CHAPTER 22

Configuring Internet Group Management Protocol for IP Multicast Support

The following sections describe how to enable Internet Group Management Protocol (IGMP) snooping and the IGMP querier function on the Cisco Catalyst 6500 Series and Cisco Catalyst 4948 Switches that connect to the Cisco TelePresence Exchange System call engines. In this configuration, IP multicast is used between the two call engines. This chapter also provides IP multicast configuration recommendations for non-Cisco switches.

Multicasting Overview

The Cisco TelePresence Exchange System employs IP multicast to replicate call states between call engine servers in a Cisco TelePresence Exchange System cluster. Therefore, the call engines must be on the same VLAN and subnet.

Note Some of the multicast traffic has a fixed TTL value of 1, which prevents the multicast traffic from being forwarded over multiple layer 3 hops.

Network interface cards (NICs) on end-stations (server or host machine) generally handle multicast traffic. To limit interrupts and congestion on end-stations that do no want to receive multicast traffic, switches can implement IGMP snooping. IGMP snooping allows a switch to learn which end-stations (in this case, the call engines) on the same VLAN want to receive the multicast traffic, and then forward traffic only to those end-station ports that sent IGMP reports and joins for specific groups. The switch then forwards the reports to multicast router (**mrouter**) ports.

By default, IGMP snooping is enabled on all Cisco switches.

IGMP Querier

You must enable the IGMP querier function to support IGMP snooping on a VLAN in which protocol independent multicast (PIM) is not active.

In a network where IP multicast routing is configured, the IP multicast router acts as the IGMP querier. If the IP multicast traffic in a VLAN only needs to be layer 2 switched, an IP multicast router is not required. Without an IP multicast router on the VLAN, you must configure the Cisco Catalyst 6500 Series and Cisco Catalyst 4948 Switches to act as the IGMP querier so that the switch can send queries.

When enabled, the IGMP querier switch sends out periodic IGMPv3 (for the Cisco Catalyst 6500) or IGMPv2 (for the Cisco Catalyst 4948) queries that trigger IGMP report messages from the end-stations (call engines). IGMP snooping listens to these IGMP reports and discovers the multicast groups that each port wishes to receive data. The switch then builds the MAC address table to allow forwarding of the traffic.

Note the following details on the Cisco implementation of the IGMP snooping querier function:

- IGMP querier must be configured on one switch within the VLAN in which the Cisco TelePresence Exchange System call engines operate. However, if the switch fails or disconnects from the VLAN, there might be an outage.
- When IGMP querier is enabled on one switch within the VLAN, it is possible for switches that do not support IGMP querier to operate within that same VLAN.
- IGMP snooping querier supports IGMP version 2 and 3.
- When enabled, the IGMP snooping querier does not start if it detects IGMP traffic from a multicast router.
- When enabled, the IGMP snooping querier starts after 60 seconds with no IGMP traffic detected from a multicast router.
- When enabled, the IGMP snooping querier disables itself if it detects IGMP traffic from a multicast router.
- When IGMP snooping is enabled, QoS does not support IGMP packets.

Note The IGMP querier feature is not supported on all switches and all platforms, therefore IGMP querier might not work for all environments. In this case, you can enable the querier function on a Cisco router. For more details, see the "Configuring PIM on a Cisco Router" section on page 22-4.

Configuring the IGMP Querier Functionality on a Cisco Switch

Before You Begin

Ensure that IGMP snooping is enabled on the Cisco Catalyst 6500 Series Switch or Cisco Catalyst 4948 Switch.

Configure a switch within the VLAN with a source address to which the IGMP querier function can forward the queries. The IP address does not need to be the default gateway.

Procedure

To configure the IGMP querier function on a Cisco Catalyst 6500 Series Switch, do the following procedure:

	Command	Purpose
Step 1	Router(config)# **ip igmp snooping**	Globally enables IGMP snooping at the global configuration mode. To disable IGMP snooping, use the **no** form of this command. **Note** By default, IGMP snooping is enabled on all Cisco routers.
Step 2	Router(config)# **interface vlan** *vlan_ID*	Selects the VLAN in which the switch and the call engines operate.
Step 3	Router(config-if)# **ip address** *ip_ address subnet_mask*	Configures the IP address for the switch, which serves as the IGMP querier within the VLAN. The switch must be in the same VLAN in which the call engines operate. When enabled, the IGMP snooping querier uses the switch IP address as the query source address.
Step 4	Router(config-if)# **ip igmp snooping querier**	Enables IGMP querier within the VLAN.
Step 5	Router(config-if)# **end**	Exits interface configuration mode.
Step 6	Router# **show ip igmp interface vlan** *vlan_ID* **| include querier**	Verifies the IGMP querier configuration of the VLAN.

Note IP addresses shown in the configurations are for example purposes only.

The following example defines an IGMP query source address within VLAN 630, and enables and verifies the IGMP querier function on the VLAN:

```
Router# interface vlan 630
Router(config-if)# ip address 10.22.143.241 255.255.255.248
Router(config-if)# igmp snooping querier
Router(config-if)# end
Router# show ip igmp interface vlan 630 | include querier
IGMP snooping fast-leave (for v2) is disabled and querier is enabled
Router#
```

Procedure

To configure the IGMP querier function on a Cisco Catalyst 4948 Switch, do the following procedure:

	Command	Purpose
Step 1	Router(config)# **ip igmp snooping**	Globally enables IGMP snooping at the global configuration mode. To disable IGMP snooping, use the **no** form of this command. **Note** By default, IGMP snooping is enabled on all Cisco routers.
Step 2	Router(config)# **interface vlan** *vlan_ID*	Selects the VLAN in which the switch and the call engines operate.

	Command	Purpose
Step 3	`Router(config-if)#` **`ip address`** *`ip_ address subnet_mask`*	Configures the IP address for the switch that serves as the IGMP querier within the VLAN. The switch must be in the same VLAN in which the call engines operate.When enabled, the IGMP querier uses the switch IP address as the query source address.
Step 4	`Router(config-if)#` **`exit`**	Exits interface configuration mode.
Step 5	`Router(config)#` **`ip igmp snooping querier`**	Enables IGMP querier functionality globally on the switch and on all VLANs on the switch.
Step 6	`Router(config)#` **`no ip igmp snooping vlan`** *`vlan_ID`* **`querier`**	Disables IGMP querier on a VLAN. Enter this command for each VLAN for which you want to disable the globally-assigned IGMP querier feature. **Note** Ensure that you do not disable IGMP querier on the VLAN in which the call engines and the switch that serves as the IGMP querier operate.
Step 7	`Router(config)#` **`ip igmp snooping vlan`** *`vlan_ID`* **`querier address`** *`ip_ address`*	Specifies the IP address for the switch that serves as the IGMP querier within the VLAN in which the call engine operates.
Step 8	`Router#` **`show ip igmp interface vlan`** *`vlan_ID`*	Verifies the IGMP querier configuration for the VLAN.

The following example defines an IGMP query source address within VLAN 585, and enables and verifies the IGMP querier function on the VLAN:

```
Router# interface vlan 585
Router(config-if)# ip address 10.22.142.242 255.255.255.224
Router(config-if)# exit
Router(config)# ip igmp snooping querier
Router(config)# no ip igmp snooping vlan 1 querier
Router(config)# ip igmp snooping vlan 585 querier address 10.22.142.242
Router# show ip igmp interface vlan 585
Vlan585 is up, line protocol is up
  Internet address is 10.22.142.242/29
  IGMP is disabled on interface
  Multicast routing is disabled on interface
  Multicast TTL threshold is 0
  No multicast groups joined by this system
  IGMP snooping is globally enabled
  IGMP snooping CGMP-AutoDetect is globally enabled
  IGMP snooping is enabled on this interface
  IGMP snooping fast-leave (for v2) is disabled
  IGMP snooping querier is enabled. Querier is 10.22.143.241 (this system)
  IGMP snooping explicit-tracking is enabled
  IGMP snooping last member query response interval is 1000 ms
  IGMP snooping report-suppression is enabled
```

Configuring PIM on a Cisco Router

You can configure PIM on Cisco IOS-based routers as well as switches that support layer 3 IP multicast routing (such as the Cisco Catalyst 6500 Series) to allow the router to operate as the IGMP querier, when IGMP querier is not supported on switches within the network.

Note IGMPv2 is the default version for Cisco routers. If IGMPv3 is required in the network, you must specify that version when configuring PIM on the router.

For details on the versions of IGMP support by platform and software version, see the *Cisco Feature Navigator* at http://www.cisco.com/go/fn.

For redundancy, Cisco recommends that you configure two routers with PIM functionality on the VLAN in which the Cisco TelePresence Exchange System call engines operate.

Cisco recommends that you reference the appropriate Cisco router configuration guide on Cisco.com to ensure that all elements of multicasting (such as multicast forwarding, multicast boundaries and rendezvous point, which is only supported on PIM sparse mode) are properly configured for the router.

Before You Begin

Enable IGMP on the switches within the network.

Procedure

To configure PIM on a Cisco router, do the following procedure:

	Command	Purpose
Step 1	`Router(config)# ip multicast-routing`	Globally enables IP multicast routing on the system. **Note** After enabling IP multicast routing on the system, you must configure PIM on the VLAN interface of the call engines. Additionally, disabling IP multicast routing does not remove PIM. PIM must be explicitly removed from the interface configurations.
Step 2	`Router(config)# interface vlan vlan_ID`	Selects the VLAN in which the router and the call engine VLAN operate.
Step 3	`Router(config-if)# ip address ip_ address subnet_mask`	Configures the IP address of the switch that connects to call engines within the VLAN. When enabled, PIM snooping querier uses the call engine IP address as the query source address.
Step 4	`Router(config-if)# ip pim sparse-mode`	Enables PIM sparse-mode on the VLAN interface.
Step 5	`Router(config-if)# ip igmp version {1|2|3}`	Sets the IGMP version type that the router uses.
Step 6	`Router(config-if)# end`	Exits interface configuration mode.
Step 7	`Router(config)# end`	Exits configuration mode.
Step 8	`Router(config)# show ip pim snooping vlan vlan-id [neighbor | mac-group | statistics | mroute [source-ip | group-ip] ]`	Shows information about a specific VLAN.

The following example enables PIM as an IGMP querier function for a router on the VLAN 630:

```
Router (config)# ip multicast-routing
Router (config)# interface vlan 630
Router(config-if)# ip address 10.22.143.241 255.255.255.248
Router(config-if)# ip pim sparse-mode
Router(config-if)# ip igmp version 3
Router(config-if)# end
Router(config)# show ip pim snooping vlan 630
3 neighbors (0 DR priority incapable, 0 Bi-dir incapable)
6 mroutes, 3 mac entries
DR is 10.10.10.4
RP DF Set
```

Configuring IGMP on a Non-Cisco Switch

The Cisco TelePresence Exchange Systems use IGMP version 2 and IGMP version 3 to join (*,G) multicast groups. Membership queries must be sent in order to maintain awareness of active receivers. Active receivers do not normally send IGMP join/reports in an unsolicited fashion; instead, they send a join at application start and when queried (IGMP RFC3376 section 4.1).

The Cisco TelePresence Exchange System call engine servers do not require or support IP multicast over multiple layer 3 hops. Therefore, multicasts occur within the VLAN. All switches that are between or directly connected to call engines must support multicast traffic without the need to see IGMP join/reports. However, because IGMP snooping specifically requires information on IGMP join/reports, a switch or router must act as a IGMP query router.

When you are configuring IGMP on a non-Cisco switch that connects to the Cisco TelePresence Exchange System call engine, note the following configuration guidelines:

- If the switch is multicast-aware and supports IGMP snooping and IGMP querier, do the following tasks:
  - Enable IGMP on the switch if it is not already active.
  - Configure the IGMP querier capability on the switch within the VLAN that the call engines operate.
- If the switch is not multicast-aware and does not support IGMP snooping or other multicast protocol, Cisco recommends placing the call engines in a dedicated VLAN to limit the multicast broadcasts that are addressed to the call engines from being broadcast to other hosts. This ensures that flooded multicast traffic in the broadcast domain will be limited to those hosts that need to receive the multicast traffic.
- If the switch does not support the IGMP querier function, but does support disabling IGMP snooping, then disable IGMP snooping on the switch.

  When you disable IGMP snooping, the multicast traffic is flooded to all hosts in the VLAN. For this reason, Cisco recommends placing the call engines in a dedicated VLAN in order to limit the multicast flooding to those hosts that need to receive the multicast traffic.
- If the switch does not support the IGMP querier function, and does not allow disabling of IGMP snooping, then configure a router interface in the call engine VLAN with PIM sparse-mode.

  Additionally, configure the router to block forwarding of multicast traffic over layer 3 hops.