



# Configuring Multicast Services

This chapter describes how to configure multicast services, including Cisco Group Management Protocol (CGMP), Internet Group Management Protocol (IGMP) snooping, 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 4000 Family, Catalyst 2948G, and Catalyst 2980G Switches*.

This chapter consists of these sections:

- [Understanding How Multicasting Works, page 15-1](#)
- [Configuring CGMP, page 15-4](#)
- [Configuring GMRP, page 15-9](#)
- [Configuring Multicast Router Ports and Group Entries, page 15-16](#)
- [Filtering IGMP Traffic, page 15-19](#)

## Understanding How Multicasting Works

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

- [Understanding Multicasting and Multicast Services Operation, page 15-1](#)
- [Joining a Multicast Group, page 15-2](#)
- [Leaving a Multicast Group, page 15-2](#)
- [Understanding GMRP Operation, page 15-3](#)

## Understanding Multicasting and Multicast Services Operation

CGMP, IGMP snooping, and GMRP manage multicast traffic in switches by allowing directed switching of IP 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.

---

CGMP and IGMP software components run on both the Cisco router and the switch. A CGMP/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 CGMP/IGMP-capable router receives an IGMP control packet, it creates a CGMP or IGMP packet that contains the request type (either join or leave), the multicast group address, and the Media Access Control (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 module interprets the packet and modifies the forwarding table automatically.

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

**Note**

---

If a spanning tree virtual LAN (VLAN) topology changes, the CGMP/IGMP-learned multicast groups on the VLAN are purged and the CGMP/IGMP-capable router generates new multicast group information.

---

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

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 8, “Configuring Spanning Tree PortFast, UplinkFast, and BackboneFast, and Loop Guard.”](#)

## 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 CGMP/IGMP-capable router then builds a CGMP/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 CGMP/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. After a number

of queries, if the router receives no reports from any host in a multicast group, the router sends a CGMP/IGMP command to the switch and requests that the switch 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 request 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.

CGMP leave-processing allows the switch to detect IGMP version 2 leave messages that were sent to the all-routers multicast address by hosts on any of the supervisor engine module ports. When the supervisor engine module receives a leave message, it starts a query-response timer. If this timer expires before a CGMP join message is received, the port is pruned from the multicast tree for the multicast group specified in the original leave message. CGMP leave processing optimizes bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously.

When CGMP fast-leave processing is enabled, the switch does not start a query response timer. The switch immediately prunes the port from the multicast tree for the multicast group by deleting the multicast MAC address from the port that received an IGMP leave message.

## Understanding GMRP Operation

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, GMRP is typically used with IGMP: 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 uses the received GMRP traffic to constrain multicasts at Layer 2 in the host's VLAN.

**Note**

In all cases, you can use CGMP or IGMP snooping to constrain multicasts at Layer 2 without the need to install or configure software on hosts.

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

When the switch receives the GMRP join message, it 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 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 15-4](#)
- [Default CGMP Configuration, page 15-4](#)
- [Enabling CGMP, page 15-5](#)
- [Enabling CGMP Leave Processing, page 15-5](#)
- [Enabling CGMP Fast-Leave Processing, page 15-6](#)
- [Displaying Multicast Router Information, page 15-6](#)
- [Displaying Multicast Group Information, page 15-7](#)
- [Displaying CGMP Statistics, page 15-8](#)
- [Disabling CGMP Leave Processing, page 15-8](#)
- [Disabling CGMP Fast-Leave Processing, page 15-8](#)
- [Disabling CGMP, page 15-9](#)

## 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 15-1](#) shows the default CGMP configuration.

**Table 15-1 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
<b>Step 1</b>	Enable CGMP on the switch.	<b>set cgmp enable</b>
<b>Step 2</b>	Verify that CGMP is enabled.	<b>show cgmp statistics [vlan_num]</b>

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 Leave Processing

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

	Task	Command
<b>Step 1</b>	Enable CGMP leave processing on the switch.	<b>set cgmp leave enable</b>
<b>Step 2</b>	Verify that CGMP leave processing is enabled.	<b>show cgmp leave</b>

This example shows how to enable CGMP 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
CGMP FastLeave: disabled
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.	<b>set cgmp fastleave enable</b>
Step 2	Verify that CGMP fast-leave processing is enabled.	<b>show cgmp leave</b>

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

```

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

CGMP:          enabled
CGMP leave:    enabled
CGMP FastLeave: 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 dynamically learned multicast router information, perform one of these tasks in privileged mode:

- Display information on dynamically learned and manually configured multicast router ports—**show multicast router** [*mod\_num/port\_num*] [*vlan\_id*]

Or:

- Display information only on those multicast router ports learned dynamically using CGMP—**show multicast router cgmp** [*mod\_num/port\_num*] [*vlan\_id*]

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

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

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"> <li>Display information about multicast groups.</li> </ul>	<b>show multicast group</b> [ <i>mac_addr</i> ] [ <i>vlan_id</i> ]
<ul style="list-style-type: none"> <li>Display only information about multicast groups learned dynamically through CGMP.</li> </ul>	<b>show multicast group cgmp</b> [ <i>mac_addr</i> ] [ <i>vlan_id</i> ]
<ul style="list-style-type: none"> <li>Display the total number of multicast addresses (groups) in each VLAN.</li> </ul>	<b>show multicast group count</b> [ <i>vlan_id</i> ]
<ul style="list-style-type: none"> <li>Display the total number of multicast addresses (groups) in each VLAN that were learned dynamically through CGMP.</li> </ul>	<b>show multicast group count cgmp</b> [ <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)

```

## Displaying CGMP Statistics

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

Task	Command
Display CGMP statistics.	<b>show cgmp statistics</b> [ <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 Leave Processing

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

Task	Command
Disable CGMP leave processing on the switch.	<b>set cgmp leave disable</b>

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

```

Console> (enable) set cgmp leave disable
CGMP leave processing disabled.
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.	<b>set cgmp fastleave disable</b>

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

```
Console> (enable) set cgmp fastleave disable
CGMP FastLeave 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.	<b>set cgmp disable</b>

This example shows how to disable CGMP:

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

## Configuring GMRP

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

- [GMRP Software Requirements, page 15-9](#)
- [Default GMRP Configuration, page 15-10](#)
- [Enabling GMRP Globally, page 15-10](#)
- [Enabling GMRP on Individual Switch Ports, page 15-11](#)
- [Disabling GMRP on Individual Switch Ports, page 15-11](#)
- [Enabling GMRP Forward-All Option, page 15-12](#)
- [Disabling GMRP Forward-All Option, page 15-12](#)
- [Configuring GMRP Registration, page 15-13](#)
- [Setting the GARP Timers, page 15-14](#)
- [Displaying GMRP Statistics, page 15-15](#)
- [Clearing GMRP Statistics, page 15-16](#)
- [Disabling GMRP on the Switch, page 15-16](#)

## GMRP Software Requirements

GMRP requires supervisor engine software release 5.1 or later.

## Default GMRP Configuration

Table 15-2 shows the default GMRP configuration.

**Table 15-2 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"> <li>Join time: 200 ms</li> <li>Leave time: 600 ms</li> <li>Leaveall time: 10,000 ms</li> </ul>

## Enabling GMRP Globally



### Note

You cannot enable GMRP if CGMP is enabled.

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

	Task	Command
Step 1	Enable GMRP on the switch.	<b>set gmrp enable</b>
Step 2	Verify the configuration.	<b>show gmrp configuration</b>

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                       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 15-10](#).

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

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

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           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 15-10](#).

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

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

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                 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.	<b>set gmrp fwdall enable <i>mod_num/port_num</i></b>

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.	<b>set gmrp fwdall disable <i>mod_num/port_num</i></b>

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 15-13](#)
- [Setting Fixed Registration Mode, page 15-13](#)
- [Setting Forbidden Registration Mode, page 15-14](#)

### 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.	<b>set gmrp registration normal</b> <i>mod_num/port_num</i>
Step 2	Verify the configuration.	<b>show gmrp configuration</b>

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.	<b>set gmrp registration fixed</b> <i>mod_num/port_num</i>
Step 2	Verify the configuration.	<b>show gmrp configuration</b>

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.	<b>set gmrp registration forbidden</b> <i>mod_num/port_num</i>
Step 2	Verify the configuration.	<b>show gmrp configuration</b>

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.	<b>set garp timer {join   leave   leaveall} timer_value</b>
Step 2	Verify the configuration.	<b>show garp timer</b>

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.	<b>show gmrp statistics [vlan_id]</b>

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> (enable)

```

## Clearing GMRP Statistics

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

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

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.	<b>set gmrp disable</b>

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 15-17](#)

- [Configuring Multicast Groups, page 15-17](#)
- [Clearing Multicast Router Ports, page 15-18](#)
- [Clearing Multicast Group Entries, page 15-18](#)

## Specifying Multicast Router Ports

When you enable CGMP 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.	<b>set multicast router</b> <i>mod_num/port_num</i>
Step 2	Verify the configuration.	<b>show multicast router</b> [ <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

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

```

## Configuring Multicast Groups

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

	Task	Command
Step 1	Add one or more multicast MAC addresses to the CAM table.	<b>set cam {static   permanent}</b> <i>multicast_mac</i> <i>mod_num/port_num</i> [ <i>vlan</i> ]
Step 2	Verify the multicast group configuration.	<b>show multicast group</b> [ <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"> <li>Disable specific manually configured multicast router ports.</li> </ul>	<b>clear multicast router</b> <i>mod_num/port_num</i>
<ul style="list-style-type: none"> <li>Disable all manually configured multicast router ports.</li> </ul>	<b>clear multicast router all</b>

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.	<b>clear cam</b> <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)

```

# Filtering IGMP Traffic

Internet Group Management Protocol (IGMP) filtering allows an administrator to configure IP multicast group profiles consisting of one or more ranges of IP multicast addresses. The administrator associates these profiles with a filtering action. These actions apply to IGMP packets, are configured on a per-switch-port basis, and are available to all VLANs associated with the physical port.

A port is set to permit or deny.

- If a port is set to permit, only matching IPs are forwarded: all others are dropped.  
If a filtering action permits a particular IGMP packet, only that packet is forwarded for processing, and all others are dropped.
- If a port is set to deny, matched IPs are dropped: all others are forwarded.  
If the filtering action causes an IGMP packet to be dropped, the switch port requesting the stream of IP multicast traffic cannot receive IP multicast traffic for that group.

**Note**

---

IGMP filtering actions do not direct IP multicast traffic forwarding. For example, IGMP filtering does not know whether CGMP or MVR is used to allow IP multicast traffic forwarding.

---

The following sections describe IGMP traffic filtering usage, requirements, and configurations.

- [Using IGMP Traffic Filtering, page 15-19](#)
- [IGMP Software Requirements, page 15-19](#)
- [Default IGMP Filter Configuration, page 15-20](#)
- [IGMP Multicast Filter Activation, page 15-20](#)
- [Configuring Port IP Multicast Filtering, page 15-21](#)

## Using IGMP Traffic Filtering

You can use IGMP filters in video service deployment of Ethernet To The Home (ETTH).

IGMP transmits video channels as IP multicast traffic using MPEG encoding. In access switches, filters specify which video channels (multicast addresses) are allowed to be received by every customer.

## IGMP Software Requirements

IGMP requires supervisor engine software release 7.1(1) or later and has the following physical restrictions for filtering through software:

- A threshold of 1024 profiles available on the Catalyst 4000
- A limit of 512 Class D multicast IP addresses which can be filtered in all profiles
- One (1) profile per port

## Default IGMP Filter Configuration

Table 15-3 shows the default IGMP traffic filter configuration.

**Table 15-3 IGMP Default Configuration**

Feature	Default Value
IGMP filtering	None
IGMP enable state	Disabled
IGMP match-action state	Deny

## IGMP Multicast Filter Activation

IGMP multicast filters are associated with each physical switch port.

The following sections show the configurations to control IGMP multicast filter activation/deactivation on the switch.

- [Enabling and Verifying IGMP Multicast Filtering, page 15-20](#)
- [Disabling and Verifying IGMP Multicast Filtering, page 15-20](#)

### Enabling and Verifying IGMP Multicast Filtering

To enable IGMP traffic filtering, perform the following in privileged mode:

	Task	Command
Step 1	Enable IGMP filtering on the switch.	<b>set igmp filter enable</b>
Step 2	Verify the configuration.	<b>show igmp filter</b>

This example shows how to enable IGMP multicast filtering on a switch.

```
Console> (enable) set igmp filter enable
igmp filter set to enable
Console> (enable)
```

This example shows how to verify the enable configuration status of IGMP multicast filtering on a switch.

```
Console> (enable) show igmp filter
igmp filter is enabled
Console> (enable)
```

### Disabling and Verifying IGMP Multicast Filtering

To disable IGMP traffic filtering, perform the following in privileged mode:

Step 1	Disable IGMP filtering on the switch.	<b>set igmp filter disable</b>
Step 2	Verify the configuration.	<b>show igmp filter</b>

This example shows how to disable IGMP multicast filtering on a switch.

```
Console> (enable) set igmp filter disable
igmp filter set to disable
Console> (enable)
```

This example shows how to verify the disable configuration status of IGMP multicast filtering on a switch.

```
Console> (enable) show igmp filter
igmp filter is disabled
Console> (enable)
```

## Configuring Port IP Multicast Filtering

IP multicast group profiles consist of one or more ranges of IP multicast addresses associated with a filtering action and are configured on a per-switch-port basis. Given a particular profile associated with a switch port, the administrator configures the filter action.

- If the filter action is to permit, the matching IGMP packet is forwarded for normal processing.
- If the filter action is to deny, the matching IGMP packet is dropped, discontinuing normal processing.

The following sections provide switch port IP multicast filtering configurations.

- [Adding and Listing an IGMP Multicast Filter Profile, page 15-21](#)
- [Permitting and Verifying an IGMP Multicast Filter Match-Action, page 15-22](#)
- [Denying and Verifying an IGMP Multicast Filter Match-Action, page 15-22](#)
- [Removing an IGMP Multicast Filter Profile, page 15-23](#)
- [Listing or Removing All IGMP Multicast Filters, page 15-23](#)
- [Assigning and Listing Port Filter Associations, page 15-24](#)
- [Removing IGMP Multicast Port Filter Associations, page 15-25](#)

### Adding and Listing an IGMP Multicast Filter Profile

To add a multicast address or a range of addresses to an IGMP multicast filter profile, perform the following in privileged mode:

	Task	Command
Step 1	Add multicast IP address or a range of IP addresses to an IGMP multicast filter profile.	<b>set igmp filter profile</b> <i>profile_id</i> <i>ip_addr</i> [- <i>ip_addr</i> ]
Step 2	List an IGMP multicast filter profile.	<b>show igmp filter profile</b> <i>profile_id</i>

This example shows how to add the multicast IP address 226.1.1.1 to IGMP multicast filter profile 1.

```
Console> (enable) set igmp filter profile 1 226.1.1.1
Successfully add ip(s) to profile
Console> (enable)
```

This example shows how to list an IP address for profile 1 when the IGMP multicast filter match-action is denied.

```
Console> (enable) show igmp filter profile 1
ProfileId 1: FilterMode deny, IP Range
-----
226.1.1.1
Console> (enable)
```

## Permitting and Verifying an IGMP Multicast Filter Match-Action

To specify an IGMP multicast filter profile on a switch to accept an IP address or a range of IP addresses, perform the following in privileged mode:

	Task	Command
Step 1	Accept an IP address or range of IP addresses.	<b>set igmp filter profile <i>profile_id</i> match-action permit</b>
Step 2	Verify the permit configuration.	<b>show igmp filter profile <i>profile_id</i> match-action</b>

This example shows how to accept an IP address or range of IP addresses.

```
Console> (enable) set igmp filter profile 1 match-action permit
igmp filter match-action set to permit
Console> (enable)
```

This example shows how to see the status of an IGMP multicast filter profile to accept IP addresses.

```
Console> (enable) show igmp filter profile 1 match-action
igmp filter match action is permit
Console> (enable)
```

## Denying and Verifying an IGMP Multicast Filter Match-Action

To specify an IGMP multicast filter profile on a switch deny an IP address or range of IP addresses, perform the following in privileged mode:

	Task	Command
Step 1	Deny an IP address or range of IP addresses.	<b>set igmp filter profile <i>profile_id</i> match-action deny</b>
Step 2	Verify the deny configuration.	<b>show igmp filter profile <i>profile_id</i> match-action</b>

This example shows how to deny an IP address or range of IP addresses.

```
Console> (enable) set igmp filter profile 1 match-action deny
igmp filter match-action set to deny
Console> (enable)
```

This example shows how to see the status of an IGMP multicast filter profile to deny IP addresses.

```
Console> (enable) show igmp filter profile 1 match-action
igmp filter match action is denied
Console> (enable)
```

## Removing an IGMP Multicast Filter Profile

To delete a multicast address from an IGMP multicast filter profile or to delete the filter profile, perform the following in privileged mode:

	Task	Command
Step 1	Remove a multicast address from an IGMP multicast filter profile or to delete the filter profile.	<b>clear igmp filter profile</b> <i>profile_id</i> [ <i>ip_addr</i> [- <i>ip_addr</i> ]  <b>all</b> ]
Step 2	List an IGMP multicast filter profile.	<b>show igmp filter profile</b> <i>profile_id</i>



### Note

When a filter is deleted, all associations between the filter and associated ports are deleted.

This example shows how to remove an IP address (226.1.1.1) from an IGMP multicast filter profile (1).

```
Console> (enable) clear igmp filter profile 1 226.1.1.1
Console> (enable)
```

This example shows how to verify that an IGMP multicast filter profile 1 was deleted.

```
Console> (enable) show igmp filter profile 1
Console> (enable)
```

## Listing or Removing All IGMP Multicast Filters

To list, delete, and verify all IGMP multicast filter profiles, perform the following in privileged mode:

	Task	Command
Step 1	List all IGMP multicast filter profiles.	<b>show igmp filter all</b>
Step 2	Remove all IGMP multicast filter profiles.	<b>clear igmp filter all</b>



### Note

When a filter is deleted, all associations between the filter and associated ports are deleted.

This example shows how to list all IGMP multicast filter profiles.

```
Console> (enable) show igmp filter all
ProfileId 1: FilterMode deny, IP Range
-----
226.1.1.1
Console> (enable)
```

This example shows how to delete all IGMP multicast filter profiles.

```
Console> (enable) clear igmp filter all
Successfully remove all the profile(s)
Console> (enable)
```

This example shows how to verify that all IGMP multicast filter profiles were deleted.

```
Console> (enable) show igmp filter all
Console> (enable)
```

## Assigning and Listing Port Filter Associations

To assign and list IGMP multicast filter associations to a port or port list, perform the following in privileged mode:

	Task	Command
Step 1	Associate IGMP multicast filters to a port or port list.	<b>set igmp filter map</b> <i>profile_id port_list</i>
Step 2	List all IGMP multicast port filter associations.	<b>show igmp filter map</b> { <i>port_list</i>   <b>all</b> }

This example shows how to set an association of module 2/port 1 to IGMP multicast filter profile 1.

```
Console> (enable) set igmp filter map 1 2/1
Console> (enable)
```

This example shows how to display the association of IGMP multicast filter profiles with module 2/port 48.

```
Console> (enable) show igmp filter map 2/48
Port      Profile
----      -
2/48      -
```

This example shows how to display the association of IGMP multicast filter profiles for all ports.

```
Console> (enable) show igmp filter map all
Port      Profile
----      -
2/1       1
2/2       -
2/3       -
2/4       -
2/5       -
2/6       -
2/7       -
2/8       -
2/9       -
2/10      -
2/11      -
2/12      -
2/13      -
2/14      -
2/15      -
2/16      -
2/17      -
2/18      -
2/19      -
2/20      -
2/21      -
2/22      -
2/23      -
2/24      -
2/25      -
2/26      -
2/27      -
2/28      -
2/29      -
2/30      -
2/31      -
```

```

2/32    -
2/33    -
2/34    -
2/35    -
2/36    -
2/37    -
2/38    -
2/39    -
2/40    -
2/41    -
2/42    -
2/43    -
2/44    -
2/45    -
2/46    -
2/47    -
2/48    -
Console> (enable)

```

## Removing IGMP Multicast Port Filter Associations

To delete the association of IGMP multicast filters with ports, perform the following in privileged mode:

	Task	Command
Step 1	Remove IGMP multicast port filter associations.	<code>clear igmp filter map { port_list   all }</code>



**Note** When the association is deleted, the filter is not deleted.

This example shows how to delete the association of IGMP multicast filter profiles with a port or list of ports.

```

Console> (enable) clear igmp filter map all
Console> (enable)

```

