

Configuring Multicast Services

This chapter describes how to configure the Cisco Group Management Protocol (CGMP) and the Internet Group Management Protocol (IGMP) snooping multicast services on the Catalyst 5000, 4000, 2948G, 2926G, and 2926 series switches.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference* for your switch.

This chapter consists of these sections:

- Understanding How Multicasting Works on page 34-1
- Configuring CGMP on page 34-3
- Configuring IGMP Snooping on page 34-8

Understanding How Multicasting Works

These sections describe how multicasting works on the Catalyst 5000, 4000, 2948G, 2926G, and 2926 series switches:

- Understanding Multicasting and CGMP/IGMP Operation on page 34-1
- Joining a Multicast Group on page 34-2
- Leaving a Multicast Group on page 34-3

Understanding Multicasting and CGMP/IGMP Operation

The Cisco Group Management Protocol (CGMP) and the Internet Group Management Protocol (IGMP) manage multicast traffic in switches by allowing directed switching of IP multicast traffic.

CGMP is supported in supervisor engine software release 2.2 or later and Cisco IOS software release 11.1(3) or later on Cisco routers.

IGMP snooping is supported in supervisor engine software release 4.1 or later and requires a Supervisor Engine III, III FSX, or III FLX with a NetFlow Feature Card (NFFC) or NFFC II. IGMP snooping is also supported on the Catalyst 2926G series switches.

Switches can use CGMP and IGMP 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, including IGMP, refer to RFC 1112.

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.”

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. If after a number of queries the router receives no reports from any host in a multicast group, the router sends a CGMP/IGMP command to the switch, telling it to remove the multicast group from its forwarding tables.

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

CGMP fast-leave-processing allows the switch to detect IGMP V.2 leave messages 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. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously.

Configuring CGMP

These sections describe how to configure CGMP:

- CGMP Configuration Guidelines on page 34-4
- Enabling CGMP on page 34-4
- Specifying Multicast Router Ports on page 34-4
- Configuring Multicast Groups on page 34-5
- Enabling CGMP Leave Processing on page 34-6
- Checking CGMP Statistics on page 34-6
- Clearing Multicast Router Ports on page 34-7
- Clearing Multicast Group Entries on page 34-7
- Disabling CGMP Leave Processing on page 34-8
- Disabling CGMP on page 34-8

CGMP Configuration Guidelines

These guidelines apply when configuring CGMP:

- CGMP requires supervisor engine software release 2.2 or later and a network connection from the switch to a router running CGMP.
- By default, CGMP is disabled, and no multicast routers are configured.
- Before you enable CGMP on the switch, you must disable IGMP snooping if it is enabled, by entering the **set igmp disable** command. If you try to enable CGMP without first disabling IGMP snooping, an error message is generated.

Enabling CGMP

To enable CGMP, perform this task in privileged mode:

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

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)

```

Specifying Multicast Router Ports

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

To statically define multicast router ports, perform this task in privileged mode:

Task	Command
Step 1 Configure multicast router ports.	set multicast router mod_num/port_num
Step 2 Verify the multicast router configuration.	show multicast router [mod_num/port_num] [vlan_id]
Step 3 Verify the multicast router information that was learned dynamically through CGMP.	show multicast router cgmp [mod_num/port_num] [vlan_id]

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)

```

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)

```

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>]
Step 3 Verify the multicast group information that was learned dynamically through CGMP.	show multicast group cgmp [<i>mac_addr</i>] [<i>vlan_id</i>]
Step 4 If desired, show the total number of multicast addresses (groups) in a VLAN.	show multicast group count [cgmp] [<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)

```

Enabling CGMP Leave Processing

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

Task	Command
Step 1 Enable CGMP leave processing on a device.	set cgmp leave enable
Step 2 Verify that CGMP leave processing is enabled.	show cgmp leave

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
Console> (enable)

```

Checking CGMP Statistics

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

Task	Command
Display CGMP statistics.	show cgmp statistics [vlan_id]

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)

```

Clearing Multicast Router Ports

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

Task	Command
• Disable specific, manually configured multicast router ports.	clear multicast router <i>mod_num/port_num</i>
• 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)

```

Disabling CGMP Leave Processing

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

Task	Command
Disable CGMP leave processing on a device.	set cgmp leave disable

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

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 Configuration Guidelines on page 34-9
- Enabling IGMP on page 34-9
- Specifying Multicast Router Ports on page 34-10
- Configuring Multicast Groups on page 34-11
- Checking IGMP Statistics on page 34-11
- Clearing Multicast Router Ports on page 34-12
- Clearing Multicast Group Entries on page 34-12
- Disabling IGMP on page 34-12

IGMP Snooping Configuration Guidelines

These guidelines apply when you are configuring IGMP snooping:

- IGMP snooping requires supervisor engine software release 4.1 or later, a Supervisor Engine III, III FSX, or III FLX with a NFFC or NFFC II, and a network connection from the switch to a router running IGMP. IGMP snooping is also supported on the Catalyst 2926G series switches.
- By default, IGMP snooping is disabled, and no multicast routers are configured.
- Before you enable IGMP snooping on the switch, you must disable CGMP if it is enabled by entering the **set cgmp disable** command. If you attempt to enable IGMP snooping without first disabling CGMP, an error message is generated.

Enabling IGMP

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

```

Specifying Multicast Router Ports

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

To statically define multicast router ports, perform this task in privileged mode:

Task	Command
Step 1 Configure multicast router ports.	set multicast router <i>mod_num/port_num</i>
Step 2 Verify the multicast router configuration.	show multicast router [<i>mod_num/port_num</i>] [<i>vlan_id</i>]
Step 3 Verify the multicast router information that was learned dynamically through IGMP.	show multicast router igmp [<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 5/7 indicates that the entry was configured manually):

```

Console> (enable) set multicast router 5/7
Port 5/7 added to multicast router port list.
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)
    
```

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} multicast_mac mod_num/port_num [vlan]
Step 2 Verify the multicast group configuration.	show multicast group [mac_addr] [vlan_id]
Step 3 Verify the multicast group information that was learned dynamically through IGMP.	show multicast group igmp [mac_addr] [vlan_id]
Step 4 If desired, show the total number of multicast addresses (groups) in a VLAN.	show multicast group count [igmp] [vlan_id]

This example shows how to define multicast groups manually and verify the configuration:

```

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 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)

```

Checking IGMP Statistics

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

Task	Command
Display IGMP snooping statistics.	show igmp statistics [vlan_id]

This example shows how to display IGMP snooping statistics:

```

Console> (enable) show igmp statistics
IGMP enabled

IGMP statistics for vlan 1:
Total valid pkts rcvd:          18951
Total invalid pkts rcvd         0
General Queries rcvd           377
Group Specific Queries rcvd     0
MAC-Based General Queries rcvd  0

```

```
Leaves recvd                14
Reports recvd               16741
Queries Xmitted             0
GS Queries Xmitted          16
Reports Xmitted             0
Leaves Xmitted              0
Failures to add GDA to EARL 0
Topology Notifications rcvd 10
IGMP packets dropped        0
Console> (enable)
```

Clearing Multicast Router Ports

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

Task	Command
• Disable specific, manually configured multicast router ports.	clear multicast router <i>mod_num/port_num</i>
• 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)
```

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)
```