



Configuring Multicast Services

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping, GARP Multicast Registration Protocol (GMRP), and Router-Port Group Management Protocol (RGMP) on the Catalyst 6500 series switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Command Reference* publication.

This chapter consists of these sections:

- [Understanding How Multicasting Works, page 42-1](#)
- [Configuring IGMP Snooping on the Switch, page 42-8](#)
- [Configuring GMRP on the Switch, page 42-17](#)
- [Configuring Multicast Router Ports and Group Entries on the Switch, page 42-25](#)
- [Understanding How RGMP Works, page 42-27](#)
- [Configuring RGMP on the Switch, page 42-28](#)
- [Displaying Multicast Protocol Status, page 42-32](#)

Understanding How Multicasting Works

These sections describe how multicasting works on the Catalyst 6500 series switches:

- [Multicasting and Multicast Services Overview, page 42-2](#)
- [Understanding How IGMP Snooping Works, page 42-2](#)
- [Understanding How GMRP Works, page 42-5](#)
- [Understanding How RGMP Works, page 42-6](#)
- [Suppressing Multicast Traffic, page 42-6](#)
- [Nonreverse Path Forwarding Multicast Fast Drop, page 42-7](#)
- [Enabling Installation of Directly Connected Subnets, page 42-7](#)
- [Understanding How the IGMP Querier Works, page 42-7](#)

Multicasting and Multicast Services Overview

IGMP snooping manages multicast traffic in switches by allowing directed switching of IP multicast traffic. GMRP is protocol independent and can manage both IP multicast traffic and any Layer 2 multicast traffic.

Switches can use IGMP snooping or GMRP to configure switch ports dynamically so that IP multicast traffic is forwarded only to those ports that are associated with IP multicast hosts. IGMP software components run on both the Cisco router and the switch.



Note

For more information on IP multicast and IGMP, refer to RFC 1112. GMRP is described in IEEE 802.1p.

You can statically configure multicast groups using the **set cam static** command. Multicast groups that are learned through IGMP snooping are dynamic. If you specify group membership for a multicast group address, your static setting supersedes any automatic manipulation by IGMP snooping or GMRP. Multicast group membership lists can consist of both user-defined settings and settings that are learned through IGMP snooping or GMRP.

Understanding How IGMP Snooping Works



Note

You cannot enable IGMP snooping on a switch if GMRP is already enabled on the switch.



Note

You can run IGMP snooping on any Catalyst 6500 series supervisor engine model (Supervisor Engine 1, Supervisor Engine 1A, and Supervisor Engine 2). A PFC is not required to enable IGMP snooping. Cisco Group Management Protocol (CGMP) is not supported on the Catalyst 6500 series switches, although CGMP server is supported on the MSFC. To support CGMP client devices, configure the MSFC as a CGMP server.

IGMP snooping manages multicast traffic at Layer 2 on the Catalyst 6500 series switches by allowing directed switching of IP multicast traffic.

Switches can use IGMP snooping to configure Layer 2 interfaces dynamically so that IP multicast traffic is forwarded only to those interfaces that have expressed interest in particular IP multicast traffic streams through IGMP join and report messages.

Catalyst 6500 series switches can distinguish IGMP control traffic from multicast data traffic. When you enable IGMP on the switch, IGMP control traffic is redirected to the CPU for further processing. This process is performed in hardware by specialized ASICs. The ASICs allow the switch to snoop IGMP control traffic with no performance penalty.

The router periodically sends out general queries to all VLANs, and as multicast receivers respond to the router's queries, the switch intercepts them. Only the first IGMP join (report) per VLAN and per IP multicast group is forwarded to the router. Subsequent reports for the same VLAN and group are suppressed. The switch processor creates one entry per VLAN in the Layer 2 forwarding table for each MAC group from which it receives an IGMP join request. All hosts that are interested in this multicast traffic send join requests and are added to the port list of this forwarding table entry. If a port is disabled, it is removed from all multicast group entries.

**Note**

IGMP version 3 is supported only on systems with a Supervisor Engine 2.

IGMP version 3 uses source-based filtering and is the industry-designated standard protocol for hosts to signal channel subscriptions in Source Specific Multicast (SSM). Source-based filtering enables hosts and routers to specify which source addresses should be allowed or blocked for a specific multicast group. When you enable IGMP version 3 snooping on a Catalyst 6500 series switch, the switch maintains IGMP version 3 states based on IGMP version 3 reports that it receives from a port on a per-group, per-VLAN basis and either allows or blocks source traffic on that port based on the type of IGMP version 3 message it receives.

**Note**

Before you can enable IGMP version 3 on a Catalyst 6500 series switch, you must first disable IP MMLS by entering the **no mls ip multicast** command from the MSFC router prompt.

**Note**

IGMP version 3 snooping is supported for INCLUDE mode only. IGMP version 3 snooping is not supported for EXCLUDE mode. For example, when the IGMP version 3 state goes to EXCLUDE mode for a particular group in a particular VLAN, the switch maintains the version 3 state in the same way as a version 3 router, and multicast traffic is sent to the ports that sent version 3 reports based on the version 3 state.

**Note**

For IGMP version 3 snooping, use Cisco IOS Release 12.1(11b)E1 or later releases on the MSFC2.

Joining a Multicast Group

In IGMP version 2, when a host wants to join an IP multicast group, it either responds to a router query or sends an IGMP join (also known as a join message) specifying the IP multicast group it wants to join (for example, group 224.1.2.3). The switch hardware recognizes that the packet is an IGMP report and redirects it to the switch CPU. The switch installs a new group entry for 01-00-5e-01-02-03 and adds the host port and the router port to that entry. The switch then relays the join from the host to all multicast router ports. The designated multicast router for the segment adds the outgoing interface (OIF) to the outgoing interface list (OIL) for the group and begins forwarding multicast traffic for 224.1.2.3 to this segment.

When a second host in this VLAN wants to join group 244.1.2.3, it sends out an IGMP join for this group. The switch hardware recognizes that this is an IGMP control packet and redirects it to the switch CPU. Because the switch already has a group entry for 01-00-5e-01-02-03 in this VLAN, it only adds the second host port to the entry. Because this is not the first host joining the group, the switch suppresses the report (the switch does not send it to the router).

IGMP version 3 reports are sent by hosts to the 224.0.0.22 address. The multicast router keeps a state record for each group on an interface, and the switch maintains a state record for each group on a per-VLAN basis. The state records contain the multicast IP address, the group timer, the source timer, and the filter mode as specified by the hosts. Hosts can specify one of the following filter modes:

- **INCLUDE mode**—In this mode, the host announces membership to a multicast group and provides a list of source IP addresses (the INCLUDE list) from which it wants to receive traffic.
- **EXCLUDE mode**—In this mode, the host announces membership to a multicast group and provides a list of source IP addresses (the EXCLUDE list) from which it does not want to receive traffic. This mode indicates that the host wants to receive traffic only from sources whose IP addresses are not listed in the EXCLUDE list. To receive traffic from all sources, a host expresses EXCLUDE mode membership with an empty EXCLUDE list.



Note The IGMP compatibility mode changes to version 1 or version 2 as soon as version 1 or version 2 messages are received for a group on a VLAN (where the version 3 state previously existed for that particular group on that VLAN).

Constraining Multicast Traffic

When a host sends multicast traffic to a group, the switch hardware does not recognize the stream as IGMP control packets; therefore, the packets are not redirected to the switch CPU. Instead, the multicast traffic is forwarded to the Media Access Control (MAC) group entry and the switch constrains the traffic to only those ports that have been added to that group entry.

The router sends IGMP general queries. The switch floods these queries on all ports in the VLAN, and hosts that are interested in a multicast group respond with an IGMP join for each group in which they are interested.

The switch intercepts these IGMP joins, and only the first join per VLAN and per IP multicast group is forwarded on the multicast router ports. Subsequent reports for the same VLAN and group are suppressed (not sent to the router). If you enable the switch for IGMP version 3 snooping, all joins are forwarded to the router ports.



Note If you have CGMP switches in your network, join and leave suppression does not occur. In a network that has both IGMP version 2 and CGMP switches, all join and leave messages are forwarded to the multicast routers so that CGMP join and leave messages can be generated by the router.

Leaving a Multicast Group

In a network running IGMP version 1 or 2, the designated multicast router for a segment continues forwarding the multicast traffic to that VLAN as long as at least one host in the VLAN wishes to receive multicast traffic. When hosts want to leave a multicast group, they can either ignore the periodic general queries that are sent by the multicast router (IGMP version 1 host behavior), or they can send an IGMP leave (IGMP version 2 host behavior). When the switch receives a leave message, it sends out a MAC-based general query on the port on which it received the leave message to determine if any of the devices that are connected to this port are interested in traffic for the specific multicast group. If this port is the last port in the VLAN, the switch sends a MAC-based general query to all ports in the VLAN. MAC-based general queries are addressed to the Layer 2 Group Destination Address (GDA) MAC address for which the IGMP leave message was received. At Layer 3, the MAC-based general queries are addressed to 224.0.0.1 (all hosts), and in the IGMP header, the group address field is set to 0.0.0.0.

If no IGMP join is received for any of the IP multicast groups that map to the MAC multicast group address, the port is removed from the multicast forwarding entry. If the port is not the last nonmulticast-router port in the entry, the switch suppresses the IGMP leave (does not send it to the router). If the port is the last nonmulticast-router port in the entry, the IGMP leave is forwarded to the multicast router ports and the MAC group forwarding entry is removed.

When the router receives the IGMP leave, it sends several IGMP group-specific queries. If no join messages are received in response to the queries, and there are no downstream routers that are connected through that interface, the router removes the interface from the OIL for that IP multicast group entry in the multicast routing table. After the last receiver leaves a multicast group, the switch floods traffic for this multicast group for few seconds. To prevent flooding of multicast traffic after the last host leaves a multicast group, enter the **set igmp flooding disable** command.

IGMP Fast-Leave Processing

IGMP snooping fast-leave processing allows the switch processor to remove an interface from the port list of a forwarding-table entry without first sending out a MAC-based general query on the port. When an IGMP leave is received on a port, the port is immediately removed from the multicast forwarding entry (or the entire entry is removed).

IGMP Fast-Block Processing

IGMP version 3 supports fast-block processing. If you enable fast-block processing on the switch, the switch immediately stops forwarding multicast packets to a port when it receives a block or exclude message from a host connected to that port.



Note

Do not use the fast-leave processing feature if more than one host is connected to each port. If you enable fast-leave when more than one host is connected to a port, some hosts might be dropped inadvertently. Fast leave is supported with IGMP version 2 hosts only.

Understanding How GMRP Works

GMRP is a Generic Attribute Registration Protocol (GARP) application that provides a constrained multicast flooding facility similar to IGMP snooping. GMRP and GARP are industry-standard protocols that are defined by the IEEE. For detailed protocol operational information, refer to 802.1p.

GMRP software components run on both the switch and on the host. (Cisco is not a source for GMRP host software.) On the host, in an IP multicast environment, you must use IGMP with GMRP; the host GMRP software spawns Layer 2 GMRP versions of the host's Layer 3 IGMP control packets. The switch receives both the Layer 2 GMRP and the Layer 3 IGMP traffic from the host. The switch forwards the Layer 3 IGMP control packets to the router and uses the received GMRP traffic to constrain multicasts at Layer 2 in the host's VLAN.

When a host wants to join an IP multicast group, it sends an IGMP join, which spawns a GMRP join. When the switch receives the GMRP join, it adds the port through which the join was received to the appropriate multicast group. The switch propagates the GMRP join to all other hosts in the VLAN, one of which is typically the multicast source. When the source is multicasting to the group, the switch forwards the multicast only to the ports from which it received join messages for the group.

The switch sends periodic GMRP queries. If a host wants to remain in a multicast group, it responds to the query and the switch does nothing. If a host does not want to remain in the multicast group, it can either send a leave message or not respond to the periodic queries from the switch. If the switch receives a leave message or receives no response from the host for the duration of the **leaveall** timer, the switch removes the host from the multicast group.

**Note**

To use GMRP in a routed environment, enable the GMRP **forwardall** option on all ports where routers are attached. (See the “[Enabling the GMRP Forward-All Option](#)” section on page 42-20.)

Understanding How RGMP Works

Without RGMP, all multicast routers receive all multicast data traffic entering the switch. With RGMP, a multicast router can request not to receive multicast traffic if that router has no downstream receivers for the multicast traffic. Catalyst 6500 series switches support RGMP, which enables a switch to reduce network congestion by forwarding multicast data traffic only to those routers that are configured to receive it.

**Note**

To use RGMP, you must enable IGMP snooping on the switch and Protocol Independent Multicast (PIM) on the routers. Only PIM sparse mode is currently supported.

All routers on the network must be RGMP capable. RGMP-capable routers periodically send an RGMP hello message to the switch. The RGMP hello message tells the switch not to send multicast data to the router unless an RGMP join has also been sent to the switch from that router. When an RGMP join is sent, the router is able to receive multicast data. To learn how to set a router to receive RGMP data, see the “[RGMP-Related CLI Commands](#)” section on page 42-31.

To stop receiving multicast data, a router must send an RGMP leave message to the switch. To disable RGMP on a router, the router must send an RGMP bye message to the switch.

[Table 42-1](#) provides a summary of the RGMP message types.

Table 42-1 RGMP Message Types

Description	Action
Hello	When the RGMP feature is enabled on the router, no multicast data traffic is sent to the router by the switch unless an RGMP join is specifically sent for a group.
Bye	When the RGMP feature is disabled on the router, all multicast data traffic is sent to the router by the switch.
Join	Multicast data traffic for a multicast MAC address from the Layer 3 group address G is sent to the router. These packets have group G in the Group Address field of the RGMP packet.
Leave	Multicast data traffic for the group G is not sent to the router. These packets have group G in the group address field of the RGMP packet.

Suppressing Multicast Traffic

On Gigabit Ethernet ports, you can limit the amount of bandwidth to be used for multicast traffic. Use the **set port broadcast** command to specify a percentage of the total bandwidth to be used for multicast traffic on Gigabit Ethernet ports.

Nonreverse Path Forwarding Multicast Fast Drop

In a redundant configuration where multiple routers connect to the same LAN segment, only one router forwards the multicast traffic from the source to the receivers on the outgoing interfaces. In this kind of topology, only the Protocol Independent Multicast designated forwarder (PIM-DF) forwards the data in the common VLAN, but the non-PIM-DF receives the forwarded multicast traffic. The redundant router (non-PIM-DF) must drop this traffic because it has arrived on the wrong interface and will fail the reverse path forwarding (RPF) check. Traffic that fails the RPF check is called non-RPF traffic.

Non-RPF multicast fast drop (MFD) rate limits the packets that fail the RPF check (non-RPF packets) and drops the majority of the non-RPF packets in the hardware. According to the multicast protocol specification, the router needs to see the non-RPF packets for the PIM assert mechanism to work, so that all the non-RPF packets cannot be dropped in the hardware. To support the PIM assert mechanism, the PFC leaks a percentage of the non-RPF flow packets to the MSFC.

Non-RPF MFD is enabled on the switch by default. Non-RPF MFD is supported with Supervisor Engine 2 only.

Enabling Installation of Directly Connected Subnets

In PIM sparse mode, a first-hop router that is the designated router (DR) for the interface may need to encapsulate the source traffic in a PIM register message and unicast it to the rendezvous point (RP). To prevent new sources for the group from being learned in the routing table, the (*,G) flows should remain completely hardware-switched flows. (subnet/mask, 224/4) entries that are installed in the hardware FIB allow both (*,G) flows to remain completely hardware-switched flows, and new, directly connected sources to be learned correctly. Installation of directly connected subnets is enabled globally by default. One (subnet/mask, 224/4) is installed per PIM-enabled interface.

Use the **show mls ip multicast connected** command to view such FIB entries.

To enable the installation of directly connected subnets, perform this task:

Task	Command
Enable the installation of directly connected subnets.	Router(config) # mls ip multicast connected

This example shows how to enable the installation of directly connected subnets:

```
Router(config)# mls ip multicast connected
Router(config)#
```

Understanding How the IGMP Querier Works

The IGMP querier feature enables IGMP snooping within a VLAN where PIM and IGMP are not configured because the multicast traffic does not need to be routed.



Note

You must enable IGMP querier for IGMP snooping to work correctly in a VLAN in which no multicast routers are present.

When you configure IGMP querier for a VLAN, the switch sends out IGMP general query messages every 125 seconds and listens for general query messages from other switches. If the switch receives a general query, a querier election starts. A querier election across switches is based either on an IP address or a MAC address. For an inbound query, if the source IP address is nonzero, the election is based on the IP address, and the switch with the lower source IP address becomes the querier. If the source IP address is zero for an inbound query, then the election is based on the source MAC address, and the switch with the lower MAC address wins the election and becomes the querier. The switch that becomes the nonquerier maintains an “other querier interval” timer. When this timer expires, the switch elects itself as the querier.

For information on enabling IGMP querier, see the [“Enabling the IGMP Querier”](#) section on page 42-13.

Configuring IGMP Snooping on the Switch

IGMP snooping allows switches to examine IGMP packets and make forwarding decisions based on their content.



Note

Quality of service (QoS) does not support IGMP traffic when IGMP snooping is enabled.

These sections describe how to configure IGMP snooping:

- [Default IGMP Snooping Configuration, page 42-8](#)
- [IGMP Snooping Configuration Guidelines, page 42-9](#)
- [Enabling IGMP Snooping, page 42-9](#)
- [Specifying IGMP Snooping Mode, page 42-10](#)
- [Enabling IGMP Fast-Leave Processing, page 42-11](#)
- [Enabling IGMP Version 3 Snooping, page 42-11](#)
- [Enabling IGMP Version 3 Fast-Block Processing, page 42-13](#)
- [Enabling the IGMP Querier, page 42-13](#)
- [Enabling IGMP Rate Limiting, page 42-14](#)
- [Displaying Multicast Router Information, page 42-14](#)
- [Displaying Multicast Group Information, page 42-15](#)
- [Displaying IGMP Snooping Statistics, page 42-16](#)
- [Disabling IGMP Fast-Leave Processing, page 42-16](#)
- [Disabling IGMP Snooping, page 42-17](#)

Default IGMP Snooping Configuration

[Table 42-2](#) shows the default IGMP snooping configuration.



Note

IGMP snooping is enabled by default in supervisor engine software release 5.5(9) and later releases and 6.3(1) and later releases.

Table 42-2 IGMP Snooping Default Configuration

Feature	Default Value
IGMP snooping	Enabled
Multicast routers	None configured

IGMP Snooping Configuration Guidelines

IGMP snooping configuration guidelines are as follows:

- There is no proxy reporting support with IGMP version 3 snooping. With IGMP version 2 snooping, only the first join and the last leave are forwarded to the router. For the group specific (GS) queries initiated by the router, the switch responds with a report if at least one port is present for the group. With IGMP version 3 snooping, all reports are forwarded to the router and the GS and group and source-specific (GSS) queries are flooded onto the VLAN to refresh the memberships.
- At least one version 3 router should be present on the VLAN for IGMP version 3 snooping to work.
- Unlike IGMP version 2 snooping, for IGMP version 3 snooping no permanent entries can be added that would be retained across reboots.
- IGMP version 2 snooping reports are captured and are sent to the supervisor engine. IGMP version 3 snooping reports are sent to the 224.0.0.22 address. Because snooping is not supported in this range, the reports are captured for the supervisor engine in addition to being flooded.
- With this release of IGMP version 3 snooping, RGMP, SPAN, and RSPAN interaction is not enabled.
- IGMP querier interoperates only with IGMP version 2 snooping. Prior to enabling IGMP version 3 snooping, IGMP querier has to be disabled.

Enabling IGMP Snooping



Note You cannot enable IGMP snooping if GMRP is enabled.

To enable IGMP snooping, perform this task in privileged mode:

	Task	Command
Step 1	Enable IGMP snooping on the switch.	set igmp enable
Step 2	Verify that IGMP snooping is enabled.	show igmp statistics [vlan]

This example shows how to enable IGMP snooping and verify the configuration:

```

Console> (enable) set igmp enable
IGMP Snooping is enabled.
Console> (enable) show igmp statistics
IGMP enabled

IGMP statistics for vlan 1:
  Transmit:
    General Queries: 0
    Group Specific Queries: 0
    Reports: 0
    Leaves: 0

  Receive:
    General Queries: 1056
    Group Specific Queries: 0
    Group and Source Specific Queries: 2
    Reports: 60379
    Leaves: 0
    Total Valid pkts: 63552
    Total Invalid pkts: 0
    Other pkts: 2115
    MAC-Based General Queries: 0
    Failures to add GDA to EARL: 0
    Topology Notifications: 0
    IGMP packets dropped: 0
    IGMP Leave msgs in the list: 0
    IGMP V3 IS_IN messages: 13
    IGMP V3 IS_EX messages: 5
    IGMP V3 TO_IN messages: 0
    IGMP V3 TO_EX messages: 1
    IGMP V3 ALLOW messages: 0
    IGMP V3 BLOCK messages: 1
Console> (enable)

```

Specifying IGMP Snooping Mode

IGMP snooping runs in either IGMP-only mode or IGMP-CGMP mode. The switch dynamically chooses either IGMP-only or IGMP-CGMP mode, depending on the traffic present on the network. IGMP-only mode is used in networks with no CGMP devices. IGMP-CGMP mode is used in networks with both IGMP and CGMP devices. Auto mode overrides the dynamic switching of the modes.

To specify the IGMP snooping mode, perform this task in privileged mode:

	Task	Command
Step 1	Specify the IGMP snooping mode.	set igmp mode {igmp-only igmp-cgmp auto}
Step 2	Display the IGMP snooping mode.	show igmp mode

This example shows how to set the IGMP mode to IGMP-only and verify the configuration:

```

Console> (enable) set igmp mode igmp-only
IGMP mode set to igmp-only
Console> (enable) show igmp mode
IGMP Mode: igmp-only
IGMP Operational Mode: igmp-only
IGMP Address Aliasing Mode: normal
Console> (enable)

```

Enabling IGMP Fast-Leave Processing

To enable IGMP fast-leave processing, perform this task in privileged mode:

	Task	Command
Step 1	Enable IGMP fast-leave processing on the switch.	set igmp fastleave enable
Step 2	Verify that IGMP fast-leave processing is enabled.	show igmp statistics

This example shows how to enable IGMP fast-leave processing and verify the configuration:

```
Console> (enable) set igmp fastleave enable
IGMP fastleave set to enable.
Console> (enable) show igmp statistics
IGMP enabled
```

```
IGMP statistics for vlan 1:
  Transmit:
    General Queries: 0
    Group Specific Queries: 0
    Reports: 0
    Leaves: 0

  Receive:
    General Queries: 1056
    Group Specific Queries: 0
    Group and Source Specific Queries: 2
    Reports: 60379
    Leaves: 0
    Total Valid pkts: 63552
    Total Invalid pkts: 0
    Other pkts: 2115
    MAC-Based General Queries: 0
    Failures to add GDA to EARL: 0
    Topology Notifications: 0
    IGMP packets dropped: 0
    IGMP Leave msgs in the list: 0
    IGMP V3 IS_IN messages: 13
    IGMP V3 IS_EX messages: 5
    IGMP V3 TO_IN messages: 0
    IGMP V3 TO_EX messages: 1
    IGMP V3 ALLOW messages: 0
    IGMP V3 BLOCK messages: 1
Console> (enable)
```

Enabling IGMP Version 3 Snooping

To enable IGMP version 3 snooping, perform this task in privileged mode:

	Task	Command
Step 1	If an MSFC is installed, disable MMLS from the MSFC router prompt.	no mls ip multicast

	Task	Command
Step 2	Enable IGMP version 3 snooping on the switch.	set igmp v3-processing enable
Step 3	Display IGMP version 3 snooping information.	show multicast v3-group show multicast router

This example shows how to enable IGMP snooping and verify the configuration:

```

Router(config)# no mls ip multicast
Multilayer Switching for Multicast is disabled for this device.
Router(config)# exit
Router# exit
Console> (enable) set igmp v3-processing enable
IGMP V3 processing enabled
Console> (enable) show multicast v3-group
Displaying V3 group information for all vlans
-----
(G,C): (227.1.1.1,2), V3 state: INC
V1/V2 Compatibility mode: none (V3)
Include list: 2.2.2.6, Src timer 125 sec, Ports: 6/29 15/1
              2.2.2.5, Src timer 125 sec, Ports: 6/29 15/1
Exclude list: NULL

(G,C): (227.1.1.1,60), V3 state: INC
V1/V2 Compatibility mode: none (V3)
Include list: 2.2.2.7, Src timer 115 sec, Ports: 13/30 15/1
              2.2.2.5, Src timer 115 sec, Ports: 13/30 15/1
              2.2.2.8, Src timer 115 sec, Ports: 13/30 15/1
Exclude list: NULL

Console> (enable) show multicast v3-group 2 227.1.1.1
----IGMP V3 information----
(G,C): (227.1.1.1,2), V3 state: INC
V1/V2 Compatibility mode: none (V3)
Include list: 2.2.2.6, Src timer 125 sec, Ports: 6/29 15/1
              2.2.2.5, Src timer 125 sec, Ports: 6/29 15/1
Exclude list: NULL

Console> (enable) show multicast v3-group
Displaying V3 group information for all vlans
-----
(G,C): (227.1.1.1,2), V3 state: EX
V1/V2 Compatibility mode: none (V3) Group timer: 125 sec
Include list: NULL
Exclude list: 2.2.2.6, Excluded Ports: 6/29
              2.2.2.5, Excluded Ports: 6/29

Console> (enable) show multicast router
Port          Vlan
-----
15/1          $ 2,60

Total Number of Entries = 1
'*' - Configured
'+' - RGMP-capable
'#' - Channeled Port
'$' - IGMP-V3 Router
Console> (enable)

```

Enabling IGMP Version 3 Fast-Block Processing

To enable IGMP version 3 fast-block processing, perform this task in privileged mode:

	Task	Command
Step 1	Enable IGMP fast-block processing on the switch.	set igmp fastblock enable
Step 2	Verify that IGMP fast-block processing is enabled.	show multicast protocols status

This example shows how to enable IGMP fast-block processing and verify the configuration:

```
Console> (enable) set igmp fastblock enable
IGMP V3 fastblock enabled
```

```
Console> (enable) show multicast protocols status
IGMP enabled
IGMP fastleave disabled
IGMP V3 processing enabled
IGMP V3 fastblock feature enabled
RGMP disabled
GMRP disabled
Console> (enable)
```

Enabling the IGMP Querier

Use the IGMP querier to support IGMP snooping within a VLAN where PIM and IGMP are not configured because the multicast traffic does not need to be routed.



Note

You can enable the IGMP querier on all the switches in the VLAN. One switch is elected as querier.

To enable the IGMP querier in a VLAN, perform these tasks in privileged mode:

Task	Command
Enable IGMP querier on a VLAN or on all VLANs.	set igmp querier disable enable vlan
Specify the time interval between the general queries sent by the switch. The default is 125 seconds.	set igmp querier vlan qi val
Specify the amount of time that the switch should wait before electing itself as the querier in the absence of general queries. The default is 300 seconds.	set igmp querier vlan oqi val
Display IGMP querier information.	show igmp querier information

This example shows how to enable IGMP querier and display querier information:

```
Console> (enable) set igmp querier enable 4001
Console> (enable) set igmp querier 4001 qi 130
Console> (enable) show igmp querier information
```

```
-----
| vlanNo | Querier State | Query Tx Count | QI (seconds) | OQI (seconds) |
-----
| 4001   | QUERIER       | 0 | 130 | 300 |
-----
```

Enabling IGMP Rate Limiting

IGMP rate limiting is disabled by default and the default rate limit is 100 packets per 30 seconds for all packet types. Valid rate-limit values are from 1 to 65535 packets per 30 seconds.



Note

If IGMP rate limiting and multicast are enabled, multicast router ports might age out sporadically because the rate of the multicast control packets (such as PIMv2 hellos or IGMP general queries) exceeds the IGMP rate limit watermarks that were configured. The default value for these watermarks is 100. We recommend that you increase the PIMv2 hello ratelimit to 3000 by entering the **set igmp ratelimit pimv2 3000** command. You can also increase the IGMP general queries rate limit; we recommend that you set the value to 500 by entering the **set igmp ratelimit general-query 500** command.

To enable IGMP rate limiting and set the rate limit for IGMP snooping packets, perform this task in privileged mode:

Task	Command
Enable IGMP rate limiting and set a rate limit for IGMP snooping packets.	set igmp ratelimit {enable disable} set igmp ratelimit {dvmrp general-query mospf1 mospf2 pimv2} rate

This example shows how to enable IGMP rate limiting:

```
Console> (enable) set igmp ratelimit enable
IGMP Ratelimiting enabled
Console> (enable)
```

This example shows how to set the IGMP rate limit for MOSPF2 to 550 packets per every 30 seconds:

```
Console> (enable) set igmp ratelimit mospf2 550
MOSPF2 Watermark set to allow 550 messages in 30 seconds
Console> (enable)
```

Displaying Multicast Router Information

When you enable IGMP snooping, the switch automatically learns to which ports a multicast router is connected.

To display the dynamically learned multicast router information, perform these tasks in privileged mode:

Task	Command
Display information on dynamically learned and manually configured multicast router ports.	show multicast router [<i>mod/port</i>] [<i>vlan_id</i>]
Display information only on those multicast router ports that are learned dynamically using IGMP snooping.	show multicast router igmp [<i>mod/port</i>] [<i>vlan_id</i>]

This example shows how to display information on all multicast router ports (the asterisk [*] next to the multicast router on port 5/7 indicates that the entry was configured manually):

```
Console> (enable) show multicast router
IGMP enabled
```

```
Port      Vlan
-----  -
1/1      1
2/1      2,99,255
5/7      * 99
```

```
Total Number of Entries = 3
'*' - Configured
Console> (enable)
```

This example shows how to display only those multicast router ports that were learned dynamically through IGMP:

```
Console> (enable) show multicast router igmp
IGMP enabled
```

```
Port      Vlan
-----  -
1/1      1
2/1      2,99,255
```

```
Total Number of Entries = 2
'*' - Configured
Console> (enable)
```

Displaying Multicast Group Information

To display information about multicast groups, perform these tasks in privileged mode:

Task	Command
Display information about multicast groups.	show multicast group [<i>mac_addr</i>] [<i>vlan_id</i>]
Display information only about multicast groups that are learned dynamically through IGMP.	show multicast group igmp [<i>mac_addr</i>] [<i>vlan_id</i>]
Display the total number of multicast addresses (groups) in each VLAN.	show multicast group count [<i>vlan_id</i>]
Display the total number of multicast addresses (groups) in each VLAN that were learned dynamically through IGMP.	show multicast group count igmp [<i>vlan_id</i>]

This example shows how to display information about all multicast groups on the switch:

```

Console> (enable) show multicast group
IGMP enabled

VLAN  Dest MAC/Route Des  Destination Ports or VCs / [Protocol Type]
-----
1      01-00-11-22-33-44*  2/6-12
1      01-11-22-33-44-55*  2/6-12
1      01-22-33-44-55-66*  2/6-12
1      01-33-44-55-66-77*  2/6-12

Total Number of Entries = 4
Console> (enable)

```

Displaying IGMP Snooping Statistics

To display IGMP snooping statistics on the switch, perform this task:

Task	Command
Display IGMP snooping statistics.	show igmp statistics [<i>vlan_id</i>]

This example shows how to display IGMP snooping statistics:

```

Console> (enable) show igmp statistics
IGMP enabled

IGMP statistics for vlan 1:
Total valid pkts rcvd:          18951
Total invalid pkts rcvd        0
General Queries rcvd           377
Group Specific Queries rcvd    0
MAC-Based General Queries rcvd 0
Leaves rcvd                    14
Reports rcvd                   16741
Queries Xmitted                0
GS Queries Xmitted             16
Reports Xmitted                0
Leaves Xmitted                 0
Failures to add GDA to EARL    0
Topology Notifications rcvd    10
IGMP packets dropped           0
Console> (enable)

```

Disabling IGMP Fast-Leave Processing

To disable IGMP fast-leave processing, perform this task in privileged mode:

Task	Command
Disable IGMP fast-leave processing on the switch.	set igmp fastleave disable

This example shows how to disable IGMP fast-leave processing on the switch:

```
Console> (enable) set igmp fastleave disable
IGMP fastleave set to disable.
Console> (enable)
```

Disabling IGMP Snooping

To disable IGMP snooping on the switch, perform this task in privileged mode:

Task	Command
Disable IGMP snooping on the switch.	set igmp disable

This example shows how to disable IGMP snooping:

```
Console> (enable) set igmp disable
IGMP feature for IP multicast disabled
Console> (enable)
```

Configuring GMRP on the Switch

These sections describe how to configure the GARP Multicast Registration Protocol (GMRP):

- [GMRP Software Requirements, page 42-17](#)
- [Default GMRP Configuration, page 42-18](#)
- [Enabling GMRP Globally, page 42-18](#)
- [Enabling GMRP on Individual Switch Ports, page 42-19](#)
- [Disabling GMRP on Individual Switch Ports, page 42-19](#)
- [Enabling the GMRP Forward-All Option, page 42-20](#)
- [Disabling the GMRP Forward-All Option, page 42-20](#)
- [Configuring GMRP Registration, page 42-21](#)
- [Setting the GARP Timers, page 42-22](#)
- [Displaying GMRP Statistics, page 42-23](#)
- [Clearing GMRP Statistics, page 42-24](#)
- [Disabling GMRP Globally on the Switch, page 42-24](#)



Note

For an overview of GMRP operation, see the [“Understanding How GMRP Works”](#) section on page 42-5.

GMRP Software Requirements

GMRP requires supervisor engine software release 5.2 or later releases.

Default GMRP Configuration

Table 42-3 shows the default GMRP configuration.

Table 42-3 GMRP Default Configuration

Feature	Default Value
GMRP enable state	Disabled
GMRP per-port enable state	Disabled
GMRP forward all	Disabled on all ports
GMRP registration	Normal on all ports
GARP/GMRP timers	<ul style="list-style-type: none"> Join time: 200 ms Leave time: 600 ms Leaveall time: 10,000 ms

Enabling GMRP Globally



Note

You cannot enable GMRP if IGMP snooping is enabled.

To enable GMRP globally, perform this task in privileged mode:

	Task	Command
Step 1	Enable GMRP globally on the switch.	set gmrp enable
Step 2	Verify the configuration.	show gmrp configuration

This example shows how to enable GMRP globally and verify the configuration:

```

Console> (enable) set gmrp enable
GMRP enabled.
Console> (enable) show gmrp configuration
Global GMRP Configuration:
GMRP Feature is currently enabled on this switch.
GMRP Timers (milliseconds):
Join = 200
Leave = 600
LeaveAll = 10000
Port based GMRP Configuration:
Port                                     GMRP Status Registration ForwardAll
-----
1/1-2,3/1,6/1-48,7/1-24                 Enabled      Normal      Disabled
Console> (enable)

```

Enabling GMRP on Individual Switch Ports


Note

You can change the per-port GMRP configuration regardless of whether GMRP is enabled globally. However, GMRP will not function on any ports until you enable it globally. For information on configuring GMRP globally on the switch, see the [“Enabling GMRP Globally”](#) section on page 42-18.

To enable GMRP on individual switch ports, perform this task in privileged mode:

	Task	Command
Step 1	Enable GMRP on an individual switch port.	set port gmrp enable <i>mod/port</i>
Step 2	Verify the configuration.	show gmrp configuration

This example shows how to enable GMRP on port 6/12 and verify the configuration:

```

Console> (enable) set port gmrp enable 6/12
GMRP enabled on port 6/12.
Console> (enable) show gmrp configuration
Global GMRP Configuration:
GMRP Feature is currently enabled on this switch.
GMRP Timers (milliseconds):
Join = 200
Leave = 600
LeaveAll = 10000
Port based GMRP Configuration:
Port                                     GMRP Status Registration ForwardAll
-----
1/1-2,3/1,6/1-9,6/12,6/15-48,7/1-24    Enabled      Normal      Disabled
6/10-11,6/13-14                        Disabled     Normal      Disabled
Console> (enable)

```

Disabling GMRP on Individual Switch Ports


Note

You can change the per-port GMRP configuration regardless of whether GMRP is enabled globally. However, GMRP will not function on any ports until you enable it globally. For information on configuring GMRP globally on the switch, see the [“Enabling GMRP Globally”](#) section on page 42-18.

To disable GMRP on individual switch ports, perform this task in privileged mode:

	Task	Command
Step 1	Disable GMRP on individual switch ports.	set port gmrp disable <i>mod/port</i>
Step 2	Verify the configuration.	show gmrp configuration

This example shows how to disable GMRP on ports 6/10–14 and verify the configuration:

```

Console> (enable) set port gmrp disable 6/10-14
GMRP disabled on ports 6/10-14.
Console> (enable) show gmrp configuration
Global GMRP Configuration:
GMRP Feature is currently enabled on this switch.
GMRP Timers (milliseconds):
Join = 200
Leave = 600
LeaveAll = 10000
Port based GMRP Configuration:
Port                                     GMRP Status Registration ForwardAll
-----
1/1-2,3/1,6/1-9,6/15-48,7/1-24         Enabled      Normal      Disabled
6/10-14                                 Disabled     Normal      Disabled
Console> (enable)

```

Enabling the GMRP Forward-All Option

When you enable the GMRP forward-all option on a port, a copy of all multicast traffic that is registered on the switch is forwarded to that port. Enable the forward-all option on any port that is connected to a router that needs to receive any multicasts (routers do not support GMRP and cannot send GMRP join messages). The forward-all option can also be used to forward all registered multicast traffic to a port with a network analyzer or probe attached.

To enable the GMRP forward-all option on a switch port, perform this task in privileged mode:

Task	Command
Enable the GMRP forward-all option on a switch port.	set gmrp fwdall enable <i>mod/port</i>

This example shows how to enable the GMRP forward-all option on port 1/1:

```

Console> (enable) set gmrp fwdall enable 1/1
GMRP Forward All groups option enabled on port 1/1.
Console> (enable)

```

Disabling the GMRP Forward-All Option

To disable the GMRP forward-all option on a port, perform this task in privileged mode:

Task	Command
Disable the GMRP forward-all option on a port.	set gmrp fwdall disable <i>mod/port</i>

This example shows how to disable the GMRP forward-all option on port 1/1:

```

Console> (enable) set gmrp fwdall disable 1/1
GMRP Forward All groups option disabled on port 1/1.
Console> (enable)

```

Configuring GMRP Registration

These sections describe how to configure GMRP registration modes on switch ports:

- [Setting Normal Registration, page 42-21](#)
- [Setting Fixed Registration, page 42-21](#)
- [Setting Forbidden Registration, page 42-22](#)

Setting Normal Registration

Configuring a port in **normal** registration mode allows dynamic GMRP multicast registration and deregistration on the port. Normal mode is the default on all switch ports.

To set normal registration on a port, perform this task in privileged mode:

	Task	Command
Step 1	Set normal registration on a port.	set gmrp registration normal <i>mod/port</i>
Step 2	Verify the configuration.	show gmrp configuration

This example shows how to set normal registration on port 2/10:

```
Console> (enable) set gmrp registration normal 2/10
GMRP Registration is set normal on port 2/10.
Console> (enable)
```

Setting Fixed Registration

When you configure a port in **fixed** registration mode, all the multicast groups that are currently registered on all ports are registered on the port, but the port ignores any subsequent registrations or deregistrations on other ports. A port in fixed registration mode continues to register multicast groups that are specific to the port. You must return the port to **normal** registration mode to deregister multicast groups on the port.

To set fixed registration on a port, perform this task in privileged mode:

	Task	Command
Step 1	Set fixed registration on a port.	set gmrp registration fixed <i>mod/port</i>
Step 2	Verify the configuration.	show gmrp configuration

This example shows how to set fixed registration on port 2/10 and verify the configuration:

```
Console> (enable) set gmrp registration fixed 2/10
GMRP Registration is set fixed on port 2/10.
Console> (enable) show gmrp configuration
Global GMRP Configuration:
GMRP Feature is currently enabled on this switch.
GMRP Timers (milliseconds):
Join = 200
Leave = 600
LeaveAll = 10000
```

```

Port based GMRP Configuration:
GMRP-Status Registration ForwardAll Port(s)
-----
Enabled      Normal      Disabled  1/1-4
                                           2/1-9,2/11-48
                                           3/1-24
                                           5/1
Enabled      Fixed      Disabled  2/10
Console> (enable)

```

Setting Forbidden Registration

Setting a port in **forbidden** registration mode deregisters all GMRP multicasts and prevents any further GMRP multicast registration on the port.

To set forbidden registration on a port, perform this task in privileged mode:

	Task	Command
Step 1	Set forbidden registration on a port.	set gmrp registration forbidden <i>mod/port</i>
Step 2	Verify the configuration.	show gmrp configuration

This example shows how to set forbidden registration on port 2/10 and verify the configuration:

```

Console> (enable) set gmrp registration forbidden 2/10
GMRP Registration is set forbidden on port 2/10.
Console> (enable) show gmrp configuration
Global GMRP Configuration:
GMRP Feature is currently enabled on this switch.
GMRP Timers (milliseconds):
Join = 200
Leave = 600
LeaveAll = 10000
Port based GMRP Configuration:
GMRP-Status Registration ForwardAll Port(s)
-----
Enabled      Normal      Disabled  1/1-4
                                           2/1-9,2/11-48
                                           3/1-24
                                           5/1
Enabled      Forbidden  Disabled  2/10
Console> (enable)

```

Setting the GARP Timers



Note

The commands **set gmrp timer** and **show gmrp timer** are aliases for **set garp timer** and **show garp timer**. The aliases may be used if desired.



Note

Modifying the GARP timer values affects the behavior of all GARP applications running on the switch, not just GMRP. (For example, GVRP uses the same timers.)

**Note**

The only ports that send out the GMRP leaveall messages are the ports that have previously received GMRP joins.

You can modify the default GARP timer values on the switch.

When setting the timer values, the value for **leave** must be equal to or greater than three times the **join** value (**leave** \geq **join** * 3). The value for **leaveall** must be greater than the value for **leave** (**leaveall** $>$ **leave**). The more registered attributes on the switch, the greater you should configure the difference between the **leave** value and the **join** value.

For better performance on switches with many registered multicast groups, increase the timer values to the order of seconds.

If you attempt to set a timer value that does not adhere to these rules, an error is returned. For example, if you set the **leave** timer to 600 ms and you attempt to configure the **join** timer to 350 ms, an error is returned. Set the **leave** timer to at least 1050 ms, and then set the **join** timer to 350 ms.

**Caution**

Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, GARP applications (for example, GMRP and GVRP) do not operate successfully.

To set the GARP timer values, perform this task in privileged mode:

	Task	Command
Step 1	Set the GARP timer values.	set garp timer {join leave leaveall} timer_value
Step 2	Verify the configuration.	show garp timer

This example shows how to set the GARP timers and verify the configuration:

```

Console> (enable) set garp timer leaveall 12000
GMRP/GARP leaveAll timer value is set to 12000 milliseconds.
Console> (enable) set garp timer leave 650
GMRP/GARP leave timer value is set to 650 milliseconds.
Console> (enable) set garp timer join 300
GMRP/GARP join timer value is set to 300 milliseconds.
Console> (enable) show garp timer
Timer      Timer Value (milliseconds)
-----
Join       300
Leave       650
LeaveAll    12000
Console> (enable)

```

Displaying GMRP Statistics

To display GMRP statistics on the switch, perform this task in privileged mode:

Task	Command
Display GMRP statistics.	show gmrp statistics [vlan_id]

This example shows how to display GMRP statistics for VLAN 23:

```

Console> show gmrp statistics 23
GMRP Statistics for vlan <23>:
Total valid GMRP Packets Received:500
Join Empties:200
Join INs:250
Leaves:10
Leave Alls:35
Empties:5
Fwd Alls:0
Fwd Unregistered:0
Total valid GMRP Packets Transmitted:600
Join Empties:200
Join INs:150
Leaves:45
Leave Alls:200
Empties:5
Fwd Alls:0
Fwd Unregistered:0
Total valid GMRP Packets Received:0
Total GMRP packets dropped:0
Total GMRP Registrations Failed:0
Console>

```

Clearing GMRP Statistics

To clear all GMRP statistics on the switch, perform this task in privileged mode:

Task	Command
Clear GMRP statistics.	clear gmrp statistics { <i>vlan_id</i> all }

This example shows how to clear the GMRP statistics for all VLANs:

```

Console> (enable) clear gmrp statistics all
Console> (enable)

```

Disabling GMRP Globally on the Switch

To disable GMRP globally on the switch, perform this task in privileged mode:

Task	Command
Disable GMRP globally on the switch.	set gmrp disable

This example shows how to disable GMRP globally on the switch:

```

Console> (enable) set gmrp disable
GMRP disabled.
Console> (enable)

```

Configuring Multicast Router Ports and Group Entries on the Switch

These sections describe how to specify multicast router ports manually and configure multicast group entries:

- [Specifying Multicast Router Ports, page 42-25](#)
- [Configuring Multicast Groups, page 42-25](#)
- [Clearing Multicast Router Ports, page 42-26](#)
- [Clearing Multicast Group Entries, page 42-26](#)

Specifying Multicast Router Ports

When you enable IGMP snooping, the switch automatically learns to which ports a multicast router is connected. However, if desired, you can manually specify multicast router ports.

To specify multicast router ports manually, perform this task in privileged mode:

	Task	Command
Step 1	Manually specify a multicast router port.	set multicast router <i>mod/port</i>
Step 2	Verify the configuration.	show multicast router [<i>mod/port</i>] [<i>vlan_id</i>]

This example shows how to specify a multicast router port manually and verify the configuration (the asterisk [*] next to the multicast router on port 3/1 indicates that the entry was configured manually):

```

Console> (enable) set multicast router 3/1
Port 3/1 added to multicast router port list.
Console> (enable) show multicast router
IGMP disabled

Port      Vlan
-----  -
2/1      99
2/2      255
3/1      * 1
7/9      2,99

Total Number of Entries = 4
'*' - Configured
Console> (enable)

```

Configuring Multicast Groups

To configure a multicast group manually, perform this task in privileged mode:



Note

With software release 7.1(1) and later releases, the maximum number of Layer 2 multicast entries is 15488.

	Task	Command
Step 1	Add one or more multicast MAC addresses to the CAM table.	set cam {static permanent} <i>multicast_mac mod/port [vlan]</i>
Step 2	Verify the multicast group configuration.	show multicast group [<i>mac_addr</i>] [<i>vlan_id</i>]

This example shows how to configure multicast groups manually and verify the configuration (the asterisks indicate that the entry was manually configured):

```

Console> (enable) set cam static 01-00-11-22-33-44 2/6-12
Static multicast entry added to CAM table.
Console> (enable) set cam static 01-11-22-33-44-55 2/6-12
Static multicast entry added to CAM table.
Console> (enable) set cam static 01-22-33-44-55-66 2/6-12
Static multicast entry added to CAM table.
Console> (enable) set cam static 01-33-44-55-66-77 2/6-12
Static multicast entry added to CAM table.
Console> (enable) show multicast group
IGMP disabled

```

```

VLAN  Dest MAC/Route Des  Destination Ports or VCs / [Protocol Type]
-----
1      01-00-11-22-33-44*  2/6-12
1      01-11-22-33-44-55*  2/6-12
1      01-22-33-44-55-66*  2/6-12
1      01-33-44-55-66-77*  2/6-12

```

```

Total Number of Entries = 4
Console> (enable)

```

Clearing Multicast Router Ports

To clear manually configured multicast router ports from the CAM table, perform one of these tasks in privileged mode:

Task	Command
Clear specific, manually configured multicast router ports.	clear multicast router <i>mod/port</i>
Clear all manually configured multicast router ports.	clear multicast router all

This example shows how to clear a manually configured multicast router port entry:

```

Console> (enable) clear multicast router 2/12
Port 2/12 cleared from multicast router port list.
Console> (enable)

```

Clearing Multicast Group Entries

To clear manually configured multicast group entries, perform this task in privileged mode:

Task	Command
Clear a multicast group entry from the CAM table.	<code>clear cam mac_addr [vlan]</code>

This example shows how to clear a multicast group entry from the CAM table:

```
Console> (enable) clear cam 01-11-22-33-44-55 1
CAM entry cleared.
Console> (enable)
```

Understanding How RGMP Works

RGMP constrains multicast traffic that exits the switch through ports to which only disinterested multicast routers are connected. Catalyst 6500 series switches support RGMP, which enables a switch to reduce network congestion by forwarding multicast data traffic to only those routers that are configured to receive it.



Note

To use RGMP, you must enable IGMP snooping on the switch. IGMP snooping constrains multicast traffic that exits through switch ports to which hosts are connected. IGMP snooping does not constrain traffic that exits through ports to which one or more multicast routers are connected.



Note

You must enable PIM on all routers and switches for RGMP to work. Currently, only PIM sparse mode is supported.

All routers on the network must be RGMP capable. RGMP-capable routers send an RGMP hello message to the switch periodically. The RGMP hello message tells the switch not to send multicast data to the router unless an RGMP join message has also been sent to the switch from that router. When an RGMP join message is sent, the router is able to receive multicast data. To learn how to set a router to receive RGMP data, see the [“RGMP-Related CLI Commands”](#) section on page 42-31.

To stop receiving multicast data, a router must send an RGMP leave message to the switch. To disable RGMP on a router, the router must send an RGMP bye message to the switch.

[Table 42-4](#) provides a summary of the RGMP packet types.

Table 42-4 RGMP Packet Types

Description	Action
Hello	When RGMP is enabled on the router, no multicast data traffic is sent to the router by the switch unless an RGMP join is specifically sent for a group.
Bye	When RGMP is disabled on the router, all multicast data traffic is sent to the router by the switch.
Join	Multicast data traffic for a multicast MAC address from the Layer 3 group address G is sent to the router. These packets have group G in the Group Address field of the RGMP packet.
Leave	Multicast data traffic for the group G is not sent to the router. These packets have group G in the group address field of the RGMP packet.

The following restrictions apply to RGMP:

- Sparse mode only—RGMP supports PIM sparse mode only. RGMP does not support PIM dense mode. RGMP explicitly supports the two AutoRP groups in dense mode by not restricting traffic to those groups but by flooding it to all router ports. For this reason, you should configure PIM sparse-dense mode. If you configure groups other than the AutoRP groups for dense mode, their traffic will not be correctly forwarded through the router ports that have been enabled for RGMP.
- To effectively constrain multicast traffic with RGMP, connect RGMP-enabled routers to separate ports on RGMP-enabled switches.
- RGMP constrains only the traffic that exits through ports on which it detects an RGMP-enabled router. If a non-RGMP enabled router is detected on a port, that port receives all multicast traffic.
- RGMP does not support directly connected sources in the network. A directly connected source will send traffic into the network without signaling this through RGMP or PIM. This traffic will not be received by an RGMP-enabled router unless the router already requested receipt of that group through RGMP. This restriction applies to hosts and to functions in routers that source multicast traffic, such as the **ping** and **mtrace** commands, and multicast applications that source multicast traffic, such as UDPTN.
- RGMP supports directly connected receivers in the network. Traffic to these receivers will be constrained by IGMP snooping, or if the receiver is a router itself, by PIM and RGMP. CGMP is not supported in networks where RGMP is enabled on routers. Enabling RGMP and CGMP on a router interface is mutually exclusive. If RGMP is enabled on an interface, CGMP is silently disabled or vice versa.
- The following properties of RGMP are the same as for IGMP snooping:
 - RGMP constrains traffic based on the multicast group, not on the sender's IP address.
 - If spanning tree topology changes occur in the network, the state is not flushed as it is with CGMP.
 - RGMP does not constrain traffic for multicast groups 224.0.0.x (x = 0...255), which allows use of PIMv2 bootstrap router (BSR) in an RGMP-controlled network.
 - RGMP in Cisco switches operates on MAC addresses, not on IP multicast addresses. Since multiple IP multicast addresses can map to one MAC address (see RFC 1112), RGMP cannot differentiate between the IP multicast groups that might map to a MAC address.
 - The capability of the switch to constrain traffic is limited by its content addressable memory (CAM) table capacity.

Configuring RGMP on the Switch

These sections describe the commands for configuring RGMP:

- [Configuring RGMP on the Supervisor Engine, page 42-28](#)
- [Configuring RGMP on the MSFC, page 42-31](#)

Configuring RGMP on the Supervisor Engine

These sections describe the commands for configuring RGMP:

- [Default RGMP Configuration, page 42-29](#)
- [Enabling and Disabling RGMP, page 42-29](#)

- [Displaying RGMP Group Information](#), page 42-29
- [Displaying RGMP VLAN Statistics](#), page 42-30
- [Displaying RGMP-Capable Router Ports](#), page 42-30
- [Clearing RGMP Statistics](#), page 42-31
- [RGMP-Related CLI Commands](#), page 42-31

Default RGMP Configuration

RGMP is disabled by default.

Enabling and Disabling RGMP



Note

To enable RGMP, you must have IGMP snooping enabled.

To enable or disable RGMP, perform these tasks in privileged mode:

Task	Command
Enable RGMP.	set rgmp enable
Disable RGMP.	set rgmp disable

This example shows how to enable RGMP:

```
Console> (enable) set rgmp enable
RGMP enabled.
Console> (enable)
```

This example shows how to disable RGMP:

```
Console> (enable) set rgmp disable
RGMP disabled.
Console> (enable)
```

Displaying RGMP Group Information

Use these commands to display all multicast groups that were joined by one or more RGMP-capable routers and to display the count of multicast groups that were joined by one or more RGMP-capable routers.

To display RGMP group information, perform these tasks in privileged mode:

Task	Command
Display all multicast groups that were joined by one or more RGMP-capable routers.	show rgmp group [<i>mac_addr</i>] [<i>vlan_id</i>]
Display the count of multicast groups that were joined by one or more RGMP-capable routers.	show rgmp group count [<i>vlan_id</i>]

This example shows how to display RGMP group information:

```

Console> (enable) show rgmp group
VlanDest MAC/Route DesRGMP Joined Router Ports
-----
1 01-00-5e-00-01-285/1,5/15
1 01-00-5e-01-01-015/1
2 01-00-5e-27-23-70*3/1, 5/1
Total Number of Entries = 3
`` - Configured
Console> (enable)

Console> (enable) show rgmp group count 1
Total Number of Entries = 2

```

Displaying RGMP VLAN Statistics

To display the RGMP statistics for a specified VLAN, perform this task in privileged mode:

Task	Command
Display the RGMP statistics for a specified VLAN.	show rgmp statistics [vlan]

This example shows how to display the RGMP statistics for a specified VLAN:

```

Console> (enable) show rgmp statistics 23
RGMP enabled
RGMP Statistics for vlan <23>:
Receive:
Valid pkts:20
Hellos:10
Joins:5
Leaves:5
Byes:0
Discarded:0
Transmit:
Total Pkts:10
Failures:0
Hellos:10
Joins:0
Leaves:0
Byes:0
Console> (enable)

```

Displaying RGMP-Capable Router Ports

This command displays the detected RGMP-capable router ports. A “+” in front of the port indicates that it is an RGMP-capable router.

To display the RGMP-capable router ports, perform this task in privileged mode:

Task	Command
Display the RGMP-capable router ports.	show multicast router [igmp rgmp] [mod/port] [vlan_id]

This example shows how to display the ports that are connected to RGMP-capable routers:

```
Console> (enable) show multicast router
Port    Vlan
-----
5/1 +   1
5/14 +  2
5/15   1
Total Number of Entries = 3
'*' - Configured
'+ ' - RGMP-capable
Console> (enable)
```

Clearing RGMP Statistics

This command clears the stored RGMP statistics.

To clear the RGMP statistics, perform this task in privileged mode:

Task	Command
Clear the RGMP statistics.	clear rgmp statistics

This example shows how to clear the RGMP statistics:

```
Console> (enable) clear rgmp statistics
RGMP statistics cleared.
Console> (enable)
```

RGMP-Related CLI Commands

The following RGMP-related CLI commands are accessible from the router:

Task	Command
Enable or disable RGMP.	ip rgmp
Enable or disable RGMP debugging.	debug ip rgmp { <i>group name</i> <i>group address</i> }

Configuring RGMP on the MSFC

To configure RGMP on a VLAN interface on the MSFC, perform this task:

	Task	Command
Step 1	Access VLAN interface configuration mode.	Router(config)# interface vlan <i>vlan_ID</i>
Step 2	Enable RGMP.	Router(config-if)# ip rgmp

You can use the **debug ip rgmp** command to monitor RGMP on the MSFC.

Displaying Multicast Protocol Status

This command displays the status (enabled or disabled) of the Layer 2 multicast protocols on the switch. To display the multicast protocol status, perform this task in privileged mode:

Task	Command
Display the multicast protocol status.	show multicast protocols status

This example shows how to display the multicast protocol status:

```
Console> (enable) show multicast protocols status
IGMP enabled
IGMP fastleave disabled
IGMP V3 processing disabled
IGMP V3 fastblock feature disabled
RGMP disabled
GMRP disabled
Console> (enable)
```