CHAPTER 15

Configuring IP Multicast

The IP multicast feature enables a host to send packets to a subset of hosts known as a multicast group. The hosts in the multicast group are the group members. Packets delivered to group members are identified by a single multicast group address. Multicast packets are delivered to a group using best-effort reliability. Any host, regardless of whether it is a member of a group, can send messages to a group. However, only the members of a group can receive the messages.

Enhancements to the IP multicast feature provide support for broadband environments. This enhanced IP multicast feature allows PPPoA, PPPoE, and RBE subscribers to participate in multicast groups and to initiate multicast messages.

The IP multicast feature supports the following protocols to implement IP multicast routing:

- Internet Group Management Protocol (IGMP)—Used between hosts on a LAN and the router(s) on that LAN to track the multicast groups of which hosts are members.
- Protocol-Independent Multicast (PIM)—Used between routers so that they can track which multicast packets to forward to each other to their directly connected LANs.
- Distance Vector Multicast Routing Protocol (DVMRP)—Used on the multicast backbone of the Internet. The Cisco IOS software supports PIM-to-DVMRP interaction. However, you cannot run DVMRP back-to-back between Cisco routers.
- Cisco Group Management Protocol (CGMP)—Used on routers connected to Cisco Catalyst switches to perform tasks similar to those performed by IGMP.

Note For more information about the IP multicast feature, see the "IP Multicast" chapter in the *Cisco IOS IP Configuration Guide*, Release 12.2.

This chapter describes the IP Multicast feature in the following topics:

Feature History for IP Multicast

Cisco IOS Release	Description	Required PRE
12.2(4)BZ1	This feature was introduced on the Cisco 10000 series router.	PRE1
12.3(7)XI1	This feature was integrated into Cisco IOS Release 12.3(7) XI1.	PRE2
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.	PRE2

Restrictions for IP Multicast

The IP Multicast feature has the following restrictions:

- Cisco 10000 series router software does not support running Distance Vector Multicast Routing Protocol (DVMRP) back to back between routers.
- If you enable IP multicast fast switching on one interface, you must enable it on all outbound interfaces on the router. Failure to do so results in the router sending duplicate multicast packets out the interface that has fast switching enabled.
- Cisco 10000 series router does not support accounting for Multicast packets on Packet over SONET (POS) line cards, Gigabit Ethernet subinterfaces, and ATM AAL5 layer type.
- The Cisco 10000 series router does not support fragmentation of multicast traffic.
- The Cisco 10000 series router does not support fragmentation on Multicast Distribution Tree (MDT). To avoid fragmentation, we recommend that the value of MDT Maximum Transmission Unit (MTU) is set to a maximum of 64000.

Configuration Tasks for IP Multicast Routing

To configure basic IP multicast routing, perform the following tasks:

- Enabling IP Multicast Routing, page 15-35
- Enabling PIM on an Interface, page 15-35
- Enabling Dense Mode, page 15-35
- Enabling Sparse Mode, page 15-36
- Enabling Sparse-Dense Mode, page 15-36
- Configuring Native Multicast Load Splitting, page 15-36
- Configuring the Control Plane Protocol Policy, page 15-36

For information on other optional basic and advanced tasks, see the “IP Multicast” chapter in the *Cisco IOS IP Configuration Guide*, Release 12.2.

Enabling IP Multicast Routing

IP multicast routing allows the Cisco IOS software to forward multicast packets. To enable IP multicast routing on the Cisco 10000 router, enter the following command in global configuration mode:

Command	Purpose
`Router(config)# ip multicast-routing`	Enables IP multicast routing.

Note If you enable IP multicast fast switching on one interface, you must enable it on **all** outbound interfaces on the router. Failure to do so results in the router sending duplicate multicast packets out the interface that has fast switching enabled.

Enabling PIM on an Interface

The protocol-independent multicast (PIM) protocol maintains the current IP multicast service mode of receiver initiated membership. Enabling PIM on an interface also enables IGMP operation on that interface. Configure an interface in one of the following modes:

- Dense mode
- Sparse mode
- Sparse-dense mode

The mode determines how the Cisco 10000 router populates its multicast routing table and how it forwards multicast packets it receives from its directly connected LANs. You must enable PIM in one of these modes for an interface to perform IP multicast routing.

For more information, see the "IP Multicast" chapter in the *Cisco IOS IP Configuration Guide*, Release 12.2.

Enabling Dense Mode

To configure PIM on an interface to be in dense mode, enter the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# ip pim dense-mode`	Enables dense mode PIM on the interface.

Enabling Sparse Mode

To configure PIM on an interface to be in sparse mode, enter the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# ip pim sparse-mode`	Enables sparse mode PIM on the interface.

Enabling Sparse-Dense Mode

When you enable sparse-dense mode, the interface is treated as dense mode if the group is in dense mode. If the group is in sparse mode, the interface is treated in sparse mode. You must have a rendezvous point (RP) if the interface is in sparse-dense mode and you want to treat the group as a sparse group. For more information, see the "IP Multicast" chapter in the *Cisco IOS IP Configuration Guide*, Release 12.2.

To enable PIM to operate in the same mode as the group, enter the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# ip pim sparse-dense-mode`	Enables PIM to operate in sparse or dense mode, depending on the multicast group.

Configuring Native Multicast Load Splitting

You can configure multicast traffic from different sources to be load split across equal cost paths to take advantage of multiple paths through the network.

For more information about configuring native multicast load splitting, see the configuration document, located at the following URL:

http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_load_splt_ecmp_ps6350_TSD_Products_Configuration_Guide_Chapter.html

Note A caveat exists for Cisco 10000 series routers; you should not configure native multicast load splitting for PE devices running EIBGP, as this can result in a loss of traffic.

Configuring the Control Plane Protocol Policy

The SPT-bit is set when the receiver sucessfully builds the shortest path tree (SPT) towards the source and starts receiving packets on this path, but before that, the packets are sent along the rendezvous point tree (RPT). Setting up the SPT is accomplished by the control plane protocol (CoPP) in the rendezvous point (RP). An RP acts as the meeting place for sources and receivers of multicast data. In a PIM-SM network, sources must send their traffic to the RP. An RP is required only in networks running Protocol Independent Multicast sparse mode (PIM-SM).

To configure the CoPP policy in the Cisco 10000 series router, use the following commands:

Command	Purpose
`Router(config)# ip access-list extended acl-copp-PIM`	Creates the ACL and enters the extended ACL configuration mode.
`Router(config-ext-nacl)# permit pim any any`	Permits all PIM packets to be implicitly sent to the rendezvous point (RP).
`Router(config-ext-nacl)# permit udp any any eq 3232`	Permits all data packets that are destined for UDP port 3232. **Note** This command is used in the multicast VPN (MVPN) extranet scenario, which requires the first data packet for the (S,G) entry to be sent to the RP and not dropped.
`Router(config-ext-nacl)# end`	Exits the extended ACL configuration mode.

For more information on multicast VPN extranet support, see the *Configuring Multicast VPN Extranet Support* guide at the following url:

http://www.cisco.com/en/US/docs/ios/12_2sb/feature/guide/extvpnsb.html

Example 15-1 shows the configuration of the CoPP policy in the Cisco 10000 series router:

Example 15-1 Control Plane Protocol Policy Configuration

```
!
ip access-list extended acl-copp-PIM
 permit pim any any

!
class-map match-any copp-PIM
 match access-group name acl-copp-PIM

!
policy-map COPP
class copp-PIM
  police 64000 8000 16000 conform-action transmit exceed-action transmit

Router# show policy-map control-plane

 Control Plane

  Service-policy input: COPP

Class-map: copp-PIM (match-any)
      3261 packets, 224098 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group name acl-copp-PIM
        3261 packets, 224098 bytes
        5 minute rate 0 bps
      Police:
        64000 bps, 8000 limit, 16000 extended limit
        conformed 17 packets, 1254 bytes; action:
        transmit
        exceeded 0 packets, 0 bytes; action:
        transmit
        violated 0 packets, 0 bytes; action:
        transmit
```