



Configuring Router-Port Group Management Protocol

Feature History

Release	Modification
Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

This chapter describes the Router-Port Group Management Protocol (RGMP). RGMP is a Cisco protocol that restricts IP multicast traffic in switched networks. RGMP is a Layer 2 protocol that enables a router to communicate to a switch (or a networking device that is functioning as a Layer 2 switch) the multicast group for which the router would like to receive or forward traffic. RGMP restricts multicast traffic at the ports of RGMP-enabled switches that lead to interfaces of RGMP-enabled routers.

For a complete description of the RGMP commands in this chapter, refer to the [Cisco IOS IP Multicast Command Reference](#). To locate documentation of other commands that appear in this chapter, use the command reference master index, or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release.

IP Multicast Routing Overview

The Cisco IOS software supports the following protocols to implement IP multicast routing:

- Internet Group Management Protocol (IGMP) is used between hosts on a LAN and the routers on that LAN to track the multicast groups of which hosts are members.
- Protocol Independent Multicast (PIM) is used between routers so that they can track which multicast packets to forward to each other and to their directly connected LANs.
- Distance Vector Multicast Routing Protocol (DVMRP) is the protocol used on the MBONE (the multicast backbone of the Internet). The Cisco IOS software supports PIM-to-DVMRP interaction.



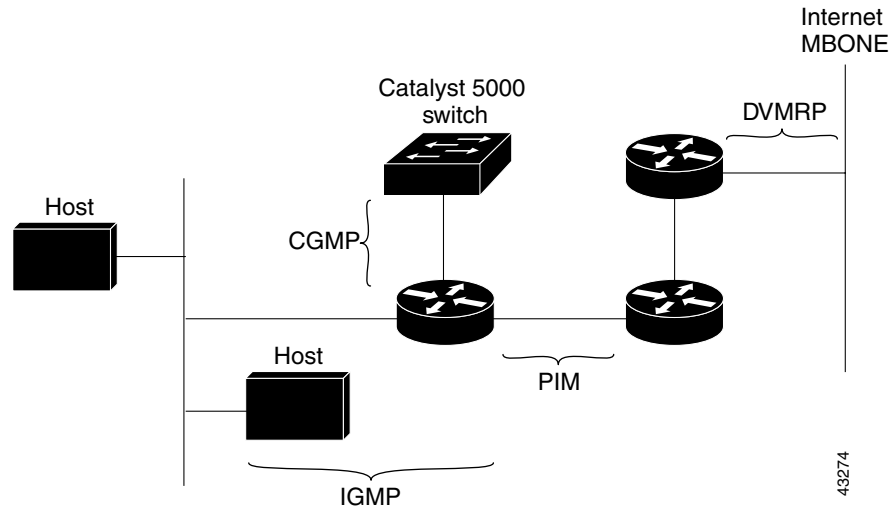
Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- Cisco Group Management Protocol (CGMP) is a protocol used on routers connected to Catalyst switches to perform tasks similar to those performed by IGMP.
- RGMP is a protocol used on routers connected to Catalyst switches or networking devices functioning as Layer 2 switches to restrict IP multicast traffic. Specifically, the protocol enables a router to communicate to a switch the IP multicast group for which the router would like to receive or forward traffic.

Figure 1 shows where these protocols operate within the IP multicast environment.

Figure 1 IP Multicast Routing Protocols



Note

CGMP and RGMP cannot interoperate on the same switched network. If RGMP is enabled on a switch or router interface, CGMP is automatically disabled on that switch or router interface; if CGMP is enabled on a switch or router interface, RGMP is automatically disabled on that switch or router interface.

RGMP Overview

RGMP enables a router to communicate to a switch the IP multicast group for which the router would like to receive or forward traffic. RGMP is designed for switched Ethernet backbone networks running PIM sparse mode (PIM-SM) or sparse-dense mode.

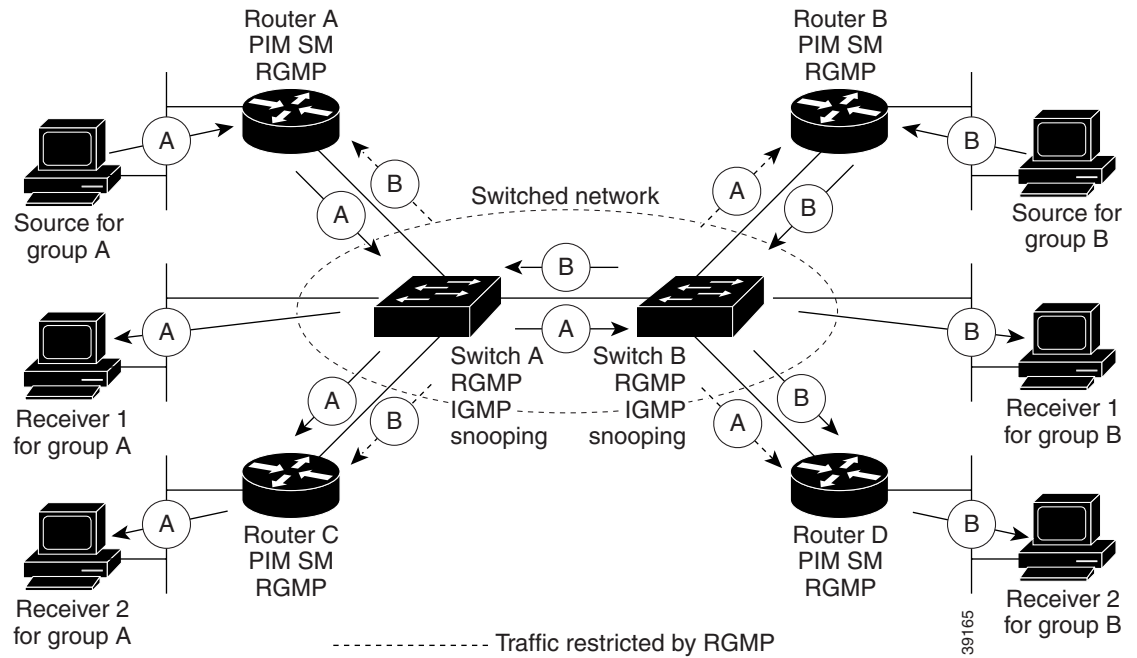


Note

RGMP-enabled switches and router interfaces in a switched network support directly connected, multicast-enabled hosts that receive multicast traffic. RGMP-enabled switches and router interfaces in a switched network do not support directly connected, multicast-enabled hosts that source multicast traffic. A multicast-enabled host can be a PC, a workstation, or a multicast application running in a router.

Figure 2 shows a switched Ethernet backbone network running PIM in sparse mode, RGMP, and IGMP snooping.

Figure 2 RGMP in a Switched Network

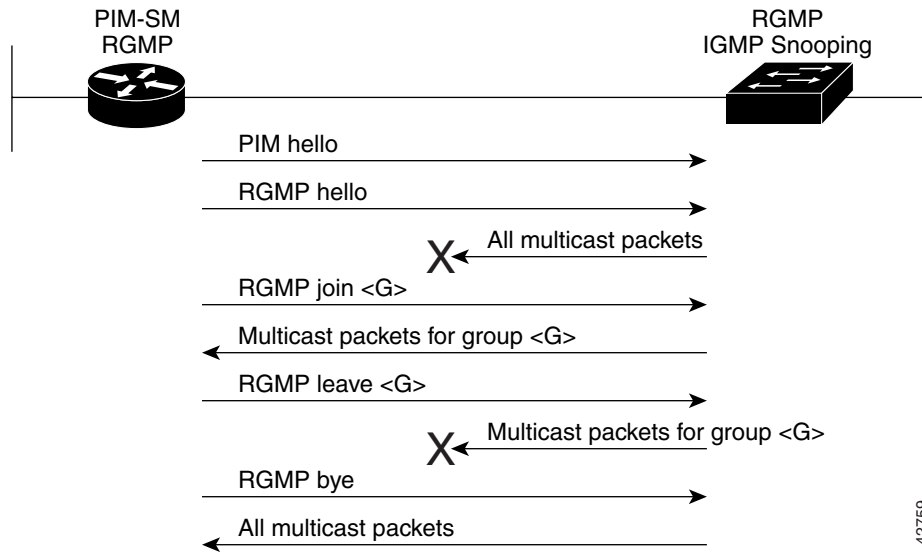


In [Figure 2](#), the sources for the two different multicast groups (the source for group A and the source for group B) send traffic into the same switched network. Without RGMP, traffic from source A is unnecessarily flooded from switch A to switch B, then to router B and router D. Also, traffic from source B is unnecessarily flooded from switch B to switch A, then to router A and router C. With RGMP enabled on all routers and switches in this network, traffic from source A would not flood router B and router D. Also, traffic from source B would not flood router A and router C. Traffic from both sources would still flood the link between switch A and switch B. Flooding over this link would still occur because RGMP does not restrict traffic on links toward other RGMP-enabled switches with routers behind them.

By restricting unwanted multicast traffic in a switched network, RGMP increases the available bandwidth for all other multicast traffic in the network and saves the processing resources of the routers.

[Figure 3](#) shows the RGMP messages sent between an RGMP-enabled router and an RGMP-enabled switch.

Figure 3 RGMP Messages



The router sends simultaneous PIM hello (or a PIM query message if PIM Version 1 is configured) and RGMP hello messages to the switch. The PIM hello message is used to locate neighboring PIM routers. The RGMP hello message instructs the switch to restrict all multicast traffic on the interface from which the switch received the RGMP hello message.

**Note**

RGMP messages are sent to the multicast address 224.0.0.25, which is the local-link multicast address reserved by the Internet Assigned Numbers Authority (IANA) for sending IP multicast traffic from routers to switches.

If RGMP is not enabled on both the router and the switch, the switch automatically forwards all multicast traffic out the interface from which the switch received the PIM hello message.

The router sends the switch an RGMP join <G> message (where G is the multicast group address) when the router wants to receive traffic for a specific multicast group. The RGMP join message instructs the switch to forward multicast traffic for group <G> out the interface from which the switch received the RGMP hello message.

**Note**

The router sends the switch an RGMP join <G> message for a multicast group even if the router is only forwarding traffic for the multicast group into a switched network. By joining a specific multicast group, the router can determine if another router is also forwarding traffic for the multicast group into the same switched network. If two routers are forwarding traffic for a specific multicast group into the same switched network, the two routers use the PIM assert mechanism to determine which router should continue forwarding the multicast traffic into the network.

The router sends the switch an RGMP leave <G> message when the router wants to stop receiving traffic for a specific multicast group. The RGMP leave message instructs the switch to stop forwarding the multicast traffic on the port from which the switch received the PIM and RGMP hello messages.

**Note**

An RGMP-enabled router cannot send an RGMP leave <G> message until the router does not receive or forward traffic from any source for a specific multicast group (if multiple sources exist for a specific multicast group).

The router sends the switch an RGMP bye message when RGMP is disabled on the router. The RGMP bye message instructs the switch to forward the router all IP multicast traffic on the port from which the switch received the PIM and RGMP hello messages, as long as the switch continues to receive PIM hello messages on the port.

RGMP Configuration Task List

To configure RGMP, perform the tasks described in the following sections. The tasks in the first two sections are required; the tasks in the remaining section are optional.

- [Enabling RGMP](#) (Required)
- [Verifying RGMP Configuration](#) (Optional)

See the end of this chapter for the section “[RGMP Configuration Example](#).”

Prerequisites

Before you enable RGMP, ensure that the following features are enabled on your router:

- IP routing
- IP multicast
- PIM in sparse mode, sparse-dense mode, source specific mode, or bidirectional mode

If your router is in a bidirectional group, make sure to enable RGMP only on interfaces that do not function as a designated forwarder (DF). If you enable RGMP on an interface that functions as a DF, the interface will not forward multicast packets up the bidirectional shared tree to the rendezvous point (RP).

You must have the following features enabled on your switch:

- IP multicast
- IGMP snooping

**Note**

Refer to the Catalyst switch software documentation for RGMP switch configuration tasks and command information.

Enabling RGMP

To enable RGMP, use the following commands on all routers in your network beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface <i>type number</i>	Specifies the router interface on which you want to configure RGMP and enters interface configuration mode.
Step 2	Router(config-if)# ip rgmp	Enables RGMP on a specified interface.

See the “[RGMP Configuration Example](#)” section later in this chapter for an example of how to configure RGMP.

Verifying RGMP Configuration

To verify that RGMP is enabled on the correct interfaces, use the **show ip igmp interface EXEC** command:

```
Router> show ip igmp interface
```

```
Ethernet1/0 is up, line protocol is up
  Internet address is 10.0.0.0/24
  IGMP is enabled on interface
  Current IGMP version is 2
  →  RGMP is enabled
  IGMP query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1000 ms
  Inbound IGMP access group is not set
  IGMP activity: 1 joins, 0 leaves
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 10.0.0.0 (this system)
  IGMP querying router is 10.0.0.0 (this system)
  Multicast groups joined (number of users):
    224.0.1.40(1)
```



Note

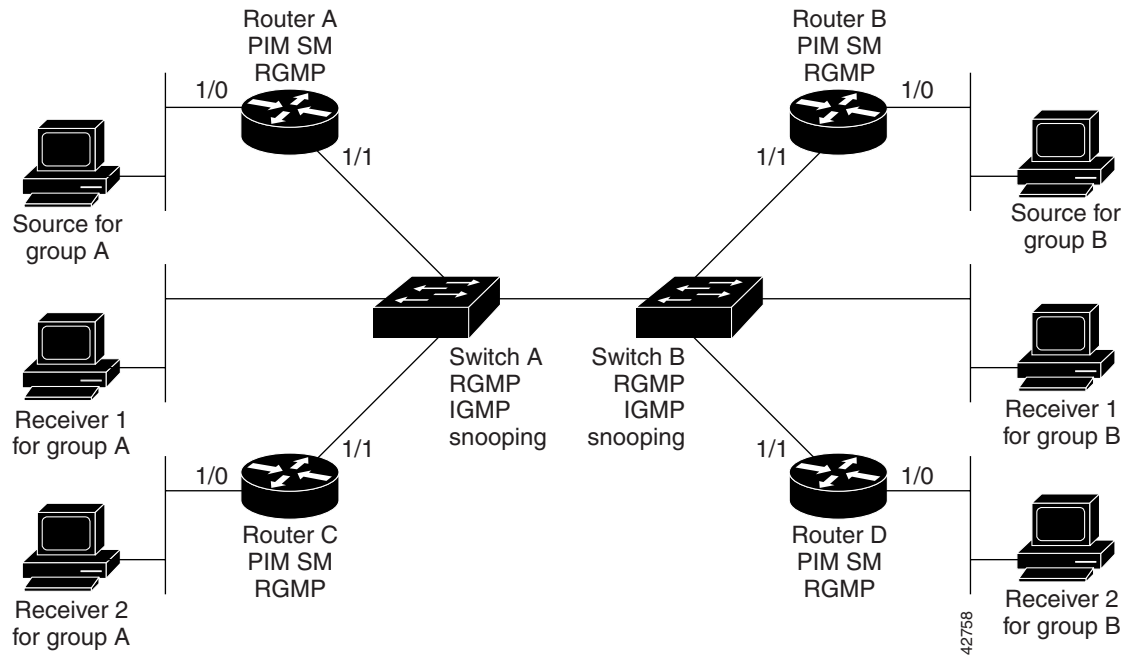
If RGMP is not enabled on an interface, no RGMP information is displayed in the **show ip igmp interface** command output for that interface.

Monitoring and Maintaining RGMP

To enable RGMP debugging, use the following command in privileged EXEC mode:

Command	Purpose
Router# debug ip rgmp [<i>group-name</i> <i>group-address</i>]	Logs debug messages sent by an RGMP-enabled router. Using the command without arguments logs RGMP Join <G> and RGMP leave <G> messages for all multicast groups configured on the router. Using the command with arguments logs RGMP join <G> and RGMP leave <G> messages for the specified group.

Figure 5 RGMP Configuration Example

**Router A Configuration**

```

ip routing
ip multicast-routing

interface ethernet 1/0
 ip address 10.0.0.1 255.0.0.0
 ip pim sparse-dense-mode
 no shutdown

interface ethernet 1/1
 ip address 10.1.0.1 255.0.0.0
 ip pim sparse-dense-mode
 ip rgmp
 no shutdown

```

Router B Configuration

```

ip routing
ip multicast-routing

interface ethernet 1/0
 ip address 10.2.0.1 255.0.0.0
 ip pim sparse-dense-mode
 no shutdown

interface ethernet 1/1
 ip address 10.3.0.1 255.0.0.0
 ip pim sparse-dense-mode
 ip rgmp
 no shutdown

```

Router C Configuration

```

ip routing
ip multicast-routing

```

```
interface ethernet 1/0
  ip address 10.4.0.1 255.0.0.0
  ip pim sparse-dense-mode
  no shutdown

interface ethernet 1/1
  ip address 10.5.0.1 255.0.0.0
  ip pim sparse-dense-mode
  ip rgmp
  no shutdown
```

Router D Configuration

```
ip routing
ip multicast-routing

interface ethernet 1/0
  ip address 10.6.0.1 255.0.0.0
  ip pim sparse-dense-mode
  no shutdown

interface ethernet 1/1
  ip address 10.7.0.1 255.0.0.0
  ip pim sparse-dense-mode
  ip rgmp
  no shutdown
```

Switch A Configuration

```
Switch> (enable) set igmp enable
Switch> (enable) set rgmp enable
```

Switch B Configuration

```
Switch> (enable) set igmp enable
Switch> (enable) set rgmp enable
```

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.

