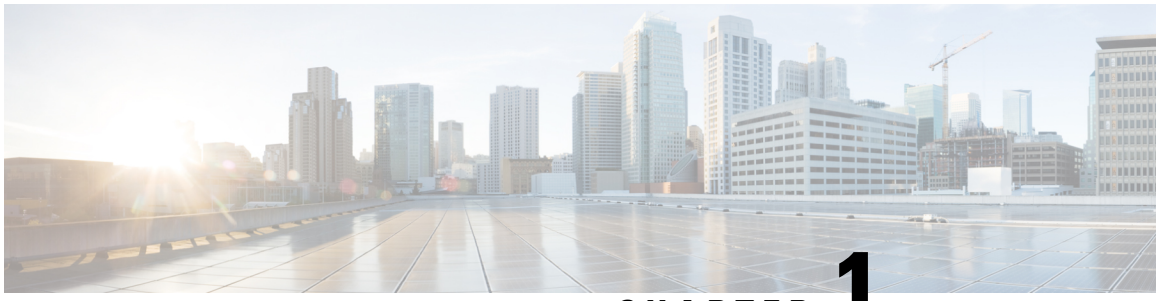
IP Multicast: IGMP Configuration Guide, Cisco IOS XE Gibraltar 16.10.x

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E (for Catalyst Switching) and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Feature Information

Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

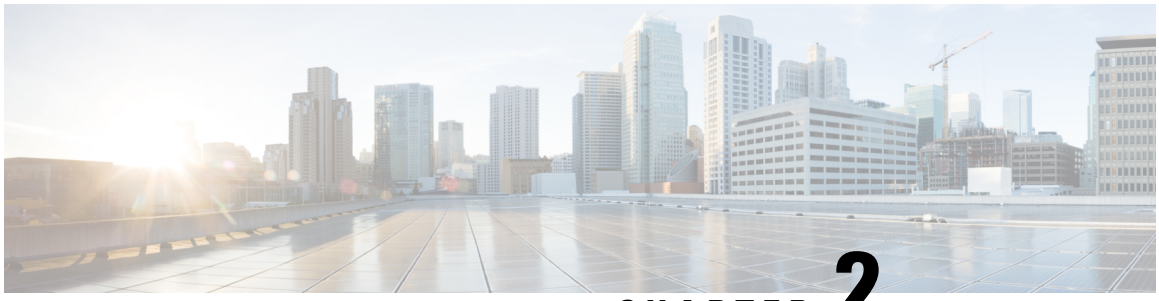
Related References

- Cisco IOS Command References, All Releases

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.



CHAPTER 2

Customizing IGMP

Internet Group Management Protocol (IGMP) is used to dynamically register individual hosts in a multicast group on a particular LAN segment. Enabling Protocol Independent Multicast (PIM) on an interface also enables IGMP operation on that interface.

This module describes ways to customize IGMP, including how to:

- Configure the router to forward multicast traffic in the absence of directly connected IGMP hosts.
- Enable an IGMP Version 3 (IGMPv3) host stack so that the router can function as a multicast network endpoint or host.
- Enable routers to track each individual host that is joined to a particular group or channel in an IGMPv3 environment.
- Control access to an SSM network using IGMP extended access lists.
- Configure an IGMP proxy that enables hosts that are not directly connected to a downstream router to join a multicast group sourced from an upstream network.

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.

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

- Before performing the tasks in this module, you should be familiar with the concepts explained in the "IP Multicast Routing Technology Overview" module.
- The tasks in this module assume that IP multicast has been enabled and that the Protocol Independent Multicast (PIM) interfaces have been configured using the tasks described in the "Configuring IP Multicast Routing" module.

Restrictions for Customizing IGMP

Traffic Filtering with Multicast Groups That Are Not Configured in SSM Mode

IGMPv3 membership reports are not utilized by the software to filter or restrict traffic for multicast groups that are not configured in Source Specific Multicast (SSM) mode. Effectively, Cisco IOS software interprets all IGMPv3 membership reports for groups configured in dense, sparse, or bidirectional mode to be group membership reports and forwards traffic from all active sources onto the network.

Interoperability with IGMP Snooping

You must be careful when using IGMPv3 with switches that support and are enabled for IGMP snooping, because IGMPv3 messages are different from the messages used in IGMP Version 1 (IGMPv1) and Version 2 (IGMPv2). If a switch does not recognize IGMPv3 messages, then hosts will not correctly receive traffic if IGMPv3 is being used. In this case, either IGMP snooping may be disabled on the switch or the router may be configured for IGMPv2 on the interface, which would remove the ability to use SSM for host applications that cannot resort to URL Rendezvous Directory (URD) or IGMP v3lite.

Interoperability with CGMP

Networks using Cisco Group Management Protocol (CGMP) will have better group leave behavior if they are configured with IGMPv2 than IGMPv3. If CGMP is used with IGMPv2 and the switch is enabled for the CGMP leave functionality, then traffic to a port joined to a multicast group will be removed from the port shortly after the last member on that port has dropped membership to that group. This fast-leave mechanism is part of IGMPv2 and is specifically supported by the CGMP fast-leave enabled switch.

With IGMPv3, there is currently no CGMP switch support of fast leave. If IGMPv3 is used in a network, CGMP will continue to work, but CGMP fast-leave support is ineffective and the following conditions apply:

- Each time a host on a new port of the CGMP switch joins a multicast group, that port is added to the list of ports to which the traffic of this group is sent.
- If all hosts on a particular port leave the multicast group, but there are still hosts on other ports (in the same virtual LAN) joined to the group, then nothing happens. In other words, the port continues to receive traffic from that multicast group.
- Only when the last host in a virtual LAN (VLAN) has left the multicast group does forwarding of the traffic of this group into the VLAN revert to no ports on the forwarding switch.

This join behavior only applies to multicast groups that actually operate in IGMPv3 mode. If legacy hosts only supporting IGMPv2 are present in the network, then groups will revert to IGMPv2 and fast leave will work for these groups.

If fast leave is needed with CGMP-enabled switches, we recommend that you not enable IGMPv3 but configure IGMPv2 on that interface.

If you want to use SSM, you need IGMPv3 and you have two configuration alternatives, as follows:

- Configure only the interface for IGMPv2 and use IGMP v3lite and URD.
- Enable IGMPv3 and accept the higher leave latencies through the CGMP switch.

Information About Customizing 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 Versions 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

IGMP Version	Description
IGMPv1	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.

IGMP Version	Description
IGMPv2	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.

Note 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 operability rules. For more information about IGMPv1 and IGMPv2 interoperability, see RFC 2236, Internet Group Management Protocol, Version 2 .

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.

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 hosts 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.

Extended ACL Support for IGMP to Support SSM in IPv4

The Extended ACL Support for IGMP to Support SSM in IPv4 feature enables IGMPv3 to accommodate extended access lists. IGMPv3 support of extended access lists allows you to leverage an important advantage of SSM in IPv4, that of filtering IGMPv3 reports based on source address, group address, or both.

Benefits of Extended Access List Support for IGMP to Support SSM in IPv4

IGMPv3 accommodates extended access lists, which allow you to leverage an important advantage of SSM in IPv4, that of basing access on source IP address. Prior to this feature, an IGMP access list accepted only a standard access list, allowing membership reports to be filtered based only on multicast group addresses.

IGMPv3 allows multicast receivers not only to join to groups, but to groups including or excluding sources. For appropriate access control, it is therefore necessary to allow filtering of IGMPv3 messages not only by group addresses reported, but by group and source addresses. IGMP extended access lists introduce this functionality. Using SSM with an IGMP extended access list (ACL) allows you to permit or deny source S and group G (S, G) in IGMPv3 reports, thereby filtering IGMPv3 reports based on source address, group address, or source and group address.

Source Addresses in IGMPv3 Reports for ASM Groups

IGMP extended access lists also can be used to permit or filter (deny) traffic based on (0.0.0.0, G), that is, (*, G) in IGMP reports that are non-SSM, such as Any Source Multicast (ASM).

Note The permit and deny statements equivalent to (*, G) are **permit host 0.0.0.0 host** *group-address* and **deny host 0.0.0.0 host group** *group-address*, respectively.

Filtering applies to IGMPv3 reports for both ASM and SSM groups, but it is most important for SSM groups because IP multicast routing ignores source addresses in IGMPv3 reports for ASM groups. Source addresses in IGMPv3 membership reports for ASM groups are stored in the IGMP cache (as displayed with the **show ip igmp membership** command), but PIM-based IP multicast routing considers only the ASM groups reported. Therefore, adding filtering for source addresses for ASM groups impacts only the IGMP cache for ASM groups.

How IGMP Checks an Extended Access List

When an IGMP extended access list is referenced in the **ip igmp access-group** command on an interface, the (S, G) pairs in the **permit** and **deny** statements of the extended access list are matched against the (S, G) pair of the IGMP reports received on the interface. For example, if an IGMP report with (S1, S2...Sn, G) is received, first the group (0.0.0.0, G) is checked against the access list statements. The convention (0.0.0.0, G) means (*, G), which is a wildcard source with a multicast group number. If the group is denied, the entire IGMP report is denied. If the group is permitted, each individual (S, G) pair is checked against the access list. Denied sources are taken out of the IGMP report, thereby denying the sources access to the multicast traffic.

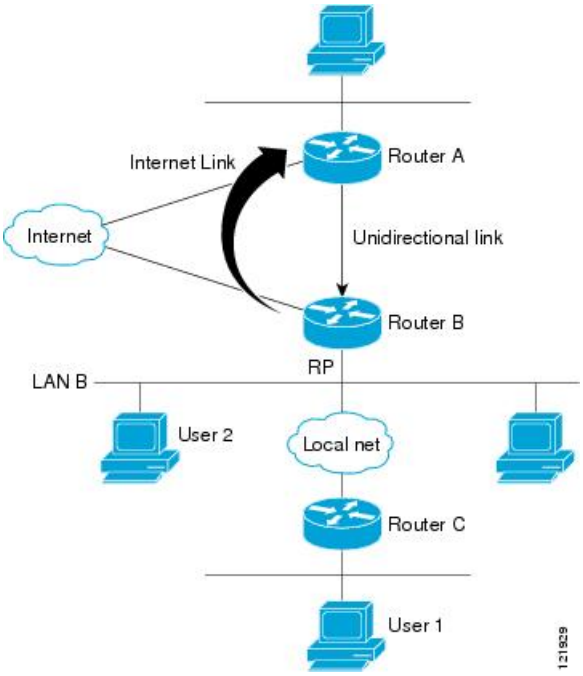
IGMP Proxy

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.

Note 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.
5. 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.

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

How to Customize 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

	Command or Action	Purpose
Step 1	**enable** **Example:** `> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `device(config)# interface gigabitethernet 1`	Enters interface configuration mode. • For the *type* and *number* arguments, specify an interface that is connected to hosts.

Step 4	Do one of the following:
	• **ip igmp join-group** *group-address*
	• **ip igmp static-group** {***** | *group-address* [**source** *source-address*]}
	Example:
	`device(config-if)# ip igmp join-group 225.2.2.2`
	Example:
	`device(config-if)# ip igmp static-group 225.2.2.2`
		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

Step 5	**end** **Example:** `device#(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show ip igmp interface** [*interface-type interface-number*] **Example:** `device# show ip igmp interface`	(Optional) Displays multicast-related information about an 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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing** [**distributed**] **Example:** `Device(config)# ip multicast-routing distributed`	Enables IP multicast routing. • The **distributed** keyword is required for IPv4 multicast..
Step 4	**ip pim ssm** {**default**	**range** *access-list*} **Example:** `Device(config)# ip pim ssm default`	Configures SSM service. • The **default** keyword defines the SSM range access list as 232/8. • The **range** keyword specifies the standard IP access list number or name that defines the SSM range.
Step 5	**ip access-list extended** *access-list* -name **Example:**	Specifies an extended named IP access list.

	Command or Action	Purpose
	`Device(config)# ip access-list extended mygroup`	
Step 6	**deny igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] **Example:** `Device(config-ext-nacl)# deny igmp host 10.1.2.3 any`	(Optional) Filters the specified source address or group address from the IGMP report, thereby restricting hosts on a subnet from membership to the (S, G) channel. • Repeat this step to restrict hosts on a subnet membership to other (S, G) channels. (These sources should be more specific than a subsequent **permit** statement because any sources or groups not specifically permitted are denied.) • Remember that the access list ends in an implicit **deny** statement. • This example shows how to create a deny statement that filters all groups for source 10.1.2.3, which effectively denies the source.
Step 7	**permit igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] **Example:** `Device(config-ext-nacl)# permit igmp any any`	Allows a source address or group address in an IGMP report to pass the IP access list. • You must have at least one **permit** statement in an access list. • Repeat this step to allow other sources to pass the IP access list. • This example shows how to allow group membership to sources and groups not denied by prior **deny** statements.
Step 8	**exit** **Example:** `Device(config-ext-nacl)# exit`	Exits the current configuration session and returns to global configuration mode.
Step 9	interface type number **Example:** `Device(config)# interface ethernet 0`	Selects an interface that is connected to hosts on which IGMPv3 can be enabled.
Step 10	**ip igmp access-group** *access-list* **Example:** `Device(config-if)# ip igmp access-group mygroup`	Applies the specified access list to IGMP reports.
Step 11	**ip pim sparse-mode** **Example:**	Enables PIM-SM on the interface. **Note** You must use sparse mode.

	Command or Action	Purpose
	`Device(config-if)# ip pim sparse-mode`	
Step 12	Repeat Steps 1 through 11 on all interfaces that require access control of SSM channel membership.	--
Step 13	**ip igmp version 3** **Example:** `Device(config-if)# ip igmp version 3`	Enables IGMPv3 on this interface. The default version of IGMP is IGMP version 2. Version 3 is required by SSM.
Step 14	Repeat Step 13 on all host-facing interfaces.	--
Step 15	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Configuring an IGMP Proxy

Perform this optional task to configure unidirectional link (UDL) routers to use the IGMP proxy mechanism. 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.

To configure an IGMP proxy, you will need to perform the following tasks:

Prerequisites for IGMP Proxy

Before configuring an IGMP proxy, ensure that the following conditions exist:

- All routers on the IGMP UDL have the same subnet address. If all routers on the UDL cannot have the same subnet address, the upstream router must be configured with secondary addresses to match all the subnets that the downstream routers are attached to.
- This task assumes that IP multicast has been enabled and that the PIM interfaces have been configured.

When enabling PIM on the interfaces for the IGMP proxy scenario, keep in mind the following guidelines:

-
  - 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) for this step 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.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 1/0/0`	Enters interface configuration mode. • For the *type* and *number* arguments, specify the interface to be used as the UDL on the upstream device.
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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Enters interface configuration mode. • For the *type* and *number* arguments, specify the interface to be used as the UDL on the downstream device for IGMP UDLR.
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	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 6	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 1/0/0`	Enters interface configuration mode. • For the *type* and *number* arguments, select an interface that is facing the nondirectly connected hosts.
Step 7	**ip igmp mroute-proxy** *type number* **Example:** `Device(config-if)# ip igmp mroute-proxy loopback 0`	Enables IGMP report forwarding of proxied (*, G) multicast static route (mroute) entries. • This step is performed to enable the forwarding of IGMP reports to a proxy service interface for all (*,

	Command or Action	Purpose
		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.
Step 8	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 9	**interface** *type number* **Example:** `Device(config)# interface loopback 0`	Enters interface configuration mode for the specified interface. • In this example, loopback interface 0 is specified.
Step 10	**ip igmp helper-address udl** *interface-type interface-number* **Example:** `Device(config-if)# ip igmp helper-address udl gigabitethernet 0/0/0`	Configures IGMP helpering for UDLR. • This step allows the downstream device to helper IGMP reports received from hosts to an upstream device connected to a UDL associated with the interface specified for the *interface-type* and *interface-number* arguments. • In the example topology, IGMP helpering is configured over loopback interface 0 on the downstream device. Loopback interface 0, thus, is configured to helper IGMP reports from hosts to an upstream device connected to Gigabit Ethernet interface 0/0/0.
Step 11	**ip igmp proxy-service** **Example:** `Device(config-if)# ip igmp proxy-service`	Enables the mroute proxy service. • When the mroute proxy service is enabled, the device periodically checks the static mroute table for (*, G) forwarding entries that match interfaces configured with the **ip igmp mroute-proxy** command (see Step 7) based on the IGMP query interval. Where there is a match, one IGMP report is created and received on this interface. **Note** The **ip igmp proxy-service** command is intended to be used with the **ip igmp helper-address** (UDL) command. • In this example, the **ip igmp proxy-service** command is configured on loopback interface 0 to enable the

	Command or Action	Purpose
		forwarding of IGMP reports out the interface for all groups on interfaces registered through the **ip igmp mroute-proxy** command (see Step 7).
Step 12	**end** **Example:** `Device(config-if)# end`	Ends the current configuration session and returns to privileged EXEC mode.
Step 13	**show ip igmp interface** **Example:** `Device# show ip igmp interface`	(Optional) Displays multicast-related information about an interface.
Step 14	**show ip igmp udlr** **Example:** `Device# show ip igmp udlr`	(Optional) Displays UDLR information for directly connected multicast groups on interfaces that have a UDL helper address configured.

Configuration Examples for Customizing 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:

```
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:

```
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.

```
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.

```
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
```

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

```
interface gigabitethernet 0/0/0
ip address 10.1.1.1 255.255.255.0
ip pim sparse-mode
!
interface gigabitethernet 1/0/0
ip address 10.2.1.1 255.255.255.0
ip pim sparse-mode
ip igmp unidirectional-link
!
interface gigabitethernet 2/0/0
ip address 10.3.1.1 255.255.255.0
```

Downstream Device Configuration

```
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 sparse-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 sparse-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

The following sections provide references related to customizing IGMP.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS IP SLAs commands	Cisco IOS IP Multicast Command Reference
Overview of the IP multicast technology area	“ IP Multicast Technology Overview ” module
Basic IP multicast concepts, configuration tasks, and examples	“ Configuring Basic IP Multicast ” or “Configuring IP Multicast in IPv6 Networks” module

Standards and RFCs

Standard/RFC	Title
RFC 1112	*Host extensions for IP multicasting*
RFC 2236	*Internet Group Management Protocol, Version 2*
RFC 3376	*Internet Group Management Protocol, Version 3*

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by these features, and support for existing MIBs has not been modified by these features.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
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.	http://www.cisco.com/cisco/web/support/index.html

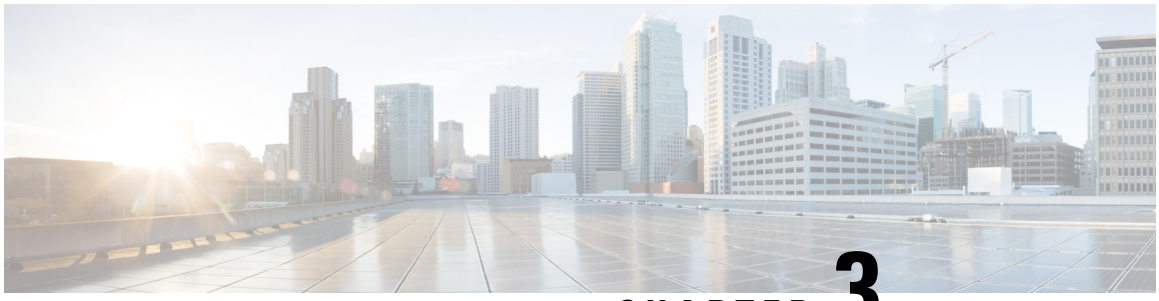
Feature Information for Customizing IGMP

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 Customizing IGMP

Feature Name	Releases	Feature Information
IGMP Version 3 - Explicit Tracking of Hosts, Groups, and Channels	Cisco IOS XE Release 3.8S	IGMPv3 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.
UDLR Tunnel ARP and IGMP Proxy	Cisco IOS XE Release 3.8S	This feature enables ARP over a unidirectional link, and overcomes the existing limitation of requiring downstream multicast receivers to be directly connected to the unidirectional link downstream router.



CHAPTER 3

IGMPv3 Host Stack

This module describes how to configure Internet Group Management Protocol (IGMP) Version 3 (v3) Host Stack feature for enabling devices to function as multicast network endpoints or hosts.

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.

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 IGMPv3 Host Stack

- IP multicast is enabled and all Protocol Independent Multicast (PIM) interfaces have been configured using the tasks described in the "Configuring Basic IP Multicast" module of the *IP Multicast: PIM Configuration Guide*.
- IGMP version 3 must be configured on the interface.
- The device must be configured for SSM. IGMPv3 membership reports are sent for SSM channels only.

Information About IGMPv3 Host Stack

IGMPv3

Internet Group Management Protocol (IGMP) is the protocol used by IPv4 devices to report their IP multicast group memberships to neighboring multicast devices. Version 3 (v3) of IGMP adds support for source filtering. Source filtering enables a multicast receiver host to signal from which groups it wants to receive multicast traffic, and from which sources this traffic is expected. That information may be used by multicast routing protocols to avoid delivering multicast packets from specific sources to networks where there are no interested receivers.

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.

IGMPv3 Host Stack

The IGMPv3 Host Stack feature enables devices to function as multicast network endpoints or hosts. The feature adds INCLUDE mode capability to the IGMPv3 host stack for Source Specific Multicast (SSM) groups. Enabling the IGMPv3 host stack ensures that hosts on a LAN can leverage SSM by enabling the device to initiate IGMPv3 joins, such as in environments where fast channel change is required in a SSM deployments.

To support of the IGMPv3 Host Stack feature, you must configure the INCLUDE mode capability on the IGMPv3 host stack for SSM groups. When the IGMPv3 Host Stack feature is configured, an IGMPv3 membership report is sent when one of the following events occurs:

- When an interface is configured to join a group and source and there is no existing state for this (S, G) channel, an IGMPv3 report of group record type ALLOW_NEW_SOURCES for the source specified is sent on that interface.
- When membership for a group and source is cancelled and there is state for this (S, G) channel, an IGMPv3 report of group record type BLOCK_OLD_SOURCES for the source specified is sent on that interface.
- When a query is received, an IGMPv3 report is sent as defined in RFC 3376.

Note For more information about IGMPv3 group record types and membership reports, see *RFC 3376, Internet Group Management Protocol, Version 3* .

How to Configure IGMPv3 Host Stack

Enabling the IGMPv3 Host Stack

Note If the **ip igmp join-group** command is configured for a group and source and IGMPv3 is not configured on the interface, (S, G) state will be created but no IGMPv3 membership reports will be sent.

Perform this task to add INCLUDE mode capability to the IGMPv3 host stack for SSM groups

.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip igmp version 3**
5. **ip igmp join-group** *group* **-** *address* **source** *source* **-** *address*
6. **end**
7. **show ip igmp groups detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface FastEthernet 1`	Enters interface configuration mode. The specified interface must be connected to hosts.
Step 4	**ip igmp version 3** **Example:** `Device(config-if)# ip igmp version 3`	Enables IGMPv3 on the interface.

	Command or Action	Purpose
Step 5	**ip igmp join-group** *group - address* **source** *source - address* **Example:** `Device(config-if)# ip igmp join-group 232.2.2.2 source 10.1.1.1`	Configures the interface to join the specified (S, G) channel and enables the device to provide INCLUDE mode capability for the (S, G) channel . **Note** Repeat this step for each channel to be configured with the INCLUDE mode capability.
Step 6	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show ip igmp groups detail** **Example:** `Device# show ip igmp groups detail`	Displays directly-connected multicast groups that were learned through IGMP.

Configuration Examples for IGMPv3 Host Stack

Example: Enabling the IGMPv3 Host Stack

The following example shows how to add INCLUDE mode capability to the IGMPv3 host stack for SSM groups:

```
interface FastEthernet0/0/0
 ip igmp join-group 232.2.2.2 source 10.1.1.1
 ip igmp join-group 232.2.2.2 source 10.5.5.5
 ip igmp join-group 232.2.2.2 source 10.5.5.6
 ip igmp join-group 232.2.2.4 source 10.5.5.5
 ip igmp join-group 232.2.2.4 source 10.5.5.6
 ip igmp version 3
```

Based on the configuration presented in the preceding example, the following is sample output from the **debug igmp** command. The messages confirm that IGMPv3 membership reports are being sent after IGMPv3 and SSM are enabled:

```
Device# debug igmp

*May 4 23:48:34.251: IGMP(0): Group 232.2.2.2 is now in the SSM range, changing
*May 4 23:48:34.251: IGMP(0): Building v3 Report on GigabitEthernet0/0/0
*May 4 23:48:34.251: IGMP(0): Add Group Record for 232.2.2.2, type 5
*May 4 23:48:34.251: IGMP(0): Add Source Record 10.1.1.1
*May 4 23:48:34.251: IGMP(0): Add Source Record 10.5.5.5
*May 4 23:48:34.251: IGMP(0): Add Source Record 10.5.5.6
*May 4 23:48:34.251: IGMP(0): Add Group Record for 232.2.2.2, type 6
*May 4 23:48:34.251: IGMP(0): No sources to add, group record removed from report
*May 4 23:48:34.251: IGMP(0): Send unsolicited v3 Report with 1 group records on
FastEthernet0/0/0
*May 4 23:48:34.251: IGMP(0): Group 232.2.2.4 is now in the SSM range, changing
*May 4 23:48:34.251: IGMP(0): Building v3 Report on GigabitEthernet0/0/0
```

```
*May 4 23:48:34.251: IGMP(0): Add Group Record for 232.2.2.4, type 5
*May 4 23:48:34.251: IGMP(0): Add Source Record 10.5.5.5
*May 4 23:48:34.251: IGMP(0): Add Source Record 10.5.5.6
*May 4 23:48:34.251: IGMP(0): Add Group Record for 232.2.2.4, type 6
*May 4 23:48:34.251: IGMP(0): No sources to add, group record removed from report
*May 4 23:48:34.251: IGMP(0): Send unsolicited v3 Report with 1 group records on
FastEthernet0/0/0
*May 4 23:48:35.231: IGMP(0): Building v3 Report on GigabitEthernet0/0/0
*May 4 23:48:35.231: IGMP(0): Add Group Record for 232.2.2.2, type 5
*May 4 23:48:35.231: IGMP(0): Add Source Record 10.1.1.1
*May 4 23:48:35.231: IGMP(0): Add Source Record 10.5.5.5
*May 4 23:48:35.231: IGMP(0): Add Source Record 10.5.5.6
*May 4 23:48:35.231: IGMP(0): Add Group Record for 232.2.2.2, type 6
*May 4 23:48:35.231: IGMP(0): No sources to add, group record removed from report
*May 4 23:48:35.231: IGMP(0): Send unsolicited v3 Report with 1 group records on
FastEthernet0/0/0
*May 4 23:48:35.231: IGMP(0): Building v3 Report on GigabitEthernet0/0/0
*May 4 23:48:35.231: IGMP(0): Add Group Record for 232.2.2.4, type 5
*May 4 23:48:35.231: IGMP(0): Add Source Record 10.5.5.5
*May 4 23:48:35.231: IGMP(0): Add Source Record 10.5.5.6
*May 4 23:48:35.231: IGMP(0): Add Group Record for 232.2.2.4, type 6
*May 4 23:48:35.231: IGMP(0): No sources to add, group record removed from report
*May 4 23:48:35.231: IGMP(0): Send unsolicited v3 Report with 1 group records on
FastEthernet0/0/0
```

The following is sample output from the **show ip igmp groups detail** command for this configuration example scenario. This command can be used to verify that the device has received membership reports for (S, G) channels that are configured to join a group. When the device is correctly receiving IGMP membership reports for a channel, the “Flags:” output field will display the L and SSM flags.

```
Device# show ip igmp groups detail

Flags: L - Local, U - User, SG - Static Group, VG - Virtual Group,
       SS - Static Source, VS - Virtual Source
Interface:      FastEthernet0/0/0
Group:          232.2.2.2
Flags:          L SSM
Uptime:         00:04:12
Group mode:     INCLUDE
Last reporter:  10.4.4.7
Group source list: © - Cisco Src Report, U - URD, R - Remote, S - Static,
                    V - Virtual, Ac - Accounted towards access control limit,
                    M - SSM Mapping, L - Local)
  Source Address   Uptime    v3 Exp   CSR Exp   Fwd  Flags
  10.1.1.1         00:04:10  stopped   stopped    Yes  L
  10.5.5.5         00:04:12  stopped   stopped    Yes  L
  10.5.5.6         00:04:12  stopped   stopped    Yes  L
Interface:      FastEthernet0/0/0
Group:          232.2.2.3
Flags:          L SSM
Uptime:         00:04:12
Group mode:     INCLUDE
Last reporter:  10.4.4.7
Group source list: © - Cisco Src Report, U - URD, R - Remote, S - Static,
                    V - Virtual, Ac - Accounted towards access control limit,
                    M - SSM Mapping, L - Local)
  Source Address   Uptime    v3 Exp   CSR Exp   Fwd  Flags
  10.5.5.5         00:04:14  stopped   stopped   Yes  L
  10.5.5.6         00:04:14  stopped   stopped   Yes  L
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP multicast commands	Cisco IOS IP Multicast Command Reference

Standards and RFCs

Standard/RFC	Title
RFC 3376	*Internet Group Management Protocol, Version 3*

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by these features, and support for existing MIBs has not been modified by these features.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
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.	http://www.cisco.com/cisco/web/support/index.html

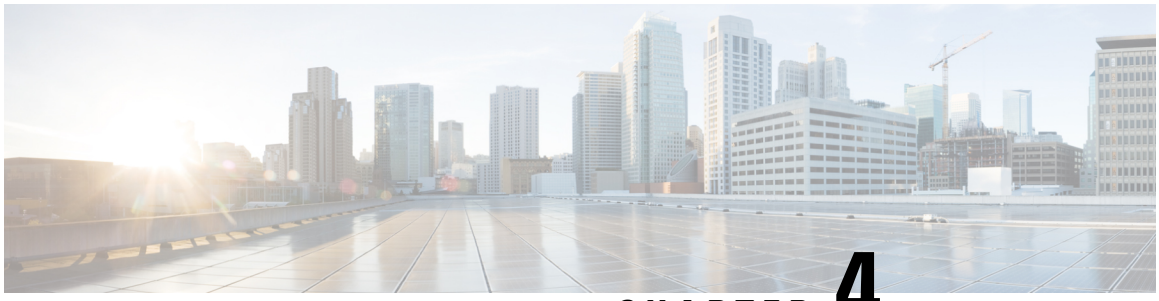
Feature Information for IGMPv3 Host Stack

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 3: Feature Information for IGMPv3 Host Stack

Feature Name	Releases	Feature Information
IGMPv3 Host Stack	12.3(14)T 12.2(33)SRE Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.3SG 15.1(1)SG 15.1(1)SY	The IGMPv3 Host Stack feature enables Cisco devices to function as multicast network endpoints or hosts. The feature adds the INCLUDE mode capability to the IGMPv3 host stack for SSM groups. Enabling the IGMPv3 host stack ensures that hosts on a LAN can leverage SSM by enabling the device to initiate IGMPv3 joins, such as in environments where fast channel change is required in a SSM deployments. The following commands were introduced or modified: **ip igmp join-group**.



CHAPTER 4

IGMP Static Group Range Support

This module describes how you can simplify the administration of networks with devices that require static group membership entries on many interfaces by configuring IGMP static group range support to specify group ranges in class maps and attach the class maps to an interface.

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.

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 Static Group Range Support

IGMP Static Group Range Support Overview

Prior to the introduction of the IGMP Static Group Range Support feature, there was no option to specify group ranges for static group membership. Administering devices that required static group membership entries on many interfaces was challenging in some network environments because each static group had to be configured individually. The result was configurations that were excessively long and difficult to manage.

The IGMP Static Group Range Support feature introduces the capability to configure group ranges in class maps and attach class maps to the interface.

Class Maps for IGMP Static Group Range Support

A class is a way of identifying a set of packets based on its contents. A class is designated through class maps. Typically, class maps are used to create traffic policies. Traffic policies are configured using the modular quality of service (QoS) command-line interface (CLI) (MQC). The normal procedure for creating traffic policies entails defining a traffic class, creating a traffic policy, and attaching the policy to an interface.

The IGMP Static Group Range Support feature introduces a type of class map that is used to define group ranges, group addresses, Source Specific Multicast (SSM) channels, and SSM channel ranges. Once created, the class map can be attached to interfaces.

Although IGMP Static Group Range Support feature uses the MQC to define class maps, the procedure for configuring IGMP static group class maps is different from the procedure used to create class maps for configuring QoS traffic policies. To configure the IGMP Static Group Range Support feature, you must perform the following:

1. Create an IGMP static group class map.
2. Define the group entries associated with the class map.
3. Attach the class map to an interface.

Unlike QoS class maps, which are defined by specifying numerous match criteria, IGMP static group class maps are defined by specifying multicast groups entries (group addresses, group ranges, SSM channels, and SSM channel ranges). Also, IGMP static group range class maps are not configured in traffic policies. Rather, the **ip ignmp static-group** command has been extended to support IGMP static group ranges.

Once a class map is attached to an interface, all group entries defined in the class map become statically connected members on the interface and are added to the IGMP cache and IP multicast route (mroute) table.

General Procedure for Configuring IGMP Group Range Support

To configure the IGMP Static Group Range Support feature, you would complete the following procedure:

1. Create an IGMP static group class map (using the **class-map type multicast-flows** command).
2. Define the group entries associated with the class map (using the **group** command).
3. Attach the class map to an interface (using the **ip igmp static-group** command).

The **class-map type multicast-flows** command is used to enter multicast-flows class map configuration mode to create or modify an IGMP static group class map.

Unlike QoS class maps, which are defined by specifying numerous match criteria, IGMP static group class maps are defined by specifying multicast groups entries (group addresses, group ranges, SSM channels, and SSM channel ranges). The following forms of the group command are entered from multicast-flows class map configuration mode to define group entries to associate with the class map:

- **group** *group-address*

Defines a group address to be associated with an IGMP static group class map.

- **group** *group-address* **to** *group-address*

Defines a range of group addresses to be associated with an IGMP static group class map.

- **group** *group-address* **source** *source-address*

Defines an SSM channel to be associated with an IGMP static group class map.

- **group** *group-address* **to** *group-address* **source** *source-address*

Defines a range of SSM channels to be associated with an IGMP static group class map.

Unlike QoS class maps, IGMP static group range class maps are not configured in traffic policies. Rather, the **ip igmp static-group** command has been extended to support IGMP static group ranges. After creating an IGMP static group class map, you can attach the class map to interfaces using the **ip igmp static-group** command with the **class-map**keyword and *class-map-name* argument. Once a class map is attached to an interface, all group entries defined in the class map become statically connected members on the interface and are added to the IGMP cache and IP multicast route (mroute) table.

Additional Guidelines for Configuring IGMP Static Group Range Support

- Only one IGMP static group class map can be attached to an interface.
- If an IGMP static group class map is modified (that is, if group entries are added to or removed from the class map using the **group** command), the group entries that are added to or removed from the IGMP static group class map are added to or deleted from the IGMP cache and the mroute table, respectively.
- If an IGMP static group class map is replaced on an interface by another class map using the **ip igmp static-group** command, the group entries associated with old class map are removed, and the group entries defined in the new class map are added to the IGMP cache and mroute table.
- The **ip igmp static-group** command accepts an IGMP static group class map for the *class-map-name* argument, regardless of whether the class map configuration exists. If a class map attached to an interface does not exist, the class map remains inactive. Once the class map is configured, all group entries associated with the class map are added to the IGMP cache and mroute table.
- If a class map is removed from an interface using the **no** form of the **ip igmp static-group** command, all group entries defined in the class map are removed from the IGMP cache and mroute tables.

Benefits of IGMP Static Group Range Support

The IGMP Static Group Range Support feature provides the following benefits:

- Simplifies the administration of devices that require many interfaces to be configured with many different **ip igmp static-group** command configurations by introducing the capability to configure group ranges in class maps and attach class maps to the **ip igmp static-group** command.
- Reduces the number of commands required to administer devices that require many **ip igmp static-group** command configurations.

How to Configure IGMP Static Group Range Support

Configuring IGMP Static Group Range Support

Perform this task to create and define an IGMP static group class and attach the class to an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type multicast-flows** *class-map-name*
4. **group** *group-address* [**to** *group-address*] [**source** *source-address*]
5. **exit**
6. Repeat Steps 3 to 5 to create additional class maps.
7. **interface** *type number*
8. **ip igmp static-group class-map** *class-map-name*
9. **ip igmp static-group ***
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**class-map type multicast-flows** *class-map-name* **Example:** `Device(config)# class-map type multicast-flows static1`	Enters multicast-flows class map configuration mode to create or modify an IGMP static group class map.
Step 4	**group** *group-address* [**to** *group-address*] [**source** *source-address*] **Example:** `Device(config-mcast-flows-cmap)# group 232.1.1.7 to 232.1.1.20`	Defines the group entries to be associated with the class map. • Repeat this step to associate additional group entires to the class map being configured.
Step 5	**exit** **Example:** `Device(config-mcast-flows-cmap)# exit`	Exits multicast-flows class-map configuration mode and returns to global configuration mode.
Step 6	Repeat Steps 3 to 5 to create additional class maps.	--
Step 7	**interface** *type number* **Example:**	Enters interface configuration mode.

	Command or Action	Purpose
	`Device(config)# interface FastEthernet 0/1`	
Step 8	**ip igmp static-group class-map** *class-map-name* **Example:** `Device(config-if)# ip igmp static-group class-map static1`	Attaches an IGMP static group class map to the interface.
Step 9	**ip igmp static-group *** **Example:** `Device(config-if)# ip igmp static-group *`	(Optional) Places the interface into all created multicast route (mroute) entries. • Depending on your Cisco software release, this step is required if the interface of a last hop device does not have any PIM neighbors and does not have a receiver. See the **ip igmp static-group** command in the *Cisco IOS IP Multicast Command Reference*.
Step 10	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode, and enters privileged EXEC mode.

Verifying IGMP Static Group Range Support

Perform this optional task to verify the contents of IGMP static group class maps configurations, and to confirm that all group entries defined in class maps were added to the IGMP cache and the mroute table after you attached class maps to interfaces.

SUMMARY STEPS

1. **show ip igmp static-group class-map** [**interface** [*type number*]]
2. **show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**]
3. **show ip mroute**

DETAILED STEPS

Step 1 **show ip igmp static-group class-map** [**interface** [*type number*]]

Displays the contents of IGMP static group class maps and the interfaces using class maps.

The following is sample output from the **show ip igmp static-group class-map** command:

Example:

```
Device# show ip igmp static-group class-map

Class-map static1
  Group address range 228.8.8.7 to 228.8.8.9
  Group address 232.8.8.7, source address 10.1.1.10
```

```
  Interfaces using the classmap:
    Loopback0
Class-map static
  Group address range 232.7.7.7 to 232.7.7.9, source address 10.1.1.10
  Group address 227.7.7.7
  Group address range 227.7.7.7 to 227.7.7.9
  Group address 232.7.7.7, source address 10.1.1.10
  Interfaces using the classmap:
    FastEthernet3/1
```

The following is sample output from the **show ip igmp static-group class-map**command with the **interface** keyword:

Example:

```
Device# show ip igmp static-group class-map interface

Loopback0
  Class-map attached: static1
FastEthernet3/1
  Class-map attached: static
```

The following is sample output from the **show ip igmp static-group class-map**command with the **interface** keyword and *type number* arguments:

Example:

```
Device# show ip igmp static-group class-map interface FastEthernet 3/1

FastEthernet3/1
  Class-map attached: static
```

Step 2 **show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**]

Displays the multicast groups with receivers that are directly connected to the device and that are learned through IGMP.

The following is sample output from the **show ip igmp groups** command:

Example:

```
device# show ip igmp groups

IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
232.7.7.7        FastEthernet3/1          00:00:09  stopped   0.0.0.0
232.7.7.9        FastEthernet3/1          00:00:09  stopped   0.0.0.0
232.7.7.8        FastEthernet3/1          00:00:09  stopped   0.0.0.0
227.7.7.7        FastEthernet3/1          00:00:09  stopped   0.0.0.0
227.7.7.9        FastEthernet3/1          00:00:09  stopped   0.0.0.0
227.7.7.8        FastEthernet3/1          00:00:09  stopped   0.0.0.0
224.0.1.40       FastEthernet3/2          01:44:50  00:02:09  10.2.2.5
224.0.1.40       Loopback0                01:45:22  00:02:32  10.3.3.4
```

Step 3 **show ip mroute**

Displays the contents of the mroute table.

The following is sample output from the **show ip mroute** command:

Example:

```
Device# show ip mroute

IP Multicast Routing Table
```

```
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(10.1.1.10, 232.7.7.7), 00:00:17/00:02:42, flags: sTI
  Incoming interface: FastEthernet3/2, RPF nbr 10.2.2.5
  Outgoing interface list:
    FastEthernet3/1, Forward/Sparse-Dense, 00:00:17/00:02:42
(10.1.1.10, 232.7.7.9), 00:00:17/00:02:42, flags: sTI
  Incoming interface: FastEthernet3/2, RPF nbr 10.2.2.5
  Outgoing interface list:
    FastEthernet3/1, Forward/Sparse-Dense, 00:00:17/00:02:42
(10.1.1.10, 232.7.7.8), 00:00:18/00:02:41, flags: sTI
  Incoming interface: FastEthernet3/2, RPF nbr 10.2.2.5
  Outgoing interface list:
    FastEthernet3/1, Forward/Sparse-Dense, 00:00:18/00:02:41
(*, 227.7.7.7), 00:00:18/00:02:41, RP 10.2.2.6, flags: SJC
  Incoming interface: FastEthernet3/2, RPF nbr 10.2.2.6
  Outgoing interface list:
    FastEthernet3/1, Forward/Sparse-Dense, 00:00:18/00:02:41
(*, 227.7.7.9), 00:00:18/00:02:41, RP 10.2.2.6, flags: SJC
  Incoming interface: FastEthernet3/2, RPF nbr 10.2.2.6
  Outgoing interface list:
    FastEthernet3/1, Forward/Sparse-Dense, 00:00:18/00:02:41
(*, 227.7.7.8), 00:00:18/00:02:41, RP 10.2.2.6, flags: SJC
  Incoming interface: FastEthernet3/2, RPF nbr 10.2.2.6
  Outgoing interface list:
    FastEthernet3/1, Forward/Sparse-Dense, 00:00:18/00:02:41
(*, 224.0.1.40), 00:01:40/00:02:23, RP 10.2.2.6, flags: SJCL
  Incoming interface: FastEthernet3/2, RPF nbr 10.2.2.6
  Outgoing interface list:
    Loopback0, Forward/Sparse-Dense, 00:01:40/00:02:23
```

Configuration Examples for IGMP Static Group Range Support

Example: Configuring IGMP Static Group Support

The following example shows how to configure a class map and attach the class map to an interface. In this example, a class map named static is configured and attached to FastEthernet interface 3/1.

```
class-map type multicast-flows static
 group 227.7.7.7
 group 232.7.7.7 to 232.7.7.9 source 10.1.1.10
 group 232.7.7.7 source 10.1.1.10
 group 227.7.7.7 to 227.7.7.9
.
.
.
!
interface FastEthernet3/1
 ip address 192.168.1. 2 255.255.255.0
```

```
 ip pim sparse-dense-mode
 ip igmp static-group class-map static
!
```

Example: Verifying IGMP Static Group Support

The following is sample output from the **show ip igmp static-group class-map** command. In this example, the output displays the contents of the IGMP static group class map named static (the class map configured in the Example: Configuring IGMP Static Group Support, on page 39 section).

```
Device# show ip igmp static-group class-map

Class-map static
  Group address range 227.7.7.7 to 227.7.7.9
  Group address 232.7.7.7, source address 10.1.1.10
  Group address range 232.7.7.7 to 232.7.7.9, source address 10.1.1.10
  Group address 227.7.7.7
  Interfaces using the classmap:
    FastEthernet3/1
```

The following is sample output from the **show ip igmp groups** command. In this example, the command is issued to confirm that the group entries defined in the class map named static (the class map configured in the Example: Configuring IGMP Static Group Support, on page 39 section) were added to the IGMP cache.

```
Device# show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
232.7.7.7        FastEthernet3/1          00:00:09  stopped   0.0.0.0
232.7.7.9        FastEthernet3/1          00:00:09  stopped   0.0.0.0
232.7.7.8        FastEthernet3/1          00:00:09  stopped   0.0.0.0
227.7.7.7        FastEthernet3/1          00:00:09  stopped   0.0.0.0
227.7.7.9        FastEthernet3/1          00:00:09  stopped   0.0.0.0
227.7.7.8        FastEthernet3/1          00:00:09  stopped   0.0.0.0
224.0.1.40       FastEthernet3/2          01:44:50  00:02:09  10.2.2.5
224.0.1.40       Loopback0                01:45:22  00:02:32  10.3.3.4
```

The following is sample output from the **show ip mroute**command. In this example, the command is issued to confirm that the group entries defined in the class map named static (the class map configured in the Example: Configuring IGMP Static Group Support, on page 39 section) were added to the mroute table.

```
Device# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(10.1.1.10, 232.7.7.7), 00:00:17/00:02:42, flags: sTI
  Incoming interface: FastEthernet3/2, RPF nbr 10.2.2.5
  Outgoing interface list:
    FastEthernet3/1, Forward/Sparse-Dense, 00:00:17/00:02:42
(10.1.1.10, 232.7.7.9), 00:00:17/00:02:42, flags: sTI
  Incoming interface: FastEthernet3/2, RPF nbr 10.2.2.5
  Outgoing interface list:
```

```
    FastEthernet3/1, Forward/Sparse-Dense, 00:00:17/00:02:42
(10.1.1.10, 232.7.7.8), 00:00:18/00:02:41, flags: sTI
  Incoming interface: FastEthernet3/2, RPF nbr 10.2.2.5
  Outgoing interface list:
    FastEthernet3/1, Forward/Sparse-Dense, 00:00:18/00:02:41
(*, 227.7.7.7), 00:00:18/00:02:41, RP 10.2.2.6, flags: SJC
  Incoming interface: FastEthernet3/2, RPF nbr 10.2.2.6
  Outgoing interface list:
    FastEthernet3/1, Forward/Sparse-Dense, 00:00:18/00:02:41
(*, 227.7.7.9), 00:00:18/00:02:41, RP 10.2.2.6, flags: SJC
  Incoming interface: FastEthernet3/2, RPF nbr 10.2.2.6
  Outgoing interface list:
    FastEthernet3/1, Forward/Sparse-Dense, 00:00:18/00:02:41
(*, 227.7.7.8), 00:00:18/00:02:41, RP 10.2.2.6, flags: SJC
  Incoming interface: FastEthernet3/2, RPF nbr 10.2.2.6
  Outgoing interface list:
    FastEthernet3/1, Forward/Sparse-Dense, 00:00:18/00:02:41
(*, 224.0.1.40), 00:01:40/00:02:23, RP 10.2.2.6, flags: SJCL
  Incoming interface: FastEthernet3/2, RPF nbr 10.2.2.6
  Outgoing interface list:
    Loopback0, Forward/Sparse-Dense, 00:01:40/00:02:23
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP multicast commands	Cisco IOS IP Multicast Command Reference

Standards and RFCs

Standard/RFC	Title
RFC 2933	*Internet Group Management Protocol MIB*

MIBs

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

Technical Assistance

Description	Link
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.	http://www.cisco.com/cisco/web/support/index.html

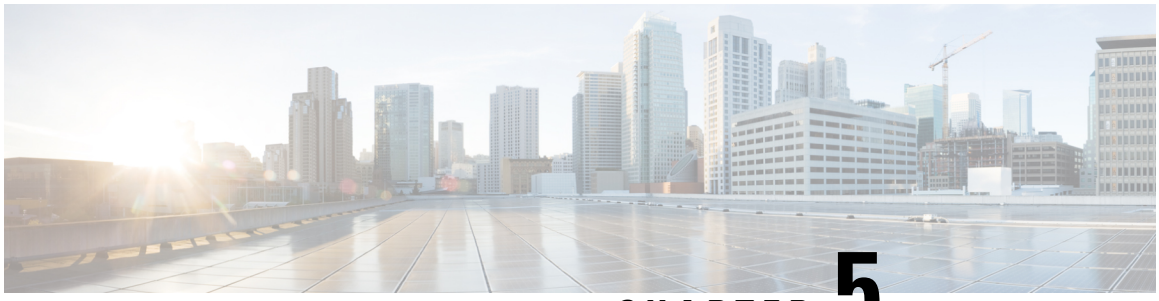
Feature Information for IGMP Static Group Range Support

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 4: Feature Information for IGMP Static Group Range Support

Feature Name	Releases	Feature Information
IGMP Static Group Range Support	12.2(18)SXF5 Cisco IOS XE Release 2.6 15.0(1)M 12.2(33)SRE 15.1(1)SG Cisco IOS XE Release 3.3SG	The IGMP Static Group Range Support feature introduces the capability to configure group ranges in class maps and attach class maps to an interface. This feature is an enhancement that simplifies the administration of networks with devices that require static group membership entries on many interfaces. The following commands were introduced or modified by this feature: **class-map type multicast-flows**, **group** (multicast-flows), **ip igmp static-group** , **show ip igmp static-group class-map**.
IGMP MIB Support Enhancements for SNMP	12.2(11)T 12.2(33)SRE Cisco IOS XE Release 2.1 15.1(1)SG 12.2(50)SY 15.0(1)S	The Internet Group Management Protocol (IGMP) is used by IP hosts to report their multicast group memberships to neighboring multicast routers. The IGMP MIB describes objects that enable users to remotely monitor and configure IGMP using Simple Network Management Protocol (SNMP). It also allows users to remotely subscribe and unsubscribe from multicast groups. The IGMP MIB Support Enhancements for SNMP feature adds full support of RFC 2933 (Internet Group Management Protocol MIB) in Cisco IOS software. There are no new or modfied commands for this feature.



CHAPTER 5

SSM Mapping

The Source Specific Multicast (SSM) Mapping feature extends the Cisco suite of SSM transition tools, which also includes URL Rendezvous Directory (URD) and Internet Group Management Protocol Version 3 Lite (IGMP v3lite). SSM mapping supports SSM transition in cases where neither URD nor IGMP v3lite is available, or when supporting SSM on the end system is impossible or unwanted due to administrative or technical reasons. SSM mapping enables you to leverage SSM for video delivery to legacy set-top boxes (STBs) that do not support IGMPv3 or for applications that do not take advantage of the IGMPv3 host stack.

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.

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 SSM Mapping

One option available for using SSM mapping is to install it together with a Domain Name System (DNS) server to simplify administration of the SSM Mapping feature in larger deployments.

Before you can configure and use SSM mapping with DNS lookups, you need to add records to a running DNS server. If you do not already have a DNS server running, you need to install one.

Restrictions for SSM Mapping

- The SSM Mapping feature does not share the benefit of full SSM. SSM mapping takes a group G join from a host and identifies this group with an application associated with one or more sources, therefore, it can only support one such application per group G. Nevertheless, full SSM applications may still share the same group also used in SSM mapping.
- Enable IGMPv3 with care on the last hop router when you rely solely on SSM mapping as a transition solution for full SSM.

Information About SSM Mapping

SSM Components

SSM is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core networking technology for the Cisco implementation of IP multicast solutions targeted for audio and video broadcast application environments and is described in RFC 3569. The following two components together support the implementation of SSM:

- Protocol Independent Multicast source-specific mode (PIM-SSM)
- Internet Group Management Protocol Version 3 (IGMPv3)

Protocol Independent Multicast (PIM) SSM, or PIM-SSM, is the routing protocol that supports the implementation of SSM and is derived from PIM sparse mode (PIM-SM). IGMP is the Internet Engineering Task Force (IETF) standards track protocol used for hosts to signal multicast group membership to routers. IGMP Version 3 supports source filtering, which is required for SSM. IGMP For SSM to run with IGMPv3, SSM must be supported in the router, the host where the application is running, and the application itself.

Benefits of Source Specific Multicast

IP Multicast Address Management Not Required

In the ISM service, applications must acquire a unique IP multicast group address because traffic distribution is based only on the IP multicast group address used. If two applications with different sources and receivers use the same IP multicast group address, then receivers of both applications will receive traffic from the senders of both applications. Even though the receivers, if programmed appropriately, can filter out the unwanted traffic, this situation would cause generally unacceptable levels of unwanted traffic.

Allocating a unique IP multicast group address for an application is still a problem. Most short-lived applications use mechanisms like Session Description Protocol (SDP) and Session Announcement Protocol (SAP) to get a random address, a solution that does not work well with a rising number of applications in the Internet. The best current solution for long-lived applications is described in RFC 2770, but this solution suffers from the restriction that each autonomous system is limited to only 255 usable IP multicast addresses.

In SSM, traffic from each source is forwarded between routers in the network independent of traffic from other sources. Thus different sources can reuse multicast group addresses in the SSM range.

Denial of Service Attacks from Unwanted Sources Inhibited

In SSM, multicast traffic from each individual source will be transported across the network only if it was requested (through IGMPv3, IGMP v3lite, or URD memberships) from a receiver. In contrast, ISM forwards traffic from any active source sending to a multicast group to all receivers requesting that multicast group. In Internet broadcast applications, this ISM behavior is highly undesirable because it allows unwanted sources to easily disturb the actual Internet broadcast source by simply sending traffic to the same multicast group. This situation depletes bandwidth at the receiver side with unwanted traffic and thus disrupts the undisturbed reception of the Internet broadcast. In SSM, this type of denial of service (DoS) attack cannot be made by simply sending traffic to a multicast group.

Easy to Install and Manage

SSM is easy to install and provision in a network because it does not require the network to maintain which active sources are sending to multicast groups. This requirement exists in ISM (with IGMPv1, IGMPv2, or IGMPv3).

The current standard solutions for ISM service are PIM-SM and MSDP. Rendezvous point (RP) management in PIM-SM (including the necessity for Auto-RP or BSR) and MSDP is required only for the network to learn about active sources. This management is not necessary in SSM, which makes SSM easier than ISM to install and manage, and therefore easier than ISM to operationally scale in deployment. Another factor that contributes to the ease of installation of SSM is the fact that it can leverage preexisting PIM-SM networks and requires only the upgrade of last hop routers to support IGMPv3, IGMP v3lite, or URD.

Ideal for Internet Broadcast Applications

The three benefits previously described make SSM ideal for Internet broadcast-style applications for the following reasons:

- The ability to provide Internet broadcast services through SSM without the need for unique IP multicast addresses allows content providers to easily offer their service (IP multicast address allocation has been a serious problem for content providers in the past).
- The prevention against DoS attacks is an important factor for Internet broadcast services because, with their exposure to a large number of receivers, they are the most common targets for such attacks.
- The ease of installation and operation of SSM makes it ideal for network operators, especially in those cases where content needs to be forwarded between multiple independent PIM domains (because there is no need to manage MSDP for SSM between PIM domains).

SSM Transition Solutions

The Cisco IOS suite of SSM transition solutions consists of the following transition solutions that enable the immediate development and deployment of SSM services, without the need to wait for the availability of full IGMPv3 support in host operating systems and SSM receiver applications:

- Internet Group Management Protocol Version 3 lite (IGMP v3lite)
- URL Rendezvous Directory (URD)
- SSM mapping

IGMP v3lite is a solution for application developers that allows immediate development of SSM receiver applications switching to IGMPv3 as soon as it becomes available.

For more information about IGMP v3lite, see the " Configuring Source Specific Multicast " module.

URD is an SSM transition solution for content providers and content aggregators that allows them to deploy receiver applications that are not yet SSM enabled (through support for IGMPv3) by enabling the receiving applications to be started and controlled through a web browser.

For more information about URD, see the see the " Configuring Source Specific Multicast " module.

SSM mapping supports SSM transition in cases where neither URD nor IGMP v3lite are available, or when supporting SSM on the end system is impossible or unwanted due to administrative or technical reasons.

SSM Mapping Overview

SSM mapping supports SSM transition when supporting SSM on the end system is impossible or unwanted due to administrative or technical reasons. Using SSM to deliver live streaming video to legacy STBs that do not support IGMPv3 is a typical application of SSM mapping.

In a typical STB deployment, each TV channel uses one separate IP multicast group and has one active server host sending the TV channel. A single server may of course send multiple TV channels, but each to a different group. In this network environment, if a router receives an IGMPv1 or IGMPv2 membership report for a particular group G, the report implicitly addresses the well-known TV server for the TV channel associated with the multicast group.

SSM mapping introduces a means for the last hop router to discover sources sending to groups. When SSM mapping is configured, if a router receives an IGMPv1 or IGMPv2 membership report for a particular group G, the router translates this report into one or more (S, G) channel memberships for the well-known sources associated with this group.

When the router receives an IGMPv1 or IGMPv2 membership report for group G, the router uses SSM mapping to determine one or more source IP addresses for group G. SSM mapping then translates the membership report as an IGMPv3 report INCLUDE (G, [S1, G], [S2, G]...[Sn, G] and continues as if it had received an IGMPv3 report. The router then sends out PIM joins toward (S1, G) to (Sn, G) and continues to be joined to these groups as long as it continues to receive the IGMPv1 or IGMPv2 membership reports and as long as the SSM mapping for the group remains the same. SSM mapping, thus, enables you to leverage SSM for video delivery to legacy STBs that do not support IGMPv3 or for applications that do not take advantage of the IGMPv3 host stack.

SSM mapping enables the last hop router to determine the source addresses either by a statically configured table on the router or by consulting a DNS server. When the statically configured table is changed, or when the DNS mapping changes, the router will leave the current sources associated with the joined groups.

Static SSM Mapping

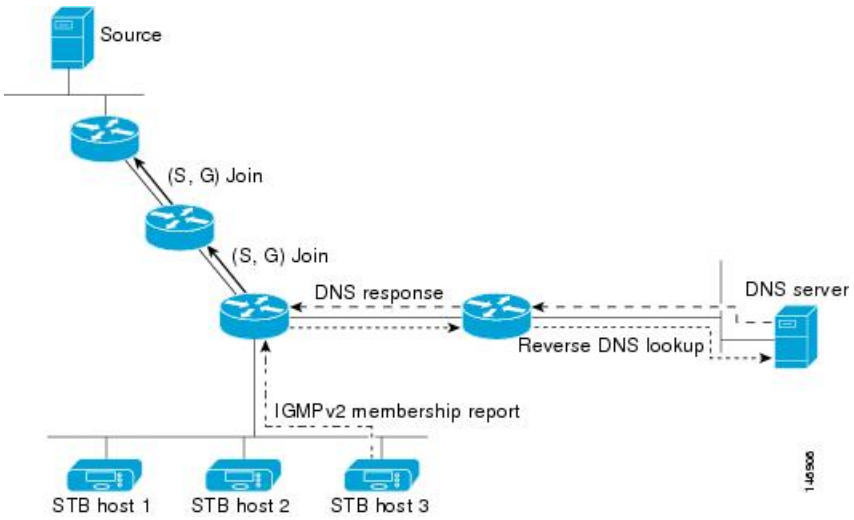
SSM static mapping enables you to configure the last hop router to use a static map to determine the sources sending to groups. Static SSM mapping requires that you configure access lists (ACLs) to define group ranges. The groups permitted by those ACLs then can be mapped to sources using the **ip igmp static ssm-map** global configuration command.

You can configure static SSM mapping in smaller networks when a DNS is not needed or to locally override DNS mappings that may be temporarily incorrect. When configured, static SSM mappings take precedence over DNS mappings.

DNS-Based SSM Mapping

DNS-based SSM mapping enables you to configure the last hop router to perform a reverse DNS lookup to determine sources sending to groups (see the figure below). When DNS-based SSM mapping is configured, the router constructs a domain name that includes the group address G and performs a reverse lookup into the DNS. The router looks up IP address resource records (IP A RRs) to be returned for this constructed domain name and uses the returned IP addresses as the source addresses associated with this group. SSM mapping supports up to 20 sources for each group. The router joins all sources configured for a group.

Figure 1: DNS-Based SSM-Mapping



The SSM mapping mechanism that enables the last hop router to join multiple sources for a group can be used to provide source redundancy for a TV broadcast. In this context, the redundancy is provided by the last hop router using SSM mapping to join two video sources simultaneously for the same TV channel. However, to prevent the last hop router from duplicating the video traffic, it is necessary that the video sources utilize a server-side switchover mechanism where one video source is active while the other backup video source is passive. The passive source waits until an active source failure is detected before sending the video traffic for the TV channel. The server-side switchover mechanism, thus, ensures that only one of the servers is actively sending the video traffic for the TV channel.

To look up one or more source addresses for a group G that includes G1, G2, G3, and G4, the following DNS resource records (RRs) must be configured on the DNS server:

G4.G3.G2.G1 [*multicast-domain*] [*timeout*]	IN A *source-address-1*
	IN A *source-address-2*
	IN A *source-address-n*

The *multicast-domain* argument is a configurable DNS prefix. The default DNS prefix is in-addr.arpa. You should only use the default prefix when your installation is either separate from the internet or if the group names that you map are global scope group addresses (RFC 2770 type addresses that you configure for SSM) that you own.

The *timeout* argument configures the length of time for which the router performing SSM mapping will cache the DNS lookup. This argument is optional and defaults to the timeout of the zone in which this entry is configured. The timeout indicates how long the router will keep the current mapping before querying the DNS

server for this group. The timeout is derived from the cache time of the DNS RR entry and can be configured for each group/source entry on the DNS server. You can configure this time for larger values if you want to minimize the number of DNS queries generated by the router. Configure this time for a low value if you want to be able to quickly update all routers with new source addresses.

Note Refer to your DNS server documentation for more information about configuring DNS RRs.

To configure DNS-based SSM mapping in the software, you must configure a few global commands but no per-channel specific configuration is needed. There is no change to the configuration for SSM mapping if additional channels are added. When DNS-based SSM mapping is configured, the mappings are handled entirely by one or more DNS servers. All DNS techniques for configuration and redundancy management can be applied to the entries needed for DNS-based SSM mapping.

SSM Mapping Benefits

- The SSM Mapping feature provides almost the same ease of network installation and management as a pure SSM solution based on IGMPv3. Some additional configuration is necessary to enable SSM mapping.
- The SSM benefit of inhibition of DoS attacks applies when SSM mapping is configured. When SSM mapping is configured the only segment of the network that may still be vulnerable to DoS attacks are receivers on the LAN connected to the last hop router. Since those receivers may still be using IGMPv1 and IGMPv2, they are vulnerable to attacks from unwanted sources on the same LAN. SSM mapping, however, does protect those receivers (and the network path leading towards them) from multicast traffic from unwanted sources anywhere else in the network.
- Address assignment within a network using SSM mapping needs to be coordinated, but it does not need assignment from outside authorities, even if the content from the network is to be transited into other networks.

How to Configure SSM Mapping

Configuring Static SSM Mapping

Perform this task to configure the last hop router in an SSM deployment to use static SSM mapping to determine the IP addresses of sources sending to groups.

Before you begin

- Enable IP multicast routing, enable PIM sparse mode, and configure SSM before performing this task. For more information, see the “Configuring Basic Multicast ”module.
- Before you configure static SSM mapping, you must configure ACLs that define the group ranges to be mapped to source addresses.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **ip igmp ssm-map enable**
4. **no ip igmp ssm-map query dns**
5. **ip igmp ssm-map static** *access-list source-address*
6. Repeat Step 5 to configure additional static SSM mappings, if required.
7. **end**
8. **show running-config**
9. **copy running-config start-up config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip igmp ssm-map enable** **Example:** `Device(config)# ip igmp ssm-map enable`	Enables SSM mapping for groups in the configured SSM range. **Note** By default, this command enables DNS-based SSM mapping.
Step 4	**no ip igmp ssm-map query dns** **Example:** `Device(config)# no ip igmp ssm-map query dns`	(Optional) Disables DNS-based SSM mapping. **Note** Disable DNS-based SSM mapping if you only want to rely on static SSM mapping. By default, the **ip igmp ssm-map** command enables DNS-based SSM mapping.
Step 5	**ip igmp ssm-map static** *access-list source-address* **Example:** `Device(config)# ip igmp ssm-map static 11 172.16.8.11`	Configures static SSM mapping. • The ACL supplied for the *access-list* argument defines the groups to be mapped to the source IP address entered for the *source-address* argument. **Note** You can configure additional static SSM mappings. If additional SSM mappings are configured and the router receives an IGMPv1 or IGMPv2 membership report for a group in the SSM range, the Cisco IOS XE software determines the source addresses associated with the group by walking each configured **ip igmp ssm-map static** command. The Cisco IOS XE software associates up to 20 sources per group.

	Command or Action	Purpose
Step 6	Repeat Step 5 to configure additional static SSM mappings, if required.	--
Step 7	**end** **Example:** `Device(config)# end`	Ends the current configuration session and returns to privileged EXEC mode.
Step 8	**show running-config** **Example:** `Device# show running-config`	Verifies your entries.
Step 9	**copy running-config start-up config** **Example:** `Device# copy running-config start-up config`	(Optional) Saves your entries in the configuration file.

What to Do Next

Proceed to the Configuring DNS-Based SSM Mapping (CLI), on page 50 or to the Verifying SSM Mapping Configuration and Operation, on page 53.

Configuring DNS-Based SSM Mapping (CLI)

Perform this task to configure the last hop router to perform DNS lookups to learn the IP addresses of sources sending to a group.

Before you begin

- Enable IP multicast routing, enable PIM sparse mode, and configure SSM before performing this task. For more information, see the "Configuring Basic Multicast"module.
- Before you can configure and use SSM mapping with DNS lookups, you need to be able to add records to a running DNS server. If you do not already have a DNS server running, you need to install one.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip igmp ssm-map enable**
4. **ip igmp ssm-map query dns**
5. **ip domain multicast** *domain-prefix*
6. **ipname-server** *server-address1* [*server-address2server-address6*]
7. Repeat Step 6 to configure additional DNS servers for redundancy, if required.
8. **end**
9. **show running-config**

10. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip igmp ssm-map enable** **Example:** `Device(config)# ip igmp ssm-map enable`	Enables SSM mapping for groups in a configured SSM range.
Step 4	**ip igmp ssm-map query dns** **Example:** `Device(config)# ip igmp ssm-map query dns`	(Optional) Enables DNS-based SSM mapping. • By default, the **ip igmp ssm-map** command enables DNS-based SSM mapping. Only the **no**form of this command is saved to the running configuration. **Note** Use this command to reenable DNS-based SSM mapping if DNS-based SSM mapping is disabled.
Step 5	**ip domain multicast** *domain-prefix* **Example:** `Device(config)# ip domain multicast ssm-map.cisco.com`	(Optional) Changes the domain prefix used by the Cisco IOS XE software for DNS-based SSM mapping. • By default, the software uses the ip-addr.arpa domain prefix.
Step 6	**ipname-server** *server-address1* [*server-address2server-address6*] **Example:** `Device(config)# ip name-server 10.48.81.21`	Specifies the address of one or more name servers to use for name and address resolution.
Step 7	Repeat Step 6 to configure additional DNS servers for redundancy, if required.	--
Step 8	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 9	**show running-config** **Example:**	Verifies your entries.

	Command or Action	Purpose
	`Device# show running-config`	
Step 10	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to Do Next

Configuring Static Traffic Forwarding with SSM Mapping

Perform this task to configure static traffic forwarding with SSM mapping on the last hop router. Static traffic forwarding can be used in conjunction with SSM mapping to statically forward SSM traffic for certain groups. When static traffic forwarding with SSM mapping is configured, the last hop router uses DNS-based SSM mapping to determine the sources associated with a group. The resulting (S, G) channels are then statically forwarded.

Before you begin

This task does not include the steps for configuring DNS-based SSM mapping. See the Configuring DNS-Based SSM Mapping (CLI), on page 50 task for more information about configuring DNS-based SSM mapping.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip igmp static-group** *group-address* **source ssm-map**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Selects an interface on which to statically forward traffic for a multicast group using SSM mapping and enters interface configuration mode.

	Command or Action	Purpose
		Note Static forwarding of traffic with SSM mapping works with either DNS-based SSM mapping or statically-configured SSM mapping.
Step 4	**ip igmp static-group** *group-address* **source ssm-map** **Example:** `Router(config-if)# ip igmp static-group 232.1.2.1 source ssm-map`	Configures SSM mapping to be used to statically forward a (S, G) channel out of the interface. • Use this command if you want to statically forward SSM traffic for certain groups, but you want to use DNS-based SSM mapping to determine the source addresses of the channels.

What to Do Next

Proceed to the Verifying SSM Mapping Configuration and Operation, on page 53.

Verifying SSM Mapping Configuration and Operation

Perform this optional task to verify SSM mapping configuration and operation.

SUMMARY STEPS

1. **enable**
2. **show ip igmp ssm-mapping**
3. **show ip igmp ssm-mapping** *group-address*
4. **show ip igmp groups** [*group-name* | *group-address* | *interface-type interface-number*] [**detail**]
5. **show host**
6. **debug ip igmp** *group-address*

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
> enable
```

Step 2 **show ip igmp ssm-mapping**

(Optional) Displays information about SSM mapping.

The following example shows how to display information about SSM mapping configuration. In this example, SSM static mapping and DNS-based SSM mapping are enabled.

Example:

```
# show ip igmp ssm-mapping
```

```
SSM Mapping  : Enabled
DNS Lookup   : Enabled
Mcast domain : ssm-map.cisco.com
Name servers : 10.0.0.3
               10.0.0.4
```

Step 3 **show ip igmp ssm-mapping** *group-address*

(Optional) Displays the sources that SSM mapping uses for a particular group.

The following example shows how to display information about the configured DNS-based SSM mapping. In this example, the router has used DNS-based mapping to map group 232.1.1.4 to sources 172.16.8.5 and 172.16.8.6. The timeout for this entry is 860000 milliseconds (860 seconds).

Example:

```
# show ip igmp ssm-mapping 232.1.1.4
Group address: 232.1.1.4
Database     : DNS
DNS name     : 4.1.1.232.ssm-map.cisco.com
Expire time  : 860000
Source list  : 172.16.8.5
             : 172.16.8.6
```

Step 4 **show ip igmp groups** [*group-name* | *group-address* | *interface-type interface-number*] [**detail**]

(Optional) Displays the multicast groups with receivers that are directly connected to the router and that were learned through IGMP.

The following is sample output from the **show ip igmp groups** command with the *group-address* argument and **detail** keyword. In this example the “M” flag indicates that SSM mapping is configured.

Example:

```
# show ip igmp group 232.1.1.4 detail
            Interface:      GigabitEthernet2/0/0
            Group:          232.1.1.4 SSM
            Uptime:         00:03:20
            Group mode:     INCLUDE
            Last reporter:  0.0.0.0
            CSR Grp Exp:    00:02:59
            Group source list: (C - Cisco Src Report, U - URD, R - Remote,
                                S - Static, M - SSM Mapping)
              Source Address   Uptime    v3 Exp   CSR Exp   Fwd  Flags
              172.16.8.3       00:03:20  stopped   00:02:59  Yes  CM
              172.16.8.4       00:03:20  stopped   00:02:59  Yes  CM
              172.16.8.5       00:03:20  stopped   00:02:59  Yes  CM
              172.16.8.6       00:03:20  stopped   00:02:59  Yes  CM
```

Step 5 **show host**

(Optional) Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.

The following is sample output from the **show host**command. Use this command to display DNS entries as they are learned by the router.

Example:

```
# show host
Default domain is cisco.com
Name/address lookup uses domain service
```

```
Name servers are 10.48.81.21
Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined
Host                      Port   Flags      Age   Type    Address(es)
10.0.0.0.ssm-map.cisco.c  None  (temp, OK)   0     IP     172.16.8.5
                                                        172.16.8.6
                                                        172.16.8.3
```

172.16.8.4

Step 6 **debug ip igmp** *group-address*

(Optional) Displays the IGMP packets received and sent and IGMP host-related events.

The following is sample output from the **debug ip igmp**command when SSM static mapping is enabled. The following output indicates that the router is converting an IGMPv2 join for group G into an IGMPv3 join:

Example:

```
IGMP(0): Convert IGMPv2 report (*,232.1.2.3) to IGMPv3 with 2 source(s) using STATIC.
```

The following is sample output from the **debug ip igmp** command when DNS-based SSM mapping is enabled. The following output indicates that a DNS lookup has succeeded:

Example:

```
IGMP(0): Convert IGMPv2 report (*,232.1.2.3) to IGMPv3 with 2 source(s) using DNS.
```

The following is sample output from the **debug ip igmp** command when DNS-based SSM mapping is enabled and a DNS lookup has failed:

IGMP(0): DNS source lookup failed for (*, 232.1.2.3), IGMPv2 report failed

Configuration Examples for SSM Mapping

SSM Mapping Example

The following configuration example shows a router configuration for SSM mapping. This example also displays a range of other IGMP and SSM configuration options to show compatibility between features. Do not use this configuration example as a model unless you understand all of the features used in the example.

Note Address assignment in the global SSM range 232.0.0.0/8 should be random. If you copy parts or all of this sample configuration, make sure to select a random address range but not 232.1.1.x as shown in this example. Using a random address range minimizes the possibility of address collision and may prevent conflicts when other SSM content is imported while SSM mapping is used.

```
!
no ip domain lookup
ip domain multicast ssm.map.cisco.com
ip name-server 10.48.81.21
```

```
!
!
ip multicast-routing distributed
ip igmp ssm-map enable
ip igmp ssm-map static 10 172.16.8.10
ip igmp ssm-map static 11 172.16.8.11
!
!
.
.
.
!
interface GigabitEthernet0/0/0
 description Sample IGMP Interface Configuration for SSM-Mapping Example
 ip address 10.20.1.2 255.0.0.0
 ip pim sparse-mode
 ip igmp last-member-query-interval 100
 ip igmp static-group 232.1.2.1 source ssm-map
 ip igmp version 3
 ip igmp explicit-tracking
 ip igmp limit 2
 ip igmp v3lite
 ip urd
!
.
.
.
!
ip pim ssm default
!
access-list 10 permit 232.1.2.10
access-list 11 permit 232.1.2.0 0.0.0.255
!
```

This table describes the significant commands shown in the SSM mapping configuration example.

Table 5: SSM Mapping Configuration Example Command Descriptions

Command	Description
no ip domain lookup	Disables IP DNS-based hostname-to-address translation. **Note** The **no ip domain-list** command is shown in the configuration only to demonstrate that disabling IP DNS-based hostname-to-address translation does not conflict with configuring SSM mapping. If this command is enabled, the Cisco IOS XE software will try to resolve unknown strings as hostnames.
ip domain multicast ssm-map.cisco.com	Specifies ssm-map.cisco.com as the domain prefix for SSM mapping.
ip name-server 10.48.81.21	Specifies 10.48.81.21 as the IP address of the DNS server to be used by SSM mapping and any other service in the software that utilizes DNS.
ip multicast-routing	Enables IP multicast routing.
ip igmp ssm-map enable	Enables SSM mapping.

Command	Description
ip igmp ssm-map static 10 172.16.8.10	Configures the groups permitted by ACL 10 to use source address 172.16.8.10. • In this example, ACL 10 permits all groups in the 232.1.2.0/25 range except 232.1.2.10.
ip igmp ssm-map static 11 172.16.8.11	Configures the groups permitted by ACL 11 to use source address 172.16.8.11. • In this example, ACL 11 permits group 232.1.2.10.
ip pim sparse-mode	Enables PIM sparse mode.
ip igmp last-member-query-interval 100	Reduces the leave latency for IGMPv2 hosts. **Note** This command is not required for configuring SSM mapping; however, configuring this command can be beneficial for IGMPv2 hosts relying on SSM mapping.
ip igmp static-group 232.1.2.1 source ssm-map	Configures SSM mapping to be used to determine the sources associated with group 232.1.2.1. The resulting (S, G) channels are statically forwarded.
ip igmp version 3	Enables IGMPv3 on this interface. **Note** This command is shown in the configuration only to demonstrate that IGMPv3 can be configured simultaneously with SSM mapping; however, it is not required.
ip igmp explicit-tracking	Minimizes the leave latency for IGMPv3 host leaving a multicast channel. **Note** This command is not required for configuring SSM mapping.
ip igmp limit 2	Limits the number of IGMP states resulting from IGMP membership states on a per-interface basis. **Note** This command is not required for configuring SSM mapping.
ip igmp v3lite	Enables the acceptance and processing of IGMP v3lite membership reports on this interface. **Note** This command is shown in the configuration only to demonstrate that IGMP v3lite can be configured simultaneously with SSM mapping; however, it is not required.
ip urd	Enables interception of TCP packets sent to the reserved URD port 465 on an interface and processing of URD channel subscription reports. **Note** This command is shown in the configuration only to demonstrate that URD can be configured simultaneously with SSM mapping; however, it is not required.

Command	Description
ip pim ssm default	Configures SSM service. The **default** keyword defines the SSM range access list as 232/8.
access-list 10 permit 232.1.2.10 **access-list 11 permit 232.1.2.0 0.0.0.255**	Configures the ACLs to be used for static SSM mapping. **Note** These are the ACLs that are referenced by the **ip igmp ssm-map static** commands in this configuration example.

DNS Server Configuration Example

To configure DNS-based SSM mapping, you need to create a DNS server zone or add records to an existing zone. If the routers that are using DNS-based SSM mapping are also using DNS for other purposes besides SSM mapping, you should use a normally-configured DNS server. If DNS-based SSM mapping is the only DNS implementation being used on the router, you can configure a fake DNS setup with an empty root zone, or a root zone that points back to itself.

The following example shows how to create a zone and import the zone data using Network Registrar:

```
Router> zone 1.1.232.ssm-map.cisco.com. create primary file=named.ssm-map
100 Ok
Router> dns reload
100 Ok
```

The following example shows how to import the zone files from a named.conf file for BIND 8:

```
Router> ::import named.conf /etc/named.conf
Router> dns reload
100 Ok:
```

Note Network Registrar version 8.0 and later support import BIND 8 format definitions.

Additional References

Related Documents

Related Topic	Document Title
SSM concepts and configuration	"Configuring Basic IP Multicast" module
Cisco IOS IP multicast commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	*Cisco IOS IP Multicast Command Reference*

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.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2365	*Administratively Scoped IP Multicast*
RFC 2770	*GLOP Addressing in 233/8*
RFC 3569	*An Overview of Source-Specific Multicast*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

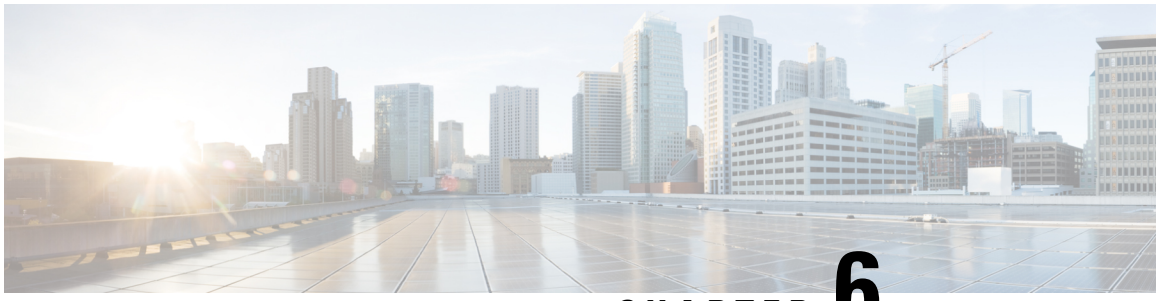
Feature Information for SSM Mapping

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 6: Feature Information for SSM Mapping

Feature Name	Releases	Feature Information
Source Specific Multicast (SSM) Mapping	12.3(2)T 12.2(18)S 12.2(18)SXD3 12.2(27)SBC 15.0(1)S Cisco IOS XE 3.1.0SG	This feature was introduced. The following commands were introduced or modified: **debug ip igmp, ip domain multicast, ip igmp ssm-map enable, ip igmp ssm-map query dns, ip igmp ssm-map static, ip igmp static-group, show ip igmp groups, show ip igmp ssm-mapping.**



CHAPTER 6

IGMP Snooping

This module describes how to enable and configure the Ethernet Virtual Connection (EVC)-based IGMP Snooping feature globally and on bridge domains.

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.

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 Snooping

IGMP Snooping

Multicast traffic becomes flooded because a device usually learns MAC addresses by looking into the source address field of all the frames that it receives. A multicast MAC address is never used as the source address for a packet. Such addresses do not appear in the MAC address table, and the device has no method for learning them.

IP Multicast Internet Group Management Protocol (IGMP), which runs at Layer 3 on a multicast device, generates Layer 3 IGMP queries in subnets where the multicast traffic must be routed. IGMP (on a device) sends out periodic general IGMP queries.

IGMP Snooping is an Ethernet Virtual Circuit (EVC)-based feature set. EVC decouples the concept of VLAN and broadcast domain. An EVC is an end-to-end representation of a single instance of a Layer 2 service being offered by a provider. In the Cisco EVC framework, bridge domains are made up of one or more Layer 2

interfaces known as service instances. A service instance is the instantiation of an EVC on a given port on a given device. A service instance is associated with a bridge domain based on the configuration.

Traditionally, a VLAN is a broadcast domain, and physical ports are assigned to VLANs as access ports; the VLAN tag in a packet received by a trunk port is the same number as the internal VLAN broadcast domain. With EVC, an Ethernet Flow Point (EFP) is configured and associated with a broadcast domain. The VLAN tag is used to identify the EFP only and is no longer used to identify the broadcast domain.

When you enable EVC-based IGMP snooping on a bridge domain, the bridge domain interface responds at Layer 2 to the IGMP queries with only one IGMP join request per Layer 2 multicast group. Each bridge domain represents a Layer 2 broadcast domain. The bridge domain interface creates one entry per subnet in the Layer 2 forwarding table for each Layer 2 multicast group from which it receives an IGMP join request. All hosts interested in this multicast traffic send IGMP join requests and are added to the forwarding table entry. During a Layer 2 lookup on a bridge domain to which the bridge domain interface belongs, the bridge domain forwards the packets to the correct EFP. When the bridge domain interface hears the IGMP Leave group message from a host, it removes the table entry of the host.

Layer 2 multicast groups learned through IGMP snooping are dynamic. However, you can statically configure Layer 2 multicast groups. If you specify group membership for a multicast group address statically, your static setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned-settings.

Restrictions for IGMP Snooping

- IGMP snooping is only supported on a Bridge Domain when OTV is enabled on ASR 1000 routers.
- If IGMP snooping is configured on a Bridge Domain with OTV enabled, then the IGMP snooping process limits the multicast traffic. In this scenario, the snooping tables are populated.
- If IGMP snooping is configured on a Bridge Domain without OTV, the IGMP snooping process does not limit multicast traffic. In this scenario, the snooping tables are not populated and the multicast traffic floods the entire VLAN.

How to Configure IGMP Snooping

Enabling IGMP Snooping

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip igmp snooping**
4. **bridge-domain** *bridge-id*
5. **ip igmp snooping**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip igmp snooping** **Example:** `Device(config)# ip igmp snooping`	Globally enables IGMP snooping after it has been disabled.
Step 4	**bridge-domain** *bridge-id* **Example:** `Device(config)# bridge-domain 100`	(Optional) Enters bridge domain configuration mode.
Step 5	**ip igmp snooping** **Example:** `Device(config-bdomain)# ip igmp snooping`	(Optional) Enables IGMP snooping on the bridge domain interface being configured. • Required only if IGMP snooping was previously explicitly disabled on the specified bridge domain.
Step 6	**end** **Example:** `Device(config-bdomain)# end`	Returns to privileged EXEC mode.

Configuring IGMP Snooping Globally

Perform this task to modify the global configuration for IGMP snooping.

Before you begin

IGMP snooping must be enabled. IGMP snooping is enabled by default.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip igmp snooping robustness-variable** *variable*
4. **ip igmp snooping tcn query solicit**
5. **ip igmp snooping tcn flood query count** *count*

6. **ip igmp snooping report-suppression**
7. **ip igmp snooping explicit-tracking-limit** *limit*
8. **ip igmp snooping last-member-query-count** *count*
9. **ip igmp snooping last-member-query-interval** *interval*
10. **ip igmp snooping check** { **ttl** | **rtr-alert-option** }
11. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip igmp snooping robustness-variable** *variable* **Example:** `Device(config)# ip igmp snooping robustness-variable 3`	(Optional) Configures IGMP snooping robustness variable.
Step 4	**ip igmp snooping tcn query solicit** **Example:** `Device(config)# ip igmp snooping tcn query solicit`	(Optional) Enables device to send TCN query solicitation even if it is not the spanning-tree root.
Step 5	**ip igmp snooping tcn flood query count** *count* **Example:** `Device(config)# ip igmp snooping tcn flood query count 4`	(Optional) Configures the TCN flood query count for IGMP snooping.
Step 6	**ip igmp snooping report-suppression** **Example:** `Device(config)# ip igmp snooping report-suppression`	(Optional) Enables report suppression for IGMP snooping.
Step 7	**ip igmp snooping explicit-tracking-limit** *limit* **Example:** `Device(config)# ip igmp snooping explicit-tracking-limit 200`	(Optional) Limits the number of reports in the IGMP snooping explicit-tracking database.

	Command or Action	Purpose
Step 8	**ip igmp snooping last-member-query-count** *count* **Example:** `Device (config)# ip igmp snooping last-member-query-count 5`	(Optional) Configures how often Internet Group Management Protocol (IGMP) snooping will send query messages in response to receiving an IGMP leave message. The default is 2 milliseconds.
Step 9	**ip igmp snooping last-member-query-interval** *interval* **Example:** `Device (config)# ip igmp snooping last-member-query-interval 200`	(Optional) Configures the length of time after which the group record is deleted if no reports are received. The default is 1000 milliseconds.
Step 10	**ip igmp snooping check** { **ttl** | **rtr-alert-option** } **Example:** `Device (config)# ip igmp snooping check ttl`	(Optional) Enforces IGMP snooping check.
Step 11	**exit** **Example:** `Device (config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring IGMP Snooping on a Bridge Domain Interface

Perform this task to modify the IGMP snooping configuration on a bridge domain interface.

Before you begin

- The bridge domain interface must be created. See the "Configuring Bridge Domain Interfaces" section of the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*.
- IGMP snooping must be enabled on the interface to be configured. IGMP snooping is enabled by default.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bridge-domain** *bridge-id*
4. **ip igmp snooping immediate-leave**
5. **ip igmp snooping robustness-variable** *variable*
6. **ip igmp snooping report-suppression**
7. **ip igmp snooping explicit-tracking**
8. **ip igmp snooping explicit-tracking-limit** *limit*
9. **ip igmp snooping last-member-query-count** *count*
10. **ip igmp snooping last-member-query-interval** *interval*
11. **ip igmp snooping access-group** {*acl-number* | *acl-name*}

12. **ip igmp snooping limit** *num* [**except** {*acl-number* | *acl-name*}]
13. **ip igmp snooping minimum-version** {**2** | **3**}
14. **ip igmp snooping check** { **ttl** | **rtr-alert-option** }
15. **ip igmp snooping static source** *source-address* **interface** *port-type port-number*
16. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**bridge-domain** *bridge-id* **Example:** `Device(config)# bridge-domain 100`	Enters bridge domain configuration mode.
Step 4	**ip igmp snooping immediate-leave** **Example:** `Device(config-bdomain)# ip igmp snooping immediate-leave`	(Optional) Enables IGMPv2 immediate-leave processing. **Note** When both immediate-leave processing and the query count are configured, fast-leave processing takes precedence.
Step 5	**ip igmp snooping robustness-variable** *variable* **Example:** `Device(config-bdomain)# ip igmp snooping robustness-variable 3`	(Optional) Configures the IGMP snooping robustness variable. The default is 2.
Step 6	**ip igmp snooping report-suppression** **Example:** `Device(config-bdomain)# ip igmp snooping report-suppression`	(Optional) Enables report suppression for all hosts on the bridge domain interface.
Step 7	**ip igmp snooping explicit-tracking** **Example:** `Device(config-bdomain)#  ip igmp snooping explicit-tracking`	(Optional) Enables IGMP snooping explicit tracking. Explicit tracking is enabled by default.
Step 8	**ip igmp snooping explicit-tracking-limit** *limit* **Example:**	(Optional) Limits the number of reports in the IGMP snooping explicit-tracking database.

	Command or Action	Purpose
	`Device(config-bdomain)# ip igmp snooping explicit-tracking-limit 200`	
Step 9	**ip igmp snooping last-member-query-count** *count* **Example:** `Device(config-bdomain)# ip igmp snooping last-member-query-count 5`	(Optional) Configures the interval for snooping query messages sent in response to receiving an IGMP leave message. The default is 2 milliseconds. **Note** When both immediate-leave processing and the query count are configured, fast-leave processing takes precedence.
Step 10	**ip igmp snooping last-member-query-interval** *interval* **Example:** `Device(config-bdomain)#  ip igmp snooping last-member-query-interval 2000`	(Optional) Configures the length of time after which the group record is deleted if no reports are received. The default is 1000 milliseconds.
Step 11	**ip igmp snooping access-group** {*acl-number* | *acl-name*} **Example:** `Device(config-bdomain)# ip igmp snooping access-group 1300`	Configures ACL-based filtering on a bridge domain.
Step 12	**ip igmp snooping limit** *num* [**except** {*acl-number* | *acl-name*}] **Example:** `Device(config-bdomain)# ip igmp snooping 4400 except test1`	(Optional) Limits the number of groups or channels allowed on a bridge domain.
Step 13	**ip igmp snooping minimum-version** {**2** | **3**} **Example:** `Device(config-bdomain)# ip igmp snooping minimum-version 2`	(Optional) Configures IGMP protocol filtering.
Step 14	**ip igmp snooping check** { **ttl** | **rtr-alert-option** } **Example:** `Device(config-bdomain)# ip igmp snooping check ttl`	(Optional) Enforces IGMP snooping check.
Step 15	**ip igmp snooping static source** *source-address* **interface** *port-type port-number* **Example:** `Device(config-bdomain)# ip igmp snooping static source 192.0.2.1 interface gigbitethernet 1/1/1`	(Optional) Configures a host statically for a Layer 2 LAN port.

	Command or Action	Purpose
Step 16	**end** **Example:** `Device(config-bdomain)# end`	Returns to privileged EXEC mode.

Configuring an EFP

Perform this task to configure IGMP snooping features on an EFP.

Before you begin

The EFP and bridge domain must be previously configured. Configuring a service instance on a Layer 2 port creates a pseudoport or Ethernet Flow Point (EFP) on which you configure Ethernet Virtual Connection (EVC) features. See the "Configuring Ethernet Virtual Connections on the Cisco ASR 1000 Router" section of the *Carrier Ethernet Configuration Guide* for configuration information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router-guard ip multicast efps**
4. **interface** *type number*
5. **service instance** *id* **ethernet**
6. **router-guard multicast**
7. **ip igmp snooping tcn flood**
8. **ip igmp snooping access-group** {*acl-number* | *acl-name*}
9. **ip igmp snooping limit** *num* [**except** {*acl-number* | *acl-name*}]
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router-guard ip multicast efps** **Example:** `Device(config)# router-guard ip multicast efps`	(Optional) Enables the router guard for all EFPs.

	Command or Action	Purpose
Step 4	**interface** *type number* **Example:** `Device(config)# interface BDI100`	(Optional) Specifies the bridge domain interface to be configured.
Step 5	**service instance** *id* **ethernet** **Example:** `Device(config-if)# service instance 333 ethernet`	(Optional) Enters Ethernet service configuration mode for configuring the EFP.
Step 6	**router-guard multicast** **Example:** `Device(config-if-srv)# router-guard multicast`	(Optional) Configures a router guard on an EFP.
Step 7	**ip igmp snooping tcn flood** **Example:** `Device(config-if-srv)# no ip igmp snooping tcn flood`	(Optional) Disables TCN flooding on an EFP. TCN flooding is enabled by default.
Step 8	**ip igmp snooping access-group** {*acl-number* | *acl-name*} **Example:** `Device(config-if-srv)# ip igmp snooping access-group 44`	(Optional) Configures ACL-based filtering on an EFP.
Step 9	**ip igmp snooping limit** *num* [**except** {*acl-number* | *acl-name*}] **Example:** `Device(config-if-srv)# ip igmp snooping limit 1300 except test1`	(Optional) Limits the number of IGMP groups or channels allowed on an EFP.
Step 10	**end** **Example:** `Device(config-if-srv)# end`	Returns to privileged EXEC mode.

Verifying IGMP Snooping

SUMMARY STEPS

1. **enable**
2. **show igmp snooping** [**count** [**bd** *bd-id*]]
3. **show igmp snooping groups bd** *bd-id* [**count** | *ip-address* [**verbose**] [**hosts** | **sources** | **summary**]]

4. **show igmp snooping membership bd** *bd-id*
5. **show igmp snooping mrouter** [**bd** *bd-id*]
6. **show igmp snooping counters** [**bd** *bd-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show igmp snooping** [**count** [**bd** *bd-id*]] **Example:** `Device(config)# show igmp snooping`	Displays configuration for IGMP snooping, globally or by bridge domain.
Step 3	**show igmp snooping groups bd** *bd-id* [**count** | *ip-address* [**verbose**] [**hosts** | **sources** | **summary**]] **Example:** `Device(config)# show igmp snooping groups bd 100`	Displays snooping information for groups by bridge domain.
Step 4	**show igmp snooping membership bd** *bd-id* **Example:** `Device(config)# show igmp snooping membership bd 100`	Displays IGMPv3 host membership information.
Step 5	**show igmp snooping mrouter** [**bd** *bd-id*] **Example:** `Device(config)# show igmp snooping mrouter`	Displays multicast ports, globally or by bridge domain.
Step 6	**show igmp snooping counters** [**bd** *bd-id*] **Example:** `Device(config)# show snooping counters`	Displays IGMP snooping counters, globally or by bridge domain.

Additional References

Technical Assistance

Description	Link
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.	http://www.cisco.com/cisco/web/support/index.html

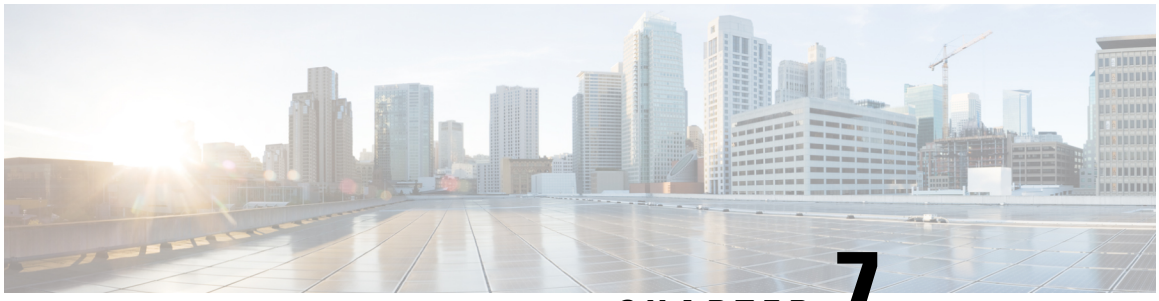
Feature Information for IGMP Snooping

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 7: Feature Information for Configuring IGMP Snooping

Feature Name	Releases	Feature Information
IGMP Snooping	Cisco IOS XE Release 3.5S 15.2(4)S	IGMP snooping is an IP multicast constraining mechanism based on the Ethernet Virtual Connection (EVC) infrastructure. IGMP snooping examines Layer 3 information (IGMP Join/Leave messages) in the IGMP packets sent between hosts and routers. The following commands were introduced or modified: **ip igmp snooping**, **ip igmp snooping check**, **ip igmp snooping explicit-track ing limit**, **ip igmp snooping immediate leave**, **ip igmp snooping last-member-query count**, **ip igmp snooping last-member-query interval**, **ip igmp snooping report-suppression**, **ip igmp snooping robustness-variable**, **ip igmp snooping static**, **ip igmp snooping tcn flood** (if-srv), **ip igmp snooping tcn flood query**, **ip igmp snooping tcn flood query solicit**, **router guard ip multicast efps**



CHAPTER 7

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

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.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface ethernet 1`	Selects an interface that is connected to hosts on which IGMPv3 can be enabled.
Step 4	**ip cgmp** [**proxy**	**router-only**] **Example:** `Device(config-if)# ip cgmp proxy`	Enables CGMP on an interface of a device connected to a Cisco Catalyst 5000 family switch. • The **proxy** 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.

	Command or Action	Purpose
Step 5	**end** **Example:** `Device(config-if)# end`	Ends the current configuration session and returns to EXEC mode.
Step 6	**clear ip cgmp** [*interface-type interface-number*] **Example:** `Device# 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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface ethernet 1`	Selects an interface that is connected to hosts.
Step 4	**ip rgmp** **Example:**	Enables RGMP on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces.

	Command or Action	Purpose
	`Device(config-if)# ip rgmp`	
Step 5	**end** **Example:** `Device(config-if)# end`	Ends the current configuration session and returns to EXEC mode.
Step 6	**debug ip rgmp** **Example:** `Device# debug ip rgmp`	(Optional) Logs debug messages sent by an RGMP-enabled device.
Step 7	**show ip igmp interface** **Example:** `Device# show ip igmp interface`	(Optional) Displays multicast-related information about an interface.

Configuration Examples for Constraining IP Multicast in a Switched Ethernet Network

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.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS IP SLAs commands	Cisco IOS IP Multicast Command Reference
IGMP snooping	The "IGMP Snooping" module of the *IP Multicast: IGMP Configuration Guide*
RGMP	The "Configuring Router-Port Group Management Protocol" module of the *IP Multicast: IGMP Configuration Guide*

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: http://www.cisco.com/go/mibs

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.	http://www.cisco.com/public/support/tac/home.shtml

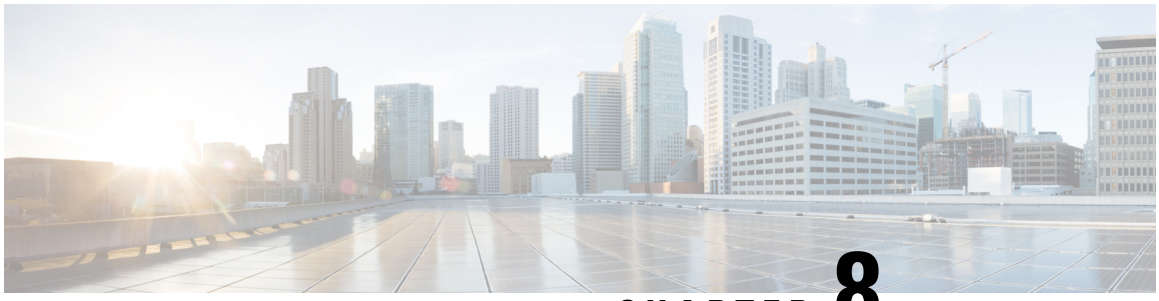
Feature Information for Constraining IP Multicast in a Switched Ethernet Network

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 8: 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.



CHAPTER 8

Configuring Router-Port Group Management Protocol

Router-Port Group Management Protocol (RGMP) is a Cisco protocol that restricts IP multicast traffic in switched networks. RGMP is a Layer 2 protocol that enables a router to communicate to a switch (or a networking device that is functioning as a Layer 2 switch) the multicast group for which the router would like to receive or forward traffic. RGMP restricts multicast traffic at the ports of RGMP-enabled switches that lead to interfaces of RGMP-enabled routers.

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.

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 RGMP

Before you enable RGMP, ensure that the following features are enabled on your router:

- IP routing
- IP multicast
- PIM in sparse mode, sparse-dense mode, source specific mode, or bidirectional mode

If your router is in a bidirectional group, make sure to enable RGMP only on interfaces that do not function as a designated forwarder (DF). If you enable RGMP on an interface that functions as a DF, the interface will not forward multicast packets up the bidirectional shared tree to the rendezvous point (RP).

You must have the following features enabled on your switch:

- IP multicast
- IGMP snooping

Note Refer to the Catalyst switch software documentation for RGMP switch configuration tasks and command information.

Information About RGMP

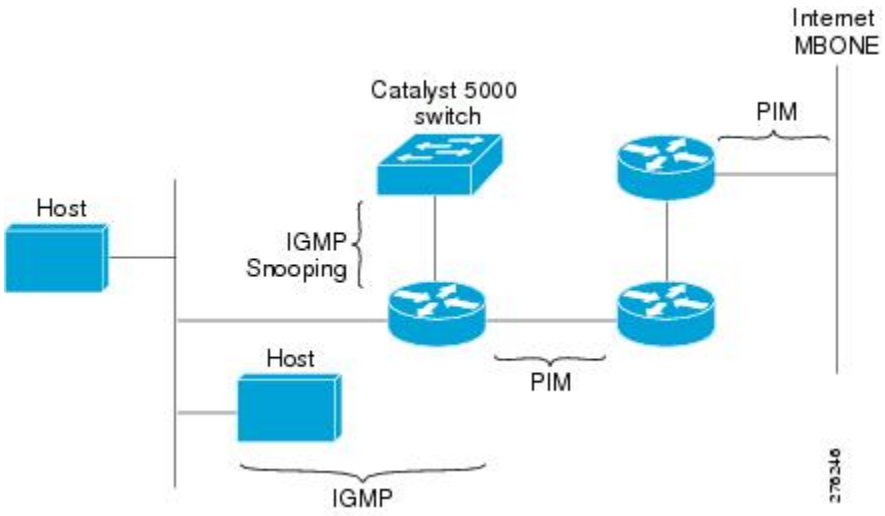
IP Multicast Routing Overview

The software supports the following protocols to implement IP multicast routing:

- Internet Group Management Protocol (IGMP) is used between hosts on a LAN and the routers on that LAN to track the multicast groups of which hosts are members.
- Protocol Independent Multicast (PIM) is used between routers so that they can track which multicast packets to forward to each other and to their directly connected LANs.
- Cisco Group Management Protocol (CGMP) is a protocol used on routers connected to Catalyst switches to perform tasks similar to those performed by IGMP.
- RGMP is a protocol used on routers connected to Catalyst switches or networking devices functioning as Layer 2 switches to restrict IP multicast traffic. Specifically, the protocol enables a router to communicate to a switch the IP multicast group for which the router would like to receive or forward traffic.

The figure shows where these protocols operate within the IP multicast environment.

Figure 2: IP Multicast Routing Protocols



Note CGMP and RGMP cannot interoperate on the same switched network. If RGMP is enabled on a switch or router interface, CGMP is automatically disabled on that switch or router interface; if CGMP is enabled on a switch or router interface, RGMP is automatically disabled on that switch or router interface.

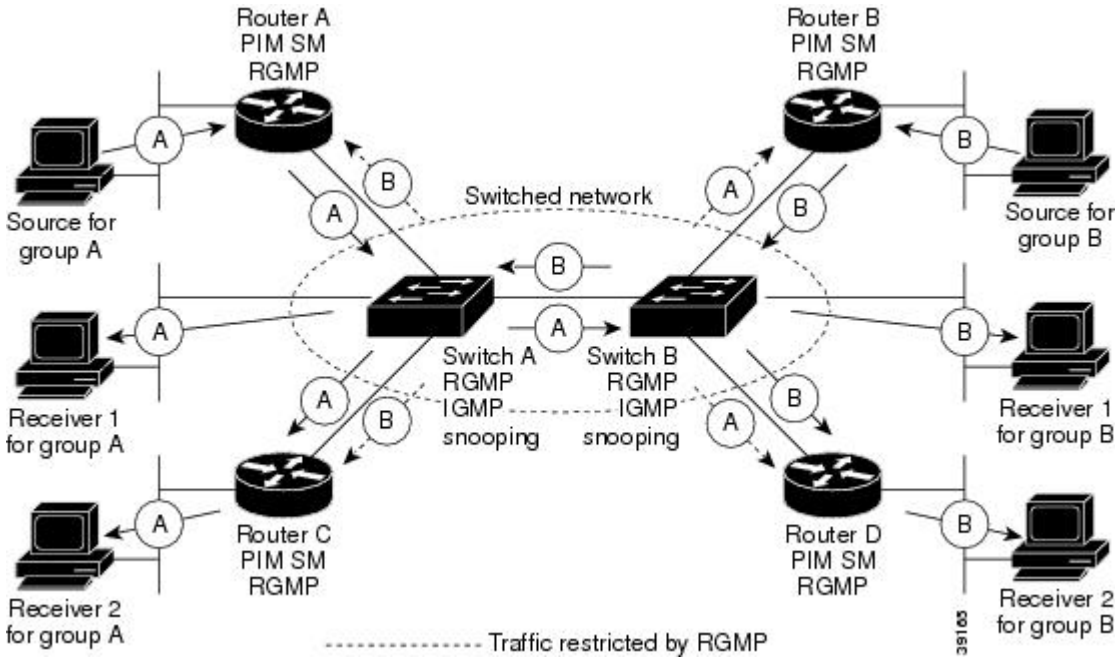
RGMP Overview

RGMP enables a router to communicate to a switch the IP multicast group for which the router would like to receive or forward traffic. RGMP is designed for switched Ethernet backbone networks running PIM sparse mode (PIM-SM) or sparse-dense mode.

Note RGMP-enabled switches and router interfaces in a switched network support directly connected, multicast-enabled hosts that receive multicast traffic. RGMP-enabled switches and router interfaces in a switched network do not support directly connected, multicast-enabled hosts that source multicast traffic. A multicast-enabled host can be a PC, a workstation, or a multicast application running in a router.

The figure shows a switched Ethernet backbone network running PIM in sparse mode, RGMP, and IGMP snooping.

Figure 3: RGMP in a Switched Network

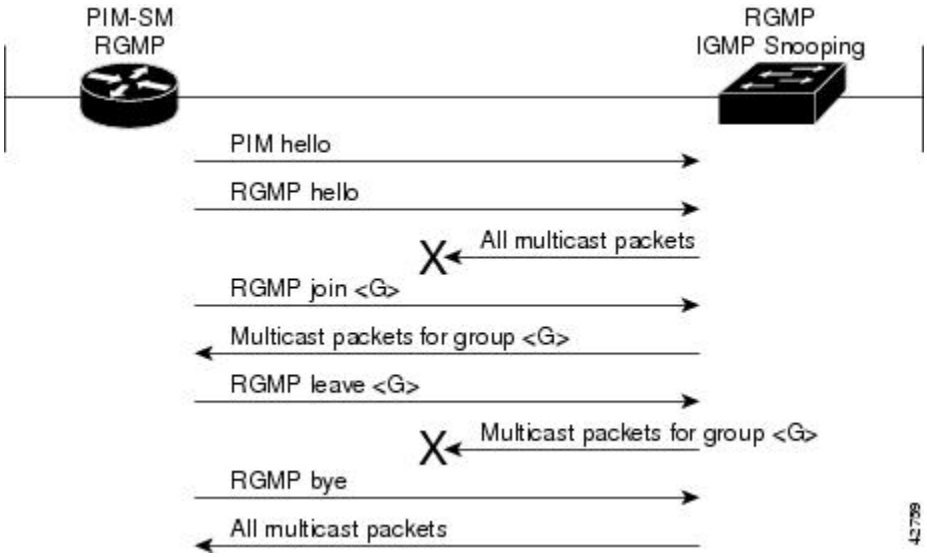


In the figure, the sources for the two different multicast groups (the source for group A and the source for group B) send traffic into the same switched network. Without RGMP, traffic from source A is unnecessarily flooded from switch A to switch B, then to router B and router D. Also, traffic from source B is unnecessarily flooded from switch B to switch A, then to router A and router C. With RGMP enabled on all routers and switches in this network, traffic from source A would not flood router B and router D. Also, traffic from source B would not flood router A and router C. Traffic from both sources would still flood the link between switch A and switch B. Flooding over this link would still occur because RGMP does not restrict traffic on links toward other RGMP-enabled switches with routers behind them.

By restricting unwanted multicast traffic in a switched network, RGMP increases the available bandwidth for all other multicast traffic in the network and saves the processing resources of the routers.

The figure shows the RGMP messages sent between an RGMP-enabled router and an RGMP-enabled switch.

Figure 4: RGMP Messages



The router sends simultaneous PIM hello (or a PIM query message if PIM Version 1 is configured) and RGMP hello messages to the switch. The PIM hello message is used to locate neighboring PIM routers. The RGMP hello message instructs the switch to restrict all multicast traffic on the interface from which the switch received the RGMP hello message.

Note RGMP messages are sent to the multicast address 224.0.0.25, which is the local-link multicast address reserved by the Internet Assigned Numbers Authority (IANA) for sending IP multicast traffic from routers to switches. If RGMP is not enabled on both the router and the switch, the switch automatically forwards all multicast traffic out the interface from which the switch received the PIM hello message.

The router sends the switch an RGMP join <G> message (where G is the multicast group address) when the router wants to receive traffic for a specific multicast group. The RGMP join message instructs the switch to forward multicast traffic for group <G> out the interface from which the switch received the RGMP hello message.

Note The router sends the switch an RGMP join <G> message for a multicast group even if the router is only forwarding traffic for the multicast group into a switched network. By joining a specific multicast group, the router can determine if another router is also forwarding traffic for the multicast group into the same switched network. If two routers are forwarding traffic for a specific multicast group into the same switched network, the two routers use the PIM assert mechanism to determine which router should continue forwarding the multicast traffic into the network.

The router sends the switch an RGMP leave <G> message when the router wants to stop receiving traffic for a specific multicast group. The RGMP leave message instructs the switch to stop forwarding the multicast traffic on the port from which the switch received the PIM and RGMP hello messages.

Note An RGMP-enabled router cannot send an RGMP leave <G> message until the router does not receive or forward traffic from any source for a specific multicast group (if multiple sources exist for a specific multicast group).

The router sends the switch an RGMP bye message when RGMP is disabled on the router. The RGMP bye message instructs the switch to forward the router all IP multicast traffic on the port from which the switch received the PIM and RGMP hello messages, as long as the switch continues to receive PIM hello messages on the port.

How to Configure RGMP

Enabling RGMP

To enable RGMP, use the following commands on all routers in your network beginning in global configuration mode:

Note CGMP and RGMP cannot interoperate on the same switched network. If RGMP is enabled on a switch or router interface, CGMP is automatically disabled on that switch or router interface; if CGMP is enabled on a switch or router interface, RGMP is automatically disabled on that switch or router interface.

SUMMARY STEPS

1. **interface** *type number*
2. **ip rgmp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface** *type number*	Specifies the router interface on which you want to configure RGMP and enters interface configuration mode.
Step 2	**ip rgmp**	Enables RGMP on a specified interface.

What to do next

See the "RGMP_Configuration_Example" section for an example of how to configure RGMP.

Verifying RGMP Configuration

To verify that RGMP is enabled on the correct interfaces, use the **show ip igmp interface**command:

```
Router> show ip igmp interface
gigabitethernet1/0 is up, line protocol is up
```

```
Internet address is 10.0.0.0/24
  IGMP is enabled on interface
Current IGMP version is 2
  RGMP is enabled
IGMP query interval is 60 seconds
IGMP querier timeout is 120 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1000 ms
Inbound IGMP access group is not set
IGMP activity: 1 joins, 0 leaves
Multicast routing is enabled on interface
Multicast TTL threshold is 0
Multicast designated router (DR) is 10.0.0.0 (this system)
IGMP querying router is 10.0.0.0 (this system)
Multicast groups joined (number of users):
    224.0.1.40(1)
```

Note If RGMP is not enabled on an interface, no RGMP information is displayed in the **show ip igmp interface** command output for that interface.

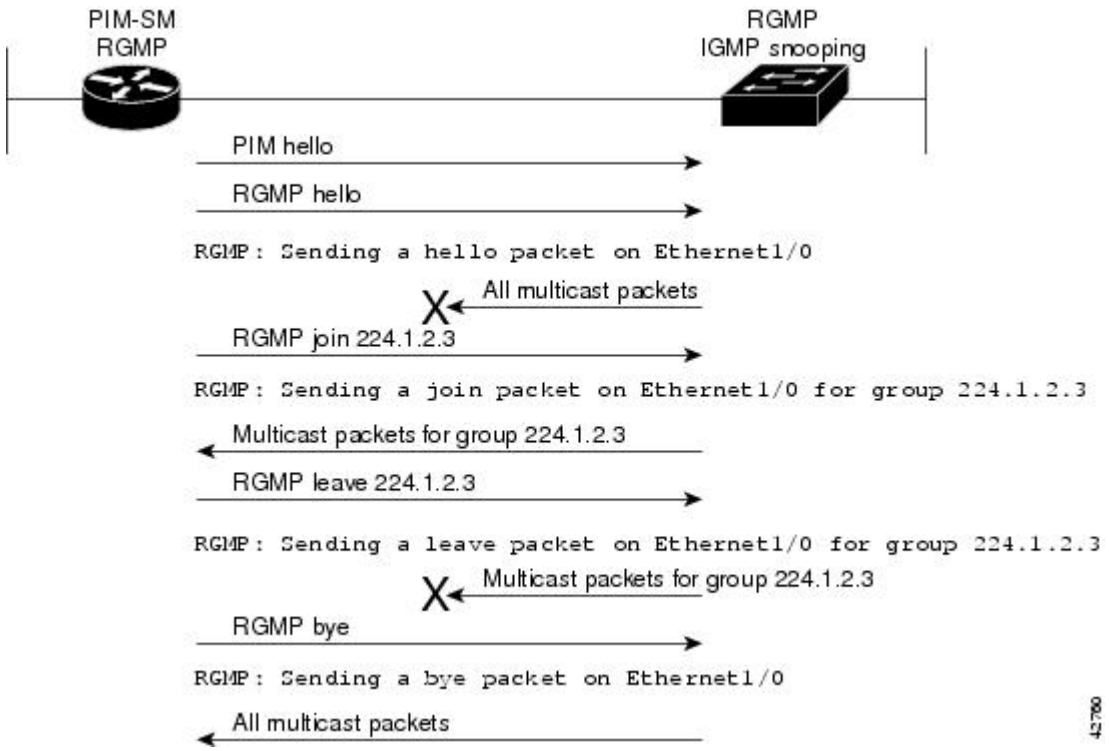
Monitoring and Maintaining RGMP

To enable RGMP debugging, use the following command in privileged EXEC mode:

Command	Purpose
`Router# debug ip rgmp`	Logs debug messages sent by an RGMP-enabled router. Using the command without arguments logs RGMP Join <G> and RGMP leave <G> messages for all multicast groups configured on the router. Using the command with arguments logs RGMP join <G> and RGMP leave <G> messages for the specified group.

The figure shows the debug messages that are logged by an RGMP-enabled router as the router sends RGMP join <G> and RGMP leave <G> messages to an RGMP-enabled switch.

Figure 5: RGMP Debug Messages

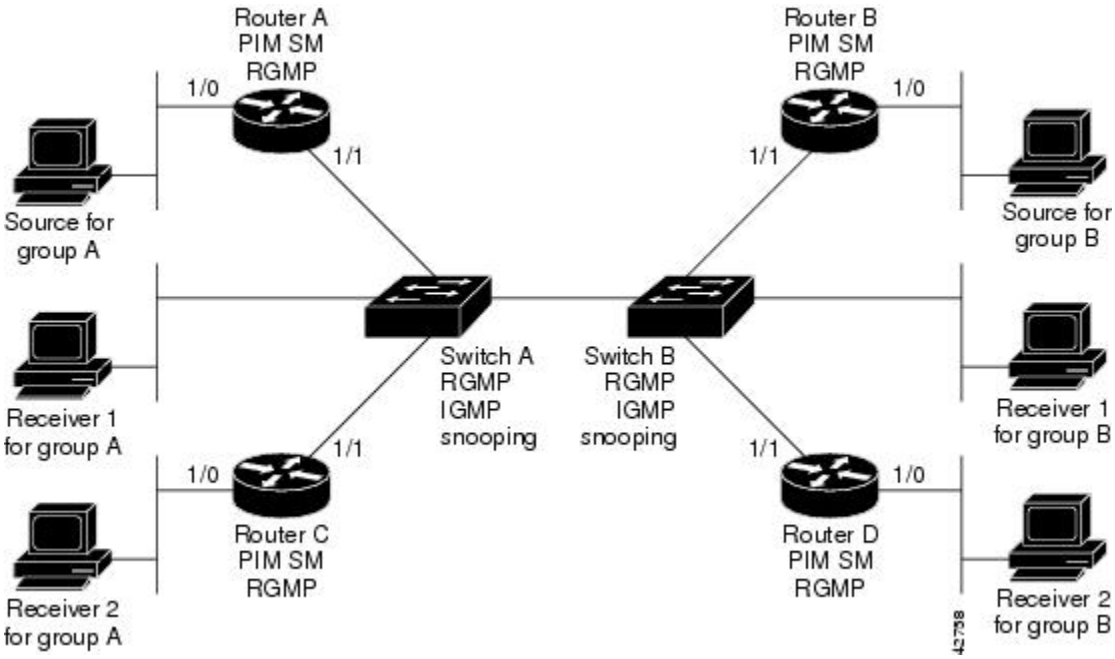


Configuration Examples for RGMP

RGMP Configuration Example

This section provides an RGMP configuration example that shows the individual configurations for the routers and switches shown in the figure.

Figure 6: RGMP Configuration Example



Router A Configuration

```
ip routing
ip multicast-routing distributed
interface gigabitethernet 1/0/0
  ip address 10.0.0.1 255.0.0.0
  ip pim sparse-dense-mode
  no shutdown
interface gigabitethernet 1/1/0
  ip address 10.1.0.1 255.0.0.0
  ip pim sparse-dense-mode
  ip rgmp
  no shutdown
```

Router B Configuration

```
ip routing
ip multicast-routing distributed
interface gigabitethernet 1/0/0
  ip address 10.2.0.1 255.0.0.0
  ip pim sparse-dense-mode
  no shutdown
interface gigabitethernet 1/1/0
  ip address 10.3.0.1 255.0.0.0
  ip pim sparse-dense-mode
  ip rgmp
  no shutdown
```

Router C Configuration

```
ip routing
```

```
ip multicast-routing distributed
interface gigabitethernet 1/0/0
  ip address 10.4.0.1 255.0.0.0
  ip pim sparse-dense-mode
  no shutdown
interface gigabitethernet 1/1/0
  ip address 10.5.0.1 255.0.0.0
  ip pim sparse-dense-mode
  ip rgmp
  no shutdown
```

Router D Configuration

```
ip routing
ip multicast-routing distributed
interface gigabitethernet 1/0/0
  ip address 10.6.0.1 255.0.0.0
  ip pim sparse-dense-mode
  no shutdown
interface gigabitethernet 1/1/0
  ip address 10.7.0.1 255.0.0.0
  ip pim sparse-dense-mode
  ip rgmp
  no shutdown
```

Switch A Configuration

```
Switch> (enable) set igmp enable
Switch> (enable) set rgmp enable
```

Switch B Configuration

```
Switch> (enable) set igmp enable
Switch> (enable) set rgmp enable
```

Additional References

The following sections provide references related to RGMP.

Related Documents

Related Topic	Document Title
PIM-SM and SSM concepts and configuration examples	“ Configuring Basic IP Multicast ” module
IP multicast commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	*Cisco IOS IP Multicast Command Reference*

Standards

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

MIBs

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

RFCs

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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

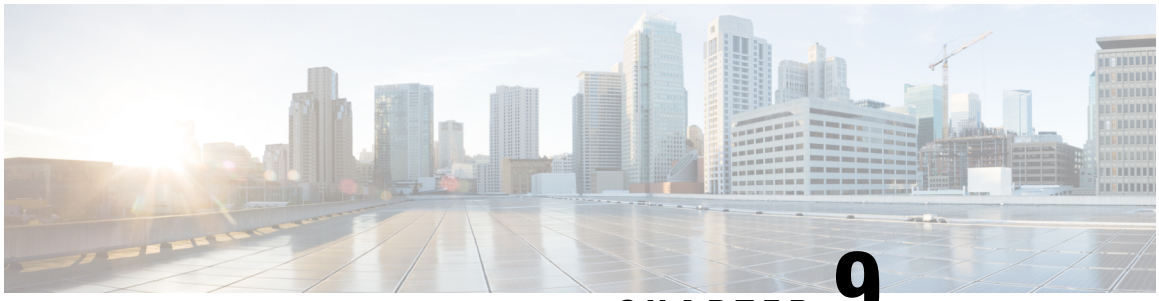
Feature Information for Router-Port Group Management Protocol

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 9: Feature Information for Router-Port Group Management Protocol

Feature Name	Releases	Feature Information
Router-Port Group Management Protocol	Cisco IOS XE Release 2.1	Router-Port Group Management Protocol (RGMP) is a Cisco protocol that restricts IP multicast traffic in switched networks. RGMP is a Layer 2 protocol that enables a router to communicate to a switch (or a networking device that is functioning as a Layer 2 switch) the multicast group for which the router would like to receive or forward traffic. RGMP restricts multicast traffic at the ports of RGMP-enabled switches that lead to interfaces of RGMP-enabled routers



CHAPTER 9

Configuring IP Multicast over Unidirectional Links

IP multicast requires bidirectional communication, yet some networks include broadcast satellite links, which are unidirectional. Unidirectional link routing (UDLR) provides three mechanisms for a router to emulate a bidirectional link to enable the routing of unicast and multicast packets over a physical unidirectional interface, such as a broadcast satellite link. The mechanisms are a UDLR tunnel, Internet Group Management Protocol (IGMP) UDLR, and IGMP proxy. This document describes a UDLR tunnel and IGMP UDLR. IGMP proxy is described in the " Customizing IGMP " module. The three mechanisms may be used independently or in combination.

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.

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 UDLR

- You understand the concepts in the " IP Multicast Technology Overview " module.
- You have IP multicast configured in your network. Refer to the " Configuring Basic IP Multicast " module.

Information About UDLR

UDLR Overview

Both unicast and multicast routing protocols forward data on interfaces from which they have received routing control information. This model requires a bidirectional link. However, some network links are unidirectional. For networks that are unidirectional (such as broadcast satellite links), a method of communication that allows for control information to operate in a unidirectional environment is necessary. (Note that IGMP is not a routing protocol.)

Specifically, in unicast routing, when a router receives an update message on an interface for a prefix, it forwards data for destinations that match that prefix out that same interface. This is the case in distance vector routing protocols. Similarly, in multicast routing, when a router receives a Join message for a multicast group on an interface, it forwards copies of data destined for that group out that same interface. Based on these principles, unicast and multicast routing protocols cannot be supported over UDLs without the use of UDLR. UDLR is designed to enable the operation of routing protocols over UDLs without changing the routing protocols themselves.

UDLR enables a router to emulate the behavior of a bidirectional link for IP operations over UDLs. UDLR has three complementary mechanisms for bidirectional link emulation, which are described in the following sections:

- UDLR Tunnel--A mechanism for routing unicast and multicast traffic.
- Internet Group Management Protocol (IGMP) UDLR--Mechanism for routing multicast traffic. This method scales well for many broadcast satellite links.
- IGMP Proxy--Mechanism for routing multicast traffic.

You can use each mechanism independently or in conjunction with the others. IGMP proxy is described in the “ Customizing IGMP ” module.

UDLR Tunnel

The UDLR tunnel mechanism enables IP and its associated unicast and multicast routing protocols to treat the unidirectional link (UDL) as being logically bidirectional. A packet that is destined on a receive-only interface is picked up by the UDLR tunnel mechanism and sent to an upstream router using a generic routing encapsulation (GRE) tunnel. The control traffic flows in the opposite direction of the user data flow. When the upstream router receives this packet, the UDLR tunnel mechanism makes it appear that the packet was received on a send-only interface on the UDL.

The purpose of the unidirectional GRE tunnel is to move control packets from a downstream node to an upstream node. The one-way tunnel is mapped to a one-way interface (that goes in the opposite direction). Mapping is performed at the link layer, so the one-way interface appears bidirectional. When the upstream node receives packets over the tunnel, it must make the upper-layer protocols act as if the packets were received on the send-capable UDL.

A UDLR tunnel supports the following functionality:

- Address Resolution Protocol (ARP) and Next Hop Resolution Protocol (NHRP) over a UDL

- Emulation of bidirectional links for all IP traffic (as opposed to only control-only broadcast/multicast traffic)
- Support for IP GRE multipoint at a receive-only tunnel

Note A UDL router can have many routing peers (for example, routers interconnected via a broadcast satellite link). As with bidirectional links, the number of peer routers a router has must be kept relatively small to limit the volume of routing updates that must be processed. For multicast operation, we recommend using the IGMP UDLR mechanism when interconnecting more than 20 routers.

IGMP UDLR

In addition to a UDLR tunnel, another mechanism that enables support of multicast routing protocols over UDLs is using IP multicast routing with IGMP, which accommodates UDLR. This mechanism scales well for many broadcast satellite links.

With IGMP UDLR, an upstream router sends periodic queries for members on the UDL. The queries include a unicast address of the router that is not the unicast address of the unidirectional interface. The downstream routers forward IGMP reports received from directly connected members (on interfaces configured to helper forward IGMP reports) to the upstream router. The upstream router adds the unidirectional interface to the (*, G) outgoing interface list, thereby enabling multicast packets to be forwarded down the UDL.

In a large enterprise network, it is not possible to be able to receive IP multicast traffic via satellite and forward the traffic throughout the network. This limitation exists because receiving hosts must be directly connected to the downstream router. However, you can use the IGMP proxy mechanism to overcome this limitation. Refer to the " Customizing IGMP " module for more information on this mechanism.

How to Route IP Multicast over Unidirectional Links

This section includes the following procedures. You can do either or both in your network.

Configuring a UDLR Tunnel

To configure a UDLR tunnel, perform the task in this section. The tunnel mode defaults to GRE. You need not assign an IP address to the tunnel (you need not use the **ip address** or **ip unnumbered** commands). You must configure the tunnel endpoint addresses.

You must configure both the upstream and downstream routers to meet the following conditions:

- On the upstream router, where the UDL can only send, you must configure the tunnel to receive. When packets are received over the tunnel, the upper-layer protocols treat the packet as though it is received over the unidirectional, send-only interface.
- On the downstream router, where the UDL can only receive, you must configure the tunnel to send. When packets are sent by upper-layer protocols over the interface, they will be redirected and sent over this GRE tunnel.

Before you begin

Before configuring UDLR tunnel, ensure that all routers on the UDL have the same subnet address. If all routers on the UDL cannot have the same subnet address, the upstream router must be configured with secondary addresses to match all the subnets that the downstream routers are attached to.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **interface tunnel** *number*
5. **tunnel udlr receive-only** *type number*
6. **tunnel source** {ip-address | *type number*}
7. **tunnel destination** {*hostname*| ip-address}
8. Move to the downstream router.
9. **enable**
10. **configure terminal**
11. **interface** *type number*
12. **interface tunnel** *number*
13. **tunnel udlr send-only** *type number*
14. **tunnel source** {ip-address | *type number*}
15. **tunnel destination** {*hostname*| ip-address}
16. **tunnel udlr address-resolution**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted. • Do this step on the upstream router.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/0/0`	Configures the unidirectional send-only interface.
Step 4	**interface tunnel** *number* **Example:** `Router(config-if)# interface tunnel 0`	Configures the receive-only tunnel interface.

	Command or Action	Purpose
Step 5	**tunnel udlr receive-only** *type number* **Example:** `Router(config-if)# tunnel udlr receive-only fastethernet 0/0/0`	Configures the UDLR tunnel. • Use the same *type* and *number* values as the unidirectional send-only interface *type* and *number* values specified with the **interface** *type number* command in Step 3.
Step 6	**tunnel source** {ip-address | *type number*} **Example:** `Router(config-if)# tunnel source 10.3.4.5`	Configures the tunnel source.
Step 7	**tunnel destination** {*hostname*| ip-address} **Example:** `Router(config-if)# tunnel destination 10.8.2.3`	Configures the tunnel destination.
Step 8	Move to the downstream router.	--
Step 9	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 10	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 11	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/0/0`	Configures the unidirectional receive-only interface.
Step 12	**interface tunnel** *number* **Example:** `Router(config-if)# interface tunnel 0`	Configures the send-only tunnel interface.
Step 13	**tunnel udlr send-only** *type number* **Example:** `Router(config-if)# tunnel udlr send-only ethernet 0`	Configures the UDLR tunnel. • Use the same *type* and *number* values as the unidirectional receive-only interface *type* and *number* values specified with the **interface** *type number* command in Step 3.
Step 14	**tunnel source** {ip-address | *type number*} **Example:**	Configures the tunnel source.

	Command or Action	Purpose
	`Router(config-if)# tunnel source 11.8.2.3`	
Step 15	**tunnel destination** {*hostname*| ip-address} **Example:** `Router(config-if)# tunnel destination 10.3.4.5`	Configures the tunnel destination.
Step 16	**tunnel udlr address-resolution** **Example:** `Router(config-if)# tunnel udlr address-resolution`	Enables the forwarding of ARP and NHRP.

Configuring IGMP UDLR

To configure an IGMP UDL, you must configure both the upstream and downstream routers. You need not specify whether the direction is sending or receiving; IGMP learns the direction by the nature of the physical connection.

When the downstream router receives an IGMP report from a host, the router sends the report to the IGMP querier associated with the UDL interface identified in the **ip igmp helper-address** command.

Before you begin

- All routers on the UDL have the same subnet address. If all routers on the UDL cannot have the same subnet address, the upstream router must be configured with secondary addresses to match all the subnets that the downstream routers are attached to.
- Multicast receivers are directly connected to the downstream routers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip igmp unidirectional-link**
5. Move to the downstream router.
6. **enable**
7. **configure terminal**
8. **ip multicast default-rpf-distance** *distance*
9. **interface** *type number*
10. **ip igmp unidirectional-link**
11. **ip igmp helper-address udl** *type number*
12. **exit**
13. **show ip igmp udlr** [*group-name*| *group-address* | *type number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted. • Begin on the upstream router.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/1/1`	Configures the interface.
Step 4	**ip igmp unidirectional-link** **Example:** `Router(config-if)# ip igmp unidirectional-link`	Configures IGMP on the interface to be unidirectional.
Step 5	Move to the downstream router.	--
Step 6	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted. • Begin on the upstream router.
Step 7	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 8	**ip multicast default-rpf-distance** *distance* **Example:** `Router# ip multicast default-rpf-distance 10`	(Optional) Sets the distance for the default RPF interface. By default, the distance for the default reverse path forwarding (RPF) interface is 15. Any explicit sources learned by routing protocols will take preference if their distance is less than the distance configured by the **ip multicast default-rpf-distance** command. Use this command on downstream routers if you want some sources to use RPF to reach the UDLR link and others to use the terrestrial paths. • If you want IGMP to prefer the UDL, set the distance to be less than the distances of the unicast routing protocols.

	Command or Action	Purpose
		• If you want IGMP to prefer the non-UDL, set the distance to be greater than the distances of the unicast routing protocols.
Step 9	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/0/0`	Configures the interface.
Step 10	**ip igmp unidirectional-link** **Example:** `Router(config-if)# ip igmp unidirectional-link`	Configures IGMP on the interface to be unidirectional.
Step 11	**ip igmp helper-address udl** *type number* **Example:** `Router(config-if)# ip igmp helper-address udl ethernet 0`	Configures the interface to be an IGMP helper. • Use this command on every downstream router, on every interface to specify the *type* and *number* values that identify the UDL interface.
Step 12	**exit** **Example:** `Router(config-if)# exit`	Exits configuration mode and returns to EXEC mode.
Step 13	**show ip igmp udlr** [*group-name*| *group-address* | *type number*] **Example:** `Router(config)# show ip igmp udlr`	(Optional) Displays UDLR information for directly connected multicast groups on interfaces that have a UDL helper address configured.

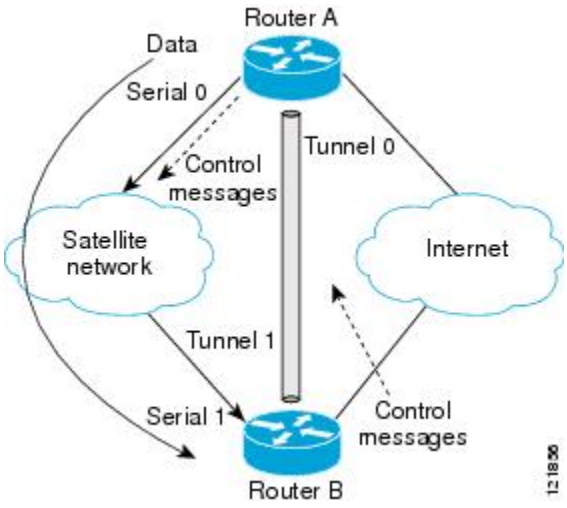
Configuration Examples for UDLR

UDLR Tunnel Example

The following example shows how to configure a UDLR tunnel. In the example, Router A (the upstream router) is configured with Open Shortest Path First (OSPF) and PIM. Serial interface 0 has send-only capability. Therefore, the UDLR tunnel is configured as receive only, and points to serial 0.

Router B (the downstream router) is configured with OSPF and PIM. Serial interface 1 has receive-only capability. Therefore, the UDLR tunnel is configured as send-only, and points to serial 1. The forwarding of ARP and NHRP is enabled. The figure below illustrates the example.

Figure 7: UDLR Tunnel Example



Router A Configuration

```
ip multicast-routing
!
! Serial0/0/0 has send-only capability
!
interface serial 0/0/0
 encapsulation hdlc
 ip address 10.1.0.1 255.255.0.0
 ip pim sparse-dense-mode
!
! Configure tunnel as receive-only UDLR tunnel.
!
interface tunnel 0
 tunnel source 10.20.0.1
 tunnel destination 10.41.0.2
 tunnel udlr receive-only serial 0/0/0
!
! Configure OSPF.
!
router ospf
 network 10.0.0.0 0.255.255.255 area 0
```

Router B Configuration

```
ip multicast-routing
!
! Serial1 has receive-only capability
!
interface serial 1/0/0
 encapsulation hdlc
 ip address 10.1.0.2 255.255.0.0
 ip pim sparse-dense-mode
!
! Configure tunnel as send-only UDLR tunnel.
!
interface tunnel 0
 tunnel source 10.41.0.2
```

```
 tunnel destination 10.20.0.1
 tunnel udlr send-only serial 1/0/0
 tunnel udlr address-resolution
!
! Configure OSPF.
!
router ospf
 network 10.0.0.0 0.255.255.255 area 0
```

IGMP UDLR Example

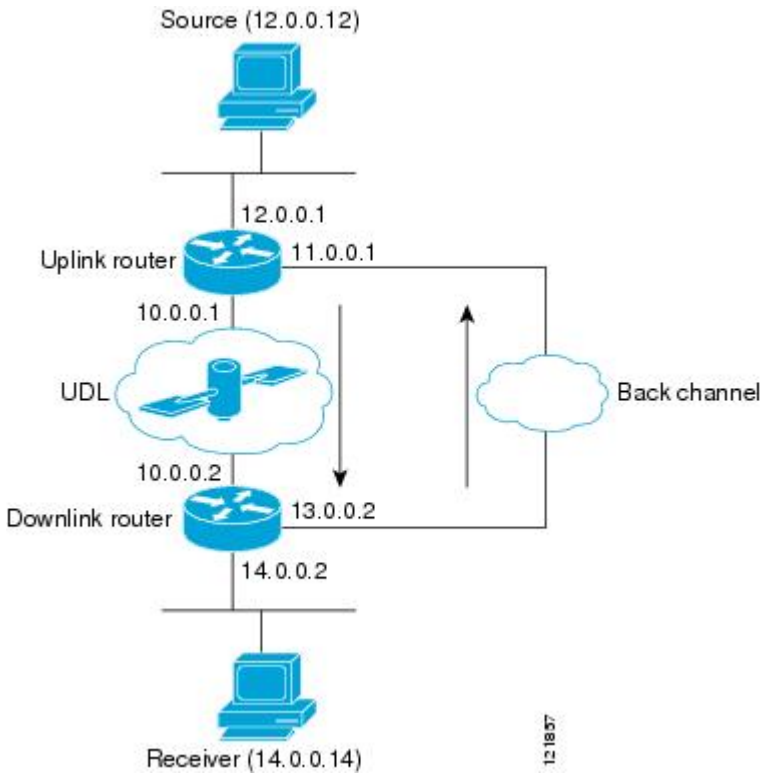
The following example shows how to configure IGMP UDLR. In this example, uplink-rtr is the local upstream router and downlink-rtr is the downstream router.

Both routers are also connected to each other by a back channel connection. Both routers have two IP addresses: one on the UDL and one on the interface that leads to the back channel. The back channel is any return route and can have any number of routers.

Note Configuring PIM on the back channel interfaces on the uplink router and downlink router is optional.

All routers on a UDL must have the same subnet address. If all routers on a UDL cannot have the same subnet address, the upstream router must be configured with secondary addresses to match all the subnets that the downstream routers are attached to.

Figure 8: IGMP Unidirectional Link Routing Example



Uplink Router (uplink-rtr) Configuration

```
ip multicast-routing
!
! Interface that source is attached to
!
interface gigabitethernet 0/0/0
 description Typical IP multicast enabled interface
 ip address 12.0.0.1 255.0.0.0
 ip pim sparse-dense-mode
!
! Back channel
!
interface gigabitethernet 1/0/0
 description Back channel which has connectivity to downlink-rtr
 ip address 11.0.0.1 255.0.0.0
 ip pim sparse-dense-mode
!
! Unidirectional link
!
interface serial 0/0/0
 description Unidirectional to downlink-rtr
 ip address 10.0.0.1 255.0.0.0
 ip pim sparse-dense-mode
 ip igmp unidirectional-link
 no keepalive
```

Downlink Router (downlink-rtr) Configuration

```
ip multicast-routing
!
! Interface that receiver is attached to, configure for IGMP reports to be
! helpered for the unidirectional interface.
!
interface gigabitethernet 0/0/0
 description Typical IP multicast-enabled interface
 ip address 14.0.0.2 255.0.0.0
 ip pim sparse-dense-mode
 ip igmp helper-address udl serial 0/0/0
!
! Back channel
!
interface gigabitethernet 1/0/0
 description Back channel that has connectivity to downlink-rtr
 ip address 13.0.0.2 255.0.0.0
 ip pim sparse-dense-mode
!
! Unidirectional link
!
interface serial 0/0/0
 description Unidirectional to uplink-rtr
 ip address 10.0.0.2 255.0.0.0
 ip pim sparse-dense-mode
 ip igmp unidirectional-link
 no keepalive
```

Integrated UDLR Tunnel IGMP UDLR and IGMP Proxy Example

The following example shows how to configure UDLR tunnels, IGMP UDLR, and IGMP proxy on both the upstream and downstream routers sharing a UDL.

Upstream Configuration

```
ip multicast-routing
!
interface Tunnel0
  ip address 9.1.89.97 255.255.255.252
  no ip directed-broadcast
  tunnel source 9.1.89.97
  tunnel mode gre multipoint
  tunnel key 5
  tunnel udlr receive-only GigabitEthernet2/3/0
!
interface GigabitEthernet2/0/0
  no ip address
  shutdown
!
! user network
interface GigabitEthernet2/1/0
  ip address 9.1.89.1 255.255.255.240
  no ip directed-broadcast
  ip pim dense-mode
  ip cgmp
  fair-queue 64 256 128
  no cdp enable
  ip rsvp bandwidth 1000 100
!
interface GigabitEthernet2/2/0
  ip address 9.1.95.1 255.255.255.240
  no ip directed-broadcast
!
! physical send-only interface
interface GigabitEthernet2/3/0
  ip address 9.1.92.100 255.255.255.240
  no ip directed-broadcast
  ip pim dense-mode
  ip nhrp network-id 5
  ip nhrp server-only
  ip igmp unidirectional-link
  fair-queue 64 256 31
  ip rsvp bandwidth 1000 100
!
router ospf 1
  network 9.1.92.96 0.0.0.15 area 1
!
ip classless
ip route 9.1.90.0 255.255.255.0 9.1.92.99
```

Downstream Configuration

```
ip multicast-routing
!
interface Loopback0
  ip address 9.1.90.161 255.255.255.252
  ip pim sparse-mode
  ip igmp helper-address udl GigabitEthernet2/3/0
  ip igmp proxy-service
!
interface Tunnel0
  ip address 9.1.90.97 255.255.255.252
  ip access-group 120 out
  no ip directed-broadcast
  no ip mroute-cache
```

```
  tunnel source 9.1.90.97
  tunnel destination 9.1.89.97
  tunnel key 5
  tunnel udlr send-only GigabitEthernet2/3/0
  tunnel udlr address-resolution
!
interface GigabitEthernet2/0/0
  no ip address
  no ip directed-broadcast
  shutdown
  no cdp enable
!
! user network
interface GigabitEthernet2/1/0
  ip address 9.1.90.1 255.255.255.240
  no ip directed-broadcast
  ip pim sparse-mode
  ip igmp mroute-proxy Loopback0
  no cdp enable
!
! Backchannel
interface GigabitEthernet2/2/0
  ip address 9.1.95.3 255.255.255.240
  no ip directed-broadcast
  no cdp enable
!
! physical receive-only interface
interface GigabitEthernet2/3/0
  ip address 9.1.92.99 255.255.255.240
  no ip directed-broadcast
  ip pim sparse-mode
  ip igmp unidirectional-link
  no keepalive
  no cdp enable
!
router ospf 1
  network 9.1.90.0 0.0.0.255 area 1
  network 9.1.92.96 0.0.0.15 area 1
!
ip classless
ip route 0.0.0.0 0.0.0.0 9.1.95.1
! set rpf to be the physical receive-only interface
ip mroute 0.0.0.0 0.0.0.0 9.1.92.96
ip pim rp-address 9.1.90.1
!
! permit ospf, ping and rsvp, deny others
access-list 120 permit icmp any any
access-list 120 permit 46 any any
access-list 120 permit ospf any any
```

Additional References

Related Documents

Related Topic	Document Title
IP multicast commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Multicast Command Reference*

Related Topic	Document Title
Tunnel interfaces	“ Implementing Tunnels ” module
IGMP and IGMP Proxy	“ Customizing IGMP ” module

MIBs

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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Configuring IP Multicast over Unidirectional Links

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 10: Feature Information for Configuring IP Multicast over Unidirectional Links

Feature Name	Releases	Feature Configuration Information
UDLR Tunnel ARP and IGMP Proxy	12.2(8)T	This feature enables arp over a unidirectional link and overcomes the existing limitation of requiring downstream multicast receivers to be directly connected to the unidirectional link downstream router.

Feature Name	Releases	Feature Configuration Information
Uni-Directional Link Routing (UDLR)	12.2(2)T 12.2(17d)SXB1	Unidirectional link routing is used to allow routing protocols to function in environments where routers are connected through unidirectional links. Unidirectional link routing enables layer 3 connectivity by tunneling routing information to the router on the upstream side of a unidirectional link.