Configuring IGMP Snooping

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

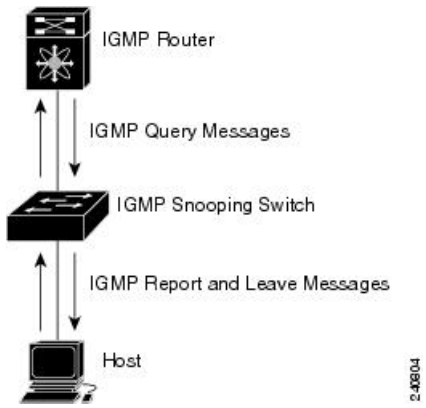
Information About IGMP Snooping

Note We recommend that you do not disable IGMP 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 multiaccess 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.

This figure 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: 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 *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 addresses.
- 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.

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.

The querier can be configured to use any IP address in the VLAN.

As a best practice, a unique IP address, one that is not already used by the switch interface or the HSRP VIP, should be configured so as to easily reference the querier. In a vPC configuration too, the querier IP should be unique on the vPC primary and secondary.

Note The IP address for the querier should not be a broadcast IP, multicast IP, or 0(0.0.0.0).

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.

The IGMP snooping querier performs querier election as described in RFC 2236. A querier election occurs in the following configurations:

- When there are multiple switch queriers configured with the same subnet on the same VLAN on different switches.
- When the configured switch querier is in the same subnet as with other Layer 3 SVI queriers.

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 a 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 a 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*.

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

IGMP Snooping across VPLS Domains

Beginning with Cisco Release 6.2(2) for the Nexus 7000 Series devices, IGMP snooping can be configured across Virtual Private LAN Service (VPLS) domains. The IGMP Snooping across VPLS Domains feature enables snooping of the IGMP packets on the pseudowire and on the Layer 2 side of the network for optimal delivery of the multicast packets.

A pseudowire is a point-to-point connection between pairs of Provider Edge (PE) devices. A pseudowire emulates services like Ethernet over an underlying core multiprotocol label switching (MPLS) network through encapsulation into a common MPLS format. A pseudowire allows carriers to converge their services to an MPLS network by encapsulating services into a common MPLS format.

By snooping IGMP packets received on a link, the device sends multicast packets only to interested end points. Once an IGMP packet going over the Layer 2 link is snooped, it is passed to the control plane. The control plane will add the link on which it was received to the multicast group. The IGMP packets coming on the pseudowire are also snooped and sent to the control plane. The control plane then adds the pseudowire to the multicast group. When a multicast packet is received, it will be sent only to the multicast group instead of flooding the VLAN.

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 flooding (OMF) for IPv6 multicast networks that require multicast forwarding over a layer 2 network.
- You must disable IGMP optimized multicast forwarding on VLANs that require forwarding of IPv6 packets.
- When a vPC peer-link runs in a F2 module, IGMP querier election does not happen. Hence do not configure vPC peer-link in a F2 module.
- 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.
- You must enable ip igmp snooping group-timeout when you use ip igmp snooping proxy general-queries. We recommend to set it to "never." If this is not done you might have multicast packet loss.

- Network applications that 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. 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 for IGMP Snooping

This table lists the default settings for 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.

Note You must enable IGMP snooping globally before any 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 the following table:

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.

Notes for IGMP Snooping Parameters

The following are additional notes about some of the IGMP snooping parameters.

- IGMP Snooping Proxy parameter

  To decrease the burden placed on the snooping switch during each IGMP general query (GQ) interval, Cisco NX-OS provides a way to decouple the periodic general query behavior of the IGMP snooping switch from the query interval configured on the multicast routers.

  Beginning with Cisco NX-OS release 5.2(1), a configuration option became available to enable the Cisco Nexus 7000 switch to consume IGMP general queries from the multicast router, rather than flooding the general queries to all the switchports.

  When receiving a general query, the switch produces proxy reports for all currently active groups and distributes the proxy reports over the period specified by the MRT that is specified in the router query. At the same time, independent of the periodic general query activity of the multicast router, the switch

sends an IGMP general query on each port in the VLAN in a round-robin fashion. It cycles through all the interfaces in the VLAN at the rate given by the following formula.

Rate = {number of interfaces in VLAN} * {configured MRT} * {number of VLANS}

When running queries in this mode, the default MRT value is 5,000 milliseconds (5 seconds), which means that in a switch that has 500 switchports in a VLAN, it would take 2,500 seconds (40 minutes) to cycle through all the interfaces in the system. This is also true when the Cisco Nexus 7000 switch itself is the querier.

This behavior ensures that only one host responds to a general query at a given time and it keeps the simultaneous reporting rate below the packet-per-second IGMP capability of the switch (approximately 3,000 to 4,000 pps).

Note When using this option, you must change the **ip igmp snooping group-timeout** parameter to a high value or to never time out.

The **ip igmp snooping proxy general-queries**[*mrt*] command causes the snooping function to proxy reply to general queries from the multicast router, while also sending round-robin general queries on each switchport with the specified MRT value (the default MRT value is 5 seconds).

- IGMP Snooping Group-timeout parameter

  Configuring the group-timeout parameter disables the behavior of expiring membership based on three missed general queries. The group membership remains on a given switchport until the switch receives an explicit IGMP leave on that port.

  The **ip igmp snooping group-timeout** {*timeout*|*never*} command modifies or disables the behavior of an expiring IGMP snooping group membership after three missed general queries.

Procedure

	Command or Action	Purpose
Step 1	**config t** **Example:** `switch# config t` `switch(config)#`	Enters global configuration mode.
Step 2	The following commands can be used to configure the IGMP snooping.	

Option	Description
ip igmp snooping `switch(config)# ip igmp snooping`	Enables IGMP snooping for the device. The default is enabled.

Command or Action	Purpose
Option	**Description**
	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. **Note** IGMP snooping can be configured across Virtual Private LAN Service (VPLS) domains.
ip igmp snooping event-history {**igmp-snoop-internal** | **mfdm** | **mfdm-sum** | **rib** | **vlan** | **vlan-events** | **vpc**} **size**	Configures the size of the event history buffer. The default is **small.**

Command or Action	Purpose
Option	**Description**
{**disabled** | **large** | **medium** | **small**} `switch(config)# ` **ip igmp snooping event-history igmp-snoop-internal size large**	
ip igmp snooping group-timeout{*minutes*|*never*} `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 `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 `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-queries [**mrt** *seconds*] `switch(config)# ` **ip igmp snooping proxy general-queries**	Configures IGMP snooping proxy for the device. The default is 5 seconds.
ip igmp snooping v3-report-suppression `switch(config)# ip igmp snooping v3-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 report-suppression `switch(config)# ip igmp snooping report-suppression`	Configures IGMPv3 report suppression and proxy reporting. The default is disabled.

	Command or Action	Purpose
	Option / **Description**	
	ip igmp snooping max-gq-miss *count* `switch(config)# ip igmp snooping max-gq-miss 5` — Configures the maximum number of general query misses permitted. The range is 3 to 5 queries. The default is 3 queries.	
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 this table.

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.

Parameter	Description
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.
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** You must configure access-group (policy filter), for this command to function correctly.

Note Beginning with Cisco Release 5.1(1), step 3 in the following procedure changed from **vlan** 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* for information on creating VLANs.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal` `switch(config)#`	Enters global 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	**Option** / **Description** **vlan** *vlan-id* `switch(config)# vlan 2` `switch(config-vlan)#` — Enters VLAN configuration mode. **vlan configuration** *vlan-id* `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	Depending on your release of Cisco NX-OS, use one of the commands in the table.

	Command or Action		Purpose
	Option	**Description**	
		create the specified VLAN.	

	Command or Action		Purpose
Step 4	**Option**	**Description**	These commands configure IGMP snooping parameters.
	ip igmp snooping `switch(config-vlan-config)# ip igmp snooping`	Enables IGMP snooping for the current VLAN. The default is enabled.	
	ip igmp snooping explicit-tracking `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 `switch(config-vlan-config)# ip igmp snooping fast-leave`	Supports IGMPv2 hosts that cannot be explicitly tracked.	

	Command or Action		Purpose
	Option	Description	
		because of the host report suppression mechanism of the IGMP 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**} `switch(config-vlan-config)# ip igmp snooping group-timeout never`	Configures the group membership timeout for the	

	Command or Action		Purpose
	Option	Description	
		specified VLANs	
	ip igmp snooping last-member-query-interval *seconds* `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. Value range from 1 to 25 seconds. The default is 1 second	
	ip igmp snooping optimise-multicast-flood `switch(config-vlan-config)# ip igmp snooping optimise-multicast-flood`	Optimises OMF on selected VLANs. The default is enabled	

	Command or Action		Purpose
	Option	**Description**	
	ip igmp snooping proxy general-queries mrt *seconds* `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* `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* `switch(config-vlan-config)# ip igmp snooping querier-timeout 300`	Configures a snooping querier timeout	

	Command or Action		Purpose
	Option	**Description**	
		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* `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	

	Command or Action		Purpose
	Option	**Description**	
		125 seconds	
	ip igmp snooping query-max-response-time *seconds* `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* `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	

	Command or Action		Purpose
	Option	**Description**	
		because multicast traffic does not need to be routed	
	ip igmp snooping startup-query-interval *seconds* `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* `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	Limits the	

	Command or Action		Purpose
	Option	**Description**	
	`switch(config-vlan-config)# ip igmp snooping report-suppression`	Enables or disables report traffic sent to multicast routers. When you disable report suppression, all IGMP reports are sent as is to multicast routers. The default is enabled.	
	ip igmp snooping mrouter interface *interface* `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	

	Command or Action		Purpose
	Option	Description	
		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* `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 `switch(config-vlan-config)# ip igmp snooping link-local-groups-suppression`	Configures link-local groups suppression for the	

	Command or Action	Purpose
	Option / **Description** specified VLANs. The default is enabled **ip igmp snooping v3-report-suppression** `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 **ip igmp snooping version** *value* `switch(config-vlan-config)# ip igmp snooping version 2` Configures the IGMP version number for the specified VLANs **Note** You must configure access-group (policy filter), for this command to function correctly.	
Step 5	**copy running-config startup-config** **Example:**	(Optional) Saves configuration changes.

	Command or Action	Purpose
	`switch(config)# copy running-config startup-config`	

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.

Procedure

	Command or Action	Purpose
Step 1	**config t** **Example:** `switch# config t` `switch(config)#`	Enters global configuration mode.
Step 2	**layer-2 multicast lookup mac** **Example:** `switch(config)# layer-2 multicast lookup mac`	Globally changes the lookup mode to be based on the MAC address. To return to the default IP lookup mode, use the **no** form of this command. **Note** After **layer-2 multicast lookup mac** is configured, the Cisco Nexus 7000 device still floods unicast traffic with multicast MAC address under the following conditions: • Both ingress and egress ports are either on M1 or M2 module. • Both ingress and egress ports are layer 2 ports (e.g. either an access port or a trunk port) in two different VLANs. Cisco Nexus 7000 device provides routing between the two VLANs. • The destination IP address is a NLB multicast/IGMP host. In other words, the destination IP is unicast and the destination MAC address starts with 0100.5E.
Step 3	**vlan** *vlan-id* **Example:**	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.

	Command or Action	Purpose
	`switch(config)# vlan 5` `switch(config-vlan)#` `layer-2 multicast lookup mac` `switch(config-vlan)# layer-2 multicast lookup mac` `switch(config-vlan)#`	
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.

Procedure

	Command or Action	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`	Configures the specified outgoing interface statically for a multicast MAC address.

	Command or Action	Purpose
	`multicast 01:00:5f:00:00:00 vlan 5 interface ethernet 2/5`	
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 configuration information, perform one of the following tasks:

Command or Action	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-id*[**detail**]]	Displays IGMP snooping static MAC addresses.
show ip igmp snooping pw vlan brief	Displays VLANs, which have pseudowire interfaces that are operationally up.

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*.

Configuration Example for IGMP Snooping

This example shows how to configure the IGMP snooping parameters:

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

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

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

The following example shows how to configure IGMP Snooping across VPLS Domains:

```
switch# configure terminal
switch(config)# ip igmp snooping
switch(config)# ip igmp snooping event-history igmp-snoop-internal size large
switch(config)# ip igmp snooping group-timeout never
switch(config)# ip igmp snooping link-local-groups-suppression
switch(config)# ip igmp snooping optimise-multicast-flood
switch(config)# ip igmp snooping proxy general-queries
```

```
switch(config)# ip igmp snooping report-suppression
switch(config)# ip igmp snooping v3-report-suppression
```

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

Related Documents

Related Topic	Document Title
VDCs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*
CLI commands	*Cisco Nexus 7000 Series NX-OS Multicast Routing 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 in CLI

Feature Name	Releases	Feature Information
ip igmp snooping max-gq-miss *count*	6.2(2)	Command added to allow you to configure the maximum number of general query misses permitted.
IGMP Snooping across VPLS domains	6.2(2)	The IGMP Snooping across VPLS Domains feature enables snooping of the IGMP packets on the pseudowire as well as on the Layer 2 side of the network for optimal delivery of the multicast packets. The following command was introduced: **show ip igmp snooping pw vlan brief**

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.
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* • *Displaying IGMP Snooping Statistics*