



Configuring CGMP

- [Finding Feature Information, page 1](#)
- [Prerequisites for Configuring CGMP, page 1](#)
- [Restrictions for CGMP, page 1](#)
- [Information About CGMP, page 2](#)
- [Enabling CGMP Server Support, page 2](#)
- [Monitoring CGMP, page 4](#)
- [Additional References, page 5](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring CGMP

The following are the prerequisites for configuring CGMP:

- When multiple Cisco CGMP-capable devices are connected to a switched network and the **ip cgmp proxy** command is needed, we recommend that all devices be configured with the same CGMP option and have precedence for becoming the IGMP querier over non-Cisco routers.

Restrictions for CGMP

The following are the restrictions for CGMP:

- CGMP is mutually exclusive with HSRPv1. You cannot enable CGMP leaving processing and HSRPv1 at the same time. However, you can enable CGMP and HSRPv2 at the same time.

Information About CGMP

Cisco Group Management Protocol or CGMP-server support is provided on the switch; no client-side functionality is provided. The switch serves as a CGMP server for devices that do not support IGMP snooping but have CGMP-client functionality.

CGMP is a protocol used on Cisco routers and multilayer switches connected to Layer 2 Catalyst switches to perform tasks similar to those performed by IGMP. CGMP permits Layer 2 group membership information to be communicated from the CGMP server to the switch. The switch can then learn on which interfaces multicast members reside instead of flooding multicast traffic to all switch interfaces. (IGMP snooping is another method to constrain the flooding of multicast packets.)

CGMP is necessary because the Layer 2 switch cannot distinguish between IP multicast data packets and IGMP report messages, which are both at the MAC level and are addressed to the same group address.

Enabling CGMP Server Support

When multiple Cisco CGMP-capable devices are connected to a switched network and you configure the **ip cgmp proxy** command, we recommend that all devices be configured with the same CGMP option and have precedence for becoming the IGMP querier over non-Cisco routers. Perform these steps to enable the CGMP server on the switch interface:

This procedure is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *interface-id***
4. **ip cgmp [proxy | router-only]**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Switch> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 3	interface interface-id Example: Switch(config)# interface gigabitethernet 1/0/1	Specifies the interface that is connected to the Layer 2 Catalyst switch, and enters interface configuration mode.
Step 4	ip cgmp [proxy router-only] Example: Switch(config-if)# ip cgmp proxy	<p>Enables CGMP on the interface.</p> <p>By default, CGMP is disabled on all interfaces.</p> <p>Enabling CGMP triggers a CGMP join message. Enable CGMP only on Layer 3 interfaces connected to Layer 2 Catalyst switches.</p> <p>(Optional) When you enter the proxy keyword, the CGMP proxy function is enabled. The proxy router advertises the existence of non-CGMP-capable routers by sending a CGMP join message with the non-CGMP-capable router MAC address and a group address of 0000.0000.0000.</p> <p>Note To perform CGMP proxy, the switch must be the IGMP querier. If you configure the ip cgmp proxy command, you must manipulate the IP addresses so that the switch is the IGMP querier, which might be the highest or lowest IP address, depending on which version of IGMP is running on the network. An IGMP Version 2 querier is selected based on the lowest IP address on the interface. An IGMP Version 1 querier is selected based on the multicast routing protocol used on the interface.</p> <p>Note To disable CGMP on the interface, use the no ip cgmp interface configuration command.</p>
Step 5	end Example: Switch(config-if)# end	Returns to privileged EXEC mode.
Step 6	show running-config Example: Switch# show running-config	Verifies your entries.

	Command or Action	Purpose
Step 7	copy running-config startup-config Example: Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

What to Do Next

Verify the Layer 2 Catalyst switch CGMP-client configuration. For more information, see the documentation that shipped with the product

Monitoring CGMP

You can display specific statistics, such as the contents of IP routing tables, caches, and databases.



Note

This release does not support per-route statistics.

You can display information to learn resource usage and solve network problems. You can also display information about node reachability and discover the routing path that packets of your device are taking through the network.

You can use any of the privileged EXEC commands in the following table to display various routing statistics.

Table 1: Commands for Displaying System and Network Statistics

Command	Purpose
ping [group-name group-address]	Sends an ICMP Echo Request to a multicast group address.
show ip igmp groups [group-name group-address type number]	Displays the multicast groups that are directly connected to the switch and that were learned through IGMP.
show ip igmp interface [type number]	Displays multicast-related information about an interface.
show ip mcache [group [source]]	Displays the contents of the IP fast-switching cache.
show ip mpacket [source-address name] [group-address name] [detail]	Displays the contents of the circular cache-header buffer.
show ip mroute [group-name group-address] [source] [summary] [count] [active kbps]	Displays the contents of the IP multicast routing table.

Command	Purpose
show ip pim interface [<i>type number</i>] [<i>count</i>] [<i>detail</i>]	Displays information about interfaces configured for PIM. This command is available in all software images.
show ip pim neighbor [<i>type number</i>]	Lists the PIM neighbors discovered by the switch. This command is available in all software images.
show ip pim rp [<i>group-name</i> <i>group-address</i>]	Displays the RP routers associated with a sparse-mode multicast group. This command is available in all software images.
show ip rpf { <i>source-address</i> <i>name</i> }	Displays how the switch is doing Reverse-Path Forwarding (that is, from the unicast routing table, DVMRP routing table, or static mroutes).
show ip sap [<i>group</i> <i>session-name</i> detail]	Displays the Session Announcement Protocol (SAP) Version 2 cache.

Additional References

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	<i>Command Reference, Cisco Release 15.2(2)E (Industrial Ethernet 3010 Switch)</i>
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS IP SLAs commands	Cisco IOS IP Multicast Command Reference

Standards and RFCs

Standard/RFC	Title
—	—

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support