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:

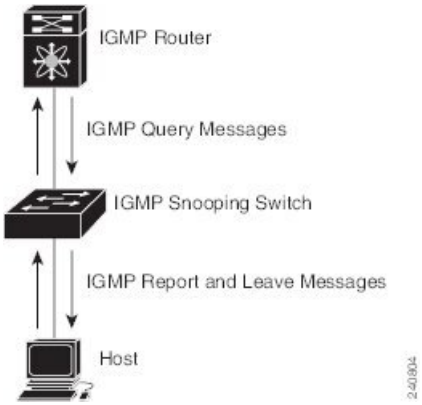
Information About IGMP Snooping

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.

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, 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.

Currently, you can configure the same SVI IP address for the switch querier and the IGMP snooping querier. Both queriers will then be active at the same time, and both queriers will send general queries to the VLAN periodically. To prevent this from happening, ensure that you use different IP addresses for the IGMP snooping querier and the switch querier.

IGMP Snooping Filter

Cisco NX-OS Release 6.0(2)A4(1) supports filtering of IGMP packets at the snooping layer. You can filter out IGMP snooping reports at the interface level. This filtering is based on a prefix-list or a route-map policy. The router compares a group to the prefix-list or route-map policy defined and performs the specified action. Thus, only groups that match the prefix-list or route-map that you specify will be filtered to the IGMP snooping reports.

Guidelines and Limitations for IGMP Snooping

IGMP snooping has the following guidelines and limitations:

- IGMP snooping is not supported with PVLAN.
- When IGMPv3 host on a VLAN leaves, it is possible that other hosts may experience traffic drop. This is seen mostly when a second consecutive leave is received from the port that already left and this impacts the other receivers on the VLAN.

To avoid this loss, you need to disable explicit host tracking under VLAN configuration using the **no ip igmp snooping explicit-tracking** command.

For example:

```
configure terminal
vlan configuration 10
no ip igmp snooping explicit-tracking
```

- In a hop-by-hop topology, the configuration of SVI on an intermediate box (second device) which is not an IGMP snooping querier causes traffic loss to hosts behind it when one of the other receivers ports behind another downstream L2 switch (third device) sends a leave. This is due to v3 suppression being disabled, IGMPv3 leave is consumed on second device. Workarounds for this issue is:
  - PIM DR and IGMP querier have to be co-located on the same box in the hop-by-hop topology. SVI in the first device should be configured with **ip pim dr-priority 10** to shift the DR from second device to the firstt device and the default suppression should be disabled on the second device, third device, and so on.
  - IGMPV3 suppression should be enabled under the VLAN configuration for the impacted VLAN on all the hops such as the second device and the third device.

For example:

```
configure terminal
vlan configuration 203
ip igmp snooping v3-report-suppression
```

Prerequisites for IGMP Snooping

IGMP snooping has the following prerequisites:

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

Default Settings 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

Parameters	Default
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

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

Table 2: IGMP Snooping Parameters

Parameter	Description
IGMP snooping	Enables IGMP snooping. 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 flooding (OMF) on all VLANs on the device. The default is enabled.
Proxy	Configures the IGMP snooping proxy for the device. The default is 5 seconds.

Parameter	Description
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. **configure terminal**
2.
3. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**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.	

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	
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 syslog-threshold percentage Example: `switch(config)# ip igmp snooping syslog-threshold 80`	Configures the syslog threshold of the IGMP snooping table.	
ip igmp snooping link-local-groups-suppression Example:	Configures link-local groups suppression for the entire device. The default is enabled.	

<table>
<tr><th></th><th colspan="2">Command or Action</th><th>Purpose</th></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><pre>switch(config)# ip igmp snooping link-local-groups-suppression</pre></td><td></td></tr>
<tr><td>ip igmp snooping optimise-multicast-flood
Example:<pre>switch(config)# ip igmp snooping optimise-multicast-flood</pre></td><td>Optimizes OMF on all VLANs on the device. The default is enabled.</td></tr>
<tr><td>ip igmp snooping v3-report-suppression
Example:<pre>switch(config)# ip igmp snooping v3-report-suppression</pre></td><td>Configures IGMPv3 report suppression and proxy reporting. The default is disabled for the global command for the entire switch and enabled per VLAN.</td></tr>
<tr><td>ip igmp snooping report-suppression
Example:<pre>switch(config)# ip igmp snooping report-suppression</pre></td><td>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.</td></tr>
</table></td><td></td></tr>
<tr><td>Step 3</td><td colspan="2">(Optional) copy running-config startup-config
Example:<pre>switch(config)# copy running-config startup-config</pre></td><td>Saves configuration changes.</td></tr>
</table>

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 3: IGMP Snooping Parameters

Parameter	Description
IGMP snooping	Enables IGMP snooping on a per-VLAN basis. The default is enabled. If the global setting is disabled, all VLANs are treated as disabled, whether they are enabled or not.
Access group	Filters IGMP packets at the snooping layer. The default is disabled.
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.
Optimise-multicast-flood	Configures optimized multicast flooding (OMF) on specified VLANs. The default is enabled.
Report policy	Filters IGMP packets at the snooping layer. The default is disabled.
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.

Parameter	Description
Robustness variable	Configures the robustness value for the specified VLANs.
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.
Version	Configures the IGMP version number for the specified VLANs.

Note You configure the IGMP snooping parameters that you want by using this configuration mode; however, the configurations apply only after you specifically create the specified VLAN.

SUMMARY STEPS

1. **configure terminal**
2. **ip igmp snooping**
3. **vlan configuration** *vlan-id*
4.
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	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.

	Command or Action	Purpose

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 {prefix-list | route-map} policy-name interface *interface slot/port* Example: `switch(config-vlan-config)# ip igmp snooping access-group prefix-list plist interface ethernet 2/2`	Configures a filter for IGMP snooping access groups based on a prefix-list or route-map policy.
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 last-member-query-interval *seconds* Example:	Removes the group from the associated VLAN port if no hosts respond to an IGMP query

Command or Action		Purpose
Option	**Description**	
`switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3`	message before the last member query interval expires. Values range from 1 to 25 seconds. The default is 1 second.	
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 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 optimise-multicast-flood Example: `switch(config-vlan-config)# ip igmp snooping optimise-multicast-flood`	Optimizes OMF on selected VLANs. The default is enabled.	
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:	Configures a snooping querier timeout value for IGMPv2 when you do not enable PIM because multicast traffic does not	

Command or Action		Purpose
Option	**Description**	
`switch(config-vlan-config)# ip igmp snooping querier-timeout 300`	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.	
ip igmp snooping report-policy { **prefix-list** | **route-map** } **policy-name interface** *interface slot/port* Example: `switch(config-vlan-config)# ip igmp snooping report-policy route-map rmap interface ethernet 2/4`	Configures a filter for IGMP snooping reports based on a prefix-list or route-map policy.	
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 static-group *group-ip-addr* [**source source -ip-addr**] **interface** *interface* Example:	Configures a Layer 2 port of a VLAN as a static member of a multicast group. You can specify the interface by	

	Command or Action		Purpose
	Option	**Description**	
	`switch(config-vlan-config)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1`	the type and the number, such as **ethernet** *slot/port*.	
	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	(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 look-up mode [**vlan** *vlan-id*]	Displays IGMP snooping lookup mode information by VLAN.
show ip igmp snooping mac-oif [**detail** | **vlan** *vlan-id*]	Displays IGMP snooping static mac oif information by VLAN and by all details
show ip igmp snooping mroute [**vlan** *vlan-id*]	Displays multicast router ports by VLAN.
show ip igmp snooping otv groups [*source* [*group*] | *group* [*source*]] [**vlan** *vlan-id*]	Displays IGMP snooping OTV information by VLAN.
show ip igmp snooping querier [**vlan** *vlan-id*]	Displays IGMP snooping queriers by VLAN.
show ip igmp snooping [**vlan** *vlan-id*]	Displays IGMP snooping configuration by VLAN.

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

Displaying IGMP Snooping Statistics

Command	Purpose
show ip igmp snooping statistics [**global** | **vlan** *vlan-id*]	Displays global or per VLAN packet and error counter statistics.

Clearing IGMP Snooping Statistics

You can clear the IGMP snooping statistics using these commands.

Command	Purpose
clear ip igmp snooping statistics vlan	Clears the IGMP snooping statistics.

Configuration Examples for IGMP Snooping

This example shows how to configure the IGMP snooping parameters:

```
configure terminal
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 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
```

The following example shows how to configure prefix lists and use them to filter IGMP snooping reports:

```
ip prefix-list plist seq 5 permit 224.1.1.1/32
ip prefix-list plist seq 10 permit 224.1.1.2/32
ip prefix-list plist seq 15 deny 224.1.1.3/32
ip prefix-list plist seq 20 deny 225.0.0.0/8 eq 32

vlan configuration 2
ip igmp snooping report-policy prefix-list plist interface Ethernet 2/2
ip igmp snooping report-policy prefix-list plist interface Ethernet 2/3
```

In the above example, the prefix-list permits 224.1.1.1 and 224.1.1.2 but rejects 224.1.1.3 and all the groups in the 225.0.0.0/8 range. The prefix-list is an implicit "deny" if there is no match. If you wish to permit everything else, add ip prefix-list plist seq 30 permit 224.0.0.0/4 eq 32.

The following example shows how to configure route maps and use them to filter IGMP snooping reports:

```
route-map rmap permit 10
match ip multicast group 224.1.1.1/32
route-map rmap permit 20
match ip multicast group 224.1.1.2/32
route-map rmap deny 30
match ip multicast group 224.1.1.3/32
```

```
route-map rmap deny 40
match ip multicast group 225.0.0.0/8

vlan configuration 2
ip igmp snooping report-policy route-map rmap interface Ethernet 2/4
ip igmp snooping report-policy route-map rmap interface Ethernet 2/5
```

In the above example, the route-map permits 224.1.1.1 and 224.1.1.2 but rejects 224.1.1.3 and all the groups in the 225.0.0.0/8 range. The route-map is an implicit "deny" if there is no match. If you wish to permit everything else, add route-map rmap permit 50 match ip multicast group 224.0.0.0/4.

Additional References

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

- Standards
- Related Documents

Related Documents

Related Topic	Document Title
CLI commands	Cisco Nexus 3548 Switch 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.	-