THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

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.

© 2013 Cisco Systems, Inc. All rights reserved.
# CONTENTS

## CHAPTER 1

### IGMP 1

- Finding Feature Information 1
- Information About IGMP 1
  - Role of the Internet Group Management Protocol 1
  - IGMP Version Differences 2
  - IGMP Join Process 5
  - IGMP Leave Process 5
  - IGMP Multicast Addresses 6
- How to Configure IGMP 6
  - Configuring the Device to Forward Multicast Traffic in the Absence of Directly Connected IGMP Hosts 6
  - Controlling Access to an SSM Network Using IGMP Extended Access Lists 8
- Configuration Examples for IGMP 10
  - Example: Configuring the Device to Forward Multicast Traffic in the Absence of Directly Connected IGMP Hosts 10
  - Controlling Access to an SSM Network Using IGMP Extended Access Lists 11
    - Example: Denying All States for a Group G 11
    - Example: Denying All States for a Source S 11
    - Example: Permitting All States for a Group G 12
    - Example: Permitting All States for a Source S 12
    - Example: Filtering a Source S for a Group G 12
- Additional References 12
- Feature Information for IGMP 13

## CHAPTER 2

### IGMP Proxy 15

- Finding Feature Information 15
- Prerequisites for IGMP Proxy 15
- Information About IGMP Proxy 16
IGMP Proxy 16

How to Configure IGMP Proxy 18
  Configuring the Upstream UDL Device for IGMP UDLR 18
  Configuring the Downstream UDL Device for IGMP UDLR with IGMP Proxy Support 19

Configuration Examples for IGMP Proxy 22
  Example: IGMP Proxy Configuration 22

Additional References 23

Feature Information for IGMP Proxy 23

CHAPTER 3

Constraining IP Multicast in a Switched Ethernet Network 25

Finding Feature Information 25

Prerequisites for Constraining IP Multicast in a Switched Ethernet Network 26

Information About IP Multicast in a Switched Ethernet Network 26
  IP Multicast Traffic and Layer 2 Switches 26
  CGMP on Catalyst Switches for IP Multicast 26
  IGMP Snooping 27
  Router-Port Group Management Protocol (RGMP) 27

How to Constrain Multicast in a Switched Ethernet Network 28
  Configuring Switches for IP Multicast 28
  Configuring IGMP Snooping 28
  Enabling CGMP 28
  Configuring IP Multicast in a Layer 2 Switched Ethernet Network 29

Configuration Examples for Constraining IP Multicast in a Switched Ethernet Network 31
  Example: CGMP Configuration 31
  RGMP Configuration Example 31

Additional References 31

Feature Information for Constraining IP Multicast in a Switched Ethernet Network 32
CHAPTER 1

IGMP

This module describes how to configure the Internet Management Group Protocol (IGMP) communications protocol used by hosts and adjacent devices on IP networks to establish multicast group memberships.

- Finding Feature Information, page 1
- Information About IGMP, page 1
- How to Configure IGMP, page 6
- Configuration Examples for IGMP, page 10
- Additional References, page 12
- Feature Information for IGMP, page 13

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.

Information About IGMP

Role of the Internet Group Management Protocol

IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Enabling PIM on an interface also enables IGMP. IGMP provides a means to automatically control and limit the flow of multicast traffic throughout your network with the use of special multicast queriers and hosts.

- A querier is a network device, such as a router, that sends query messages to discover which network devices are members of a given multicast group.
• A host is a receiver, including routers, that sends report messages (in response to query messages) to inform the querier of a host membership. Hosts use IGMP messages to join and leave multicast groups.

Hosts identify group memberships by sending IGMP messages to their local multicast device. Under IGMP, devices listen to IGMP messages and periodically send out queries to discover which groups are active or inactive on a particular subnet.

**IGMP Version Differences**

There are three versions of IGMP, as defined by Request for Comments (RFC) documents of the Internet Engineering Task Force (IETF). IGMPv2 improves over IGMPv1 by adding the ability for a host to signal desire to leave a multicast group and IGMPv3 improves over IGMPv2 mainly by adding the ability to listen to multicast originating from a set of source IP addresses only.

*Table 1: IGMP Versions*

<table>
<thead>
<tr>
<th>IGMP Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMPv1</td>
<td>Provides the basic query-response mechanism that allows the multicast device to determine which multicast groups are active and other processes that enable hosts to join and leave a multicast group. RFC 1112 defines the IGMPv1 host extensions for IP multicasting.</td>
</tr>
<tr>
<td>IGMPv2</td>
<td>Extends IGMP, allowing such capabilities as the IGMP leave process, group-specific queries, and an explicit maximum response time field. IGMPv2 also adds the capability for devices to elect the IGMP querier without dependence on the multicast protocol to perform this task. RFC 2236 defines IGMPv2.</td>
</tr>
<tr>
<td>IGMPv3</td>
<td>Provides for source filtering, which enables a multicast receiver host to signal to a device which groups it wants to receive multicast traffic from, and from which sources this traffic is expected. In addition, IGMPv3 supports the link local address 224.0.0.22, which is the destination IP address for IGMPv3 membership reports; all IGMPv3-capable multicast devices must listen to this address. RFC 3376 defines IGMPv3.</td>
</tr>
</tbody>
</table>
By default, enabling a PIM on an interface enables IGMPv2 on that device. IGMPv2 was designed to be as backward compatible with IGMPv1 as possible. To accomplish this backward compatibility, RFC 2236 defined special interoperability rules. If your network contains legacy IGMPv1 hosts, you should be familiar with these interoperability rules. For more information about IGMPv1 and IGMPv2 interoperability, see RFC 2236, Internet Group Management Protocol, Version 2.

**Note**

**Devices That Run IGMPv1**

IGMPv1 devices send IGMP queries to the “all-hosts” multicast address of 224.0.0.1 to solicit multicast groups with active multicast receivers. The multicast receivers also can send IGMP reports to the device to notify it that they are interested in receiving a particular multicast stream. Hosts can send the report asynchronously or in response to the IGMP queries sent by the device. If more than one multicast receiver exists for the same multicast group, only one of these hosts sends an IGMP report message; the other hosts suppress their report messages.

In IGMPv1, there is no election of an IGMP querier. If more than one device on the segment exists, all the devices send periodic IGMP queries. IGMPv1 has no special mechanism by which the hosts can leave the group. If the hosts are no longer interested in receiving multicast packets for a particular group, they simply do not reply to the IGMP query packets sent from the device. The device continues sending query packets. If the device does not hear a response in three IGMP queries, the group times out and the device stops sending multicast packets on the segment for the group. If the host later wants to receive multicast packets after the timeout period, the host simply sends a new IGMP join to the device, and the device begins to forward the multicast packet again.

If there are multiple devices on a LAN, a designated router (DR) must be elected to avoid duplicating multicast traffic for connected hosts. PIM devices follow an election process to select a DR. The PIM device with the highest IP address becomes the DR.

The DR is responsible for the following tasks:

- Sending PIM register and PIM Join and Prune messages toward the rendezvous point (RP) to inform it about host group membership.
- Sending IGMP host-query messages.
- Sending host-query messages by default every 60 seconds in order to keep the IGMP overhead on hosts and networks very low.

**Devices That Run IGMPv2**

IGMPv2 improves the query messaging capabilities of IGMPv1.

The query and membership report messages in IGMPv2 are identical to the IGMPv1 messages with two exceptions:

- IGMPv2 query messages are broken into two categories: general queries (identical to IGMPv1 queries) and group-specific queries.
- IGMPv1 membership reports and IGMPv2 membership reports have different IGMP type codes.

IGMPv2 also enhances IGMP by providing support for the following capabilities:

- Querier election process--Provides the capability for IGMPv2 devices to elect the IGMP querier without having to rely on the multicast routing protocol to perform the process.
• Maximum Response Time field--A new field in query messages permits the IGMP querier to specify the maximum query-response time. This field permits the tuning of the query-response process to control response burstiness and to fine-tune leave latencies.

• Group-Specific Query messages--Permits the IGMP querier to perform the query operation on a specific group instead of all groups.

• Leave-Group messages--Provides hosts with a method of notifying devices on the network that they wish to leave the group.

Unlike IGMPv1, in which the DR and the IGMP querier are typically the same device, in IGMPv2 the two functions are decoupled. The DR and the IGMP querier are selected based on different criteria and may be different devices on the same subnet. The DR is the device with the highest IP address on the subnet, whereas the IGMP querier is the device with the lowest IP address.

Query messages are used to elect the IGMP querier as follows:

1. When IGMPv2 devices start, they each multicast a general query message to the all-systems group address of 224.0.0.1 with their interface address in the source IP address field of the message.

2. When an IGMPv2 device receives a general query message, the device compares the source IP address in the message with its own interface address. The device with the lowest IP address on the subnet is elected the IGMP querier.

3. All devices (excluding the querier) start the query timer, which is reset whenever a general query message is received from the IGMP querier. If the query timer expires, it is assumed that the IGMP querier has gone down, and the election process is performed again to elect a new IGMP querier.

By default, the timer is two times the query interval.

Devices Running IGMPv3

IGMPv3 adds support for source filtering, which enables a multicast receiver host to signal to a device which groups it wants to receive multicast traffic from, and from which sources this traffic is expected. This membership information enables the software to forward traffic only from those sources from which receivers requested the traffic.

IGMPv3 supports applications that explicitly signal sources from which they want to receive traffic. With IGMPv3, receivers signal membership to a multicast group in the following two modes:

• INCLUDE mode--In this mode, the receiver announces membership to a group and provides a list of IP addresses (the INCLUDE list) from which it wants to receive traffic.

• EXCLUDE mode--In this mode, the receiver announces membership to a group and provides a list of IP addresses (the EXCLUDE list) from which it does not want to receive traffic. In other words, the host wants to receive traffic only from sources whose IP addresses are not listed in the EXCLUDE list. To receive traffic from all sources, like in the case of the Internet Standard Multicast (ISM) service model, a host expresses EXCLUDE mode membership with an empty EXCLUDE list.

IGMPv3 is the industry-designated standard protocol for hosts to signal channel subscriptions in an SSM network environment. For SSM to rely on IGMPv3, IGMPv3 must be available in the network stack portion of the operating systems running on the last hop devices and hosts and be used by the applications running on those hosts.

In IGMPv3, hosts send their membership reports to 224.0.0.22; all IGMPv3 devices, therefore, must listen to this address. Hosts, however, do not listen or respond to 224.0.0.22; they only send their reports to that address.
In addition, in IGMPv3, there is no membership report suppression because IGMPv3 hosts do not listen to the reports sent by other hosts. Therefore, when a general query is sent out, all hosts on the wire respond.

**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 it wants to join. The IGMP join process is the same for IGMPv1 and IGMPv2 hosts.

In IGMPv3, the join process for hosts proceeds as follows:

- When a host wants to join a group, it sends an IGMPv3 membership report to 224.0.0.22 with an empty EXCLUDE list.
- When a host wants to join a specific channel, it sends an IGMPv3 membership report to 224.0.0.22 with the address of the specific source included in the INCLUDE list.
- When a host wants to join a group excluding particular sources, it sends an IGMPv3 membership report to 224.0.0.22 excluding those sources in the EXCLUDE list.

**Note**

If some IGMPv3 hosts on a LAN wish to exclude a source and others wish to include the source, then the device will send traffic for the source on the LAN (that is, inclusion trumps exclusion in this situation).

**IGMP Leave Process**

The method that hosts use to leave a group varies depending on the version of IGMP in operation.

**IGMPv1 Leave Process**

There is no leave-group message in IGMPv1 to notify the devices on the subnet that a host no longer wants to receive the multicast traffic from a specific group. The host simply stops processing traffic for the multicast group and ceases responding to IGMP queries with IGMP membership reports for the group. As a result, the only way IGMPv1 devices know that there are no longer any active receivers for a particular multicast group on a subnet is when the devices stop receiving membership reports. To facilitate this process, IGMPv1 devices associate a countdown timer with an IGMP group on a subnet. When a membership report is received for the group on the subnet, the timer is reset. For IGMPv1 devices, this timeout interval is typically three times the query interval (3 minutes). This timeout interval means that the device may continue to forward multicast traffic onto the subnet for up to 3 minutes after all hosts have left the multicast group.

**IGMPv2 Leave Process**

IGMPv2 incorporates a leave-group message that provides the means for a host to indicate that it wishes to stop receiving multicast traffic for a specific group. When an IGMPv2 host leaves a multicast group, if it was the last host to respond to a query with a membership report for that group, it sends a leave-group message to the all-devices multicast group (224.0.0.2).
**IGMPv3 Leave Process**

IGMPv3 enhances the leave process by introducing the capability for a host to stop receiving traffic from a particular group, source, or channel in IGMP by including or excluding sources, groups, or channels in IGMPv3 membership reports.

**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.

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 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 device is querying.
- IGMP group membership reports are destined to the group IP address for which the device is reporting.
- IGMPv2 leave-group messages are destined to the address 224.0.0.2 (all devices on a subnet).
- IGMPv3 membership reports are destined to the address 224.0.0.22; all IGMPv3-capable multicast devices must listen to this address.

**How to Configure IGMP**

**Configuring the Device to Forward Multicast Traffic in the Absence of Directly Connected IGMP Hosts**

Perform this optional task to configure the device to forward multicast traffic in the absence of directly connected IGMP hosts.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type number
4. Do one of the following:
   - ip igmp join-group group-address
   - ip igmp static-group { * | group-address [source source-address] }
5. end
6. show ip igmp interface [interface-type interface-number]
# DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| Example: | Device> enable | |
| Step 2 | configure terminal | Enters global configuration mode. |
| Example: | Device# configure terminal | |
| Step 3 | interface type number | Enters interface configuration mode.  
  • For the type and number arguments, specify an interface that is connected to hosts. |
| Example: | Device(config)# interface gigabitethernet 1 | |
| Step 4 | Do one of the following:  
  • ip igmp join-group group-address  
  • ip igmp static-group {* | group-address [source source-address]}} | The first sample shows how to configure an interface on the device to join the specified group.  
  • With this method, the device accepts the multicast packets in addition to forwarding them. Accepting the multicast packets prevents the device from fast switching.  
  The second example shows how to configure static group membership entries on an interface.  
  • With this method, the device does not accept the packets itself, but only forwards them. Hence, this method allows fast switching. The outgoing interface appears in the IGMP cache, but the device itself is not a member, as evidenced by lack of an “L” (local) flag in the multicast route entry. |
| Example: | Device(config-if)# ip igmp join-group 225.2.2.2 | |
| Example: | Device(config-if)# ip igmp static-group 225.2.2.2 | |
| Step 5 | end | Returns to privileged EXEC mode. |
| Example: | Device(config-if)# end | |
| Step 6 | show ip igmp interface [interface-type interface-number] | (Optional) Displays multicast-related information about an interface. |
| Example: | Device# show ip igmp interface | |
Controlling Access to an SSM Network Using IGMP Extended Access Lists

Perform this optional task to control access to an SSM network by using an IGMP extended access list that filters SSM traffic based on source address, group address, or both.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **ip multicast-routing [distributed]**
4. **ip pim ssm {default | range access-list}**
5. **ip access-list extended access-list-name**
6. **deny igmp source source-wildcard destination destination-wildcard [igmp-type] [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]**
7. **permit igmp source source-wildcard destination destination-wildcard [igmp-type] [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]**
8. **exit**
9. **interface type number**
10. **ip igmp access-group access-list**
11. **ip pim sparse-mode**
12. Repeat Steps 1 through 11 on all interfaces that require access control of SSM channel membership.
13. **ip igmp version 3**
14. Repeat Step 13 on all host-facing interfaces.
15. **end**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>ip multicast-routing [distributed]</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config)# ip multicast-routing distributed</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`ip pim ssm {default</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# ip pim ssm default</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# ip pim ssm range 10.1.2.0/16</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# ip pim ssm range 232/8</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# ip pim ssm range 232.1.0.0/16</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>ip access-list extended access-list -name</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ip access-list extended mygroup</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>deny igmp source source-wildcard destination destination-wildcard [igmp-type] [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-ext-nacl)# deny igmp host 10.1.2.3 any</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>permit igmp source source-wildcard destination destination-wildcard [igmp-type] [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-ext-nacl)# permit igmp any any</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>exit</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-ext-nacl)# exit</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 9</td>
<td>interface type number</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# interface ethernet 0</td>
</tr>
<tr>
<td></td>
<td>Selects an interface that is connected to hosts on which IGMPv3 can be enabled.</td>
</tr>
<tr>
<td>Step 10</td>
<td>ip igmp access-group  access-list</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# ip igmp access-group mygroup</td>
</tr>
<tr>
<td></td>
<td>Applies the specified access list to IGMP reports.</td>
</tr>
<tr>
<td>Step 11</td>
<td>ip pim sparse-mode</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# ip pim sparse-mode</td>
</tr>
<tr>
<td></td>
<td>Enables PIM-SM on the interface.</td>
</tr>
<tr>
<td></td>
<td>Note You must use sparse mode.</td>
</tr>
<tr>
<td>Step 12</td>
<td>Repeat Steps 1 through 11 on all interfaces that require access control of SSM channel membership.</td>
</tr>
<tr>
<td></td>
<td>--</td>
</tr>
<tr>
<td>Step 13</td>
<td>ip igmp version 3</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# ip igmp version 3</td>
</tr>
<tr>
<td></td>
<td>Enables IGMPv3 on this interface. The default version of IGMP is IGMP version 2. Version 3 is required by SSM.</td>
</tr>
<tr>
<td>Step 14</td>
<td>Repeat Step 13 on all host-facing interfaces.</td>
</tr>
<tr>
<td></td>
<td>--</td>
</tr>
<tr>
<td>Step 15</td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# end</td>
</tr>
<tr>
<td></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

### Configuratio Examples for IGMP

#### Example: Configuring the Device to Forward Multicast Traffic in the Absence of Directly Connected IGMP Hosts

The following example shows how to configure a device to forward multicast traffic in the absence of directly connected IGMP hosts using the **ip igmp join-group** command. With this method, the device accepts the multicast packets in addition to forwarding them. Accepting the multicast packets prevents the device from fast switching.
In this example, Fast Ethernet interface 0/0/0 on the device is configured to join the group 225.2.2.2:

```plaintext
interface FastEthernet0/0/0
 ip igmp join-group 225.2.2.2
```

The following example shows how to configure a device to forward multicast traffic in the absence of directly connected IGMP hosts using the `ip igmp static-group` command. With this method, the device does not accept the packets itself, but only forwards them. Hence, this method allows fast switching. The outgoing interface appears in the IGMP cache, but the device itself is not a member, as evidenced by lack of an “L” (local) flag in the multicast route entry.

In this example, static group membership entries for group 225.2.2.2 are configured on Fast Ethernet interface 0/1/0:

```plaintext
interface FastEthernet0/1/0
 ip igmp static-group 225.2.2.2
```

---

**Controlling Access to an SSM Network Using IGMP Extended Access Lists**

This section contains the following configuration examples for controlling access to an SSM network using IGMP extended access lists:

---

**Note**

Keep in mind that access lists are very flexible: there are many combinations of permit and deny statements one could use in an access list to filter multicast traffic. The examples in this section simply provide a few examples of how it can be done.

---

**Example: Denying All States for a Group G**

The following example shows how to deny all states for a group G. In this example, Fast Ethernet interface 0/0/0 is configured to filter all sources for SSM group 232.2.2.2 in IGMPv3 reports, which effectively denies this group.

```plaintext
ip access-list extended test1
 deny igmp any host 232.2.2.2
 permit igmp any any
!
interface FastEthernet0/0/0
 ip igmp access-group test1
```

**Example: Denying All States for a Source S**

The following example shows how to deny all states for a source S. In this example, Gigabit Ethernet interface 1/1/0 is configured to filter all groups for source 10.2.1.32 in IGMPv3 reports, which effectively denies this source.

```plaintext
ip access-list extended test2
 deny igmp host 10.2.1.32 any
 permit igmp any any
!
interface GigabitEthernet1/1/0
 ip igmp access-group test2
```
Example: Permitting All States for a Group G

The following example shows how to permit all states for a group G. In this example, Gigabit Ethernet interface 1/2/0 is configured to accept all sources for SSM group 232.1.1.10 in IGMPv3 reports, which effectively accepts this group altogether.

```
ip access-list extended test3
   permit igmp any host 232.1.1.10
!interface GigabitEthernet1/2/0
   ip igmp access-group test3
```

Example: Permitting All States for a Source S

The following example shows how to permit all states for a source S. In this example, Gigabit Ethernet interface 1/2 is configured to accept all groups for source 10.6.23.32 in IGMPv3 reports, which effectively accepts this source altogether.

```
ip access-list extended test4
   permit igmp host 10.6.23.32 any
!interface GigabitEthernet1/2/0
   ip igmp access-group test4
```

Example: Filtering a Source S for a Group G

The following example shows how to filter a particular source S for a group G. In this example, Gigabit Ethernet interface 0/3/0 is configured to filter source 232.2.2.2 for SSM group 232.2.30.30 in IGMPv3 reports.

```
ip access-list extended test5
   deny igmp host 10.4.4.4 host 232.2.30.30
   permit igmp any any
!interface GigabitEthernet0/3/0
   ip igmp access-group test5
```

Additional References

The following sections provide references related to customizing IGMP.

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>Cisco IOS IP SLAs commands</td>
<td>Cisco IOS IP Multicast Command Reference</td>
</tr>
<tr>
<td>Overview of the IP multicast technology area</td>
<td>“ IP Multicast Technology Overview ” module</td>
</tr>
<tr>
<td>Basic IP multicast concepts, configuration tasks, and examples</td>
<td>“ Configuring Basic IP Multicast ” or “Configuring IP Multicast in IPv6 Networks” module</td>
</tr>
</tbody>
</table>
Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1112</td>
<td>Host extensions for IP multicasting</td>
</tr>
<tr>
<td>RFC 2236</td>
<td>Internet Group Management Protocol, Version 2</td>
</tr>
<tr>
<td>RFC 3376</td>
<td>Internet Group Management Protocol, Version 3</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by these features, and support for existing MIBs has not been modified by these features.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS XE 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></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for IGMP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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.
## Table 2: Feature Information for IGMP

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP</td>
<td>—</td>
<td>Provides the basic query-response mechanism that allows the multicast device to determine which multicast groups are active and other processes that enable hosts to join and leave a multicast group. RFC 1112 defines the IGMPv1 host extensions for IP multicasting.</td>
</tr>
<tr>
<td>IGMP version 2</td>
<td>12.2(27)SBB</td>
<td>Extends IGMP, allowing such capabilities as the IGMP leave process, group-specific queries, and an explicit maximum response time field. IGMPv2 also adds the capability for routers to elect the IGMP querier without dependence on the multicast protocol to perform this task.</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 2.1</td>
<td></td>
</tr>
<tr>
<td>IGMP version 3</td>
<td>12.2(27)SBB</td>
<td>Provides for source filtering, which enables a multicast receiver host to signal to a router which groups it wants to receive multicast traffic from, and from which sources this traffic is expected. In addition, IGMPv3 supports the link local address 224.0.0.22, which is the destination IP address for IGMPv3 membership reports; all IGMPv3-capable multicast routers must listen to this address.</td>
</tr>
<tr>
<td></td>
<td>12.4(15)T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 2.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 3.2SE</td>
<td></td>
</tr>
</tbody>
</table>
IGMP Proxy

This module describes how to configure IGMP proxy to enable a device to send an IGMP report to a specified destination IP address.

- Finding Feature Information, page 15
- Prerequisites for IGMP Proxy, page 15
- Information About IGMP Proxy, page 16
- How to Configure IGMP Proxy, page 18
- Configuration Examples for IGMP Proxy, page 22
- Additional References, page 23
- Feature Information for IGMP Proxy, page 23

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 IGMP Proxy

- All devices on the IGMP UDL have the same subnet address. If all devices on the UDL cannot have the same subnet address, the upstream device must be configured with secondary addresses to match all of the subnets to which the downstream devices are attached.
- IP multicast is enabled and the PIM interfaces are configured.
Use the following guidelines when configuring PIM interfaces for IGMP proxy:

- Use PIM sparse mode (PIM-SM) when the interface is operating in a sparse-mode region and you are running static RP, bootstrap (BSR), or Auto-RP with the Auto-RP listener capability.
- Use PIM sparse-dense mode when the interface is running in a sparse-dense mode region and you are running Auto-RP without the Auto-RP listener capability.
- Use PIM dense mode (PIM-DM) when the interface is operating in dense mode and is, thus, participating in a dense-mode region.
- Use PIM-DM with the proxy-register capability when the interface is receiving source traffic from a dense-mode region that needs to reach receivers that are in a sparse-mode region.

Information About IGMP Proxy

IGMP Proxy

An IGMP proxy enables hosts in a unidirectional link routing (UDLR) environment that are not directly connected to a downstream router to join a multicast group sourced from an upstream network.

The figure below illustrates a sample topology that shows two UDLR scenarios:

- Traditional UDL routing scenario--A UDL device with directly connected receivers.
- IGMP proxy scenario--UDL device without directly connected receivers.

IGMP UDLs are needed on the upstream and downstream devices.
Scenario 1--Traditional UDLR Scenario (UDL Device with Directly Connected Receivers)

For scenario 1, no IGMP proxy mechanism is needed. In this scenario, the following sequence of events occurs:

1. User 2 sends an IGMP membership report requesting interest in group G.
2. Router B receives the IGMP membership report, adds a forwarding entry for group G on LAN B, and proxies the IGMP report to Router A, which is the UDLR upstream device.
3. The IGMP report is then proxied across the Internet link.
4. Router A receives the IGMP proxy and maintains a forwarding entry on the unidirectional link.

Scenario 2--IGMP Proxy Scenario (UDL Device without Directly Connected Receivers)

For scenario 2, the IGMP proxy mechanism is needed to enable hosts that are not directly connected to a downstream device to join a multicast group sourced from an upstream network. In this scenario, the following sequence of events occurs:

1. User 1 sends an IGMP membership report requesting interest in group G.
2. Router C sends a PIM Join message hop-by-hop to the RP (Router B).
3. Router B receives the PIM Join message and adds a forwarding entry for group G on LAN B.
4. Router B periodically checks its mroute table and proxies the IGMP membership report to its upstream UDL device across the Internet link.
Router A creates and maintains a forwarding entry on the unidirectional link (UDL).

In an enterprise network, it is desirable to be able to receive IP multicast traffic via satellite and forward the traffic throughout the network. With unidirectional link routing (UDLR) alone, scenario 2 would not be possible because receiving hosts must be directly connected to the downstream device, Router B. The IGMP proxy mechanism overcomes this limitation by creating an IGMP report for (*, G) entries in the multicast forwarding table. To make this scenario functional, therefore, you must enable IGMP report forwarding of proxied (*, G) multicast static route (mroute) entries (using the `ip igmp mroute-proxy` command) and enable the mroute proxy service (using the `ip igmp proxy-service` command) on interfaces leading to PIM-enabled networks with potential members.

Because PIM messages are not forwarded upstream, each downstream network and the upstream network have a separate domain.

## How to Configure IGMP Proxy

### Configuring the Upstream UDL Device for IGMP UDLR

Perform this task to configure the upstream UDL device for IGMP UDLR.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `ip igmp unidirectional-link`
5. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>interface type number</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

#### Example:

Device(config)# interface gigabitethernet 1/0/0

- For the `type` and `number` arguments, specify the interface to be used as the UDL on the upstream device.

### Purpose

#### Step 4

**ip igmp unidirectional-link**

**Example:**

Device(config-if)# ip igmp unidirectional-link

Configures IGMP on the interface to be unidirectional for IGMP UDLR.

#### Step 5

**end**

**Example:**

Device(config-if)# end

Ends the current configuration session and returns to privileged EXEC mode.

---

**Configuring the Downstream UDL Device for IGMP UDLR with IGMP Proxy Support**

Perform this task to configure the downstream UDL device for IGMP UDLR with IGMP proxy support.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface *type* *number*
4. ip igmp unidirectional-link
5. exit
6. interface *type* *number*
7. ip igmp mroute-proxy *type* *number*
8. exit
9. interface *type* *number*
10. ip igmp helper-address udl *interface-type* *interface-number*
11. ip igmp proxy-service
12. end
13. show ip igmp interface
14. show ip igmp udlr
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface gigabitethernet 0/0/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip igmp unidirectional-link</td>
<td>Configures IGMP on the interface to be unidirectional for IGMP UDLR.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# ip igmp unidirectional-link</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits interface configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> interface type number</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface gigabitethernet 1/0/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> ip igmp mroute-proxy type number</td>
<td>Enables IGMP report forwarding of proxied (*, G) multicast static route (mroute) entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# ip igmp mroute-proxy loopback 0</td>
<td></td>
</tr>
</tbody>
</table>

- For the type and number arguments, specify the interface to be used as the UDL on the downstream device for IGMP UDLR.
- For the type and number arguments, select an interface that is facing the nondirectly connected hosts.
- This step is performed to enable the forwarding of IGMP reports to a proxy service interface for all (*, G) forwarding entries in the multicast forwarding table.
- In this example, the ip igmp mroute-proxy command is configured on Gigabit Ethernet interface 1/0/0 to request that IGMP reports be sent to loopback interface 0 for all groups in the mroute table that are forwarded to Gigabit Ethernet interface 1/0/0.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>exit</td>
<td>Exits interface configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# exit</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>interface type number</td>
<td>Enters interface configuration mode for the specified interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# interface loopback 0</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>ip igmp helper-address udl interface-type interface-number</td>
<td>Configures IGMP helpering for UDLR.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# ip igmp helper-address udl gigabitethernet 0/0/0</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>ip igmp proxy-service</td>
<td>Enables the mroute proxy service.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# ip igmp proxy-service</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>end</td>
<td>Ends the current configuration session and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>
### Configuration Examples for IGMP Proxy

#### Example: IGMP Proxy Configuration

The following example shows how to configure the upstream UDL device for IGMP UDLR and the downstream UDL device for IGMP UDLR with IGMP proxy support.

**Upstream Device Configuration**

```plaintext
interface gigabitethernet 0/0/0
 ip address 10.1.1.1 255.255.255.0
 ip pim dense-mode

interface gigabitethernet 1/0/0
 ip address 10.2.1.1 255.255.255.0
 ip pim dense-mode
 ip igmp unidirectional-link

interface gigabitethernet 2/0/0
 ip address 10.3.1.1 255.255.255.0
```

**Downstream Device Configuration**

```plaintext
ip pim rp-address 10.5.1.1 5
 access-list 5 permit 239.0.0.0 0.255.255.255

interface loopback 0
 ip address 10.7.1.1 255.255.255.0
 ip pim dense-mode
 ip igmp helper-address udl ethernet 0
 ip igmp proxy-service

interface gigabitethernet 0/0/0
 ip address 10.2.1.2 255.255.255.0
 ip pim dense-mode
 ip igmp unidirectional-link

interface gigabitethernet 1/0/0
 ip address 10.5.1.1 255.255.255.0
```
ip pim sparse-mode
ip igmp mroute-proxy loopback 0
!
interface gigabitethernet 2/0/0
ip address 10.6.1.1 255.255.255.0

## Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>Cisco IOS IP Multicast commands</td>
<td>Cisco IOS IP Multicast Command Reference</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS XE 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></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

## Feature Information for IGMP Proxy

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.
Table 3: Feature Information for IGMP Proxy

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Proxy</td>
<td>Cisco IOS XE Release 3.2SE</td>
<td>IGMP proxy enables hosts in a unidirectional link routing (UDLR) environment that are not directly connected to a downstream router to join a multicast group sourced from an upstream network. The following commands were introduced or modified: <code>ip igmp helper-address</code>, <code>ip igmp mroute-proxy</code>, <code>ip igmp proxy-service</code>, <code>ip igmp unidirectional-link</code>.</td>
</tr>
</tbody>
</table>
CHAPTER 3

Constraining IP Multicast in a Switched Ethernet Network

This module describes how to configure devices 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 routing device-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.

- Finding Feature Information, page 25
- Prerequisites for Constraining IP Multicast in a Switched Ethernet Network, page 26
- Information About IP Multicast in a Switched Ethernet Network, page 26
- How to Constrain Multicast in a Switched Ethernet Network, page 28
- Configuration Examples for Constraining IP Multicast in a Switched Ethernet Network, page 31
- Additional References, page 31
- Feature Information for Constraining IP Multicast in a Switched Ethernet Network, page 32

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 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

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.

Cisco Group Management Protocol (CGMP), Router Group Management Protocol (RGMP), and IGMP snooping efficiently constrain IP multicast in a Layer 2 switching environment.

- 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 device 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 device 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 device port also is added to the entry for the multicast group. Multicast device 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

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

CGMP is a protocol used on devices 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.

Note

- CGMP should be enabled only on 802 or ATM media, or LAN emulation (LANE) over ATM.
- CGMP should be enabled only on devices 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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number</td>
<td>Selects an interface that is connected to hosts on which IGMPv3 can be enabled.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# interface ethernet 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip cgmp [proxy</td>
<td>router-only]</td>
<td>Enables CGMP on an interface of a device connected to a Cisco Catalyst 5000 family switch.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# ip cgmp proxy</td>
<td>• The <code>proxy</code> keyword enables the CGMP proxy function. When enabled, any device that is not CGMP-capable will be advertised by the proxy router. The proxy router advertises the existence of other non-CGMP-capable devices by sending a CGMP Join message with the MAC address of the non-CGMP-capable device and group address of 0000.0000.0000.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Ends the current configuration session and returns to EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# end</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> clear ip cgmp [interface-type interface-number]</td>
<td>(Optional) Clears all group entries from the caches of Catalyst switches.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Device# clear ip cgmp</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type number</td>
<td>Selects an interface that is connected to hosts.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# interface ethernet 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip rgmp</td>
<td>Enables RGMP on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# ip rgmp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Ends the current configuration session and returns to EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> debug ip rgmp</td>
<td>(Optional) Logs debug messages sent by an RGMP-enabled device.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# debug ip rgmp</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>Command or Action</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>show ip igmp interface</td>
</tr>
</tbody>
</table>

Example: CGMP Configuration

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.

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
</tbody>
</table>
Feature Information for Constraining IP Multicast in a Switched Ethernet Network

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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.

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a></td>
</tr>
</tbody>
</table>
## Table 4: Feature Information for Constraining IP Multicast in a Switched Ethernet Network

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS</td>
<td>--</td>
<td>For information about feature support in Cisco IOS software, use Cisco Feature Navigator.</td>
</tr>
</tbody>
</table>