



# Configuring Basic IP Multicast Routing

- [Prerequisites for Basic IP Multicast Routing, on page 1](#)
- [Restrictions for Basic IP Multicast Routing, on page 1](#)
- [Information About Basic IP Multicast Routing, on page 2](#)
- [How to Configure Basic IP Multicast Routing, on page 3](#)
- [Monitoring and Maintaining Basic IP Multicast Routing, on page 12](#)
- [Additional References for IP Multicast, on page 16](#)
- [Feature History and Information for IP Multicast, on page 17](#)

## Prerequisites for Basic IP Multicast Routing

The following are the prerequisites for configuring basic IP multicast routing:

- To use this feature, the device must be running the IP services feature set. The IP Services image contains complete multicast routing.
- You must configure the PIM version and the PIM mode in order to perform IP multicast routing. The switch populates its multicast routing table and forwards multicast packets it receives from its directly connected LANs according to the mode setting. You can configure an interface to be in the PIM dense mode, sparse mode, or sparse-dense mode.
- Enabling PIM on an interface also enables IGMP operation on that interface. (To participate in IP multicasting, the multicast hosts, routers, and multilayer device must have IGMP operating. )

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.

## Restrictions for Basic IP Multicast Routing

The following are the restrictions for IP multicast routing:

- IP multicast routing is not supported on switches running the LAN base feature set.
- High-availability support for Layer 3 multicast routing is not supported.
- You cannot have a device stack containing a mix of Catalyst 3850 and Catalyst 3650 devices.

## Information About Basic 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 devices 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.



### Note

For complete syntax and usage information for the commands used in this chapter, see the *IP Multicast Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*. For information on configuring the Multicast Source Discovery Protocol (MSDP), see the *Catalyst 3850 Routing Configuration Guide*.

## Multicast Forwarding Information Base Overview

The device uses the Multicast Forwarding Information Base (MFIB) architecture and the Multicast Routing Information Base (MRIB) for IP multicast.

The MFIB architecture provides both modularity and separation between the multicast control plane (Protocol Independent Multicast [PIM] and Internet Group Management Protocol [IGMP]) and the multicast forwarding plane (MFIB). This architecture is used in Cisco IOS IPv6 multicast implementations.

MFIB itself is a multicast routing protocol independent forwarding engine; that is, it does not depend on PIM or any other multicast routing protocol. It is responsible for:

- Forwarding multicast packets
- Registering with the MRIB to learn the entry and interface flags set by the control plane
- Handling data-driven events that must be sent to the control plane
- Maintaining counts, rates, and bytes of received, dropped, and forwarded multicast packets

The MRIB is the communication channel between MRIB clients. Examples of MRIB clients are PIM, IGMP, the multicast routing (mroute) table, and the MFIB.

## 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.                  |

| Feature                           | Default Setting     |
|-----------------------------------|---------------------|
| PIM mode                          | No mode is defined. |
| PIM stub routing                  | None configured.    |
| PIM RP address                    | None configured.    |
| PIM domain border                 | Disabled.           |
| PIM multicast boundary            | None.               |
| Candidate BSRs                    | Disabled.           |
| Candidate RPs                     | Disabled.           |
| Shortest-path tree threshold rate | 0 kb/s.             |
| PIM router query message interval | 30 seconds.         |

# How to Configure 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.

### Before you begin

You must configure the PIM version and the PIM mode. The switch populates its multicast routing table and forwards multicast packets it receives from its directly connected LANs according to the mode setting.

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.

### Procedure

|               | Command or Action   | Purpose  |
|---------------|---|--|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br>Device> <b>enable</b> | Enables privileged EXEC mode.<br>Enter your password, if prompted. |

|               | Command or Action   | Purpose  |
|---------------|---|--|
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>Device# configure terminal</pre>   | Enters global configuration mode.  |
| <b>Step 3</b> | <b>ip multicast-routing</b><br><b>Example:</b><br><pre>Device(config)# ip multicast-routing</pre>   | <p>Enables IP multicast routing.</p> <p>IP multicast routing is supported with Multicast Forwarding Information Base (MFIB) and Multicast Routing Information Base (MRIB).</p>   |
| <b>Step 4</b> | <b>interface <i>interface-id</i></b><br><b>Example:</b><br><pre>Device(config)# interface gigabitethernet 1/0/1</pre>                     | <p>Specifies the Layer 3 interface on which you want to enable multicast routing, and enters interface configuration mode.</p> <p>The specified interface must be one of the following:</p> <ul style="list-style-type: none"> <li>• A routed port—A physical port that has been configured as a Layer 3 port by entering the <b>no switchport</b> interface configuration command. You will also need to enable IP PIM sparse-dense-mode on the interface, and join the interface as a statically connected member to an IGMP static group.</li> <li>• An SVI—A VLAN interface created by using the <b>interface vlan <i>vlan-id</i></b> global configuration command. You will also need to enable IP PIM sparse-dense-mode on the VLAN, join the VLAN as a statically connected member to an IGMP static group, and then enable IGMP snooping on the VLAN, the IGMP static group, and physical interface.</li> </ul> <p>These interfaces must have IP addresses assigned to them.</p> |
| <b>Step 5</b> | <b>ip pim {dense-mode   sparse-mode   sparse-dense-mode}</b><br><b>Example:</b><br><pre>Device(config-if)# ip pim sparse-dense-mode</pre> | <p>Enables 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.</li> </ul>   |

|               | Command or Action   | Purpose  |
|---------------|---|--|
|               |   | <ul style="list-style-type: none"> <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> To disable PIM on an interface, use the <b>no ip pim</b> interface configuration command.</p> |
| <b>Step 6</b> | <b>end</b><br><b>Example:</b><br><pre>Device(config-if)# end</pre>  | Returns to privileged EXEC mode.   |
| <b>Step 7</b> | <b>show running-config</b><br><b>Example:</b><br><pre>Device# show running-config</pre>                               | Verifies your entries.   |
| <b>Step 8</b> | <b>copy running-config startup-config</b><br><b>Example:</b><br><pre>Device# copy running-config startup-config</pre> | (Optional) Saves your entries in the configuration file.   |

## Configuring IP Multicast Forwarding

You can use the following procedure to configure IPv4 Multicast Forwarding Information Base (MFIB) interrupt-level IP multicast forwarding of incoming packets or outgoing packets on the device.



**Note** After you have enabled IP multicast routing by using the **ip multicast-routing** command, IPv4 multicast forwarding is enabled. Because IPv4 multicast forwarding is enabled by default, you can use the **no** form of the **ip mfib** command to disable IPv4 multicast forwarding.

### Procedure

|               | Command or Action  | Purpose  |
|---------------|--|--|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br><pre>Device&gt; enable</pre> | Enables privileged EXEC mode.<br>Enter your password, if prompted. |

|               | Command or Action   | Purpose  |
|---------------|---|--|
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br><br>Device# <code>configure terminal</code>                                 | Enters global configuration mode.                        |
| <b>Step 3</b> | <b>ip mfib</b><br><b>Example:</b><br><br>Device(config)# <code>ip mfib</code>   | Enables IP multicast forwarding.                         |
| <b>Step 4</b> | <b>exit</b><br><b>Example:</b><br><br>Device(config)# <code>exit</code>   | Returns to privileged EXEC mode.                         |
| <b>Step 5</b> | <b>show running-config</b><br><b>Example:</b><br><br>Device# <code>show running-config</code>                               | Verifies your entries.                                   |
| <b>Step 6</b> | <b>copy running-config startup-config</b><br><b>Example:</b><br><br>Device# <code>copy running-config startup-config</code> | (Optional) Saves your entries in the configuration file. |

## Configuring a Static Multicast Route (mroute)

You can use the following procedure to configure static mroutes. Static mroutes are similar to unicast static routes but differ in the following ways:

- Static mroutes are used to calculate RPF information, not to forward traffic.
- Static mroutes cannot be redistributed.

Static mroutes are strictly local to the device on which they are defined. Because Protocol Independent Multicast (PIM) does not have its own routing protocol, there is no mechanism to distribute static mroutes throughout the network. Consequently, the administration of static mroutes tends to be more complicated than the administration of unicast static routes.

When static mroutes are configured, they are stored on the device in a separate table referred to as the static mroute table. When configured, the **ip mroute** command enters a static mroute into the static mroute table for the source address or source address range specified for the source-address and mask arguments. Sources that match the source address or that fall in the source address range specified for the source-address argument will RPF to either the interface associated with the IP address specified for the *rpf-address* argument or the

local interface on the device specified for the *interface-type* and *interface-number* arguments. If an IP address is specified for the *rpf-address* argument, a recursive lookup is done from the unicast routing table on this address to find the directly connected neighbor.

If there are multiple static mroutes configured, the device performs a longest-match lookup of the mroute table. When the mroute with the longest match (of the source-address) is found, the search terminates and the information in the matching static mroute is used. The order in which the static mroutes are configured is not important.

The administrative distance of an mroute may be specified for the optional distance argument. If a value is not specified for the distance argument, the distance of the mroute defaults to zero. If the static mroute has the same distance as another RPF source, the static mroute will take precedence. There are only two exceptions to this rule: directly connected routes and the default unicast route.

### Procedure

|               | Command or Action   | Purpose   |
|---------------|---|---|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br>Device> <b>enable</b>   | Enables privileged EXEC mode.<br>Enter your password, if prompted.  |
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br>Device# <b>configure terminal</b>   | Enters global configuration mode.   |
| <b>Step 3</b> | <b>ip mroute</b> [ <i>vrf vrf-name</i> ] <i>source-address mask</i> { <i>fallback-lookup</i> { <b>global</b>   <b>vrf vrf-name</b> } [ <i>protocol</i> ] { <i>rpf-address</i>   <i>interface-type interface-number</i> }} [ <i>distance</i> ]<br><b>Example:</b><br>Device(configure)# <b>ip mroute 10.1.1.1 255.255.255.255 10.2.2.2</b> | The source IP address 10.1.1.1 is configured to be reachable through the interface associated with IP address 10.2.2.2. |
| <b>Step 4</b> | <b>exit</b><br><b>Example:</b><br>Device(config)# <b>exit</b>   | Returns to privileged EXEC mode.  |
| <b>Step 5</b> | <b>show running-config</b><br><b>Example:</b><br>Device# <b>show running-config</b>   | (Optional) Verifies your entries.   |

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

## Configuring Optional IP Multicast Routing Features

### Defining the IP Multicast Boundary

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

This procedure is optional.

#### Procedure

|               | Command or Action  | Purpose   |
|---------------|--|---|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br><pre>Device&gt; enable</pre>   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>  |
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>Device# configure terminal</pre>  | Enters global configuration mode.   |
| <b>Step 3</b> | <b>access-list access-list-number deny source</b><br><b>[source-wildcard]</b><br><b>Example:</b><br><pre>Device(config)# access-list 12 deny 224.0.1.39 access-list 12 deny 224.0.1.40</pre> | Creates a standard access list, repeating the command as many times as necessary. <ul style="list-style-type: none"> <li>• For <i>access-list-number</i>, the range is 1 to 99.</li> <li>• The <b>deny</b> keyword denies access if the conditions are matched.</li> <li>• For <i>source</i>, enter multicast addresses 224.0.1.39 and 224.0.1.40, which carry Auto-RP information.</li> <li>• (Optional) For <i>source-wildcard</i>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.</li> </ul> |



|               | Command or Action   | Purpose   |
|---------------|---|---|
|               |   | The access list is always terminated by an implicit deny statement for everything.  |
| <b>Step 4</b> | <b>interface</b> <i>interface-id</i><br><b>Example:</b><br><pre>Device(config)# interface gigabitethernet 1/0/1</pre>               | <p>Specifies the interface to be configured, and enters interface configuration mode.</p> <p>The specified interface must be one of the following:</p> <ul style="list-style-type: none"> <li>• A routed port—A physical port that has been configured as a Layer 3 port by entering the <b>no switchport</b> interface configuration command.</li> <li>• An SVI—A VLAN interface created by using the <b>interface vlan</b> <i>vlan-id</i> global configuration command.</li> </ul> <p>These interfaces must have IP addresses assigned to them.</p> |
| <b>Step 5</b> | <b>ip multicast boundary</b> <i>access-list-number</i><br><b>Example:</b><br><pre>Device(config-if)# ip multicast boundary 12</pre> | Configures the boundary, specifying the access list you created in Step 2.  |
| <b>Step 6</b> | <b>end</b><br><b>Example:</b><br><pre>Device(config)# end</pre>   | Returns to privileged EXEC mode.  |
| <b>Step 7</b> | <b>show running-config</b><br><b>Example:</b><br><pre>Device# show running-config</pre>   | Verifies your entries.  |
| <b>Step 8</b> | <b>copy running-config startup-config</b><br><b>Example:</b><br><pre>Device# copy running-config startup-config</pre>               | (Optional) Saves your entries in the configuration file.  |

## Configuring sdr Listener Support

### Enabling sdr Listener Support

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

This procedure is optional.

#### Procedure

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

|               | Command or Action   | Purpose   |
|---------------|---|---|
|               |   | These interfaces must have IP addresses assigned to them.                 |
| <b>Step 4</b> | <b>ip sap listen</b><br><b>Example:</b><br><br>Device(config-if)# <b>ip sap listen</b>                                | Enables the device software to listen to session directory announcements. |
| <b>Step 5</b> | <b>end</b><br><b>Example:</b><br><br>Device(config-if)# <b>end</b>  | Returns to privileged EXEC mode.  |
| <b>Step 6</b> | <b>show running-config</b><br><b>Example:</b><br><br>Device# <b>show running-config</b>                               | Verifies your entries.  |
| <b>Step 7</b> | <b>copy running-config startup-config</b><br><b>Example:</b><br><br>Device# <b>copy running-config startup-config</b> | (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.

#### Procedure

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

|               | Command or Action   | Purpose  |
|---------------|---|--|
| <b>Step 3</b> | <b>ip sap cache-timeout</b> <i>minutes</i><br><b>Example:</b><br>Device(config)# <b>ip sap cache-timeout 30</b>   | 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 <i>minutes</i> , the range is 1 to 1440 minutes (24 hours). |
| <b>Step 4</b> | <b>end</b><br><b>Example:</b><br>Device(config)# <b>end</b>   | Returns to privileged EXEC mode.   |
| <b>Step 5</b> | <b>show running-config</b><br><b>Example:</b><br>Device# <b>show running-config</b>                               | Verifies your entries.   |
| <b>Step 6</b> | <b>show ip sap</b><br><b>Example:</b><br>Device# <b>show ip sap</b>   | Displays the SAP cache.  |
| <b>Step 7</b> | <b>copy running-config startup-config</b><br><b>Example:</b><br>Device# <b>copy running-config startup-config</b> | (Optional) Saves your entries in the configuration file.   |

## Monitoring and Maintaining Basic IP Multicast Routing

### 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 the following table to clear IP multicast caches, tables, and databases.

**Table 2: Commands for Clearing Caches, Tables, and Databases**

| Command  | Purpose   |
|--|---|
| <b>clear ip igmp group</b> { <b>group</b> [ <i>hostname</i>   <i>IP address</i> ]   <b>vrf name group</b> [ <i>hostname</i>   <i>IP address</i> ] }  | Deletes entries from the IGMP cache.  |
| <b>clear ip mfib</b> { <b>counters</b> [ <i>group</i>   <i>source</i> ]   <b>global counters</b> [ <i>group</i>   <i>source</i> ]   <b>vrf *</b> }   | Clears all active IPv4 Multicast Forwarding Information Base (MFIB) traffic counters. |
| <b>clear ip mrm</b> { <b>status-report</b> [ <i>source</i> ] }   | IP multicast routing clear commands.  |
| <b>clear ip mroute</b> { * [ <i>hostname</i>   <i>IP address</i> ]   <b>vrf name group</b> [ <i>hostname</i>   <i>IP address</i> ] }   | Deletes entries from the IP multicast routing table.                                  |
| <b>clear ip msdp</b> { <b>peer</b>   <b>sa-cache</b>   <b>statistics</b>   <b>vrf</b> }  | Clears the Multicast Source Discovery Protocol (MSDP) cache.                          |
| <b>clear ip multicast</b> { <b>limit</b>   <b>redundancy statistics</b> }  | Clears the IP multicast information.  |
| <b>clear ip pim</b> { <b>df</b> [ <i>int</i>   <b>rp</b> <i>rp address</i> ]   <b>interface</b>   <b>rp-mapping</b> [ <i>rp address</i> ]   <b>vrf vpn name</b> { <b>df</b>   <b>interface</b>   <b>rp-mapping</b> } | Clears the PIM cache.   |
| <b>clear ip sap</b> [ <i>group-address</i>   “ <i>session-name</i> ” ]   | Deletes 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 usage and solve network problems. You can also display information about node reachability and discover the routing path that packets of your device are taking through the network.

You can use any of the privileged EXEC commands in the following table to display various routing statistics.

**Table 3: Commands for Displaying System and Network Statistics**

| Command  | Purpose  |
|--|--|
| <b>ping</b> [ <i>group-name</i>   <i>group-address</i> ] | Sends an ICMP Echo Request to a multicast group address. |
| <b>show ip igmp filter</b>                               | Displays IGMP filter information.                        |

| Command  | Purpose   |
|--|---|
| <b>show ip igmp groups</b><br>[ <i>group-name</i>   <i>group-address</i>   <i>type-number</i> ]  | Displays the multicast groups that are directly connected to the device and that were learned through IGMP. |
| <b>show ip igmp interface</b> [ <i>type number</i> ]   | Displays multicast-related information about an interface.  |
| <b>show ip igmp profile</b> [ <i>profile_number</i> ]  | Displays IGMP profile information.  |
| <b>show ip igmp ssm-mapping</b> [ <i>hostname/IP address</i> ]   | Displays IGMP SSM mapping information.  |
| <b>show ip igmp static-group</b> { <b>class-map</b> [ <b>interface</b> [ <i>type</i> ] ]   | Displays static group information.  |
| <b>show ip igmp membership</b> [ <i>name/group address</i>   <b>all</b>   <b>tracked</b> ]   | Displays IGMP membership information for forwarding.  |
| <b>show ip igmp vrf</b>  | Displays the selected VPN Routing/Forwarding instance by name.  |
| <b>show ip mfib</b> [ <i>type number</i> ]   | Displays the IP multicast forwarding information base.  |
| <b>show ip mrrib</b> { <b>client</b>   <b>route</b>   <b>vrf</b> }   | Displays the multicast routing information base.  |
| <b>show ip mrm</b> { <b>interface</b>   <b>manager</b>   <b>status-report</b> }  | Displays the IP multicast routing monitor information.  |
| <b>show ip mroute</b> [ <i>group-name</i>   <i>group-address</i> ]<br>[ <i>source</i> ] [ <b>count</b>   <b>interface</b>   <b>proxy</b>   <b>pruned</b>   <b>summary</b>   <b>verbose</b> ] | Displays the contents of the IP multicast routing table.  |
| <b>show ip msdp</b> { <b>count</b>   <b>peer</b>   <b>rpf-peer</b>   <b>sa-cache</b>   <b>summary</b>   <b>vrf</b> }   | Displays the Multicast Source Discovery Protocol (MSDP) information.  |
| <b>show ip multicast</b> [ <b>interface</b>   <b>limit</b>   <b>mpls</b>   <b>redundancy</b>   <b>vrf</b> ]  | Displays global multicast information.  |
| <b>show ip pim all-vrfs</b> { <b>tunnel</b> }  | Display all VRFs.   |
| <b>show ip pim autorp</b>  | Display global auto-RP information.   |
| <b>show ip pim boundary</b> [ <i>type number</i> ]   | Displays boundary information.  |
| <b>show ip pim bsr-router</b>  | Display bootstrap router information (version 2).   |
| <b>show ip pim interface</b> [ <i>type number</i> ] [ <b>count</b>   <b>detail</b>   <b>df</b>   <b>stats</b> ]  | Displays information about interfaces configured for PIM. This command is available in all software images. |
| <b>show ip pim neighbor</b> [ <i>type number</i> ]   | Lists the PIM neighbors discovered by the device. This command is available in all software images.         |

| Command   | Purpose   |
|---|---|
| <code>show ip pim mdt [ bgp ]</code>                          | Displays multicast tunnel information.  |
| <code>show ip pim rp [group-name   group-address]</code>      | Displays the RP routers associated with a sparse-mode multicast group. This command is available in all software images.  |
| <code>show ip pim rp-hash [group-name   group-address]</code> | Displays the RP to be chosen based upon the group selected.   |
| <code>show ip pim tunnel [ tunnel   verbose ]</code>          | Displays the registered tunnels.  |
| <code>show ip pim vrf name</code>                             | Displays VPN routing and forwarding instances.  |
| <code>show ip rpf {source-address   name}</code>              | Displays how the device is doing Reverse-Path Forwarding (that is, from the unicast routing table, DVMRP routing table, or static mroutes).<br><br>Command parameters include: <ul style="list-style-type: none"> <li>• <i>Host name or IP address</i>—IP name or group address.</li> <li>• <b>Select</b>—Group-based VRF select information.</li> <li>• <b>vrf</b>—Selects VPN Routing/Forwarding instance.</li> </ul> |
| <code>show ip sap [group   “session-name”   detail]</code>    | Displays the Session Announcement Protocol (SAP) Version 2 cache.<br><br>Command parameters include: <ul style="list-style-type: none"> <li>• <i>A.B.C.D</i>—IP group address.</li> <li>• <i>WORD</i>—Session name (in double quotes).</li> <li>• <b>detail</b>—Session details.</li> </ul>   |

## Displaying Multicast Peers, Packet Rates and Loss Information, and Path Tracing

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

**Table 4: Commands for Displaying Multicast Peers, Packet Rates and Loss Information, and Path Tracing**

| Command  | Purpose  |
|--|--|
| <code>mrinfo { [hostname   address]   vrf }</code> | Queries a multicast router or multilayer device about which neighboring multicast devices are peering with it. |
| <code>mstat { [hostname   address]   vrf }</code>  | Displays IP multicast packet rate and information loss.  |

## 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:

```
Device(config)# access-list 1 deny 239.0.0.0 0.255.255.255
Device(config)# access-list 1 permit 224.0.0.0 15.255.255.255
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip multicast boundary 1
```

### Example: Responding to mrimfo Requests

The software answers mrimfo requests sent by mroutered systems and Cisco routers and multilayer devices. The software returns information about neighbors through DVMRP tunnels and all the routed interfaces. This information includes the metric (always set to 1), the configured TTL threshold, the status of the interface, and various flags. You can also use the **mrimfo** privileged EXEC command to query the router or device itself, as in this example:

```
Device# mrimfo
171.69.214.27 (mm1-7kd.cisco.com) [version cisco 11.1] [flags: PMS]:
171.69.214.27 -> 171.69.214.26 (mm1-r7kb.cisco.com) [1/0/pim/querier]
171.69.214.27 -> 171.69.214.25 (mm1-45a.cisco.com) [1/0/pim/querier]
171.69.214.33 -> 171.69.214.34 (mm1-45c.cisco.com) [1/0/pim]
171.69.214.137 -> 0.0.0.0 [1/0/pim/querier/down/leaf]
171.69.214.203 -> 0.0.0.0 [1/0/pim/querier/down/leaf]
171.69.214.18 -> 171.69.214.20 (mm1-45e.cisco.com) [1/0/pim]
171.69.214.18 -> 171.69.214.19 (mm1-45c.cisco.com) [1/0/pim]
171.69.214.18 -> 171.69.214.17 (mm1-45a.cisco.com) [1/0/pim]
```

## Additional References for IP Multicast

### Related Documents

| Related Topic  | Document Title |
|--|----------------|
| For complete syntax and usage information for the commands used in this chapter. |                |

### Standards and RFCs

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



**MIBs**

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

**Technical Assistance**

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

## Feature History and Information for IP Multicast

| Release            | Modification                 |
|--------------------|------------------------------|
| Cisco IOS XE 3.2SE | This feature was introduced. |

