



Configuring Multicast Services

This chapter describes how to configure multicast services, including Cisco Group Management Protocol (CGMP), Internet Group Management Protocol (IGMP) snooping, Router Group Management Protocol (RGMP), and GARP Multicast Registration Protocol (GMRP) on the Catalyst enterprise LAN switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference—Catalyst 5000 Family, 4000 Family, 2926G Series, 2948G, and 2980G Switches*.

This chapter consists of these sections:

- Understanding How Multicasting Works, page 16-1
- Configuring CGMP, page 16-9
- Configuring IGMP Snooping, page 16-14
- Configuring RGMP, page 16-19
- Configuring GMRP, page 16-23
- Configuring Multicast Router Ports and Group Entries, page 16-31

Understanding How Multicasting Works

These sections describe how multicasting works on the Catalyst enterprise LAN switches:

- Multicasting and Multicast Services Overview, page 16-2
- Understanding How CGMP Works, page 16-2
- Understanding How IGMP Snooping Works, page 16-5
- Understanding How RGMP Works, page 16-7
- Understanding How GMRP Works, page 16-8

Multicasting and Multicast Services Overview

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

Switches can use CGMP, IGMP snooping, or GMRP to dynamically configure switch ports 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. RFC 2236 describes Internet Group Management Protocol, Version 2.

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

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

Understanding How CGMP Works

These sections describe CGMP:

- CGMP Overview, page 16-2
- Joining a Multicast Group, page 16-3
- Constraining Multicast Traffic, page 16-3
- Leaving a Multicast Group, page 16-3
- CGMP Leave Processing, page 16-4
- Interaction Between CGMP Leave Processing and HSRP, page 16-4

CGMP Overview

When the CGMP-capable router receives an IGMP control packet, it creates a CGMP packet that contains the request type (either join or leave), the multicast group address, and the Media Access Control (MAC) address of the host that sent the IGMP control packet. The router sends the packet to a well-known MAC address, 01-00-0c-dd-dd-dd, to which all CGMP-capable switches listen. When a CGMP-capable switch receives the packet, the supervisor engine module interprets the packet and modifies the forwarding table automatically.



Note

If a spanning tree virtual LAN (VLAN) topology changes, the CGMP-learned multicast groups on the VLAN are purged and the CGMP-capable router generates new multicast group information. We recommend that you enable the spanning tree PortFast feature on ports to which hosts are directly connected if you are using CGMP. For information on configuring spanning-tree PortFast, see Chapter 9, “Configuring Spanning-Tree PortFast, UplinkFast, and BackboneFast.”

If a CGMP-learned port link is disabled for any reason, that port is removed from any multicast group memberships.

**Note**

You cannot enable CGMP on a switch if IGMP snooping or GMRP is already enabled on that switch.

Joining a Multicast Group

When a host wants to join an IP multicast group, it sends an unsolicited IGMP join message specifying the IP multicast group it wants to join. The IGMP join also contains the Group Destination Address (GDA), the Unicast Source Address (USA), the Multicast Destination IP, and the Unicast Source IP. The router receives the IGMP join and adds the interface to the outgoing interface list (OIL) for the group. The router then builds a CGMP join using the USA of the host and the GDA contained in the join from the host and multicasts the join to the well-known CGMP multicast address to which Cisco Catalyst family switches with CGMP enabled listen.

Upon receipt of the CGMP join, each switch performs a CAM table lookup 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 CAM table, the switch creates a multicast forwarding entry for that GDA and adds the multicast router port and the port returned by the lookup. The host associated with that port receives multicast traffic for that multicast group. As the router sends group queries, the hosts respond with join messages, and a CGMP join is generated each time a join is received, keeping the multicast entries in the switch updated.

Constraining Multicast Traffic

When a host begins sending multicast traffic, this traffic hits the multicast forwarding entry for that GDA and the switch forwards the traffic only to those ports associated with that entry.

Leaving a Multicast Group

The CGMP-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 generates a CGMP join for that host. If a host does not want to remain in the multicast group, it does not respond to the router query. In IGMP version 1, this is the only way hosts can leave a multicast group. After a number of queries, if the router receives no join messages from any host in a multicast group, the router sends a CGMP leave to the switch and requests that the switch remove the multicast group from its forwarding tables.

In IGMP version 2, a host can also send an IGMP leave message for the group it wants to leave. When the CGMP-capable router receives the IGMP leave message from the host, it sends an IGMP group-specific query. Any hosts still in the group receive this query and send an IGMP join if they wish to receive traffic for this group. As long there are hosts interested in the group, the router does not generate a CGMP leave message for that GDA and all switch ports remain joined to the multicast forwarding entry for that group.

**Note**

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 (IGMP v2), or no hosts respond to the router's IGMP queries (IGMP v1). Once the last host leaves the group, the multicast router generates a CGMP leave for the GDA. When the switch receives the CGMP leave, the multicast forwarding entry for that GDA is removed from the forwarding table.

CGMP Leave Processing

When the switch is operating in CGMP mode, CGMP leave processing should be enabled to ensure minimal leave latency. CGMP leave processing allows the switch to detect IGMP version 2 leave messages sent to the all-routers multicast address (224.0.0.2) by hosts. When the supervisor engine module detects a leave message, it sends a MAC-based General Query and starts a query-response timer. If this timer expires before a CGMP join is received for the group specified in the leave message, the port is pruned from the multicast forwarding entry for the multicast group specified in the original leave message. CGMP leave processing ensures optimal bandwidth management for all hosts on a switched network, and is required when multicast receivers frequently change membership among multiple high-bandwidth groups e.g. video-on-demand channel surfing.

Interaction Between CGMP Leave Processing and HSRP

In a network topology where there are both multicast routers and also non-multicast router running HSRP, enabling CGMP leave processing on a switch can cause the following problems:

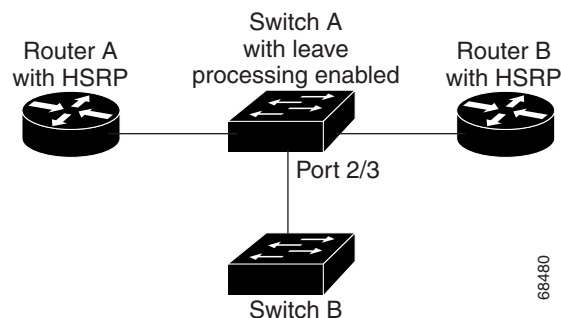
- HSRP communication between routers breaks

Because HSRP and multicast protocols both use the 224.0.0.2 Layer 3 address, HSRP hellos are captured and flooded on multicast router ports only when CGMP leave processing is enabled. As a result, non-multicast routers running HSRP will not see HSRP hello messages from other routers and HSRP communication will break down.

In the example in Figure 16-1, if Router A and Router B are running HSRP but only Router A is learned as a multicast router, Router B will never see HSRP hellos from A.

To prevent HSRP communication from breaking when CGMP leave processing is enabled, configure a static router port on the non-multicast routers using the **set multicast router** command.

Figure 16-1 Interaction between HSRP and CGMP Leave Processing



- Downstream switches flood traffic destined to the HSRP MAC address

When HSRP is running on the routers and CGMP leave processing is enabled, links to downstream switches are not learned as multicast router ports. This causes HSRP MAC entries in the CAM tables of downstream switches to age out, and host traffic destined to the HSRP MAC is flooded on all ports in the VLAN.

In the example in Figure 16-1, when HSRP routers respond (with the HSRP gateway address and MAC) to ARPs from hosts connected to Switch B, Switch B gets a CAM entry for the HSRP MAC. But after 300 seconds this entry is aged out (unless another host connected to Switch B sends out an ARP) because the HSRP hellos are intercepted by Switch A and flooded only on the multicast router ports (recall that the link to Switch B is not learned as a multicast router port). Once the entry is gone, all traffic with a Destination MAC identical to the HSRP MAC is flooded in the VLAN.

If links to downstream switches are not learned as multicast router ports, HSRP hellos are not forwarded on those links and the CAM table entries for the HSRP MAC address are not refreshed. To prevent this from happening, configure a static multicast router port on the connection to the downstream switches using the **set multicast router *mod/port*** command. In the example in Figure 16-1, this would mean that to prevent Switch B from being dropped, port 2/3 on Switch A must be configured as a static multicast router port.

Understanding How IGMP Snooping Works

These sections describe IGMP snooping:

- IGMP Snooping Overview, page 16-5
- Joining a Multicast Group, page 16-3
- Constraining Multicast Traffic, page 16-6
- Leaving a Multicast Group, page 16-6
- IGMP Fast-Leave Processing, page 16-7

IGMP Snooping Overview

IGMP snooping manages multicast traffic at Layer 2 on the Catalyst 5000 family switches by allowing directed switching of IP multicast traffic.

Switches can use IGMP snooping to configure Layer 2 interfaces dynamically so that IP multicast traffic is forwarded only to those interfaces associated with IP multicast devices.



Note

For more information on IP multicast and IGMP, refer to RFC 1112 and RFC 2236.

Catalyst 5000 series switches can distinguish IGMP control traffic from multicast data traffic. When IGMP is enabled on the switch, IGMP control traffic is redirected to the CPU for further processing. This process is performed in hardware by specialized ASICs, which allow the switch to snoop IGMP control traffic with no performance penalty.

The route processor sends out periodic general queries to all VLANs, and as multicast receivers respond to the router's queries, the switch intercepts them. Only the first IGMP join, per VLAN, per IP multicast group is forwarded to the router. Subsequent join messages 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 interested in this multicast traffic send join requests and are added to the port list of this forwarding table entry.

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



Note

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

Joining a Multicast Group

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

When a second host wants to join group 224.1.2.3, it sends out an IGMP report for this group. The switch hardware recognizes that this is an IGMP control packet and redirects it to the switch CPU. Since the switch already has a group entry for 01-00-5e-01-02-03, it just adds the second host port to the entry. Because this is not the first host joining the group, the switch suppresses the report (it is not sent to the router).

Constraining Multicast Traffic

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

The router sends IGMP general queries every 60 seconds by default. The switch floods these queries on all ports in the VLAN, and hosts that are interested in a multicast group respond with an IGMP join for each group in which they are interested.

The switch intercepts these IGMP joins, and only the first join per VLAN and per IP multicast group is forwarded on the multicast router ports. Subsequent reports for the same VLAN and group are suppressed, meaning they are not sent to the router.

**Note**

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

Leaving a Multicast Group

The designated multicast router for a segment continues forwarding the multicast traffic to that VLAN as long as at least one host in the VLAN wishes to receive multicast traffic. When hosts want to leave a multicast group, they can either ignore the periodic general queries sent by the multicast router (IGMP v1 host behavior), or they can send an IGMP leave (IGMP v2 host behavior). When the switch receives a leave message, it sends out a MAC-based general query on the port on which it received the leave message to determine if any devices connected to this port are interested in traffic for the specific multicast group. If this port is the last port in the VLAN, the switch sends a MAC-based general query to all ports in the VLAN. MAC-based general queries are addressed to the Layer 2 Group Destination Address (GDA) MAC address for which the IGMP leave message was received. At Layer 3, the MAC-based general queries are addressed to 224.0.0.1 (all hosts), and in the IGMP header, the group address field is set to 0.0.0.0.

If no IGMP report 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 non-multicast-router port in the entry, the switch suppresses the IGMP leave (it is not sent to the router). If the port is the last non-multicast-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 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 to 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).

**Note**

Only use the fast-leave processing feature if only one host is connected to each port. If fast-leave is enabled when more than one host is connected to a port, some hosts might be dropped inadvertently. Fast leave is supported only with IGMP version 2 hosts.

Understanding How RGMP Works

RGMP packets are sent with the IP header's protocol type field set to 2 (IGMP) to the reserved "All Switches" IP address 224.0.0.25 (MAC address 01-00-5e-00-00-19). RGMP-capable switches listen for, and process, RGMP packets received on this address.

Without RGMP, all multicast routers receive all multicast data traffic entering the switch. With RGMP, a multicast router can request not to receive multicast traffic if that router has no downstream receivers for the multicast traffic. Catalyst enterprise LAN 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, IGMP Snooping must be enabled on the switch. Protocol independent multicast (PIM) must be enabled 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 periodic RGMP hello messages on all RGMP-configured interfaces. The RGMP hello message tells the switch not to send multicast data to the router unless an RGMP join has also been sent to the switch from that router. When an RGMP join is sent, the router is able to receive multicast data. To learn how to set a router to receive RGMP data, see the "RGMP-Related CLI Commands" section on page 16-23.

To stop receiving multicast data on a given interface for a given group, an RGMP-capable router sends an RGMP leave message on that interface. When RGMP is disabled on the router, an RGMP bye message is sent on all RGMP-configured interfaces.

Table 16-1 provides a summary of the RGMP packet types.

Table 16-1 RGMP Message Types

Description	Action
Hello	When the RGMP feature is enabled on the router, no multicast data traffic is sent to the router by the switch unless an RGMP join is specifically sent for a group.
Bye	When RGMP feature is disabled on the router, all multicast data traffic will be sent to the router by the switch.
Join	Multicast data traffic for a multicast MAC address from the L3 group address G are sent to the router. These packets will have group G in the Group Address field of the RGMP packet.
Leave	Multicast data traffic for the group G will not be sent to the router. These packets will have group G in the group address field of the RGMP packet.

Understanding How GMRP Works

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

GMRP can register and deregister multicast group addresses at the MAC layer throughout the Layer 2-connected network. GMRP is Layer 3-protocol independent, which allows it to support the multicast traffic of any Layer 3 protocol (such as IP, IPX, and so forth).

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 generates Layer 2 GMRP versions of the host's Layer 3 IGMP control packets. The switch receives both the Layer 2 GMRP and the Layer 3 IGMP traffic from the host. The switch forwards the Layer 3 IGMP control packets to the router, and uses the received GMRP traffic to constrain multicasts at Layer 2 in the host's VLAN.

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

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

The switch sends periodic GMRP queries. If a host wants to remain in a multicast group, it responds to the query. 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 forward-all option on all ports where routers are attached.

Configuring CGMP

These sections describe how to configure CGMP:

- CGMP Hardware and Software Requirements, page 16-9
- Default CGMP Configuration, page 16-9
- Enabling CGMP, page 16-9
- Enabling CGMP Fast-Leave Processing, page 16-10
- Displaying Multicast Router Information, page 16-11
- Displaying Multicast Group Information, page 16-12
- Checking CGMP Statistics, page 16-12
- Disabling CGMP Fast-Leave Processing, page 16-13
- Disabling CGMP, page 16-13

CGMP Hardware and Software Requirements

CGMP requires these hardware and software versions:

- Supervisor engine software release 2.2 or later
- Router running CGMP

Default CGMP Configuration

Table 16-2 shows the default CGMP configuration.

Table 16-2 CGMP Default Configuration

Feature	Default Value
CGMP enable state	Disabled
Multicast routers	None configured

Enabling CGMP



Note

You cannot enable CGMP if IGMP snooping or GMRP is enabled.

To enable CGMP, perform this task in privileged mode:

	Task	Command
Step 1	Enable CGMP on the switch.	<code>set cgmp enable</code>
Step 2	Verify that CGMP is enabled.	<code>show cgmp statistics [vlan_num]</code>

This example shows how to enable CGMP and verify the configuration:

```

Console> (enable) set cgmp enable
CGMP support for IP multicast enabled.
Console> (enable) show cgmp statistics 1
CGMP enabled

CGMP statistics for vlan 1:
valid rx pkts received          211915
invalid rx pkts received        0
valid cgmp joins received       211729
valid cgmp leaves received      186
valid igmp leaves received      0
valid igmp queries received     3122
igmp gs queries transmitted     0
igmp leaves transmitted        0
failures to add GDA to EARL    0
topology notifications received 80
number of CGMP packets dropped 2032227
Console> (enable)

```

Enabling CGMP Fast-Leave Processing

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

	Task	Command
Step 1	Enable CGMP fast-leave processing on the switch.	set cgmp leave enable
Step 2	Verify that CGMP fast-leave processing is enabled.	show cgmp leave

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

```

Console> (enable) set cgmp leave enable
CGMP leave processing enabled.
Console> (enable)
Console> (enable) show cgmp leave

CGMP:          enabled
CGMP leave:    enabled
Console> (enable)

```

Displaying Multicast Router Information

When you enable CGMP, 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
<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 CGMP. 	show multicast router cgmp [<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 3/1 indicates that the entry was configured manually):

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

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

```
Console> (enable) show multicast router cgmp
CGMP enabled
IGMP disabled
```

```
Port      Vlan
-----  -
2/1      99
2/2      255
7/9      2,99
```

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

Displaying Multicast Group Information

To display information about multicast groups, perform one of 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 CGMP. 	show multicast group cgmp [<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 CGMP. 	show multicast group count cgmp [<i>vlan_id</i>]

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

```
Console> (enable) show multicast group
CGMP enabled
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)
```

Checking CGMP Statistics

To check CGMP statistics on the switch, perform this task:

Task	Command
Display CGMP statistics.	show cgmp statistics [<i>vlan_id</i>]

This example shows how to display CGMP statistics:

```

Console> (enable) show cgmp statistics
CGMP enabled

CGMP statistics for vlan 1:
valid rx pkts received          211915
invalid rx pkts received        0
valid cgmp joins received       211729
valid cgmp leaves received      186
valid igmp leaves received      0
valid igmp queries received     3122
igmp gs queries transmitted     0
igmp leaves transmitted         0
failures to add GDA to EARL    0
topology notifications received 80
number of CGMP packets dropped 2032227
Console> (enable)

```

Disabling CGMP Fast-Leave Processing

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

Task	Command
Disable CGMP fast-leave processing on the switch.	set cgmp leave disable

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

```

Console> (enable) set cgmp leave disable
CGMP leave processing disabled.
Console> (enable)

```

Disabling CGMP

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

Task	Command
Disable CGMP on the switch.	set cgmp disable

This example shows how to disable CGMP:

```

Console> (enable) set cgmp disable
CGMP support for IP multicast disabled.
Console> (enable)

```

Configuring IGMP Snooping

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

These sections describe how to configure IGMP snooping:

- IGMP Snooping Hardware and Software Requirements, page 16-14
- Default IGMP Snooping Configuration, page 16-14
- Enabling IGMP, page 16-15
- Enabling IGMP Fast-Leave Processing, page 16-15
- Displaying Multicast Router Information, page 16-16
- Displaying Multicast Group Information, page 16-17
- Displaying IGMP Statistics, page 16-18
- Disabling IGMP Fast-Leave Processing, page 16-18
- Disabling IGMP, page 16-19

IGMP Snooping Hardware and Software Requirements

IGMP snooping requires these hardware and software versions:

- Supervisor Engine II G or III G, or Supervisor Engine III or III F with a NFFC or NFFC II, or Catalyst 2926G series switch
- Supervisor engine software release 4.1 or later. Certain hardware requires a later version of software (for example, the NFFC II requires software release 4.3 or later)
- Router running IGMP

Default IGMP Snooping Configuration

Table 16-3 shows the default IGMP snooping configuration.

Table 16-3 IGMP Snooping Default Configuration

Feature	Default Value
IGMP snooping	Disabled
Multicast routers	None configured

Enabling IGMP



Note You cannot enable IGMP snooping if CGMP or 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.
CGMP is disabled.
Console> (enable) show igmp statistics
IGMP enabled
IGMP fastleave disabled

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)

```

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 one of 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
CGMP disabled
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
CGMP disabled
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 one of 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
CGMP disabled
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 check 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 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)

```

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 RGMP

The following sections describe the commands for configuring RGMP on your switch.

- Default RGMP Configuration, page 16-19
- Enabling and Disabling RGMP, page 16-20
- Displaying RGMP Group Information, page 16-20
- Displaying and Clearing RGMP VLAN Statistics, page 16-21
- Displaying RGMP-Capable Router Ports, page 16-21
- Displaying Multicast Protocol Status, page 16-22
- Clearing RGMP Statistics, page 16-22
- RGMP-Related CLI Commands, page 16-23

Default RGMP Configuration

Table 16-4 shows the RGMP default configuration.

Table 16-4 RGMP Default Configuration

Feature	Default Value
RGMP	Disabled

Enabling and Disabling RGMP



Note

To enable RGMP, you must have IGMP enabled.

To enable or disable RGMP, perform the following task in privileged mode:

Task	Command
<ul style="list-style-type: none"> Enable RGMP. 	set rgmp enable
<ul style="list-style-type: none"> Disable RGMP. 	set rgmp disable

This example shows how to enable RGMP:

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

This example shows how to disable RGMP:

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

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 [<i>mac_addr</i>] [<i>vlan_id</i>]
<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 [<i>vlan_id</i>]

This example shows how to display RGMP group information:

```
Console> 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> 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 one of these tasks in privileged mode:

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

This example shows how to display RGMP statistics:

```
Console> 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
```

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 plus in front of the router port indicates that it is an RGMP-capable router.

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

Task	Command
Display RGMP-capable router ports.	<code>show multicast router [igmp rgmp] [mod_num/port_num] [vlan_id]</code>

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

```

Console> show multicast router
PortVlan
-----
5/1 +1
5/14 +2
5/151

Total Number of Entries = 3
'*' - Configured
'+ ' - RGMP-capable

```

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 the following 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> show multicast protocols status
IGMP disabled
IGMP fastleave enabled
RGMP enabled
GMRP disabled

```

Clearing RGMP Statistics

To clear stored RGMP statistics, perform the following 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 commands are accessible from the router:

Command	Purpose
<code>ip rgmp</code>	<ul style="list-style-type: none"> • Enable or disable RGMP.
<code>debug ip rgmp {group_name group_address}</code>	<ul style="list-style-type: none"> • Enable or disable RGMP debugging.
<code>ip rgmp interface interface_unit_name</code>	<ul style="list-style-type: none"> • Display RGMP status on an interface.
<code>ip rgmp groups {group_name group_address}</code>	<ul style="list-style-type: none"> • Display groups for which RGMP has joined.

Configuring GMRP

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

- GMRP Hardware and Software Requirements, page 16-23
- Default GMRP Configuration, page 16-24
- Enabling GMRP Globally, page 16-24
- Enabling GMRP on Individual Switch Ports, page 16-25
- Disabling GMRP on Individual Switch Ports, page 16-25
- Enabling GMRP Forward-All Option, page 16-26
- Disabling GMRP Forward-All Option, page 16-26
- Configuring GMRP Registration, page 16-27
- Setting the GARP Timers, page 16-28
- Displaying GMRP Statistics, page 16-29
- Clearing GMRP Statistics, page 16-30
- Disabling GMRP on the Switch, page 16-30



Note

For an overview of GMRP operation, see the “Understanding How RGMP Works” section on page 16-7.

GMRP Hardware and Software Requirements

GMRP requires these software and hardware versions:

- Supervisor engine software release 5.1 or later
- Supervisor Engine II, IIG, III, III F, or III G

Default GMRP Configuration

Table 16-5 shows the default GMRP configuration.

Table 16-5 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 CGMP or 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 16-24.

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 16-24.

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. We recommend enabling the forward-all option on any port connected to a router. 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 Mode, page 16-27
- Setting Fixed Registration Mode, page 16-27
- Setting Forbidden Registration Mode, page 16-28

Setting Normal Registration Mode

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 configure GMRP normal registration on a port, perform this task in privileged mode:

	Task	Command
Step 1	Configure 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 configure 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 Mode

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 configure GMRP fixed registration on a port, perform this task in privileged mode:

	Task	Command
Step 1	Configure 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 configure 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 Mode

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

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

	Task	Command
Step 1	Configure 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 configure 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.)

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

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

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

```

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

```

Displaying GMRP Statistics

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

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

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

```

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

```

Clearing GMRP Statistics

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

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

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

```

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

```

Disabling GMRP 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 manually specify multicast router ports and configure multicast group entries:

- Specifying Multicast Router Ports, page 16-31
- Configuring Multicast Groups, page 16-32
- Clearing Multicast Router Ports, page 16-32
- Clearing Multicast Group Entries, page 16-33

Specifying Multicast Router Ports

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

To statically define multicast router ports, 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 define 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
CGMP enabled
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 statically configure a multicast group, 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</i> <i>mod_num/port_num</i> [<i>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 define 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
CGMP enabled
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"> Disable specific manually configured multicast router ports. 	clear multicast router <i>mod_num/port_num</i>
<ul style="list-style-type: none"> Disable 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 disable 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)
```

