C H A P T E R 29

Configuring RGMP

This chapter supplements the information and procedures about Router-Port Group Management Protocol (RGMP) in the Release 12.2 publication at this URL:

http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfrgmp.html

This chapter consists of these sections:

Understanding How RGMP Works

RGMP constrains multicast traffic that exits the Catalyst 6500 series switch through ports to which only disinterested multicast routers are connected. RGMP reduces network congestion by forwarding multicast traffic to only those routers that are configured to receive it.

Note To use RGMP, you must enable IGMP snooping on the Catalyst 6500 series switch. IGMP snooping constrains multicast traffic that exits through LAN ports to which hosts are connected. IGMP snooping does not constrain traffic that exits through LAN ports to which one or more multicast routers are connected.

Note You must enable Protocol Independent Multicast (PIM) on all routers and switches for RGMP to work. Only PIM sparse mode is currently supported.

All routers on the network must be RGMP-capable. RGMP-capable routers send RGMP hello messages periodically. The RGMP hello message tells the Catalyst 6500 series switch not to send multicast data to the router unless an RGMP join message has also been sent to the Catalyst 6500 series switch from that router. When an RGMP join message is sent, the router is able to receive multicast data.

To stop receiving multicast data, a router must send an RGMP leave message to the Catalyst 6500 series switch. To disable RGMP on a router, the router must send an RGMP bye message to the Catalyst 6500 series switch.

Table 29-1 provides a summary of the RGMP packet types.

Table 29-1   RGMP Packet Types

Description	Action
Hello	When RGMP is enabled on the router, no multicast data traffic is sent to the router by the Catalyst 6500 series 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 Catalyst 6500 series 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.

Default RGMP Configuration

RGMP is permanently enabled on Layer 2 LAN ports. RGMP is disabled by default on Layer 3 interfaces.

RGMP Configuration Guidelines and Restrictions

When configuring RGMP, follow these guidelines and restrictions:

- Either RGMP or PIM snooping can be enabled in a VLAN but not both.

- RGMP supports PIM sparse mode. RGMP does not support PIM dense mode. RGMP explicitly supports the two AutoRP groups in dense mode by not restricting traffic to those groups but by flooding it to all router ports. For this reason, you should configure PIM sparse-dense mode. If you configure groups other than the AutoRP groups for dense mode, their traffic will not be correctly forwarded through router ports that have been enabled for RGMP.

- To effectively constrain multicast traffic with RGMP, connect RGMP-enabled routers to separate ports on RGMP-enabled Catalyst 6500 series switches. (VLAN interfaces satisfy this restriction.)

- RGMP only constrains traffic that exits through LAN ports on which it detects an RGMP-enabled router. If a non-RGMP enabled router is detected on a LAN port, that port receives all multicast traffic.

- RGMP does not support directly connected multicast sources in the network. A directly connected multicast source will send multicast traffic into the network without signaling through RGMP or PIM. This multicast traffic will not be received by an RGMP-enabled router unless the router already requested receipt of that multicast group through RGMP. This restriction applies to hosts and to functions in routers that source multicast traffic, such as the **ping** and **mtrace** commands and multicast applications that source multicast traffic, such as UDPTN.

- RGMP supports directly connected receivers in the network. Traffic to these receivers will be constrained by IGMP snooping, or if the receiver is a router itself, by PIM and RGMP.

- CGMP is not supported in networks where RGMP is enabled on routers. You cannot enable both RGMP and CGMP on a Layer 3 interface. If RGMP is enabled on a Layer 3 interface, CGMP is silently disabled and vice versa.

- The following properties of RGMP are the same as for IGMP snooping:

  - RGMP constrains traffic based on the multicast group, not on the sender's IP address.

  - If spanning tree topology changes occur in the network, the state is not flushed as it is with Cisco Group Management Protocol (CGMP).

  - RGMP does not constrain traffic for multicast groups 224.0.0.x (x = 0...255), which allows use of PIMv2 bootstrap router (BSR) in an RGMP-controlled network.

  - RGMP in Cisco network devices operates on MAC addresses, not on IP multicast addresses. Because multiple IP multicast addresses can map to one MAC address (see RFC 1112), RGMP cannot differentiate between the IP multicast groups that might map to a MAC address.

  - The capability of the Catalyst 6500 series switch to constrain traffic is limited by its content-addressable memory (CAM) table capacity.

Enabling RGMP on Layer 3 Interfaces

To enable RGMP on a Layer 3 interface, perform this task:

	Command	Purpose
Step 1	Router(config)# **interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*} | {**port-channel** *number*}}	Selects an interface to configure.
Step 2	Router(config-if)# **ip rgmp**	Enables RGMP on the Layer 3 interface.
	Router(config-if)# **no ip rgmp**	Disables RGMP on the Layer 3 interface.
Step 3	Router(config-if)# **end**	Exits configuration mode.
Step 4	Router# **debug ip rgmp** [*name_or_group_address*]	(Optional) Monitors RGMP.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, or **ge-wan**

This example shows how to configure RGMP on FastEthernet port 3/3:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 3/3
Router(config-if)# ip rgmp
Router(config-if)# end
Router#
```