



Configuring Basic IP Multicast Routing

- [Finding Feature Information, page 1](#)
- [Prerequisites for Basic IP Multicast Routing, page 1](#)
- [Restrictions for Basic IP Multicast Routing, page 2](#)
- [Information About Basic IP Multicast Routing, page 2](#)
- [How to Configure Basic IP Multicast Routing, page 4](#)
- [Monitoring and Maintaining Basic IP Multicast Routing, page 13](#)
- [Additional References, page 16](#)
- [Feature History and Information for IP Multicast, page 17](#)

Finding Feature Information

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

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

Prerequisites for Basic IP Multicast Routing

The following are the prerequisites for configuring basic IP 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.

Related Topics

[Configuring Basic IP Multicast Routing](#), on page 4

[Information About Basic IP Multicast Routing](#), on page 2

[IP Multicast Routing Protocols](#)

Restrictions for Basic IP Multicast Routing

The following are the restrictions for IP multicast routing:

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.

Related Topics

[Configuring Basic IP Multicast Routing](#), on page 4

[Prerequisites for Basic IP Multicast Routing](#), on page 1

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.

Related Topics

[Configuring IP Multicast Forwarding \(CLI\)](#), on page 6

Multicast Routing and Device Stacks

For all multicast routing protocols, the entire stack appears as a single router to the network and operates as a single multicast router.

In a device stack, the active device performs these functions:

- It is responsible for completing the IP multicast routing functions of the stack. It fully initializes and runs the IP multicast routing protocols.
- It builds and maintains the multicast routing table for the entire stack.
- It is responsible for distributing the multicast routing table to all stack members.

The stack members perform these functions:

- They act as multicast routing standby devices and are ready to take over if there is a active device failure. If the active device fails, all stack members delete their multicast routing tables. The newly elected active device starts building the routing tables and distributes them to the stack members.
- They do not build multicast routing tables. Instead, they use the multicast routing table that is distributed by the active device.

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.

Feature	Default Setting
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
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters the global configuration mode.

	Command or Action	Purpose
Step 3	<p>interface <i>interface-id</i></p> <p>Example:</p> <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"> • A routed port—A physical port that has been configured as a Layer 3 port by entering the no switchport interface configuration command. You will also need to enable IP PIM sparse-dense-mode on the interface, and join the interface as a statically connected member to an IGMP static group. • An SVI—A VLAN interface created by using the interface vlan <i>vlan-id</i> global configuration command. You will also need to enable IP PIM sparse-dense-mode on the VLAN, join the VLAN as a statically connected member to an IGMP static group, and then enable IGMP snooping on the VLAN, the IGMP static group, and physical interface. <p>These interfaces must have IP addresses assigned to them.</p>
Step 4	<p>ip pim {dense-mode sparse-mode sparse-dense-mode}</p> <p>Example:</p> <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"> • dense-mode—Enables dense mode of operation. • sparse-mode—Enables sparse mode of operation. If you configure sparse mode, you must also configure an RP. • sparse-dense-mode—Causes the interface to be treated in the mode in which the group belongs. Sparse-dense mode is the recommended setting. <p>Note To disable PIM on an interface, use the no ip pim interface configuration command.</p>
Step 5	<p>end</p> <p>Example:</p> <pre>Device(config-if)# end</pre>	<p>Returns to privileged EXEC mode.</p>
Step 6	<p>show running-config</p> <p>Example:</p> <pre>Device# show running-config</pre>	<p>Verifies your entries.</p>

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

Related Topics

[Information About Basic IP Multicast Routing, on page 2](#)

[IP Multicast Routing Protocols](#)

[Prerequisites for Basic IP Multicast Routing, on page 1](#)

Configuring IP Multicast Forwarding (CLI)

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
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters the global configuration mode.
Step 3	ip mfib Example: Device(config)# ip mfib	Enables IP multicast forwarding.

	Command or Action	Purpose
Step 4	exit Example: Device (config) # exit	Returns to privileged EXEC mode.
Step 5	show running-config Example: Device# show running-config	Verifies your entries.
Step 6	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Related Topics

[Multicast Forwarding Information Base Overview](#) , on page 2

Configuring a Static Multicast Route (mroute) (CLI)

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
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters the global configuration mode.
Step 3	ip mroute [vrf vrf-name] source-address mask { fallback-lookup {global vrf vrf-name } [protocol] {rpf-address interface-type interface-number} } [distance] Example: Device (configure)# ip mroute 10.1.1.1 255.255.255.255 10.2.2.2	The source IP address 10.1.1.1 is configured to be reachable through the interface associated with IP address 10.2.2.2.
Step 4	exit Example: Device (config)# exit	Returns to privileged EXEC mode.
Step 5	show running-config Example: Device# show running-config	(Optional) Verifies your entries.
Step 6	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring Optional IP Multicast Routing Features

Defining the IP Multicast Boundary (CLI)

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

This procedure is optional.

Procedure

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

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

Related Topics

[Multicast Boundaries](#)

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

[IP Multicast Boundary](#)

[Multicast Group Transmission Scheme](#)

[Example: Configuring an IP Multicast Boundary, on page 15](#)

Configuring sdr Listener Support

Enabling sdr Listener Support (CLI)

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

This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters the global configuration mode.
Step 3	interface <i>interface-id</i> Example: Device(config)# interface gigabitethernet 1/0/1	Specifies the interface to be enabled for sdr, and enters interface configuration mode. The specified interface must be one of the following: <ul style="list-style-type: none"> • A routed port—A physical port that has been configured as a Layer 3 port by entering the no switchport interface configuration command. You will also need to enable IP PIM sparse-dense-mode on the interface, and join the interface as a statically connected member to an IGMP static group. For a configuration example, see Example: Interface Configuration as a Routed Port • An SVI—A VLAN interface created by using the interface vlan <i>vlan-id</i> global configuration command. You will also need to enable IP PIM sparse-dense-mode on the VLAN, join the VLAN as a statically connected member to an IGMP static group, and then enable IGMP snooping on the VLAN, the IGMP static group, and physical interface. For a configuration example, see Example: Interface Configuration as an SVI These interfaces must have IP addresses assigned to them.
Step 4	ip sap listen Example: Device(config-if)# ip sap	Enables the device software to listen to session directory announcements.

	Command or Action	Purpose
	<code>listen</code>	
Step 5	end Example: Device(config-if)# <code>end</code>	Returns to privileged EXEC mode.
Step 6	show running-config Example: Device# <code>show running-config</code>	Verifies your entries.
Step 7	copy running-config startup-config Example: Device# <code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

Limiting How Long an sdr Cache Entry Exists (CLI)

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
Step 1	enable Example: Device> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# <code>configure terminal</code>	Enters the global configuration mode.

	Command or Action	Purpose
Step 3	ip sap cache-timeout <i>minutes</i> Example: Device(config)# ip sap cache-timeout 30	Limits how long a Session Announcement Protocol (SAP) 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 1440 minutes (24 hours).
Step 4	end Example: Device(config)# end	Returns to privileged EXEC mode.
Step 5	show running-config Example: Device# show running-config	Verifies your entries.
Step 6	show ip sap Example: Device# show ip sap	Displays the SAP cache.
Step 7	copy running-config startup-config Example: Device# copy running-config startup-config	(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
clear ip igmp group { group [<i>hostname</i> <i>IP address</i>] vrf name group [<i>hostname</i> <i>IP address</i>] }	Deletes entries from the IGMP cache.
clear ip mroute { * [<i>hostname</i> <i>IP address</i>] vrf name group [<i>hostname</i> <i>IP address</i>] }	Deletes entries from the IP multicast routing table.
clear ip sap [<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
ping [<i>group-name</i> <i>group-address</i>]	Sends an ICMP Echo Request to a multicast group address.
show ip igmp groups [<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.
show ip igmp interface [<i>type number</i>]	Displays multicast-related information about an interface.
show ip mroute [<i>group-name</i> <i>group-address</i>] [<i>source</i>] [count interface proxy pruned summary verbose]	Displays the contents of the IP multicast routing table.
show ip pim interface [<i>type number</i>] [count detail df stats]	Displays information about interfaces configured for PIM. This command is available in all software images.
show ip pim neighbor [<i>type number</i>]	Lists the PIM neighbors discovered by the device. This command is available in all software images.
show ip pim rp [<i>group-name</i> <i>group-address</i>]	Displays the RP routers associated with a sparse-mode multicast group. This command is available in all software images.

Command	Purpose
show ip rpf { <i>source-address</i> <i>name</i> }	Displays how the device is doing Reverse-Path Forwarding (that is, from the unicast routing table, DVMRP routing table, or static mroutes). Command parameters include: <ul style="list-style-type: none"> • <i>Host name</i> or <i>IP address</i>—IP name or group address. • Select—Group-based VRF select information. • vrf—Selects VPN Routing/Forwarding instance.
show ip sap [<i>group</i> " <i>session-name</i> " detail]	Displays the Session Announcement Protocol (SAP) Version 2 cache. Command parameters include: <ul style="list-style-type: none"> • <i>A.B.C.D</i>—IP group address. • <i>WORD</i>—Session name (in double quotes). • detail—Session details.

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

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
```

Related Topics

[Defining the IP Multicast Boundary \(CLI\)](#)
[IP Multicast Boundary](#)
[Multicast Group Transmission Scheme](#)

Example: Responding to mriinfo Requests

The software answers mriinfo 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 **mriinfo** privileged EXEC command to query the router or device itself, as in this example:

```
Device# mriinfo
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

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	See the IP Multicast Routing Commands section of the <i>Command Reference, Cisco IOS XE Everest 16.5.1a (Catalyst 9500 Series Switches)</i>
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

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 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: http://www.cisco.com/go/mibs

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>	http://www.cisco.com/support

Feature History and Information for IP Multicast

Release	Modification
Cisco IOS XE Everest 16.5.1a	This feature was introduced.

