Configuring IGMP Snooping

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

This chapter includes the following sections:

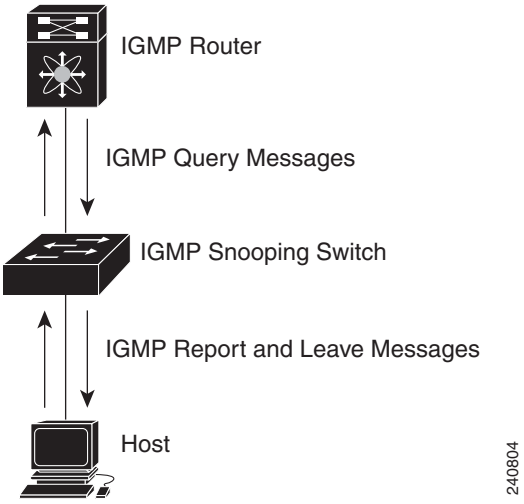
Information About IGMP Snooping

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

The Internet Group Management Protocol (IGMP) snooping software examines Layer 2 IP multicast traffic within a VLAN to discover the ports where interested receivers reside. Using the port information, IGMP snooping can reduce bandwidth consumption in a multi-access LAN environment to avoid flooding the entire VLAN. The IGMP snooping feature tracks which ports are attached to multicast-capable routers to help the routers forward IGMP membership reports. The IGMP snooping software responds to topology change notifications. By default, IGMP snooping is enabled on the switch.

Figure 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 address rather than MAC address.
- Optimized multicast flooding (OMF) that forwards unknown traffic to routers only and performs no data driven state creation.

For more information about IGMP snooping, see RFC 4541.

This section includes the following topics:

IGMPv1 and IGMPv2

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

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

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

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

IGMPv3

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

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

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

IGMP Snooping Querier

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

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

IGMP Filtering on Router Ports

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

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

IGMP filtering is typically used in a virtual port channel (vPC) topology or in a small network with a simple topology where the network traffic is predictable.

IGMP Snooping on Virtual Port Channels

IGMP snooping on a vPC switch is determined by the vPC peer link that receives an IGMP report or query. The multicast control packets required for IGMP snooping need to be seen by IGMP in both the vPC switches.

When an IGMP report or query is received by the vPC peer link on a non-vPC port, the vPC peer link on the switch acts as an output interface (OIF) for a multicast group or router port and floods the packet on the vPC peer link, vPC links, and non-vPC links using Cisco Fabric Services (CFS), which means that the individual packets are encapsulated as CFS packets and sent over the vPC peer link. The peer vPC switch that receives this packet on the vPC peer link floods it on all non-vPC links and adds the peer link to the router port list.

When an IGMP report or query is received by the vPC peer link on a vPC port, the vPC port acts as the router port list and the switch floods the packet on the vPC link, vPC peer link, and non-vPC links using CFS. The peer vPC switch that receives this packet on the vPC peer link floods it on all non-vPC links and adds the vPC port to the router port list. If the vPC port is down, the IGMP snooping software on the switch forwards the packet to the vPC peer link and the peer vPC switch then forwards the packets to all VLANs.

When IGMP snooping on a vPC switch goes down or is not enabled, the IGMP report or query is sent through the vPC peer link to the peer vPC switch that is running IGMP snooping. The vPC peer link is set as an OIF for a multicast group or router port.

If switch virtual interfaces (SVIs) are enabled on the VLANs of the vPC peers, each vPC peer acts as a designated router (DR) to forward the multicast traffic. If the vPC peer link fails, the SVIs and vPC peer links on the vPC secondary switch also goes down. The primary vPC switch then forwards all traffic.

IGMP Snooping with VRFs

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

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

For information about configuring VRFs, see the *Cisco Nexus 5500 Series NX-OS Unicast Routing Configuration Guide, Release 7.0.*

Licensing Requirements for IGMP Snooping

The following table shows the licensing requirements for this feature:

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

Prerequisites for IGMP Snooping

IGMP snooping has the following prerequisites:

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

Guidelines and Limitations for IGMP Snooping

IGMP snooping has the following guidelines and limitations:

Note The **Optimised Multicast Flooding** (OMF) feature in IGMP snooping is not supported in Cisco Nexus 5000 Series switches and Cisco Nexus 6000 Series switches.

- If you are configuring vPC peers, the differences in the IGMP snooping configuration options between the two switches have the following results:
  - If IGMP snooping is enabled on one switch but not the other, then the switch 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 switches, one switch expires the multicast state faster while the other switch 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 switches, only one of them will be active because an IGMP snooping querier shuts down if a query is seen in the traffic.
  - A vPC peer link is a valid link for IGMP multicast forwarding.
  - If the vPC link on a switch is configured as an output interface (OIF) for a multicast group or router port, the vPC link on the peer switch must also be configured as an output interface for a multicast group or router port.
  - In SVI VLANs, the vPC peers must have the multicast forwarding state configured for the vPC VLANs to forward multicast traffic directly through the vPC link instead of the peer link.
  - Fabric Extenders do not support mrouter ports.
- On Cisco Nexus 5548 switch, multicast traffic to groups in the range [225-239].0.0.x should not be used as there will be no S, G, or multicast MAC addresses learned for these groups. For example, use group 225.0.1.10 instead of group 225.0.0.10.

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 switch	Disabled
IGMPv3 report suppression per VLAN	Enabled

Configuring IGMP Snooping Parameters

To affect the operation of the IGMP snooping process, you can configure the optional IGMP snooping parameters described in Table 1-2.

Table 1-2 IGMP Snooping Parameters

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

Table 1-2 IGMP Snooping Parameters (continued)

Parameter	Description
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.

SUMMARY STEPS

1. **configure terminal**
2. **ip igmp snooping**
3. **vlan** *vlan-id*
4. **ip igmp snooping**
   ip igmp snooping explicit-tracking
   ip igmp snooping fast-leave
   ip igmp snooping last-member-query-interval *seconds*
   ip igmp snooping querier *ip-address*
   ip igmp snooping report-suppression
   ip igmp snooping mrouter interface *interface*
   ip igmp snooping static-group *group-ip-addr* [**source** *source-ip-addr*] **interface** *interface*
   ip igmp snooping link-local-groups-suppression
   ip igmp snooping v3-report-suppression
   no ip igmp snooping mrouter vpc-peer-link
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

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

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

	Command	Purpose

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

Step 4	**ip igmp snooping** **Example:** `switch(config-vlan)# ip igmp snooping`	Enables IGMP snooping for the current VLAN. The default is enabled.
	ip igmp snooping explicit-tracking **Example:** `switch(config-vlan)# ip igmp snooping explicit-tracking`	Tracks IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis. The default is enabled on all VLANs.
	ip igmp snooping fast-leave **Example:** `switch(config-vlan)# ip igmp snooping fast-leave`	Supports IGMPv2 hosts that cannot be explicitly tracked because of the host report suppression mechanism of the IGMPv2 protocol. When you enable fast leave, the IGMP software assumes that no more than one host is present on each VLAN port. The default is disabled for all VLANs.
	ip igmp snooping last-member-query-interval *seconds* **Example:** `switch(config-vlan)# ip igmp snooping last-member-query-interval 3`	Removes the group from the associated VLAN port if no hosts respond to an IGMP query message before the last member query interval expires. Values range from 1 to 25 seconds. The default is 1 second.
	ip igmp snooping querier *ip-address* **Example:** `switch(config-vlan)# ip igmp snooping querier 172.20.52.106`	Configures a snooping querier when you do not enable PIM because multicast traffic does not need to be routed. The IP address is used as the source in messages.
	ip igmp snooping report-suppression **Example:** `switch(config-vlan)# ip igmp snooping report-suppression`	Limits the membership report traffic sent to multicast-capable routers. When you disable report suppression, all IGMP reports are sent as is to multicast-capable routers. The default is enabled. **Note** This command can also be entered in global configuration mode to affect all interfaces.
	ip igmp snooping mrouter interface *interface* **Example:** `switch(config-vlan)# ip igmp snooping mrouter interface ethernet 2/1`	Configures a static connection to a multicast router. The interface to the router must be in the selected VLAN. You can specify the interface by the type and the number, such as **ethernet** *slot/port.* **Note** If this is a QSFP+ GEM, the *slot*/*port* syntax is *slot*/*QSFP-module*/*port*.
	ip igmp snooping static-group *group-ip-addr* [**source** *source*-ip-addr] **interface** *interface* **Example:** `switch(config-vlan)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1`	Configures a Layer 2 port of a VLAN as a static member of a multicast group. You can specify the interface by the type and the number, such as **ethernet** *slot/port.* **Note** If this is a QSFP+ GEM, the *slot*/*port* syntax is *slot*/*QSFP-module*/*port*.

	Command	Purpose
	ip igmp snooping link-local-groups-suppression **Example:** `switch(config-vlan)# ip igmp snooping link-local-groups-suppression`	Configures link-local groups suppression. The default is enabled. **Note** This command can also be entered in global configuration mode to affect all interfaces.
	ip igmp snooping v3-report-suppression **Example:** `switch(config-vlan)# ip igmp snooping v3-report-suppression`	Configures IGMPv3 report suppression and proxy reporting. The default is disabled for the global command for the entire switch and enabled per VLAN. **Note** This command can also be entered in global configuration mode to affect all interfaces.
	no ip igmp snooping mrouter vpc-peer-link **Example:** `switch(config)# no ip igmp snooping mrouter vpc-peer-link`	Sends multicast traffic over a vPC peer-link to each receiver VLAN that does not have orphan ports.
Step 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves configuration changes.

Verifying the IGMP Snooping Configuration

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

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

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x, 6x, 7x*.

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 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x, 6x, 7x.*

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
    no ip igmp snooping mrouter vpc-peer-link
```

Where to Go Next

You can enable the following features that work with PIM:

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

Additional References

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

- Related Documents, page 73
- Standards, page 73

Related Documents

Related Topic	Document Title
CLI commands	*Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x, 6x, 7x.*

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.	—