



Configuring IGMP

This chapter describes how to configure the Internet Group Management Protocol (IGMP) on Cisco NX-OS switches for IPv4 networks.

This chapter includes the following sections:

- [Information About IGMP, page 11](#)
- [Licensing Requirements for IGMP, page 14](#)
- [Default Settings for IGMP, page 14](#)
- [Configuring IGMP Parameters, page 15](#)
- [Verifying the IGMP Configuration, page 23](#)
- [Configuration Examples for IGMP, page 24](#)
- [Where to Go Next, page 24](#)

Information About IGMP

IGMP is an IPv4 protocol that a host uses to request multicast data for a particular group. Using the information obtained through IGMP, the software maintains a list of multicast group or channel memberships on a per-interface basis. The systems that receive these IGMP packets send multicast data that they receive for requested groups or channels out the network segment of the known receivers.

By default, the IGMP process is running. You cannot enable IGMP manually on an interface. IGMP is automatically enabled when you perform one of the following configuration tasks on an interface:

- Enable PIM
- Statically bind a local multicast group
- Enable link-local group reports

This section includes the following topics:

- [IGMP Versions, page 11](#)
- [IGMP Basics, page 12](#)
- [Virtualization Support, page 14](#)

IGMP Versions

The switch supports IGMPv2 and IGMPv3, as well as IGMPv1 report reception.

By default, the software enables IGMPv2 when it starts the IGMP process. You can enable IGMPv3 on interfaces where you want its capabilities.

IGMPv3 includes the following key changes from IGMPv2:

- Support for Source-Specific Multicast (SSM), which builds shortest path trees from each receiver to the source, through the following features:
 - Host messages that can specify both the group and the source.
 - The multicast state that is maintained for groups and sources, not just for groups as in IGMPv2.
- Hosts no longer perform report suppression, which means that hosts always send IGMP membership reports when an IGMP query message is received.

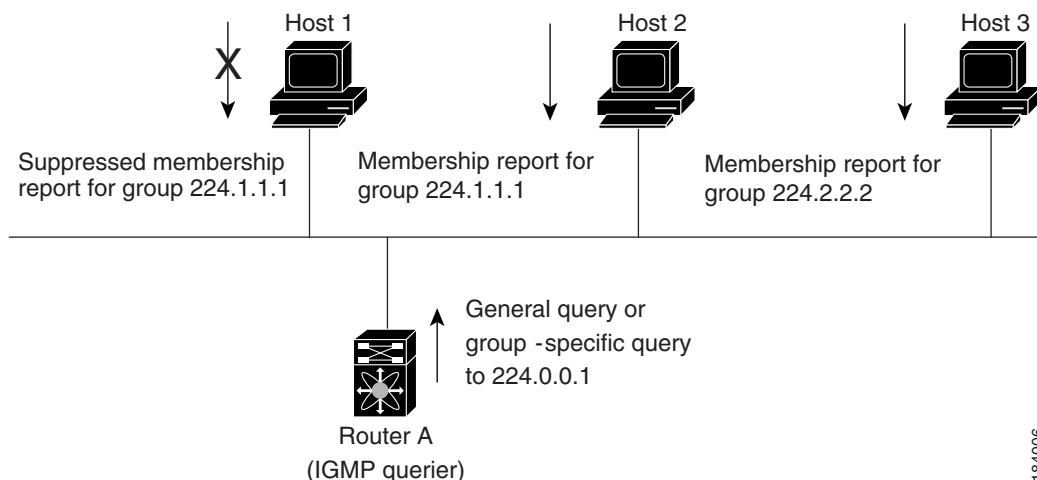
For detailed information about IGMPv2, see [RFC 2236](#).

For detailed information about IGMPv3, see [RFC 3376](#).

IGMP Basics

The basic IGMP process of a router that discovers multicast hosts is shown in [Figure 2-1](#). Hosts 1, 2, and 3 send unsolicited IGMP membership report messages to initiate receiving multicast data for a group or channel.

Figure 2-1 IGMPv1 and IGMPv2 Query-Response Process



184006

In [Figure 2-1](#), router A, which is the IGMP designated querier on the subnet, sends query messages to the all-hosts multicast group at 224.0.0.1 periodically to discover whether any hosts want to receive multicast data. You can configure the group membership timeout value that the router uses to determine that no members of a group or source exist on the subnet. For more information about configuring the IGMP parameters, see the “[Configuring IGMP Interface Parameters](#)” section on page 2-15.

The software elects a router as the IGMP querier on a subnet if it has the lowest IP address. As long as a router continues to receive query messages from a router with a lower IP address, it resets a timer that is based on its querier timeout value. If the querier timer of a router expires, it becomes the designated querier. If that router later receives a host query message from a router with a lower IP address, it drops its role as the designated querier and sets its querier timer again.

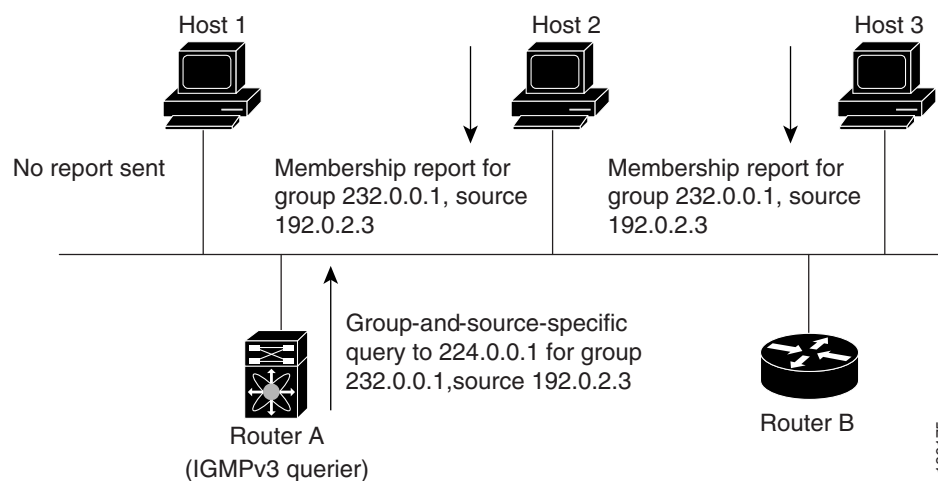
In [Figure 2-1](#), host 1's membership report is suppressed and host 2 sends its membership report for group 224.1.1.1 first. Host 1 receives the report from host 2. Because only one membership report per group needs to be sent to the router, other hosts suppress their reports to reduce network traffic. Each host waits for a random time interval to avoid sending reports at the same time. You can configure the query maximum response time parameter to control the interval in which hosts randomize their responses.

**Note**

IGMPv1 and IGMPv2 membership report suppression occurs only on hosts that are connected to the same port.

In [Figure 2-2](#), router A sends the IGMPv3 group-and-source-specific query to the LAN. Hosts 2 and 3 respond to the query with membership reports that indicate that they want to receive data from the advertised group and source. This IGMPv3 feature supports SSM. For information about configuring SSM translation to support SSM for IGMPv1 and IGMPv2 hosts, see the [“Configuring an IGMP SSM Translation”](#) section on page 2-21.

Figure 2-2 IGMPv3 Group-and-Source-Specific Query

**Note**

IGMPv3 hosts do not perform IGMP membership report suppression.

Messages sent by the designated querier have a time-to-live (TTL) value of 1, which means that the messages are not forwarded by the directly connected routers on the subnet. You can configure the frequency and number of query messages sent specifically for IGMP startup, and you can configure a short query interval at startup so that the group state is established as quickly as possible. Although usually unnecessary, you can tune the query interval used after startup to a value that balances the responsiveness to host group membership messages and the traffic created on the network.

**Caution**

Changing the query interval can severely impact multicast forwarding.

When a multicast host leaves a group, a host that runs IGMPv2 or later sends an IGMP leave message. To check if this host is the last host to leave the group, the software sends an IGMP query message and starts a timer that you can configure called the last member query response interval. If no reports are received before the timer expires, the software removes the group state. The router continues to send multicast traffic for a group until its state is removed.

You can configure a robustness value to compensate for packet loss on a congested network. The robustness value is used by the IGMP software to determine the number of times to send messages.

Link local addresses in the range 224.0.0.0/24 are reserved by the Internet Assigned Numbers Authority (IANA). Network protocols on a local network segment use these addresses; routers do not forward these addresses because they have a TTL of 1. By default, the IGMP process sends membership reports only for nonlink local addresses, but you can configure the software to send reports for link local addresses.

For more information about configuring the IGMP parameters, see the [“Configuring IGMP Interface Parameters” section on page 2-15](#).

Virtualization Support

Cisco NX-OS supports virtual routing and forwarding (VRF). You can define multiple VRF instances. A VRF configured with IGMP supports the following IGMP features:

- IGMP is enabled or disabled on per interface
- IGMPv1, IGMPv2, and IGMPv3 provide router-side support
- IGMPv2 and IGMPv3 provide host-side support
- Supports configuration of IGMP querier parameters
- IGMP reporting is supported for link local multicast groups
- IGMP SSM-translation supports mapping of IGMPv2 groups to a set of sources
- Supports multicast trace-route (Mtrace) server functionality to process Mtrace requests

For information about configuring VRFs, see the *Cisco Nexus 5500 Series NX-OS Unicast Routing Configuration Guide, Release 6.0*.

Licensing Requirements for IGMP

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	IGMP 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 <i>Cisco NX-OS Licensing Guide</i> .
	Note Make sure the LAN Base Services license is installed on the switch to enable the Layer 3 interfaces.

Default Settings for IGMP

Table 2-1 lists the default settings for IGMP parameters.

Table 2-1 Default IGMP Parameters

Parameters	Default
IGMP version	2
Startup query interval	30 seconds

Table 2-1 *Default IGMP Parameters (continued)*

Parameters	Default
Startup query count	2
Robustness value	2
Querier timeout	255 seconds
Query timeout	255 seconds
Query max response time	10 seconds
Query interval	125 seconds
Last member query response interval	1 second
Last member query count	2
Group membership timeout	260 seconds
Report link local multicast groups	Disabled
Enforce router alert	Disabled
Immediate leave	Disabled

Configuring IGMP Parameters

You can configure the IGMP global and interface parameters to affect the operation of the IGMP process.

This section includes the following topics:

- [Configuring IGMP Interface Parameters, page 15](#)
- [Configuring an IGMP SSM Translation, page 21](#)
- [Configuring the Enforce Router Alert Option Check, page 22](#)



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.


Configuring IGMP Interface Parameters

You can configure the optional IGMP interface parameters described in [Table 2-2](#).

Table 2-2 IGMP Interface Parameters

Parameter	Description
IGMP version	IGMP version that is enabled on the interface. The IGMP version can be 2 or 3. The default is 2.
Static multicast groups	<p>Multicast groups that are statically bound to the interface. You can configure the groups to join the interface with the (*, G) state or specify a source IP to join with the (S, G) state. You can specify a route-map policy name that lists the group prefixes, group ranges, and source prefixes to use with the match ip multicast command.</p> <p>Note Although you can configure the (S, G) state, the source tree is built only if you enable IGMPv3. For information about SSM translation, see the “Configuring an IGMP SSM Translation” section on page 2-21.</p> <p>You can configure a multicast group on all the multicast-capable routers on the network so that pinging the group causes all the routers to respond.</p>
Static multicast groups on OIF	<p>Multicast groups that are statically bound to the output interface. You can configure the groups to join the output interface with the (*, G) state or specify a source IP to join with the (S, G) state. You can specify a route-map policy name that lists the group prefixes, group ranges, and source prefixes to use with the match ip multicast command.</p> <p>Note Although you can configure the (S, G) state, the source tree is built only if you enable IGMPv3. For information about SSM translation, see the “Configuring an IGMP SSM Translation” section on page 2-21.</p> <p>Note When you configure static ip igmp join command on the interface, ensure that ip routing multicast software-replicate command is also configured.</p>
Startup query interval	Startup query interval. By default, this interval is shorter than the query interval so that the software can establish the group state as quickly as possible. Values range from 1 to 18,000 seconds. The default is 31 seconds.
Startup query count	Number of queries sent at startup that are separated by the startup query interval. Values range from 1 to 10. The default is 2.
Robustness value	Robustness variable that you can tune to reflect expected packet loss on a congested network. You can increase the robustness variable to increase the number of times that packets are resent. Values range from 1 to 7. The default is 2.
Querier timeout	Number of seconds that the software waits after the previous querier has stopped querying and before it takes over as the querier. Values range from 1 to 65,535 seconds. The default is 255 seconds.
Query max response time	Maximum response time advertised in IGMP queries. You can tune the burstiness of IGMP messages on the network by setting a larger value so that host responses are spread out over a longer time. This value must be less than the query interval. Values range from 1 to 25 seconds. The default is 10 seconds.

Table 2-2 IGMP Interface Parameters (continued)

Parameter	Description
Query interval	Frequency at which the software sends IGMP host query messages. You can tune the number of IGMP messages on the network by setting a larger value so that the software sends IGMP queries less often. Values range from 1 to 18,000 seconds. The default is 125 seconds.
Last member query response interval	Interval in which the software sends a response to an IGMP query after receiving a host leave message from the last known active host on the subnet. If no reports are received in the interval, the group state is deleted. You can use this value to tune how quickly the software stops transmitting on the subnet. The software can detect the loss of the last member of a group or source more quickly when the values are smaller. Values range from 1 to 25 seconds. The default is 1 second.
Last member query count	Number of times that the software sends an IGMP query, separated by the last member query response interval, in response to a host leave message from the last known active host on the subnet. Values range from 1 to 5. The default is 2.  Caution Setting this value to 1 means that a missed packet in either direction causes the software to remove the multicast state from the queried group or channel. The software may wait until the next query interval before the group is added again.
Group membership timeout	Group membership interval that must pass before the router decides that no members of a group or source exist on the network. Values range from 3 to 65,535 seconds. The default is 260 seconds.
Report link local multicast groups	Option that enables sending reports for groups in 224.0.0.0/24. Link local addresses are used only by protocols on the local network. Reports are always sent for nonlink local groups. The default is disabled.
Report policy	Access policy for IGMP reports that is based on a route-map policy ¹ .
Access groups	Option that configures a route-map policy ¹ to control the multicast groups that hosts on the subnet serviced by an interface can join.
Immediate leave	Option that minimizes the leave latency of IGMPv2 group memberships on a given IGMP interface because the switch does not send group-specific queries. When immediate leave is enabled, the switch removes the group entry from the multicast routing table immediately upon receiving a leave message for the group. The default is disabled. Note Use this command only when there is one receiver behind the interface for a given group.

1. To configure route-map policies, see the *Cisco Nexus 5500 Series NX-OS Unicast Routing Configuration Guide, Release 6.0*.

For information about configuring multicast route maps, see the “[Configuring Route Maps to Control RP Information Distribution](#)” section on page 3-50.


SUMMARY STEPS

1. configure terminal

2. **interface** *interface*
3. **no switchport**
4. **ip igmp version** *value*
ip igmp static-oif {*group* [*source source*] | **route-map** *policy-name*}
ip igmp static-oif {*group* [*source source*] | **route-map** *policy-name*}
ip igmp startup-query-interval *seconds*
ip igmp startup-query-count *count*
ip igmp robustness-variable *value*
ip igmp querier-timeout *seconds*
ip igmp query-timeout *seconds*
ip igmp query-max-response-time *seconds*
ip igmp query-interval *interval*
ip igmp last-member-query-response-time *seconds*
ip igmp last-member-query-count *count*
ip igmp group-timeout *seconds*
ip igmp report-link-local-groups
ip igmp report-policy *policy*
ip igmp access-group *policy*
ip igmp immediate-leave
5. (Optional) **show ip igmp interface** [*interface*] [*vrf vrf-name* | **all**] [**brief**]
6. (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	interface <i>interface</i> Example: switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface mode on the interface type and number, such as ethernet <i>slot/port</i> . Note If this is a QSFP+ GEM, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> .
Step 3	no switchport Example: switch(config-if)# no switchport switch(config-if)#	Configures the interface as a Layer 3 interface.
Step 4	ip igmp version <i>value</i> Example: switch(config-if)# ip igmp version 3	Sets the IGMP version to the value specified. Values can be 2 or 3. The default is 2. The no form of the command sets the version to 2.

	Command	Purpose
Step 5	<p>ip igmp static-oif {group [source source] route-map policy-name}</p> <p>Example: switch(config-if)# ip igmp static-oif 230.0.0.0</p>	<p>Statically binds a multicast group to the interface. If you specify only the group address, the (*, G) state is created. If you specify the source address, the (S, G) state is created. You can specify a route-map policy name that lists the group prefixes, group ranges, and source prefixes to use with the match ip multicast command.</p> <p>Note A source tree is built for the (S, G) state only if you enable IGMPv3.</p> <p> Caution The switch CPU must be able to handle the traffic generated by using this command.</p>
Step 6	<p>ip igmp static-oif {group [source source] route-map policy-name}</p> <p>Example: switch(config-if)# ip igmp static-oif 230.0.0.0</p>	<p>Statically binds a multicast group to the outgoing interface, which is handled by the switch hardware. If you specify only the group address, the (*, G) state is created. If you specify the source address, the (S, G) state is created. You can specify a route-map policy name that lists the group prefixes, group ranges, and source prefixes to use with the match ip multicast command.</p> <p>Note A source tree is built for the (S, G) state only if you enable IGMPv3.</p>
Step 7	<p>ip igmp startup-query-interval seconds</p> <p>Example: switch(config-if)# ip igmp startup-query-interval 25</p>	<p>Sets the query interval used when the software starts up. Values can range from 1 to 18,000 seconds. The default is 31 seconds.</p>
Step 8	<p>ip igmp startup-query-count count</p> <p>Example: switch(config-if)# ip igmp startup-query-count 3</p>	<p>Sets the query count used when the software starts up. Values can range from 1 to 10. The default is 2.</p>
Step 9	<p>ip igmp robustness-variable value</p> <p>Example: switch(config-if)# ip igmp robustness-variable 3</p>	<p>Sets the robustness variable. You can use a larger value for a lossy network. Values can range from 1 to 7. The default is 2.</p>
Step 10	<p>ip igmp querier-timeout seconds</p> <p>Example: switch(config-if)# ip igmp querier-timeout 300</p>	<p>Sets the querier timeout that the software uses when deciding to take over as the querier. Values can range from 1 to 65,535 seconds. The default is 255 seconds.</p>
Step 11	<p>ip igmp query-timeout seconds</p> <p>Example: switch(config-if)# ip igmp query-timeout 300</p>	<p>Sets the query timeout that the software uses when deciding to take over as the querier. Values can range from 1 to 65,535 seconds. The default is 255 seconds.</p> <p>Note This command has the same functionality as the ip igmp querier-timeout command.</p>

	Command	Purpose
Step 12	<pre>ip igmp query-max-response-time seconds</pre> <p>Example: <pre>switch(config-if)# ip igmp query-max-response-time 15</pre></p>	Sets the response time advertised in IGMP queries. Values can range from 1 to 25 seconds. The default is 10 seconds.
Step 13	<pre>ip igmp query-interval interval</pre> <p>Example: <pre>switch(config-if)# ip igmp query-interval 100</pre></p>	Sets the frequency at which the software sends IGMP host query messages. Values can range from 1 to 18,000 seconds. The default is 125 seconds.
Step 14	<pre>ip igmp last-member-query-response-time seconds</pre> <p>Example: <pre>switch(config-if)# ip igmp last-member-query-response-time 3</pre></p>	Sets the query interval waited after sending membership reports before the software deletes the group state. Values can range from 1 to 25 seconds. The default is 1 second.
Step 15	<pre>ip igmp last-member-query-count count</pre> <p>Example: <pre>switch(config-if)# ip igmp last-member-query-count 3</pre></p>	Sets the number of times that the software sends an IGMP query in response to a host leave message. Values can range from 1 to 5. The default is 2.
Step 16	<pre>ip igmp group-timeout seconds</pre> <p>Example: <pre>switch(config-if)# ip igmp group-timeout 300</pre></p>	Sets the group membership timeout for IGMPv2. Values can range from 3 to 65,535 seconds. The default is 260 seconds.
Step 17	<pre>ip igmp report-link-local-groups</pre> <p>Example: <pre>switch(config-if)# ip igmp report-link-local-groups</pre></p>	Enables sending reports for groups in 224.0.0.0/24. Reports are always sent for nonlink local groups. By default, reports are not sent for link local groups.
Step 18	<pre>ip igmp report-policy policy</pre> <p>Example: <pre>switch(config-if)# ip igmp report-policy my_report_policy</pre></p>	Configures a route-map policy to control the multicast groups that a PIM-enabled interface can join.
Step 19	<pre>ip igmp access-group policy</pre> <p>Example: <pre>switch(config-if)# ip igmp access-group my_access_policy</pre></p>	Configures a route-map policy to control the multicast groups that a PIM-enabled interface can join.
Step 20	<pre>ip igmp immediate-leave</pre> <p>Example: <pre>switch(config-if)# ip igmp immediate-leave</pre></p>	<p>Enables the switch to remove the group entry from the multicast routing table immediately upon receiving a leave message for the group. This command allows you to minimize the leave latency of IGMPv2 group memberships on a given IGMP interface because the switch does not send group-specific queries. The default is disabled.</p> <p>Note Use this command only when there is one receiver behind the interface for a given group.</p>

	Command	Purpose
Step 21	<pre>show ip igmp interface [interface] [vrf vrf-name all] [brief]</pre> <p>Example: switch(config)# show ip igmp interface</p>	(Optional) Displays IGMP information about the interface.
Step 22	<pre>copy running-config startup-config</pre> <p>Example: switch(config)# copy running-config startup-config</p>	(Optional) Saves configuration changes.

Configuring an IGMP SSM Translation

You can configure an SSM translation to provide SSM support when the router receives IGMPv1 or IGMPv2 membership reports. Only IGMPv3 provides the capability to specify group and source addresses in membership reports. By default, the group prefix range is 232.0.0.0/8. To modify the PIM SSM range, see the “[Configuring SSM](#)” section on page 3-48.

Table 2-3 lists the example SSM translations.

Table 2-3 Example SSM Translations

Group Prefix	Source Address
232.0.0.0/8	10.1.1.1
232.0.0.0/8	10.2.2.2
232.1.0.0/16	10.3.3.3
232.1.1.0/24	10.4.4.4

Table 2-4 shows the resulting MRIB routes that the IGMP process creates when it applies an SSM translation to the IGMP membership report. If more than one translation applies, the router creates the (S, G) state for each translation.

Table 2-4 Example Result of Applying SSM Translations

IGMPv2 Membership Report	Resulting MRIB Route
232.1.1.1	(10.4.4.4, 232.1.1.1)
232.2.2.2	(10.1.1.1, 232.2.2.2) (10.2.2.2, 232.2.2.2)



Note

This feature is similar to SSM mapping found in some Cisco IOS software.

SUMMARY STEPS

1. **configure terminal**
2. **ip igmp ssm-translate** *group-prefix source-addr*
3. (Optional) **show running-configuration igmp**

4. (Optional) `copy running-config startup-config`

DETAILED STEPS

	Command	Purpose
Step 1	<code>configure terminal</code> Example: switch# <code>configure terminal</code> switch(config)#	Enters configuration mode.
Step 2	<code>ip igmp ssm-translate group-prefix source-addr</code> Example: switch(config)# <code>ip igmp ssm-translate 232.0.0.0/8 10.1.1.1</code>	Configures the translation of IGMPv1 or IGMPv2 membership reports by the IGMP process to create the (S,G) state as if the router had received an IGMPv3 membership report.
Step 3	<code>show running-configuration igmp</code> Example: switch(config)# <code>show running-configuration igmp</code>	(Optional) Shows the running-configuration information, including <code>ssm-translate</code> command lines.
Step 4	<code>copy running-config startup-config</code> Example: switch(config)# <code>copy running-config startup-config</code>	(Optional) Saves configuration changes.

Configuring the Enforce Router Alert Option Check

You can configure the enforce router alert option check for IGMPv2 and IGMPv3 packets.

SUMMARY STEPS

1. `configure terminal`
2. `ip igmp enforce-router-alert`
`no ip igmp enforce-router-alert`
3. (Optional) `show running-configuration igmp`
4. (Optional) `copy running-config startup-config`

DETAILED STEPS

	Command	Purpose
Step 1	<code>configure terminal</code> Example: switch# <code>configure terminal</code> switch(config)#	Enters configuration mode.

	Command	Purpose
Step 2	ip igmp enforce-router-alert Example: switch(config)# ip igmp enforce-router-alert	Enables the enforce router alert option check for IGMPv2 and IGMPv3 packets. By default, the enforce router alert option check is enabled.
	no ip igmp enforce-router-alert Example: switch(config)# no ip igmp enforce-router-alert	Disables the enforce router alert option check for IGMPv2 and IGMPv3 packets. By default, the enforce router alert option check is enabled.
Step 3	show running-configuration igmp Example: switch(config)# show running-configuration igmp	(Optional) Shows the running-configuration information, including the enforce-router-alert command line.
Step 4	copy running-config startup-config Example: switch(config)# copy running-config startup-config	(Optional) Saves configuration changes.

Verifying the IGMP Configuration

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

Command	Purpose
show ip igmp interface [<i>interface</i>] [vrf <i>vrf-name</i> all] [brief]	Displays IGMP information about all interfaces or a selected interface, the default VRF, a selected VRF, or all VRFs. If IGMP is in vPC mode, displays vPC statistics.
show ip igmp groups [<i>group</i> <i>interface</i>] [vrf <i>vrf-name</i> all]	Displays the IGMP attached group membership for a group or interface, the default VRF, a selected VRF, or all VRFs.
show ip igmp route [<i>group</i> <i>interface</i>] [vrf <i>vrf-name</i> all]	Displays the IGMP attached group membership for a group or interface, the default VRF, a selected VRF, or all VRFs.
show ip igmp local-groups	Displays the IGMP local group membership.
show running-configuration igmp	Displays the IGMP running-configuration information.
show startup-configuration igmp	Displays the IGMP startup-configuration information.

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*.

Configuration Examples for IGMP

This example shows how to configure the IGMP parameters:

```
switch# configure terminal
switch(config)# ip igmp ssm-translate 232.0.0.0/8 10.1.1.1
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip igmp version 3
switch(config-if)# ip igmp static-oif 230.0.0.0
switch(config-if)# ip igmp startup-query-interval 25
switch(config-if)# ip igmp startup-query-count 3
switch(config-if)# ip igmp robustness-variable 3
switch(config-if)# ip igmp querier-timeout 300
switch(config-if)# ip igmp query-timeout 300
switch(config-if)# ip igmp query-max-response-time 15
switch(config-if)# ip igmp query-interval 100
switch(config-if)# ip igmp last-member-query-response-time 3
switch(config-if)# ip igmp last-member-query-count 3
switch(config-if)# ip igmp group-timeout 300
switch(config-if)# ip igmp report-link-local-groups
switch(config-if)# ip igmp report-policy my_report_policy
switch(config-if)# ip igmp access-group my_access_policy
```

This example shows how to configure a route map that accepts all multicast reports (joins):

```
switch(config)# route-map foo
switch(config-route-map)# exit
switch(config)# interface vlan 10
switch(config-if)# no switchport
switch(config-if)# ip pim sparse-mode
switch(config-if)# ip igmp report-policy foo
```

This example shows how to configure a route map that denies all multicast reports (joins):

```
switch(config)# route-map foo deny 10
switch(config-route-map)# exit
switch(config)# interface vlan 5
switch(config-if)# ip pim sparse-mode
switch(config-if)# ip igmp report-policy foo
```

Where to Go Next

You can enable the following features that work with PIM and IGMP:

- [Chapter 4, “Configuring IGMP Snooping”](#)
- [Chapter 5, “Configuring MSDP”](#)