

How CGMP Leave Processing Functions

This document describes how the Cisco Group Management Protocol (CGMP) leaves processing functions; it also includes its interaction with the Hot Standby Router Protocol (HSRP).

The introduction of Internet Group Management Protocol Version 2 (IGMPv2) brings new functionality, including *leave group* messages. Cisco has added new functionality to CGMP to work with *leave group* messages: *CGMP leave processing*. *CGMP leave processing* allows switches to detect the IGMPv2 *leave group* messages. Hosts send *leave group* messages to the all-router multicast address, 224.0.0.2, when they no longer wish to receive data for that group. The switch supervisor engine module intercepts messages.

When the supervisor engine module detects an IGMPv2 *leave group* message, it starts a query-response timer, and then sends an IGMP *membership query* message from the port that received the IGMPv2 *leave group* message.

If the timer expires before an IGMP *membership report* message is received on that port, the corresponding port multicast Media Access Control (MAC) address is removed from the switch-forwarding table.

If this port is also the last active port in the multicast group, then the switch forwards the IGMPv2 *leave group* message to all known router ports.

The router then starts the normal deletion process by sending a *group-specific query*. If the router receives no response, it removes this group from its multicast routing table for that interface.

The router then sends a CGMP *leave* to the switch. Upon receipt, the switch erases the group from the static table.

When CGMP *leave processing* is enabled, The switch needs to intercept IGMP leave group messages. In order to accomplish this, two entries are added as system addresses to the content-addressable memory (CAM) table. These two entries directly relate to the IP addresses used by IGMP. They are *igmp leave* messages (224.0.0.2) and *igmp membership query* messages (224.0.0.1.)

You can verify these addresses have been added with the command:

```
Show Cam System
```

```
5000-1> (enable) sh cam sys
```

```
VLAN Dest MAC/Route Des Destination Ports or VCs
```

```
-----  
Output removed for clarity
```

```
2 01-00-5e-00-00-01# 1/3
```

```
2 01-00-5e-00-00-02# 1/3
```

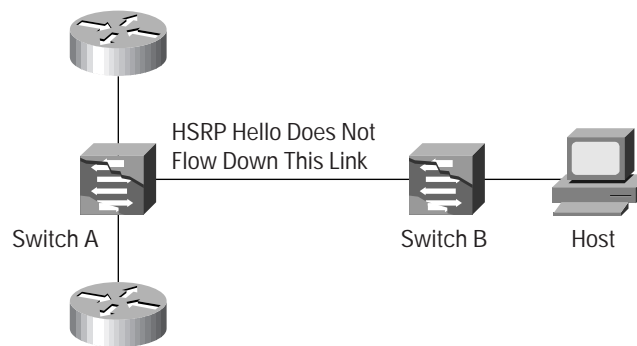
Notes on Using CGMP Leave Processing

1. *Enabling CGMP leave processing*—CGMP *leave processing* is disabled by default. To enable CGMP leave processing, enter the `set cgmp leave enable` command.
2. *How CGMP switches learn router ports*—When CGMP leave processing is enabled, Catalyst® switches learn router ports through the Protocol Independent Multicast (PIM)-v1, Hot Standby Router Protocol (HSRP), and CGMP *self-join* messages. When CGMP *leave processing* is disabled, switches discover router ports through CGMP *self-join* messages only.
3. *HSRP/CGMP interaction*—HSRP uses MAC 01-00-5e-00-00-02. This address is the all-routers address, the same address that IGMP *membership report* messages use. With CGMP *leave* enabled, all HSRP packets go to the switch CPU because they are, at a MAC level, identical to IGMP *membership report* messages. Because these are not IGMP packets, the switch relays them to all known router ports.
4. *HSRP and CGMP possible issue*—If HSRP and CGMP *leave processing* are both in use, then in certain topologies, unicast flooding can occur. As stated in point 3, frames addressed to HSRP are not flooded across the virtual LAN (VLAN), but are intercepted and forwarded to the switch CPU. When a packet is identified as not being IGMP, it is forwarded to all router ports, but if a host is not locally connected to the switch where the HSRP routers are located, then unicast flooding can occur.

Example

Two switches are connected together. One switch, Switch A, has two HSRP routers directly attached and is also CGMP *leave processing* enabled. The other, Switch B, has a workstation attached that is sending data to the HSRP virtual MAC address.

Figure 1



Because of the way IGMP/HSRP packets are processed, and because they are sent only to known router ports, HSRP frames are not forwarded to Switch B, meaning that Switch B will never learn the location of the HSRP virtual MAC address. Therefore, traffic from the workstation located on Switch B directed to the HSRP virtual MAC address would be flooded across Switch B.

This effect can be resolved by forcing the CGMP *leave processing*-enabled switch to treat the connecting link as a router link with the following command:

```
Set multicast router mod_num/port_num
```

5. *Link Local addresses*—Link local addresses are reserved IP multicast addresses in the range 224.0.0.0-224.0.0.255. IP multicast packets whose addresses map into the MAC address range between 01-00-5E-00-00-00 and 01-00-5E-00-00-FF are meant to traverse the local Layer 3 segment, and as such are not meant to be constrained by CGMP. Because IP multicast groups on Ethernet networks have a 32 -1 Layer 3 address-to-MAC address overlap, care should be taken to choose IP multicast group addresses that do not match link local MAC addresses.

Example

Group 225.128.0.9, though not a link local group, would map to the same MAC addresses as 224.0.0.9, which is used by Routing Information Protocol (RIP) Version 2.

Known Problems with CGMP Leave Processing

CSCdm05087 has been identified in Cisco Catalyst software Version 4.4(1). This occurs only when CGMP is disabled and then enabled, while CGMP *leave processing* is disabled. A CAM entry for HSRP and CGMP (0100.5e00.0002) is mistakenly added to the CAM table. This entry should be added only when CGMP *leave processing* is enabled.

The workaround is to enable and disable CGMP *leave processing*:

```
set cgmp leave enable
set cgmp leave disable
```



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
www.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela

Copyright © 2000 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (8/005R)