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, page 4-1
- Licensing Requirements for IGMP Snooping, page 4-4
- Prerequisites for IGMP Snooping, page 4-4
- Default Settings, page 4-4
- Configuring IGMP Snooping Parameters, page 4-5
- Verifying the IGMP Snooping Configuration, page 4-7
- Displaying IGMP Snooping Statistics, page 4-8
- Configuration Examples for IGMP Snooping, page 4-8
- Where to Go Next, page 4-8
- Additional References, page 4-8
- Feature History for IGMP Snooping, page 4-9

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 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.
Information About IGMP Snooping

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.”

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 Filtering on Router Ports, 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.
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 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.
Licensing Requirements for IGMP Snooping

The following table shows the licensing requirements for this feature:

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

Default Settings

Table 4-1 lists the default settings for IGMP snooping parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP snooping</td>
<td>Enabled</td>
</tr>
<tr>
<td>Explicit tracking</td>
<td>Enabled</td>
</tr>
<tr>
<td>Fast leave</td>
<td>Disabled</td>
</tr>
<tr>
<td>Last member query interval</td>
<td>1 second</td>
</tr>
<tr>
<td>Snooping querier</td>
<td>Disabled</td>
</tr>
<tr>
<td>Report suppression</td>
<td>Enabled</td>
</tr>
<tr>
<td>Link-local groups suppression</td>
<td>Enabled</td>
</tr>
<tr>
<td>IGMPv3 report suppression for the entire switch</td>
<td>Disabled</td>
</tr>
<tr>
<td>IGMPv3 report suppression per VLAN</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
Configuring IGMP Snooping Parameters

To affect the operation of the IGMP snooping process, you can configure the optional IGMP snooping parameters described in Table 4-2.

Table 4-2  IGMP Snooping Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP snooping</td>
<td>Enables IGMP snooping on the switch or on a per-VLAN basis. The default is enabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If the global setting is disabled, then all VLANs are treated as disabled, whether they are enabled or not.</td>
</tr>
<tr>
<td>Explicit tracking</td>
<td>Tracks IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis. The default is enabled.</td>
</tr>
<tr>
<td>Fast leave</td>
<td>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.</td>
</tr>
<tr>
<td>Last member query interval</td>
<td>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.</td>
</tr>
<tr>
<td>Snooping querier</td>
<td>Configures a snooping querier on an interface when you do not enable PIM because multicast traffic does not need to be routed.</td>
</tr>
<tr>
<td>Report suppression</td>
<td>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.</td>
</tr>
<tr>
<td>Multicast router</td>
<td>Configures a static connection to a multicast router. The interface to the router must be in the selected VLAN.</td>
</tr>
<tr>
<td>Static group</td>
<td>Configures a Layer 2 port of a VLAN as a static member of a multicast group.</td>
</tr>
<tr>
<td>Link-local groups suppression</td>
<td>Configures link-local groups suppression on the switch or on a per-VLAN basis. The default is enabled.</td>
</tr>
<tr>
<td>IGMPv3 report suppression</td>
<td>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.</td>
</tr>
</tbody>
</table>

SUMMARY STEPS

1. configure terminal
2. ip igmp snooping
3. vlan vlan-id
## Configuring IGMP Snooping Parameters

Send document comments to nexus3k-docfeedback@cisco.com

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*  
   *(Optional) copy running-config startup-config*

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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. |
| **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. |
Chapter 4 Configuring IGMP Snooping

Verifying the IGMP Snooping Configuration

Send document comments to nexus3k-docfeedback@cisco.com

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip igmp snooping querier ip-address</td>
<td>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.</td>
</tr>
<tr>
<td>Example: switch(config-vlan)# ip igmp snooping querier 172.20.52.106</td>
<td></td>
</tr>
<tr>
<td>ip igmp snooping report-suppression</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>
<tr>
<td>Example: switch(config-vlan)# ip igmp snooping report-suppression</td>
<td></td>
</tr>
<tr>
<td>ip igmp snooping mrouter interface interface</td>
<td>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.</td>
</tr>
<tr>
<td>Example: switch(config-vlan)# ip igmp snooping mrouter interface ethernet 2/1</td>
<td></td>
</tr>
<tr>
<td>ip igmp snooping static-group group-ip-addr [source source-ip-addr] interface interface</td>
<td>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.</td>
</tr>
<tr>
<td>Example: switch(config-vlan)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1</td>
<td></td>
</tr>
<tr>
<td>ip igmp snooping link-local-groups-suppression</td>
<td>Configures link-local groups suppression. The default is enabled.</td>
</tr>
<tr>
<td>Example: switch(config-vlan)# ip igmp snooping link-local-groups-suppression</td>
<td></td>
</tr>
<tr>
<td>ip igmp snooping v3-report-suppression</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>Example: switch(config-vlan)# ip igmp snooping v3-report-suppression</td>
<td></td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Saves configuration changes.</td>
</tr>
<tr>
<td>Example: switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Verifying the IGMP Snooping Configuration

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip igmp snooping [vlan vlan-id]</td>
<td>Displays IGMP snooping configuration by VLAN.</td>
</tr>
<tr>
<td>show ip igmp snooping groups [source [group]</td>
<td>Displays IGMP snooping information about groups by VLAN.</td>
</tr>
<tr>
<td>group [source]] [vlan vlan-id] [detail]</td>
<td></td>
</tr>
</tbody>
</table>
Displaying IGMP Snooping Statistics

Use the `show ip igmp snooping statistics vlan` command to display IGMP snooping statistics.
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 3000 Series Command Reference.

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
```

Where to Go Next

You can enable the following features that work with PIM:

- Chapter 2, “Configuring IGMP”
- Chapter 5, “Configuring MSDP”

Additional References

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

- Related Documents, page 4-9
Feature History for IGMP Snooping

Table 4-3 lists the release history for this feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Snooping</td>
<td>5.0(3)U1(1)</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>