Configuring Basic IP Multicast Routing

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.

Restrictions for Basic IP Multicast Routing

The following are the restrictions for IP multicast routing:

- IP Multicast routing is supported only on Catalyst 3560-CX switches.

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.

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.

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.

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**}
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Switch> **enable**	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** Switch# **configure terminal**	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:**	Specifies the Layer 3 interface on which you want to enable multicast routing, and enters interface configuration mode.

	Command or Action	**Purpose**
	Switch(config)# **interface gigabitethernet 1/0/1**	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.
	Example:	By default, no mode is configured.
		The keywords have these meanings:
	Switch(config-if)# **ip pim sparse-dense-mode**	• **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**	Returns to privileged EXEC mode.
	Example:	
	Switch(config-if)# **end**	
Step 6	**show running-config**	Verifies your entries.
	Example:	
	Switch# **show running-config**	
Step 7	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.
	Example:	

Command or Action	Purpose
Switch# **copy running-config startup-config**	

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.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Switch> **enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Switch# **configure terminal**	Enters global configuration mode.
Step 3	**access-list** *access-list-number* **deny** *source* [*source-wildcard*] **Example:** Switch(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 *access-list-number*, the range is 1 to 99. • The **deny** keyword denies access if the conditions are matched. • For *source*, enter multicast addresses 224.0.1.39 and 224.0.1.40, which carry Auto-RP information.

	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. The access list is always terminated by an implicit deny statement for everything.
Step 4	**interface** *interface-id* **Example:** Switch(config)# **interface gigabitethernet 1/0/1**	Specifies the interface to be configured, and enters interface configuration mode.
Step 5	**ip multicast boundary** *access-list-number* **Example:** Switch(config-if)# **ip multicast boundary 12**	Configures the boundary, specifying the access list you created in Step 2.
Step 6	**end** **Example:** Switch(config)# **end**	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** Switch# **show running-config**	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** Switch# **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.

	Command or Action	**Purpose**
Step 2	**ip routing** **Example:** `Switch(config)# ip routing`	Enables IP routing mode.
Step 3	**ip vrf** *vrf-name* **Example:** `Switch(config)# ip vrf vpn1`	Names the VRF, and enter VRF configuration mode.
Step 4	**rd** *route-distinguisher* **Example:** `Switch(config-vrf)# rd 100:2`	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 an arbitrary number (A.B.C.D:y)
Step 5	**route-target** {**export** | **import** | **both**} *route-target-ext-community* **Example:** `Switch(config-vrf)# route-target import 100:2`	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* should be the same as the *route-distinguisher* entered in Step 4.
Step 6	**import map** *route-map* **Example:** `Switch(config-vrf)# import map importmap1`	(Optional) Associates a route map with the VRF.
Step 7	**ip multicast-routing vrf** *vrf-name* **distributed** **Example:** `Switch(config-vrf)# ip multicast-routing vrf vpn1 distributed`	(Optional) Enables global multicast routing for VRF table.
Step 8	**interface** *interface-id* **Example:** `Switch(config-vrf)# interface gigabitethernet 1/0/2`	Specifies the Layer 3 interface to be associated with the VRF, and enter interface configuration mode. The interface can be a routed port or an SVI.
Step 9	**ip vrf forwarding** *vrf-name* **Example:** `Switch(config-if)# ip vrf forwarding vpn1`	Associates the VRF with the Layer 3 interface.
Step 10	**ip address** *ip-address* **mask** **Example:**	Configures IP address for the Layer 3 interface.

	Command or Action	Purpose
	Switch(config-if)# ip address 10.1.5.1 255.255.255.0	
Step 11	**ip pim sparse-dense mode** **Example:** Switch(config-if)# ip pim sparse-dense mode	Enables PIM on the VRF-associated Layer 3 interface.
Step 12	**end** **Example:** Switch(config)# **end**	Returns to privileged EXEC mode.
Step 13	**show ip vrf** [**brief**	**detail**	**interfaces**] [*vrf-name*] **Example:** Switch# show ip vrf detail vpn1	Verifies the configuration. Displays 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.

Advertising Multicast Multimedia Sessions Using SAP Listener

Enable SAP listener support when you want to use session description and announcement protocols and applications to assist the advertisement of multicast multimedia conferences and other multicast sessions and to communicate the relevant session setup information to prospective participants.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sap cache-timeout** *minutes*
4. **interface** *type number*
5. **ip sap listen**
6. **end**
7. **clear ip sap** [*group-address* | " *session-name* "]
8. **show ip sap** [*group-address* | " *session-name* "| **detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Router> enable	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ip sap cache-timeout** *minutes* **Example:** Router(config)# ip sap cache-timeout 600	(Optional) Limits how long a SAP cache entry stays active in the cache. • By default, SAP cache entries are deleted 24 hours after they are received from the network.
Step 4	**interface** *type number* **Example:** Router(config)# interface ethernet 1	Selects an interface that is connected to hosts on which IGMPv3 can be enabled.
Step 5	**ip sap listen** **Example:** Router(config-if)# ip sap listen	Enables the software to listen to session directory announcements.
Step 6	**end** **Example:** Router(config-if)# end	Ends the session and returns to EXEC mode.
Step 7	**clear ip sap** [*group-address* | " *session-name* "] **Example:** Router# clear ip sap "Sample Session"	Deletes a SAP cache entry or the entire SAP cache.
Step 8	**show ip sap** [*group-address* | " *session-name* "| **detail**] **Example:** Router# show ip sap 224.2.197.250 detail	(Optional) Displays the SAP cache.

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 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.

Command	Purpose
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 pim interface [*type number*] [**count** | **detail** | **df** | **stats**]	Displays information about interfaces configured for PIM. This command is available in all software images.
show ip pim neighbor [*type number*]	Lists the PIM neighbors discovered by the device. This command is available in all software images.
show ip pim rp [*group-name* | *group-address*]	Displays the RP routers associated with a sparse-mode multicast group. This command is available in all software images.
show ip rpf {*source-address* | *name*}	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: • *Host name* or *IP address*—IP name or group address. • **Select**—Group-based VRF select information. • **vrf**—Selects VPN Routing/Forwarding instance.
show ip sap [*group* | **"***session-name***"** | **detail**]	Displays the Session Announcement Protocol (SAP) Version 2 cache. Command parameters include: • *A.B.C.D*—IP group address. • *WORD*—Session name (in double quotes). • **detail**—Session details.