



CHAPTER 51

Configuring Multicast Services

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



Note

For complete syntax and usage information for the commands that are 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 51-1](#)
- [Configuring IGMP Snooping on the Switch, page 51-10](#)
- [Configuring GMRP on the Switch, page 51-20](#)
- [Configuring Multicast Router Ports and Group Entries on the Switch, page 51-27](#)
- [Understanding How RGMP Works, page 51-29](#)
- [Configuring RGMP on the Switch, page 51-31](#)
- [Displaying the Multicast Protocol Status, page 51-35](#)
- [Understanding How Bidirectional PIM Works, page 51-35](#)
- [Configuring Bidirectional PIM on the Switch, page 51-36](#)

Understanding How Multicasting Works

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

- [Multicasting and Multicast Services Overview, page 51-2](#)
- [Understanding How IGMP Snooping Works, page 51-2](#)
- [Understanding How GMRP Works, page 51-6](#)
- [Understanding How RGMP Works, page 51-6](#)
- [Suppressing Multicast Traffic, page 51-7](#)
- [Rate-Limiting RPF Failure Traffic, page 51-7](#)
- [Enabling the Installation of Directly Connected Subnets, page 51-8](#)
- [Understanding IGMP Querier, page 51-8](#)

- [Redundancy for Multicast Traffic, page 51-9](#)

Multicasting and Multicast Services Overview

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

The switches can use IGMP snooping or GMRP to configure the switch ports dynamically so that the IP multicast traffic is forwarded only to those ports that are associated with the IP multicast hosts. The 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 the multicast groups by entering the **set cam static** command. The 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. The 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, Supervisor Engine 2, Supervisor Engine 720, and Supervisor Engine 32). A PFC is not required to enable IGMP snooping. Cisco Group Management Protocol (CGMP) is not supported on the Catalyst 6500 series switches, although the CGMP server is supported on the MSFC. To support the CGMP client devices, configure the MSFC as a CGMP server.



Note

IGMP version 3 snooping is not supported on the systems with a Supervisor Engine 1 or Supervisor Engine 1A.

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

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

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

Periodically, the router sends out general queries to all VLANs. As the 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 the 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.

IGMP version 3 snooping uses source-based filtering and is the industry-designated standard protocol for the hosts to signal channel subscriptions in Source Specific Multicast (SSM). The source-based filtering enables the 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 the IGMP version 3 states based on the IGMP version 3 reports that it receives from a port on a per-group, per-VLAN basis and either allows or blocks the source traffic on that port based on the type of IGMP version 3 message that it receives. If the switch receives the IGMP version 2 snooping reports for SSM, the reports are forwarded to the MSFC2 and a system error message is generated.

**Note**

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

IGMP Version 3 Snooping Restrictions

The following restrictions apply to IGMP version 3 snooping:

- With software release 8.3(1), it is mandatory that you run Cisco IOS Release 12.2(17d)SXB1 if you plan on using IGMP version 3 snooping with MMLS.
- IGMP version 3 snooping should be used with PIM-SSM only. For the IGMP version 3 reports that are received in non-SSM mode, IGMP version 2 snooping is performed.
- IGMP version 3 snooping is supported for INCLUDE mode only. IGMP version 3 snooping is not supported for EXCLUDE mode. IGMP version 3 reports pertaining to EXCLUDE mode are not processed but are just flooded on the VLAN.
- IGMP version 3 snooping will not discover the routers running Multicast OSPF (MOSPF) or Distance Vector Multicast Routing Protocol (DVMRP) in software release 8.3(1) and later releases.
- SPAN, RSPAN, private VLANs, and RGMP are not supported with IGMP version 3 snooping.
- IGMP version 3 snooping is supported for Single-Router Mode (SRM) only. Although Supervisor Engine 2 supports Dual-Router Mode (DRM), IGMP version 3 snooping does not support DRM.
- IGMP version 3 snooping is not supported on the systems with a Supervisor Engine 1 or Supervisor Engine 1A.
- *, G/m hardware switching for the SSM flows is supported for the ACEs that have only the permit action. The deny action should not be used for SSM. Configuring an ACE with the deny action when SSM is used may cause data loss for the IGMP version 2 snooping hosts, which operate under regular PIM sparse mode.
- A system that is configured for Layer 2 switching supports only approximately 700 ACLs.

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 to which 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 the multicast traffic for 224.1.2.3 to this segment.

When a second host in this VLAN wants to join group 224.1.2.3, 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).

The IGMP version 3 reports are sent by the 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. The 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 the 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 the traffic. This mode indicates that the host wants to receive the traffic only from those sources with IP addresses that are not listed in the EXCLUDE list. To receive the traffic from all sources, a host expresses EXCLUDE mode membership with an empty EXCLUDE list.

**Note**

If IP MMLS is disabled, 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 the multicast traffic to a group, the switch hardware does not recognize the stream as IGMP control packets. 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 the IGMP general queries. The switch floods these queries on all ports in the VLAN, and the 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. The 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 the 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 the multicast traffic. When the 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). In the systems with a Supervisor Engine 1 or 2, 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 the 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 the ports in the VLAN. The 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 244.0.0.1 (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.

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 the 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.

The 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 the 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 the 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 the 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 the 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 the routers are attached. (See the [“Enabling the GMRP Forward-All Option on a Switch Port”](#) section on page 51-22.)

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 the 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 the 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. The RGMP-capable routers periodically send an RGMP hello message to the switch. The RGMP hello message tells the switch not to send the 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 the multicast data. To learn how to set a router to receive the RGMP data, see the [“RGMP-Related CLI Commands”](#) section on page 51-34.

To stop receiving the 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 51-1](#) provides a summary of the RGMP message types.

Table 51-1 *RGMP Message 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.

Suppressing Multicast Traffic

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

Rate-Limiting RPF Failure Traffic

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 topology, only the Protocol Independent Multicast-designated forwarder (PIM-DF) forwards the data in the common VLAN, and 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. The traffic that fails the RPF check is called the non-RPF traffic.

According to the multicast protocol specification, the router needs to receive the non-RPF packets for the PIM assert mechanism to function properly, so that all non-RPF packets cannot be dropped in the hardware.

PFC3A has enhanced hardware support for non-RPF packet rate limiting. On receiving a non-RPF packet, PFC3A creates a non-RPF entry (which contains source, group, and ingress interface information) in the NetFlow table, if there is no matching entry already present, and then bridges the non-RPF packet on the incoming VLAN and to MSFC3. The non-RPF packets that already have a matching NetFlow entry are only bridged on the incoming VLAN and are not sent to MSFC3.

The non-RPF entries in the NetFlow table are periodically aged out so that the non-RPF packets are leaked to MSFC3 for the PIM assert mechanism to function properly.

Rate limiting of RPF failures is enabled by default.

Enabling the 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 the new sources for the group from being learned in the routing table, the (*,G) flows should remain completely hardware-switched flows. The (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. The installation of directly connected subnets is enabled globally by default. One (subnet/mask, 224/4) is installed per PIM-enabled interface.

Enter the **show mls ip multicast connected** command to view these FIB entries.

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

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

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

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

Understanding IGMP Querier

IGMP querier 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 the general query messages from the other switches. If the switch receives a general query, a querier election starts. A querier election across the 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 51-16.

Redundancy for Multicast Traffic

Redundancy for multicast traffic requires the following conditions:

- Unicast routing protocol such as OSPF or EIGRP

PIM uses RPF checks on the unicast routing table to determine the proper paths for multicast data to traverse. If a unicast routing path changes, PIM relies upon the unicast routing protocol (OSPF) to properly converge, so that the RPF checks used by PIM continue to work and show valid unicast paths to and from the source IP address of the server sourcing the multicast stream.

- PIM configured on all related Layer 3 interfaces

The unicast routing table is used to do path selection for PIM. PIM uses RPF checks to ultimately determine the shortest path tree (SPT) between the client (receiver VLAN) and the source (multicast VLAN). Therefore, the objective of PIM is to find the shortest unicast path between the receiver subnet and the source subnet. You do not need to configure anything else for multicast when the unicast routing protocol is working as expected and PIM is configured on all the Layer 3 links associated with the unicast routing protocol.

Configuring IGMP Snooping on the Switch

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


Note

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

These sections describe how to configure IGMP snooping:

- [Default IGMP Snooping Configuration, page 51-10](#)
- [IGMP Snooping Configuration Guidelines, page 51-11](#)
- [Enabling IGMP Snooping, page 51-11](#)
- [Enabling IGMP Flooding, page 51-12](#)
- [Specifying the IGMP Snooping Mode, page 51-12](#)
- [Specifying the IGMP Leave-Query Type, page 51-13](#)
- [Enabling IGMP Fast-Leave Processing, page 51-13](#)
- [Enabling IGMP Version 3 Snooping, page 51-14](#)
- [Enabling IGMP Version 3 Fast-Block Processing, page 51-15](#)
- [Enabling IGMP Rate Limiting, page 51-15](#)
- [Enabling the IGMP Querier, page 51-16](#)
- [Displaying Multicast Router Information, page 51-17](#)
- [Displaying Multicast Group Information, page 51-18](#)
- [Displaying IGMP Snooping Statistics, page 51-18](#)
- [Disabling IGMP Fast-Leave Processing, page 51-19](#)
- [Disabling IGMP Snooping, page 51-19](#)

Default IGMP Snooping Configuration

[Table 51-2](#) shows the default IGMP snooping configuration.


Note

IGMP snooping is enabled by default in all supervisor engine software releases in the 7.x and 8.x release trains. It is enabled by default in software release 5.5(9) and later releases in the 5.x release train and in software release 6.3(1) and later releases in the 6.x train.

Table 51-2 IGMP Snooping Default Configuration

Feature	Default Value
IGMP snooping	Enabled
Multicast routers	None configured

IGMP Snooping Configuration Guidelines

This section describes the IGMP snooping configuration guidelines:

- 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 that are 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, group, and source-specific (GSS) queries are flooded onto the VLAN to refresh the memberships.
- At least one version 3 router must 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 sent to the supervisor engine. The 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, the RGMF, SPAN, and RSPAN interaction is not enabled.
- IGMP querier interoperates only with IGMP version 2 snooping. Before you enable IGMP version 3 snooping, you must disable IGMP querier.

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.	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)

```

Enabling IGMP Flooding

When you disable IGMP flooding, the source traffic is never flooded in the VLAN and is sent only to the router ports. IGMP flooding is enabled by default.

To enable or disable IGMP flooding, perform this task in privileged mode:

	Task	Command
Step 1	Enable or disable IGMP flooding.	set igmp flooding {enable disable}
Step 2	Display the IGMP flooding state.	show igmp flooding

These examples show how to enable and disable IGMP flooding:

```

Console> (enable) set igmp flooding enable
IGMP Flooding enabled (default)
Console> (enable) set igmp flooding disable
IGMP Flooding disabled
Console> (enable)
Console> (enable) show igmp flooding
Mcast flooding disabled
Console> (enable)

```

Specifying the 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 that is present on the network. IGMP-only mode is used in the networks with no CGMP devices. IGMP-CGMP mode is used in the 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 specify 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)
```

Specifying the IGMP Leave-Query Type

You can specify the IGMP leave-query type to be used when a port receives a leave message from a host. When you specify a MAC-based general query, a leave query is sent for the exact GDA, and the version 1 or 2 hosts that have at least one membership for a group using that GDA will respond. When you specify a general query, the reports from all version 1 and 2 hosts for all groups are registered. You can also specify the auto mode. If you specify auto mode, a group-specific query is sent if there are no version 1 hosts in the network and a general query is sent if there are version 1 hosts in the network. A group-specific query provides faster network convergence.

By default, a MAC-based general query is sent when a port receives a leave message.

To specify the leave-query type, perform this task in privileged mode:

	Task	Command
Step 1	Specify the IGMP leave-query type.	set igmp leave-query-type auto-mode general-query mac-gen-query
Step 2	Display the IGMP leave-query type.	show igmp leave-query-type

This example shows how to set the IGMP leave-query type to a group-specific-query:

```
Console> (enable) set igmp leave-query-type auto-mode
IGMP Leave Query Type set to auto-mode
Console> (enable) show igmp leave-query-type
IGMP Leave Query Type : Group-Specific Query
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 multicast protocols status

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.
Warning:Can cause disconnectivity if there are more than one host joining the
        same group per access port.
console> (enable) show multicast protocols status
IGMP disabled
IGMP fastleave enabled
IGMP V3 processing disabled
IGMP V3 fastblock feature disabled
RGMP enabled
GMRP disabled
Console> (enable)

```

Enabling IGMP Version 3 Snooping

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

	Task	Command
Step 1	Enable IGMP version 3 snooping.	set igmp v3-processing enable
Step 2	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:

```

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.	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 IGMP Rate Limiting

Enter the **set multicast ratelimit** command to rate limit the multicast packets. The multicast packet rate limiting is disabled by default, and the default rate limit is 0 packets per second (pps).

To enable multicast rate limiting and specify a rate limit, perform this task in privileged mode:

	Task	Command
Step 1	Enable multicast rate limiting and specify a rate limit.	set multicast ratelimit {disable enable} set multicast ratelimit rate rate
Step 2	Display multicast rate limiting information.	show multicast ratelimit-info

This example shows how to enable multicast rate limiting and specify a rate limit:

```

Console> (enable) set multicast ratelimit enable
Enabling Multicast Ratelimiting
Set a non-zero threshold rate to operationally enable multicast ratelimiting
Console> (enable) set multicast ratelimit rate 1000
Multicast ratelimit watermark rate is set to 1000 pps
Console> (enable) show multicast ratelimit-info
Multicast ratelimiting enabled
Ratelimit threshold rate: 1000 pps
VLAN  RateLimited-Since          Ratelimited-for(seconds)
-----
Console> (enable)

```

Enabling the IGMP Querier

Enter 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 the querier.

To enable the IGMP querier in a VLAN, perform one of 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
Specify an IP address for the IGMP querier. If you do not specify an IP address, the default IP address is 0.0.0.0.	set igmp querier address ip_address vlan
Display IGMP querier information.	show igmp querier information

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

```

Console> (enable) set igmp querier enable 4001
IGMP querier is enabled for VLAN(s) 4001
Console> (enable) set igmp querier 4001 qi 130
QI for VLAN(s) 4001 set to 130 second(s)
Console> (enable) set igmp querier address 40.1.1.1 4001
Querier Address for vlan 4001 set to 40.1.1.1
Console> (enable) show igmp querier information
VLAN Querier Address Querier State      Query Tx Count  QI (sec)  OQI (sec)
-----
4001 40.1.1.1      QUERIER                0           130       300
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 one of these tasks in privileged mode:

Task	Command
Display information on the 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 2/1 indicates that the entry was configured manually):

```
Console> (enable) show multicast router
Port          Vlan
-----
 2/1          *          @ 99
 2/2          @ 201
16/1          +          @ 10,200-201

Total Number of Entries = 3
'*' - Configured
'+' - RGMP-capable
'#' - Channeled Port
'$' - IGMP-V3 Router
'@' - IGMP-Querier Router
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
'*' - Configured
'+' - RGMP-capable
'#' - Channeled Port
'$' - IGMP-V3 Router
'@' - IGMP-Querier Router
Console> (enable)
```

Displaying Multicast Group Information

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

Task	Command
Display information about the multicast groups.	show multicast group [<i>mac_addr</i>] [<i>vlan_id</i>]
Display information only about the 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 the IGMP snooping statistics on the switch, perform this task:

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

This example shows how to display the IGMP snooping statistics:

```
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: 10
    Group Specific Queries: 0
```

```

Group and Source Specific Queries: 0
    Reports: 0
    Leaves: 0
    Total Valid pkts: 20
    Total Invalid pkts: 0
    Other pkts: 5
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: 0
IGMP V3 IS_EX messages: 0
IGMP V3 TO_IN messages: 0
IGMP V3 TO_EX messages: 0
IGMP V3 ALLOW messages: 0
IGMP V3 BLOCK messages: 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.	set igmp fastleave disable

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

```

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

```

Disabling IGMP Snooping

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

Task	Command
Disable IGMP snooping.	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 51-20](#)
- [Default GMRP Configuration, page 51-20](#)
- [Enabling GMRP Globally, page 51-21](#)
- [Enabling GMRP on Individual Switch Ports, page 51-21](#)
- [Disabling GMRP on Individual Switch Ports, page 51-22](#)
- [Enabling the GMRP Forward-All Option on a Switch Port, page 51-22](#)
- [Disabling the GMRP Forward-All Option on a Switch Port, page 51-23](#)
- [Configuring GMRP Registration, page 51-23](#)
- [Setting the GARP Timers, page 51-25](#)
- [Displaying GMRP Statistics, page 51-26](#)
- [Clearing GMRP Statistics, page 51-26](#)
- [Disabling GMRP Globally on the Switch, page 51-27](#)



Note

For an overview of GMRP operation, see the [“Understanding How GMRP Works”](#) section on page 51-6.

GMRP Software Requirements

GMRP requires supervisor engine software release 5.2 or later releases.

Default GMRP Configuration

[Table 51-3](#) shows the default GMRP configuration.

Table 51-3 *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.	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, see the [“Enabling GMRP Globally”](#) section on page 51-21.

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

	Task	Command
Step 1	Enable GMRP on an individual switch port.	set port gmrp enable mod/port
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
-----
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, see the [“Enabling GMRP Globally”](#) section on page 51-21.

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

	Task	Command
Step 1	Disable GMRP on the individual switch ports.	set port gmrp disable mod/port
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
-----
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 on a Switch Port

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 mod/port

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 on a Switch Port

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

Task	Command
Disable the GMRP forward-all option on a switch 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 the GMRP registration modes on the switch ports:

- [Setting Normal Registration, page 51-23](#)
- [Setting Fixed Registration, page 51-24](#)
- [Setting Forbidden Registration, page 51-24](#)

Setting Normal Registration

Configuring a switch 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 the normal registration on a switch port, perform this task in privileged mode:

	Task	Command
Step 1	Set the normal registration on a switch 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 switch 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 switch port in fixed registration mode continues to register the multicast groups that are specific to the port. You must return the port to **normal** registration mode to deregister the multicast groups on the port.

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

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

This example shows how to set the 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 switch port in **forbidden** registration mode deregisters all GMRP multicasts and prevents any further GMRP multicast registration on the port.

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

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

This example shows how to set the 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 the 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 the 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, the 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 } <i>timer_value</i>
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 the GMRP statistics on the switch, perform this task in privileged mode:

Task	Command
Display the GMRP statistics.	show gmrp statistics [<i>vlan_id</i>]

This example shows how to display the 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 the 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 the multicast router ports manually and configure the multicast group entries:

- [Specifying Multicast Router Ports, page 51-27](#)
- [Configuring Multicast Groups, page 51-28](#)
- [Clearing Multicast Router Ports, page 51-29](#)
- [Clearing Multicast Group Entries, page 51-29](#)

Specifying Multicast Router Ports

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

To specify the 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 [igmp rgmp][<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 2/2 indicates that the entry was configured manually):

```

Console> (enable) set multicast router 2/2
Port 2/2 added to multicast router port list.
console> (enable) show multicast router
Port          Vlan
-----
2/2          *          50
8/48         @          10
16/1         @        200-201

Total Number of Entries = 3
'*' - Configured
'+' - RGMP-capable
'#' - Channeled Port
'$' - IGMP-V3 Router
'@' - IGMP-Querier Router
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 the 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 the manually configured multicast router ports, perform one of these tasks in privileged mode:

Task	Command
Clear the 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:

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

Clearing Multicast Group Entries

To clear the manually configured multicast group entries from the CAM table, perform this task in privileged mode:

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

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 the multicast traffic that exits the switch through the ports to which only the disinterested multicast routers are connected. Catalyst 6500 series switches support RGMP, which enables a switch to reduce network congestion by forwarding the 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 the multicast traffic that exits through the switch ports to which the hosts are connected. IGMP snooping does not constrain the traffic that exits through the 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 the 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 the multicast data. To learn how to set a router to receive the RGMP data, see the “[RGMP-Related CLI Commands](#)” section on page 51-34.

To stop receiving the 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 51-4 provides a summary of the RGMP packet types.

Table 51-4 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.

These 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 the 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 the multicast traffic with RGMP, connect the RGMP-enabled routers to separate the ports on the RGMP-enabled switches.
- RGMP constrains only the traffic that exits through the 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 the directly connected sources in the network. A directly connected source will send the 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 the hosts and to the functions in the routers that source the multicast traffic, such as the **ping** and **mtrace** commands, and the multicast applications that source the multicast traffic, such as UDPTN.
- RGMP supports the directly connected receivers in the network. The traffic to these receivers will be constrained by IGMP snooping, or if the receiver is a router, by PIM and RGMP. CGMP is not supported in the networks where RGMP is enabled on the 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 the traffic that is 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 the traffic for multicast groups 224.0.0.x (x = 0...255), which allow use of the PIMv2 bootstrap router (BSR) in an RGMP-controlled network.
 - RGMP in the Cisco switches operates on the MAC addresses, not on the IP multicast addresses. Because 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 the 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 51-31](#)
- [Configuring RGMP on the MSFC, page 51-35](#)

Configuring RGMP on the Supervisor Engine

These sections describe the commands for configuring RGMP:

- [Default RGMP Configuration, page 51-31](#)
- [Enabling and Disabling RGMP, page 51-32](#)
- [Displaying RGMP Group Information, page 51-32](#)
- [Displaying RGMP VLAN Statistics, page 51-33](#)
- [Displaying RGMP-Capable Router Ports, page 51-33](#)
- [Clearing RGMP Statistics, page 51-34](#)
- [RGMP-Related CLI Commands, page 51-34](#)

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 one of 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 one of 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 given VLAN, perform this task in privileged mode:

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

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
Bytes:0
Discarded:0
Transmit:
Total Pkts:10
Failures:0
Hellos:10
Joins:0
Leaves:0
Bytes: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 [<i>igmp</i> <i>rgmp</i>] [<i>mod/port</i>] [<i>vlan_id</i>]

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

```
Console> (enable) show multicast router
Port          Vlan
-----
 2/2          +      @ 40
 8/48         @ 10
16/1          +      @ 200-201

Total Number of Entries = 3
'*' - Configured
'+' - RGMP-capable
'#' - Channeled Port
'$' - IGMP-V3 Router
'@' - IGMP-Querier Router
Console> (enable)
```

This example shows how to display only the RGMP-capable router ports:

```

Console> (enable) show multicast router rgmp
Port          Vlan
-----
 2/2      +      @ 40
16/1      +      @ 200

Total Number of Entries = 2
'*' - Configured
'+' - RGMP-capable
'#' - Channeled Port
'$' - IGMP-V3 Router
'@' - IGMP-Querier Router
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

This command enables or disables the RGMP-related commands from the router.

To enable or disable RGMP, perform one of these tasks in configuration mode:

Task	Command
Enable RGMP.	Router(config)# ip rgmp
Disable RGMP.	Router(config)# no ip rgmp

This command enables or disables RGMP debugging.

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

Task	Command
Enable RGMP debugging.	Router# debug ip rgmp [<i>group-name</i> <i>group-address</i>]
Disable RGMP debugging.	Router# no 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 the 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)
```

Understanding How Bidirectional PIM Works

Supervisor Engine 720 supports the hardware forwarding of the bidirectional Protocol Independent Multicast (PIM) groups. To support the bidirectional PIM groups, Supervisor Engine 720 implements a new mode called designated forwarder (DF) mode. The designated forwarder is the router that is elected to forward the packets to and from a segment for a bidirectional PIM group. In DF mode, the supervisor engine accepts the packets from the reverse path forwarding (RPF) interface and from the DF interface.

When the supervisor engine is forwarding the bidirectional PIM groups, the RPF interface is always included in the outgoing interface list of (*,G) entry, and the DF interfaces are included depending on IGMP/PIM joins.

If the route to the RP becomes unavailable, the group is changed to dense mode. If the RPF link to the RP becomes unavailable, the bidirectional flow is removed from the hardware FIB.

Configuring Bidirectional PIM on the Switch

These sections show how to configure bidirectional PIM and display the bidirectional PIM configuration information and statistics:

- [Configuring Bidirectional PIM, page 51-36](#)
- [Enabling or Disabling Bidirectional PIM Globally, page 51-36](#)
- [Configuring the Rendezvous Point for Bidirectional Groups, page 51-37](#)
- [Setting the Bidirectional PIM Scan Interval, page 51-37](#)
- [Displaying Bidirectional PIM Information, page 51-38](#)

Configuring Bidirectional PIM

To configure bidirectional PIM, perform these steps:

-
- Step 1** Enable bidirectional PIM globally.
- Step 2** Configure the rendezvous point for the bidirectional group.
-

These steps are described in detail in the following sections.

Enabling or Disabling Bidirectional PIM Globally

To enable or disable bidirectional PIM, perform one of these tasks:

Task	Command
Enable bidirectional PIM globally on the switch.	Router(config)# ip pim bidir-enable
Disable bidirectional PIM globally on the switch.	Router(config)# [no] ip pim bidir-enable

This example shows how to enable bidirectional PIM on the switch:

```
Router(config)# ip pim bidir-enable
Router(config)#
```

This example shows how to disable bidirectional PIM on the switch:

```
Router(config)# no ip pim bidir-enable
Router(config)#
```

Configuring the Rendezvous Point for Bidirectional Groups



Note

The traffic flow for the groups mapping to only four bidirectional rendezvous points (RPs) is hardware switched. The traffic to the rest of the groups is software forwarded.

To configure the rendezvous point for a bidirectional group statically, perform this task:

Task	Command
Step 1 Statically configure the IP address of the rendezvous point for the group. When you specify the override keyword, the static rendezvous point is used.	Router(config)# ip pim rp-address <i>ip_address</i> <i>access-list</i> [override]
Step 2 Configure an access list.	Router(config)# access-list <i>access-list</i> permit deny <i>ip_address</i>
Step 3 Configure the system to use Auto-RP to configure groups for which the router will act as an RP.	Router(config)# ip pim send-rp-announce <i>type</i> <i>number</i> scope <i>ttl-value</i> [group-list <i>access-list</i>] [interval <i>seconds</i>] [bidir]
Step 4 Configure a standard IP access list.	Router(config)# ip access-list standard <i>access-list-name</i> permit deny <i>ip_address</i>
Step 5 Enable MLS IP multicast.	Router(config)# mls ip multicast

This example shows how to configure a static rendezvous point for a bidirectional group:

```
Router(config)# ip pim rp-address 10.0.0.1 10 bidir override
Router(config)# access-list 10 permit 224.1.0.0 0.0.255.255
Router(config)# ip pim send-rp-announce Loopback0 scope 16 group-list c21-rp-list-0 bidir
Router(config)# ip access-list standard c21-rp-list-0 permit 230.31.31.1 0.0.255.255
```

Setting the Bidirectional PIM Scan Interval

You can specify the interval between the bidirectional PIM RP Reverse Path Forwarding (RPF) scans.

To set the bidirectional RP RPF scan interval, perform one of these tasks:

Task	Command
Set the bidirectional RP RPF scan interval; valid values are from 1 to 1000 seconds. The default is 10 seconds.	Router(config)# mls ip multicast bidir gm-scan-interval <i>interval</i>
Restore the default.	Router(config)# no mls ip multicast bidir gm-scan-interval

This example shows how to set the bidirectional RP RPF scan interval:

```
Router(config)# mls ip multicast bidir gm-scan-interval 30
Router(config)#
```

This example shows how to restore the default bidirectional RP RPF scan interval:

```
Router(config)# no mls ip multicast bidir gm-scan-interval
Router(config)#
```

Displaying Bidirectional PIM Information

To display the bidirectional PIM information, perform one of these tasks:

Task	Command
Display the mappings between the PIM groups and the rendezvous points and show the learned rendezvous points in use.	Router# show ip pim rp mapping [in-use]
Display the PIM group to the active rendezvous-point mappings.	Router# show mls ip multicast rp-mapping [rp-address]
Display information based on the group/mask ranges in the RP-mapping cache.	Router# show mls ip multicast rp-mapping gm-cache
Display information based on the DF list in the RP-mapping cache.	Router# show mls ip multicast rp-mapping df-cache
Display the bidirectional PIM information.	Router# show mls ip multicast bidir
Display information about the multicast routing table.	Router# show ip mroute

This example shows how to display information about the PIM group and rendezvous-point mappings:

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP (Auto-RP)
This system is an RP-mapping agent
Group(s) 230.31.0.0/16
  RP 60.0.0.60 (?), v2v1, bidir
    Info source:60.0.0.60 (?), elected via Auto-RP
      Uptime:00:03:47, expires:00:02:11
  RP 50.0.0.50 (?), v2v1, bidir
    Info source:50.0.0.50 (?), via Auto-RP
      Uptime:00:03:04, expires:00:02:55
  RP 40.0.0.40 (?), v2v1, bidir
    Info source:40.0.0.40 (?), via Auto-RP
      Uptime:00:04:19, expires:00:02:38
```

This example shows how to display information in the IP multicast routing table that is related to bidirectional PIM:

```
Router# show ip mroute bidirectional
(*, 225.1.3.0), 00:00:02/00:02:57, RP 3.3.3.3, flags:BC
  Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
  Outgoing interface list:
    GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:02/00:00:00,H
    Vlan30, Forward/Sparse-Dense, 00:00:02/00:02:57, H

(*, 225.1.2.0), 00:00:04/00:02:55, RP 3.3.3.3, flags:BC
  Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
  Outgoing interface list:
    GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:04/00:00:00,H
    Vlan30, Forward/Sparse-Dense, 00:00:04/00:02:55, H

(*, 225.1.4.1), 00:00:00/00:02:59, RP 3.3.3.3, flags:BC
  Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
  Outgoing interface list:
    GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:00/00:00:00,H
    Vlan30, Forward/Sparse-Dense, 00:00:00/00:02:59, H
```

This example show how to display information that is related to a specific multicast route:

```
Router# show ip mroute 239.1.1.2 4.4.4.4
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
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode

(4.4.4.4, 239.1.1.2), 1d02h/00:03:20, flags:FTZ
Incoming interface:Loopback0, RPF nbr 0.0.0.0, Partial-SC
Outgoing interface list:
  Vlan10, Forward/Sparse-Dense, 1d02h/00:02:39 (ttl-threshold 5)
```

This example shows how to display the entries for a specific multicast group address:

```
Router# show mls ip multicast group 230.31.31.1
Multicast hardware switched flows:
(*, 230.31.31.1) Incoming interface:Vlan611, Packets switched:1778
Hardware switched outgoing interfaces:Vlan131 Vlan151 Vlan415 Gi4/16 Vlan611
RPF-MFD installed
```

This example shows how to display the PIM group to the active rendezvous-point mappings:

```
Router# show mls ip multicast rp-mapping
State:H - Hardware Switched, I - Install Pending, D - Delete Pending, Z - Zombie

RP Address      State      RPF      DF-count   GM-count
60.0.0.60      H         V1611    4          1
```

This example shows how to display information that is based on the group/mask ranges in the RP-mapping cache:

```
Router# show mls ip multicast rp-mapping gm-cache
State:H - Hardware Switched, I - Install Pending, D - Delete Pending,
      Z - Zombie

RP Address      State      Group      Mask      State      Packet/Byte-count
60.0.0.60      H         230.31.0.0 255.255.0.0 H          100/6400
```

This example shows how to display information about the specific MLS IP multicasting groups:

```
Router# show mls ip multicast rp-mapping df-cache
State:H - Hardware Switched, I - Install Pending, D - Delete Pending, Z - Zombie

RP Address      State      DF      State
60.0.0.60      H         V1131   H
60.0.0.60      H         V1151   H
60.0.0.60      H         V1415   H
60.0.0.60      H         Gi4/16   H
```

