Configuring IGMP Snooping

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping on Cisco Nexus 3600 platform switches.

This chapter includes the following sections:

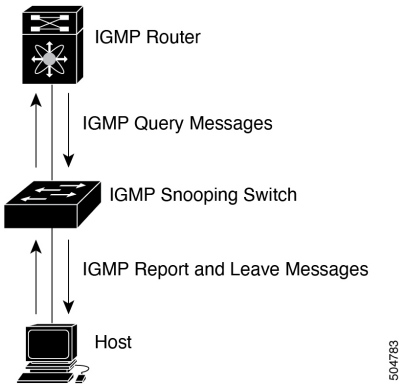
Information About IGMP Snooping

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.

The following 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 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, the switch sends out periodic queries (with the source address of the configured querier address). These queries trigger IGMP report messages from hosts that want to receive IP multicast traffic.

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.

Guidelines and Limitations for IGMP Snooping

IGMP snooping has the following guidelines and limitations:

- Cisco Nexus 3600 platform switches support IGMP snooping for IPv4 only.
- Cisco Nexus 3600 platform switches support IGMP snooping with vPCs.
- The IGMP snooping configuration must be identical on both vPC peers in a vPC pair. Either enable or disable IGMP snooping on both vPC peers.

Note Enabling or disabling IGMP snooping on both vPC peers also enables the forwarding of IGMP queries from different MVR source VLANs into the same MVR receiver VLAN. The resulting IGMP queries may send out queries with different versions and query interval. If you prefer to maintain the behavior before Cisco NX-OS Release 7.0(3)I3(1), use the **mvr-suppress-query** command. For more information about suppressing IGMP general query forwarding, see Suppressing IGMP Query Forwarding from VLANs.

- In releases before Cisco NX-OS Release 7.0(3)I3(1), 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.

Default Settings for IGMP Snooping

The following table lists the default settings for IGMP snooping parameters.

Table 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 switch	Disabled

Parameters	Default
IGMPv3 report suppression per VLAN	Enabled

Note

- When a SPAN session is configured with a multicast router port being the source port, the destination port sees all the multicast traffic even when there is no traffic that is actually being forwarded to the source port. This is due to a current limitation of the multicast/SPAN implementation.
- Cisco Nexus 3548 Series switches replicate unknown multicast traffic to multicast router ports of all VLANs, although the multicast traffic is received in one particular VLAN. This is a default behavior and cannot be configured.

Configuring IGMP Snooping Parameters

To affect the operation of the IGMP snooping process, you can configure the optional IGMP snooping parameters described in the following table.

Table 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.
Access group	Configures a policy to filter IGMP joins per VLAN.
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.

Parameter	Description
Proxy leave messages	Changes the destination address of proxy leave messages to the address of the group that is leaving. Normally, IGMP proxy leave messages generated by the IGMP snooping module use the 224.0.0.2 multicast router address when all hosts leave the group. You should implement this configuration if your multicast applications rely on receiving reports and leave messages to start or stop multicast traffic based on the destination address of the packet.
Floods report and leaves	Floods IGMP reports on all active interfaces of the VLAN or only on specific interfaces and leaves. IGMP reports typically are forwarded to multicast router ports as detected by the IGMP snooping module and are not flooded in the VLAN. However, this command forces the switch to send IGMP reports to custom ports belonging to the VLAN in addition to the multicast router ports. You should implement this configuration if your multicast applications require the ability to view IGMP reports in order to transmit traffic.
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.
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

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 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.

Step 3	**vlan configuration** *vlan-id*
	Example:
	`switch(config)# vlan configuration 100`
	`switch(config-vlan-config)#`
		Configures a VLAN and enters VLAN configuration mode.

Step 4		

Option	Description
Command	Purpose
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 access-group route-map-name Example: `switch(config-vlan-config)# ip igmp snooping access-group rmap`	Configures a policy to filter IGMP joins per VLAN. The default is disabled.
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:	Supports IGMPv2 hosts that cannot be explicitly tracked because of the

Command or Action		Purpose
Option	**Description**	
`switch(config-vlan-config)# ip igmp snooping fast-leave`	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-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.	
[**no**] **ip igmp snooping proxy-leave use-group-address** Example: `switch(config-vlan-config)# ip igmp snooping proxy-leave use-group-address`	Changes the destination address of proxy leave messages to the address of the group that is leaving. Normally, IGMP proxy leave messages generated by the IGMP snooping module use the 224.0.0.2 multicast router address when all hosts leave the group. You should implement this configuration if your multicast applications rely on receiving reports and leave messages to start or stop multicast traffic based on the destination address of the packet.	
[**no**] **ip igmp snooping report-flood** { **all** | **interface ethernet** *slot/port*} Example:	Floods IGMP reports on all active interfaces of the VLAN or only on specific interfaces and leaves.	

Command or Action		Purpose
Option	**Description**	
`switch(config-vlan-config)# ip igmp snooping report-flood interface ethernet 1/2 ip igmp snooping report-flood interface ethernet 1/3`	IGMP reports typically are forwarded to multicast router ports as detected by the IGMP snooping module and are not flooded in the VLAN. However, this command forces the switch to send IGMP reports to custom ports belonging to the VLAN in addition to the multicast router ports. You should implement this configuration if your multicast applications require the ability to view IGMP reports in order to transmit traffic.	
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 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. **Note** This command can also be entered in global configuration mode to affect all interfaces.	

Command or Action		Purpose
Option	**Description**	
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. The default is enabled. **Note** This command can also be entered in global configuration mode to affect all interfaces.	
ip igmp snooping v3-report-suppression Example: `switch(config-vlan-config)# 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.	

	Command or Action		Purpose
	Option	Description	
		Note	This command can also be entered in global configuration mode to affect all interfaces.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`		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 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.

Setting the Interval for Multicast Routes

When the switch has high multicast route creation or deletion rates (for example, too many IGMP join or leave requests), the switch cannot program the multicast routes into the hardware as fast as the requests are made. To resolve this problem, you can configure an interval after which multicast routes are programmed into the hardware.

When you have very low multicast route creations or deletions per second, configure a low interval (up to 50 milliseconds). A low interval enables the hardware to be programmed faster than it would be by using the default interval of 1 second.

When you have very high multicast route creations or deletions per second, configure a high interval (up to 2 seconds). A high interval enables the hardware to be programmed over a longer period of time without dropping the requests.

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.

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
```