CHAPTER 5

Configuring IGMP Snooping

Note The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this chapter. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping on a Cisco NX-OS switch.

This chapter includes the following sections:

Information About IGMP Snooping

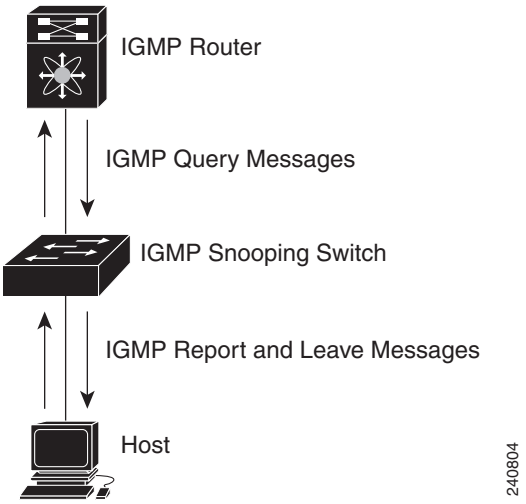
Note We recommend that you do not disable IGMP snooping on the switch. If you disable IGMP snooping, you may see reduced multicast performance because of excessive false flooding within the switch.

The Internet Group Management Protocol (IGMP) snooping software examines Layer 2 IP multicast traffic within a VLAN to discover the ports where interested receivers reside. Using the port information, IGMP snooping can reduce bandwidth consumption in a multi-access LAN environment to avoid

flooding the entire VLAN. The IGMP snooping feature tracks which ports are attached to multicast-capable routers to help the routers forward IGMP membership reports. The IGMP snooping software responds to topology change notifications. By default, IGMP snooping is enabled on the switch.

Figure 5-1 shows an IGMP snooping switch that sits between the host and the IGMP router. The IGMP snooping switch snoops the IGMP membership reports and Leave messages and forwards them only when necessary to the connected IGMP routers.

Figure 5-1 IGMP Snooping Switch



The IGMP snooping software operates upon IGMPv1, IGMPv2, and IGMPv3 control plane packets where Layer 3 control plane packets are intercepted and influence the Layer 2 forwarding behavior.

For more information about IGMP, see Chapter 3, "Configuring IGMP."

The Cisco NX-OS IGMP snooping software has the following proprietary features:

- Source filtering that allows forwarding of multicast packets based on destination and source IP.
- Multicast forwarding based on IP address rather than MAC address.
- Optimized multicast flooding (OMF) that forwards unknown traffic to routers only and performs no data driven state creation.

For more information about IGMP snooping, see RFC 4541.

This section includes the following topics:

IGMPv1 and IGMPv2

Both IGMPv1 and IGMPv2 support membership report suppression, which means that if two hosts on the same subnet want to receive multicast data for the same group, then the host that receives a member report from the other host suppresses sending its report. Membership report suppression occurs for hosts that share a port.

If no more than one host is attached to each VLAN switch port, then you can configure the fast leave feature in IGMPv2. The fast leave feature does not send last member query messages to hosts. As soon as the software receives an IGMP leave message, the software stops forwarding multicast data to that port.

IGMPv1 does not provide an explicit IGMP leave message, so the software must rely on the membership message timeout to indicate that no hosts remain that want to receive multicast data for a particular group.

Note The software ignores the configuration of the last member query interval when you enable the fast leave feature because it does not check for remaining hosts.

IGMPv3

The IGMPv3 snooping implementation on Cisco NX-OS supports full IGMPv3 snooping, which provides constrained flooding based on the (S, G) information in the IGMPv3 reports. This source-based filtering enables the switch to constrain multicast traffic to a set of ports based on the source that sends traffic to the multicast group.

By default, the software tracks hosts on each VLAN port. The explicit tracking feature provides a fast leave mechanism. Because every IGMPv3 host sends membership reports, report suppression limits the amount of traffic that the switch sends to other multicast-capable routers. When report suppression is enabled, and no IGMPv1 or IGMPv2 hosts requested the same group, the software provides proxy reporting. The proxy feature builds the group state from membership reports from the downstream hosts and generates membership reports in response to queries from upstream queriers.

Even though the IGMPv3 membership reports provide a full accounting of group members on a LAN segment, when the last host leaves, the software sends a membership query. You can configure the parameter last member query interval. If no host responds before the timeout, the software removes the group state.

IGMP Snooping Querier

When PIM is not enabled on an interface because the multicast traffic does not need to be routed, you must configure an IGMP snooping querier to send membership queries. You define the querier in a VLAN that contains multicast sources and receivers but no other active querier.

When an IGMP snooping querier is enabled, it sends out periodic IGMP queries that trigger IGMP report messages from hosts that want to receive IP multicast traffic. IGMP snooping listens to these IGMP reports to establish appropriate forwarding.

IGMP Filtering on Router Ports

IGMP filtering allows users to configure a router port on the switch that leads the switch to a Layer 3 multicast switch. The switch stores all manually configured static router ports in its router port list.

When an IGMP packet is received, the switch forwards the traffic through the router port in the VLAN. The switch recognizes a port as a router port through the PIM hello message or the IGMP query received by the switch.

IGMP Snooping with VRFs

You can define multiple virtual routing and forwarding (VRF) instances. An IGMP process supports all VRFs.

You can use the **show** commands with a VRF argument to provide a context for the information displayed. The default VRF is used if no VRF argument is supplied.

For information about configuring VRFs, see the *Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide.*

Licensing Requirements for IGMP Snooping

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	IGMP snooping requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*. **Note** Make sure the LAN Base Services license is installed on the switch to enable the Layer 3 interfaces.

Prerequisites for IGMP Snooping

IGMP snooping has the following prerequisites:

- You are logged onto the switch.
- For global commands, you are in the correct virtual routing and forwarding (VRF) mode. The default configuration mode shown in the examples in this chapter applies to the default VRF.

Default Settings

Table 5-1 lists the default settings for IGMP snooping parameters.

Table 5-1 Default IGMP Snooping Parameters

Parameters	Default
IGMP snooping	Enabled
Explicit tracking	Enabled
Fast leave	Disabled
Last member query interval	1 second
Snooping querier	Disabled
Report suppression	Enabled
Link-local groups suppression	Enabled

Table 5-1 Default IGMP Snooping Parameters (continued)

Parameters	Default
IGMPv3 report suppression for the entire switch	Disabled
IGMPv3 report suppression per VLAN	Enabled

Configuring IGMP Snooping

You configure IGMP snooping globally or per VLAN on the Cisco Nexus 3000 Series devices using the IGMP Snooping pane. You can also view the IGMP snooping status per VLAN.

Note If IGMP Snooping is disabled for the device and enabled for specified VLANs, the functionality is disabled for the VLAN as well.
However, if IGMP Snooping is disabled for the VLAN and enabled for the device, the functionality remains disabled for the VLAN.
Report Suppression and IGMPv3 Report Suppression function the same way.

This section contains the following sections:

Configuring IGMP Snooping Global Parameters

DETAILED STEPS

To set the IGMP snooping parameters for the entire device, follow these steps:

Step 1 From the Feature Selector pane, choose **Switching > Multicast > IGMP Snooping** to open the IGMP Snooping pane.

Step 2 In the Summary pane, click the device to set the IGMP snooping globally for the entire device.

Step 3 In the Details pane, click the **Device Details** tab.

Step 4 From the IGMP Snooping drop-down list, choose **Enabled** or **Disabled**.

IGMP Snooping is enabled by default.

Step 5 From the Report Suppression drop-down list, choose **Enabled** or **Disabled**.

Report Suppression is enabled by default.

Step 6 From the IGMPv3 Report Suppression drop-down list, choose **Enabled** or **Disabled**.

IGMPv3 Report Suppression is disabled by default globally for the entire device.

Step 7 From the Link-local Group Suppression drop-down list, choose **Enabled** or **Disabled**.

Link-Local Group Suppression is enabled by default.

Step 8 In the Event History Buffer Settings area, from the drop-down lists, choose **disabled**, **small**, **medium**, or **large** for each of the following:

- vPC
- IGMP Snoop Internal
- MFDM-Sum
- MFDM
- VLAN
- VLAN Events

The default buffer sizes for vPC, IGMP Snoop Internal, MFDM-Sum, and MFDM are small. The default buffer sizes for VLAN and VLAN Events are medium.

Step 9 (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.

Configuring IGMP Snooping Parameters per VLAN

DETAILED STEPS

To set the IGMP snooping parameters per VLAN, follow these steps:

Step 1 From the Feature Selector pane, choose **Switching > Multicast > IGMP Snooping** to open the IGMP Snooping pane.

Step 2 In the Summary pane, click the device that has the VLANs for which you want to configure IGMP snooping.

Step 3 Click the VLAN for which you want to configure IGMP Snooping.

Step 4 In the Details pane, click the **Details** tab.

The VLAN ID box displays the VLAN number that you are working on.

Step 5 From the IGMP Snooping drop-down list, choose **Enabled** or **Disabled**.

IGMP Snooping is enabled per VLAN by default.

Step 6 From the Report Suppression drop-down list, choose **Enabled** or **Disabled**.

Report Suppression is enabled per VLAN by default.

Step 7 From the IGMPv3 Report Suppression drop-down list, choose **Enabled** or **Disabled**.

IGMPv3 Report Suppression is enabled per VLAN by default. Once you enable IGMPv3 Report Suppression for the entire device, you do not have to enable that feature for each VLAN.

Step 8 From the Link-local Group Suppression drop-down list, choose **Enabled** or **Disabled**.

Link-Local Group Suppression is enabled per VLAN by default.

Step 9 From the Fast Leave drop-down list, choose **Enabled** or **Disabled**.

Fast Leave is disabled per VLAN by default.

Step 10 From the Explicit Tracking drop-down list, choose **Enabled** or **Disabled**.

Explicit tracking is enabled per VLAN by default.

Step 11 Enter the number of seconds that you want in the Last Member Query Interval field.

The default value for Last Member Query Interval is 1 second for each VLAN, and the maximum value is 25 seconds.

Step 12 (Optional) Enter the IP address for IGMP snooping querier for the switch.

Step 13 (Optional) Right-click in the Static Multicast Group area and choose **Add Row** or **Delete**.

a. Click **Delete** to delete a static multicast group.

b. (Optional) To add a static multicast group, enter the IP address of the multicast source in the Source Address field, the IP address of the multicast group in the Group Address field, and the interface joining the group in the Interface field.

Note Ethernet and port channel are the supported interfaces for this field.

Step 14 (Optional) Right-click in the Static Multicast Router area and choose **Add Row** or **Delete**.

a. Click **Delete** to delete an interface to a static multicast router.

b. To add an interface to the static multicast router, choose the interface from the drop-down list in the Interface field and click **OK**.

Note Ethernet and port channel are the supported interfaces for this field.

Step 15 (Optional) From the menu bar, choose **File > Deploy** to apply your changes to the device.

Viewing IGMP Snooping Status per VLAN

To view the status of the IGMP multicast groups, the IGMP multicast routers, the IGMP snooping explicit tracking feature, and the IGMP snooping querier, follow these steps:

Step 1 From the Feature Selector pane, choose **Switching > Multicast > IGMP Snooping** to open the IGMP Snooping pane.

Step 2 In the Summary pane, click the device that has the VLANs for which you want to configure IGMP snooping.

Step 3 Click the VLAN for which you want to configure IGMP Snooping.

Step 4 In the Details pane, click the **Status** tab.

Step 5 Click the Multicast Groups section.

The section expands to allow you to Refresh the display and displays the following information for each multicast group discovered using IGMP snooping: Group Address, Source Address, IGMP Version, the Type of multicast group, and the Interfaces that have shown interest in this multicast group.

Step 6 Click the Multicast Routers section.

The section expands to allow you to Refresh the display and displays the following information for each multicast router: Interface connected to the multicast router, Type, Up Time for the entry, and Expiry Time for the entry.

Step 7 Click the Explicit Tracking section.

The section expands to allow you to Refresh the display and displays the following explicit tracking information for each VLAN: Source Address for the multicast traffic, multicast Group Address, Interface that has shown interest in the multicast traffic, Reporter Address of the host machine that has shown interest in the multicast traffic, Up Time for the entry, Last Join Time, and Expiry Time for the entry.

Step 8 Click the Querier section.

The section expands to allow you to Refresh the display and displays the following IGMP snooping information for each VLAN: IP Address of the querier, IGMP Version, Expiry Time for the entry, and Interface on which the querier is discovered.

Configuring IGMP Snooping Parameters

To affect the operation of the IGMP snooping process, you can configure the optional IGMP snooping parameters described in Table 5-2.

Table 5-2 IGMP Snooping Parameters

Parameter	Description
IGMP snooping	Enables IGMP snooping on the switch or on a per-VLAN basis. The default is enabled. **Note** If the global setting is disabled, then all VLANs are treated as disabled, whether they are enabled or not.
Explicit tracking	Tracks IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis. The default is enabled.
Fast leave	Enables the software to remove the group state when it receives an IGMP Leave report without sending an IGMP query message. This parameter is used for IGMPv2 hosts when no more than one host is present on each VLAN port. The default is disabled.
Last member query interval	Sets the interval that the software waits after sending an IGMP query to verify that no hosts that want to receive a particular multicast group remain on a network segment. If no hosts respond before the last member query interval expires, the software removes the group from the associated VLAN port. Values range from 1 to 25 seconds. The default is 1 second.
Snooping querier	Configures a snooping querier on an interface when you do not enable PIM because multicast traffic does not need to be routed.
Report suppression	Limits the membership report traffic sent to multicast-capable routers on the switch or on a per-VLAN basis. When you disable report suppression, all IGMP reports are sent as is to multicast-capable routers. The default is enabled.
Multicast router	Configures a static connection to a multicast router. The interface to the router must be in the selected VLAN.
Static group	Configures a Layer 2 port of a VLAN as a static member of a multicast group.

Table 5-2 IGMP Snooping Parameters (continued)

Parameter	Description
Link-local groups suppression	Configures link-local groups suppression on the switch or on a per-VLAN basis. The default is enabled.
IGMPv3 report suppression	Configures IGMPv3 report suppression and proxy reporting on the switch or on a per-VLAN basis. The default is disabled for the entire switch and enabled per VLAN.

SUMMARY STEPS

1. **configure terminal**
2. **ip igmp snooping**
3. **vlan** *vlan-id*
4. **ip igmp snooping**
   ip igmp snooping explicit-tracking
   ip igmp snooping fast-leave
   ip igmp snooping last-member-query-interval *seconds*
   ip igmp snooping querier *ip-address*
   ip igmp snooping report-suppression
   ip igmp snooping mrouter interface *interface*
   ip igmp snooping static-group *group-ip-addr* [**source** *source-ip-addr*] **interface** *interface*
   ip igmp snooping link-local-groups-suppression
   ip igmp snooping v3-report-suppression
   (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters configuration mode.

Step 2	**ip igmp snooping** **Example:** `switch(config)# ip igmp snooping`	Enables IGMP snooping. The default is enabled. **Note** If the global setting is disabled with the **no** form of this command, then IGMP snooping on all VLANs is disabled, whether IGMP snooping is enabled on a VLAN or not. If you disable IGMP snooping, Layer 2 multicast frames flood to all modules.

Step 3	**vlan** *vlan-id*
	
	Example:
	`switch(config)# vlan 2`
	`switch(config-vlan)#`
		Enters VLAN configuration mode.

Step 4	**ip igmp snooping** **Example:** `switch(config-vlan)# ip igmp snooping`	Enables IGMP snooping for the current VLAN. The default is enabled.

Command	Purpose
ip igmp snooping explicit-tracking **Example:** `switch(config-vlan)# ip igmp snooping explicit-tracking`	Tracks IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis. The default is enabled on all VLANs.
ip igmp snooping fast-leave **Example:** `switch(config-vlan)# ip igmp snooping fast-leave`	Supports IGMPv2 hosts that cannot be explicitly tracked because of the host report suppression mechanism of the IGMPv2 protocol. When you enable fast leave, the IGMP software assumes that no more than one host is present on each VLAN port. The default is disabled for all VLANs.
ip igmp snooping last-member-query-interval *seconds* **Example:** `switch(config-vlan)# ip igmp snooping last-member-query-interval 3`	Removes the group from the associated VLAN port if no hosts respond to an IGMP query message before the last member query interval expires. Values range from 1 to 25 seconds. The default is 1 second.
ip igmp snooping querier *ip-address* **Example:** `switch(config-vlan)# ip igmp snooping querier 172.20.52.106`	Configures a snooping querier when you do not enable PIM because multicast traffic does not need to be routed. The IP address is used as the source in messages.
ip igmp snooping report-suppression **Example:** `switch(config-vlan)# ip igmp snooping report-suppression`	Limits the membership report traffic sent to multicast-capable routers. When you disable report suppression, all IGMP reports are sent as is to multicast-capable routers. The default is enabled. **Note** This command can also be entered in global configuration mode to affect all interfaces.
ip igmp snooping mrouter interface *interface* **Example:** `switch(config-vlan)# ip igmp snooping mrouter interface ethernet 2/1`	Configures a static connection to a multicast router. The interface to the router must be in the selected VLAN. You can specify the interface by the type and the number, such as **ethernet** *slot/port.*
ip igmp snooping static-group *group-ip-addr* [**source** *source*-ip-addr] **interface** *interface* **Example:** `switch(config-vlan)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1`	Configures a Layer 2 port of a VLAN as a static member of a multicast group. You can specify the interface by the type and the number, such as **ethernet** *slot/port.*
ip igmp snooping link-local-groups-suppression **Example:** `switch(config-vlan)# ip igmp snooping link-local-groups-suppression`	Configures link-local groups suppression. The default is enabled. **Note** This command can also be entered in global configuration mode to affect all interfaces.

	Command	Purpose
	ip igmp snooping v3-report-suppression **Example:** `switch(config-vlan)# ip igmp snooping v3-report-suppression`	Configures IGMPv3 report suppression and proxy reporting. The default is disabled for the global command for the entire switch and enabled per VLAN. **Note** This command can also be entered in global configuration mode to affect all interfaces.
Step 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves configuration changes.

Verifying the IGMP Snooping Configuration

To display the IGMP snooping configuration information, perform one of the following tasks:

Command	Purpose
show ip igmp snooping [**vlan** *vlan-id*]	Displays IGMP snooping configuration by VLAN.
show ip igmp snooping groups [*source* [*group*] | *group* [*source*]] [**vlan** *vlan-id*] [**detail**]	Displays IGMP snooping information about groups by VLAN.
show ip igmp snooping querier [**vlan** *vlan-id*]	Displays IGMP snooping queriers by VLAN.
show ip igmp snooping mroute [**vlan** *vlan-id*]	Displays multicast router ports by VLAN.
show ip igmp snooping explicit-tracking [**vlan** *vlan-id*]	Displays IGMP snooping explicit tracking information by VLAN.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 3000 Series Command Reference,*.

Displaying IGMP Snooping Statistics

You can select and display various statistics for the entire device in the following categories:

- IGMP snooping global statistics
- IGMP snooping global vPC statistics

You can select and display various statistics per VLAN in the following categories:

- IGMP snooping VLAN statistics
- IGMP snooping VLAN vPC statistics

Use the **show ip igmp snooping statistics vlan** command to display IGMP snooping statistics.

Use the **clear ip igmp snooping statistics vlan** command to clear IGMP snooping statistics.

For detailed information about using these commands, see the *Cisco Nexus 3000 Series Command Reference,*.

Configuration Examples for IGMP Snooping

This example shows how to configure the IGMP snooping parameters:

```
configure terminal
  ip igmp snooping
  vlan 2
    ip igmp snooping
    ip igmp snooping explicit-tracking
    ip igmp snooping fast-leave
    ip igmp snooping last-member-query-interval 3
    ip igmp snooping querier 172.20.52.106
    ip igmp snooping report-suppression
    ip igmp snooping mrouter interface ethernet 2/1
    ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1
    ip igmp snooping link-local-groups-suppression
    ip igmp snooping v3-report-suppression
```

Where to Go Next

You can enable the following features that work with PIM:

- Chapter 3, “Configuring IGMP”
- Chapter 6, “Configuring MSDP”

Field Descriptions for Configuring IGMP Snooping

This section describes the fields shown on the IGMP Snooping pane and includes the following:

- Device: Device Details Tab, page 5-12
- VLANs: Details Tab, page 5-13
- VLANs: Status Tab, page 5-14

Device: Device Details Tab

Table 5-3 Device: Device Details Tab

Element	Description
IGMP Snooping	Status of IGMP snooping. The range is enabled or disabled, and the default value is enabled.
Report Suppression	Status of report suppression. The range is enabled or disabled, and the default is enabled.
IGMPv3 Report Suppression	Status of IGMPv3 report suppression. The range is enabled or disabled, and the default is disabled.
Link-local Group Suppression	Status of the link-local group suppression. The range is enabled or disabled, and the default is enabled.
Event History Buffer Settings	

Table 5-3 Device: Device Details Tab (continued)

Element	Description
Type	Type of event history buffer. The types and the defaults are as follows: • vPC—small • IGMP Internal Snoop—small • MFDM-Sum—small • MFDM—small • VLAN—medium • VLAN Events—medium
Size	Size and status of the event history buffer. The valid values are as follows: • disabled • small • medium • large

VLANs: Details Tab

Table 5-4 VLANs: Details Tab

Element	Description
VLAN ID	*Display only.* VLAN number.
IGMP Snooping	Status of IGMP snooping. The range is enabled and disabled. The default is enabled.
Report Suppression	Status of report suppression. The range is enabled and disabled. The default is enabled.
IGMPv3 Report Suppression	Status of IGMPv3 report suppression. The range is enabled and disabled.
Link-local Group Suppression	Status of link-local group suppression. The range is enabled and disabled,.
Fast Leave	Status of fast leave. The range is enabled or disabled, and the default is disabled.
Explicit Tracking	Status of explicit tracking. The range is enabled or disabled, and the default is enabled.
Last Member Query Interval	Last member query interval in seconds. The range is 1 to 25, and the default is 1 second.
Switch Querier	IP address for the IGMP snooping switch querier.
Static Multicast Group	
Source Address	IP address of the multicast source.
Group Address	IP address of the multicast group.
Interface	Interface on which the multicast group or source is configured.

Table 5-4 VLANs: Details Tab (continued)

Element	Description
Static Multicast Router	
Interface	Interface on which the multicast router is configured.

VLANs: Status Tab

Table 5-5 VLANs: Status Tab

Element	Description
Multicast Group	
Group Address	*Display only.* IP address of the multicast group discovered by IGMP snooping.
Source Address	*Display only.* IP address of the multicast source.
IGMP Version	*Display only.* IGMP version. Valid values are as follows: • v1 • v2 • v3
Type	*Display only.* Type of discovered multicast group address discovered. Valid values are as follows: • S—static • D—dynamic • R—router port
Interface	*Display only.* List of interfaces that have shown interest in the multicast group.
Multicast Routers	
Interface	*Display only.* Interface connected to the multicast router.
Type	*Display only.* Type of multicast address. Valid values are as follows: • S—static • D—dynamic • V—vPC peer link • I—internal
Up Time	*Display only.* Time the entry has been up.
Expiry Time	*Display only.* Time at which this entry expires.
Explicit Tracking	
Source Address	*Display only.* IP address of the source for the multicast traffic.
Group Address	*Display only.* IP address for the multicast group.
Interface	*Display only.* Interface that has shown interest in receiving the multicast traffic.

Table 5-5 VLANs: Status Tab (continued)

Element	Description
Reporter Address	*Display only.* Host machine that has shown interest in receiving the multicast traffic.
Up Time	*Display only.* Length of time that the entry has been up.
Last Join Time	*Display only.* Time at which this entry was added.
Expiry Time	*Display only.* Time at which this entry expires.
Querier	
Querier Address	*Display only.* IP address of the IGMP snooping querier.
IGMP Version	*Display only.* IGMP version. Valid values are as follows: • v1 • v2 • v3.
Expiry Time	*Display only.* Time at which this entry expires.
Interface	*Display only.* Interface on which the querier is defined or discovered. **Note** The value is Self when the local device is the IGMP snooping querier.

Additional References

For additional information related to implementing IGMP snooping, see the following sections:

- Related Documents, page 5-15
- Standards, page 5-15
- Feature History for IGMP Snooping, page 5-16
- Feature History for IGMP Snooping in GUI, page 5-16

Related Documents

Related Topic	Document Title
CLI commands	*Cisco Nexus 3000 Series Command Reference,*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for IGMP Snooping

Table 5-6 lists the release history for this feature.

Table 5-6 Feature History for IGMP Snooping

Feature Name	Releases	Feature Information
IGMP Snooping	5.0(3)U1(1)	This feature was introduced.

Feature History for IGMP Snooping in GUI

Table 5-7 lists the release history for this feature.

Table 5-7 Feature History for IGMP Snooping

Feature Name	Releases	Feature Information
IGMP Snooping	5.0(1)	Introduced.