



## CHAPTER 2

# Configuring IGMP and MLD

---

This chapter describes how to configure Internet Group Management Protocol (IGMP) for IPv4 networks and Multicast Listener Discovery (MLD) for IPv6 networks.

This chapter includes the following sections:

- [IGMP, page 2-1](#)
- [MLD, page 2-14](#)
- [Additional References, page 2-25](#)

## IGMP

This section describes how to configure IGMP on your IPv4 networks.

This section includes the following topics:

- [Information About IGMP, page 2-1](#)
- [Licensing Requirements for IGMP, page 2-4](#)
- [Prerequisites for IGMP, page 2-5](#)
- [Configuring IGMP Parameters, page 2-5](#)
- [Verifying IGMP Configuration, page 2-12](#)
- [IGMP Example Configuration, page 2-13](#)
- [Where to Go Next, page 2-13](#)
- [Default Settings for IGMP, page 2-13](#)

## 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

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

- Enable link-local group reports

This section includes the following topics:

- [IGMP Versions, page 2-2](#)
- [IGMP Basics, page 2-2](#)
- [Virtualization Support, page 2-4](#)

## 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.

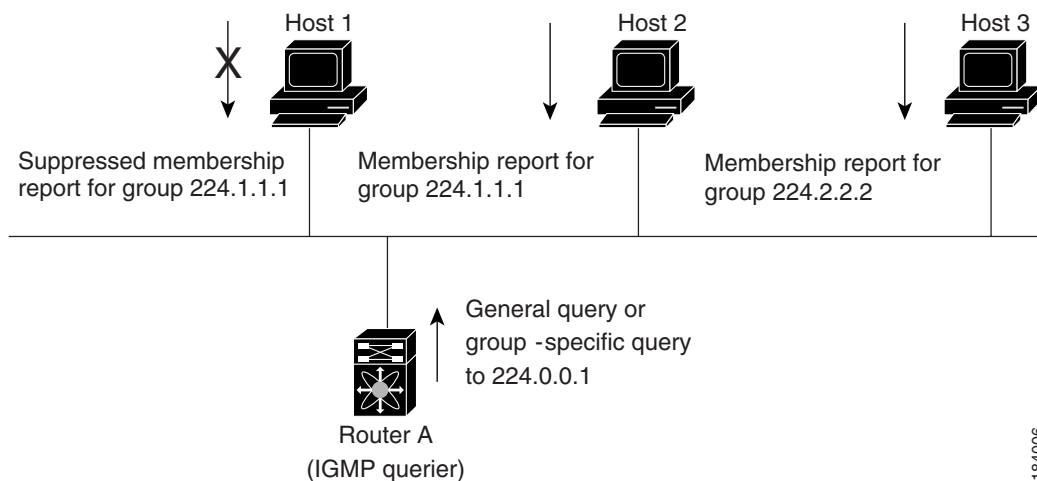
For detailed information about IGMPv2, see [RFC 2236](#).

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

## IGMP Basics

The basic IGMP process of a router that discovers multicast hosts is shown in [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

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

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 2-5](#).

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.

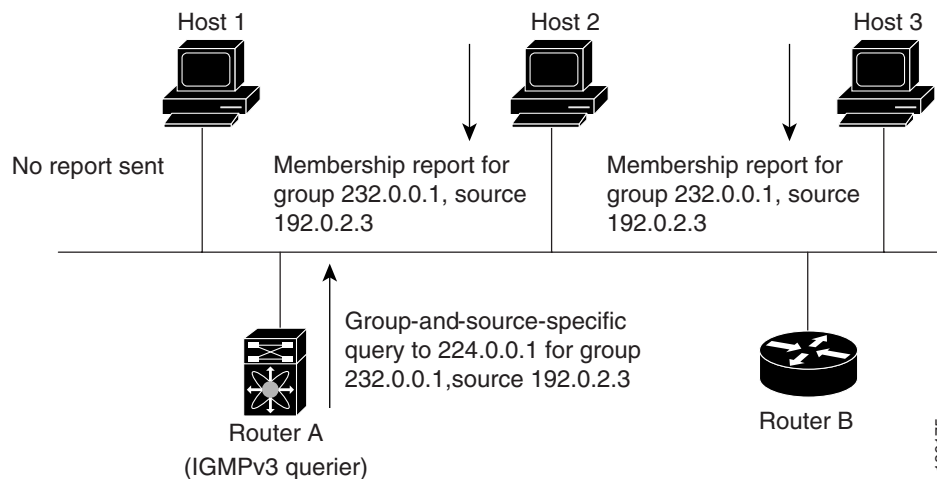
In [Figure 2-1](#), host 1’s membership report is suppressed and host 2 sends its membership report for group 224.1.1.1 first. Host 1 receives the report from host 2. Because only one membership report per group needs to be sent to the router, other hosts suppress their reports to reduce network traffic. 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 2-10](#).

**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

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

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 2-5.

## 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 [Chapter 4, “Configuring IGMP Snooping.”](#)

You can use the **show** commands with a VRF argument to provide a context for the information displayed. The default VRF is used if no VRF argument is supplied.

For information about configuring VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.0*.

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

## Licensing Requirements for IGMP

The following table shows the licensing requirements for this feature:

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

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

## 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.

## 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 2-5](#)
- [Configuring an IGMP SSM Translation, page 2-10](#)
- [Restarting the IGMP Process, page 2-11](#)



### 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 2-1](#).

**Table 2-1** 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.</p> <p><b>Note</b> 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 <a href="#">“Configuring an IGMP SSM Translation” section on page 2-10</a>.</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>

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

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

Parameter	Description
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.</p> <p><b>Note</b> 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 <a href="#">“Configuring an IGMP SSM Translation” section on page 2-10</a>.</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.
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	<p>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.</p> <p> <b>Caution</b> 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.</p>

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

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

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 routing-rules policy <sup>1</sup> .
Access groups	Option that configures a routing-rules policy <sup>1</sup> to control the multicast groups that hosts on the subnet serviced by an interface can join.

1. To configure routing-rules policies, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0*.

## SUMMARY STEPS

1. **config t**
2. **interface *interface***
3. **ip igmp version *value***  
**ip igmp join-group *group-addr* [source *source-addr*]**  
**ip igmp static-oif *group-addr* [source *source-addr*]**  
**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***
4. **show ip igmp interface [*interface*] [vrf *vrf-name* | all] [brief]**
5. **copy running-config startup-config**

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

## DETAILED STEPS

	Command	Purpose
Step 1	<pre>config t</pre> <p><b>Example:</b> switch# config t switch(config)#</p>	Enters configuration mode.
Step 2	<pre>interface interface</pre> <p><b>Example:</b> switch(config)# interface ethernet 2/1 switch(config-if)#</p>	Enters interface mode on the interface type and number, such as <b>ethernet</b> <i>slot/port</i> .
Step 3	<pre>ip igmp version value</pre> <p><b>Example:</b> switch(config-if)# ip igmp version 3</p>	<p>Sets the IGMP version to the value specified. Values can be 2 or 3. The default is 2.</p> <p>The <b>no</b> form of the command sets the version to 2.</p>
	<pre>ip igmp join-group group-addr [source source-addr]</pre> <p><b>Example:</b> switch(config-if)# ip igmp join-group 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.</p> <p><b>Note</b> A source tree is built for the (S, G) state only if you enable IGMPv3.</p>
	<pre>ip igmp static-oif group-addr [source source-addr]</pre> <p><b>Example:</b> 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 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.</p> <p><b>Note</b> A source tree is built for the (S, G) state only if you enable IGMPv3.</p>
	<pre>ip igmp startup-query-interval seconds</pre> <p><b>Example:</b> 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>
	<pre>ip igmp startup-query-count count</pre> <p><b>Example:</b> 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>
	<pre>ip igmp robustness-variable value</pre> <p><b>Example:</b> 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>



**Caution** The device CPU must handle the traffic generated by using this command.

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

Command	Purpose
<p><b>ip igmp querier-timeout</b> <i>seconds</i></p> <p><b>Example:</b>  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>
<p><b>ip igmp query-timeout</b> <i>seconds</i></p> <p><b>Example:</b>  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><b>Note</b> This command has the same functionality as the <b>ip igmp querier-timeout</b> command.</p>
<p><b>ip igmp query-max-response-time</b> <i>seconds</i></p> <p><b>Example:</b>  switch(config-if)# ip igmp  query-max-response-time 15</p>	<p>Sets the response time advertised in IGMP queries. Values can range from 1 to 25 seconds. The default is 10 seconds.</p>
<p><b>ip igmp query-interval</b> <i>interval</i></p> <p><b>Example:</b>  switch(config-if)# ip igmp  query-interval 100</p>	<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.</p>
<p><b>ip igmp last-member-query-response-time</b> <i>seconds</i></p> <p><b>Example:</b>  switch(config-if)# ip igmp  last-member-query-response-time 3</p>	<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.</p>
<p><b>ip igmp last-member-query-count</b> <i>count</i></p> <p><b>Example:</b>  switch(config-if)# ip igmp  last-member-query-count 3</p>	<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.</p>
<p><b>ip igmp group-timeout</b> <i>seconds</i></p> <p><b>Example:</b>  switch(config-if)# ip igmp group-timeout  300</p>	<p>Sets the group membership timeout for IGMPv2. Values can range from 3 to 65,535 seconds. The default is 260 seconds.</p>
<p><b>ip igmp report-link-local-groups</b></p> <p><b>Example:</b>  switch(config-if)# ip igmp  report-link-local-groups</p>	<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.</p>
<p><b>ip igmp report-policy</b> <i>policy</i></p> <p><b>Example:</b>  switch(config-if)# ip igmp report-policy  my_report_policy</p>	<p>Configures an access policy for IGMP reports that is based on a routing-rules policy.</p>
<p><b>ip igmp access-group</b> <i>policy</i></p> <p><b>Example:</b>  switch(config-if)# ip igmp access-group  my_access_policy</p>	<p>Configures a routing-rules policy to control the multicast groups that hosts on the subnet serviced by an interface can join.</p>

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

	Command	Purpose
Step 4	<code>show ip igmp interface [interface] [vrf vrf-name   all] [brief]</code>  <b>Example:</b> switch(config)# show ip igmp interface	(Optional) Displays IGMP information about the interface.
Step 5	<code>copy running-config startup-config</code>  <b>Example:</b> switch(config)# copy running-config startup-config	(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 3-28.

Table 2-2 lists the example SSM translations.

**Table 2-2 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 2-3 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 2-3 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. `config t`
2. `ip igmp ssm-translate group-prefix source-addr`
3. `show running-config | include ssm-translate`

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

4. `copy running-config startup-config`

## DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code>  <b>Example:</b> switch# <code>config t</code> switch(config)#	Enters configuration mode.
Step 2	<code>ip igmp ssm-translate group-prefix source-addr</code>  <b>Example:</b> 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-config   include ssm-translate</code>  <b>Example:</b> switch(config)# <code>show running-config   include ssm-translate</code>	(Optional) Shows ssm-translate configuration lines in the running configuration.
Step 4	<code>copy running-config startup-config</code>  <b>Example:</b> switch(config)# <code>copy running-config startup-config</code>	(Optional) Saves configuration changes.

## Restarting the IGMP Process

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

## SUMMARY STEPS

1. `restart igmp`
2. `config t`
3. `ip igmp flush-routes`
4. `show running-config | include flush-routes`
5. `copy running-config startup-config`

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

## DETAILED STEPS

	Command	Purpose
Step 1	<b>restart igmp</b>  <b>Example:</b> switch# restart igmp	Restarts the IGMP process.
Step 2	<b>config t</b>  <b>Example:</b> switch# config t switch(config)#	Enters configuration mode.
Step 3	<b>ip igmp flush-routes</b>  <b>Example:</b> switch(config)# ip igmp flush-routes	Removes routes when the IGMP process is restarted. By default, routes are not flushed.
Step 4	<b>show running-config   include flush-routes</b>  <b>Example:</b> switch(config)# show running-config   include flush-routes	(Optional) Shows flush-routes configuration lines in the running configuration.
Step 5	<b>copy running-config startup-config</b>  <b>Example:</b> switch(config)# copy running-config startup-config	(Optional) Saves configuration changes.

## Verifying IGMP Configuration

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

Command	Purpose
<b>show ip igmp interface</b> [ <i>interface</i> ] [ <b>vrf</b> <i>vrf-name</i>   <b>all</b> ] [ <b>brief</b> ]	Displays IGMP information about all interfaces or a selected interface, the default VRF, a selected VRF, or all VRFs.
<b>show ip igmp groups</b> [ <i>group</i>   <i>interface</i> ] [ <b>vrf</b> <i>vrf-name</i>   <b>all</b> ]	Displays the IGMP attached group membership for a group or interface, the default VRF, a selected VRF, or all VRFs.
<b>show ip igmp route</b> [ <i>group</i>   <i>interface</i> ] [ <b>vrf</b> <i>vrf-name</i>   <b>all</b> ]	Displays the IGMP attached group membership for a group or interface, the default VRF, a selected VRF, or all VRFs.
<b>show ip igmp local-groups</b>	Displays the IGMP local group membership.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference, Release 4.0*.

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

## IGMP Example Configuration

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

```

## 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”](#)

## Default Settings for IGMP

Table 2-4 lists the default settings for IGMP parameters.

**Table 2-4** 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

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

## MLD

This section describes how to configure MLD on your IPv6 networks.

This section includes the following topics:

- [Information About MLD, page 2-14](#)
- [Licensing Requirements for MLD, page 2-17](#)
- [Prerequisites for MLD, page 2-17](#)
- [Configuring MLD Parameters, page 2-17](#)
- [Verifying MLD Configuration, page 2-24](#)
- [MLD Example Configuration, page 2-24](#)
- [Where to Go Next, page 2-25](#)
- [Default Settings for MLD, page 2-25](#)

## Information About MLD

MLD is an IPv6 protocol that a host uses to request multicast data for a particular group. Using the information obtained through MLD, the software maintains a list of multicast group or channel memberships on a per-interface basis. The devices that receive MLD packets send the multicast data that they receive for requested groups or channels out the network segment of the known receivers.

MLDv1 is derived from IGMPv2, and MLDv2 is derived from IGMPv3. IGMP uses IP Protocol 2 message types, while MLD uses IP Protocol 58 message types, which is a subset of the ICMPv6 messages.

The MLD process is started automatically on the device. You cannot enable MLD manually on an interface. MLD is automatically enabled when you perform one of the following configuration tasks on an interface:

- Enable PIM6
- Statically bind a local multicast group
- Enable link-local group reports

This section includes the following topics:

- [MLD Versions, page 2-14](#)
- [MLD Basics, page 2-15](#)
- [Virtualization Support, page 2-17](#)

## MLD Versions

The device supports MLDv1 and MLDv2. MLDv2 supports MLDv1 listener reports.

By default, the software enables MLDv2 when it starts the MLD process. You can enable MLDv1 on interfaces where you want only its capabilities.

MLDv2 includes the following key changes from MLDv1:

- Support for Source-Specific Multicast (SSM), which builds shortest path trees from each receiver to the source, through the following features:

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

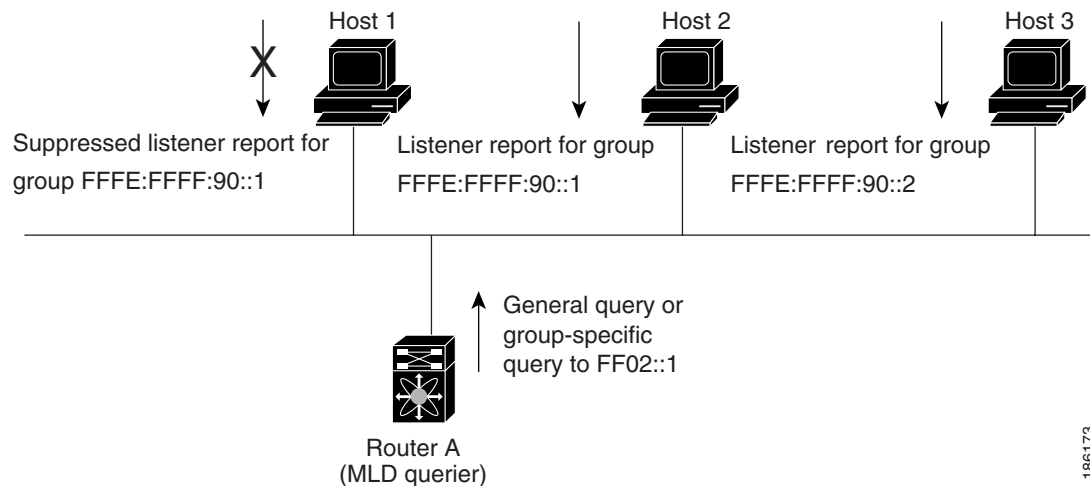
- Host messages that can specify both the group and the source.
- The multicast state that is maintained for groups and sources, not just for groups as in MLDv1.
- Hosts no longer perform report suppression, which means that hosts always send MLD listener reports when an MLD query message is received.

For detailed information about MLDv1, see [RFC 2710](#). For detailed information about MLDv2, see [RFC 3810](#).

## MLD Basics

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

**Figure 2-3** MLD Query-Response Process



In [Figure 2-3](#), router A, which is the MLD designated querier on the subnet, sends a general query message to the link-scope all-nodes multicast address FF02::1 periodically to discover what multicast groups hosts want to receive. The group-specific query is used to discover whether a specific group is requested by any hosts. 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 MLD parameters, see the “[Configuring MLD Interface Parameters](#)” section on [page 2-18](#).

In [Figure 2-3](#), host 1’s listener report is suppressed, and host 2 sends its listener report for group FFFE:FFFF:90::1 first. Host 1 receives the report from host 2. Because only one listener 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

MLDv1 membership report suppression occurs only on hosts that are connected to the same port.

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

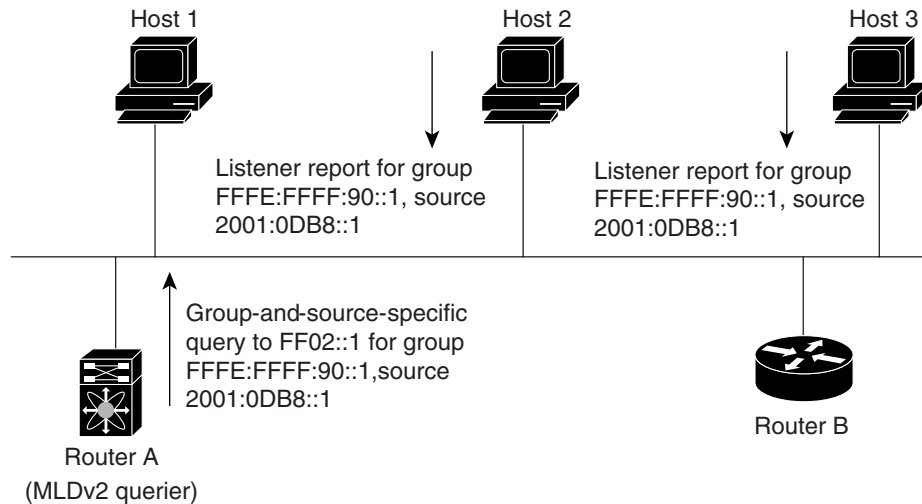
In Figure 2-4, router A sends the MLDv2 group-and-source-specific query to the LAN. Hosts 2 and 3 respond to the query with listener reports that indicate that they want to receive data from the advertised group and source. This MLDv2 feature supports SSM. For information about configuring SSM translation to support SSM for MLDv1 hosts, see the “Configuring an MLD SSM Translation” section on page 2-22.



**Note**

In MLDv2, all hosts respond to queries.

**Figure 2-4 MLDv2 Group-and-Source-Specific Query**



The software elects a router as the MLD 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 remains a non querier and 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.

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, and you can configure the frequency and number of query messages sent specifically for MLD startup. 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 responsiveness to host group membership and the traffic created on the network.



**Caution**

If you change the query interval, you can severely impact multicast forwarding in your network.

When a multicast host leaves a group, it should send a done message for MLDv1, or a listener report that excludes the group to the link-scope all-routers multicast address FF02::2. To check if this host is the last host to leave the group, the software sends an MLD 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 the packet loss on a congested network. The robustness value is used by the MLD software to determine the number of times to send messages.

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

Link local addresses in the range FF02::0/16 have link scope, as defined 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 MLD process sends listener 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 MLD parameters, see the [“Configuring MLD Interface Parameters” section on page 2-18](#).

## 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 MLD process can run per VDC. The MLD process supports all VRFs in that VDC.

You can use the **show** commands with a VRF argument to provide a context for the information displayed. The default VRF is used if no VRF argument is supplied.

For information about configuring VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.0*.

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

## Licensing Requirements for MLD

The following table shows the licensing requirements for this feature:

Product	License Requirement
NX-OS	MLD requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the <i>Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0</i> .

## Prerequisites for MLD

MLD 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.

## Configuring MLD Parameters

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

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

**Note**

Before you can access the MLD commands, you must enable the MLD feature.

This section includes the following topics:

- [Configuring MLD Interface Parameters, page 2-18](#)
- [Configuring an MLD SSM Translation, page 2-22](#)

**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 MLD Interface Parameters


You can configure the optional MLD interface parameters described in [Table 2-5](#).

**Table 2-5 MLD Interface Parameters**

Parameter	Description
MLD version	MLD version that is enabled on the interface. MLDv2 supports MLDv1. The MLD version can be 1 or 2. 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.</p> <p><b>Note</b> Although you can configure the (S, G) state, the source tree is built only if you enable MLDv2. For information about SSM translation, see the <a href="#">“Configuring an MLD SSM Translation” section on page 2-22</a>.</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.</p> <p><b>Note</b> Although you can configure the (S, G) state, the source tree is built only if you enable MLDv2. For information about SSM translation, see the <a href="#">“Configuring an MLD SSM Translation” section on page 2-22</a>.</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 30 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.

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

**Table 2-5 MLD Interface Parameters (continued)**

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 MLD queries. You can tune the burstiness of MLD 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 MLD host query messages. You can tune the number of MLD messages on the network by setting a larger value so that the software sends MLD queries less often. Values range from 1 to 18,000 seconds. The default is 125 seconds.
Last member query response interval	Query interval for response to an MLD query that the software sends 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 MLD 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.  <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p> <b>Caution</b> 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 can wait until the next query interval before the group is added again.</p> </div>
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 FF02::0/16. 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 MLD reports that is based on a routing-rules policy <sup>1</sup> .
Access groups	Option that configures a routing-rules policy <sup>1</sup> to control the multicast groups that hosts on the subnet serviced by an interface can join.

1. To configure routing-rules policies, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0*.

## SUMMARY STEPS

1. **config t**
2. **interface** *interface*


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

3. **ipv6 mld version** *value*  
**ipv6 mld join-group** *group-addr* [**source** *source-addr*]  
**ipv6 mld static-oif** *group-addr* [**source** *source-addr*]  
**ipv6 mld startup-query-interval** *seconds*  
**ipv6 mld startup-query-count** *count*  
**ipv6 mld robustness-variable** *value*  
**ipv6 mld querier-timeout** *seconds*  
**ipv6 mld query-timeout** *seconds*  
**ipv6 mld query-max-response-time** *seconds*  
**ipv6 mld query-interval** *interval*  
**ipv6 mld last-member-query-response-time** *seconds*  
**ipv6 mld last-member-query-count** *count*  
**ipv6 mld group-timeout** *seconds*  
**ipv6 mld report-link-local-groups**  
**ipv6 mld report-policy** *policy*  
**ipv6 mld access-group** *policy*
4. **show ipv6 mld interface** [*interface*] [**vrf** *vrf-name* | **all**] [**brief**]
5. **copy running-config startup-config**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>config t</b>  <b>Example:</b> switch# config t switch(config)#	Enters configuration mode.
Step 2	<b>interface</b> <i>interface</i>  <b>Example:</b> switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface mode on the interface type and number, such as <b>ethernet</b> <i>slot/port</i> .
Step 3	<b>ipv6 mld version</b> <i>value</i>  <b>Example:</b> switch(config-if)# ipv6 mld version 3	Sets the MLD version to the value specified. Values can be 1 or 2. The default is 2.  The <b>no</b> form of the command sets the version to 2.

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

Command	Purpose
<p><b>ipv6 mld join-group</b> <i>group-addr</i> [<b>source</b> <i>source-addr</i>]</p> <p><b>Example:</b> switch(config-if)# ipv6 mld join-group FFFE::1</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.</p> <p><b>Note</b> A source tree is built for the (S, G) state only if you enable MLDv2.</p> <p> <b>Caution</b> The device CPU must handle the traffic generated by using this command.</p>
<p><b>ipv6 mld static-oif</b> <i>group-addr</i> [<b>source</b> <i>source-addr</i>]</p> <p><b>Example:</b> switch(config-if)# ipv6 mld static-oif FFFE::1</p>	<p>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.</p> <p><b>Note</b> A source tree is built for the (S, G) state only if you enable MLDv2.</p>
<p><b>ipv6 mld startup-query-interval</b> <i>seconds</i></p> <p><b>Example:</b> switch(config-if)# ipv6 mld 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>
<p><b>ipv6 mld startup-query-count</b> <i>count</i></p> <p><b>Example:</b> switch(config-if)# ipv6 mld 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>
<p><b>ipv6 mld robustness-variable</b> <i>value</i></p> <p><b>Example:</b> switch(config-if)# ipv6 mld 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>
<p><b>ipv6 mld querier-timeout</b> <i>seconds</i></p> <p><b>Example:</b> switch(config-if)# ipv6 mld 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>
<p><b>ipv6 mld query-timeout</b> <i>seconds</i></p> <p><b>Example:</b> switch(config-if)# ipv6 mld 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><b>Note</b> This command has the same functionality as the <b>ipv6 mld querier-timeout</b> command.</p>
<p><b>ipv6 mld query-max-response-time</b> <i>seconds</i></p> <p><b>Example:</b> switch(config-if)# ipv6 mld query-max-response-time 15</p>	<p>Sets the response time advertised in MLD queries. Values can range from 1 to 25 seconds. The default is 10 seconds.</p>

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

Command	Purpose
<b>ipv6 mld query-interval</b> <i>interval</i>  <b>Example:</b> switch(config-if)# ipv6 mld query-interval 100	Sets the frequency at which the software sends MLD host query messages. Values can range from 1 to 18,000 seconds. The default is 125 seconds.
<b>ipv6 mld last-member-query-response-time</b> <i>seconds</i>  <b>Example:</b> switch(config-if)# ipv6 mld 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.
<b>ipv6 mld last-member-query-count</b> <i>count</i>  <b>Example:</b> switch(config-if)# ipv6 mld last-member-query-count 3	Sets the number of times that the software sends an MLD query in response to a host leave message. Values can range from 1 to 5. The default is 2.
<b>ipv6 mld group-timeout</b> <i>seconds</i>  <b>Example:</b> switch(config-if)# ipv6 mld group-timeout 300	Sets the group membership timeout for MLDv2. Values can range from 3 to 65,535 seconds. The default is 260 seconds.
<b>ipv6 mld report-link-local-groups</b>  <b>Example:</b> switch(config-if)# ipv6 mld 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.
<b>ipv6 mld report-policy</b> <i>policy</i>  <b>Example:</b> switch(config-if)# ipv6 mld report-policy my_report_policy	Configures an access policy for MLD reports that is based on a routing-rules policy.
<b>ipv6 mld access-group</b> <i>policy</i>  <b>Example:</b> switch(config-if)# ipv6 mld access-group my_access_policy	Configures a routing-rules policy to control the multicast groups that hosts on the subnet serviced by an interface can join.
<b>Step 4</b> <b>show ipv6 mld interface</b> [ <i>interface</i> ] [ <b>vrf</b> <i>vrf-name</i>   <b>all</b> ] [ <b>brief</b> ]  <b>Example:</b> switch(config)# show ipv6 mld interface	(Optional) Displays MLD information about the interface.
<b>Step 5</b> <b>copy running-config startup-config</b>  <b>Example:</b> switch(config)# copy running-config startup-config	(Optional) Saves configuration changes.

## Configuring an MLD SSM Translation

You can configure an SSM translation to provide SSM support when the router receives MLDv1 listener reports. Only MLDv2 provides the capability to specify group and source addresses in listener reports. By default, the group prefix range is FF3x/96. To modify the PIM SSM range, see the [“Configuring SSM”](#) section on page 3-28.

Table 2-6 lists the example SSM translations.

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

**Table 2-6 Example SSM Translations**

Group Prefix	Source Address
FF30::0/16	2001:0DB8:0:ABCD::1
FF30::0/16	2001:0DB8:0:ABCD::2
FF30:30::0/24	2001:0DB8:0:ABCD::3
FF32:40::0/24	2001:0DB8:0:ABCD::4

Table 2-7 shows the resulting M6RIB routes that the MLD process creates when it applies an SSM translation to the MLD v1 listener report. If more than one translation applies, the router creates the (S, G) state for each translation.

**Table 2-7 Example Result of Applying SSM Translations**

MLDv1 Listener Report	Resulting M6RIB Route
FF32:40::40	(2001:0DB8:0:ABCD::4, FF32:40::40)
FF30:10::10	(2001:0DB8:0:ABCD::1, FF30:10::10) (2001:0DB8:0:ABCD::2, FF30:10::10)

## SUMMARY STEPS

1. `config t`
2. `ipv6 [icmp] mld ssm-translate group-prefix source-addr`
3. `show running-config ssm-translate`
4. `copy running-config startup-config`

## DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code>  <b>Example:</b> switch# config t switch(config)#	Enters configuration mode.
Step 2	<code>ipv6 [icmp] mld ssm-translate group-prefix source-addr</code>  <b>Example:</b> switch(config)# ipv6 mld ssm-translate FF30::0/16 2001:0DB8:0:ABCD::1	Configures the translation of MLDv1 listener reports by the MLD process to create the (S,G) state as if the router had received an MLDv2 listener report.

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

	Command	Purpose
Step 3	<b>show running-config ssm-translate</b>  <b>Example:</b> switch(config)# show running-config ssm-translate	(Optional) Shows ssm-translate configuration lines in the running configuration.
Step 4	<b>copy running-config startup-config</b>  <b>Example:</b> switch(config)# copy running-config startup-config	(Optional) Saves configuration changes.

## Verifying MLD Configuration

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

Command	Purpose
<b>show ipv6 mld interface</b> [ <i>interface</i> ] [ <b>vrf</b> <i>vrf-name</i>   <b>all</b> ] [ <b>brief</b> ]	Displays MLD information about all interfaces or a selected interface, the default VRF, a selected VRF, or all VRFs.
<b>show ipv6 mld groups</b> [ <i>group</i>   <i>interface</i> ] [ <b>vrf</b> <i>vrf-name</i>   <b>all</b> ]	Displays the MLD attached group membership for a group or interface, the default VRF, a selected VRF, or all VRFs.
<b>show ipv6 mld route</b> [ <i>group</i>   <i>interface</i> ] [ <b>vrf</b> <i>vrf-name</i>   <b>all</b> ]	Displays the MLD attached group membership for a group or interface, the default VRF, a selected VRF, or all VRFs.
<b>show ipv6 mld local-groups</b>	Displays the MLD local group membership.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference, Release 4.0*.

## MLD Example Configuration

The following example shows how to configure the MLD parameters:

```

config t
  ipv6 mld ssm-translate FF30::0/16 2001:0DB8:0:ABCD::1
  interface ethernet 2/1
    ipv6 mld version 3
    ipv6 mld join-group FFFE::1
    ipv6 mld startup-query-interval 25
    ipv6 mld startup-query-count 3
    ipv6 mld robustness-variable 3
    ipv6 mld querier-timeout 300
    ipv6 mld query-timeout 300
    ipv6 mld query-max-response-time 15
    ipv6 mld query-interval 100
    ipv6 mld last-member-query-response-time 3
    ipv6 mld last-member-query-count 3
    ipv6 mld group-timeout 300
    ipv6 mld report-link-local-groups
    ipv6 mld report-policy my_report_policy

```

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

```
ipv6 mld access-group my_access_policy
```

## Where to Go Next

You can configure the MBGP feature that works with PIM6 and MLD:

- [Chapter 5, “Configuring MSDP”](#)

## Default Settings for MLD

[Table 2-8](#) lists the default settings for MLD parameters.

**Table 2-8**      *Default MLD Parameters*

Parameters	Default
MLD 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

## Additional References

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

- [Related Documents, page 2-26](#)
- [Standards, page 2-26](#)
- [Appendix A, “IETF RFCs”](#)
- [Technical Assistance, page 2-26](#)

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

## Related Documents

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

## Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## Technical Assistance

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