CHAPTER 1

Configuring IGMP Snooping

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

This chapter includes the following sections:

- Information About IGMP Snooping, page 1-1
- Licensing Requirements for IGMP Snooping, page 1-4
- Prerequisites for IGMP Snooping, page 1-5
- Guidelines and Limitations for IGMP Snooping, page 1-5
- Default Settings, page 1-6
- Configuring IGMP Snooping Parameters, page 1-6
- Verifying IGMP Snooping Configuration, page 1-16
- Displaying IGMP Snooping Statistics, page 1-17
- Configuration Example for IGMP Snooping, page 1-17
- Where to Go Next, page 1-17
- Additional References, page 1-18
- Feature History for IGMP Snooping in CLI, page 1-18

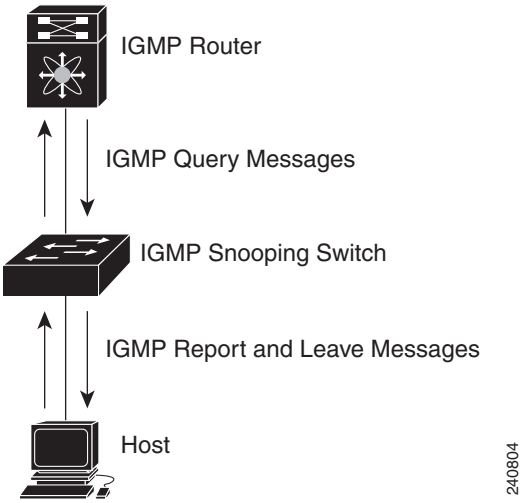
Information About IGMP Snooping

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

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. IGMP snooping 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 device.

Figure 1-1 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 1-1 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 1, "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 addresses rather than MAC address.
- Beginning with Cisco Release 5.2(1) for the Nexus 7000 Series devices, multicast forwarding alternately based on the 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, page 1-3
- IGMPv3, page 1-3
- IGMP Snooping Querier, page 1-3
- Static Multicast MAC Address, page 1-4
- IGMP Snooping with VDCs and VRFs, page 1-4

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, 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 device 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 device 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.

Static Multicast MAC Address

Beginning with the Cisco Release 5.2(1) for the Nexus 7000 Series devices, you configure an outgoing interface statically for a multicast MAC address. Also, you can configure the IGMP snooping to use a MAC-based lookup mode.

Previously, the system performs the lookup on Layer 2 multicast table using the destination IP address rather than the destination MAC address. However, some applications share a single unicast cluster IP and multicast cluster MAC address. The system forwards traffic destined to the unicast cluster IP address by the last-hop router with the shared multicast MAC address. This action can be accomplished by assigning a static multicast MAC address for the destination IP address for the end host or cluster.

The default lookup mode remains IP, but you can configure the lookup type to MAC address-based. You can configure the lookup mode globally or per VLAN:

- If the VDC contains ports from only an M Series module and the global lookup mode is set to IP, VLANs can be set to either one of the two lookup modes. But, if the global lookup mode is set to MAC address, the operational lookup mode for all the VLANs changes to MAC-address mode.
- If the VDC contains ports from both an M Series module and an F Series module and if you change the lookup mode to a MAC address in any VLAN, the operation lookup mode changes for all of the VLANs to a MAC-address based. With these modules in the chassis, you have the same lookup mode globally and for the VLANs. Similarly, if the global lookup mode is MAC-address based, the operational lookup mode for all VLAN is also MAC-address based.

Note Changing the lookup mode is disruptive. Multicast forwarding is not optimal until all multicast entries are programmed with the new lookup mode. Also, when 32 IP addresses are mapped to a single MAC address, you might see suboptimal forwarding on the device.

IGMP Snooping with VDCs and VRFs

A virtual device context (VDC) is a logical representation of a set of system resources. Within each VDC, you can define multiple virtual routing and forwarding (VRF) instances. One IGMP process can run per VDC. The IGMP process supports all VRFs in that VDC and performs the function of IGMP snooping within that VDC.

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 VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.2*.

For information about configuring VRFs, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x.*

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*.

Prerequisites for IGMP Snooping

IGMP snooping has the following prerequisites:

- You are logged onto the device.
- You are in the correct virtual device context (VDC). A VDC is a logical representation of a set of system resources. You can use the **switchto vdc** command with a VDC number.
- 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.

Guidelines and Limitations for IGMP Snooping

IGMP snooping has the following guidelines and limitations:

- You must disable IGMP optimized multicast forwarding (OMF) for IPv6 multicast networks that require multicast forwarding over a layer 2 network.
- If you are configuring vPC peers, the differences in the IGMP snooping configuration options between the two devices have the following results:
  - If IGMP snooping is enabled on one device but not on the other, the device on which snooping is disabled floods all multicast traffic.
  - A difference in multicast router or static group configuration can cause traffic loss.
  - The fast leave, explicit tracking, and report suppression options can differ if they are used for forwarding traffic.
  - If a query parameter is different between the devices, one device expires the multicast state faster while the other device continues to forward. This difference results in either traffic loss or forwarding for an extended period.
  - If an IGMP snooping querier is configured on both devices, only one of them will be active because an IGMP snooping querier shuts down if a query is seen in the traffic.

Network applications that use unicast destination IP addresses with multicast destination MAC addresses

Network applications which use unicast destination IP addresses with multicast destination MAC addresses might require the configuration of IGMP snooping to use MAC-based forwarding lookups on the switch.

If the destination MAC address used for this kind of applications is a non-IP multicast MAC address, use the **mac address-table multicast** command to statically configure the port membership.

In addition, if the destination MAC address is in the IP multicast range, 0100.5E00.0000 to 0100.5E7F.FFFF, use static IGMP snooping membership entries for the corresponding Layer 3 IP multicast address to configure the port membership. For example, if the application uses destination MAC address 0100.5E01.0101, configure a static IGMP snooping membership entry for an IP multicast address that maps to that MAC address. An example of this is **ip igmp snooping static-group 239.1.1.1**.

Default Settings

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

Table 1-1 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
IGMPv3 report suppression for the entire device	Disabled
IGMPv3 report suppression per VLAN	Enabled

Configuring IGMP Snooping Parameters

Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

You can configure IGMP snooping both globally and per VLAN. This section includes the following topics:

- Configuring Global IGMP Snooping Parameters, page 1-7
- Configuring IGMP Snooping Parameters per VLAN, page 1-9
- Changing the Lookup Mode, page 1-14
- Configuring a Static Multicast MAC Address, page 1-15

Note You must enable IGMP snooping globally before any of the other commands take effect.

Configuring Global IGMP Snooping Parameters

To affect the operation of the IGMP snooping process globally, you can configure the optional IGMP snooping parameters described in Table 1-1.

Table 1-2 Global IGMP Snooping Parameters

Parameter	Description
IGMP snooping	Enables IGMP snooping on the active VDC. The default is enabled. **Note** If the global setting is disabled, all VLANs are treated as disabled, whether they are enabled or not.
Event history	Configures the size of the IGMP snooping history buffers. The default is small.
Group timeout	Configures the group membership timeout for all VLANs on the device.
Link-local groups suppression	Configures link-local groups suppression on the device. The default is enabled.
Optimise-multicast-flood	Configures Optimized Multicast Flood (OMF) on all VLANs on the device. The default is enabled.
Proxy	Configures IGMP snooping proxy for the device. The default is 5 seconds.
Report suppression	Limits the membership report traffic sent to multicast-capable routers on the device. When you disable report suppression, all IGMP reports are sent as is to multicast-capable routers. The default is enabled.
IGMPv3 report suppression	Configures IGMPv3 report suppression and proxy reporting on the device. The default is disabled.

SUMMARY STEPS

1. **config t**
2. **ip igmp snooping**

   ip igmp snooping event-history

   ip igmp snooping group-timeout {*minutes* | **never**}

   ip igmp snooping link-local-groups-suppression

   ip igmp optimise-multicast-flood

   ip igmp snooping proxy general-inquiries [**mrt** *seconds*]

   ip igmp snooping report-suppression

   ip igmp snooping v3-report-suppression
3. **(Optional) copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters configuration mode.
Step 2	**ip igmp snooping** **Example:** switch(config)# ip igmp snooping	Enables IGMP snooping for the device. The default is enabled. **Note** If the global setting is disabled with the **no** form of this command, 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.
	ip igmp snooping event-history **Example:** switch(config)# ip igmp snooping event-history	Configures the size of the event history buffer. The default is **small**.
	ip igmp snooping group-timeout {*minutes* | **never**} **Example:** switch(config)# ip igmp snooping group-timeout never	Configures the group membership timeout value for all VLANs on the device.
	ip igmp snooping link-local-groups-suppression **Example:** switch(config)# ip igmp snooping link-local-groups-suppression	Configures link-local groups suppression for the entire device. The default is enabled.
	ip igmp snooping optimise-multicast-flood **Example:** switch(config)# ip igmp snooping optimise-multicast-flood	Optimizes OMF on all VLANs on the device. The default is enabled.
	ip igmp snooping proxy general-inquiries [**mrt** *seconds*] **Example:** switch(config)# ip igmp snooping proxy general-inquiries	Configures IGMP snooping proxy for the device. The default is 5 seconds.
	ip igmp snooping report-suppression **Example:** switch(config)# 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.

	Command	Purpose
	ip igmp snooping v3-report-suppression **Example:** `switch(config)# ip igmp snooping v3-report-suppression`	Configures IGMPv3 report suppression and proxy reporting. The default is disabled.
Step 3	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves configuration changes.

Configuring IGMP Snooping Parameters per VLAN

To affect the operation of the IGMP snooping process per VLAN, you can configure the optional IGMP snooping parameters described in Table 1-3.

Table 1-3 IGMP Snooping Parameters per VLAN

Parameter	Description
IGMP snooping	Enables IGMP snooping on a per-VLAN basis. The default is enabled. **Note** If the global setting is disabled, 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.
Group timeout	Configures the group membership timeout for the specified VLANs.
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.
Optimise-multicast-flood	Configures Optimized Multicast Flood (OMF) on specified VLANs. The default is enabled.
Proxy	Configures IGMP snooping proxy for the specified VLANs. The default is 5 seconds.

Table 1-3 IGMP Snooping Parameters per VLAN (continued)

Parameter	Description
Snooping querier	Configures a snooping querier on an interface when you do not enable PIM because multicast traffic does not need to be routed. You can also configure the following values for the snooping querier: • timeout—Timeout value for IGMPv2 • interval—Time between query transmissions • maximum response time—MRT for query messages • startup count—Number of queries sent at startup • startup interval—Interval between queries at startup
Robustness variable	Configures the robustness value for the specified VLANs.
Report suppression	Limits the membership report traffic sent to multicast-capable routers 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.
Link-local groups suppression	Configures link-local groups suppression on a per-VLAN basis. The default is enabled.
IGMPv3 report suppression	Configures IGMPv3 report suppression and proxy reporting on a per-VLAN basis. The default is enabled per VLAN.
Version	Configures the IGMP version number for the specified VLANs.

Note Beginning with Cisco Release 5.1(1), step 3 in the following configuration changed from **vlan** *vlan-id* to **vlan configuration** *vlan-id.*
You configure the IP IGMP snooping parameters that you want by using this configuration mode; however, the configurations apply only after you specifically create the specified VLAN. See the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*, for information on creating VLANs.

SUMMARY STEPS

1. **config t**
2. **ip igmp snooping**
3. **vlan** *vlan-id*

   vlan configuration *vlan-id*—Beginning with Cisco Release 5.1(1), use this command
4. **ip igmp snooping**

   ip igmp snooping explicit-tracking

   ip igmp snooping fast-leave

   ip igmp snooping group-timeout {*minutes* | **never**}

ip igmp snooping last-member-query-interval *seconds*

ip igmp optimised-multicast-flood

ip igmp snooping proxy general-queries [**mrt** *seconds*]

ip igmp snooping querier *ip-address*

ip igmp snooping querier-timeout *seconds*

ip igmp snooping query-interval *seconds*

ip igmp snooping query-max-response-time *seconds*

ip igmp snooping startup-query-count *value*

ip igmp snooping startup-query-interval *seconds*

ip igmp snooping robustness-variable *value*

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

ip igmp snooping version *value*

5. **(Optional) copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

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

Step 2	**ip igmp snooping** **Example:** `switch(config)# ip igmp snooping`	Enables IGMP snooping for the current VDC. The default is enabled. **Note** If the global setting is disabled with the **no** form of this command, 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.

	vlan configuration *vlan-id*
	
	Example:
	`switch(config)# vlan configuration 2`
	`switch(config-vlan-config)#`
		Beginning with Cisco Release 5.1(1), use this command to configure the IGMP snooping parameters you want for the VLAN. These configurations do not apply until you specifically create the specified VLAN.

	Command	Purpose
Step 4	**ip igmp snooping** **Example:** `switch(config-vlan-config)# ip igmp snooping`	Enables IGMP snooping for the current VLAN. The default is enabled.
	ip igmp snooping explicit-tracking **Example:** `switch(config-vlan-config)# 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-config)# 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 group-timeout {*minutes* | **never**} **Example:** `switch(config-vlan-config)# ip igmp snooping group-timeout never`	Configures the group membership timeout for the specified VLANs.
	ip igmp snooping last-member-query-interval *seconds* **Example:** `switch(config-vlan-config)# 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 optimised-multicast-flood **Example:** `switch(config-vlan-config)# ip igmp snooping optimised-multicast-flood`	Optimizes OMF on selected VLANs. The default is enabled.
	ip igmp snooping proxy general-queries [**mrt** | *seconds*] **Example:** `switch(config-vlan-config)# ip igmp snooping proxy general-queries`	Configures an IGMP snooping proxy for specified VLANs. The default is 5 seconds.
	ip igmp snooping querier *ip-address* **Example:** `switch(config-vlan-config)# 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 querier-timeout *seconds* **Example:** `switch(config-vlan-config)# ip igmp snooping querier-timeout 300`	Configures a snooping querier timeout value for IGMPv2 when you do not enable PIM because multicast traffic does not need to be routed. The default is 255 seconds.
	ip igmp snooping query-interval *seconds* **Example:** `switch(config-vlan-config)# ip igmp snooping query-interval 120`	Configures a snooping query interval when you do not enable PIM because multicast traffic does not need to be routed. The default value is 125 seconds.

Command	Purpose
ip igmp snooping query-max-response-time *seconds* **Example:** `switch(config-vlan-config)# ip igmp snooping query-max-response-time 12`	Configures a snooping MRT for query messages when you do not enable PIM because multicast traffic does not need to be routed. The default value is 10 seconds.
ip igmp snooping startup-query-count *value* **Example:** `switch(config-vlan-config)# ip igmp snooping startup-query-count 5`	Configures snooping for a number of queries sent at startup when you do not enable PIM because multicast traffic does not need to be routed.
ip igmp snooping startup-query-interval *seconds* **Example:** `switch(config-vlan-config)# ip igmp snooping startup-query-interval 15000`	Configures a snooping query interval at startup when you do not enable PIM because multicast traffic does not need to be routed.
ip igmp snooping robustness-variable *value* **Example:** `switch(config-vlan-config)# ip igmp snooping robustness-variable 5`	Configures the robustness value for the specified VLANs. The default value is 2.
ip igmp snooping report-suppression **Example:** `switch(config-vlan-config)# 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.
ip igmp snooping mrouter interface *interface* **Example:** `switch(config-vlan-config)# 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-config)# 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-config)# ip igmp snooping link-local-groups-suppression`	Configures link-local groups suppression for the specified VLANs. The default is enabled.
ip igmp snooping v3-report-suppression **Example:** `switch(config-vlan-config)# ip igmp snooping v3-report-suppression`	Configures IGMPv3 report suppression and proxy reporting for the specified VLANs. The default is enabled per VLAN.

	Command	Purpose
	ip igmp snooping version *value* **Example:** switch(config-vlan-config)# ip igmp snooping version 2	Configures the IGMP version number for the specified VLANs.
Step 5	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	(Optional) Saves configuration changes.

Changing the Lookup Mode

Beginning with Cisco Release 5.2(1) for the Nexus 7000 Series chassis, you can configure the lookup mode to be based on the MAC address either globally or per VLAN.

SUMMARY STEPS

1. **config t**
2. **layer-2 multicast lookup mode**

   Use this command to change the lookup mode globally
3. **vlan** *vlan-id*
   layer-2 multicast lookup mac

   Use these 2 commands to change the lookup mode per VLAN. See the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x* for information on the VLAN configuration mode.
4. **exit**
5. (Optional) **show ip igmp snooping lookup-mode** [**vlan** *vlan-id*]
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**layer-2 multicast lookup mode** **Example:** switch(config)# layer-2 multicast lookup mode	Globally changes the lookup mode to be based on MAC address. To return to the default IP lookup mode, use the **no** form of this command.

	Command	Purpose

Step 3	**vlan** *vlan-id*
	
	Example:
	`switch(config)# vlan 5`
	`switch(config-vlan)#`
	
	layer-2 multicast lookup mode
	
	Example:
	`switch(config-vlan)# layer-2 multicast lookup mode`
	`switch(config-vlan)`
		Changes the lookup mode to be based on the MAC address for the specified VLANs. To return to the default IP lookup mode for these VLANs, use the **no** form of this command.

Step 4	**exit**
	
	Example:
	`switch(config)# exit`
	`switch#`
		Exits configuration and/or VLAN configuration mode.

Step 5	**show ip igmp snooping lookup-mode** [**vlan** *vlan-id*] **Example:** `switch# show ip igmp snooping lookup-mode`	(Optional) Displays the IGMP snooping lookup mode.
Step 6	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring a Static Multicast MAC Address

Beginning with Cisco Release 5.2(1) for the Nexus 7000 Series chassis, you can configure an outgoing interface statically for a multicast MAC address.

SUMMARY STEPS

1. **config t**
2. **mac address-table multicast** *multicast-mac-addr* **vlan** *vlan-id* **interface** *slot/port*
3. **exit**
4. (Optional) **show ip igmp snooping mac-oif** [**detail** | **vlan** *vlan-id* [**detail**]]
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**mac address-table multicast** *multicast-mac-addr* **vlan** *vlan-id* **interface** *slot/port* **Example:** switch(config)# mac address-table multicast 01:00:5f:00:00:00 vlan 5 interface ethernet 2/5	Configures the specified outgoing interface statically for a multicast MAC address.
Step 3	**exit** **Example:** switch(config)# exit switch#	Exits configuration and/or VLAN configuration mode.
Step 4	**show ip igmp snooping mac-oif** [**detail** | **vlan** *vlan-id* [**detail**]] **Example:** switch# show feature-set	(Optional) Displays the IGMP snooping static MAC addresses.
Step 5	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Verifying 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 the 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.
show ip igmp snooping lookup-mode [**vlan** *vlan-id*]	Displays the IGMP snooping lookup mode.
show ip igmp snooping mac-oif [**detail** | **vlan** *vlan-i*d [**detail**]]	Displays IGMP snooping static MAC addresses.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference, Release 5.x*.

Displaying IGMP Snooping Statistics

Use the **show ip igmp snooping statistics vlan** command to display IGMP snooping statistics. You can see the virtual port channel (vPC) statistics in this output.

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 7000 Series NX-OS Multicast Routing Command Reference, Release 5.x*.

Configuration Example for IGMP Snooping

The following example shows how to configure the IGMP snooping parameters:

```
config t
  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
```

The following example shows how to configure the IGMP snooping parameters beginning with Cisco Release 5.1(1):

```
config t
  ip igmp snooping
  vlan configuration 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
```

These configurations do not apply until you specifically create the specified VLAN. See *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x* for information on creating VLANs.

Where to Go Next

You can enable the following features that work with PIM:

- Chapter 1, “Configuring IGMP”
- Chapter 1, “Configuring MLD”
- Chapter 1, “Configuring MSDP”

Additional References

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

- Related Documents, page 1-18
- Standards, page 1-18
- Feature History for IGMP Snooping in CLI, page 1-18

Related Documents

Related Topic	Document Title
VDCs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.2*
CLI commands	*Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference, Release 5.x*

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 in CLI

Table 1-4 lists the release history for this feature.

Table 1-4 Feature History for IGMP Snooping

Feature Name	Releases	Feature Information
Configuring lookup mode to MAC and assigning a static MAC address	5.2(1)	You can configure IGMP snooping to use the forwarding lookup mode as MAC-based, as well as assign a static MAC address.

Table 1-4 Feature History for IGMP Snooping

Feature Name	Releases	Feature Information
vlan configuration *vlan-id*	5.1(1)	Command added to allow you to configure a VLAN before you actually create the VLAN.
vPC	4.1(3)	List of guidelines and limitations that apply to a vPC. Display vPC statistics with the **show ip igmp snooping statistics vlan** command. The following sections provide information about this feature: • "Guidelines and Limitations for IGMP Snooping" section on page 1-5 • "Displaying IGMP Snooping Statistics" section on page 1-17