RP.

When a router receives a Join or Leave message, and the router is not the DF for the receiving interface, the message is ignored. Otherwise, the router updates the shared tree in the same way as in sparse mode.

In a network where all routers support bidirectional shared trees, (S, G) Join and Leave messages are ignored. There is also no need to send PIM assert messages because the DF election procedure eliminates parallel downstream paths from any RP. An RP never joins a path back to the source, nor will it send any register stops.

## Packet Forwarding

A router creates (*, G) entries only for bidirectional groups. The olist of a (*, G) entry includes all the interfaces for which the router has been elected DF and that have received either an IGMP or PIM Join message. If a router is located on a sender-only branch, it will also create a (*, G) state, but the olist will not include any interfaces.

If a packet is received from the RPF interface toward the RP, the packet is forwarded downstream according to the olist of the (*, G) entry. Otherwise, only the router that is the DF for the receiving interface forwards the packet upstream toward the RP; all other routers must discard the packet.

### Benefits of Bidirectional PIM

- Bidir-PIM removes the performance cost of maintaining a routing state table for a large number of sources.
- Bidir-PIM is designed to be used for many-to-many applications within individual PIM domains. Multicast groups in bidirectional PIM mode can scale to an arbitrary number of sources without incurring overhead due to the number of sources.

## Default PIM Routing Configuration

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

***Table 1: 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. |
| 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

This procedure is optional.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Switch# configure terminal` | Enters the global configuration mode. |
| **Step 3** | **interface** *interface-id*<br><br>**Example:**<br><br>`Switch(config)# interface gigabitethernet 1/0/1` | Specifies the interface on which you want to enable PIM stub routing, and enters interface configuration mode.<br><br>The specified interface must be one of the following:<br><br>• A routed port—A physical port that has been configured as a Layer 3 port by entering the **no switchport** 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.<br><br>• An SVI—A VLAN interface created by using the **interface vlan** *vlan-id* 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.<br><br>These interfaces must have IP addresses assigned to them. |
| **Step 4** | **ip pim passive**<br><br>**Example:**<br><br>`Switch(config-if)# ip pim passive` | Configures the PIM stub feature on the interface. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **end**<br><br>**Example:**<br><br>`Switch(config)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **show ip pim interface**<br><br>**Example:**<br><br>`Switch# show ip pim interface` | (Optional) Displays the PIM stub that is enabled on each interface. |
| **Step 7** | **show running-config**<br><br>**Example:**<br><br>`Switch# show running-config` | Verifies your entries. |
| **Step 8** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

### Related Topics

PIM Stub Routing, on page 7
Example: Enabling PIM Stub Routing, on page 58
Example: Verifying PIM Stub Routing, on page 58
Restrictions for Configuring PIM Stub Routing, on page 3

# 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 PIMv1 and PIMv2 Interoperability, on page 2.

### Related Topics

Rendezvous Points, on page 9

## Manually Assigning an RP to Multicast Groups

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 switch responds to the group as dense and uses the dense-mode PIM techniques.

This procedure is optional.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters the global configuration mode. |
| **Step 3** | **ip pim rp-address** *ip-address* [*access-list-number*] [**override**] | Configures the address of a PIM RP.<br><br>By default, no PIM RP address is configured. You must configure the IP address of RPs on all routers and multilayer switches (including the RP). |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Switch(config)# ip pim rp-address 10.1.1.1 20 override` | **Note** If there is no RP configured for a group, the switch treats the group as dense, using the dense-mode PIM techniques.<br>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. The access list conditions specify for which groups the device is an RP.<br>• For *ip-address*, enter the unicast address of the RP in dotted-decimal notation.<br>• (Optional) For *access-list-number*, enter an IP standard access list number from 1 to 99. If no access list is configured, the RP is used for all groups.<br>• (Optional) The **override** 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.<br>**Note** To remove an RP address, use the **no ip pim rp-address ip-address** [*access-list-number*] [**override**] global configuration command. |
| **Step 4** | **access-list** *access-list-number* {**deny** \| **permit**} *source* [*source-wildcard*]<br>**Example:**<br>`Switch(config)# access-list 25 permit 10.5.0.1 255.224.0.0` | Creates a standard access list, repeating the command as many times as necessary.<br>• For *access-list-number*, enter the access list number specified in Step 2.<br>• The **deny** keyword denies access if the conditions are matched.<br>• The **permit** keyword permits access if the conditions are matched.<br>• For *source*, enter the multicast group address for which the RP should be used.<br>• (Optional) For *source-wildcard*, 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.<br>The access list is always terminated by an implicit deny statement for everything. |
| **Step 5** | **end**<br>**Example:**<br>`Switch(config)# end` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **show running-config**<br><br>**Example:**<br><br>`Switch# show running-config` | Verifies your entries. |
| **Step 7** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

### Related Topics

Example: Manually Assigning an RP to Multicast Groups, on page 59

## Setting Up Auto-RP in a New Internetwork

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.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **show running-config**<br><br>**Example:**<br><br>`Switch# show running-config` | 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 **ip pim rp-address** global configuration command.<br>**Note** This step is not required for spare-dense-mode environments.<br>The selected RP should have good connectivity and be available across the network. Use this RP for the global groups (for |

| | Command or Action | Purpose |
|---|---|---|
| | | 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. |
| **Step 3** | **configure terminal**<br><br>**Example:**<br><br>`Switch# configure terminal` | Enters the global configuration mode. |
| **Step 4** | **ip pim send-rp-announce** *interface-id* **scope** *ttl* **group-list** *access-list-number* **interval** *seconds*<br><br>**Example:**<br><br>`Switch(config)# ip pim send-rp-announce gigabitethernet 1/0/5 scope 20 group-list 10 interval 120` | Configures another PIM device to be the candidate RP for local groups.<br>• For *interface-id*, enter the interface type and number that identifies the RP address. Valid interfaces include physical ports, port channels, and VLANs.<br>• For **scope** *ttl*, 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.<br>• For **group-list** *access-list-number*, enter an IP standard access list number from 1 to 99. If no access list is configured, the RP is used for all groups.<br>• For **interval** *seconds*, specify how often the announcement messages must be sent. The default is 60 seconds. The range is 1 to 16383. |
| **Step 5** | **access-list** *access-list-number* {**deny** \| **permit**} *source* [*source-wildcard*]<br><br>**Example:**<br><br>`Switch(config)# access-list 10 permit 10.10.0.0` | Creates a standard access list, repeating the command as many times as necessary.<br>• For *access-list-number*, enter the access list number specified in Step 3.<br>• The **deny** keyword denies access if the conditions are matched.<br>• The **permit** keyword permits access if the conditions are matched.<br>• For *source*, enter the multicast group address range for which the RP should be used.<br>• (Optional) For *source-wildcard*, 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.<br><br>**Note** Recall that the access list is always terminated by an implicit deny statement for everything. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **ip pim send-rp-discovery scope** *ttl*<br><br>**Example:**<br>`Switch(config)# ip pim send-rp-discovery scope 50` | Finds a switch whose connectivity is not likely to be interrupted, and assign it the role of RP-mapping agent.<br><br>For **scope** *ttl*, 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. |
| **Step 7** | **end**<br><br>**Example:**<br>`Switch(config)# end` | Returns to privileged EXEC mode. |
| **Step 8** | **show running-config**<br><br>**Example:**<br>`Switch# show running-config` | Verifies your entries. |
| **Step 9** | **show ip pim rp mapping**<br><br>**Example:**<br>`Switch# show ip pim rp mapping` | Displays active RPs that are cached with associated multicast routing entries. |
| **Step 10** | **show ip pim rp**<br><br>**Example:**<br>`Switch# show ip pim rp` | Displays the information cached in the routing table. |
| **Step 11** | **copy running-config startup-config**<br><br>**Example:**<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

### Related Topics

Auto-RP, on page 9
Example: Configuring Auto-RP, on page 59
Restrictions for Configuring Auto-RP and BSR, on page 3

## Adding Auto-RP to an Existing Sparse-Mode Cloud

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.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **show running-config**<br><br>**Example:**<br><br>`Switch# show running-config` | 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 **ip pim rp-address** global configuration command.<br>**Note** This step is not required for spare-dense-mode environments.<br>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. |
| **Step 3** | **configure terminal**<br><br>**Example:**<br><br>`Switch# configure terminal` | Enters the global configuration mode. |
| **Step 4** | **ip pim send-rp-announce** *interface-id* **scope** *ttl* **group-list** *access-list-number* **interval** *seconds*<br><br>**Example:**<br><br>`Switch(config)# ip pim send-rp-announce gigabitethernet 1/0/5 scope 20 group-list 10 interval 120` | Configures another PIM device to be the candidate RP for local groups.<br>• For *interface-id*, enter the interface type and number that identifies the RP address. Valid interfaces include physical ports, port channels, and VLANs.<br>• For **scope** *ttl*, 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.<br>• For **group-list** *access-list-number*, enter an IP standard access list number from 1 to 99. If no access list is configured, the RP is used for all groups. |

| | Command or Action | Purpose |
|---|---|---|
| | | • For **interval** *seconds*, specify how often the announcement messages must be sent. The default is 60 seconds. The range is 1 to 16383.<br><br>**Note** To remove the PIM device configured as the candidate RP, use the **no ip pim send-rp-announce** interface-id global configuration command. |
| **Step 5** | **access-list** *access-list-number* {**deny** \| **permit**} *source* [*source-wildcard*]<br><br>**Example:**<br><br>`Switch(config)# access-list 10 permit 224.0.0.0 15.255.255.255` | Creates a standard access list, repeating the command as many times as necessary.<br><br>• For *access-list-number*, enter the access list number specified in Step 3.<br><br>• The **deny** keyword denies access if the conditions are matched.<br><br>• The **permit** keyword permits access if the conditions are matched.<br><br>• For *source*, enter the multicast group address range for which the RP should be used.<br><br>• (Optional) For *source-wildcard*, 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.<br><br>Recall that the access list is always terminated by an implicit deny statement for everything. |
| **Step 6** | **ip pim send-rp-discovery scope** *ttl*<br><br>**Example:**<br><br>`Switch(config)# ip pim send-rp-discovery scope 50` | Finds a switch whose connectivity is not likely to be interrupted, and assigns it the role of RP-mapping agent.<br><br>For **scope** *ttl*, 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.<br><br>**Note** To remove the switch as the RP-mapping agent, use the **no ip pim send-rp-discovery** global configuration command. |
| **Step 7** | **end**<br><br>**Example:**<br><br>`Switch(config)# end` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | **show running-config**<br><br>**Example:**<br>`Switch# show running-config` | Verifies your entries. |
| **Step 9** | **show ip pim rp mapping**<br><br>**Example:**<br>`Switch# show ip pim rp mapping` | Displays active RPs that are cached with associated multicast routing entries. |
| **Step 10** | **show ip pim rp**<br><br>**Example:**<br>`Switch# show ip pim rp` | Displays the information cached in the routing table. |
| **Step 11** | **copy running-config startup-config**<br><br>**Example:**<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

### Related Topics

PIM Sparse Mode, on page 5

## Configuring Sparse Mode with a Single Static RP

A rendezvous point (RP) is required in networks running Protocol Independent Multicast sparse mode (PIM-SM). In PIM-SM, traffic will be forwarded only to network segments with active receivers that have explicitly requested multicast data.

This section describes how to configure sparse mode with a single static RP.

### Before You Begin

All access lists that are needed when sparse mode is configured with a single static RP should be configured prior to beginning the configuration task.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Switch> enable` | • Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip multicast-routing** [**distributed**]<br>**Example:**<br>`Switch(config)# ip multicast-routing` | Enables IP multicast routing.<br>• Use the **distributed** keyword to enable Multicast Distributed Switching. |
| **Step 4** | **interface** *type number*<br>**Example:**<br>`Switch(config)# interface gigabitethernet 1/0/0` | Selects an interface that is connected to hosts on which PIM can be enabled. |
| **Step 5** | **ip pim sparse-mode**<br>**Example:**<br>`Switch(config-if)# ip pim sparse-mode` | Enables PIM on an interface. You must use sparse mode. |
| **Step 6** | Repeat Steps 1 through 5 on every interface that uses IP multicast. | -- |
| **Step 7** | **exit**<br>**Example:**<br>`Switch(config-if)# exit` | Returns to global configuration mode. |
| **Step 8** | **ip pim rp-address** *rp-address* [*access-list*] [**override**]<br>**Example:**<br>`Switch(config)# ip pim rp-address 192.168.0.0` | Configures the address of a PIM RP for a particular group.<br>• The optional *access-list* argument is used to specify the number or name a standard access list that defines the multicast groups to be statically mapped to the RP.<br>**Note** If no access list is defined, the RP will map to all multicast groups, 224/4.<br>• The optional **override** keyword is used to specify that if dynamic and static group-to-RP mappings |

| | Command or Action | Purpose |
|---|---|---|
| | | are used together and there is an RP address conflict, the RP address configured for a static group-to-RP mapping will take precedence.<br><br>**Note** If the **override** keyword is not specified and there is RP address conflict, dynamic group-to-RP mappings will take precedence over static group-to-RP mappings. |
| **Step 9** | **end**<br><br>**Example:**<br><br>`Switch(config)# end` | Ends the current configuration session and returns to EXEC mode. |
| **Step 10** | **show ip pim rp** [**mapping**] [*rp-address*]<br><br>**Example:**<br><br>`Switch# show ip pim rp mapping` | (Optional) Displays RPs known in the network and shows how the router learned about each RP. |
| **Step 11** | **show ip igmp groups** [*group-name* \| *group-address*\| *interface-type interface-number*] [**detail**]<br><br>**Example:**<br><br>`Switch# show ip igmp groups` | (Optional) Displays the multicast groups having receivers that are directly connected to the router and that were learned through IGMP.<br><br>• 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. |
| **Step 12** | **show ip mroute**<br><br>**Example:**<br><br>`Switch# show ip mroute` | (Optional) Displays the contents of the IP mroute table. |
| **Step 13** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

### Related Topics

PIM Sparse Mode, on page 5

## Preventing Join Messages to False RPs

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 switches 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.

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:

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

This procedure is optional.

### Related Topics

Example: Preventing Join Messages to False RPs, on page 60

## Filtering Incoming RP Announcement Messages

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.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters the global configuration mode. |
| **Step 3** | **ip pim rp-announce-filter rp-list** *access-list-number* **group-list** *access-list-number* | Filters incoming RP announcement messages.<br><br>Enter this command on each mapping agent in the network. Without this command, all incoming RP-announce messages are accepted by default. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Switch(config)# ip pim rp-announce-filter rp-list 10 group-list 14` | For **rp-list** *access-list-number*, configure an access list of candidate RP addresses that, if permitted, is accepted for the group ranges supplied in the **group-list** *access-list-number* variable. If this variable is omitted, the filter applies to all multicast groups.<br>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.<br>**Note** To remove a filter on incoming RP announcement messages, use the **no ip pim rp-announce-filter rp-list** *access-list-number* [**group-list** *access-list-number*] global configuration command. |
| **Step 4** | **access-list** *access-list-number* {**deny** \| **permit**} *source* [*source-wildcard*]<br>**Example:**<br>`Switch(config)# access-list 10 permit 10.8.1.0 255.255.224.0` | Creates a standard access list, repeating the command as many times as necessary.<br>• For *access-list-number*, enter the access list number specified in Step 2.<br>• The **deny** keyword denies access if the conditions are matched.<br>• The **permit** keyword permits access if the conditions are matched.<br>• Create an access list that specifies from which routers and multilayer switches the mapping agent accepts candidate RP announcements (rp-list ACL).<br>• Create an access list that specifies the range of multicast groups from which to accept or deny (group-list ACL).<br>• For *source*, enter the multicast group address range for which the RP should be used.<br>• (Optional) For *source-wildcard*, 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.<br>The access list is always terminated by an implicit deny statement for everything. |
| **Step 5** | **end**<br>**Example:**<br>`Switch(config)# end` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **show running-config**<br><br>**Example:**<br><br>`Switch# show running-config` | Verifies your entries. |
| **Step 7** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

### Related Topics

Example: Filtering Incoming RP Announcement Messages, on page 60

# 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

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

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Switch# configure terminal` | Enters the global configuration mode. |
| **Step 3** | **interface** *interface-id*<br><br>**Example:**<br><br>`Switch(config)# interface gigabitethernet 1/0/1` | Specifies the interface to be configured, and enters interface configuration mode.<br><br>The specified interface must be one of the following:<br><br>• A routed port—A physical port that has been configured as a Layer 3 port by entering the **no switchport** 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.<br><br>• An SVI—A VLAN interface created by using the **interface vlan** *vlan-id* 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.<br><br>These interfaces must have IP addresses assigned to them. |
| **Step 4** | **ip pim bsr-border**<br><br>**Example:**<br><br>`Switch(config-if)# ip pim bsr-border` | Defines a PIM bootstrap message boundary for the PIM domain.<br><br>Enter this command on each interface that connects to other bordering PIM domains. This command instructs the switch to neither send nor receive PIMv2 BSR messages on this interface.<br><br>**Note** To remove the PIM border, use the **no ip pim bsr-border** interface configuration command. |
| **Step 5** | **end**<br><br>**Example:**<br><br>`Switch(config)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **show running-config**<br><br>**Example:**<br><br>`Switch# show running-config` | Verifies your entries. |
| **Step 7** | **copy running-config startup-config** | (Optional) Saves your entries in the configuration file. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Switch# copy running-config startup-config` | |

### Related Topics

PIM Domain Border, on page 11

## Defining the IP Multicast Boundary

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.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Switch# configure terminal` | Enters the global configuration mode. |
| **Step 3** | **access-list** *access-list-number* **deny** *source* [*source-wildcard*]<br>**Example:**<br>`Switch(config)# access-list 12 deny 224.0.1.39`<br>`access-list 12 deny 224.0.1.40` | Creates a standard access list, repeating the command as many times as necessary.<br>• For *access-list-number*, the range is 1 to 99.<br>• The **deny** keyword denies access if the conditions are matched.<br>• For *source*, enter multicast addresses 224.0.1.39 and 224.0.1.40, which carry Auto-RP information.<br>• (Optional) For *source-wildcard*, 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. |

| | Command or Action | Purpose |
|---|---|---|
| | | The access list is always terminated by an implicit deny statement for everything. |
| **Step 4** | **interface** *interface-id*<br><br>**Example:**<br><br>`Switch(config)# interface gigabitethernet 1/0/1` | Specifies the interface to be configured, and enters interface configuration mode.<br><br>The specified interface must be one of the following:<br><br>• A routed port—A physical port that has been configured as a Layer 3 port by entering the **no switchport** 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.<br><br>• An SVI—A VLAN interface created by using the **interface vlan** *vlan-id* 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.<br><br>These interfaces must have IP addresses assigned to them. |
| **Step 5** | **ip multicast boundary** *access-list-number*<br><br>**Example:**<br><br>`Switch(config-if)# ip multicast boundary 12` | Configures the boundary, specifying the access list you created in Step 2.<br><br>**Note** To remove the boundary, use the **no ip multicast boundary** interface configuration command. |
| **Step 6** | **end**<br><br>**Example:**<br><br>`Switch(config)# end` | Returns to privileged EXEC mode. |
| **Step 7** | **show running-config**<br><br>**Example:**<br><br>`Switch# show running-config` | Verifies your entries. |
| **Step 8** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config` | (Optional) Saves your entries in the configuration file. |

| | Command or Action | Purpose |
|---|---|---|
| | `startup-config` | |

### Related Topics

Example: Defining the IP Multicast Boundary to Deny Auto-RP Information, on page 59

## Configuring Candidate BSRs

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.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Switch# configure terminal` | Enters the global configuration mode. |
| **Step 3** | **ip pim bsr-candidate** *interface-id hash-mask-length* [*priority*]<br><br>**Example:**<br><br>`Switch(config)# ip pim bsr-candidate gigabitethernet 1/0/3 28 100` | Configures your switch to be a candidate BSR.<br>• For *interface-id*, enter the interface on this switch 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.<br>• For *hash-mask-length*, 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.<br>• (Optional) For *priority*, 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. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** To remove this device as a candidate BSR, use the **no ip pim bsr-candidate** global configuration command. |
| **Step 4** | **end**<br><br>**Example:**<br><br>`Switch(config)# end` | Returns to privileged EXEC mode. |
| **Step 5** | **show running-config**<br><br>**Example:**<br><br>`Switch# show running-config` | Verifies your entries. |
| **Step 6** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

### Related Topics

Bootstrap Router, on page 10
Example: Configuring Candidate BSRs, on page 60
Restrictions for Configuring Auto-RP and BSR, on page 3

## Configuring the Candidate RPs

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 switches 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 switches 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 switches as RPs.

## Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Switch# configure terminal` | Enters the global configuration mode. |
| **Step 3** | **ip pim rp-candidate** *interface-id* [**group-list** *access-list-number*]<br><br>**Example:**<br><br>`Switch(config)# ip pim rp-candidate gigabitethernet 1/0/5 group-list 10` | Configures your switch to be a candidate RP.<br>• For *interface-id*, specify the interface whose associated IP address is advertised as a candidate RP address. Valid interfaces include physical ports, port channels, and VLANs.<br>• (Optional) For **group-list** *access-list-number*, enter an IP standard access list number from 1 to 99. If no group-list is specified, the switch is a candidate RP for all groups.<br><br>**Note** To remove this device as a candidate RP, use the **no ip pim rp-candidate** interface-id global configuration command. |
| **Step 4** | **access-list** *access-list-number* {**deny** \| **permit**} *source* [*source-wildcard*]<br><br>**Example:**<br><br>`Switch(config)# access-list 10 permit 239.0.0.0 0.255.255.255` | Creates a standard access list, repeating the command as many times as necessary.<br>• For *access-list-number*, enter the access list number specified in Step 2.<br>• The **deny** keyword denies access if the conditions are matched. The **permit** keyword permits access if the conditions are matched.<br>• For *source*, enter the number of the network or host from which the packet is being sent.<br>• (Optional) For *source-wildcard*, 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.<br><br>The access list is always terminated by an implicit deny statement for everything. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **end**<br><br>**Example:**<br>`Switch(config)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **show running-config**<br><br>**Example:**<br>`Switch# show running-config` | Verifies your entries. |
| **Step 7** | **copy running-config startup-config**<br><br>**Example:**<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

### Related Topics

Example: Configuring Candidate RPs, on page 61

# Delaying the Use of PIM Shortest-Path Tree

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.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **access-list** *access-list-number* {**deny** \| **permit**} *source* [*source-wildcard*]<br><br>**Example:**<br><br>`Switch(config)# access-list 16 permit 225.0.0.0 0.255.255.255` | Creates a standard access list.<br>• For *access-list-number*, the range is 1 to 99.<br>• The **deny** keyword denies access if the conditions are matched.<br>• The **permit** keyword permits access if the conditions are matched.<br>• For *source*, specify the multicast group to which the threshold will apply.<br>• (Optional) For *source-wildcard*, 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.<br><br>The access list is always terminated by an implicit deny statement for everything. |
| **Step 4** | **ip pim spt-threshold** {*kbps* \| **infinity**} [**group-list** *access-list-number*]<br><br>**Example:**<br><br>`Switch(config)# ip pim spt-threshold infinity group-list 16` | Specifies the threshold that must be reached before moving to shortest-path tree (spt).<br>• For *kbps*, specify the traffic rate in kilobits per second. The default is 0 kbps.<br>**Note** Because of switch hardware limitations, 0 kbps is the only valid entry even though the range is 0 to 4294967.<br>• Specify **infinity** if you want all sources for the specified group to use the shared tree, never switching to the source tree.<br>• (Optional) For **group-list** *access-list-number*, 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.<br><br>**Note** To return to the default setting, use the **no ip pim spt-threshold** {**kbps** \| **infinity**} global configuration command. |
| **Step 5** | **end**<br><br>**Example:**<br><br>`Switch(config)# end` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **show running-config**<br><br>**Example:**<br><br>`Switch# show running-config` | Verifies your entries. |
| **Step 7** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

### Related Topics

PIM Shared Tree and Source Tree, on page 14

# Modifying the PIM Router-Query Message Interval

PIM routers and multilayer switches 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.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Switch# configure terminal` | Enters the global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **interface** *interface-id*<br><br>**Example:**<br><br>`Switch(config)# interface gigabitethernet 1/0/1` | Specifies the interface to be configured, and enters interface configuration mode.<br><br>The specified interface must be one of the following:<br><br>• A routed port—A physical port that has been configured as a Layer 3 port by entering the **no switchport** 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.<br><br>• An SVI—A VLAN interface created by using the **interface vlan** *vlan-id* 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.<br><br>These interfaces must have IP addresses assigned to them. |
| **Step 4** | **ip pim query-interval** *seconds*<br><br>**Example:**<br><br>`Switch(config-if)# ip pim query-interval 45` | Configures the frequency at which the switch sends PIM router-query messages.<br><br>The default is 30 seconds. The range is 1 to 65535.<br><br>**Note** To return to the default setting, use the **no ip pim query-interval** [**seconds**] interface configuration command. |
| **Step 5** | **end**<br><br>**Example:**<br><br>`Switch(config)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **show ip igmp interface** [*interface-id*]<br><br>**Example:**<br><br>`Switch# show ip igmp interface` | Verifies your entries. |
| **Step 7** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuring Bidirectional PIM

Follow these steps to configure bidirectional PIM:

### Before You Begin

All required access lists must be configured before configuring bidirectional PIM.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Switch> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip multicast-routing** [**distributed**]<br><br>**Example:**<br><br>`Switch(config)# ip multicast-routing` | Enables IP multicast routing.<br><br>• Use the **distributed** keyword to enable Multicast Distributed Switching. |
| **Step 4** | **interface** *type number*<br><br>**Example:**<br><br>`Switch(config)# interface gigabitethernet 1/0/0` | Selects an interface that is connected to hosts on which PIM can be enabled. |
| **Step 5** | **ip pim sparse-mode**<br><br>**Example:**<br><br>`Switch(config-if)# ip pim sparse-mode` | Enables sparse mode. |
| **Step 6** | **exit**<br><br>**Example:**<br><br>`Switch(config-if)# exit` | Returns to global configuration mode. |
| **Step 7** | **ip pim bidir-enable** | Enables bidir-PIM on a router. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Switch(config)# ip pim bidir-enable` | • Perform this step on every router. |
| **Step 8** | **ip pim rp-address** *rp-address* [*access-list*] [**override**] **bidir**<br>**Example:**<br>`Switch(config)# ip pim rp-address 10.0.1.1 45 bidir` | Configures the address of a PIM RP for a particular group.<br>• Perform this step on every router.<br>• This command defines the RP as bidirectional and defines the bidirectional group by way of the access list.<br>• The optional **override** keyword is used to specify that if dynamic and static group-to-RP mappings are used together and there is an RP address conflict, the RP address configured for a static group-to-RP mapping will take precedence.<br>**Note** If the **override** keyword is not specified and there is RP address conflict, dynamic group-to-RP mappings will take precedence over static group-to-RP mappings. |
| **Step 9** | **end**<br>**Example:**<br>`Switch(config-if)# end` | Exits interface configuration mode and returns to privileged EXEC mode. |
| **Step 10** | Repeat Steps 2 through 9 on every multicast-enabled interface on every router. | -- |
| **Step 11** | **show ip pim rp** [**mapping**] [*rp-address*]<br>**Example:**<br>`Switch# show ip pim rp` | (Optional) Displays active RPs that are cached with associated multicast routing entries. |
| **Step 12** | **show ip mroute**<br>**Example:**<br>`Switch# show ip mroute` | (Optional) Displays the contents of the IP mroute table. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 13** | **show ip pim interface** [*type number*] [**df** \| **count**] [*rp-address*]<br><br>**Example:**<br><br>`Switch# show ip pim interface` | (Optional) Displays information about the elected DF for each RP of an interface, along with the unicast routing metric associated with the DF. |
| **Step 14** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

**Related Topics**

Bidir-PIM Overview, on page 17

# Verifying PIM Operations

## Verifying IP Multicast Operation in a PIM-SM or a PIM-SSM Network

When you verify the operation of IP multicast in a PIM-SM network environment or in an PIM-SSM network environment, a useful approach is to begin the verification process on the last hop router, and then continue the verification process on the routers along the SPT until the first hop router has been reached. The goal of the verification is to ensure that IP multicast traffic is being routed properly through an IP multicast network.

Perform the following optional tasks to verify IP multicast operation in a PIM-SM or a PIM-SSM network. The steps in these tasks help to locate a faulty hop when sources and receivers are not operating as expected.

**Note** If packets are not reaching their expected destinations, you might want consider disabling IP multicast fast switching, which would place the router in process switching mode. If packets begin reaching their proper destinations after IP multicast fast switching has been disabled, then the issue most likely was related to IP multicast fast switching.

### Verifying IP Multicast on the First Hop Router

Enter these commands on the first hop router to verify IP multicast operations on the first hop router:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **show ip mroute** [*group-address*]<br><br>**Example:**<br>`Switch# show ip mroute 239.1.2.3`<br>`(*, 239.1.2.3), 00:18:10/stopped, RP 172.16.0.1, flags: SPF`<br>`  Incoming interface: Serial1/0, RPF nbr 172.31.200.2`<br>`  Outgoing interface list: Null`<br><br>`(10.0.0.1, 239.1.2.3), 00:18:10/00:03:22, flags: FT`<br>`  Incoming interface: GigabitEthernet0/0/0, RPF nbr 0.0.0.0`<br><br>`  Outgoing interface list:`<br>`  Serial1/0, Forward/Sparse-Dense, 00:18:10/00:03:19` | Confirms that the F flag has been set for mroutes on the first hop router. |
| **Step 3** | **show ip mroute active** [*kb/s*]<br><br>**Example:**<br>`Switch# show ip mroute active`<br>`Active IP Multicast Sources - sending >= 4 kbps`<br><br>`Group: 239.1.2.3, (?)`<br>`  Source: 10.0.0.1 (?)`<br>`  Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)` | Displays information about active multicast sources sending to groups. The output of this command provides information about the multicast packet rate for active sources.<br><br>**Note** By default, the output of the **show ip mroute** command with the **active** keyword displays information about active sources sending traffic to groups at a rate greater than or equal to 4 kb/s. To display information about active sources sending low-rate traffic to groups (that is, traffic less than 4 kb/s), specify a value of 1 for the *kb/s* argument. Specifying a value of 1 for this argument displays information about active sources sending traffic to groups at a rate equal to or greater than 1 kb/s, which effectively displays information about all possible active source traffic. |

## Verifying IP Multicast on Routers Along the SPT

Enter these commands on routers along the SPT to verify IP multicast operations on routers along the SPT in a PIM-SM or PIM-SSM network:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **show ip mroute** [*group-address*]<br><br>**Example:**<br>`Switch# show ip mroute 239.1.2.3`<br>`(*, 239.1.2.3), 00:17:56/00:03:02, RP 172.16.0.1, flags: S`<br>`  Incoming interface: Null, RPF nbr 0.0.0.0`<br>`  Outgoing interface list:`<br>`  GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:17:56/00:03:02`<br><br>`(10.0.0.1, 239.1.2.3), 00:15:34/00:03:28, flags: T`<br>`  Incoming interface: Serial1/0, RPF nbr 172.31.200.1`<br>`  Outgoing interface list:`<br>`  GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:15:34/00:03:02` | Confirms the RPF neighbor towards the source for a particular group or groups. |
| **Step 3** | **show ip mroute active**<br><br>**Example:**<br>`Switch# show ip mroute active`<br>`Active IP Multicast Sources - sending >= 4 kbps`<br><br>`Group: 239.1.2.3, (?)`<br>`  Source: 10.0.0.1 (?)`<br>`  Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)` | Displays information about active multicast sources sending to groups. The output of this command provides information about the multicast packet rate for active sources.<br><br>**Note** By default, the output of the **show ip mroute** command with the **active** keyword displays information about active sources sending traffic to groups at a rate greater than or equal to 4 kb/s. To display information about active sources sending low-rate traffic to groups (that is, traffic less than 4 kb/s), specify a value of 1 for the *kb/s* argument. Specifying a value of 1 for this argument displays information about active sources sending traffic to groups at a rate equal to or greater than 1 kb/s, which effectively displays information about all possible active source traffic. |

## Verifying IP Multicast Operation on the Last Hop Router

Enter these commands on the last hop router to verify IP multicast operations on the last hop router:

## Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **show ip igmp groups**<br><br>**Example:**<br>`Switch# show ip igmp groups`<br>`IGMP Connected Group Membership`<br>`Group Address  Interface  Uptime  Expires  Last Reporter`<br>`239.1.2.3  GigabitEthernet1/0/0  00:05:14  00:02:14  10.1.0.6`<br>`224.0.1.39  GigabitEthernet0/0/0  00:09:11  00:02:08  172.31.100.1` | Verifies IGMP memberships on the last hop router. This information will confirm the multicast groups with receivers that are directly connected to the last hop router and that are learned through IGMP. |
| **Step 3** | **show ip pim rp mapping**<br><br>**Example:**<br>`Switch# show ip pim rp mapping`<br>`PIM Group-to-RP Mappings`<br><br>`Group(s) 224.0.0.0/4`<br>`  RP 172.16.0.1 (?), v2v1`<br>`  Info source: 172.16.0.1 (?), elected via Auto-RP`<br>`  Uptime: 00:09:11, expires: 00:02:47` | Confirms that the group-to-RP mappings are being populated correctly on the last hop router.<br><br>**Note** Ignore this step if you are verifying a last hop router in a PIM-SSM network. The **show ip pim rp mapping**command does not work with routers in a PIM-SSM network because PIM-SSM does not use RPs. In addition, if configured correctly, PIM-SSM groups do not appear in the output of the **show ip pim rp mapping**command. |
| **Step 4** | **show ip mroute**<br><br>**Example:**<br>`Switch# show ip mroute`<br>`(*, 239.1.2.3), 00:05:14/00:03:04, RP 172.16.0.1, flags: SJC`<br>`  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1`<br>`  Outgoing interface list:`<br>`  GigabitEthernet1/0, Forward/Sparse-Dense, 00:05:10/00:03:04`<br><br>`(10.0.0.1, 239.1.2.3), 00:02:49/00:03:29, flags: T`<br>`  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1`<br>`  Outgoing interface list:`<br>`  GigabitEthernet1/0, Forward/Sparse-Dense, 00:02:49/00:03:04`<br><br>`(*, 224.0.1.39), 00:10:05/stopped, RP 0.0.0.0, flags: DC` | Verifies that the mroute table is being populated properly on the last hop router. |

| | Command or Action | Purpose |
|---|---|---|
| | Incoming interface: Null, RPF nbr 0.0.0.0<br>Outgoing interface list:<br>GigabitEthernet1/0, Forward/Sparse-Dense, 00:05:15/00:00:00<br>GigabitEthernet0/0, Forward/Sparse-Dense, 00:10:05/00:00:00<br><br>(172.16.0.1, 224.0.1.39), 00:02:00/00:01:33, flags: PTX<br>Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1 | |
| **Step 5** | **show ip interface** [*type number*]<br><br>**Example:**<br>`Switch# show ip interface GigabitEthernet 0/0/0`<br>GigabitEthernet0/0 is up, line protocol is up<br>Internet address is 172.31.100.2/24<br>Broadcast address is 255.255.255.255<br>Address determined by setup command<br>MTU is 1500 bytes<br>Helper address is not set<br>Directed broadcast forwarding is disabled<br>Multicast reserved groups joined: 224.0.0.1 224.0.0.22 224.0.0.13<br>224.0.0.5 224.0.0.6<br>Outgoing access list is not set<br>Inbound access list is not set<br>Proxy ARP is enabled<br>Local Proxy ARP is disabled<br>Security level is default<br>Split horizon is enabled<br>ICMP redirects are always sent<br>ICMP unreachables are always sent<br>ICMP mask replies are never sent<br>IP fast switching is enabled<br>IP fast switching on the same interface is disabled<br>IP Flow switching is disabled<br>IP CEF switching is disabled<br>IP Fast switching turbo vector<br>IP multicast fast switching is enabled<br>IP multicast distributed fast switching is disabled<br>IP route-cache flags are Fast<br>Router Discovery is disabled<br>IP output packet accounting is disabled<br>IP access violation accounting is disabled<br>TCP/IP header compression is disabled<br>RTP/IP header compression is disabled<br>Policy routing is disabled<br>Network address translation is disabled<br>WCCP Redirect outbound is disabled<br>WCCP Redirect inbound is disabled<br>WCCP Redirect exclude is disabled<br>BGP Policy Mapping is disabled | Verifies that multicast fast switching is enabled for optimal performance on the outgoing interface on the last hop router.<br><br>**Note** Using the **no ip mroute-cache** interface command disables IP multicast fast-switching. When IP multicast fast switching is disabled, packets are forwarded through the process-switched path. |
| **Step 6** | **show ip pim interface count**<br><br>**Example:**<br>`Switch# show ip pim interface count`<br><br>State: * - Fast Switched, D - Distributed Fast Switched<br>H - Hardware Switching Enabled<br>Address Interface FS | Confirms that multicast traffic is being forwarded on the last hop router. |

| | Command or Action | Purpose |
|---|---|---|
| | Mpackets In/Out<br>172.31.100.2 GigabitEthernet0/0/0 *<br>4122/0<br>10.1.0.1 GigabitEthernet1/0/0 *<br>0/3193 | |
| **Step 7** | **show ip mroute count**<br><br>**Example:**<br>Switch# **show ip mroute count**<br>IP Multicast Statistics<br>6 routes using 4008 bytes of memory<br>3 groups, 1.00 average sources per group<br>Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second<br>Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)<br><br>Group: 239.1.2.3, Source count: 1, Packets forwarded: 3165, Packets received: 3165<br>RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0<br>Source: 10.0.0.1/32, Forwarding: 3165/20/28/4, Other: 0/0/0<br><br>Group: 224.0.1.39, Source count: 1, Packets forwarded: 21, Packets received: 120<br>Source: 172.16.0.1/32, Forwarding: 21/1/48/0, Other: 120/0/99<br><br>Group: 224.0.1.40, Source count: 1, Packets forwarded: 10, Packets received: 10<br>Source: 172.16.0.1/32, Forwarding: 10/1/48/0, Other: 10/0/0 | Confirms that multicast traffic is being forwarded on the last hop router. |
| **Step 8** | **show ip mroute active** [*kb/s*]<br><br>**Example:**<br>Switch# **show ip mroute active**<br>Active IP Multicast Sources - sending >= 4 kbps<br><br>Group: 239.1.2.3, (?)<br>Source: 10.0.0.1 (?)<br>Rate: 20 pps/4 kbps(1sec), 4 kbps(last 50 secs), 4 kbps(life avg) | Displays information about active multicast sources sending traffic to groups on the last hop router. The output of this command provides information about the multicast packet rate for active sources.<br><br>**Note** By default, the output of the **show ip mroute** command with the **active** keyword displays information about active sources sending traffic to groups at a rate greater than or equal to 4 kb/s. To display information about active sources sending low-rate traffic to groups (that is, traffic less than 4 kb/s), specify a value of 1 for the *kb/s* argument. Specifying a value of 1 for this argument displays information about active sources sending traffic to groups at a rate equal to or greater than 1 kb/s, which effectively displays information about all possible active source traffic. |

## Using PIM-Enabled Routers to Test IP Multicast Reachability

If all the PIM-enabled routers and access servers that you administer are members of a multicast group, pinging that group causes all routers to respond, which can be a useful administrative and debugging tool.

To use PIM-enabled routers to test IP multicast reachability, perform the following tasks:

### Configuring Routers to Respond to Multicast Pings

Follow these steps to configure a router to respond to multicast pings. Perform the task on all the interfaces of a router and on all the routers participating in the multicast network:

#### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br><br>`Switch(config)# interface gigabitethernet 1/0/0` | Enters interface configuration mode.<br><br>For the *type* and *number* arguments, specify an interface that is directly connected to hosts or is facing hosts. |
| **Step 4** | **ip igmp join-group** *group-address*<br><br>**Example:**<br><br>`Switch(config-if)# ip igmp join-group 225.2.2.2` | (Optional) Configures an interface on the router to join the specified group.<br><br>For the purpose of this task, configure the same group address for the *group-address* argument on all interfaces on the router participating in the multicast network.<br><br>**Note** With this method, the router accepts the multicast packets in addition to forwarding them. Accepting the multicast packets prevents the router from fast switching. |
| **Step 5** | Repeat Step 3 and Step 4 for each interface on the router participating in the multicast network. | -- |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **end**<br><br>**Example:**<br><br>`Switch(config-if)# end` | Ends the current configuration session and returns to privileged EXEC mode. |

### Pinging Routers Configured to Respond to Multicast Pings

Follow these steps on a router to initiate a ping test to the routers configured to respond to multicast pings. This task is used to test IP multicast reachability in a network.

#### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **ping** *group-address*<br><br>**Example:**<br><br>`Switch# ping 225.2.2.2` | Pings an IP multicast group address.<br><br>A successful response indicates that the group address is functioning. |

# Monitoring and Troubleshooting PIM

## Monitoring PIM Information

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

***Table 2: PIM Monitoring Commands***

| Command | Purpose |
|---|---|
| **show ip pim interface** | Displays information about interfaces configured for Protocol Independent Multicast (PIM). |
| **show ip pim neighbor** | Displays the PIM neighbor information. |

| Command | Purpose |
|---|---|
| **show ip pim rp**[*group-name* \| *group-address*] | Displays RP routers associated with a sparse-mode multicast group. This command is available in all software images. |

# 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 3: RP Mapping Monitoring Commands***

| Command | Purpose |
|---|---|
| **show ip pim rp** [[*group-name* \| *group-address*] \| **mapping**] | Displays all available RP mappings and metrics.<br>• (Optional) For *group-name*, specify the name of the group about which to display RPs.<br>• (Optional) For *group-address*, specify the address of the group about which to display RPs.<br>• (Optional) Use the **mapping** keyword to display all group-to-RP mappings of which the Cisco device is aware (either configured or learned from Auto-RP). |
| **show ip pim rp-hash** *group* | Displays the RP that was selected for the specified group. That is, on a PIMv2 router or multilayer switch, confirms that the same RP is the one that a PIMv1 system chooses. For *group*, enter the group address for which to display RP information. |

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

***Table 4: BSR Monitoring Commands***

| Command | Purpose |
|---|---|
| **show ip pim bsr** | Displays information about the elected BSR. |

# 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).

### Related Topics

PIM Versions, on page 7

# 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 **spare-dense-mode** enabled. PIM stub routing is enabled on the VLAN 100 interfaces and on Gigabit Ethernet port 20.

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

### Related Topics

Enabling PIM Stub Routing , on page 22

PIM Stub Routing, on page 7

## Example: Verifying PIM Stub Routing

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

```
Switch# 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
```

### Related Topics

Enabling PIM Stub Routing , on page 22
PIM Stub Routing, on page 7

# 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:

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

### Related Topics

Manually Assigning an RP to Multicast Groups , on page 24

# 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 switch serves as RP:

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

### Related Topics

Setting Up Auto-RP in a New Internetwork , on page 26
Auto-RP, on page 9

# 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:

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

### Related Topics

Defining the IP Multicast Boundary , on page 38

# 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:

```
Switch(config)# ip pim rp-announce-filter rp-list 10 group-list 20
Switch(config)# access-list 10 permit host 172.16.5.1
Switch(config)# access-list 10 permit host 172.16.2.1
Switch(config)# access-list 20 deny 239.0.0.0 0.0.255.255
Switch(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 , on page 34

# 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:

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

### Related Topics

Preventing Join Messages to False RPs , on page 34

# 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.

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

### Related Topics

Configuring Candidate BSRs , on page 40
Bootstrap Router, on page 10

# Example: Configuring Candidate RPs

This example shows how to configure the switch 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.

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

### Related Topics

Configuring the Candidate RPs , on page 41

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| For complete syntax and usage information for the commands used in this chapter. | *Command Reference, Cisco IOS Release 15.2(2)E (Catalyst 3750-X and 3560-X Switches)* |
| Configuring Bidirection Forwarding Detection, Configuring EIGRP | *Software Configuration Guide, Cisco IOS Release 15.2(2)E (Catalyst 3750-X and 3560-X Switches)* |
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| Cisco IOS IP SLAs commands | Cisco IOS IP Multicast Command Reference |

### Error Message Decoder

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

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| PIM is defined in RFC 4601 and in these Internet Engineering Task Force (IETF) Internet drafts. | • *Protocol Independent Multicast (PIM): Motivation and Architecture*<br>• *Protocol Independent Multicast (PIM), Dense Mode Protocol Specification*<br>• *Protocol Independent Multicast (PIM), Sparse Mode Protocol Specification*<br>• *draft-ietf-idmr-igmp-v2-06.txt, Internet Group Management Protocol, Version 2*<br>• *draft-ietf-pim-v2-dm-03.txt, PIM Version 2 Dense Mode* |

### MIBs

| MIB | MIBs Link |
|---|---|
| All 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:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>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.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/support |