Configuring IGMP

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

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

IGMP Versions

The device 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.

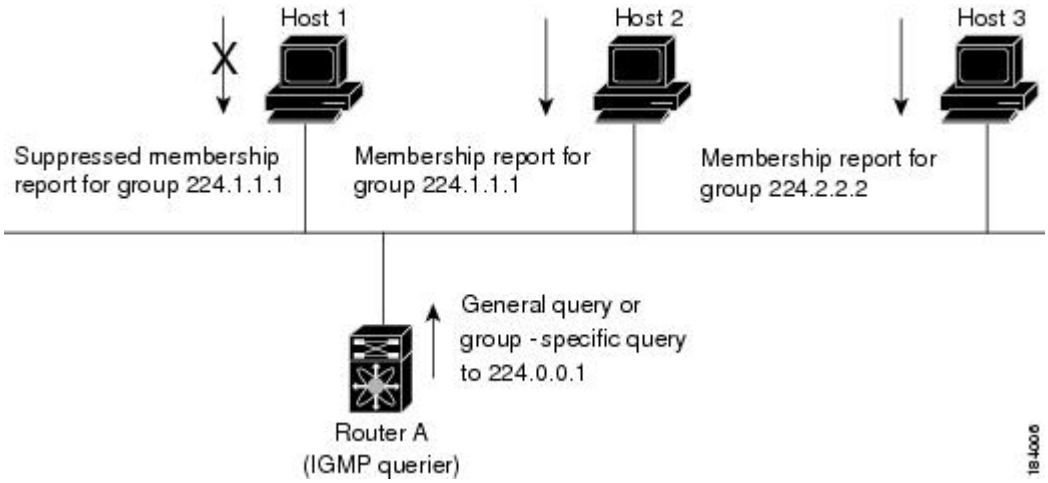
For detailed information about IGMPv2, see RFC 2236.

For detailed information about IGMPv3, see RFC 3376.

IGMP Basics

The basic IGMP process of a router that discovers multicast hosts is shown in the figure below. Hosts 1, 2, and 3 send unsolicited IGMP membership report messages to initiate receiving multicast data for a group or channel.

Figure 1: IGMPv1 and IGMPv2 Query-Response Process



In the figure below, 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 *Configuring IGMP Interface Parameters*.

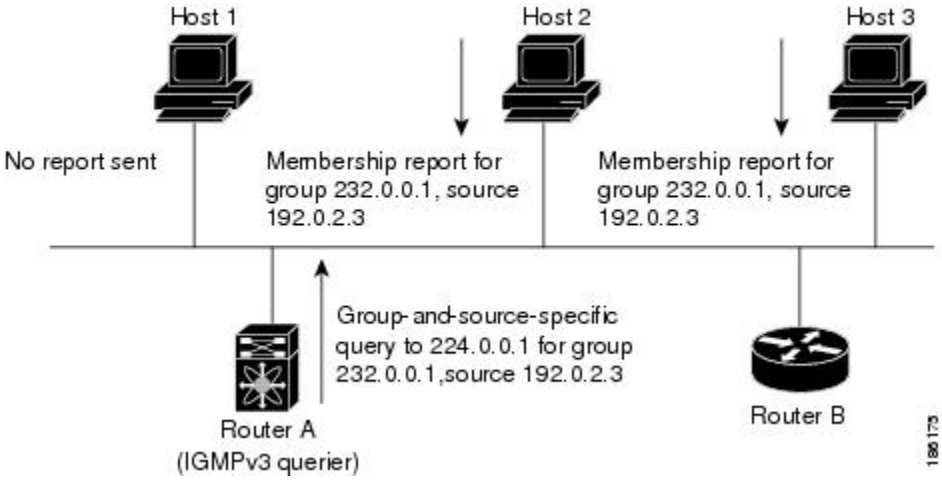
The software elects a router as the IGMP querier on a subnet if it has the lowest IP address. As long as a router continues to receive query messages from a router with a lower IP address, it resets a timer that is based on its querier timeout value. If the querier timer of a router expires, it becomes 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 this figure, 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 this figure, 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 *Configuring an IGMP SSM Translation*.

Figure 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 *Configuring IGMP Interface Parameters*.

Virtualization Support

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 *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*.

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

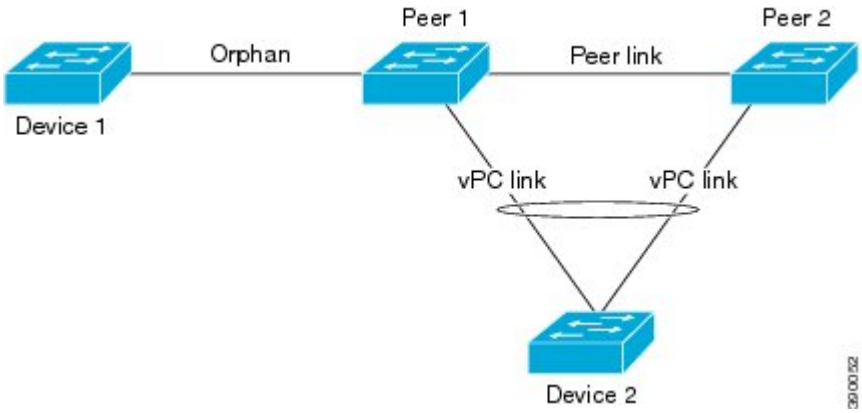
IGMP vPC Incremental Sync

The IGMP vPC incremental sync feature enables routes on the virtual port channel (vPC) peer to synchronize with other routes while the peer link is being established. This feature is a Layer 2 IPv4 multicast feature that enables faster convergence in vPC topologies. This feature enables Layer 2 Internet Group Management Protocol (IGMP) states to be synchronized between vPC peer devices in a triggered and incremental manner instead of periodic synchronization.

Overview of IGMP vPC Incremental Sync

The IGMP vPC Incremental Sync feature sends incremental updates to the peer link using Cisco Fabric Service (CFS), instead of sending all Join and Leave messages. The routes between peers are synced while the peer link is being set up.

Figure 3: Sample topology for implementing IGMP vPC Incremental Sync



Peer 1 is a vPC peer that receives the join/query/protocol independent multicast (PIM) hello either from Device 1 or from Device 2, which is on the vPC link. Peer 2 is a vPC peer that receives incremental updates from Peer 1 on the CFS. Device 1 acts as an orphan. Any port that is not configured as a vPC, but carries a vPC VLAN, is called an orphan.

The vPC peer link synchronizes states between the vPC peer devices. In addition to carrying control traffic between two VPC devices, the vPC peer link also carries multicast and broadcast data traffic. In some link failure scenarios, it also carries unicast traffic.

Interfaces that receive Query and PIM hello are added as device ports. Interfaces that receive Join messages are added as group outgoing interfaces (OIFs). Interfaces that receive Leave messages, delete the OIF from the group entry.

Benefits of IGMP vPC Incremental Sync

- Reduces CFS congestion.
- Results in faster convergence.

Prerequisites for IGMP vPC Incremental Sync

vPC peers must have the same version of the Cisco software image.

Verifying IGMP vPC Incremental Sync

Command	Purpose
show ip igmp internal vpc	Displays the summary of the IGMP vPC incremental sync configuration.

Prerequisites for IGMP

IGMP 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 configuration 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

This table lists the default settings for IGMP parameters.

Table 1: Default IGMP Parameters

Parameters	Default
IGMP version	2
Startup query interval	30 seconds
Startup query count	2
Robustness value	2
Querier timeout	255 seconds
Query timeout	255 seconds

Parameters	Default
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.

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 this table.

Table 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.

Parameter	Description
Static multicast groups	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. **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 *Configuring an IGMP SSM Translation*. 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.
Static multicast groups on OIF	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. **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*.
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.

Parameter	Description
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.
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. 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.

Parameter	Description
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 to control the multicast groups that hosts on the subnet serviced by an interface can join. **Note** Only the **match ip multicast group** command is supported in this route map policy. The **match ip address** command for matching an ACL is not supported.
Immediate leave	Option that minimizes the leave latency of IGMPv2 group memberships on a given IGMP interface because the device does not send group-specific queries. When immediate leave is enabled, the device will remove 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 7000 Series NX-OS Unicast Routing Configuration Guide.

For information about configuring multicast route maps, see *Configuring Route Maps to Control RP Information Distribution*.

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters configuration mode.

Step 2	**interface** *interface*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface mode on the interface type and number, such as *ethernet slot/port.*

Step 3		These commands are used to configure the IGMP interface parameters.

Option	Description
ip igmp version *value*	Sets the IGMP version to the value specified.

Command or Action	Purpose
Option	**Description**
`switch(config-if)# ip igmp version 3`	Values can be 2 or 3. The default is 2. The **no** form of the command sets the version to 2.
ip igmp join-group {**group** [**source** *source*] | **route-map** *policy-name*} `switch(config-if)# ip igmp join-group 230.0.0.0`	Statically binds a multicast group to the outgoing interface, which is handled by the device 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. **Note** A source tree is built for the (S, G) state only if you enable IGMPv3.

Command or Action	Purpose
Option	**Description**
	Caution The device CPU must be able to handle the traffic generated by using this command. Because of CPU load constraints, using this command, especially in any form of scale, is not recommended. Consider using the **ip igmp static-oif** command instead.
ip igmp static-oif {*group* [**source** *source*] | **route-map** *policy-name*} `switch(config-if)# ip igmp static-oif 230.0.0.0`	Statically binds a multicast group to the outgoing interface, which is handled by the device 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. **Note** A source tree is built for the (S, G) state only if you enable IGMPv3.
ip igmp startup-query-interval *seconds*	Sets the query interval used when the software

Command or Action	Purpose
Option	**Description**
`switch(config-if)# ip igmp startup-query-interval 25`	starts up. Values can range from 1 to 18,000 seconds. The default is 31 seconds.
ip igmp startup-query-count *count* `switch(config-if)# ip igmp startup-query-count 3`	Sets the query count used when the software starts up. Values can range from 1 to 10. The default is 2.
ip igmp robustness-variable *value* `switch(config-if)# ip igmp robustness-variable 3`	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.
ip igmp querier-timeout *seconds* `switch(config-if)# ip igmp querier-timeout 300`	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.
ip igmp query-timeout *seconds* `switch(config-if)# ip igmp query-timeout 300`	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. **Note** This command has the same functionality as the **ip igmp querier-timeout** command.
ip igmp query-max-response-time *seconds* Example `switch(config-if)# ip igmp query-max-response-time 15`	Sets the response time advertised in IGMP queries. Values can range from 1 to 25 seconds. The default is 10 seconds.
ip igmp query-interval *interval*	Sets the frequency at which the software sends

Command or Action	Purpose
Option	**Description**
`switch(config-if)# ip igmp query-interval 100`	IGMP host query messages. Values can range from 1 to 18,000 seconds. The default is 125 seconds.
ip igmp last-member-query-response-time *seconds* `switch(config-if)# ip igmp last-member-query-response-time 3`	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.
ip igmp last-member-query-count *count* `switch(config-if)# ip igmp last-member-query-count 3`	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.
ip igmp group-timeout *seconds* `switch(config-if)# ip igmp group-timeout 300`	Sets the group membership timeout for IGMPv2. Values can range from 3 to 65,535 seconds. The default is 260 seconds.
ip igmp report-link-local-groups `switch(config-if)# ip igmp report-link-local-groups`	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.
ip igmp report-policy *policy* `switch(config-if)# ip igmp report-policy my_report_policy`	Configures an access policy for IGMP reports that is based on a route-map policy.
ip igmp access-group *policy* `switch(config-if)# ip igmp access-group my_access_policy`	Configures a route-map policy to control the multicast groups that hosts on the subnet serviced by an interface can join.

	Command or Action	Purpose
	Option	**Description**
		Note Only the **match ip multicast group** command is supported in this route map policy. The **match ip address** command for matching an ACL is not supported.
	ip igmp immediate-leave `switch(config-if)# ip igmp immediate-leave`	Enables the device to remove the group entry from the multicast routing table immediately upon receiving a leave message for the group. Use this command to minimize the leave latency of IGMPv2 group memberships on a given IGMP interface because the device does not send group-specific queries. The default is disabled. **Note** Use this command only when there is one receiver behind the interface for a given group.
Step 4	**show ip igmp interface** [*interface*] [**vrf** *vrf-name* | **all**] [**brief**] **Example:** `switch(config)# show ip igmp interface`	(Optional) Displays IGMP information about the interface.
Step 5	**copy running-config startup-config** **Example:**	(Optional) Saves configuration changes.

	Command or Action	Purpose
	`switch(config)# copy running-config startup-config`	

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 IMPv3 provides the capability to specify group and source addresses in membership reports. By default, the group prefix range is 232.0.0./8. To modify the PIM SSM range, see *Configuring SSM.*

The Internet Group Management Protocol (IGMP) Source-Specific Multicast (SSM) Translation feature enables a SSM-based multicast core network to be deployed when the multicast host do not support IGMPv3 or is forced to send group joins instead of (S,G) reports to interoperate with layer-2 switches. The IGMP SSM-Translation feature provides the functionality to configure multiple sources for the same SSM group. Protocol Independent Multicast (PIM) must be configured on the device before configuring the SSM translation.

This Table lists the example SSM Translations.

Table 3: Table 3 Example SSM Translation

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

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

Table 4: Table 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.

The SSM translation configures source addresses per Virtual Routing and Forwarding (VRF) mode on the device to be mapped to specific SSM group ranges received in an IGMP report. The MRIB creates the (S,G) state rather than (*, G) state.

The IGMP SSM-Translation works in the following way:

- When an IGMPv1 or IGMPv2 report is received on an interface, the IGMP querier performs a translation table search for the reporting group.
- If there are configured source entries for the reporting group, the IGMP process adds to the interface that the report is received on to an (Si,G) entry corresponding to each configured source Si. These entries are stored in the MRIB for software and hardware multicast forwarding.
- If there are no configured source entries for the reporting group, the IGMP process adds to the interface that the report is received on to an (*,G) entry in the MRIB. This is the typical IGMP functionality.
- The periodic group reports helps to keep the state of the translated (S,G) alive. If there are no incoming reports, all entries time out at the same time.
- If an IGMPv2 leave message is received for the group and a corresponding translated entry exist, all entries expire at the same time unless an overriding report is received.

Procedure

	Command or Action	Purpose

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

Step 2	**ip igmp ssm-translate** *group-prefix source-addr* **Example:** `Device(config)# ip igmp ssm-translate 232.0.0.0/8 10.1.1.1`	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	**show running-configuration igmp** **Example:** `Device(config)# show running-configuration igmp`	(Optional) shows the running-configuration information, including *ssm-translate* command lines.
Step 4	**show ip igmp groups** **Example:** `Device(config)# show ip igmp groups`	(Optional) Displays the IGMP attached group membership for a group or interface, the default VRF, a selected VRF, or all VRFs.
Step 5	**show ip mroute** **Example:**	(Optional) Shows IP multicast routing table for default VRF.

	Command or Action	Purpose
	`Device(config)# show ip mroute`	
Step 6	**copy running-config startup-config** **Example:** `Device(config)# copy running-config startup-config`	(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.

Procedure

	Command or Action	Purpose

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

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.
Step 3	**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 4	**show running-configuration igmp** **Example:** `switch(config)# show running-configuration igmp`	(Optional) Displays the running-configuration information, including the *enforce-router-alert* command line.
Step 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves configuration changes.

Restarting the IGMP Process

You can restart the IGMP process and optionally flush all routes.

Procedure

	Command or Action	Purpose
Step 1	**restart igmp** **Example:** `switch# restart igmp`	Restarts the IGMP process.

Step 2	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 3	**ip igmp flush-routes** **Example:** `switch(config)# ip igmp flush-routes`	Removes routes when the IGMP process is restarted. By default, routes are not flushed.
Step 4	**show running-configuration igmp** **Example:** `switch(config)# show running-configuration igmp`	(Optional) Displays the running-configuration information, including the *flush-routes* command lines.
Step 5	**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	Description
show ip igmp interface [*interface*] [**vrf** *vrf-name* | **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. Use this command to display vPC statistics.
show ip igmp groups [{**source** [*group*]}] | {**group** [*source*]}] [**interface**] [**summary**] [**vrf** *vrf-name* | **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 [{**source** [*group*]}] | {**group** [*source*]}] [**interface**] [**summary**] [**vrf** *vrf-name* | **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.

Command	Description
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 7000 Series NX-OS Multicast Routing Command Reference*.

Configuration Examples for IGMP

The following example shows how to configure the IGMP parameters:

```
config t
  ip igmp ssm-translate 232.0.0.0/8 10.1.1.1
  interface ethernet 2/1
    ip igmp version 3
    ip igmp join-group 230.0.0.0
    ip igmp startup-query-interval 25
    ip igmp startup-query-count 3
    ip igmp robustness-variable 3
    ip igmp querier-timeout 300
    ip igmp query-timeout 300
    ip igmp query-max-response-time 15
    ip igmp query-interval 100
    ip igmp last-member-query-response-time 3
    ip igmp last-member-query-count 3
    ip igmp group-timeout 300
    ip igmp report-link-local-groups
    ip igmp report-policy my_report_policy
    ip igmp access-group my_access_policy
```

Feature History for IGMP

This table lists the release history for this feature.

Table 5: Feature History for IGMP

Feature Name	Releases	Feature Information
IGMP vPC Incremental Sync	6.2(2)	The **show ip igmp internal vpc** command was introduced.
ip igmp groups and **ip igmp route** commands.	6.1(1)	Commands updated with summary parameter. • **ip igmp groups** • **ip igmp route**

Feature Name	Releases	Feature Information
vPC	4.1(3)	Displays vPC statistics with the **show ip igmp interface**command. The following section provides information about this feature: • *Verifying the IGMP Configuration*.
Immediate Leave	4.1(3)	Minimizes the leave latency of IGMPv2 or MLDv1 group memberships on a given IGMP or MLD interface because the device does not send group-specific queries. For more information, see *Configuring IGMP Interface Parameters*.