



Configuring Basic IP Multicast Routing

- [Information About Basic IP Multicast Routing, on page 1](#)
- [How to Configure Basic IP Multicast Routing, on page 2](#)
- [Monitoring and Maintaining Basic IP Multicast Routing, on page 12](#)
- [Configuration Examples for Basic IP Multicast Routing, on page 14](#)

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 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 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 (mroutd) 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.
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

This section provides information about configuring basic IP multicast routing.

Configuring Basic IP Multicast Routing

Before you begin



Note By default, multicast routing is disabled, and there is no default mode setting. To enable multicast routing, use the **ip multicast-routing** command.

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. The multicast source address

must be on the directly connected incoming interface (that is part of the same subnet) of the first-hop router for both PIM dense mode and PIM any-source multicast mode. 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: <pre>Device> enable</pre>	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	interface interface-id Example: <pre>Device(config)# interface gigabitethernet 1/1</pre>	Specifies the Layer 3 interface on which you want to enable multicast routing, and enters interface configuration mode. The specified interface must be one of the following: • 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 vlan-id global configuration command. You will also need to enable IP PIM sparse-dense-mode on the VLAN, join the VLAN as a statically connected member to an IGMP static group, and then enable IGMP snooping on the VLAN, the IGMP static group, and physical interface. These interfaces must have IP addresses assigned to them.
Step 4	ip pim {dense-mode sparse-mode sparse-dense-mode}	Enables a PIM mode on the interface. By default, no mode is configured.

	Command or Action	Purpose
	Example: Device(config-if) # ip pim sparse-mode	The keywords have these meanings: • 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. Note To disable PIM on an interface, use the no ip pim interface configuration command.
Step 5	end Example: Device(config-if) # end	Returns to privileged EXEC mode.
Step 6	show running-config Example: Device# show running-config	Verifies your entries.
Step 7	copy running-config startup-config Example: Device# copy running-config startup-config	(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.

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 global configuration mode.
Step 3	ip mfib Example: Device(config)# ip mfib	Enables IP multicast forwarding.
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.

Configuring a Static Multicast Route (mroute)

- 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. Enter your password, if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters 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(config)# 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 Multicast VRFs

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	ip routing Example: Switch(config)# ip routing	Enables IP routing.
Step 3	ip vrf vrf-name Example: Switch(config)# ip vrf vrf-name	Configures a VRF table and enters VRF configuration mode.
Step 4	ip multicast-routing vrf vrf-name Example: Switch(config-vrf)# ip multicast-routing vrf vrf-name	(Optional) Enables global multicast routing for VRF table.
Step 5	rd route-distinguisher Example: Switch (config-vrf)# rd route-distinguisher	Creates a VRF table by specifying a route distinguisher. Enter either an AS number and an arbitrary number (xxx:y) or an IP address and arbitrary number (A.B.C.D:y).
Step 6	route-target {export import both} route-target-ext-community Example: Switch(config-vrf)# route-target {export import both} route-target-ext-community	Creates a list of import, export, or import and export route target communities for the specified VRF. Enter either an AS system number and an arbitrary number (xxx:y) or an IP address and an arbitrary number (A.B.C.D:y). The route-target-ext-community value should be the same as the route-distinguisher value entered in Step 4.
Step 7	import map route-map Example: Switch(config-vrf)# import map route-map	(Optional) Associates a route map with the VRF.
Step 8	interface interface-id Example: Switch (config)# interface interface-id	Enters interface configuration mode and specifies the Layer 3 interface to be associated with the VRF. The interface can be a routed port or a SVI.

	Command or Action	Purpose
Step 9	vrf forwarding vrf-name Example: Switch (config-sg-tacacs+)# vrf forwarding vrf-name	Associates the VRF with the Layer 3 interface.
Step 10	ip address ip-address mask Example: Switch (config-if)# ip address ip-address mask	Configures IP address for the Layer 3 interface.
Step 11	ip pim sparse-mode Example: Switch(config-if)# ip pim sparse-mode	Enables PIM on the VRF-associated Layer 3 interface.
Step 12	end Example: Switch(config-if)# end	Returns to privileged EXEC mode.
Step 13	show ip vrf [brief detail interfaces] [vrf-name] Example: show ip vrf [brief detail interfaces] [vrf-name]	Verifies the configuration. Display information about the configured VRFs.
Step 14	copy running-config startup-config Example: Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Example

The following example shows how to configure multicast within a VRF table:

```
Switch(config)# ip routing
Switch(config)# ip vrf multiVrfA
Switch(config-vrf)# ip multicast-routing vrf multiVrfA
Switch(config-vrf)# interface GigabitEthernet3/1
Switch(config-if)# vrf forwarding multiVrfA
Switch(config-if)# ip address 172.21.200.203 255.255.255.0
Switch(config-if)# ip pim sparse-mode
```

Configuring Optional IP Multicast Routing Features

This section provides information about 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
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	access-list access-list-number deny source [source-wildcard] 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. • 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 interface-id Example: Device(config)# interface gigabitethernet 1/1	Specifies the interface to be configured, and enters interface configuration mode.
Step 5	ip multicast boundary access-list-number Example: Device(config-if)# ip multicast boundary 12	Configures the boundary, specifying the access list you created in Step 2.
Step 6	end Example:	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Device (config) # end	
Step 7	show running-config Example: Device# show running-config	Verifies your entries.
Step 8	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring sdr Listener Support

This section provides information about 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
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface interface-id Example: Device (config) # interface gigabitethernet 1/1	Specifies the interface to be enabled for sdr, and enters interface configuration mode.
Step 4	ip sap listen Example: Device (config-if) # ip sap listen	Enables the device software to listen to session directory announcements.
Step 5	end Example: Device (config-if) # end	Returns to privileged EXEC mode.
Step 6	show running-config Example:	Verifies your entries.

	Command or Action	Purpose
	Device# <code>show running-config</code>	
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

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. Enter your password, if prompted.
Step 2	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 3	ip sap cache-timeout <i>minutes</i> Example: Device(config)# <code>ip sap cache-timeout 30</code>	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)# <code>end</code>	Returns to privileged EXEC mode.
Step 5	show running-config Example: Device# <code>show running-config</code>	Verifies your entries.
Step 6	show ip sap Example: Device# <code>show ip sap</code>	Displays the SAP cache.

	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.

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 [hostname IP address] vrf name group [hostname IP address] }	Deletes entries from the IGMP cache.
clear ip mroute { * [hostname IP address] vrf name group [hostname IP address] }	Deletes entries from the IP multicast routing table.
clear ip sap [group-address “session-name”]	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 [group-name group-address]	Sends an ICMP Echo Request to a multicast group address.
show ip igmp filter	Displays IGMP filter information.
show ip igmp groups [group-name group-address type-number]	Displays the multicast groups that are directly connected to the device and that were learned through IGMP.
show ip igmp interface [type number]	Displays multicast-related information about an interface.
show ip igmp profile [profile_number]	Displays IGMP profile information.
show ip igmp ssm-mapping [hostname/IP address]	Displays IGMP SSM mapping information.
show ip igmp static-group {class-map [interface [type]]}	Displays static group information.
show ip igmp membership [name/group address all tracked]	Displays IGMP membership information for forwarding.
show ip igmp vrf	Displays the selected VPN Routing/Forwarding instance by name.
show ip mfib [type number]	Displays the IP multicast forwarding information base.
show ip mrrib { client route vrf }	Displays the multicast routing information base.
show ip mrm { interface manager status-report }	Displays the IP multicast routing monitor information.
show ip mroute [group-name group-address] [source] [count interface proxy pruned summary verbose]	Displays the contents of the IP multicast routing table.
show ip msdp { count peer rpf-peer sa-cache summary vrf }	Displays the Multicast Source Discovery Protocol (MSDP) information.
show ip multicast [interface limit mpls redundancy vrf]	Displays global multicast information.
show ip pim all-vrfs { tunnel }	Display all VRFs.
show ip pim autorp	Display global auto-RP information.
show ip pim boundary [type number]	Displays boundary information.

Command	Purpose
show ip pim bsr-router	Display bootstrap router information (version 2).
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 mdt [bgp]	Displays multicast tunnel information.
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.
show ip pim rp-hash [<i>group-name</i> <i>group-address</i>]	Displays the RP to be chosen based upon the group selected.
show ip pim tunnel [<i>tunnel</i> <i>verbose</i>]	Displays the registered tunnels.
show ip pim vrf <i>name</i>	Displays VPN routing and forwarding instances.
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: • <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: • <i>A.B.C.D</i>—IP group address. • <i>WORD</i>—Session name (in double quotes). • detail—Session details.

Configuration Examples for Basic IP Multicast Routing

This section provides configuration examples for Basic IP Multicast Routing.

Example: Configuring an IP Multicast Boundary

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

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

Example: Responding to mrinfo Requests

The software answers mrinfo requests sent by mrouted systems and Cisco routers and multilayer switches. 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 **mrinfo** privileged EXEC command to query the router or switch itself, as in this example:

```
Switch# mrinfo
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]
```

 Example: Responding to minfo Requests