



Configuring Multicast Services

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping, GARP Multicast Registration Protocol (GMRP), and Router Group Management Protocol (RGMP) on the Catalyst 6000 family switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6000 Family Command Reference* publication.

This chapter consists of these sections:

- Understanding How Multicasting Works, page 34-1
- Configuring IGMP Snooping, page 34-4
- Configuring GMRP, page 34-9
- Configuring Multicast Router Ports and Group Entries, page 34-17
- Understanding How RGMP Works, page 34-19
- Configuring RGMP, page 34-20

Understanding How Multicasting Works

These sections describe how multicasting works on the Catalyst 6000 family switches:

- Understanding Multicasting and Multicast Services Operation, page 34-2
- Joining a Multicast Group, page 34-2
- Leaving a Multicast Group, page 34-3
- Understanding GMRP, page 34-3

Understanding Multicasting and Multicast Services Operation

IGMP snooping and GMRP manage multicast traffic in switches by allowing directed switching of IP 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 associated with IP multicast hosts.

**Note**

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

IGMP software components run on both the Cisco router and the switch. An IGMP-capable IP multicast router sees all IGMP packets and can inform the switch when specific hosts join or leave IP multicast groups.

When the IGMP-capable router receives an IGMP control packet, it creates an IGMP packet that contains the request type (either join or leave), the multicast group address, and the MAC address of the host. The router sends the packet to a well-known address to which all switches listen. When a switch receives the packet, the supervisor engine interprets the packet and modifies the forwarding table automatically.

Multicast groups learned through IGMP snooping are dynamic, but you can statically configure multicast groups using the **set cam static** command. If you specify group membership for a multicast group address, your static setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings, but when static multicast entries are configured, source-only entry creation for source-only traffic will not occur. As a result the multicast router ports will not be added to those entries, and traffic is not forwarded to the router ports.

**Note**

If a spanning-tree VLAN topology changes, the IGMP snooping-learned multicast groups on the VLAN are purged and the IGMP-capable router generates new multicast group information.

If an IGMP snooping-learned port link is disabled for any reason, that port is removed from any multicast group memberships.

Joining a Multicast Group

When a host wants to join an IP multicast group, it sends an IGMP join message specifying its MAC address and the IP multicast group it wants to join. The IGMP-capable router then builds an IGMP join message and multicasts the join message to the well-known address to which the switches listen.

Upon receipt of the join message, each switch searches its Enhanced Address Recognition Logic (EARL) table to determine if it contains the MAC address of the host asking to join the multicast group. If a switch finds the MAC address of the host in its EARL table associating the MAC address with a nontrunking port, the switch creates a multicast forwarding entry in the EARL forwarding table. The host associated with that port receives multicast traffic for that multicast group. In this way, the EARL automatically learns the MAC addresses and port numbers of the IP multicast hosts.

Leaving a Multicast Group

The IGMP-capable router sends periodic multicast group queries. If a host wants to remain in a multicast group, it responds to the query from the router. In this case, the router does nothing. If a host does not want to remain in the multicast group, it does not respond to the router query. If after a number of queries the router receives no reports from any host in a multicast group, the router sends an IGMP command to the switch, telling it to remove the multicast group from its forwarding tables.

**Note**

If there are other hosts in the same multicast group and they *do* respond to the multicast group query, the router does not tell the switch to remove the group from its forwarding tables. The router does not remove a multicast group from the forwarding tables of the switch until all the hosts in the group ask to leave the group.

Understanding GMRP

GARP Multicast Registration Protocol (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 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, GMRP is typically used with IGMP; 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 uses the received GMRP traffic to constrain multicasts at Layer 2 in the host's VLAN.

**Note**

In all cases, you can use IGMP snooping to constrain multicasts at Layer 2 without the need to install or configure software on hosts. Note that the traditional CGMP client functionality provided by the switch processor (SP) is not supported on Catalyst 6000 family switches (CGMP is enabled using **set cgmp enable** on other Catalyst switches). However, CGMP server functionality is supported at the route processor (RP) on the Catalyst 6000 family MSFC virtual interfaces to support switches that only support CGMP.

When a host wants to join an IP multicast group, it sends an IGMP join message, which spawns a GMRP join message.

Upon receipt of the GMRP join message, the switch adds the port through which the join message was received to the appropriate multicast group. The switch propagates the GMRP join message 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. In this case, 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 GMRP Forward-All Option” section on page 34-12).

Configuring IGMP Snooping

Internet Group Management Protocol (IGMP) snooping allows switches to examine IGMP packets and make forwarding decisions based on their content.

**Note**

QoS does not support IGMP traffic when IGMP snooping is enabled.

These sections describe how to configure IGMP snooping:

- Default IGMP Snooping Configuration, page 34-4
- Enabling IGMP, page 34-4
- Enabling IGMP Fast-Leave Processing, page 34-5
- Displaying Multicast Router Information, page 34-6
- Displaying Multicast Group Information, page 34-7
- Displaying IGMP Statistics, page 34-8
- Disabling IGMP Fast-Leave Processing, page 34-8
- Disabling IGMP, page 34-9

Default IGMP Snooping Configuration

Table 34-1 shows the default IGMP snooping configuration.

Table 34-1 IGMP Snooping Default Configuration

Feature	Default Value
IGMP snooping	Disabled
Multicast routers	None configured

Enabling IGMP

**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_num]

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:
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)

```

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 leave

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 fastleave 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
Other Pkts rcvd                0
Queries Xmitted                0
GS Queries Xmitted            16
Reports Xmitted                0
Leaves Xmitted                 0
Failures to add GDA to EARL    0
Topology Notifications rcvd    10
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
<ul style="list-style-type: none"> Display information on dynamically learned and manually configured multicast router ports. 	show multicast router [<i>mod_num/port_num</i>] [<i>vlan_id</i>]
<ul style="list-style-type: none"> Display information only on those multicast router ports learned dynamically using IGMP snooping. 	show multicast router igmp [<i>mod_num/port_num</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
<ul style="list-style-type: none"> Display information about multicast groups. 	show multicast group [<i>mac_addr</i>] [<i>vlan_id</i>]
<ul style="list-style-type: none"> Display only information about multicast groups learned dynamically through IGMP. 	show multicast group igmp [<i>mac_addr</i>] [<i>vlan_id</i>]
<ul style="list-style-type: none"> Display the total number of multicast addresses (groups) in each VLAN. 	show multicast group count [<i>vlan_id</i>]
<ul style="list-style-type: none"> 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 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

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

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

- GMRP Software Requirements, page 34-9
- Default GMRP Configuration, page 34-9
- Enabling GMRP Globally, page 34-10
- Enabling GMRP on Individual Switch Ports, page 34-10
- Disabling GMRP on Individual Switch Ports, page 34-11
- Enabling GMRP Forward-All Option, page 34-12
- Disabling GMRP Forward-All Option, page 34-12
- Configuring GMRP Registration, page 34-13
- Setting the GARP Timers, page 34-15
- Displaying GMRP Statistics, page 34-16
- Clearing GMRP Statistics, page 34-16
- Disabling GMRP on the Switch, page 34-17



Note

For an overview of GMRP operation, see the “Understanding GMRP” section on page 34-3.

GMRP Software Requirements

GMRP requires supervisor engine software release 5.2 or later.

Default GMRP Configuration

Table 34-2 shows the default GMRP configuration.

Table 34-2 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 on the switch.	set gmrp enable
Step 2	Verify the configuration.	show gmrp configuration

This example shows how to enable GMRP 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 34-10.

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_num/port_num</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 34-10.

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_num/port_num</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 GMRP Forward-All Option

When you enable the GMRP forward-all option on a port, a copy of all multicast traffic registered on the switch is forwarded to that port. Enable the forward-all option on any port connected to a router that needs to receive any multicasts (routers do not support GMRP and so 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 forward a copy of all GMRP multicast packets registered on the switch to a 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_num/port_num</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 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_num/port_num</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 34-13
- Setting Fixed Registration, page 34-13
- Setting Forbidden Registration, page 34-14

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_num/port_num</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 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_num/port_num</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_num/port_num</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 } <i>timer_value</i>
Step 2	Verify the configuration.	show garp timer

This example shows how to set 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 [<i>vlan_id</i>]

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 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

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

- Specifying Multicast Router Ports, page 34-17
- Configuring Multicast Groups, page 34-18
- Clearing Multicast Router Ports, page 34-19
- Clearing Multicast Group Entries, page 34-19

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_num/port_num</i>
Step 2	Verify the configuration.	show multicast router [<i>mod_num/port_num</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:

	Task	Command
Step 1	Add one or more multicast MAC addresses to the CAM table.	set cam {static permanent} <i>multicast_mac mod_num/port_num [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 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, perform one of these tasks in privileged mode:

Task	Command
<ul style="list-style-type: none"> Clear specific, manually configured multicast router ports. 	clear multicast router <i>mod_num/port_num</i>
<ul style="list-style-type: none"> 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.	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

Multicast routers receive all multicast data traffic unless they are configured to do otherwise. Catalyst 6000 family 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.



Note

You must enable Protocol Independent Multicast (PIM) on all routers and switches for RGMP to work. Only PIM sparse mode is currently 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 34-23.

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 34-3 provides a summary of the RGMP packet types.

Table 34-3 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.

Configuring RGMP

The following sections describe the commands for configuring RGMP on the Catalyst 6000 family switch.

Default RGMP Configuration

RGMP is disabled by default.

Enabling and Disabling RGMP



Note

To enable RGMP, you must have IGMP enabled.

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

Task	Command
• Enable RGMP.	<code>set rgmp enable</code>
• Disable RGMP.	<code>set rgmp disable</code>

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
<ul style="list-style-type: none"> Display all multicast groups that were joined by one or more RGMP-capable routers. 	show rgmp group [mac_addr] [vlan_id]
<ul style="list-style-type: none"> Display the count of multicast groups that were joined by one or more RGMP-capable routers. 	show rgmp group count [vlan_id]

This example shows how to display RGMP group information:

```
Console> (enable) show rgmp group
VlanDest MAC/Route DesRGMP Joined Router Ports
-----
101-00-5e-00-01-285/1, 5/15
101-00-5e-01-01-015/1
201-00-5e-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 and Clearing RGMP VLAN Statistics

To display and clear RGMP statistics for a given VLAN, perform these tasks in privileged mode:

Task	Command
<ul style="list-style-type: none"> Display the RGMP statistics for a specified VLAN. 	show rgmp statistics [vlan]
<ul style="list-style-type: none"> Clear RGMP statistics. 	clear rgmp statistics

This example shows how to display RGMP statistics:

```
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)
```

This example shows how to clear RGMP statistics:

```
Console> (enable) clear rgmp statistics
```

Displaying RGMP-Capable Router Ports

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

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

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

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

```
Console> (enable) show multicast router
PortVlan
-----
5/1 +1
5/14 +2
5/151
Total Number of Entries = 3
'*' - Configured
'+ ' - RGMP-capable
Console> (enable)
```

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 disabled
IGMP fastleave enabled
RGMP enabled
GMRP disabled
```

Clearing RGMP Statistics

This command clears stored RGMP statistics.

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

Task	Command
Clear RGMP statistics.	clear rgmp statistics

This example shows how to clear RGMP statistics:

```
Console> (enable) clear rgmp statistics
```

RGMP-Related CLI Commands

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

Task	Command
<ul style="list-style-type: none"> • Enable or disable RGMP. 	ip rgmp
<ul style="list-style-type: none"> • Enable or disable RGMP debugging. 	debug ip rgmp {group name or address}

