

Using RGMP: Basics and Case Study

Document ID: 12034

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

RGMP Reduces Load on the Network

RGMP in Detail

- What Causes the Router to Send RGMP Packets
- What Happens When a Switch Receives RGMP Packets
- RGMP Configuration and Verification

RGMP on Catalyst 6000 Running Cisco IOS System Software

Case Study

- Enabling RGMP on the Switch
- Enabling RGMP on the Routers
- RGMP Operation in VLAN 2
- RGMP Join Operation in VLAN 3
- RGMP Leave Operation
- RGMP Bye Operation

Related Information

Introduction

Router–Port Group Management Protocol (RGMP) is used with IGMP snooping to constrain multicast traffic to layers where it is really needed. IGMP snooping sends multicast traffic to all router ports. With RGMP, multicast traffic is only sent to ports that need to receive it. RGMP is designed to run on the backbone of the multicast network; basic knowledge of multicasting (IGMP, PIM, multicast routing) is helpful for understanding this document.

Note that a new feature now exists that replaces RGMP and is more scalable. This feature is called protocol independent multicast (PIM) snooping and it performs the same goal as RGMP. PIM snooping is out of the scope of this document.

For more information, refer to [Configuring PIM Snooping](#).

Prerequisites

Requirements

Readers of this document should be aware of these protocol limitations:

- You need to run RGMP on both the routers and the switches.
- You need to enable IGMP snooping on the switches.
- RGMP will only work for groups configured with PIM sparse mode.
- Sources sending multicast traffic that are directly connected to an RGMP switch are not supported.
- Connecting multiple routers to the same switch port is not supported (two routers on the same hub, for example).

- Connecting multiple routers to the same non-RGMP switch is not supported.
- RGMP only allows you to restrict traffic towards a directly connected router or towards a router connected being a non-RGMP capable switch. RGMP is not capable of restricting traffic to a multicast router connected behind another RGMP capable switch.

Failure to follow these restrictions may result in breaks in multicast connectivity.

Components Used

RGMP is a protocol that runs between Catalyst switches and routers, both of which need to support RGMP in order for the feature to work. The following switches support RGMP:

- Catalyst 6000: since software version 5.4
- Catalyst 6000 running Cisco IOS® System Software: since software 12.1(3a)E3
- Catalyst 5000: since software version 5.4

RGMP is supported in the following versions of the Cisco IOS router software:

- 12.3 Mainline
- 12.3T
- 12.2 Mainline
- 12.2.S
- 12.2T
- 12.1E
- 12.1T (beginning with version 12.1(5)T1)
- 12.0S (beginning with version 12.0(10)S)
- 12.0ST (beginning with version 12.0(11)ST)

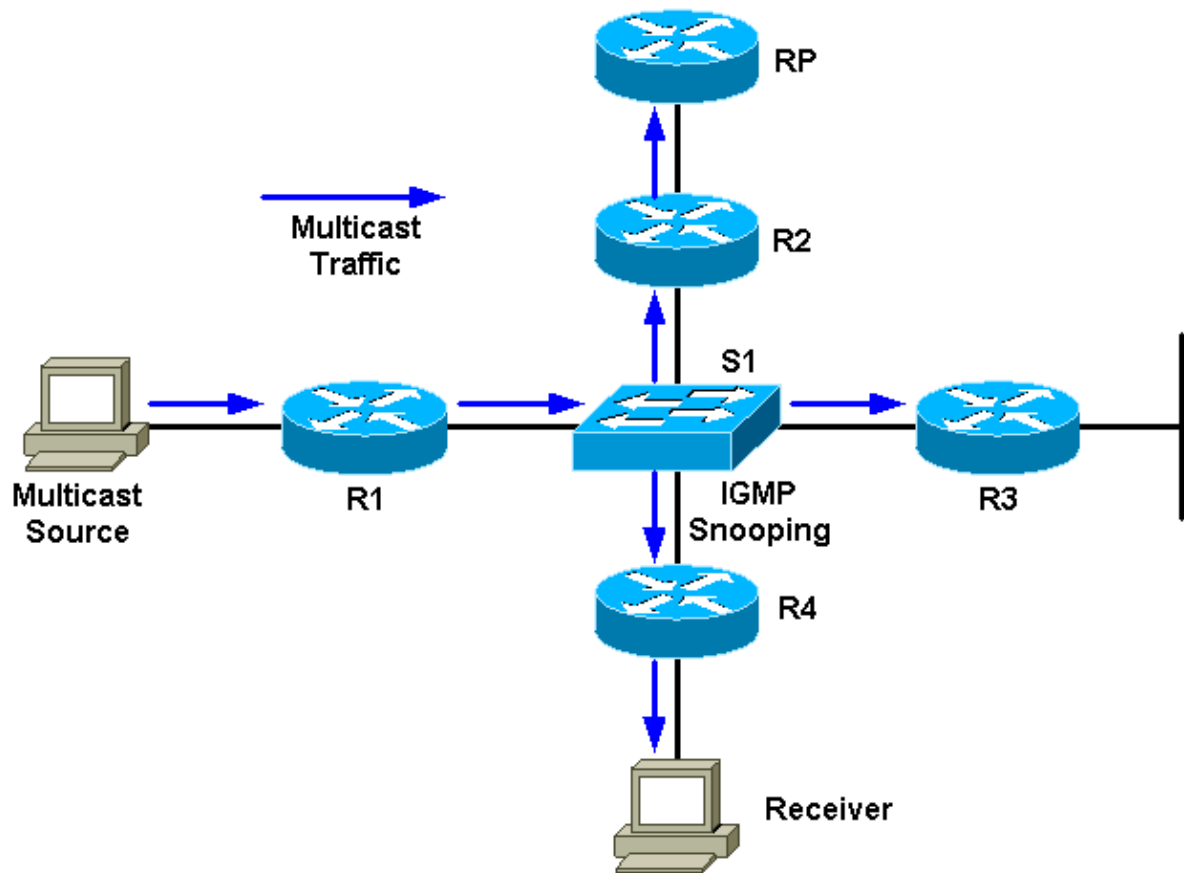
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

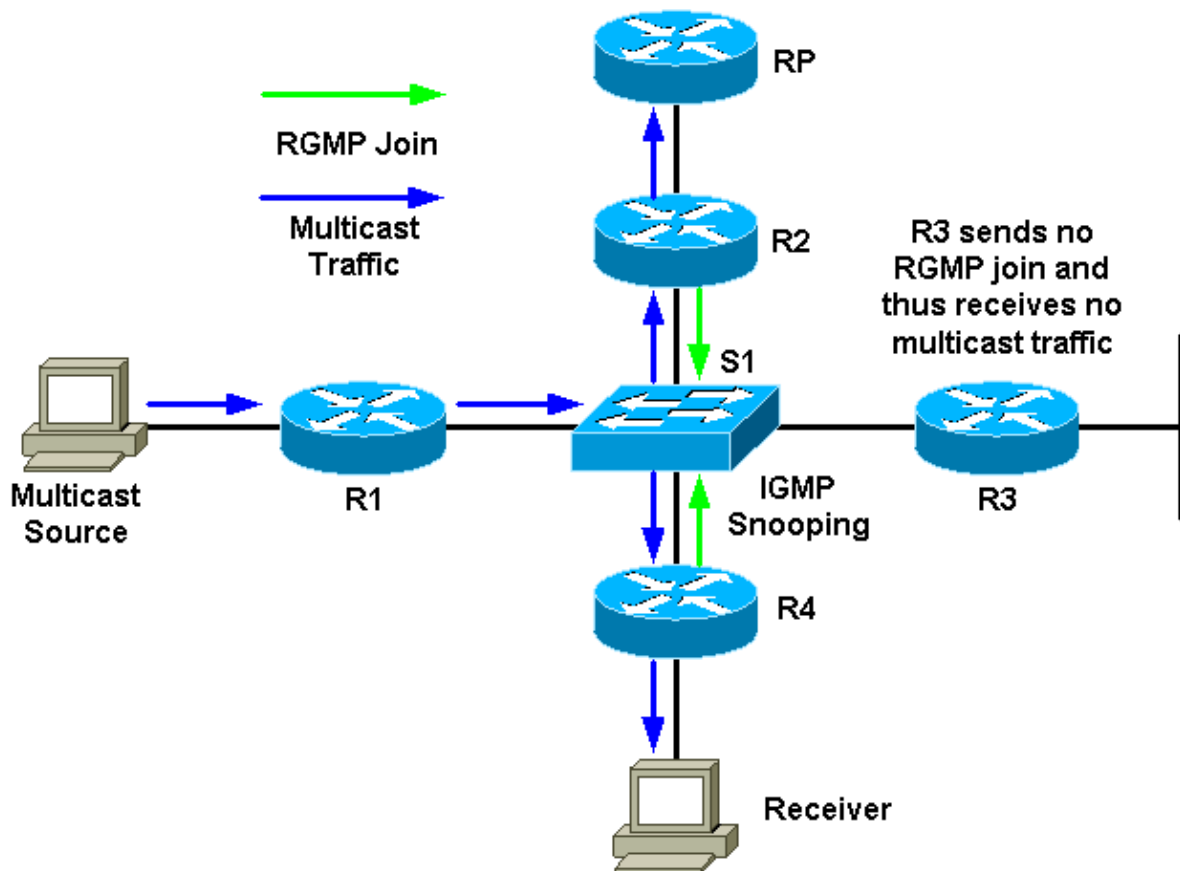
RGMP Reduces Load on the Network

The purpose of RGMP is to eliminate unnecessary multicast traffic. This diagram shows a hypothetical network without RGMP enabled:



There is one multicast source connected to R1 and one receiver connected to R4. The RP for the group is behind R2. The traffic is forwarded by R1 to the switch (per PIM and mroute table, as there is a receiver behind the switch interface). The switch will detect this source-only network with IGMP snooping and will create a static Content-Addressable Memory (CAM) entry pointing to all routers: R1, R2, R3, and R4. The multicast traffic will be sent to all routers, including R3, which does not need the traffic. If the multicast traffic is high in volume, it can create unnecessary load to router R3. RGMP has been created to overcome this problem.

This diagram shows the same network with RGMP enabled (assuming that the routers and switch are RGMP-capable):



R2 and R4 will send an RGMP join for that multicast group to the switch. R3 will not send an RGMP join. As a result, the switch will only forward the multicast traffic received from R1 for that group to R2 and R4 and not to R3. This decreases traffic on the network.

RGMP in Detail

RGMP is, like CGMP, a protocol that runs between a router and a switch. Routers send RGMP packets, and switches listen for RGMP packets. Switches never send RGMP packets, and routers ignore any RGMP packets they might receive. RGMP packets are IP packets of type IGMP and are sent to the reserved group address 224.0.0.25 (MAC address 01-00-5e-00-00-19). As IGMP packets, they are sent with a Time To Live (TTL) of 1. The address 224.0.0.25 is a reserved address corresponding to all switch multicast addresses. An RGMP packet contains basically a Type field, a group address field, and a checksum.

This table shows the different Type fields available for RGMP packets:

| Description | Action |
|-------------|--|
| Hello | When RGMP is enabled on the router, no multicast data traffic is sent to the router by the switch unless an RGMP join is specifically sent for a group. |
| Bye | When RGMP is disabled on the router, all multicast data traffic is sent to the router by the switch. |
| Join | Multicast data traffic for a multicast MAC address from the Layer 3 group address G is sent to the router. These packets have group G in the Group Address field of the RGMP packet. |

| | |
|-------|---|
| Leave | Multicast data traffic for the group G is not sent to the router. These packets have group G in the group address field of the RGMP packet. |
|-------|---|

Hello and Bye packets use 0.0.0.0 as the group address in the RGMP packet. Join and Leave use the group address that interests the router (to join or to leave).

RGMP packets use the following types of addresses:

| Type of Address | Address Used |
|---|---|
| Destination MAC address of all RGMP packets | 01-00-5e-00-00-19 |
| Destination IP address of all RGMP packets | 224.0.0.25 |
| Group address used in RGMP Hello and Bye | 0.0.0.0 |
| Group address used in RGMP Join and Leave | Multicast group for which Join or Leave is sent |

What Causes the Router to Send RGMP Packets

RGMP Hello

Whenever RGMP is enabled on the router, the router sends out an RGMP Hello message to the switch indicating that the switch should not forward multicast data traffic to this router unless an RGMP Join is specifically sent for a group. Also, note that PIM must be configured on the router for this feature to work. RGMP Hello messages are sent at the same retransmission intervals as PIM Hello messages (default is 30 seconds). RGMP Hello messages always precede PIM Hello messages.

RGMP Bye

Whenever RGMP is disabled on the router, it sends an RGMP Bye message to indicate to the switch that the router is no longer doing RGMP and that all multicast traffic should again be forwarded to this router.

RGMP Join

Whenever a router sends a PIM Join, it also constructs an RGMP Join and sends it out on the same interface on which PIM Join is to be sent out. Using the previous diagrams as an example, R4 sends a PIM Join message to the RP when it receives an IGMP Report from the Receiver for group G. It also sends an RGMP Join on the same interface, which is then captured by the switch S1. S1 processes the packet and adds that router port to the static Layer 2 entry (static CAM entry) for the group G. This allows forwarding traffic for the group G on this port.

To summarize:

- RGMP Join is sent whenever a router creates a (*,G) entry and is sent on the same interface as it sends a PIM Join message.
- RGMP Join is sent whenever a router creates a (S,G) entry. Router will send a PIM Join message on the interface towards S and hence RGMP Join is also sent on the same interface towards S.
- RGMP Join is sent whenever PIM Join is sent, but not when PIM Join is received.

- If there are multiple sources sending to group G and there is one (*,G) entry, only one RGMP Join will be sent out.

RGMP Leave

Whenever a router sends out a PIM Prune message for a (*,G) or (S,G), it also checks to see if there is at least one other mroute entry for this group for the interface on which the PIM Prune was sent. If there is no other entry, an RGMP Leave is sent on the same interface.

What Happens When a Switch Receives RGMP Packets

With RGMP disabled and IGMP snooping enabled on the switch, each multicast group forwarding entry in the switch has a list of output ports that includes all of the multicast router ports as well as all of the ports on which interested hosts are joined to the multicast group. When RGMP is enabled, the following things change:

- Switches do not send any multicast group to an RGMP-capable router unless the router specifically requests it (except for the reserved group in the range 224.0.0.x and for 224.0.1.[39–40]).
- Switches still send multicast traffic from all groups to non-RGMP-capable routers.

RGMP Hello

When an RGMP Hello packet is received from a router port, the switch marks this router port as RGMP-capable, and general multicast traffic is no longer sent to that multicast router port.

Note: RGMP Hello packets are generally not forwarded out of the chassis. RGMP Hello packets are only forwarded out once the first RGMP Hello is received on a port. The port is then marked as an RGMP port and the Hello packet is forwarded on to another RGMP-capable multicast router port..

RGMP Bye

On the receipt of RGMP Bye, unmark the router port as RGMP router port and add this port on all existing group in that VLAN.

RGMP Join

When an RGMP Join packet is received for a specific group, the switch adds the router port from which the RGMP Join was received to the list of destination ports for that group. RGMP Joins are also forwarded to all RGMP-capable router ports.

RGMP Leave

When an RGMP Leave packet is received for a specific group, the switch removes the router port from the group of ports interested in receiving that group.

RGMP Configuration and Verification

To enable RGMP on a switch:

```
#set igmp enable

!--- If this has not been done previously.

#set rgmp enable
```

You can verify the setup by typing:

```
#sh rgmp group
#sh multi router
#sh rgmp stat
#sh multi group
```

To configure RGMP on a router:

```
#ip rgmp
!--- In interface mode.
```

and, if not done previously:

```
#ip multicast-routing
!--- In global configuration mode.

#ip pim sparse-mode
!--- In interface mode.
```

RGMP on Catalyst 6000 Running Cisco IOS System Software

RGMP on the Catalyst 6000 running Cisco IOS System Software has these characteristics:

- Enabled by default on all L2 port (switchport) and can not be disabled
- Needs to be enables on any L3 multicast port if the L3 multicast interface is needed to act as the RGMP router; this is done by issuing the **ip rgmp** command in the interface mode (as on regular Cisco IOS routers).

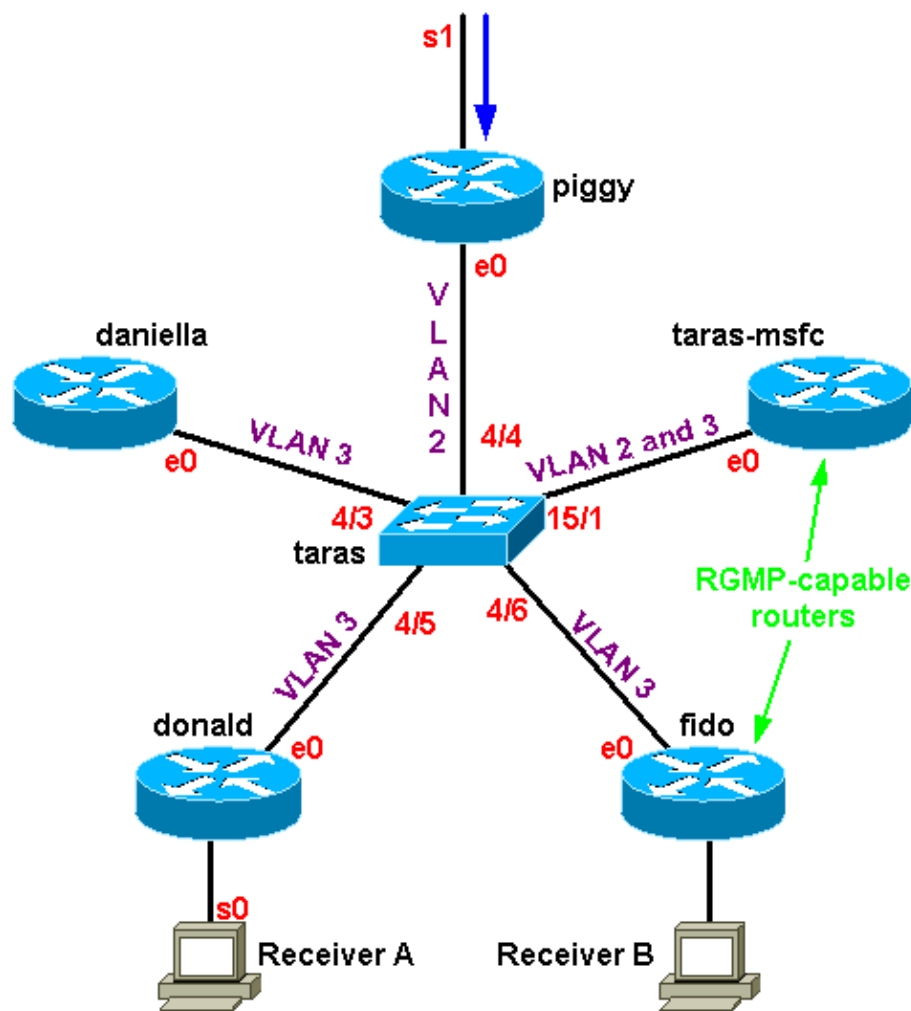
Interfaces running RGMP and any other RGMP router detected by IGMP snooping can be verified by issuing the following command:

```
Boris#show ip igmp snooping mrouter
vlan          ports
-----+-----
   1   Po3,Router
  10   Gi3/8,Router
  11   Gi3/8,Router
 100   Router
 101   Router
 198   Po3,Router
 199   Po3,Router+
 222   Router
'+'- RGMP capable router port
Boris#
```

The preceding output shows a Catalyst 6000 running Cisco IOS Software with the **ip rgmp** command configured on VLAN 199 interface. On VLAN 199, the router is marked as RGMP capable. The router in Cisco IOS Software stands for the 6500 router itself in VLAN 199.

Case Study

This diagram represents an actual network using RGMP:



In this case, only fido and the Multilayer Switch Feature Card (MSFC) in taras are RGMP-capable routers; donald, daniella, and piggy are non-RGMP-capable routers. There is a multicast source 4.4.4.1 sending to 224.1.1.1 located on the serial behind piggy. Taras-msfc is doing the Inter-VLAN routing between VLAN 2 and VLAN 3. There is no receiver in VLAN 2 but two receivers in VLAN 3: one behind fido and one behind donald.

Note: In the next section, output not preceded by a specific command is assumed to be from `debug ip rgmp` on the routers and `set trace mcast 5` on the switch.

Enabling RGMP on the Switch

First, enable RGMP on taras (a Catalyst 6000 switch), assuming that none of the routers are configured for RGMP yet. As soon as RGMP is enabled, the switch adds the multicast MAC address 01-00-5e-00-00-19 to the system CAM table, which means that it starts to listen to all packets sent to that MAC address. This is the address that corresponds to 224.0.0.25, which is used by RGMP:

```
taras (enable) set rgmp enable
RGMP enabled.
```

```
taras (enable) show cam sys
```

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

| VLAN | Dest MAC/Route | Des | [CoS] | Destination Ports or VCs | [Protocol Type] |
|------|-------------------|-----|-------|--------------------------|-----------------|
| 1 | 00-d0-00-3f-8b-fc | R# | | 15/1 | |
| 1 | 00-d0-00-3f-8b-ff | # | | 1/3 | |
| 1 | 01-00-0c-cc-cc-cc | # | | 1/3 | |
| 1 | 01-00-0c-cc-cc-cd | # | | 1/3 | |
| 1 | 01-00-0c-dd-dd-dd | # | | 1/3 | |
| 1 | 01-00-5e-00-00-19 | # | | 1/3 | |
| 1 | 01-80-c2-00-00-00 | # | | 1/3 | |
| 1 | 01-80-c2-00-00-01 | # | | 1/3 | |
| 2 | 00-d0-00-3f-8b-fc | R# | | 15/1 | |
| 2 | 01-00-0c-cc-cc-cc | # | | 1/3 | |
| 2 | 01-00-0c-cc-cc-cd | # | | 1/3 | |
| 2 | 01-00-0c-dd-dd-dd | # | | 1/3 | |
| 2 | 01-00-5e-00-00-19 | # | | 1/3 | |
| 2 | 01-80-c2-00-00-00 | # | | 1/3 | |
| 2 | 01-80-c2-00-00-01 | # | | 1/3 | |
| 3 | 00-d0-00-3f-8b-fc | R# | | 15/1 | |
| 3 | 01-00-0c-cc-cc-cc | # | | 1/3 | |
| 3 | 01-00-0c-cc-cc-cd | # | | 1/3 | |
| 3 | 01-00-0c-dd-dd-dd | # | | 1/3 | |
| 3 | 01-00-5e-00-00-19 | # | | 1/3 | |
| 3 | 01-80-c2-00-00-00 | # | | 1/3 | |
| 3 | 01-80-c2-00-00-01 | # | | 1/3 | |

Enabling RGMP on the Routers

Now enable RGMP on taras–msfc and fido. The router is configured in the interface mode, and as **debug ip rgmp** is running you can see that the router starts to send RGMP Hello packets on that interface every 30 seconds.

```
taras(config-if)#ip rgmp
00:10:24: RGMP: Sending a Hello packet on Ethernet0
00:10:54: RGMP: Sending a Hello packet on Ethernet0
00:11:24: RGMP: Sending a Hello packet on Ethernet0
00:11:54: RGMP: Sending a Hello packet on Ethernet0
```

If you now look at the switch, you can see that ports 4/6 and 15/1 are marked as RGMP–capable router ports. Notice that the switch always receives an RGMP Hello just before a PIM Hello:

```
MCAST-IGMPQ:recvd an RGMP Hello on the port 15/1 vlanNo 3 GDA 0.0.0.0
MCAST-RGMP: Received RGMP Hello in vlanNo 3 on port 15/1
MCAST-IGMPQ:recvd a PIM V2 packet of type HELLO on the port 15/1 vlanNo 3
```

```
taras (debug-eng) show multi ro
Port      Vlan
-----
4/3       3
4/4       2
4/5       3
4/6       + 3
15/1      + 2-3

Total Number of Entries = 5
'*' - Configured
'+' - RGMP-capable
```

RGMP Operation in VLAN 2

Since there is an active receiver behind donald (there is not yet a receiver behind fido), the multicast traffic in VLAN 2 needs to be forwarded onto VLAN 3. So the MSFC in taras needs to get the traffic in VLAN 2.

However, since RGMP is enabled, the switch no longer forwards the multicast traffic to the MSFC. The MSFC must send an RGMP Join on VLAN 2 to the switch as a request to receive that group.

The router sends:

```
16:10:28: RGMP: Sending a Join packet on Vlan2 for group 224.1.1.1
16:10:29: RGMP: Sending a Join packet on Vlan2 for group 224.1.1.1
```

The supervisor on the switch receives it:

```
MCAST-RGMP: Received RGMP Join for 224.1.1.1 in vlanNo 2 on port 15/1
```

Using the **show rgmp** group, you can see that port 15/1 has joined group 01-00-5e-01-01-01 in VLAN 2. Notice that in VLAN 3, the static CAM entry is present, but the only router port included in the port list is that of the non-RGMP-capable router (that is, 15/1 and 4/6 are not in the port list for the entry in VLAN 3 because those routers are RGMP-capable and did not send an RGMP join in VLAN 3). Notice also in the static CAM table that the groups 01-00-5e-00-01-[27,28], corresponding to 224.0.1.[39,40] used by auto-rp, are not affected by RGMP operation. All traffic for these groups is still going to all multicast routers, regardless of whether they are RGMP-capable:

```
taras (enable) show cam sta
```

```
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry $ = Dot1x Security Entry
```

| VLAN | Dest MAC/Route Des | [CoS] | Destination Ports or VCs / [Protocol Type] |
|------|--------------------|-------|--|
| 2 | 01-00-5e-01-01-01 | | 4/4,15/1 |
| 2 | 01-00-5e-00-01-27 | | 4/4,15/1 |
| 2 | 01-00-5e-00-01-28 | | 4/4,15/1 |
| 3 | 01-00-5e-01-01-01 | | 4/5,4/3 |
| 3 | 01-00-5e-00-01-27 | | 4/3,4/5-6,15/1 |
| 3 | 01-00-5e-00-01-28 | | 4/3,4/5-6,15/1 |

```
taras (enable) show rgmp group 01-00-5e-01-01-01
RGMP enabled
```

| VLAN | Dest MAC/Route Des | [CoS] | RGMP Joined Router Ports |
|------|--------------------|-------|--------------------------|
| 2 | 01-00-5e-01-01-01 | | 15/1 |

```
Total Number of Entries = 1
```

Now look at the RGMP stats for VLAN 2. The switch is regularly receiving RGMP Hello and RGMP Join packets. It gets one RGMP Hello every 30 seconds from taras-msfc, and taras-msfc sends an RGMP Join for 224.1.1.1 each time it sends a PIM Join for that group:

```
taras (enable) show rgmp stat 2
RGMP enabled
RGMP statistics for vlan 2:
```

```
Receive :
  Valid pkts:          67
  Hellos:              40
  Joins:               27
  Leaves:              0
  Join Alls:           0
  Leave Alls:          0
  Byes:                0
  Discarded:           0
Transmit :
  Total pkts:          0
```

```

Failures:          0
Hellos:            0
Joins:             0
Leaves:           0
Join Alls:        0
Leave Alls:        0
Byes:             0

```

Up to this point, taras–msfc and fido have only sent Hello packets in VLAN 3:

```

taras (enable) show rgmp stat 3
RGMP enabled
RGMP statistics for vlan 3:

Receive :
  Valid pkts:          468
  Hellos:              468
  Joins:               0
  Leaves:              0
  Join Alls:          0
  Leave Alls:         0
  Byes:                0
  Discarded:          0
Transmit :
  Total pkts:          0
  Failures:            0
  Hellos:              0
  Joins:               0
  Leaves:              0
  Join Alls:          0
  Leave Alls:         0
  Byes:                0

```

RGMP Join Operation in VLAN 3

If you now start Receiver B behind fido, the RGMP–capable router will send an RGMP Join to the switch for group 224.1.1.1. The switch will receive it and add port 4/6 (fido) to the list of interested receivers for that group in VLAN 3.

On the router, you see:

```

01:07:49: RGMP: Sending a Join packet on Ethernet0 for group 224.1.1.1
01:07:49: RGMP: Sending a Join packet on Ethernet0 for group 224.1.1.1
01:07:49: RGMP: Sending a Join packet on Ethernet0 for group 224.1.1.1
01:07:51: RGMP: Sending a Join packet on Ethernet0 for group 224.1.1.1

```

The switch receives the RGMP Join and adds router port 4/6 to the static entry. You can see the result in various **show** commands:

```

MCAST-IGMPQ:rcvcd an RGMP Join  on the port 4/6 vlanNo 3 GDA 224.1.1.1
MCAST-RGMP: Received RGMP Join for 224.1.1.1 in vlanNo 3 on port 4/6
EARL-MCAST: SetRGMPPortInGDA: RGMP port 4/6 in vlanNo 3 joining for the first time
for this group 224.1.1.1

```

```

MCAST-RELAY:Relaying packet on port 15/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP RELAY msg on port 15/1 vlanNo 3

```

```

taras (enable) show rgmp group
RGMP enabled

```

```

VLAN  Dest MAC/Route Des  [CoS]  RGMP Joined Router Ports
-----

```

```

2      01-00-5e-01-01-01      15/1
3      01-00-5e-01-01-01      4/6

```

Total Number of Entries = 2

taras (enable) **show cam sta 01-00-5e-01-01-01**

* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry \$ = Dot1x Security Entry

| VLAN | Dest MAC/Route Des | [CoS] | Destination Ports or VCs / [Protocol Type] |
|------|--------------------|-------|--|
| 2 | 01-00-5e-01-01-01 | | 4/4,15/1 |
| 3 | 01-00-5e-01-01-01 | | 4/3,4/5-6 |

taras (enable) **show rgmp stat 3**

RGMP enabled

RGMP statistics for vlan 3:

Receive :

```

Valid pkts:          542
Hellos:              532
Joins:               10
Leaves:              0
Join Alls:           0
Leave Alls:           0
Byes:                0
Discarded:           0

```

Transmit :

```

Total pkts:          0
Failures:            0
Hellos:              0
Joins:               0
Leaves:              0
Join Alls:           0
Leave Alls:           0
Byes:                0

```

RGMP Leave Operation

Assume that Receiver B is not interested anymore, so fido no longer needs the multicast traffic for that group and will send a PIM Prune for the group in the interface. The router also sends an RGMP Leave for the group to let the switch know that it is not interested in that group anymore.

When Receiver B is still active, **show ip mroute** shows the (S,G) entry with a C flag, telling you there is a connected receiver interested:

```
fido#show ip mroute 224.1.1.1
```

IP Multicast Routing Table

Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,

L - Local, P - Pruned, R - RP-bit set, F - Register flag,

T - SPT-bit set, J - Join SPT, M - MSDP created entry,

X - Proxy Join Timer Running, A - Advertised via MSDP, U - URD,

I - Received Source Specific Host Report

Outgoing interface flags: H - Hardware switched

Timers: Uptime/Expires

Interface state: Interface, Next-Hop or VCD, State/Mode

```
(* , 224.1.1.1), 00:01:18/00:00:00, RP 10.10.10.1, flags: SJCL
```

```
  Incoming interface: Ethernet0, RPF nbr 33.3.3.1
```

```
  Outgoing interface list:
```

```
    Serial0, Forward/Sparse-Dense, 00:01:18/00:01:41
```

```
(4.4.4.1, 224.1.1.1), 00:01:16/00:02:59, flags: CLJT
```

```
  Incoming interface: Ethernet0, RPF nbr 33.3.3.1
```

```
  Outgoing interface list:
```

Serial0, Forward/Sparse-Dense, 00:01:16/00:01:43

When Receiver B is no longer interested, PIM will send a prune message, but the (S,G) entry is not removed immediately. The timer (highlighted in red) is counting down until the entry times out. Note that at this point, the entry is still there but with the P flag telling us it is pruned and will timeout.

```
01:15:25: PIM: Send v2 Prune on Ethernet0 to 33.3.3.1 for (10.10.10.1/32, 224.1.1.1), WC-b
01:15:25: PIM: Received v2 Join/Prune on Ethernet0 from 33.3.3.4, not to us
01:15:28: RGMP: Sending a Hello packet on Ethernet0
01:15:29: PIM: Received v2 Join/Prune on Ethernet0 from 33.3.3.3, not to us
01:15:29: PIM: Join-list: (*, 224.1.1.1) RP 10.10.10.1, RPT-bit set, WC-bit set, S-bit set
01:15:29: PIM: Join-list: (4.4.4.1/32, 224.1.1.1), S-bit set
```

IP Multicast Routing Table

```
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Advertised via MSDP, U - URD,
       I - Received Source Specific Host Report
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
```

```
(*, 224.1.1.1), 00:08:31/00:02:39, RP 10.10.10.1, flags: SJP
  Incoming interface: Ethernet0, RPF nbr 33.3.3.1
  Outgoing interface list: Null
```

```
(4.4.4.1, 224.1.1.1), 00:08:29/00:02:29, flags: PJT
  Incoming interface: Ethernet0, RPF nbr 33.3.3.1
  Outgoing interface list: Null
```

After the (S,G) entry finally times out, fido sends an RGMP Leave to the switch for group 224.1.1.1:

```
01:18:50: RGMP: Sending a Leave packet on Ethernet0 for group 224.1.1.1
01:18:58: RGMP: Sending a Hello packet on Ethernet0
```

After the switch receives the RGMP Leave, you can see in the RGMP group that there are no longer any entries for VLAN 3:

```
MCAST-IGMPQ:recvd an RGMP Leave on the port 4/6 vlanNo 3 GDA 224.1.1.1
MCAST-RGMP: Received RGMP Leave for 224.1.1.1 in vlanNo 3 on port 4/6
EARL-MCAST: ClearRGMPPortInGDA last RGMP port going away for all groups - delete rgmp_info
too for GDA 01-00-5e-01-01-01 vlanNo 3
MCAST-RELAY:Relaying packet on port 15/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP RELAY msg on port 15/1 vlanNo 3
```

```
taras (debug-eng) show rgmp group
RGMP enabled
```

| VLAN | Dest MAC/Route Des | [CoS] | RGMP Joined Router Ports |
|------|--------------------|-------|--------------------------|
| 2 | 01-00-5e-01-01-01 | | 15/1 |

```
taras (debug-eng) show rgmp stat 3
RGMP enabled
RGMP statistics for vlan 3:
```

```
Receive :
  Valid pkts: 588
  Hellos: 574
  Joins: 11
  Leaves: 3
  Join Alls: 0
  Leave Alls: 0
```

```
Byes: 0
Discarded: 0
```

RGMP Bye Operation

If you disable RGMP on fido, it will send an RGMP Bye, and the switch will change 4/6 from an RGMP router port to a normal router port:

On fido:

```
01:24:45: RGMP: Sending a Bye packet on Ethernet0
```

On the switch:

```
MCAST-IGMPQ:rcvd an RGMP Bye on the port 4/6 vlanNo 3 GDA 0.0.0.0
MCAST-RGMP: Received RGMP Bye in vlanNo 3 on port 4/6
MCAST-RELAY:Relaying packet on port 15/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP RELAY msg on port 15/1 vlanNo 3
```

```
taras (debug-eng) show rgmp stat 3
RGMP enabled
RGMP statistics for vlan 3:
```

```
Receive :
  Valid pkts: 603
  Hellos: 588
  Joins: 11
  Leaves: 3
  Join Alls: 0
  Leave Alls: 0
  Byes: 1
  Discarded: 0
Transmit :
  Total pkts: 0
  Failures: 0
  Hellos: 0
  Joins: 0
  Leaves: 0
  Join Alls: 0
  Leave Alls: 0
  Byes: 0
```

```
taras (enable) show multi router
```

| Port | Vlan |
|------|-------|
| 4/3 | 3 |
| 4/4 | 2 |
| 4/5 | 3 |
| 4/6 | 3 |
| 4/48 | 1 |
| 15/1 | + 2-3 |

Related Information

- [LAN Product Support](#)
 - [LAN Switching Technology Support](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

