CHAPTER 5

# Configuring IGMP Snooping

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping.

This chapter includes the following topics:


- Information about IGMP Snooping, page 5-1
- Prerequisites for IGMP Snooping, page 5-3
- Default Settings, page 5-3
- Configuring IGMP Snooping, page 5-4
- Verifying the IGMP Snooping Configuration, page 5-6
- Example Configuration for IGMP Snooping, page 5-7
- Additional References, page 5-7
- Feature History for IGMP Snooping, page 5-8


# Information about IGMP Snooping

This section includes the following topics:

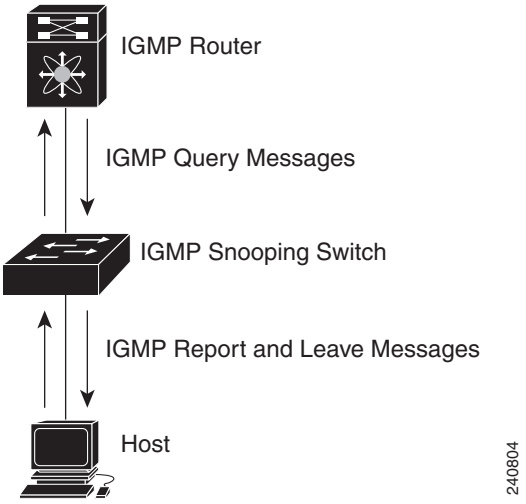

- IGMP Snooping, page 5-1
- IGMPv1 and IGMPv2, page 5-2
- IGMPv3, page 5-3
- IGMP Snooping Query Feature, page 5-3


## IGMP Snooping

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 device.

Figure 5-1 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 5-1 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.

The Cisco Nexus 1000V IGMP snooping implementation 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.

# IGMPv1 and IGMPv2

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 time-out to indicate that no hosts remain that want to receive multicast data for a particular group.

Report suppression is not supported and is disabled by default.

**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 Nexus 1000V 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 queries.

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 time-out, the software removes the group state.

## IGMP Snooping Query Feature

When the multicast traffic does not need to be routed, you must configure an external switch to query membership. On the external switch, define the query feature in a VLAN that contains multicast sources and receivers but no other active query feature.

When an IGMP snooping query feature is enabled, it sends out periodic IGMP queries that trigger IGMP report messages from hosts wanting to receive IP multicast traffic. IGMP snooping listens to these IGMP reports to identify accurate forwarding.

# Prerequisites for IGMP Snooping

IGMP snooping has the following prerequisites:

- You are logged in to the switch.
- A querier must be running on the uplink switches on the VLANs that contain multicast sources and receivers.

# Default Settings

Table 5-1 lists the default settings for IGMP snooping parameters.

*Table 5-1 Default IGMP Snooping Parameters*

| Parameters | Default |
|---|---|
| IGMP snooping | Enabled |
| IGMPv3 Explicit tracking | Enabled |
| IGMPv2 Fast leave | Disabled |
| Last member query interval | 1 second |

*Table 5-1 Default IGMP Snooping Parameters (continued)*

| Parameters | Default |
|---|---|
| Snooping querier | Disabled |
| IGMPv1/v2 Report suppression | Disabled |
| IGMPv3 Report suppression | Disabled |

# Configuring IGMP Snooping

Use this procedure to configure IGMP snooping.

## BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.

**Note** Be aware that the NX-OS commands may differ from those used in Cisco IOS.

- Table 5-2 lists and describes the configurable IGMP snooping parameters.

*Table 5-2 IGMP Snooping Parameters*

| Parameter | Description |
|---|---|
| IGMP snooping | Enables IGMP snooping globally or on a per-VLAN basis. The default is enabled.<br>**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 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. |
| 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 disabled. |
| 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. |

**Note** Be aware that the NX-OS commands may differ from those used in Cisco IOS.

## SUMMARY STEPS

1. **config t**
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 mrouter interface** *interface*

   **ip igmp snooping static-group** *group-ip-addr* **interface** *interface*
5. **copy running-config startup-config**

## DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **config t**<br><br>**Example:**<br>`n1000v# config t`<br>`n1000v(config)#` | Enters global configuration mode. |
| **Step 2** | **ip igmp snooping**<br><br>**Example:**<br>`n1000v(config)# ip igmp snooping`<br>`n1000v(config)#` | Enables IGMP snooping in the running configuration. The default is enabled.<br>**Note** If disabled, then IGMP snooping on all VLANs is disabled, whether IGMP snooping is enabled on a VLAN or not. |
| **Step 3** | **vlan** *vlan-id*<br><br>**Example:**<br>`n1000v(config)# vlan 2`<br>`n1000v(config-vlan)#` | Enters global configuration mode for the specified VLAN. |
| **Step 4** | **ip igmp snooping**<br><br>**Example:**<br>`n1000v(config-vlan)# ip igmp snooping` | Enables IGMP snooping for the specific VLAN in the running configuration.<br>The default is enabled. |
| | **ip igmp snooping explicit-tracking**<br><br>**Example:**<br>`n1000v(config-vlan)# ip igmp snooping explicit-tracking`<br>`n1000v(config-vlan)#` | Tracks IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis in the running configuraiton.<br>The default is enabled on all VLANs. |

| | Command | Purpose |
|---|---|---|
| | **ip igmp snooping fast-leave**<br><br>**Example:**<br>n1000v(config-vlan)# ip igmp snooping fast-leave<br>n1000v(config-vlan)# | Enables fast-leave for the specified VLAN in the running configuration.<br><br>Fast-leave supports IGMPv2 hosts that cannot be explicitly tracked because of the host report suppression mechanism of the IGMPv2 protocol.<br><br>When you enable fast leave, the IGMP software assumes that no more than one host is present on each VLAN port.<br><br>The default is disabled for all VLANs. |
| | ip igmp snooping last-member-query-interval *seconds*<br><br>Example:<br>n1000v(config-vlan)# ip igmp snooping last-member-query-interval 3<br>n1000v(config-vlan)# | Establishes a time interval in seconds after which the group is removed from the associated VLAN port if no hosts respond to an IGMP query message. This interval is saved in the running configuration<br><br>Allowable intervals are from 1 (default) to 25 seconds. |
| | **ip igmp snooping mrouter interface** *interface*<br><br>**Example:**<br>n1000v(config-vlan)# ip igmp snooping mrouter interface ethernet 2/1<br>n1000v(config-vlan)# | Configures a static connection to a multicast router in the running configuraiton.<br><br>The interface to the router must be in the specified 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* **interface** *interface*<br><br>**Example:**<br>n1000v(config-vlan)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1<br>n1000v(config-vlan)# | Configures a Layer 2 port of a VLAN as a static member of a multicast group in the running configuration.<br><br>You can specify the interface by the type and the number, such as **ethernet** *slot/port*. |
| **Step 5** | **copy running-config startup-config**<br><br>**Example:**<br>n1000v# copy running-config startup-config | (Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration. |

# Verifying the IGMP Snooping Configuration

Use the following commands to display the IGMP snooping configuration information.

| Command | Purpose |
|---|---|
| **show ip igmp snooping** [**vlan** *vlan-id*] | Displays IGMP snooping configuration by VLAN. |
| **show ip igmp snooping groups** [**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. |

| Command | Purpose |
|---|---|
| **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 commands and their output, see the *Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)*.

# Example Configuration for IGMP Snooping

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

```
n1000v# config t
n1000v(config)# ip igmp snooping
n1000v(config)# vlan 2
n1000v(config-vlan)# ip igmp snooping
n1000v(config-vlan)# ip igmp snooping explicit-tracking
n1000v(config-vlan)# ip igmp snooping mrouter interface ethernet 2/1
n1000v(config-vlan)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1
n1000v(config-vlan)# copy run start
[########################################] 100%
n1000v(config-vlan)# exit
n1000v(config)# exit
n1000v#
```

# Additional References

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


- Related Documents, page 5-7
- Standards, page 5-8


## Related Documents

| Related Topic | Document Title |
|---|---|
| Port Profiles | *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)* |
| Interfaces | *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)* |
| Complete command syntax, command modes, command history, defaults, usage guidelines, and examples | *Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)* |

## 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

This section provides the release history for the IGMP snooping feature.

*Table 5-3*

| Feature Name | Releases | Feature Information |
|---|---|---|
| IGMP Snooping | 4.0(4)SV1(1) | This feature was introduced. |
| Report suppression | 4.0(4)SV1(3) | Removed support for report suppression. |