# Configuring IP Multicast Routing


- Finding Feature Information, page 1
- Prerequisites for IP Multicast Routing, page 1
- Restrictions for IP Multicast Routing, page 2
- Information About IP Multicast Routing, page 2
- How to Configure Basic IP Multicast Routing, page 4
- Monitoring IP Multicast Routing, page 10
- Configuration Examples for IP Multicast Routing, page 11
- Where to Go Next, page 11
- Additional References, page 12
- Feature History and Information for IP Multicast Routing, page 13


## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

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

## Prerequisites for IP Multicast Routing

You must enable basic 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.

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.

**Note** If you enable PIM on multiple interfaces, when most of these interfaces are not on the outgoing interface list, and IGMP snooping is disabled, the outgoing interface might not be able to sustain line rate for multicast traffic because of the extra replication.

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.

# Restrictions for IP Multicast Routing

The following are the restrictions for IP multicast routing:

- The switch supports homogeneous stacking, but does not support mixed stacking.

# Information About IP Multicast Routing

IP multicasting is an 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.

## Multicast Boundaries

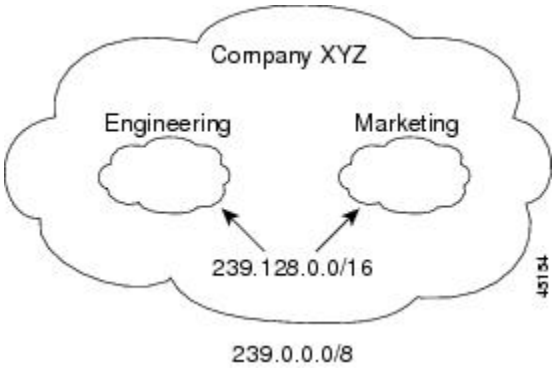
Administratively-scoped boundaries can be used to limit the forwarding of multicast traffic outside of a domain or subdomain. This approach uses a special range of multicast addresses, called administratively-scoped addresses, as the boundary mechanism. If you configure an administratively-scoped boundary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

The following figure 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 1: 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.

# Default IP Multicast Routing Configuration

This table displays the default IP multicast routing configuration.

***Table 1: Default IP 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. |

| Feature | Default Setting |
|---|---|
| Candidate RPs | Disabled. |
| Shortest-path tree threshold rate | 0 kb/s. |
| PIM router query message interval | 30 seconds. |

# How to Configure Basic IP Multicast Routing

## Configuring Basic IP Multicast Routing

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

This procedure is required.

### SUMMARY STEPS

1. **configure terminal**
2. **ip multicast-routing distributed**
3. **interface** *interface-id*
4. **ip pim version** [**1** | **2**]
5. **ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**}
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br><br>`Switch# configure terminal` | Enters the global configuration mode. |
| **Step 2** | **ip multicast-routing distributed**<br><br>**Example:**<br><br>`Switch(config)# ip multicast-routing distributed` | Enables IP multicast distributed switching<br><br>**Note** To disable multicasting, use the **no ip multicast-routing distributed** global configuration command. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **interface** *interface-id*<br><br>**Example:**<br><br>`Switch(config)# interface gigabitethernet 1/0/1` | Specifies the Layer 3 interface on which you want to enable multicast 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.<br><br>• An SVI—A VLAN interface created by using the **interface vlan** *vlan-id* global configuration command.<br><br>These interfaces must have IP addresses assigned to them. |
| **Step 4** | **ip pim version** [**1** \| **2**]<br><br>**Example:**<br><br>`Switch(config-if)# ip pim version 2` | Configures the PIM version on the interface.<br><br>By default, Version 2 is enabled and is the recommended setting.<br><br>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.<br><br>**Note** To return to the default PIM version, use the **no ip pim version** interface configuration command. |
| **Step 5** | **ip pim** {**dense-mode** \| **sparse-mode** \| **sparse-dense-mode**}<br><br>**Example:**<br><br>`Switch(config-if)# ip pim sparse-dense-mode` | Enables a PIM mode on the interface.<br><br>By default, no mode is configured.<br><br>The keywords have these meanings:<br><br>• **dense-mode—**Enables dense mode of operation.<br><br>• **sparse-mode—**Enables sparse mode of operation. If you configure sparse mode, you must also configure an RP.<br><br>• **sparse-dense-mode—**Causes the interface to be treated in the mode in which the group belongs. Sparse-dense mode is the recommended setting.<br><br>**Note** To disable PIM on an interface, use the **no ip pim** interface configuration command. |
| **Step 6** | **end**<br><br>**Example:**<br><br>`Switch(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 7** | **show running-config**<br><br>**Example:**<br><br>`Switch# show running-config` | Verifies your entries. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | **copy running-config startup-config**<br><br>**Example:**<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuring an IP Multicast Boundary

This procedure is optional.

## SUMMARY STEPS

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

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters the global configuration mode. |
| **Step 2** | **access-list** {*access-list-number* \| **deny** \| **permit** *source* [*source-wildcard*] }<br><br>**Example:**<br>`Switch(config)# access-list 99 permit any` | 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. 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. |

| | Command or Action | Purpose |
|---|---|---|
| | | • (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 3** | **interface** *interface-id*<br><br>**Example:**<br><br>`Switch(config)# interface gigabitEthernet1/0/1` | Specifies the interface to be configured, and enters interface configuration mode. |
| **Step 4** | **ip multicast boundary** *access-list-number*<br><br>**Example:**<br><br>`Switch(config-if)# ip multicast boundary 99` | 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 5** | **end**<br><br>**Example:**<br><br>`Switch(config-if)# 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**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

### Related Topics

Example: Configuring an IP Multicast Boundary, on page 11

# 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.

This procedure is optional.

### SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **ip sap listen**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br><br>`Switch# configure terminal` | Enters the global configuration mode. |
| **Step 2** | **interface** *interface-id*<br><br>**Example:**<br><br>`Switch(config)# interface` | Specifies the interface to be enabled for sdr, and enters interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **gigabitethernet 1/0/1** | |
| **Step 3** | **ip sap listen**<br><br>**Example:**<br><br>`Switch(config-if)# ip sap listen` | Enables the switch software to listen to session directory announcements.<br><br>**Note** To disable sdr support, use the **no ip sdr listen** interface configuration command. |
| **Step 4** | **end**<br><br>**Example:**<br><br>`Switch(config-if)# 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. |

## 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 unnecessarily kept.

This procedure is optional.

### SUMMARY STEPS

1. **configure terminal**
2. **ip sap cache-timeout** *minutes*
3. **end**
4. **show running-config**
5. **show ip sap**
6. **copy running-config startup-config**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters the global configuration mode. |
| **Step 2** | **ip sap cache-timeout** *minutes*<br><br>**Example:**<br>`Switch(config)# ip sap cache-timeout 30` | Limits how long a Session Announcement Protocol (SAP) cache entry stays active in the cache.<br>By default, entries are never deleted from the cache.<br>For *minutes*, the range is 1 to 1440 minutes (24 hours). |
| **Step 3** | **end**<br><br>**Example:**<br>`Switch(config)# end` | Returns to privileged EXEC mode. |
| **Step 4** | **show running-config**<br><br>**Example:**<br>`Switch# show running-config` | Verifies your entries. |
| **Step 5** | **show ip sap**<br><br>**Example:**<br>`Switch# show ip sap` | Displays the SAP cache. |
| **Step 6** | **copy running-config startup-config**<br><br>**Example:**<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file.<br>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.<br>To display the session directory cache, use the **show ip sdr** privileged EXEC command. |

# Monitoring IP Multicast Routing

You can use the privileged EXEC commands in the following table to monitor IP multicast routers, packets, and paths.

*Table 2: Commands for Monitoring IP Multicast Routing*

| Command | Purpose |
|---|---|
| **mrinfo** [*hostname* \| *address*] [*source-address* \| *interface*]<br>**mrinfo** { [*hostname* \| *address*] \| **vrf** } | Queries a multicast router or multilayer switch about which neighboring multicast devices are peering with it. |
| **mstat** *source* [*destination*] [*group*]<br>**mstat** { [*hostname* \| *address*] \| **vrf** } | Displays IP multicast packet rate and loss information. |
| **mtrace** *source* [*destination*] [*group*]<br>**mtrace** { [*hostname* \| *address*] \| **vrf** } | Traces the path from a source to a destination branch for a multicast distribution tree for a given group. |

# Configuration Examples for IP Multicast Routing

## Example: Configuring an IP Multicast Boundary

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 gigabitethernet1/0/1
Switch(config-if)# ip multicast boundary 1
```

### Related Topics

Configuring an IP Multicast Boundary, on page 6

# Where to Go Next

You can configure the following for your IP multicast configuration:

- IGMP feature support
- CGMP feature support
- PIM feature support
- SSM feature support

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| For complete syntax and usage information for the commands used in this book. | *Catalyst 2960-XR Switch IP Multicast Command Reference* |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| RFC 1112 | *Host Extensions for IP Multicasting* |
| RFC 2236 | *Internet Group Management Protocol, Version 2* |
| RFC 4601 | *Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification* |

### 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 |

# Feature History and Information for IP Multicast Routing

| Release | Modification |
|---|---|
| Cisco IOS 15.0(2)EX1 | This feature was introduced. |