



CHAPTER 4

Configuring IGMP Snooping

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

This chapter includes the following sections:

- [Information About IGMP Snooping, page 4-1](#)
- [Licensing Requirements for IGMP Snooping, page 4-4](#)
- [Prerequisites for IGMP Snooping, page 4-4](#)
- [Configuring IGMP Snooping Parameters, page 4-4](#)
- [Verifying IGMP Snooping Configuration, page 4-7](#)
- [IGMP Snooping Configuration Example, page 4-7](#)
- [Where to Go Next, page 4-8](#)
- [Default Settings, page 4-8](#)
- [Additional References, page 4-8](#)

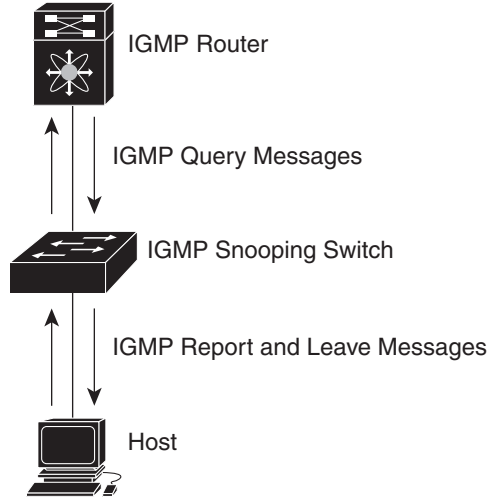
Information About IGMP Snooping

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 4-1](#) 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.

Send document comments to nexus7k-docfeedback@cisco.com

Figure 4-1 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 2, “Configuring IGMP and MLD.”](#)

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, page 4-2](#)
- [IGMPv3, page 4-3](#)
- [IGMP Snooping Querier, page 4-3](#)
- [IGMP Snooping with VDCs and VRFs, page 4-3](#)

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.

Send document comments to nexus7k-docfeedback@cisco.com



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.

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 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. For information about IGMP snooping, see [Chapter 4, “Configuring IGMP Snooping.”](#)

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, Release 4.0*.

For information about configuring VRFs, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0*.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Licensing Requirements for IGMP Snooping

The following table shows the licensing requirements for this feature:

| Product | License Requirement |
|---------|---|
| 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 NX-OS licensing scheme, see the <i>Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0</i> . |

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.

Configuring IGMP Snooping Parameters

To affect the operation of the IGMP snooping process, you can configure the optional IGMP snooping parameters described in [Table 4-1](#).

Table 4-1 IGMP Snooping Parameters

| Parameter | Description |
|----------------------------|---|
| IGMP snooping | Enables IGMP snooping on the active VDC or on a per-VLAN basis. The default is disabled. 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. |

Send document comments to nexus7k-docfeedback@cisco.com

Table 4-1 IGMP Snooping Parameters (continued)

| Parameter | Description |
|--------------------|--|
| Snooping querier | Configures a snooping querier on an interface when you do not enable PIM because multicast traffic does not need to be routed. The default is disabled. |
| 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. |
| 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

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.

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 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*
5. **copy running-config startup-config**

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

| | Command | Purpose |
|--------|--|--|
| Step 1 | <pre>config t</pre> <p>Example: switch# config t switch(config)#</p> | Enters configuration mode. |
| Step 2 | <pre>ip igmp snooping</pre> <p>Example: switch(config)# ip igmp snooping</p> | <p>Enables IGMP snooping for the current VDC. The default is enabled.</p> <p>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.</p> |
| Step 3 | <pre>vlan vlan-id</pre> <p>Example: switch(config)# vlan 2 switch(config-vlan)#</p> | Enters VLAN configuration mode. |
| Step 4 | <pre>ip igmp snooping</pre> <p>Example: switch(config-vlan)# ip igmp snooping</p> | Enables IGMP snooping for the current VLAN. The default is disabled. |
| | <pre>ip igmp snooping explicit-tracking</pre> <p>Example: switch(config-vlan)# ip igmp snooping explicit-tracking</p> | Tracks IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis. The default is enabled on all VLANs. |
| | <pre>ip igmp snooping fast-leave</pre> <p>Example: switch(config-vlan)# ip igmp snooping fast-leave</p> | 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. |
| | <pre>ip igmp snooping last-member-query-interval seconds</pre> <p>Example: switch(config-vlan)# ip igmp snooping last-member-query-interval 3</p> | 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. |
| | <pre>ip igmp snooping querier ip-address</pre> <p>Example: switch(config-vlan)# ip igmp snooping querier 172.20.52.106</p> | 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. The default is disabled. |
| | <pre>ip igmp snooping report-suppression</pre> <p>Example: switch(config-vlan)# ip igmp snooping report-suppression</p> | <p>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.</p> <p>Note This command can also be entered in global configuration mode to affect all interfaces.</p> |

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

| Command | Purpose |
|--|---|
| ip igmp snooping mrouter interface <i>interface</i> 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 . |
| ip igmp snooping static-group <i>group-ip-addr [source source-ip-addr]</i> 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 . |
| Step 5 copy running-config startup-config Example: switch(config)# copy running-config startup-config | (Optional) Saves configuration changes. |

Verifying 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 [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 7000 Series NX-OS Multicast Routing Command Reference, Release 4.0*.

IGMP Snooping Configuration Example

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

```

config t
 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

```

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

```
ip igmp snooping mrouter interface ethernet 2/1
ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1
```

Where to Go Next

You can enable the following features that work with PIM:

- [Chapter 2, “Configuring IGMP and MLD”](#)
- [Chapter 5, “Configuring MSDP”](#)

Default Settings

[Table 4-2](#) lists the default settings for IGMP snooping parameters.

Table 4-2 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 |

Additional References

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

- [Related Documents, page 4-8](#)
- [Standards, page 4-9](#)
- [MIBs, page 4-9](#)
- [Appendix A, “IETF RFCs”](#)
- [Technical Assistance, page 4-9](#)

Related Documents

| Related Topic | Document Title |
|---------------|--|
| VDCs | <i>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.0</i> |
| CLI commands | <i>Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference, Release 4.0</i> |

Send document comments to nexus7k-docfeedback@cisco.com

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. | — |

MIBs

| MIBs | MIBs Link |
|---|--|
| <ul style="list-style-type: none">CISCO-IGMP-SNOOPING-MIB | To locate and download MIBs, go to the following URL: http://www.cisco.com/NX-OS/mibs |

Technical Assistance

| Description | Link |
|--|---|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | http://www.cisco.com/public/support/tac/home.shtml |

Send document comments to nexus7k-docfeedback@cisco.com