

# Multicast in a Campus Network: CGMP and IGMP Snooping

Document ID: 10559

---

## **Introduction**

### **Before You Begin**

- Conventions
- Prerequisites
- Components Used
- Background Information

### **Multicast Address**

#### **Internet Group Management Protocol**

- IGMPv1
- IGMPv2
- IGMPv3
- Interoperability Between IGMPv1 and IGMPv2
- Interoperability Between IGMPv1/IGMPv2 and IGMPv3
- IGMP on a Router
- Practical Example on a Router

#### **Cisco Group Management Protocol**

- CGMP Frames and Message Types
- Learning Router Ports
- Joining a Group with CGMP
- Leaving a Group With CGMP
- CGMP and Source-Only Network
- Configuring Cisco Routers and Switches to Enable CGMP
- Practical Example of CGMP Use and Debug Command and Output

#### **IGMP Snooping**

- IGMP Snooping Overview
- Learning the Router Port
- Joining a Group With IGMP Snooping
- IGMP / CGMP Interaction
- Multicast Source-Only Network
- Limitations
- Configuration of IGMP Snooping on Cisco Switches
- Practical Example of IGMP Snooping

#### **Related Information**

---

## **Introduction**

The purpose of Cisco Group Management Protocol (CGMP) and Internet Group Management Protocol (IGMP) snooping is to restrain multicast traffic in a switched network. By default, a LAN switch floods multicast traffic within the broadcast domain, and this can consume a lot of bandwidth if many multicast servers are sending streams to the segment.

## **Before You Begin**

## Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

## Prerequisites

There are no specific prerequisites for this document.

## Components Used

This document is not restricted to specific software and hardware versions.

## Background Information

Multicast traffic becomes flooded because a switch usually learns MAC addresses by looking into the source address field of all the frames it receives. A multicast MAC address is never used as source address for a packet. Such addresses do not appear in the MAC address table, and the switch has no method for learning them.

The first solution to this issue is to configure static MAC addresses for each group and each client. This solution works well, however, it is neither scalable nor dynamic. You use this solution on a Catalyst 4000, 5000, or 6000 switch by issuing one of the following commands:

- **set cam static** *<multicast\_mac>* *<mod/port>*
- **set cam permanent** *<multicast\_mac>* *<mod/port>*

These two commands have the same effect, except that the static entries disappear at reboot, and permanent entries do not.

The second solution is to use CGMP, which is a Cisco proprietary protocol that runs between the multicast router and the switch. CGMP enables the Cisco multicast router to understand IGMP messages sent by hosts, and informs the switch about the information contained in the IGMP packet.

The last (and most efficient) solution is to use IGMP snooping. With IGMP snooping, the switch intercepts IGMP messages from the host itself and updates its MAC table accordingly. Advanced hardware is required to support IGMP snooping.

CGMP configurations given in this document are for Catalyst 4000 and 5000 switches running CatOS (CGMP is not supported on Catalyst 6000 switches), and IGMP snooping configurations are for Catalyst 5000 and 6000 switches running CatOS. For more information on configuring multicast capability on other switch platforms, refer to Multicast Catalyst Switches Support Matrix for configuration guides of specific switches.

The following section briefly describes a multicast address, explains the functionality of IGMP, and provides additional detail on CGMP and IGMP snooping.

## Multicast Address

1. Multicast IP addresses are Class D IP addresses. Therefore, all IP addresses from 224.0.0.0 to 239.255.255.255 are multicast IP addresses. They are also referred to as Group Destination Addresses (GDA).

2. For each GDA there is an associated MAC address. This MAC address is formed by 01–00–5e, followed by the last 23 bits of the GDA translated into hex, as shown below.

- ◆ 239.20.20.20 corresponds to MAC 01–00–5e–14–14–14.
- ◆ 239.10.10.10 corresponds to MAC 01–00–5e–0a–0a–0a.

Consequently, this is not a one–to–one mapping, but a one–to–many mapping. From these two addresses, you can see that the first octet (239) is not used in the MAC address. So the multicast addresses with the same last three octet but different first octet have overlapping MAC addresses.

3. Some Multicast IP addresses are reserved for special use, as shown below.

- ◆ 224.0.0.1 – All multicast–capable hosts.
- ◆ 224.0.0.2 – All multicast–capable routers.
- ◆ 224.0.0.5 and 224.0.0.6 are used by Open Shortest Path First (OSPF).

In general, addresses from 224.0.0.1 to 224.0.0.255 are reserved and used by various protocols (standard or proprietary, such as Hot Standby Router Protocol (HSRP)). Cisco recommends that you not use these for GDA in a multicast network. CGMP and IGMP snooping do not work with this reserved address range.

## Internet Group Management Protocol

IGMP is a standard defined in RFC1112 for IGMPv1, in RFC2236 for IGMPv2 and in RFC3376 for IGMPv3. IGMP specifies how a host can register with a router in order to receive specific multicast traffic. The next section gives a brief overview on IGMP.

### IGMPv1

IGMP Version 1 (IGMPv1) messages are transmitted in IP datagrams and contain the following fields:

- Version: 1
- Type: There are two types of IGMP messages, Membership Query and Membership Report.
- Checksum
- GDA

Membership reports are issued by hosts that want to receive a specific multicast group (GDA). Membership queries are issued by routers at regular intervals to check whether there is still a host interested in the GDA in that segment.

Host membership reports are issued either unsolicited (when the host wants to receive GDA traffic first) or in response to a membership query. They are sent with the following fields:

#### L2 Information

- Source MAC: Host MAC address
- Destination MAC: Destination MAC for the GDA

#### L3 Information

- Source IP: IP address of the host
- Destination IP: GDA

## IGMP Packet

- IGMP data contains, furthermore, the GDA and some other fields.

Host membership queries are sent by the router to the all-multicast address: 224.0.0.1. These queries use 0.0.0.0 in the IGMP GDA field. A host for each group must respond to that query, or the router stops forwarding the traffic for that GDA to that segment (after three attempts). The router keeps a multicast routing entry for each source, and links it to a list of outgoing interfaces (interface from where the IGMP report came). After three IGMP query attempts with no answer, this interface is erased from the outgoing interface list for all entries linked to that GDA.

**Note:** IGMPv1 has no leave mechanism. If a host no longer wants to receive the traffic, it simply quits. If it is the last host on the subnet, the router does not receive any answer to its query, and deletes the GDA for that subnet.

## IGMPv2

In IGMP Version 2 (IGMPv2), the version field has been removed, and the type field can now accept different values. The types are shown below.

- Membership Query
- IGMPv1 Membership Report
- Version 2 Membership Report
- Leave Group

Descriptions of the most important new features added in IGMPv2 are listed below.

- IGMP Leave Message: when a host wants to leave a group, it should send a Leave Group IGMP message to destination 224.0.0.2 (instead of leaving silently like in IGMPv1).
- A router can now send a group-specific query by sending a Membership Query to the group GDA instead of sending it to 0.0.0.0.

## IGMPv3

In IGMP Version 3 (IGMPv3), there is a type field that can have the following values:

- Membership query
- Version 3 Membership Report

An implementation of IGMPv3 *must* also support the following three message types, for interoperation with previous versions of IGMP:

- Version 1 Membership Report [RFC1112]
- Version 2 Membership Report [RFC2236]
- Version 2 Leave Group [RFC2236]

IGMPv3 adds support for source filtering, that is, the ability for a system to report interest in receiving packets from specific source addresses, or from **all but** specific source addresses sent to a specific multicast address. This feature is also called Source Specific Multicast (SSM).

In order for a computer to support SSM, it must support IGMPv3. Relatively few OS, however, support IGMPv3. Windows XP supports IGMPv3, and there are IGMPv3 support patches available for FreeBSD and

Linux.

Administrators must distinguish between IGMPv3 support at the router level and IGMPv3 snooping at the switch level. They are two different features.

### **Support of IGMPv3 on Catalyst Switches (L2)**

- The Catalyst 6000 running hybrid mode software (CatOS on Supervisor and Cisco IOS® Software on MSFC) officially supports IGMPv3 snooping starting in version 7.5(1).
- In versions prior to 7.5(1), the Catalyst 6000 switch did not have official support for IGMPv3, but it should normally be able to handle IGMPv3 packets.
- The Catalyst 6000 running Integrated IOS Software supports IGMPv3 at the router level (L3 interface) starting in Version 12.1(8a)E.
- The Catalyst 4000 only supports IGMPv3 at the router level on the Supervisor III and IV. It does not support IGMPv3 snooping.

### **Support of IGMPv3 on Cisco Routers (L3)**

IGMPv3 is supported on all platforms running Cisco IOS® software Release 12.1(5)T and later releases. More information can be found in IGMP Version 3 documentation. For more information on SSM with IGMPv3, IGMP v3lite, and URL Rendezvous Directory (URD), please refer to Source-Specific Multicast with IGMPv3, IGMP v3lite, and URD documentation.

### **Caveats**

When a switch is running IGMP snooping, it intercepts the IGMP packets and populates the static Layer 2 (L2) forwarding table based on the content of the intercepted packets. When there are IGMPv1 or v2 hosts on the network, the switch reads the IGMP Joins and Leaves to determine which hosts want to receive which multicast stream, or stop receiving the multicast stream.

IGMPv3 is more complicated, because it uses not only the group address (multicast address), but also the sources from which traffic is expected. Apart from the Catalyst 6000 switch running CatOS 7.5 or later and Native IOS Version 12.1(8a)E or later, no other switches are currently able to effectively snoop those packets and build a forwarding table based on this information. Therefore, IGMP snooping should be turned off when there is an IGMPv3 host on the switch. When IGMP snooping is turned off, the switch cannot dynamically build a L2 forwarding table for the multicast streams. In other words, the switch floods the multicast streams.

When IGMP snooping is disabled, one solution is to manually configure multicast dynamic Content-Addressable Memory (CAM) entries in order to avoid flooding the subnet with multicast traffic. This is an administrative burden, however, and is not a dynamic solution. When a client no longer wants to receive the traffic, the CAM entry is not removed from the switch (unless by manual intervention), so network traffic is still addressed to the host.

Also, when using IGMPv3 in the network, switches using CGMP work normally apart from the fact that CGMP Fastleave does not work. If CGMP Fastleave is needed, it is best to revert to IGMPv2.

The outstanding platform-specific caveats can be found in the release notes for the respective switches.

## **Interoperability Between IGMPv1 and IGMPv2**

With IGMPv1 and IGMPv2, only one router per IP subnet sends queries. This router is called the query router. In IGMPv1, the query router is chosen with the help of multicast routing protocol. In IGMPv2, it is

chosen by the lowest IP address among the routers. Below are several possibilities:

### **Scenario 1: IGMPv1 Router with a Mix of IGMPv1 and IGMPv2 Hosts**

The router does not understand the IGMPv2 report, and thus, all hosts must only use the IGMPv1 report.

### **Scenario 2: IGMPv2 Router with a Mix of IGMPv2 and IGMPv3 Hosts**

IGMPv1 hosts do not understand the IGMPv2 query or the IGMPv2 group membership query. The router must only use IGMPv1, and suspend the leave operation.

### **Scenario 3: IGMPv1 Router and IGMPv2 Router Located on the Same Segment**

The IGMPv1 router has no way to detect the IGMPv2 router. Therefore, the IGMPv2 router must be configured by the administrator as a IGMPv1 router. In any case, it possible that they do not agree on the query router.

## **Interoperability Between IGMPv1/IGMPv2 and IGMPv3**

With all versions of IGMP, only one router per IP subnet sends queries. This router is called the query router. In IGMPv1, the query router is chosen with the help of the multicast routing protocol. In IGMPv2 and IGMPv3, it is chosen by the lowest IP address among the routers. Below are several interoperability options.

### **Scenario 1: IGMPv1/IGMPv2 Router with a Mix of IGMPv1/IGMPv2 and IGMPv3 Hosts**

Because the router does not understand the IGMPv3 reports, all hosts use the IGMPv1/IGMPv2 reports.

### **Scenario 2: IGMPv3 Router with a Mix of IGMPv1/IGMPv2 and IGMPv3 Hosts**

The IGMPv1/IGMPv2 hosts do not understand the IGMPv3 query or IGMPv3 membership query. The router must only use the IGMP version that corresponds to the lowest IGMP client version present. If there are IGMPv3 and IGMPv2 clients, the router uses IGMPv2. If there are IGMPv1, IGMPv2, and IGMPv3 clients, the router uses IGMPv1.

### **Scenario 3: Different Version Routers on the Same Segment**

When routers of different versions are present on the same segment, the lower-version routers have no means to detect the higher-version routers. Therefore, the different routers must be configured by the administrator as the same version. This version has to match the lowest version on any querying router present.

## **IGMP on a Router**

If, by default, there is no user registered to a specific group in a subnet, the router does not forward multicast traffic for that group into that subnet. That means that a router needs to receive an IGMP report for a GDA in order to add it to the multicast routing table and to start forwarding traffic for that group.

On a router, you need to perform the following actions:

1. Enable multicast routing in the global mode, as shown below.

```
ip multicast-routing
```

2. Configure a multicast routing protocol on the involved interface, as shown below.

```
ip pim dense-mode
```

3. Monitor IGMP, as shown below.

```
show ip igmp interface
show ip igmp group
show ip mroute
```

4. Configure a router to send the IGMP report (on the interface), as shown below.

```
ip igmp join-group [GDA_ip_address]
ip igmp version [1 | 2 | 3]
```

## Practical Example on a Router

A router is configured to route between two subinterfaces, Fast-Ethernet 0.2 and Fast-Ethernet 0.3. Both interfaces are also configured to run IGMP. In the output below, you can see the IGMP version, the group joined, and so on.

### Configuration

```
ip multicast-routing

interface FastEthernet0
 no ip address
 no ip directed-broadcast
!
interface FastEthernet0.2
 encapsulation isl 2
 ip address 10.2.2.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
!
interface FastEthernet0.3
 encapsulation isl 3
 ip address 10.3.3.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
!
```

### show ip igmp interface

```
Fa0.2 is up, line protocol is up
Internet address is 10.2.2.1/24
IGMP is enabled on interface
Current IGMP version is 2
CGMP is disabled on interface
IGMP query interval is 60 seconds
IGMP querier timeout is 120 seconds
IGMP max query response time is 10 seconds
Inbound IGMP access group is not set
IGMP activity: 3 joins, 2 leaves
Multicast routing is enabled on interface
Multicast TTL threshold is 0
Multicast designated router (DR) is 10.2.2.1 (this system)
IGMP querying router is 10.2.2.1 (this system)
Multicast groups joined: 224.0.1.40

Fa0.3 is up, line protocol is up
```

```

Internet address is 10.3.3.1/24
IGMP is enabled on interface
Current IGMP version is 2
CGMP is disabled on interface
IGMP query interval is 60 seconds
IGMP querier timeout is 120 seconds
IGMP max query response time is 10 seconds
Inbound IGMP access group is not set
IGMP activity: 1 joins, 1 leaves
Multicast routing is enabled on interface
Multicast TTL threshold is 0
Multicast designated router (DR) is 10.3.3.1 (this system)
IGMP querying router is 10.3.3.1 (this system)
No multicast groups joined

```

## show ip mroute and show ip igmp group

```

Router_A#show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.10.10.10), 00:01:15/00:02:59, RP 0.0.0.0, flags: DJC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0.3, Forward/Dense, 00:01:16/00:00:00

(10.2.2.2, 239.10.10.10), 00:00:39/00:02:20, flags: CT
  Incoming interface: FastEthernet0.2, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0.3, Forward/Dense, 00:00:39/00:00:00

Router_A#show ip igmp groups
IGMP Connected Group Membership
Group Address      Interface          Uptime    Expires    Last Reporter
239.10.10.10      Fa0.3             00:02:48  00:02:04  10.3.3.2
Router_A#

```

# Cisco Group Management Protocol

For CGMP support on Catalyst switches, refer to Multicast Catalyst Switches Support Matrix.

## CGMP Frames and Message Types

CGMP was first implemented by Cisco to restrain multicast traffic in a L2 network. Because a switch is, by essence, not capable of looking at L3 packets, it cannot distinguish an IGMP packet. With CGMP, the router provides the interface between the hosts. The routers "talk" IGMP, and the switches "talk" CGMP.

CGMP frames are Ethernet frames with the destination MAC address 01-00-0c-dd-dd-dd, and with a Subnetwork Access Protocol (SNAP) header with the value 0x2001. The CGMP frames contain the following fields:

- Version: 1 or 2.
- Message Type: Join or Leave.

- Count: The number of multicast/unicast address pairs in the message.
- GDA: The 48-bit MAC address of the multicast group.
- Unicast Source Address (USA): The 48-bit MAC unicast address of the devices that wants to join the GDA.

**Note:** The value of the count field determines how many times the last two fields display.

By default, the processors of a switch (called NMP in Catalyst) only listen to multicast addresses when the **show cam system** command is issued. When you enable CGMP on a switch, the address 01-00-0c-dd-dd-dd is added to the **show cam system** command output.

The table below lists all of the possible CGMP messages.

GDA	USA	Join/Leave	Meaning
Mcast MAC	Client MAC	Join	Add port to group.
Mcast MAC	Client MAC	Leave	Delete port from group.
00-00-00-00-00-00	Router MAC	Join	Assign router port.
00-00-00-00-00-00	Router MAC	Leave	Unassign router port.
Mcast MAC	00-00-00-00-00-00	Leave	Delete group.
00-00-00-00-00-00	00-00-00-00-00-00	Leave	Delete all groups.

## Learning Router Ports

The switch needs to be aware of all router ports so that they are automatically added to any newly created multicast entries. The switch learns router ports when it receives a CGMP Join to GDA 00-00-00-00-00-00 with Router MAC USA (third type of message in the table). These messages are generated by the router on all interfaces configured to run CGMP. There is also a static method, however, for configuring router ports on the switch.

## Joining a Group with CGMP

- A new client requests to receive traffic for a GDA, so the client sends an IGMP Membership report message.
- The router receives the IGMP report, processes it, and sends a CGMP message to the switch. The router copies the destination MAC address into the GDA field of the CGMP Join, and copies the source MAC address into the USA of the CGMP join. It then sends it back to the switch.
- A switch with CGMP enabled needs to listen to the CGMP 01-00-0c-dd-dd-dd addresses. The

processor of the switch looks into the CAM table for the USA. Once the USA is seen in the CAM table, the switch knows which port the USA is located on, and does one of the following:

- ◆ Creates a new static entry for the GDA and links the USA port to it along with all router ports.
- ◆ Adds the USA port to the list of the ports for this GDA (if the static entry already exists).

## Leaving a Group With CGMP

Static entries learned with CGMP are permanent, unless a spanning tree topology change occurs in the VLAN, or the router sends one of the last CGMP Leave messages in the previous table.

When IGMPv1 is the host, do not send IGMP Leave messages. The router only sends Leave messages if it does not receive a reply to three consecutive IGMP queries. This means that no port is deleted from a group if any users are still interested in that group.

With the introduction of IGMPv2 and the presence of IGMP Leave, Cisco added to the original CGMP specification (CGMPv2). This addition is called CGMP Fast–Leave.

CGMP Fast–Leave processing allows the switch to detect IGMPv2 Leave messages sent to the all–router multicast address (224.0.0.2) 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 and sends a message on the port on which that leave was received to determine if there is still a host willing to receive this multicast group on that port. 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. If it is the last port in the multicast group, it forwards the IGMP Leave message to all router ports. The router then starts the normal deletion process by sending a group–specific query. Because no responses are received, the router removes this group from the multicast routing table for that interface. It also sends a CGMP Leave message to the switch that erases the group from the static table. Fast–Leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously.

When CGMP Leave is enabled, two entries are added to the **show cam system** command output, as shown below.

```
01-00-5e-00-00-01
01-00-5e-00-00-02
```

IGMP Leave uses 224.0.0.2 and IGMP Query uses 224.0.0.1.

Use the following steps to troubleshoot CGMP:

1. Due to a conflict with the HSRP, CGMP Leave processing is disabled by default. HSRP uses MAC address 01–00–5e–00–00–02, which is the same as IGMP Leave with IGMP Version 2. With CGMP Fast–Leave, all HSRP packets go to the switch CPU. Because an HSRP message is not an IGMP packet, the switch regenerates all such messages and sends them to all router ports. Routers receiving `hsrp hello` or `hsrp peers` lose connectivity. Therefore, in debugging HSRP problems, try disabling CGMP Fast–Leave.

To enable CGMP Leave processing, issue the **set cgmp leave enable** command.

2. When CGMP Leave processing is enabled, the Catalyst 5000 family switch learns router ports through PIM–v1, HSRP, and CGMP Self–Join messages. When CGMP Leave processing is disabled, the Catalyst 5000 family switch learns router ports through CGMP Self–Join messages only.

3. CGMP does not prune multicast traffic for any IP multicast address that maps into the MAC address range of 01-00-5E-00-00-00 to 01-00-5E-00-00-FF. The reserved IP multicast addresses, in the range 224.0.0.0 to 224.0.0.255, are used to forward local IP multicast traffic in a single L3 hop.

## CGMP and Source-Only Network

A source-only network is a segment with only a source multicast and no real client. Therefore, there is a chance that no IGMP reports are generated in that segment. CGMP still needs to restrict the flooding of this source (for router use only) however. If a router detects multicast traffic on one interface with no IGMP report, it is identified as a multicast source-only network. The router generates a CGMP Join message for itself, and the switch simply adds this group (with only the router port).

## Configuring Cisco Routers and Switches to Enable CGMP

The commands below are only valid for Catalyst 4000 and 5000 series (plus 2901, 2902, 2926, 2948G, and 4912).

- Multicast Router

Enable IP multicasting (global command):

- ◆ **ip multicast-routing**

Enable each interface running CGMP (interface mode) with the following commands:

- ◆ **ip pim <sparse-mode/dense-mode>**

- ◆ **ip igmp**

- ◆ **ip cgmp**

Debug the L2 multicast problem with the following commands:

- ◆ **debug ip igmp**

- ◆ **debug ip cgmp**

- Catalyst 4000 or 5000 series

Enable/disable CGMP with the following commands:

- ◆ **set cgmp <enable/disable>**

Enable/disable CGMP Fast-Leave with the following commands:

- ◆ **set cgmp leave <enable/disable>**

Configure the multicast router (static) with the following commands:

- ◆ **set multicast router <slot /port>**

Clear the multicast router with the following commands:

- ◆ **clear multicast router <slot/port>**

Listed below are various commands to verify the CGMP operation.

- ◆ **show cam static**

- ◆ **show cgmp statistic <VLAN\_id>**

- ◆ **show cgmp leave**

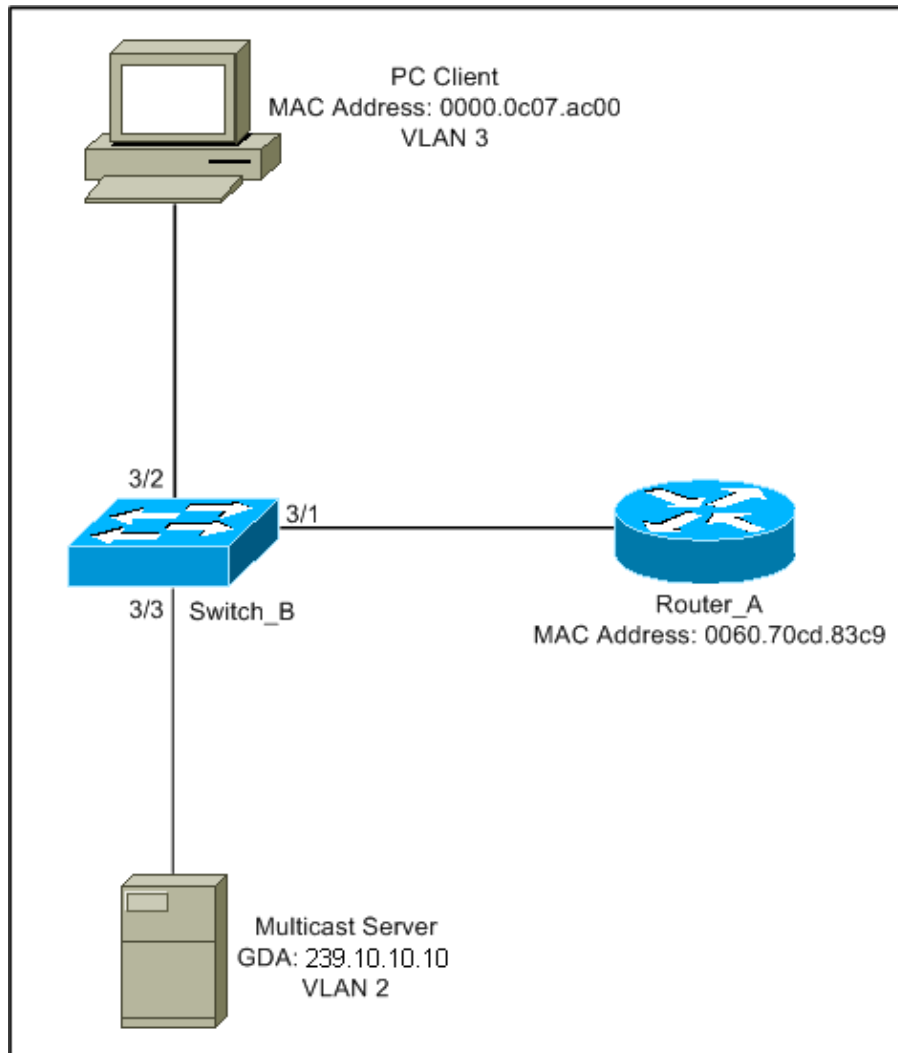
- ◆ **show multicast router**

- ◆ **show multicast group**

- ◆ show multicast group cgmp
- ◆ show multicast group count

## Practical Example of CGMP Use and Debug Command and Output

This is a practical configuration example for a Cisco router and Catalyst switches.



This configuration shows the operations involved as a host joins a group. This configuration also shows the operations as a host leaves a group with Fast-Leave enabled. Sniffer traces and the configuration of the switch and the router are also provided.

### Joining a Group with CGMP

Refer to these steps when joining a group with CGMP.

1. Enable CGMP on the switch, as shown below.

```
Switch_B (enable) set cgmp en
MCAST-CGMP: Set CGMP Sys Entrie
MCAST-CGMP: Set CGMP Sys Entrie
MCAST-CGMP: Set CGMP Sys Entrie
CGMP support for IP multicast enabled.
```

```
Switch_B (enable)
```

As you can see below, the entry 01-00-0c-dd-dd-dd is included for all VLANs in the **show cam system** command output. In addition, as the network is running CGMP Fast-Leave, you can see the entries for 01-00-5e-00-00-01 and 01-00-5e-00-00-02.

```
Switch_B (enable) show cgmp leave
```

```
CGMP:          enabled
```

```
CGMP leave:    enabled
```

```
Switch_B (enable) show cam system
```

```
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
```

```
X = Port Security Entry
```

VLAN	Dest MAC/Route Des	[CoS]	Destination Ports or VCs / [Protocol Type]
1	00-10-2f-00-14-00 #		7/1
1	00-e0-fe-4b-f3-ff #		1/9
1	01-00-0c-cc-cc-cc #		1/9
1	01-00-0c-cc-cc-cd #		1/9
1	01-00-0c-dd-dd-dd #		1/9
1	01-00-0c-ee-ee-ee #		1/9
1	01-80-c2-00-00-00 #		1/9
1	01-80-c2-00-00-01 #		1/9
2	00-10-2f-00-14-00 #		7/1
2	01-00-0c-cc-cc-cc #		1/9
2	01-00-0c-cc-cc-cd #		1/9
2	01-00-0c-dd-dd-dd #		1/9
2	01-80-c2-00-00-00 #		1/9
2	01-80-c2-00-00-01 #		1/9
3	01-00-0c-cc-cc-cc #		1/9
3	01-00-0c-cc-cc-cd #		1/9
3	01-00-0c-dd-dd-dd #		1/9
3	01-80-c2-00-00-00 #		1/9
3	01-80-c2-00-00-01 #		1/9

Total Matching CAM Entries Displayed = 19

- The router sends a CGMP Join message to GDA 00-00-00-00-00-00 with the USA MAC of the router. Therefore, the router port is added to the router port list (see the first example below).

### On the router

```
6d01h: CGMP: Sending self Join on Fa0.3
```

```
6d01h:      GDA 0000.0000.0000, USA 0060.70cd.83c9
```

### On the switch

```
MCAST-CGMP-JOIN: recvd CGMP JOIN msg on port 3/1 vlanNo 2
```

```
MCAST-CGMP-JOIN: join GDA 00-00-00-00-00-00 MCAST-CGMP-JOIN:USA 00-60-70-cd-83-c9
```

```
MCAST-ROUTER: Adding QUERIER port 3/1, vlanNo 2
```

```
MCAST-ROUTER: Creating RouterPortTimer for port 3/1, vlanNo 2
```

```
Switch_B (enable) show multi router
```

```
CGMP enabled
```

```
IGMP disabled
```

Port	Vlan
3/1	2-3

```
Total Number of Entries = 1
*' - Configured
```

3. The PC on 3/1 sends IGMP a report containing the GDA: 239.10.10.10 (see frame 2 below). Shown below is the **show ip igmp group** command output on the router Router\_A.

This shows that the router now forwards traffic for 224.10.10.10 to fa0.3 . This is a consequence of the reception of the IGMP report from 10.3.3.2, which is the client PC.

```
Router_A#show ip igmp groups
IGMP Connected Group Membership
Group Address      Interface      Uptime    Expires    Last Reporter
239.10.10.10      Fa0.3         00:02:48  00:02:04  10.3.3.2
Router_A#
```

4. The router receives the report and sends a CGMP Join message along with the following information:

- ◆ Source MAC: MAC address of router
- ◆ Dest MAC: 01-00-cc-dd-dd-dd
- ◆ Contents: MAC address of the client PC (USA): 00-00-0c-07-ac-00 MAC address of the multicast group: 01-00-5e-0a-0a-0a (see frame 3 below)

#### On the router

```
6d01h: IGMP: Received v2 Report from 10.3.3.2 (Fa0.3) for 239.10.10.10
6d01h: CGMP: Received IGMP Report on Fa0.3
6d01h:      from 10.3.3.2 for 239.10.10.10
6d01h: CGMP: Sending Join on Fa0.3
```

5. The switch with 01-00-cc-dd-dd-dd in the **show cam system** command output has CGMP enabled. The switch is able to process the packet.

The switch makes a lookup in the dynamic CAM table to determine on which port the MAC address of the client PC is located. The address is located on port 3/2, and the switch makes a static entry in the CAM table for 01-00-5e-0a-0a-0a bounded to port 3/2. The switch also adds the router port 3/1 to the static entry for that GDA.

#### On the switch

```
MCAST-CGMP-JOIN: recvd CGMP JOIN msg on port 3/1 vlanNo 3
MCAST-CGMP-JOIN: join GDA 01-00-5e-0a-0a-0a MCAST-CGMP-JOIN:USA 00-60-5c-f4-bd-e2
MCAST-CGMP-JOIN: 3/2/3: index 81
MCAST-CGMP-JOIN: recvd CGMP JOIN msg on port 3/1 vlanNo 2
MCAST-CGMP-JOIN: join GDA 01-00-5e-00-01-28 MCAST-CGMP-JOIN:USA 00-60-70-cd-83-c9
MCAST-CGMP-JOIN: 3/1/2: index 80
```

6. All subsequent traffic for multicast group 239.10.10.10 are forwarded only to this port in this VLAN. Below is the static entry in the Catalyst switch where 3/1 is the router port and 3/2 is the client port.

```
Switch_B (enable) show cam static
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des      [CoS]  Destination Ports or VCs / [Protocol Type]
----  -
3      01-00-5e-0a-0a-0a         ----- 3/1-2
Total Matching CAM Entries Displayed = 3
Switch_B (enable)
```

## Leaving a Group With CGMP Fast-Leave Enabled

The example below requires that the client is an IGMP Version 2 client and that Fast-Leave is enabled on the switch.

1. The following procedure enables CGMP Fast-Leave. Look at the **show cgmp leave** command output to determine if it is enabled. Also, look at the **show cam system** command output to determine if the switch is listening to 01-00-5e-00-00-01 and 01-00-5e-00-00-02 (addresses used for the leave).

```
Switch_B (enable) show cgmp leave

CGMP:          enabled
CGMP leave:    enabled
Switch_B (enable) show cam sys
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des  [CoS]  Destination Ports or VCs / [Protocol Type]
----  -
1      00-10-2f-00-14-00 #      7/1
1      00-e0-fe-4b-f3-ff #      1/9
1      01-00-0c-cc-cc-cc #      1/9
1      01-00-0c-cc-cc-cd #      1/9
1      01-00-0c-dd-dd-dd #      1/9
1      01-00-0c-ee-ee-ee #      1/9
1      01-80-c2-00-00-00 #      1/9
1      01-80-c2-00-00-01 #      1/9
2      00-10-2f-00-14-00 #      7/1
2      01-00-0c-cc-cc-cc #      1/9
2      01-00-0c-cc-cc-cd #      1/9
2      01-00-0c-dd-dd-dd #      1/9
2      01-00-5e-00-00-01 #      1/9
2      01-00-5e-00-00-02 #      1/9
2      01-80-c2-00-00-00 #      1/9
2      01-80-c2-00-00-01 #      1/9
3      01-00-0c-cc-cc-cc #      1/9
3      01-00-0c-cc-cc-cd #      1/9
3      01-00-0c-dd-dd-dd #      1/9
3      01-00-5e-00-00-01 #      1/9
3      01-00-5e-00-00-02 #      1/9
3      01-80-c2-00-00-00 #      1/9
Do you wish to continue y/n [n]? y
Total Matching CAM Entries Displayed = 22
```

2. The client sends a IMPG Leave message to 224.0.0.2. The switch intercepts it and sends an IGMP Query on the port on which he receives the leave. The following is **debug** output on the switch:

```
MCAST-IGMP-LEAVE:Recvd leave on port 3/2 vlanNo 3
MCAST-IGMP-LEAVE:router_port_tbl[vlanNo].QueryTime = 0
MCAST-IGMP-LEAVE:deletion_timer = 1
MCAST-SEND:Transmitting IGMP Mac Based GS Query msg on port 3/2 vlanNo 3
MCAST-SEND: Transmit Succeeded for IGMP Group Specific Query msg on port 3/2 vlanNo 3
```

3. Because no response was received, the Catalyst forwards the IGMP Leave message to the router, as shown below.

```
MCAST-TIMER:IGMPLeaveTimer expired on port 3/2 vlanNo 3 GDA 01-00-5e-0a-0a-0a
MCAST-TIMER:IGMPLeaveTimer expiry: Transmit IGMP Leave on port 3/1 vlanNo 3
MCAST-SEND:Transmitting IGMP Leave msg on port 3/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP Leave Message on port 3/1 vlanNo 3
```

4. The router receives an IGMP Leave message, so it sends a CGMP Leave message to the switch and also deletes the group from its IGMP group list. Below is the **debug** command output on the router.

### On the router

```
IGMP: Received Leave from 10.200.8.108 (Fa0.3) for 239.10.10.10
IGMP: Send v2 Query on Fa0.3 to 239.10.10.10
IGMP: Send v2 Query on Fa0.3 to 239.10.10.10
CGMP: Sending Leave on Fa0.3
      GDA 0100.5e0a.0a0a, USA 0000.0000.0000
IGMP: Deleting 239.10.10.10 on Fa0.3
```

## CGMP Traces and Configuration

### Frame 1

Frame 1 is a CGMP Join frame to GDA 00-00-00-00-00-00. It is used to add the router port to the router port list.

```
ISL: ----- ISL Protocol Packet -----
ISL:
ISL: Destination Address           = 01000C0000
ISL: Type                         = 0 (Ethernet)
ISL: User                         = 0 (Normal)
ISL: Source Address               = 8C958B7B1000
ISL: Length                       = 76
ISL: Constant value              = 0xAAAA03
ISL: Vendor ID                   = 0x8C958B
ISL: Virtual LAN ID (VLAN)       = 2
ISL: Bridge Protocol Data Unit (BPDU) = 0
ISL: Port Index                  = 193
ISL: Reserved
ISL:
ETHER: ----- Ethernet Header -----
ETHER:
ETHER: Destination = Multicast 0100CDDDDDD

!--- Send to the CGMP
!--- macaddress present in show cam sys
!--- command output.

ETHER: Source           = Station Ciscoll411E1
ETHER: 802.3 length = 24
ETHER:
LLC: ----- LLC Header -----
LLC:
LLC: DSAP Address = AA, DSAP IG Bit = 00 (Individual Address)
LLC: SSAP Address = AA, SSAP CR Bit = 00 (Command)
LLC: Unnumbered frame: UI
LLC:
SNAP: ----- SNAP Header -----
SNAP:
SNAP: Vendor ID = Ciscol
SNAP: Type = 2001 (CGMP)
SNAP:
CGMP: ----- CGMP -----
CGMP:
CGMP: Version   = 16
CGMP: Type      = 0 (Join)
```

```

CGMP: Reserved
CGMP: Count      = 1
CGMP:
CGMP: Group Destination Address and Unicast Source Address
CGMP:
CGMP:   GDA      =0000.0000.0000
CGMP:   USA      =0000.0C14.11E1

```

*!--- MAC address of the router.*

```
CGMP:
```

The frame 1 result is on the switch, with 3/1 being the port that is connected to the router:

## Frame 2

Frame 2 is an IGMP membership report sent by the host to request (or confirm) that users want to receive traffic for group 239.10.10.10.

```

ISL: ----- ISL Protocol Packet -----
ISL:
ISL: Destination Address          = 01000C0000
ISL: Type                        = 0 (Ethernet)
ISL: User                        = 0 (Normal)
ISL: Source Address              = 8C958B7B1000
ISL: Length                      = 76
ISL: Constant value              = 0xAAAA03
ISL: Vendor ID                   = 0x8C958B
ISL: Virtual LAN ID (VLAN)       = 2
ISL: Bridge Protocol Data Unit (BPDU) = 0
ISL: Port Index                  = 195
ISL: Reserved
ISL:

```

```

ETHER: ----- Ethernet Header -----
ETHER:
ETHER: Destination = Multicast 01005E0A0A0A

```

*!--- Destination is the GDA MAC.*

```
ETHER: Source      = Station Cisco176DCCA
```

*!--- Sourced by the PC connected in 3/1.*

```

ETHER: Ethertype = 0800 (IP)
ETHER:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = C0
IP:   110. .... = internetwork control
IP:   ...0 .... = normal delay
IP:   .... 0... = normal throughput
IP:   .... .0.. = normal reliability
IP: Total length = 28 bytes
IP: Identification = 0
IP: Flags          = 0X
IP:   .0.. .... = may fragment
IP:   ..0. .... = last fragment
IP: Fragment offset = 0 bytes

```

```

IP: Time to live      = 1 seconds/hops
IP: Protocol         = 2 (IGMP)
IP: Header checksum  = CC09 (correct)
IP: Source address   = [10.1.1.2]
IP: Destination address = [224.10.10.10]
IP: No options
IP:
IGMP: ----- IGMP header -----
IGMP:
IGMP: Version        = 1
IGMP: Type           = 6 (Ver2 Membership Report)
IGMP: Unused         = 0x00
IGMP: Checksum       = FFEA (correct)
IGMP: Group Address  = [224.10.10.10]
IGMP:

```

### Frame 3

Frame 3 is the CGMP frame sent by the router to the switch to tell the switch to add a static entry for 01-00-5e-0a-0a-0a.

```

ISL: ----- ISL Protocol Packet -----
ISL:
ISL: Destination Address      = 01000C0000
ISL: Type                    = 0 (Ethernet)
ISL: User                    = 0 (Normal)
ISL: Source Address          = 8C958B7B1000
ISL: Length                  = 76
ISL: Constant value         = 0xAAAA03
ISL: Vendor ID               = 0x8C958B
ISL: Virtual LAN ID (VLAN)   = 2
ISL: Bridge Protocol Data Unit (BPDU) = 0
ISL: Port Index              = 193
ISL: Reserved
ISL:
ETHER: ----- Ethernet Header -----
ETHER:
ETHER: Destination = Multicast 01000CDDDDDD
ETHER: Source      = Station Cisco11411E1
ETHER: 802.3 length = 24
ETHER:
LLC: ----- LLC Header -----
LLC:
LLC: DSAP Address = AA, DSAP IG Bit = 00 (Individual Address)
LLC: SSAP Address = AA, SSAP CR Bit = 00 (Command)
LLC: Unnumbered frame: UI
LLC:
SNAP: ----- SNAP Header -----
SNAP:
SNAP: Vendor ID = Cisc01
SNAP: Type = 2001 (CGMP)
SNAP:
CGMP: ----- CGMP -----
CGMP:
CGMP: Version      = 16
CGMP: Type         = 0 (Join)
CGMP: Reserved
CGMP: Count        = 1
CGMP:
CGMP: Group Destination Address and Unicast Source Address
CGMP:
CGMP: GDA          =0100.5E0A.0A0A

```

```
!--- GDA MAC added in show cam static
!--- command output.
```

```
CGMP:    USA    =0000.0C76.DCCA
```

```
!--- MAC of the PC in 3/1.
```

```
CGMP:
```

Below is the configuration of the router and the switch.

```
Router_A (router) Configuration:
```

```
Router_A#write terminal
Building configuration...
```

```
Current configuration:
```

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router_A
!
!
ip subnet-zero
ip multicast-routing
ip dvmrp route-limit 20000

interface FastEthernet0
 no ip address
 no ip directed-broadcast
!
interface FastEthernet0.1
 encapsulation isl 1
 ip address 10.1.1.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
!
interface FastEthernet0.2
 encapsulation isl 2
 ip address 10.2.2.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
 ip cgmp
!
interface FastEthernet0.3
 encapsulation isl 3
 ip address 10.3.3.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
 ip cgmp
!
```

```
Switch_B configuration for CGMP:
```

```

#cgmp
set cgmp enable
set cgmp leave enable
!

CGMP statistics for VLAN 3:

Switch_B (enable) show cgmp sta 3
CGMP enabled

CGMP statistics for vlan 3:
valid rx pkts received          109
invalid rx pkts received        0
valid cgmp joins received       108
valid cgmp leaves received      1
valid igmp leaves received      1
valid igmp queries received     63
igmp gs queries transmitted     1
igmp leaves transmitted         1
failures to add GDA to EARL     0
topology notifications received 0
Switch_B (enable)

```

## IGMP Snooping

IGMP snooping is another feature that allows you to directly capture IGMP frames. For IGMP snooping support on Catalyst switches, refer to Multicast Catalyst Switches Support Matrix.

### IGMP Snooping Overview

IGMP snooping, as implied by the name, is a feature that allows the switch to "listen in" on the IGMP conversation between hosts and routers. When a switch hears an IGMP report from a host for a given multicast group, the switch adds the host's port number to the GDA list for that group. And, when the switch hears an IGMP Leave, it removes the host's port from the CAM table entry.

### Learning the Router Port

The switch listens to the following messages in order to detect router ports with IGMP snooping:

- IGMP Membership query send to 01-00-5e-00-00-01
- PIMv1 hello send to 01-00-5e-00-00-02
- PIMv2 hello send to 01-00-5e-00-00-0d
- DVMRP probes send to 01-00-5e-00-04
- MOSPF message send to 01-00-5e-00-05 or 06

By enabling IGMP snooping on a switch, all the above MAC entries are added to the **show cam system** command output of the snooping switch. Once a router port is detected, it is added to the port list of all GDAs in that VLAN.

### Joining a Group With IGMP Snooping

The following are two joining scenarios:

Scenario A: Host A is the first host to join a group in the segment.

1. Host A sends an unsolicited IGMP Membership report.
2. The switch intercepts the IGMP Membership report that was sent by the host that wanted to join the group.
3. The switch creates a multicast entry for that group and links it to the port on which it has received the report and to all router ports.
4. The switch forwards the IGMP report to all router ports. This is so the router also receives the IGMP report, and updates its multicast routing table accordingly.

Scenario B: Host B now is the second host to join the same group.

1. Host B sends an unsolicited IGMP Membership report.
2. The switch intercepts the IGMP Membership report sent by the host that wants to join the group.
3. The switch does not necessarily forward the IGMP report to all router ports. Actually, the switch forwards IGMP reports to router ports using proxy reporting, and only forwards one report per group within 10s.

**Note:** In order to maintain group membership, the multicast router sends a IGMP query every 60 seconds. This query is intercepted by the switch, and forwarded to all ports on the switch. All hosts that are members of the group answer that query. But, given the fact that the switch intercepts the reply report as well, the other host does not see each of the other reports, and thus, all hosts send a report (instead of one per group). The switch then uses Proxy Reporting as well, to forward only one report per group among all received responses.

Assume Host A wants to leave the group, but Host B still wants to receive the group.

- The switch captures the IGMP Leave message from Host A.
- The switch issues a group-specific IGMP Query for the group on that port (and only on that port).
- If the switch does not receive a report, it discards this port from the entry. If it receives a response from that port, it does nothing and discards the leave.
- Host B is still interested by that group on that switch. This would not be the last non-router port in the entry. Therefore, the switch does not forward the Leave message.

Now, assume Host B wants to leave the group and Host B is the last user interested by this group in this segment.

- The switch captures the IGMP Leave message from Host A.
- The switch issues a group-specific IGMP Query for that group on that port.
- If the switch does not receives a report, it discards this port from the entry.
- This is the last non-router port for that GDA. The switch forwards the IGMP Leave message to all router ports and removes the entry from its table.

## IGMP / CGMP Interaction

In some networks, due to hardware limitations, you might not be able to run IGMP snooping on all switches. In this case, you might need to run CGMP on some switches in the same network.

Note that this is a special case. The switch running IGMP snooping detects CGMP messages and detects that some switches in the network are running CGMP. Therefore, it moves to a special IGMP-CGMP mode and disables the proxy reporting. This is absolutely necessary for the proper operation of CGMP, because routers use the source MAC address of the IGMP report in order to create a CGMP Join. Routers running CGMP need to see all IGMP reports, so proxy reporting must be disabled. Any reports sent to the router should only be those strictly needed for IGMP snooping.

## Multicast Source–Only Network

If the segment contains only one multicast server (multicast source) and no client, you might end up with a situation where you do not have any IGMP packets in that segment, but you do have a lot of multicast traffic. In this case, the switch simply forwards the traffic from that group to everybody in the segment. Fortunately, a switch running IGMP snooping is able to detect these multicast streams and adds a multicast entry for that group with only the router port. These entries are flagged internally as `mcast_source_only` and are aged out each 5 minutes, or when the router port goes away. Note that even after this aging, the address is relearned within a few seconds if the traffic continues.

## Limitations

As with CGMP, GDAs that map to a MAC that falls in the range `01-00-5e-00-00-xx` is never pruned by IGMP snooping.

## Configuration of IGMP Snooping on Cisco Switches

To enable/disable IGMP snooping, issue the following command:

- **set igmp** *<enable/disable>*

To configure the multicast router (static), issue the following command:

- **set multicast router** *<mod/port>*
- **clear multicast router** *<mod |port | all>*

To monitor and check IGMP statistics, issue the following commands:

- **show igmp statistics** *<VLAN\_id>*
- **show multicast router**

## Practical Example of IGMP Snooping

The setup for this example is similar to that CGMP testing, used earlier in this document. The only difference is that port 3/2 and 3/3 are both connected to the same VLAN and are both client–configured to join group 224.10.10.10.

The following example explains several manipulations, looks at what the switch does, and examines the resulting output. In the following example, *Switch\_B* is a Catalyst 5500 running IGMP snooping, and *Router\_A* is the multicast router connected to port 3/1.

1. Enable IGMP snooping on the switch and see the result by issuing the **debug** command. Notice that each set of entries has been added to the **show cam sys** command output, allowing for the detection of the router port through PIM, MOSPF, and so on.

```
Switch_B (enable) set igmp en

MCAST-IGMP: Set Sys Entries
MCAST-SYS-ENTRIES: Add system Entries in vlan 1
MCAST-IGMP: Set Sys Entries
MCAST-SYS-ENTRIES: Add system Entries in vlan 2
MCAST-IGMP: Set Sys Entries
MCAST-SYS-ENTRIES: Add system Entries in vlan 3
```

IGMP feature for IP multicast enabled

Switch\_B (enable) show cam sys

\* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.  
X = Port Security Entry

VLAN	Dest MAC/Route Des	[CoS]	Destination Ports or VCs / [Protocol Type]
1	00-10-2f-00-14-00 #		7/1
1	00-e0-fe-4b-f3-ff #		1/9
1	01-00-0c-cc-cc-cc #		1/9
1	01-00-0c-cc-cc-cd #		1/9
1	01-00-0c-dd-dd-dd #		1/9
1	01-00-0c-ee-ee-ee #		1/9
1	01-00-5e-00-00-01 #		1/9
1	01-00-5e-00-00-04 #		1/9
1	01-00-5e-00-00-05 #		1/9
1	01-00-5e-00-00-06 #		1/9
1	01-00-5e-00-00-0d #		1/9
1	01-80-c2-00-00-00 #		1/9
1	01-80-c2-00-00-01 #		1/9
2	00-10-2f-00-14-00 #		7/1
2	01-00-0c-cc-cc-cc #		1/9
2	01-00-0c-cc-cc-cd #		1/9
2	01-00-0c-dd-dd-dd #		1/9
2	01-00-5e-00-00-01 #		1/9
2	01-00-5e-00-00-04 #		1/9
2	01-00-5e-00-00-05 #		1/9
2	01-00-5e-00-00-06 #		1/9
2	01-00-5e-00-00-0d #		1/9

2. The switch receives a PIMv2 packet from router Router\_A and adds the router port.

```
MCAST-IGMPQ:recvd a PIM V2 packet of type HELLO on the port 3/1 vlanNo 2
MCAST-ROUTER: Adding port 3/1, vlanNo 2
MCAST-ROUTER: Creating RouterPortTimer for port 3/1, vlanNo 2
MCAST-IGMPQ:recvd a PIM V2 packet of type HELLO on the port 3/1 vlanNo 3
MCAST-ROUTER: Adding port 3/1, vlanNo 3
MCAST-ROUTER: Creating RouterPortTimer for port 3/1, vlanNo 3
```

```
Switch_B (enable) show multi router
CGMP disabled
IGMP enabled
```

```
Port      Vlan
-----  -
3/1      2-3
```

```
Total Number of Entries = 1
'*' - Configured
Switch_B (enable)
```

3. Connect a new host in group 224.10.10.10 (on port 3/2). This host sends an IGMP membership report. The report is received, snooped by the switch, the entry is added, and the IGMP report is forwarded to the router.

### On Switch\_B

```
MCAST-IGMPQ:recvd an IGMP V2 Report on the port 3/2 vlanNo 3 GDA 224.10.10.10
MCAST-RELAY:Relaying packet on port 3/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP RELAY msg on port 3/1 vlanNo 3
```

```
Switch_B (enable) show cam static
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  -
3      01-00-5e-0a-0a-0a        -----  3/1-2
```

4. Add one more user in VLAN 3 on port 3/3, as shown below.

```
Switch_B (enable) show cam static

* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  -
3      01-00-5e-0a-0a-0a        -----  3/1-3
```

5. Remove port 3/2. Port 3/2 sends an IGMP Leave message; the switch sends back an IGMP group-specific query on port 3/2 and starts a timer. When the timer expires without receiving a response, it deletes the port from the group.

```
MCAST-IGMPQ:recvd an IGMP Leave on the port 3/2 vlanNo 3 GDA 224.10.10.10
MCAST-IGMPQ-LEAVE:router_port_tbl[vlanNo].QueryTime = 0
MCAST-DEL-TIMER: Deletion Timer Value set to Random Value 1
MCAST-SEND:Transmitting IGMP Mac Based GS Query msg on port 3/2 vlanNo 3
MCAST-SEND: Transmit Succeeded for IGMP Group Specific Query msg on port 3/2 vlanNo 3
MCAST-TIMER:IGMPLeaveTimer expired on port 3/2 vlanNo 3 GDA 01-00-5e-0a-0a-0a
MCAST-TIMER:IGMPLeaveTimer:delete leave timer
```

```
Switch_B (enable) show cam static
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  -
3      01-00-5e-0a-0a-0a        -----  3/1,3/3
```

6. The host on port 3/3 leaves the group and sends an IGMP Leave message. The only difference from the previous point is that the IGMP Leave message is finally forwarded to the router port.

```
MCAST-IGMPQ:recvd an IGMP Leave on the port 3/3 vlanNo 3 GDA 224.10.10.10
MCAST-SEND:Transmitting IGMP Mac Based GS Query msg on port 3/3 vlanNo 3
MCAST-SEND: Transmit Succeeded for IGMP Group Specific Query msg on port 3/3 vlanNo 3
MCAST-TIMER:IGMPLeaveTimer expired on port 3/3 vlanNo 3 GDA 01-00-5e-0a-0a-0a
MCAST-TIMER:IGMPLeaveTimer expiry: Transmit IGMP Leave on port 3/1 vlanNo 3
MCAST-SEND:Transmitting IGMP Leave msg on port 3/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP Leave Message on port 3/1 vlanNo 3
MCAST-TIMER:IGMPLeaveTimer:delete leave timer
```

The subnet configuration is now back at the beginning, its state in Step 1. The multicast entry has disappeared from the **show cam static** command output.

To finish, view an example of the **show igmp static** command output, as shown below.

```
Switch_B (enable) show igmp stat 2
IGMP enabled
```

```
IGMP statistics for vlan 2:
Total valid pkts rcvd:      329
Total invalid pkts rcvd    0
General Queries rcvd      82
Group Specific Queries rcvd 0
MAC-Based General Queries rcvd 0
Leaves rcvd                0
Reports rcvd               82
Queries Xmitted            0
GS Queries Xmitted         0
Reports Xmitted            0
Leaves Xmitted             0
Failures to add GDA to EARL 0
Topology Notifications rcvd 0
```

```
Switch_B (enable) show igmp stat 3
IGMP enabled
```

```
IGMP statistics for vlan 3:
Total valid pkts rcvd:      360
Total invalid pkts rcvd    0
General Queries rcvd      93
Group Specific Queries rcvd 6
MAC-Based General Queries rcvd 0
Leaves rcvd                11
Reports rcvd               64
Queries Xmitted            0
GS Queries Xmitted         14
Reports Xmitted            0
Leaves Xmitted             10
Failures to add GDA to EARL 0
Topology Notifications rcvd 1
Switch_B (enable)
```

---

## Related Information

- [Multicast Catalyst Switches Support Matrix](#)
- [IP Multicast Support Page](#)
- [Cisco Technology Support](#)
- [Cisco Product Support](#)
- [Technical Support – Cisco Systems](#)

---

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Jul 09, 2007

Document ID: 10559

---