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

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 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.

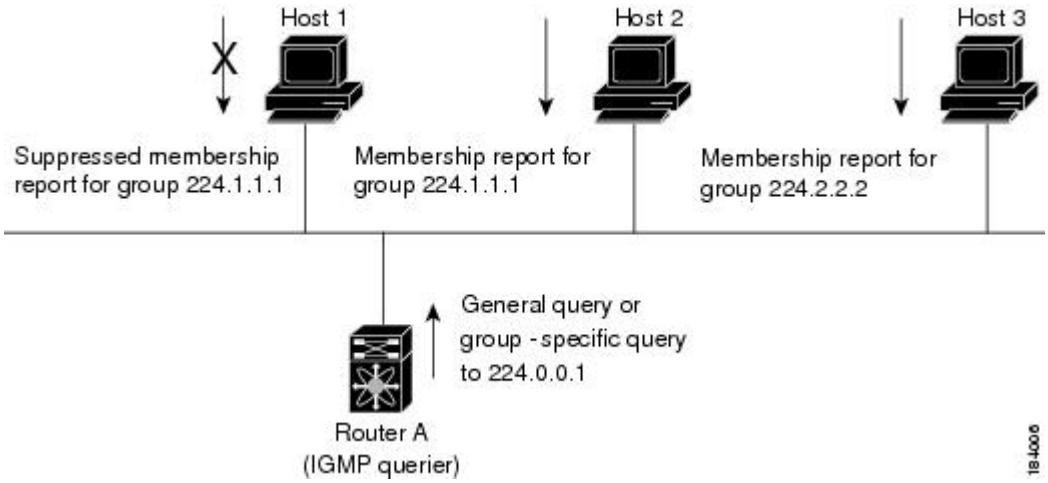
For detailed information about IGMPv2, see RFC 2236.

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 1. 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 Figure 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.

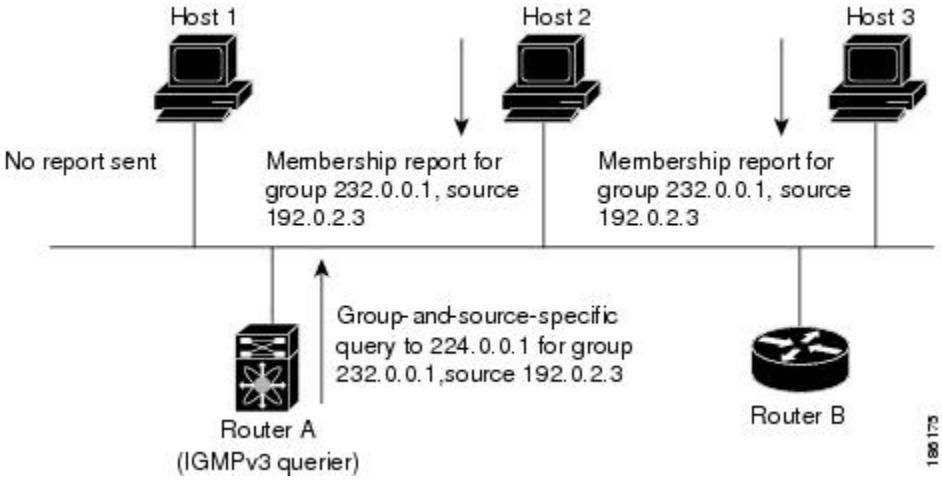
The software elects a router as the IGMP querier on a subnet if it has the lowest IP address. As long as a router continues to receive query messages from a router with a lower IP address, it resets a timer that is based on its querier timeout value. If the querier timer of a router expires, it becomes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

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 the Configuring IGMP Interface Parameters section.

Virtualization Support

Cisco NX-OS suports 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 3548 Switch NX-OS Unicast Routing Configuration Guide*.

Limitations

In Cisco NX-OS releases older than Cisco NX-OS Release 6.0(2)A1(1), you can use the ip igmp join-group command to bind a Nexus 3548 switch to a multicast group. The switch generates an Internet Group Management Protocol (IGMP)-join for the specified group, and any multicast packets destined to the group are sent to the CPU. If there are receivers connected to the Nexus 3548 switch, which request for the group, then a copy of the packet is also sent to the receiver.

In Cisco NX-OS Release 6.0(2)A1(1) and higher releases, you cannot use the ip igmp join-group command to program any Outgoing Interface Lists (OILs). Even if there are receivers that request for the stream, no packets are sent to them. To bind a Nexus 3548 switch to a multicast group, use the ip igmp static-oif command instead of the ip igmp join-group command.

IGMP 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.

For information about configuring VRFs, see the *Cisco Nexus 3548 Switch NX-OS Unicast Routing Configuration Guide*.

Default Settings for IGMP

Table 1 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
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 the table below.

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.
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 the Configuring an IGMP SSM Translation section. 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 section.
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.

Parameter	Description
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 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.

Parameter	Description
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. **Tip** To configure route-map policies, see the *Cisco Nexus 3548 NX-OS Unicast Routing Configuration Guide*.
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.
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 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.

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

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`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*..

	Command or Action	Purpose

Step 3	**no switchport**
	Example:
	`switch(config-if)# no switchport`
	`switch(config-if)#`	

Step 4	**ip igmp version** *value* **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.
Step 5	**ip igmp join-group** {**group** [**source** *source*] | **route-map** *policy-name*} **Example:** `switch(config-if)# ip igmp join-group 230.0.0.0`	Configures an interface on the device to join the specified group or channel. The device accepts the multicast packets for CPU consumption only. **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.
Step 6	**ip igmp static-oif** {*group* [**source** *source*] | **route-map** *policy-name*} **Example:** `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.
Step 7	**ip igmp startup-query-interval** *seconds* **Example:** `switch(config-if)# ip igmp startup-query-interval 25`	Sets the query interval used when the software starts up. Values can range from 1 to 18,000 seconds. The default is 31 seconds.
Step 8	**ip igmp startup-query-count** *count* **Example:** `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.

	Command or Action	Purpose
Step 9	**ip igmp robustness-variable** *value* **Example:** `switch(config-if)# ip igmp robustness-variable 3`	Sets the robustness variable. Values can range from 1 to 7. The default is 2.
Step 10	**ip igmp querier-timeout** *seconds* **Example:** `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.
Step 11	**ip igmp query-timeout** *seconds* **Example:** `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.
Step 12	**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.
Step 13	**ip igmp query-interval** *interval* **Example:** `switch(config-if)# ip igmp query-interval 100`	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	**ip igmp last-member-query-response-time** *seconds* **Example:** `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.
Step 15	**ip igmp last-member-query-count** *count* **Example:** `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.
Step 16	**ip igmp group-timeout** *seconds* **Example:** `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.
Step 17	**ip igmp report-link-local-groups** **Example:**	Enables sending reports for groups in 224.0.0.0/24. Reports are always sent for

	Command or Action	Purpose
	`switch(config-if)# ip igmp report-link-local-groups`	nonlink local groups. By default, reports are not sent for link local groups.
Step 18	**ip igmp report-policy** *policy* **Example:** `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.
Step 19	**ip igmp access-group** *policy* **Example:** `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. **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.
Step 20	**ip igmp immediate-leave** **Example:** `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 21	(Optional) **show ip igmp interface** [*interface*] [**vrf** *vrf-name* | **all**] [**brief**] **Example:** `switch(config)# show ip igmp interface`	Displays IGMP information about the interface.
Step 22	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration. Saves the 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 (PIM) section.

Table 3 lists the example SSM translations.

Table 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 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 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.

Procedure

	Command or Action	Purpose

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

Step 2	**ip igmp ssm-translate** *group-prefix source-addr* **Example:** `switch(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	(Optional) **show running-configuration igmp** **Example:** `switch(config)# show running-configuration igmp`	Shows the running-configuration information, including **ssm-translate** command lines.

	Command or Action	Purpose
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

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

Configuring IGMP Host Proxy

This section contains the following information:

Overview of the feature

The IGMP host proxy feature helps to connect PIM enabled multicast network domain to a domain that does not understand PIM. This feature configures an interface as a proxy interface that proxies PIM joins/prunes that are received on the internal PIM network to IGMP joins/leaves.

IGMP Join Process

When a host wants to join a multicast group, the host sends one or more unsolicited Membership Reports for the multicast group that it wants to join.

IGMP Leave Process

IGMPv2 leaves are sent when the last host in the multicast network leaves. Therefore on receipt of the PIM prune from the last host, IGMPv2 leaves are sent upstream to indicate no more interest.

IGMP Multicast Addresses

IP multicast traffic uses group addresses, which are Class D IP addresses. The high-order four bits of a Class D address are 1110. Therefore, host group addresses can be in the range 224.0.0.0 to 239.255.255.255.

The multicast addresses in the range 224.0.0.0 to 224.0.0.255 are reserved for use by routing protocols and other network control traffic. The address 224.0.0.0 is guaranteed not to be assigned to any group.

IGMP packets are transmitted using the IP multicast group addresses as follows:

- IGMP general queries are destined to the address 224.0.0.1 (all systems on a subnet).
- IGMP group-specific queries are destined to the group IP address for which the router is querying.
- IGMP group membership reports are destined to the group IP address for which the router is reporting.
- IGMPv2 Leave messages are destined to the address 224.0.0.2 (all routers on a subnet).

Guidelines and Limitations

See the following guidelines and limitations for configuring IGMP host proxy:

- Excluding or blocking a list of sources according to IGMPv3 (RFC 3376) is not supported.
- IGMP Host proxy proxies PIM joins/prunes received to IGMP joins/prunes on the proxy interface.
- Disable snooping if the proxy interface is a VLAN.
- It can be used to connect the network that understands only IGMP.
- The host proxy interface is a Layer 3 interface.
- The (S,G) entries have the RPF as the IGMP host proxy interfaces.
- The ideal configuration point is the RP.
- The IGMP host proxy can be in a query mode or unsolicited mode.
- If the reports need to be sent without the presence of a querier, configure the IGMP host proxy in unsolicited mode.
- Configure the IGMP host proxy unsolicited mode on a layer 3 physical port.
- The IGMP host proxy interface should have IP enabled.
- The PIM should not be enabled on the host proxy interface.
- The IGMP static/join group should not be configured on the IGMP host proxy interface.

- IGMP host proxy does not work with route-maps if a route-map uses **ip prefix-lists** in the match clause. Be sure to use **ip multicast** in the route-map match clause.

How to Configure IGMP Host Proxy

Perform the following steps to configure IGMP host proxy:

Table 5: Configuring IGMP Host Proxy

Step	Command	Purpose
Step 1	**configure terminal** Example: `switch# configure terminal switch(config)#`	Enters configuration mode.
Step 2	**interface vlan** *interface*	Enters VLAN interface mode.
Step 3	**no shutdown**	Configures the interface in no shutdown mode.
Step 4	**ip address** *ip address*	Configures the IP address.
Step 5	[**no**] **ip igmp host-proxy** [**unsolicited** [*time*] | **route-map** *route-map-name* [**unsolicited** [*time*]] | **prefix-list** *prefix-list-name* [**unsolicited** [*time*]]]	Configures the IGMP host proxy for the route-map.
Step 6	**show ip igmp groups**	Displays the IGMP connected group membership for VRF with H type for host proxy.
Step 7	**show ip igmp int vlan** *interface*	Displays the IGMP interfaces for VRF.
Step 8	**show ip igmp local-groups vlan** *interface*	Displays the IGMP locally joined group membership for VRF.
Step 9	show ip pim host-proxy	Displays the PIM host proxy interfaces.

Verifying the IGMP Configuration

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

Command	Purpose
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.

Command	Purpose
show ip igmp groups *group*|*interface*] [**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*group* | *interface* **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.
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 3000 Series Multicast Routing Command Reference.

Configuration Examples for IGMP

The following 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 join-group 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
switch(config-if)# ip igmp immediate-leave
```

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:

-
-