



## Configuring IP Multicast Routing

---

This chapter describes how to configure IP multicast routing on the Cisco ME 3400 Ethernet Access switch. IP multicasting is a more efficient way to use network resources, especially for bandwidth-intensive services such as audio and video. IP multicast routing enables a host (source) to send packets to a group of hosts (receivers) anywhere within the IP network by using a special form of IP address called the *IP multicast group address*. The sending host inserts the multicast group address into the IP destination address field of the packet, and IP multicast routers and multilayer switches forward incoming IP multicast packets out all interfaces that lead to members of the multicast group. Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message.

To use this feature, the switch must be running the metro IP access image.



### Note

For complete syntax and usage information for the commands used in this chapter, see the *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2*.

---

This chapter consists of these sections:

- [Understanding Cisco's Implementation of IP Multicast Routing, page 34-2](#)
- [Configuring IP Multicast Routing, page 34-7](#)
- [Configuring Advanced PIM Features, page 34-21](#)
- [Configuring Optional IGMP Features, page 34-25](#)
- [Configuring Optional Multicast Routing Features, page 34-31](#)
- [Monitoring and Maintaining IP Multicast Routing, page 34-34](#)

For information on configuring the Multicast Source Discovery Protocol (MSDP), see [Chapter 35, "Configuring MSDP."](#)

# Understanding Cisco's Implementation of IP Multicast Routing

The switch supports these protocols to implement IP multicast routing:

- Internet Group Management Protocol (IGMP) is used among hosts on a LAN and the routers (and multilayer switches) on that LAN to track the multicast groups of which hosts are members.
- Protocol-Independent Multicast (PIM) protocol is used among routers and multilayer switches to track which multicast packets to forward to each other and to their directly connected LANs.

This section contains this information:

- [Understanding IGMP, page 34-2](#)
- [Understanding PIM, page 34-3](#)
- [Configuring IP Multicast Routing, page 34-7](#)

## Understanding IGMP

To participate in IP multicasting, multicast hosts, routers, and multilayer switches must have the IGMP operating. This protocol defines the querier and host roles:

- A querier is a network device that sends query messages to discover which network devices are members of a given multicast group.
- A host is a receiver that sends report messages (in response to query messages) to inform a querier of a host membership.

A set of queriers and hosts that receive multicast data streams from the same source is called a multicast group. Queriers and hosts use IGMP messages to join and leave multicast groups.

Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message. Membership in a multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. A host can be a member of more than one multicast group at a time. How active a multicast group is and what members it has can vary from group to group and from time to time. A multicast group can be active for a long time, or it can be very short-lived. Membership in a group can constantly change. A group that has members can have no activity.

IP multicast traffic uses group addresses, which are class D addresses. The high-order bits of a Class D address are 1110. Therefore, host group addresses can be in the range 224.0.0.0 through 239.255.255.255. Multicast addresses in the range 224.0.0.0 to 240.0.0.255 are reserved for use by routing protocols and other network control traffic. The address 224.0.0.0 is guaranteed not to be assigned to any group.

IGMP packets are sent using these IP multicast group addresses:

- IGMP general queries are destined to the address 224.0.0.1 (all systems on a subnet).
- IGMP group-specific queries are destined to the group IP address for which the switch is querying.
- IGMP group membership reports are destined to the group IP address for which the switch is reporting.
- IGMP Version 2 (IGMPv2) leave messages are destined to the address 224.0.0.2 (all-multicast-routers on a subnet). In some old host IP stacks, leave messages might be destined to the group IP address rather than to the all-routers address.

## IGMP Version 1

IGMP Version 1 (IGMPv1) primarily uses a query-response model that enables the multicast router and multilayer switch to find which multicast groups are active (have one or more hosts interested in a multicast group) on the local subnet. IGMPv1 has other processes that enable a host to join and leave a multicast group. For more information, see RFC 1112.

## IGMP Version 2

IGMPv2 extends IGMP functionality by providing such features as the IGMP leave process to reduce leave latency, group-specific queries, and an explicit maximum query response time. IGMPv2 also adds the capability for routers to elect the IGMP querier without depending on the multicast protocol to perform this task. For more information, see RFC 2236.

## Understanding PIM

PIM is called *protocol-independent*: regardless of the unicast routing protocols used to populate the unicast routing table, PIM uses this information to perform multicast forwarding instead of maintaining a separate multicast routing table.

PIM is defined in RFC 2362, *Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*. PIM is defined in these Internet Engineering Task Force (IETF) Internet drafts:

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

## PIM Versions

PIMv2 includes these improvements over PIMv1:

- A single, active rendezvous point (RP) exists per multicast group, with multiple backup RPs. This single RP compares to multiple active RPs for the same group in PIMv1.
- A bootstrap router (BSR) provides a fault-tolerant, automated RP discovery and distribution mechanism 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. We strongly recommend 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 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.

## PIM Modes

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

### PIM DM

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

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

### PIM SM

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

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

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

## Auto-RP

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

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

Mapping agents periodically multicast the contents of their Group-to-RP mapping cache. Thus, all routers and switches automatically discover which RP to use for the groups they support. If a router or switch fails to receive RP-discovery messages and the Group-to-RP mapping information expires, it

switches to a statically configured RP that was defined with the **ip pim rp-address** global configuration command. If no statically configured RP exists, the router or switch changes the group to dense-mode operation.

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

## Bootstrap Router

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

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

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

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

## Multicast Forwarding and Reverse Path Check

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

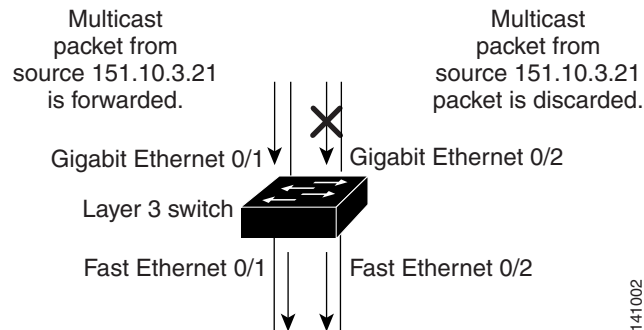
With multicasting, the source is sending traffic to an arbitrary group of hosts represented by a multicast group address in the destination address field of the IP packet. To decide whether to forward or drop an incoming multicast packet, the router or multilayer switch uses a reverse path forwarding (RPF) check on the packet as follows and shown in [Figure 34-1](#):

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

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

Figure 34-1 shows port 2 receiving a multicast packet from source 151.10.3.21. Table 34-1 shows that the port on the reverse path to the source is port 1, not port 2. Because the RPF check fails, the multilayer switch discards the packet. Another multicast packet from source 151.10.3.21 is received on port 1, and the routing table shows this port is on the reverse path to the source. Because the RPF check passes, the switch forwards the packet to all port in the outgoing port list.

**Figure 34-1 RPF Check**



**Table 34-1 Routing Table Example for an RPF Check**

Network	Port
151.10.0.0/16	Gigabit Ethernet 0/1
198.14.32.0/32	Fast Ethernet 0/1
204.1.16.0/24	Fast Ethernet 0/2

PIM uses both source trees and RP-rooted shared trees to forward datagrams (described in the “PIM DM” section on page 34-4 and the “PIM SM” section on page 34-4). 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).

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.

Dense-mode PIM uses only source trees and use RPF as previously described.

# Configuring IP Multicast Routing

These sections contain this configuration information:

- [Default Multicast Routing Configuration, page 34-7](#)
- [Multicast Routing Configuration Guidelines, page 34-7](#)
- [Configuring Basic Multicast Routing, page 34-9](#) (required)
- [Configuring a Rendezvous Point, page 34-10](#) (required if the interface is in sparse-dense mode, and you want to treat the group as a sparse group)
- [Using Auto-RP and a BSR, page 34-20](#) (required for non-Cisco PIMv2 devices to interoperate with Cisco PIM v1 devices))
- [Monitoring the RP Mapping Information, page 34-21](#) (optional)
- [Troubleshooting PIMv1 and PIMv2 Interoperability Problems, page 34-21](#) (optional)

## Default Multicast Routing Configuration

[Table 34-2](#) shows the default multicast routing configuration.

**Table 34-2** *Default Multicast Routing Configuration*

Feature	Default Setting
Multicast routing	Disabled on all interfaces.
PIM version	Version 2.
PIM mode	No mode is defined.
PIM RP address	None configured.
PIM domain border	Disabled.
PIM multicast boundary	None.
Candidate BSRs	Disabled.
Candidate RPs	Disabled.
Shortest-path tree threshold rate	0 kbps.
PIM router query message interval	30 seconds.

## Multicast Routing Configuration Guidelines

To avoid misconfiguring multicast routing on your switch, review the information in these sections:

- [PIMv1 and PIMv2 Interoperability, page 34-8](#)
- [Auto-RP and BSR Configuration Guidelines, page 34-8](#)

## PIMv1 and PIMv2 Interoperability

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. We recommend that you use PIMv2. The BSR mechanism interoperates with Auto-RP on Cisco routers and multilayer switches. For more information, see the [“Auto-RP and BSR Configuration Guidelines” section on page 34-8](#).

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 have these recommendations:

- Use Auto-RP throughout the region.
- Configure sparse-dense mode throughout the region.

If Auto-RP is not already configured in the PIMv1 regions, configure Auto-RP. For more information, see the [“Configuring Auto-RP” section on page 34-12](#).

## Auto-RP and BSR Configuration Guidelines

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.

- 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.
- 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. For more information, see the [“Using Auto-RP and a BSR”](#) section on page 34-20.

## Configuring Basic Multicast Routing

You must enable IP multicast routing and configure the PIM version and the PIM mode. Then the software can forward multicast packets, and the switch can populate its multicast routing table.



### Note

To enable IP multicast routing, the switch must be running the metro IP access image.

You can configure an interface to be in PIM dense mode, sparse mode, or sparse-dense mode. The switch populates its multicast routing table and forwards multicast packets it receives from its directly connected LANs according to the mode setting. You must enable PIM in one of these modes for an interface to perform IP multicast routing. Enabling PIM on an interface also enables IGMP operation on that interface.

In populating the multicast routing table, dense-mode interfaces are always added to the table. Sparse-mode interfaces are added to the table only when periodic join messages are received from downstream devices or when there is a directly connected member on the interface. When forwarding from a LAN, sparse-mode operation occurs if there is an RP 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 receiver’s first-hop router might send join messages toward the source to build a source-based distribution tree.

By default, multicast routing is disabled, and there is no default mode setting. This procedure is required.

Beginning in privileged EXEC mode, follow these steps to enable IP multicasting, to configure a PIM version, and to configure a PIM mode. This procedure is required.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ip multicast-routing distributed</b>	Enable IP multicast distributed switching.
Step 3	<b>interface</b> <i>interface-id</i>	Specify the Layer 3 interface on which you want to enable multicast routing, and enter interface configuration mode.  The specified interface must be one of the following: <ul style="list-style-type: none"> <li>• A routed port: a physical port that has been configured as a Layer 3 port by entering the <b>no switchport</b> interface configuration command.</li> <li>• An SVI: a VLAN interface created by using the <b>interface vlan</b> <i>vlan-id</i> global configuration command.</li> </ul> These interfaces must have IP addresses assigned to them. For more information, see the <a href="#">“Configuring Layer 3 Interfaces”</a> section on page 9-20.
Step 4	<b>no shutdown</b>	Enable the port, if necessary. By default, user network interfaces (UNIs) are disabled, and network node interfaces (NNIs) are enabled.

	Command	Purpose
Step 5	<code>ip pim version [1   2]</code>	<p>Configure the PIM version on the interface.</p> <p>By default, Version 2 is enabled and is the recommended setting.</p> <p>An interface in PIMv2 mode automatically downgrades to PIMv1 mode if that interface has a PIMv1 neighbor. The interface returns to Version 2 mode after all Version 1 neighbors are shut down or upgraded.</p> <p>For more information, see the <a href="#">“PIMv1 and PIMv2 Interoperability” section on page 34-8</a>.</p>
Step 6	<code>ip pim {dense-mode   sparse-mode   sparse-dense-mode}</code>	<p>Enable a PIM mode on the interface.</p> <p>By default, no mode is configured.</p> <p>The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>dense-mode</b>—Enables dense mode of operation.</li> <li>• <b>sparse-mode</b>—Enables sparse mode of operation. If you configure sparse-mode, you must also configure an RP. For more information, see the <a href="#">“Configuring a Rendezvous Point” section on page 34-10</a>.</li> <li>• <b>sparse-dense-mode</b>—Causes the interface to be treated in the mode in which the group belongs. Sparse-dense-mode is the recommended setting.</li> </ul> <p><b>Note</b> After you enable a PIM mode on the interface, the <b>ip mroute-cache distributed</b> interface configuration command is automatically entered for the interface and appears in the running configuration.</p>
Step 7	<code>end</code>	Return to privileged EXEC mode.
Step 8	<code>show running-config</code>	Verify your entries.
Step 9	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

To disable multicasting, use the **no ip multicast-routing distributed** global configuration command. To return to the default PIM version, use the **no ip pim version** interface configuration command. To disable PIM on an interface, use the **no ip pim** interface configuration command.

## Configuring a Rendezvous Point

You must have an RP if the interface is in sparse-dense mode and if you want to treat the group as a sparse group. You can use several methods, as described in these sections:

- [Manually Assigning an RP to Multicast Groups, page 34-11](#)
- [Configuring Auto-RP, page 34-12](#) (a standalone, Cisco-proprietary protocol separate from PIMv1)
- [Configuring PIMv2 BSR, page 34-16](#) (a standards track protocol in the Internet Engineering Task Force (IETF))

You can use Auto-RP, BSR, or a combination of both, depending on the PIM version you are running and the types of routers in your network. For more information, see the [“PIMv1 and PIMv2 Interoperability” section on page 34-8](#) and the [“Auto-RP and BSR Configuration Guidelines” section on page 34-8](#).

## Manually Assigning an RP to Multicast Groups

This section explains how to manually configure an RP. If the 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's 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. RPs are not members of the multicast group; rather, 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 treats the group as dense and uses the dense-mode PIM techniques.

Beginning in privileged EXEC mode, follow these steps to manually configure the address of the RP. This procedure is optional.

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ip pim rp-address ip-address [access-list-number] [override]</code>	<p>Configure the address of a PIM RP.</p> <p>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). If there is no RP configured for a group, the switch treats the group as dense, using the dense-mode PIM techniques.</p> <p>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.</p> <ul style="list-style-type: none"> <li>For <i>ip-address</i>, enter the unicast address of the RP in dotted-decimal notation.</li> <li>(Optional) For <i>access-list-number</i>, enter an IP standard access list number from 1 to 99. If no access list is configured, the RP is used for all groups.</li> <li>(Optional) The <b>override</b> keyword means that if there is a conflict between the RP configured with this command and one learned by Auto-RP or BSR, the RP configured with this command prevails.</li> </ul>
Step 3	<code>access-list access-list-number {deny   permit} source [source-wildcard]</code>	<p>Create a standard access list, repeating the command as many times as necessary.</p> <ul style="list-style-type: none"> <li>For <i>access-list-number</i>, enter the access list number specified in Step 2.</li> <li>The <b>deny</b> keyword denies access if the conditions are matched. The <b>permit</b> keyword permits access if the conditions are matched.</li> <li>For <i>source</i>, enter the multicast group address for which the RP should be used.</li> <li>(Optional) For <i>source-wildcard</i>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</li> </ul> <p>Recall that the access list is always terminated by an implicit deny statement for everything.</p>
Step 4	<code>end</code>	Return to privileged EXEC mode.

	Command	Purpose
Step 5	<code>show running-config</code>	Verify your entries.
Step 6	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

To remove an RP address, use the **no ip pim rp-address** *ip-address* [*access-list-number*] [**override**] global configuration command.

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
```

## Configuring Auto-RP

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

- It is easy to use multiple RPs within a network to serve different group ranges.
- It provides load splitting among different RPs and arrangement of RPs according to the location of group participants.
- It avoids inconsistent, manual RP configurations on every router and multilayer switch in a PIM network, which can cause connectivity problems.



### Note

If you configure PIM in sparse mode or sparse-dense mode and do not configure Auto-RP, you must manually configure an RP as described in the [“Manually Assigning an RP to Multicast Groups”](#) section on page 34-11.



### Note

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.

These sections describe how to configure Auto-RP:

- [Setting up Auto-RP in a New Internetwork](#), page 34-12 (optional)
- [Adding Auto-RP to an Existing Sparse-Mode Cloud](#), page 34-13 (optional)
- [Preventing Join Messages to False RPs](#), page 34-14 (optional)
- [Filtering Incoming RP Announcement Messages](#), page 34-15 (optional)

For overview information, see the [“Auto-RP”](#) section on page 34-4.

### 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. Follow the process described in the [“Adding Auto-RP to an Existing Sparse-Mode Cloud”](#) section on page 34-13. However, omit Step 3 if you want to configure a PIM router as the RP for the local group.

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

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

Beginning in privileged EXEC mode, follow these steps to deploy Auto-RP in an existing sparse-mode cloud. This procedure is optional.

	Command	Purpose
Step 1	<code>show running-config</code>	<p>Verify that a default RP is already configured on all PIM devices and the RP in the sparse-mode network. It was previously configured with the <code>ip pim rp-address</code> global configuration command.</p> <p>This step is not required for sparse-dense-mode environments.</p> <p>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.</p>
Step 2	<code>configure terminal</code>	Enter global configuration mode.
Step 3	<code>ip pim send-rp-announce interface-id scope ttl group-list access-list-number interval seconds</code>	<p>Configure another PIM device to be the candidate RP for local groups.</p> <ul style="list-style-type: none"> <li>For <code>interface-id</code>, enter the interface type and number that identifies the RP address. Valid interfaces include physical ports, port channels, and VLANs.</li> <li>For <code>scope ttl</code>, specify the time-to-live value in hops. Enter a hop count that is high enough so that the RP-announce messages reach all mapping agents in the network. There is no default setting. The range is 1 to 255.</li> <li>For <code>group-list access-list-number</code>, enter an IP standard access list number from 1 to 99. If no access list is configured, the RP is used for all groups.</li> <li>For <code>interval seconds</code>, specify how often the announcement messages must be sent. The default is 60 seconds. The range is 1 to 16383.</li> </ul>
Step 4	<code>access-list access-list-number {deny   permit} source [source-wildcard]</code>	<p>Create a standard access list, repeating the command as many times as necessary.</p> <ul style="list-style-type: none"> <li>For <code>access-list-number</code>, enter the access list number specified in Step 3.</li> <li>The <code>deny</code> keyword denies access if the conditions are matched. The <code>permit</code> keyword permits access if the conditions are matched.</li> <li>For <code>source</code>, enter the multicast group address range for which the RP should be used.</li> <li>(Optional) For <code>source-wildcard</code>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</li> </ul> <p>Recall that the access list is always terminated by an implicit deny statement for everything.</p>

	Command	Purpose
Step 5	<b>ip pim send-rp-discovery scope ttl</b>	Find a switch whose connectivity is not likely to be interrupted, and assign it the role of RP-mapping agent.  For <b>scope ttl</b> , specify the time-to-live value in hops to limit the RP discovery packets. All devices within the hop count from the source device receive the Auto-RP discovery messages. These messages tell other devices which group-to-RP mapping to use to avoid conflicts (such as overlapping group-to-RP ranges). There is no default setting. The range is 1 to 255.
Step 6	<b>end</b>	Return to privileged EXEC mode.
Step 7	<b>show running-config</b> <b>show ip pim rp mapping</b> <b>show ip pim rp</b>	Verify your entries.  Display active RPs that are cached with associated multicast routing entries.  Display the information cached in the routing table.
Step 8	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To remove the PIM device configured as the candidate RP, use the **no ip pim send-rp-announce interface-id** global configuration command. To remove the switch as the RP-mapping agent, use the **no ip pim send-rp-discovery** global configuration command.

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 gigabitethernet0/1 scope 31 group-list 5
Switch(config)# access-list 5 permit 224.0.0.0 15.255.255.255
```

### Preventing Join Messages to False RPs

Find 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. This procedure is optional.

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
```

## 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.

Beginning in privileged EXEC mode, follow these steps to filter incoming RP announcement messages. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ip pim rp-announce-filter rp-list access-list-number group-list access-list-number</b>	<p>Filter incoming RP announcement messages.</p> <p>Enter this command on each mapping agent in the network. Without this command, all incoming RP-announce messages are accepted by default.</p> <p>For <b>rp-list access-list-number</b>, configure an access list of candidate RP addresses that, if permitted, is accepted for the group ranges supplied in the <b>group-list access-list-number</b> variable. If this variable is omitted, the filter applies to all multicast groups.</p> <p>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.</p>
Step 3	<b>access-list access-list-number {deny   permit} source [source-wildcard]</b>	<p>Create a standard access list, repeating the command as many times as necessary.</p> <ul style="list-style-type: none"> <li>For <i>access-list-number</i>, enter the access list number specified in Step 2.</li> <li>The <b>deny</b> keyword denies access if the conditions are matched. The <b>permit</b> keyword permits access if the conditions are matched.</li> <li>Create an access list that specifies from which routers and multilayer switches the mapping agent accepts candidate RP announcements (rp-list ACL).</li> <li>Create an access list that specifies the range of multicast groups from which to accept or deny (group-list ACL).</li> <li>For <i>source</i>, enter the multicast group address range for which the RP should be used.</li> <li>(Optional) For <i>source-wildcard</i>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</li> </ul> <p>Recall that the access list is always terminated by an implicit deny statement for everything.</p>
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show running-config</b>	Verify your entries.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

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.

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
```

In this example, 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.

## Configuring PIMv2 BSR

These sections describe how to set up BSR in your PIMv2 network:

- [Defining the PIM Domain Border, page 34-16](#) (optional)
- [Defining the IP Multicast Boundary, page 34-17](#) (optional)
- [Configuring Candidate BSRs, page 34-18](#) (optional)
- [Configuring Candidate RPs, page 34-19](#) (optional)

For overview information, see the “[Bootstrap Router](#)” section on page 34-5.

### Defining the PIM Domain Border

As IP multicast becomes more widespread, the chance of one PIMv2 domain bordering another PIMv2 domain is increasing. Because these 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 these 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 co-mingle candidate RP advertisements, resulting in the election of RPs in the wrong domain.

Beginning in privileged EXEC mode, follow these steps to define the PIM domain border. This procedure is optional.

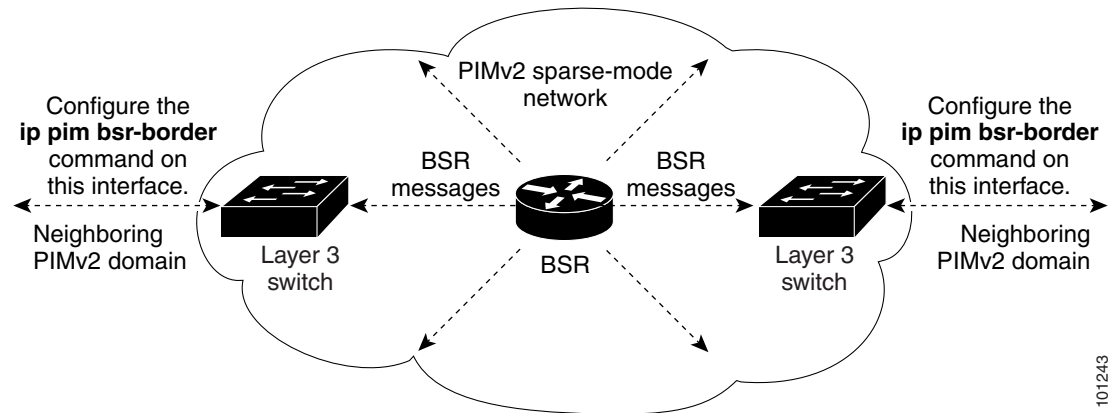
	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Specify the interface to be configured, and enter interface configuration mode.
Step 3	<b>no shutdown</b>	Enable the port, if necessary. By default, UNIs are disabled, and NNIs are enabled.
Step 4	<b>ip pim bsr-border</b>	Define a PIM bootstrap message boundary for the PIM domain. Enter this command on each interface that connects to other bordering PIM domains. This command instructs the switch to neither send or receive PIMv2 BSR messages on this interface as shown in <a href="#">Figure 34-2</a> .
Step 5	<b>end</b>	Return to privileged EXEC mode.



	Command	Purpose
Step 6	<code>show running-config</code>	Verify your entries.
Step 7	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

To remove the PIM border, use the **no ip pim bsr-border** interface configuration command.

**Figure 34-2** Constraining PIMv2 BSR Messages



101243

## 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.

Beginning in privileged EXEC mode, follow these steps to define a multicast boundary. This procedure is optional.

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>access-list access-list-number deny source [source-wildcard]</code>	Create a standard access list, repeating the command as many times as necessary. <ul style="list-style-type: none"> <li>For <i>access-list-number</i>, the range is 1 to 99.</li> <li>The <b>deny</b> keyword denies access if the conditions are matched.</li> <li>For <i>source</i>, enter multicast addresses 224.0.1.39 and 224.0.1.40, which carry Auto-RP information.</li> <li>(Optional) For <i>source-wildcard</i>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</li> </ul> Recall that the access list is always terminated by an implicit deny statement for everything.
Step 3	<code>interface interface-id</code>	Specify the interface to be configured, and enter interface configuration mode.
Step 4	<code>no shutdown</code>	Enable the port, if necessary. By default, UNIs are disabled, and NNIs are enabled.

	Command	Purpose
Step 5	<b>ip multicast boundary</b> <i>access-list-number</i>	Configure the boundary, specifying the access list you created in Step 2.
Step 6	<b>end</b>	Return to privileged EXEC mode.
Step 7	<b>show running-config</b>	Verify your entries.
Step 8	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To remove the boundary, use the **no ip multicast boundary** interface configuration command.

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)# interface gigabitethernet0/1
Switch(config-if)# ip multicast boundary 1
```

### 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.

Beginning in privileged EXEC mode, follow these steps to configure your switch as a candidate BSR. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ip pim bsr-candidate</b> <i>interface-id</i> <i>hash-mask-length</i> [ <i>priority</i> ]	Configure your switch to be a candidate BSR. <ul style="list-style-type: none"> <li>For <i>interface-id</i>, 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.</li> <li>For <i>hash-mask-length</i>, specify the mask length (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter.</li> <li>(Optional) For <i>priority</i>, enter a number from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the device with the highest IP address is selected as the BSR. The default is 0.</li> </ul>
Step 3	<b>end</b>	Return to privileged EXEC mode.
Step 4	<b>show running-config</b>	Verify your entries.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To remove this device as a candidate BSR, use the **no ip pim bsr-candidate** global configuration command.

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 gigabitethernet0/2
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 gigabitethernet0/2 30 10
```

## Configuring 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. 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.

Beginning in privileged EXEC mode, follow these steps to configure your switch to advertise itself as a PIMv2 candidate RP to the BSR. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ip pim rp-candidate</b> <i>interface-id</i> [ <b>group-list</b> <i>access-list-number</i> ]	Configure your switch to be a candidate RP. <ul style="list-style-type: none"> <li>• For <i>interface-id</i>, specify the interface whose associated IP address is advertised as a candidate RP address. Valid interfaces include physical ports, port channels, and VLANs.</li> <li>• (Optional) For <b>group-list</b> <i>access-list-number</i>, 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.</li> </ul>
Step 3	<b>access-list</b> <i>access-list-number</i> { <b>deny</b>   <b>permit</b> } <i>source</i> [ <i>source-wildcard</i> ]	Create a standard access list, repeating the command as many times as necessary. <ul style="list-style-type: none"> <li>• For <i>access-list-number</i>, enter the access list number specified in Step 2.</li> <li>• The <b>deny</b> keyword denies access if the conditions are matched. The <b>permit</b> keyword permits access if the conditions are matched.</li> <li>• For <i>source</i>, enter the number of the network or host from which the packet is being sent.</li> <li>• (Optional) For <i>source-wildcard</i>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</li> </ul> <p>Recall that the access list is always terminated by an implicit deny statement for everything.</p>
Step 4	<b>end</b>	Return to privileged EXEC mode.

	Command	Purpose
Step 5	<code>show running-config</code>	Verify your entries.
Step 6	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

To remove this device as a candidate RP, use the `no ip pim rp-candidate interface-id` global configuration command.

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 gigabitethernet0/2 group-list 4
Switch(config)# access-list 4 permit 239.0.0.0 0.255.255.255
```

## Using Auto-RP and a BSR

If there are only Cisco devices in your network (no routers from other vendors), there is no need to configure a BSR. Configure Auto-RP in a network that is running both PIMv1 and PIMv2.

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 router or multilayer switch be both the Auto-RP mapping agent and the BSR.

If you must have one or more BSRs, we have these recommendations:

- Configure the candidate BSRs as the RP-mapping agents for Auto-RP. For more information, see the “[Configuring Auto-RP](#)” section on page 34-12 and the “[Configuring Candidate BSRs](#)” section on page 34-18.
- 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.

Beginning in privileged EXEC mode, follow these steps to verify the consistency of group-to-RP mappings. This procedure is optional.

	Command	Purpose
Step 1	<code>show ip pim rp [[group-name   group-address]   mapping]</code>	<p>On any Cisco device, display the available RP mappings.</p> <ul style="list-style-type: none"> <li>• (Optional) For <i>group-name</i>, specify the name of the group about which to display RPs.</li> <li>• (Optional) For <i>group-address</i>, specify the address of the group about which to display RPs.</li> <li>• (Optional) Use the <b>mapping</b> keyword to display all group-to-RP mappings of which the Cisco device is aware (either configured or learned from Auto-RP).</li> </ul>
Step 2	<code>show ip pim rp-hash group</code>	<p>On a PIMv2 router or multilayer switch, confirm that the same RP is the one that a PIMv1 system chooses.</p> <p>For <i>group</i>, enter the group address for which to display RP information.</p>

## Monitoring the RP Mapping Information

To monitor the RP mapping information, use these commands in privileged EXEC mode:

- **show ip pim bsr** displays information about the elected BSR.
- **show ip pim rp-hash** *group* displays the RP that was selected for the specified group.
- **show ip pim rp** [*group-name* | *group-address* | **mapping**] displays how the switch learns of the RP (through the BSR or the Auto-RP mechanism).

## 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 the RPs are interacting with the DRs properly (by responding with register-stops and forwarding decapsulated data packets from registers).

## Configuring Advanced PIM Features

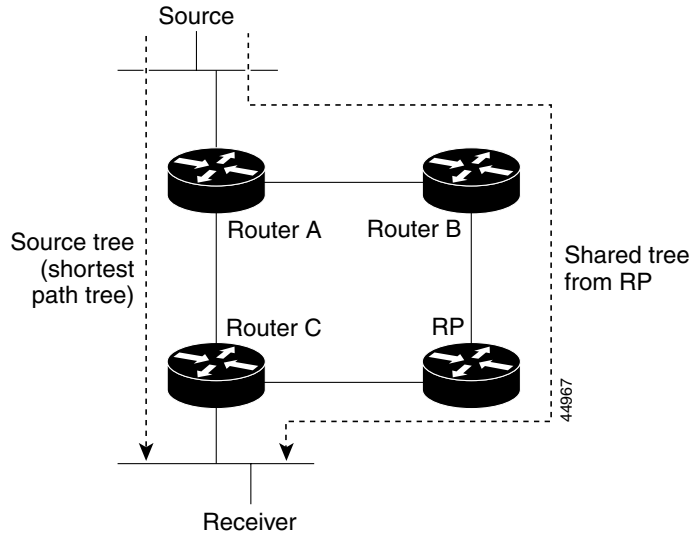
These sections describe the optional advanced PIM features:

- [Understanding PIM Shared Tree and Source Tree, page 34-21](#)
- [Delaying the Use of PIM Shortest-Path Tree, page 34-23](#) (optional)
- [Modifying the PIM Router-Query Message Interval, page 34-24](#) (optional)

## Understanding PIM Shared Tree and Source Tree

By default, members of a group receive data from senders to the group across a single data-distribution tree rooted at the RP. [Figure 34-3](#) 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 34-3 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. For more information, see the [“Delaying the Use of PIM Shortest-Path Tree”](#) section on page 34-23.

## Delaying the Use of PIM Shortest-Path Tree

The change from shared to source tree happens when the first data packet arrives at the last-hop router (Router C in Figure 34-3). This change occurs because the **ip pim spt-threshold** global configuration command controls that timing.

The shortest-path tree requires more memory than the shared tree but reduces delay. You might 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.

Beginning in privileged EXEC mode, follow 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.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>access-list</b> <i>access-list-number</i> { <b>deny</b>   <b>permit</b> } <i>source</i> [ <i>source-wildcard</i> ]	<p>Create a standard access list.</p> <ul style="list-style-type: none"> <li>For <i>access-list-number</i>, the range is 1 to 99.</li> <li>The <b>deny</b> keyword denies access if the conditions are matched. The <b>permit</b> keyword permits access if the conditions are matched.</li> <li>For <i>source</i>, specify the multicast group to which the threshold will apply.</li> <li>(Optional) For <i>source-wildcard</i>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</li> </ul> <p>Recall that the access list is always terminated by an implicit deny statement for everything.</p>
Step 3	<b>ip pim spt-threshold</b> { <i>kbps</i>   <b>infinity</b> } [ <b>group-list</b> <i>access-list-number</i> ]	<p>Specify the threshold that must be reached before moving to shortest-path tree (spt).</p> <ul style="list-style-type: none"> <li>For <i>kbps</i>, specify the traffic rate in kilobits per second. The default is 0 kbps.</li> </ul> <p><b>Note</b> Because of switch hardware limitations, 0 kbps is the only valid entry even though the range is 0 to 4294967.</p> <ul style="list-style-type: none"> <li>Specify <b>infinity</b> if you want all sources for the specified group to use the shared tree, never switching to the source tree.</li> <li>(Optional) For <b>group-list</b> <i>access-list-number</i>, specify the access list created in Step 2. If the value is 0 or if the group-list is not used, the threshold applies to all groups.</li> </ul>

	Command	Purpose
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show running-config</b>	Verify your entries.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no ip pim spt-threshold** {*kbits* | **infinity**} global configuration command.

## Modifying the PIM Router-Query Message Interval

PIM routers and multilayer switches send PIM router-query messages to find which device will be the 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.

Beginning in privileged EXEC mode, follow these steps to modify the router-query message interval. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Specify the interface to be configured, and enter interface configuration mode.
Step 3	<b>no shutdown</b>	Enable the port, if necessary. By default, UNIs are disabled, and NNIs are enabled.
Step 4	<b>ip pim query-interval</b> <i>seconds</i>	Configure the frequency at which the switch sends PIM router-query messages.  The default is 30 seconds. The range is 1 to 65535.
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show ip igmp interface</b> [ <i>interface-id</i> ]	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no ip pim query-interval** [*seconds*] interface configuration command.



# Configuring Optional IGMP Features

These sections contain this configuration information:

- [Default IGMP Configuration, page 34-25](#)
- [Configuring the Switch as a Member of a Group, page 34-25](#) (optional)
- [Controlling Access to IP Multicast Groups, page 34-26](#) (optional)
- [Changing the IGMP Version, page 34-27](#) (optional)
- [Modifying the IGMP Host-Query Message Interval, page 34-28](#) (optional)
- [Changing the IGMP Query Timeout for IGMPv2, page 34-29](#) (optional)
- [Changing the Maximum Query Response Time for IGMPv2, page 34-29](#) (optional)
- [Configuring the Switch as a Statically Connected Member, page 34-30](#) (optional)

## Default IGMP Configuration

Table 34-3 shows the default IGMP configuration.

**Table 34-3**     *Default IGMP Configuration*

Feature	Default Setting
Multilayer switch as a member of a multicast group	No group memberships are defined.
Access to multicast groups	All groups are allowed on an interface.
IGMP version	Version 2 on all interfaces.
IGMP host-query message interval	60 seconds on all interfaces.
IGMP query timeout	60 seconds on all interfaces.
IGMP maximum query response time	10 seconds on all interfaces.
Multilayer switch as a statically connected member	Disabled.

## Configuring the Switch as a Member of a Group

You can configure the switch as a member of a multicast group and discover multicast reachability in a network. If all the multicast-capable routers and multilayer switches that you administer are members of a multicast group, pinging that group causes all these devices to respond. The devices respond to IGMP echo-request packets addressed to a group of which they are members. Another example is the multicast trace-route tools provided in the software.



### Caution

Performing this procedure might impact the CPU performance because the CPU will receive all data traffic for the group address.

Beginning in privileged EXEC mode, follow these steps to configure the switch to be a member of a group. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Specify the interface to be configured, and enter interface configuration mode.
Step 3	<b>no shutdown</b>	Enable the port, if necessary. By default, UNIs are disabled, and NNIs are enabled.
Step 4	<b>ip igmp join-group</b> <i>group-address</i>	Configure the switch to join a multicast group. By default, no group memberships are defined. For <i>group-address</i> , specify the multicast IP address in dotted decimal notation.
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show ip igmp interface</b> [ <i>interface-id</i> ]	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To cancel membership in a group, use the **no ip igmp join-group** *group-address* interface configuration command.

This example shows how to enable the switch to join multicast group 255.2.2.2:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip igmp join-group 255.2.2.2
```

## Controlling Access to IP Multicast Groups

The switch sends IGMP host-query messages to find which multicast groups have members on attached local networks. The switch then forwards to these group members all packets addressed to the multicast group. You can place a filter on each interface to restrict the multicast groups that hosts on the subnet serviced by the interface can join.

Beginning in privileged EXEC mode, follow these steps to filter multicast groups allowed on an interface. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Specify the interface to be configured, and enter interface configuration mode.
Step 3	<b>no shutdown</b>	Enable the port, if necessary. By default, UNIs are disabled, and NNIs are enabled.
Step 4	<b>ip igmp access-group</b> <i>access-list-number</i>	Specify the multicast groups that hosts on the subnet serviced by an interface can join. By default, all groups are allowed on an interface. For <i>access-list-number</i> , specify an IP standard access list number. The range is 1 to 99.

	Command	Purpose
Step 5	<b>exit</b>	Return to global configuration mode.
Step 6	<b>access-list</b> <i>access-list-number</i> { <b>deny</b>   <b>permit</b> } <i>source</i> [ <i>source-wildcard</i> ]	<p>Create a standard access list.</p> <ul style="list-style-type: none"> <li>For <i>access-list-number</i>, specify the access list created in Step 3.</li> <li>The <b>deny</b> keyword denies access if the conditions are matched. The <b>permit</b> keyword permits access if the conditions are matched.</li> <li>For <i>source</i>, specify the multicast group that hosts on the subnet can join.</li> <li>(Optional) For <i>source-wildcard</i>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</li> </ul> <p>Recall that the access list is always terminated by an implicit deny statement for everything.</p>
Step 7	<b>end</b>	Return to privileged EXEC mode.
Step 8	<b>show ip igmp interface</b> [ <i>interface-id</i> ]	Verify your entries.
Step 9	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To disable groups on an interface, use the **no ip igmp access-group** interface configuration command.

This example shows how to configure hosts attached to a port as able to join only group 255.2.2.2:

```
Switch(config)# access-list 1 255.2.2.2 0.0.0.0
Switch(config-if)# interface gigabitethernet0/1
Switch(config-if)# ip igmp access-group 1
```

## Changing the IGMP Version

By default, the switch uses IGMP Version 2, which provides features such as the IGMP query timeout and the maximum query response time.

All systems on the subnet must support the same version. The switch does not automatically detect Version 1 systems and switch to Version 1. You can mix Version 1 and Version 2 hosts on the subnet because Version 2 routers or switches always work correctly with IGMPv1 hosts.

Configure the switch for Version 1 if your hosts do not support Version 2.

Beginning in privileged EXEC mode, follow these steps to change the IGMP version. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Specify the interface to be configured, and enter interface configuration mode.
Step 3	<b>no shutdown</b>	Enable the port, if necessary. By default, UNIs are disabled, and NNIs are enabled.

	Command	Purpose
Step 4	<b>ip igmp version</b> {1   2}	Specify the IGMP version that the switch uses.  <b>Note</b> If you change to Version 1, you cannot configure the <b>ip igmp query-interval</b> or the <b>ip igmp query-max-response-time</b> interface configuration commands.
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show ip igmp interface</b> [ <i>interface-id</i> ]	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no ip igmp version** interface configuration command.

## Modifying the IGMP Host-Query Message Interval

The switch periodically sends IGMP host-query messages to discover which multicast groups are present on attached networks. These messages are sent to the all-hosts multicast group (224.0.0.1) with a time-to-live (TTL) of 1. The switch sends host-query messages to refresh its knowledge of memberships present on the network. If, after some number of queries, the software discovers that no local hosts are members of a multicast group, the software stops forwarding multicast packets to the local network from remote origins for that group and sends a prune message upstream toward the source.

The switch elects a PIM designated router (DR) for the LAN (subnet). The DR is the router or multilayer switch with the highest IP address for IGMPv2. For IGMPv1, the DR is elected according to the multicast routing protocol that runs on the LAN. The designated router is responsible for sending IGMP host-query messages to all hosts on the LAN. In sparse mode, the designated router also sends PIM register and PIM join messages toward the RP router.

Beginning in privileged EXEC mode, follow these steps to modify the host-query interval. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Specify the interface to be configured, and enter interface configuration mode.
Step 3	<b>no shutdown</b>	Enable the port, if necessary. By default, UNIs are disabled, and NNIs are enabled.
Step 4	<b>ip igmp query-interval</b> <i>seconds</i>	Configure the frequency at which the designated router sends IGMP host-query messages.  By default, the designated router sends IGMP host-query messages every 60 seconds to keep the IGMP overhead very low on hosts and networks. The range is 1 to 65535.
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show ip igmp interface</b> [ <i>interface-id</i> ]	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no ip igmp query-interval** interface configuration command.

## Changing the IGMP Query Timeout for IGMPv2

If you are using IGMPv2, you can specify the period of time before the switch takes over as the querier for the interface. By default, the switch waits twice the query interval controlled by the **ip igmp query-interval** interface configuration command. After that time, if the switch has received no queries, it becomes the querier.

You can configure the query interval by entering the **show ip igmp interface *interface-id*** privileged EXEC command.

Beginning in privileged EXEC mode, follow these steps to change the IGMP query timeout. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface <i>interface-id</i></b>	Specify the interface to be configured, and enter interface configuration mode.
Step 3	<b>no shutdown</b>	Enable the port, if necessary. By default, UNIs are disabled, and NNIs are enabled.
Step 4	<b>ip igmp querier-timeout <i>seconds</i></b>	Specify the IGMP query timeout. The default is 60 seconds (twice the query interval). The range is 60 to 300.
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show ip igmp interface [<i>interface-id</i>]</b>	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no ip igmp querier-timeout** interface configuration command.

## Changing the Maximum Query Response Time for IGMPv2

If you are using IGMPv2, you can change the maximum query response time advertised in IGMP queries. The maximum query response time enables the switch to quickly detect that there are no more directly connected group members on a LAN. Decreasing the value enables the switch to prune groups faster.

Beginning in privileged EXEC mode, follow these steps to change the maximum query response time. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface <i>interface-id</i></b>	Specify the interface to be configured, and enter interface configuration mode.
Step 3	<b>no shutdown</b>	Enable the port, if necessary. By default, UNIs are disabled, and NNIs are enabled.
Step 4	<b>ip igmp query-max-response-time <i>seconds</i></b>	Change the maximum query response time advertised in IGMP queries. The default is 10 seconds. The range is 1 to 25.

	Command	Purpose
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show ip igmp interface</b> [ <i>interface-id</i> ]	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no ip igmp query-max-response-time** interface configuration command.

## Configuring the Switch as a Statically Connected Member

Sometimes there is either no group member on a network segment or a host cannot report its group membership by using IGMP. However, you might want multicast traffic to go to that network segment. These are ways to pull multicast traffic down to a network segment:

- Use the **ip igmp join-group** interface configuration command. With this method, the switch accepts the multicast packets in addition to forwarding them. Accepting the multicast packets prevents the switch from fast switching.
- Use the **ip igmp static-group** interface configuration command. With this method, the switch does not accept the packets itself, but only forwards them. This method enables fast switching. The outgoing interface appears in the IGMP cache, but the switch itself is not a member, as evidenced by lack of an *L* (local) flag in the multicast route entry.

Beginning in privileged EXEC mode, follow these steps to configure the switch itself to be a statically connected member of a group (and enable fast switching). This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Specify the interface to be configured, and enter interface configuration mode.
Step 3	<b>no shutdown</b>	Enable the port, if necessary. By default, UNIs are disabled, and NNIs are enabled.
Step 4	<b>ip igmp static-group</b> <i>group-address</i>	Configure the switch as a statically connected member of a group. By default, this feature is disabled.
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show ip igmp interface</b> [ <i>interface-id</i> ]	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To remove the switch as a member of the group, use the **no ip igmp static-group** *group-address* interface configuration command.

# Configuring Optional Multicast Routing Features

These sections describe how to configure optional multicast routing features:

- [Configuring sdr Listener Support, page 34-31](#) (optional)—for MBONE multimedia conference session and set up
- [Configuring an IP Multicast Boundary, page 34-32](#) (optional)—to control bandwidth utilization.

## Configuring sdr Listener Support

The MBONE is the small subset of Internet routers and hosts that are interconnected and capable of forwarding IP multicast traffic. Other multimedia content is often broadcast over the MBONE. Before you can join a multimedia session, you need to know what multicast group address and port are being used for the session, when the session is going to be active, and what sort of applications (audio, video, and so forth) are required on your workstation. The MBONE Session Directory Version 2 (sdr) tool provides this information. This freeware application can be downloaded from several sites on the World Wide Web, one of which is <http://www.video.ja.net/mice/index.html>.

SDR is a multicast application that listens to a well-known multicast group address and port for Session Announcement Protocol (SAP) multicast packets from SAP clients, which announce their conference sessions. These SAP packets contain a session description, the time the session is active, its IP multicast group addresses, media format, contact person, and other information about the advertised multimedia session. The information in the SAP packet is displayed in the SDR Session Announcement window.

## Enabling sdr Listener Support

By default, the switch does not listen to session directory advertisements.

Beginning in privileged EXEC mode, follow these steps to enable the switch to join the default session directory group (224.2.127.254) on the interface and listen to session directory advertisements. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface <i>interface-id</i></b>	Specify the interface to be enabled for sdr, and enter interface configuration mode.
Step 3	<b>no shutdown</b>	Enable the port, if necessary. By default, UNIs are disabled, and NNIs are enabled.
Step 4	<b>ip sdr listen</b>	Enable sdr listener support.
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show running-config</b>	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To disable sdr support, use the **no ip sdr listen** interface configuration command.

## Limiting How Long an sdr Cache Entry Exists

By default, entries are never deleted from the sdr cache. You can limit how long the entry remains active so that if a source stops advertising SAP information, old advertisements are not needlessly kept.

Beginning in privileged EXEC mode, follow these steps to limit how long an sdr cache entry stays active in the cache. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ip sdr cache-timeout</b> <i>minutes</i>	Limit how long an sdr cache entry stays active in the cache. By default, entries are never deleted from the cache. For <i>minutes</i> , the range is 1 to 4294967295.
Step 3	<b>end</b>	Return to privileged EXEC mode.
Step 4	<b>show running-config</b>	Verify your entries.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no ip sdr cache-timeout** global configuration command. To delete the entire cache, use the **clear ip sdr** privileged EXEC command.

To display the session directory cache, use the **show ip sdr** privileged EXEC command.

## Configuring an IP Multicast Boundary

Administratively-scoped boundaries can be used to limit the forwarding of multicast traffic outside of a domain or subdomain. This approach uses a special range of multicast addresses, called *administratively-scoped addresses*, as the boundary mechanism. If you configure an administratively-scoped boundary on a routed interface, multicast traffic whose multicast group addresses fall in this range can not enter or exit this interface, thereby providing a firewall for multicast traffic in this address range.



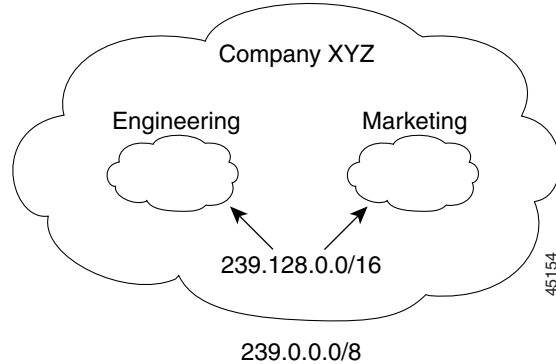
### Note

Multicast boundaries and TTL thresholds control the scoping of multicast domains; however, TTL thresholds are not supported by the switch. You should use multicast boundaries instead of TTL thresholds to limit the forwarding of multicast traffic outside of a domain or a subdomain.

Figure 34-4 shows that Company XYZ has an administratively-scoped boundary set for the multicast address range 239.0.0.0/8 on all routed interfaces at the perimeter of its network. This boundary prevents any multicast traffic in the range 239.0.0.0 through 239.255.255.255 from entering or leaving the network. Similarly, the engineering and marketing departments have an administratively-scoped boundary of 239.128.0.0/16 around the perimeter of their networks. This boundary prevents multicast traffic in the range of 239.128.0.0 through 239.128.255.255 from entering or leaving their respective networks.



Figure 34-4 Administratively-Scoped Boundaries



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

The IANA has designated the multicast address range 239.0.0.0 to 239.255.255.255 as the administratively-scoped addresses. This range of addresses can then be reused in domains administered by different organizations. The addresses would be considered local, not globally unique.

Beginning in privileged EXEC mode, follow these steps to set up an administratively-scoped boundary. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>access-list</b> <i>access-list-number</i> { <b>deny</b>   <b>permit</b> } <i>source</i> [ <i>source-wildcard</i> ]	Create a standard access list, repeating the command as many times as necessary. <ul style="list-style-type: none"> <li>For <i>access-list-number</i>, the range is 1 to 99.</li> <li>The <b>deny</b> keyword denies access if the conditions are matched. The <b>permit</b> keyword permits access if the conditions are matched.</li> <li>For <i>source</i>, enter the number of the network or host from which the packet is being sent.</li> <li>(Optional) For <i>source-wildcard</i>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</li> </ul> Recall that the access list is always terminated by an implicit deny statement for everything.
Step 3	<b>interface</b> <i>interface-id</i>	Specify the interface to be configured, and enter interface configuration mode.
Step 4	<b>no shutdown</b>	Enable the port, if necessary. By default, UNIs are disabled, and NNIs are enabled.
Step 5	<b>ip multicast boundary</b> <i>access-list-number</i>	Configure the boundary, specifying the access list you created in Step 2.
Step 6	<b>end</b>	Return to privileged EXEC mode.

	Command	Purpose
Step 7	<code>show running-config</code>	Verify your entries.
Step 8	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

To remove the boundary, use the **no ip multicast boundary** interface configuration command.

This example shows how to set up a boundary for all administratively-scoped addresses:

```
Switch(config)# access-list 1 deny 239.0.0.0 0.255.255.255
Switch(config)# access-list 1 permit 224.0.0.0 15.255.255.255
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip multicast boundary 1
```

## Monitoring and Maintaining IP Multicast Routing

These sections describe how to monitor and maintain IP multicast routing:

- [Clearing Caches, Tables, and Databases, page 34-34](#)
- [Displaying System and Network Statistics, page 34-34](#)
- [Monitoring IP Multicast Routing, page 34-35](#)

### Clearing Caches, Tables, and Databases

You can remove all contents of a particular cache, table, or database. Clearing a cache, table, or database might be necessary when the contents of the particular structure are or suspected to be invalid.

You can use any of the privileged EXEC commands in [Table 34-4](#) to clear IP multicast caches, tables, and databases:

**Table 34-4** Commands for Clearing Caches, Tables, and Databases

Command	Purpose
<code>clear ip igmp group [group-name   group-address   interface]</code>	Delete entries from the IGMP cache.
<code>clear ip mroute [*   group [source]]</code>	Delete entries from the IP multicast routing table.
<code>clear ip pim auto-rp rp-address</code>	Clear the Auto-RP cache.
<code>clear ip sdr [group-address   "session-name"]</code>	Delete the Session Directory Protocol Version 2 cache or an sdr cache entry.

### Displaying System and Network Statistics

You can display specific statistics, such as the contents of IP routing tables, caches, and databases.



**Note**

This release does not support per-route statistics.

You can display information to learn resource utilization and solve network problems. You can also display information about node reachability and discover the routing path your device's packets are taking through the network.

You can use any of the privileged EXEC commands in [Table 34-5](#) to display various routing statistics:

**Table 34-5** *Commands for Displaying System and Network Statistics*

Command	Purpose
<b>ping</b> [ <i>group-name</i>   <i>group-address</i> ]	Send an ICMP Echo Request to a multicast group address.
<b>show ip igmp groups</b> [ <i>group-name</i>   <i>group-address</i>   <i>type number</i> ]	Display the multicast groups that are directly connected to the switch and that were learned through IGMP.
<b>show ip igmp interface</b> [ <i>type number</i> ]	Display multicast-related information about an interface.
<b>show ip mcache</b> [ <i>group</i> [ <i>source</i> ]]	Display the contents of the IP fast-switching cache.
<b>show ip mpacket</b> [ <i>source-address</i>   <i>name</i> ] [ <i>group-address</i>   <i>name</i> ] [ <b>detail</b> ]	Display the contents of the circular cache-header buffer.
<b>show ip mroute</b> [ <i>group-name</i>   <i>group-address</i> ] [ <i>source</i> ] [ <b>summary</b> ] [ <b>count</b> ] [ <b>active kbps</b> ]	Display the contents of the IP multicast routing table.
<b>show ip pim interface</b> [ <i>type number</i> ] [ <b>count</b> ]	Display information about interfaces configured for PIM.
<b>show ip pim neighbor</b> [ <i>type number</i> ]	List the PIM neighbors discovered by the switch.
<b>show ip pim rp</b> [ <i>group-name</i>   <i>group-address</i> ]	Display the RP routers associated with a sparse-mode multicast group.
<b>show ip rpf</b> { <i>source-address</i>   <i>name</i> }	Display how the switch is doing Reverse-Path Forwarding (that is, from the unicast routing table or static mroutes).
<b>show ip sdr</b> [ <i>group</i>   " <i>session-name</i> "   <b>detail</b> ]	Display the Session Directory Protocol Version 2 cache.

## Monitoring IP Multicast Routing

You can use the privileged EXEC commands in [Table 34-6](#) to monitor IP multicast routers, packets, and paths:

**Table 34-6** *Commands for Monitoring IP Multicast Routing*

Command	Purpose
<b>mrinfo</b> [ <i>hostname</i>   <i>address</i> ] [ <i>source-address</i>   <i>interface</i> ]	Query a multicast router or multilayer switch about which neighboring multicast devices are peering with it.
<b>mstat</b> <i>source</i> [ <i>destination</i> ] [ <i>group</i> ]	Display IP multicast packet rate and loss information.
<b>mtrace</b> <i>source</i> [ <i>destination</i> ] [ <i>group</i> ]	Trace the path from a source to a destination branch for a multicast distribution tree for a given group.

