



# Constraining IP Multicast in a Switched Ethernet Network

---

This module describes how to configure routers to use the Cisco Group Management Protocol (CGMP) in switched Ethernet networks to control multicast traffic to Layer 2 switch ports and the Router-Port Group Management Protocol (RGMP) to constrain IP multicast traffic on router-only network segments.

The default behavior for a Layer 2 switch is to forward all multicast traffic to every port that belongs to the destination LAN on the switch. This behavior reduces the efficiency of the switch, whose purpose is to limit traffic to the ports that need to receive the data. This behavior requires a constraining mechanism to reduce unnecessary multicast traffic, which improves switch performance.

## Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

## Finding Feature Information in This Document

Not all features may be supported in your Cisco IOS software release. Use the [“Feature Information for Constraining IP Multicast in a Switched Ethernet Network”](#) to find information about feature support and configuration.

## Contents

- [Prerequisites for Constraining IP Multicast in a Switched Ethernet Network, page 2](#)
- [Information About IP Multicast in a Switched Ethernet Network, page 2](#)
- [How to Constrain Multicast in a Switched Ethernet Network, page 4](#)
- [Configuration Examples for Constraining IP Multicast in a Switched Ethernet Network, page 7](#)
- [Additional References, page 7](#)
- [Feature Information for Constraining IP Multicast in a Switched Ethernet Network, page 8](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

# Prerequisites for Constraining IP Multicast in a Switched Ethernet Network

Before using the tasks in this module, you should be familiar with the concepts described in the “[IP Multicast Technology Overview](#)” module.

## Information About IP Multicast in a Switched Ethernet Network

Before you perform the tasks in this module, you should understand the following concepts:

- [IP Multicast Traffic and Layer 2 Switches, page 2](#)
- [CGMP on Catalyst Switches for IP Multicast, page 2](#)
- [IGMP Snooping, page 3](#)
- [Router-Port Group Management Protocol \(RGMP\), page 3](#)

## IP Multicast Traffic and Layer 2 Switches

The default behavior for a Layer 2 switch is to forward all multicast traffic to every port that belongs to the destination LAN on the switch. This behavior reduces the efficiency of the switch, whose purpose is to limit traffic to the ports that need to receive the data. This behavior requires a constraining mechanism to reduce unnecessary multicast traffic, which improves switch performance.

Three methods that efficiently constrain IP multicast in a Layer 2 switching environment are described in the following sections:

- [CGMP on Catalyst Switches for IP Multicast, page 2](#)
- [IGMP Snooping, page 3](#)
- [Router-Port Group Management Protocol \(RGMP\), page 3](#)

**Note**

---

CGMP and IGMP snooping are used on subnets that include end users or receiver clients. RGMP is used on routed segments that contain only routers, such as in a collapsed backbone.

---

RGMP and CGMP cannot interoperate. However, Internet Group Management Protocol (IGMP) can interoperate with CGMP and RGMP snooping.

## CGMP on Catalyst Switches for IP Multicast

CGMP is a Cisco-developed protocol used on routers connected to Catalyst switches to perform tasks similar to those performed by IGMP. CGMP is necessary for those Catalyst switches that do not distinguish between IP multicast data packets and IGMP report messages, both of which are addressed to the same group address at the MAC level. The switch can distinguish IGMP packets, but would need to use software on the switch, greatly impacting its performance.

You must configure CGMP on the multicast routers and the Layer 2 switches. The result is that, with CGMP, IP multicast traffic is delivered only to those Catalyst switch ports that are attached to interested receivers. All other ports that have not explicitly requested the traffic will not receive it unless these ports are connected to a multicast router. Multicast router ports must receive every IP multicast data packet.

Using CGMP, when a host joins a multicast group, it multicasts an unsolicited IGMP membership report message to the target group. The IGMP report is passed through the switch to the router for normal IGMP processing. The router (which must have CGMP enabled on this interface) receives the IGMP report and processes it as it normally would, but also creates a CGMP Join message and sends it to the switch. The Join message includes the MAC address of the end station and the MAC address of the group it has joined.

The switch receives this CGMP Join message and then adds the port to its content-addressable memory (CAM) table for that multicast group. All subsequent traffic directed to this multicast group is then forwarded out the port for that host.

The Layer 2 switches are designed so that several destination MAC addresses could be assigned to a single physical port. This design allows switches to be connected in a hierarchy and also allows many multicast destination addresses to be forwarded out a single port.

The router port also is added to the entry for the multicast group. Multicast routers must listen to all multicast traffic for every group because IGMP control messages are also sent as multicast traffic. The rest of the multicast traffic is forwarded using the CAM table with the new entries created by CGMP.

## IGMP Snooping

IGMP snooping is an IP multicast constraining mechanism that runs on a Layer 2 LAN switch. IGMP snooping requires the LAN switch to examine, or “snoop,” some Layer 3 information (IGMP Join/Leave messages) in the IGMP packets sent between the hosts and the router. When the switch receives the IGMP host report from a host for a particular multicast group, the switch adds the port number of the host to the associated multicast table entry. When the switch hears the IGMP Leave group message from a host, the switch removes the table entry of the host.

Because IGMP control messages are sent as multicast packets, they are indistinguishable from multicast data at Layer 2. A switch running IGMP snooping must examine every multicast data packet to determine if it contains any pertinent IGMP control information. IGMP snooping implemented on a low-end switch with a slow CPU could have a severe performance impact when data is sent at high rates. The solution is to implement IGMP snooping on high-end switches with special application-specific integrated circuits (ASICs) that can perform the IGMP checks in hardware. CGMP is a better option for low-end switches without special hardware.

## Router-Port Group Management Protocol (RGMP)

CGMP and IGMP snooping are IP multicast constraining mechanisms designed to work on routed network segments that have active receivers. They both depend on IGMP control messages that are sent between the hosts and the routers to determine which switch ports are connected to interested receivers.

Switched Ethernet backbone network segments typically consist of several routers connected to a switch without any hosts on that segment. Because routers do not generate IGMP host reports, CGMP and IGMP snooping will not be able to constrain the multicast traffic, which will be flooded to every port on the VLAN. Routers instead generate Protocol Independent Multicast (PIM) messages to Join and Prune multicast traffic flows at a Layer 3 level.

Router-Port Group Management Protocol (RGMP) is an IP multicast constraining mechanism for router-only network segments. RGMP must be enabled on the routers and on the Layer 2 switches. A multicast router indicates that it is interested in receiving a data flow by sending an RGMP Join message for a particular group. The switch then adds the appropriate port to its forwarding table for that multicast group—similar to the way it handles a CGMP Join message. IP multicast data flows will be forwarded only to the interested router ports. When the router no longer is interested in that data flow, it sends an RGMP Leave message and the switch removes the forwarding entry.

If there are any routers that are not RGMP-enabled, they will continue to receive all multicast data.

## How to Constrain Multicast in a Switched Ethernet Network

This section describes the following tasks:

- [Configuring Switches for IP Multicast, page 4](#)
- [Configuring IGMP Snooping, page 4](#)
- [Enabling CGMP on a Router, page 4](#) (optional)
- [Configuring IP Multicast in a Layer 2 Switched Ethernet Network, page 5](#) (optional)

### Configuring Switches for IP Multicast

If you have switching in your multicast network, consult the documentation for the switch you are working with for information about how to configure IP multicast.

### Configuring IGMP Snooping

No configuration is required on the router. Consult the documentation for the switch you are working with to determine how to enable IGMP snooping and follow the provided instructions.

### Enabling CGMP on a Router

CGMP is a protocol used on routers connected to Catalyst switches to perform tasks similar to those performed by IGMP. CGMP is necessary because the Catalyst 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.

### Restrictions

- CGMP should be enabled only on 802 or ATM media, or LAN emulation (LANE) over ATM.
- CGMP should be enabled only on routers connected to Catalyst switches.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*

4. `ip cgmp [proxy | router-only]`
5. `end`
6. `clear ip cgmp [interface-type interface-number]`

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<code>interface type number</code>  <b>Example:</b> Router(config)# interface ethernet 1	Selects an interface that is connected to hosts on which IGMPv3 can be enabled.
<b>Step 4</b>	<code>ip cgmp [proxy   router-only]</code>  <b>Example:</b> Router(config-if)# ip cgmp proxy	Enables CGMP on an interface of a router connected to a Cisco Catalyst 5000 family switch. <ul style="list-style-type: none"> <li>• The <b>proxy</b> keyword enables the CGMP proxy function. When enabled, any router that is not CGMP-capable will be advertised by the proxy router. The proxy router advertises the existence of other non-CGMP-capable routers by sending a CGMP Join message with the MAC address of the non-CGMP-capable router and group address of 0000.0000.0000.</li> </ul>
<b>Step 5</b>	<code>end</code>  <b>Example:</b> Router(config-if)# end	Ends the current configuration session and returns to EXEC mode.
<b>Step 6</b>	<code>clear ip cgmp [interface-type interface-number]</code>  <b>Example:</b> Router# clear ip cgmp	(Optional) Clears all group entries from the caches of Catalyst switches.

## Configuring IP Multicast in a Layer 2 Switched Ethernet Network

Perform this task to configure IP multicast in a Layer 2 Switched Ethernet network using RGMP.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`

3. **interface** *type number*
4. **ip rgmp**
5. **end**
6. **debug ip rgmp**
7. **show ip igmp interface**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface ethernet 1	Selects an interface that is connected to hosts.
<b>Step 4</b>	<b>ip rgmp</b>  <b>Example:</b> Router(config-if)# ip rgmp	Enables RGMP on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces.
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Router(config-if)# end	Ends the current configuration session and returns to EXEC mode.
<b>Step 6</b>	<b>debug ip rgmp</b>  <b>Example:</b> Router# debug ip rgmp	(Optional) Logs debug messages sent by an RGMP-enabled router.
<b>Step 7</b>	<b>show ip igmp interface</b>  <b>Example:</b> Router# show ip igmp interface	(Optional) Displays multicast-related information about an interface.

# Configuration Examples for Constraining IP Multicast in a Switched Ethernet Network

This section provides the following configuration examples:

- [CGMP Configuration: Example, page 7](#)
- [RGMP Configuration: Example, page 7](#)

## CGMP Configuration: Example

The following example is for a basic network environment where multicast source(s) and multicast receivers are in the same VLAN. The desired behavior is that the switch will constrain the multicast forwarding to those ports that request the multicast stream.

A 4908G-L3 router is connected to the Catalyst 4003 on port 3/1 in VLAN 50. The following configuration is applied on the GigabitEthernet1 interface. Note that there is no **ip multicast-routing** command configured because the router is not routing multicast traffic across its interfaces.

```
interface GigabitEthernet1
 ip address 192.168.50.11 255.255.255.0
 ip pim dense-mode
 ip cgmp
```

## RGMP Configuration: Example

The following example shows how to configure RGMP on a router:

```
ip multicast-routing
ip pim sparse-mode
interface ethernet 0
 ip rgmp
```

## Additional References

The following sections provide references related to constraining IP multicast in a switched Ethernet network.

## Related Documents

Related Topic	Document Title
IP multicast commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<a href="#">Cisco IOS IP Multicast Command Reference</a>

## MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## 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>

# Feature Information for Constraining IP Multicast in a Switched Ethernet Network

[Table 1](#) lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Releases 12.2(1) or later appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator (<http://www.cisco.com/go/fn>). You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click Cancel at the login dialog box and follow the instructions that appear.

**Table 1** *Feature Information for Constraining IP Multicast in a Switched Ethernet Network*

Feature Name	Releases	Feature Configuration Information
Cisco IOS	—	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
CGMP - Cisco Group Management Protocol	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.

