IPv4 Multicast Layer 3 Features

- Prerequisites for IPv4 Multicast Layer 3 Features, page 14-1
- Restrictions for IPv4 Multicast Layer 3 Features, page 14-1
- Information About IPv4 Multicast Layer 3 Features, page 14-2
- Default Settings for IPv4 Multicast Layer 3 Features, page 14-15
- How to Configure IPv4 Multicast Layer 3 Features, page 14-15

Note

- For complete syntax and usage information for the commands used in this chapter, see these publications:

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY supports only Ethernet interfaces. Cisco IOS Release 15.1SY does not support any WAN features or commands.

Tip

For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum

Prerequisites for IPv4 Multicast Layer 3 Features

None.

Restrictions for IPv4 Multicast Layer 3 Features

IP multicast Layer 3 switching is not provided for an IP multicast flow in the following situations:

- For IP multicast groups that fall into the range 224.0.0.* (where * is in the range 0 to 255), which is used by routing protocols. Layer 3 switching is supported for groups 225.0.0.* through 239.0.0.* and 224.128.0.* through 239.128.0.*.

Note Groups in the 224.0.0.* range are reserved for routing control packets and must be flooded to all forwarding ports of the VLAN. These addresses map to the multicast MAC address range 01-00-5E-00-00-*xx*, where *xx* is in the range 0–0xFF.

- For PIM auto-RP multicast groups (IP multicast group addresses 224.0.1.39 and 224.0.1.40).
- For packets with IP options. However, packets in the flow that do not specify IP options are hardware switched.
- If a (S,G) entry for sparse mode does not have the SPT-bit, RPT-bit, or Pruned flag set.
- A (*,G) entry is not hardware switched if at least one (S,G) entry has an RPF different from the (*,G) entry's RPF and the (S,G) is not hardware switched.
- If the ingress interface of a (S,G) or (*,G) entry is null, except if the (*,G) entry is a IPv4 bidirectional PIM entry and the switch is the RP for the group.
- If you enable IP multicast Layer 3 switching, IP accounting for Layer 3 interfaces does not report accurate values. The **show ip accounting** command is not supported.

Information About IPv4 Multicast Layer 3 Features

- IPv4 Multicast Layer 3 Features Overview, page 14-2
- Distributed MRIB and MFIB Infrastructure, page 14-3
- Multicast Layer 3 Hardware Features Entries, page 14-4
- Layer 3-Switched Multicast Statistics, page 14-4
- Layer 3-Switched Multicast Packet Rewrite, page 14-5
- Replication Modes, page 14-5
- Local Egress Replication Mode, page 14-6
- PIM-SM hardware register support, page 14-6
- PIM-SM hardware SPT-switchover support, page 14-6
- Control Plane Policing (CoPP), page 14-7
- Non-RPF Traffic Processing, page 14-7
- Multicast Boundary, page 14-7
- IPv4 Bidirectional PIM, page 14-8
- Supported Multicast Features, page 14-8

IPv4 Multicast Layer 3 Features Overview

Multicast Layer 3 switching on a Supervisor Engine 2T uses application-specific integrated circuits (ASICs) to provide hardware-supported forwarding forwarding for IP multicast data packet flows between IP subnets, which offloads processor-intensive multicast forwarding and replication from the route processor.

The Policy Feature Card (PFC) and Distributed Forwarding Cards (DFCs) use the forwarding information base (FIB) and adjacency table to switch IP Multicast flows in hardware. The FIB table provides support for different entry and mask values; for example, (S/32, G/32) and (*/0, G/32). The RPF RAM is used to identify packets arriving on a directly connected subnet.

The result of a FIB lookup is an adjacency, which provides the replication list for the entry. Different from earlier supervisor engines, the Supervisor Engine 2T performs packet rewrite after replication, which provides enhanced sharing capabilities for outgoing interfaces.

Also different from earlier supervisor engines, the Supervisor Engine 2T performs Layer 2 and Layer 3 forwarding decisions separately. For a routed interface, the final LTL for a packet is determined based only on Layer 3 information. For VLAN interfaces, the LTL for the packet is determined based only on the Layer 2 lookup.

Distributed MRIB and MFIB Infrastructure

The Supervisor Engine 2T uses an MRIB- and MFIB-based software model for IPv4 multicast traffic. The MRIB/MFIB infrastructure supports multiple Layer 3 multicast protocols (for example, PIM Sparse-mode, SSM, and bidirectional PIM) for both IPv4 and IPv6 flows and provides consistent CLI for both IPv4 and IPv6 addresses.

The Multicast Routing Information Base (MRIB) is a collection of multicast entries keyed on source, group, and group mask. The multicast control plane programs the entries. An entry can have one or more associated interfaces with different flags indicating the role of the interface in the forwarding plane. On the Supervisor Engine 2T, the PFC and each DFC has an instance of the Multicast Forwarding Information Base (MFIB), which registers as a client of the MRIB. The MFIB registers its interest with the MRIB for the entries and associated flags, and maintains a local database keyed on source, group, and group mask based on MRIB updates.

Without hardware support, the MFIB would forward the multicast traffic. On the Supervisor Engine 2T, in addition to any required software forwarding, the MFIB also sends multicast route updates for the Layer 3 switching hardware tables. The communication between the MRIB, MFIB, and the Layer 3 switching hardware tables is based on the following:

- Multicast entries
- Flags set on multicast entries
- Interfaces associated with multicast entries

Note With other supervisor engines, some flows are switched partially in hardware and partially in software. With a Supervisor Engine 2T, multicast flows are switched either in software or in hardware.

Examples of mroute, MRIB, and MFIB information:

```
Router# show ip mroute
(100.1.1.3, 239.2.1.1), 00:00:53/00:02:08, flags: sTI
  Incoming interface: TenGigabitEthernet3/0, RPF nbr 0.0.0.0
  Outgoing interface list:
    TenGigabitEthernet3/1, Forward/Sparse-Dense, 00:00:51/00:02:08
    TenGigabitEthernet3/2, Forward/Sparse-Dense, 00:00:51/00:02:08
    TenGigabitEthernet3/3, Forward/Sparse-Dense, 00:00:51/00:02:08

Router# show ip mrib route
(100.1.1.3,239.2.1.1)
  TenGigabitEthernet3/1 Flags: A
  TenGigabitEthernet3/2 Flags: F
```

```
  TenGigabitEthernet3/3 Flags: F
  TenGigabitEthernet3/4 Flags: F

Router# show ip mfib
(100.1.1.3,239.2.1.1) Flags:
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   TenGigabitEthernet3/1 Flags: A
     Pkts: 0/0
   TenGigabitEthernet3/2 Flags: F
     Pkts: 0/0
   TenGigabitEthernet3/3 Flags: F
     Pkts: 0/0
   TenGigabitEthernet3/4 Flags: F
     Pkts: 0/0
```

Multicast Layer 3 Hardware Features Entries

This section describes how the PFC and the DFCs maintain Layer 3 switching information in hardware tables.

The PFC and DFC populate the (S,G) or (*,G) flows in the hardware FIB table with the appropriate masks; for example, (S/32, G/32) and (*/0, G/32). The RPF interface and the adjacency pointer information is also stored in each entry. The adjacency table contains the rewrite and a pointer to the replication entries. If a flow matches a FIB entry, the RPF check compares the incoming interface/VLAN with the entry. A mismatch is an RPF failure, which can be rate limited if this feature is enabled. In the event of a forwarding information database (FIB) fatal error, the default error action is for the system to reset and the FIB to reload.

The PFC and any DFCs run an MFIB client, which registers as a client to the MRIB on the RP. The hardware tables are programmed based on MFIB updates to install or delete entries for a traffic flow, or the addition and deletion of outgoing interfaces to an existing hardware entry.

These commands affect the Layer 3 switching entries:

- When you clear the multicast routing table using the **clear ip mroute** command, all multicast Layer 3 switching cache entries are cleared.
- When you disable IP multicast routing on the RP using the **no ip multicast-routing** command, all multicast Layer 3 switching cache entries on the PFC are purged.
- When you disable hardware-supported multicast Layer 3 switching on an interface with the **no platform multicast forwarding ip** interface mode command, flows that use the interface as the RPF interface are routed only by the RP in software.
- When you disable MFIB forwarding on an individual interface basis using the **no ip mfib forwarding ip** command, flows that use this interface as the RPF interface will not be forwarded in hardware or by MFIB.

Layer 3-Switched Multicast Statistics

While a flow is being switched in hardware, the entry is kept alive in software on the basis of the packet forwarding statistics for the flow. The MFIB entry on the PFC periodically pulls and aggregates the entry statistics from the PFC and every DFC. The statistics increment the hardware forwarding counters for an entry. A software or hardware forwarding counter increment resets the expiration timer for that multicast route.

Note A (*,G) state is created on the PIM-RP or for PIM-dense mode but is not used for forwarding the flows, and Layer 3 switching entries are not created for these flows.

Layer 3-Switched Multicast Packet Rewrite

When a multicast packet is Layer 3 switched from a multicast source to a destination multicast group, the PFC and the DFCs perform a packet rewrite that is based on information learned from the RP and stored in the adjacency table.

For example, Server A sends a multicast packet addressed to IP multicast group G1. If there are members of group G1 on VLANs other than the source VLAN, the PFC must perform a packet rewrite when it replicates the traffic to the other VLANs (the switch also bridges the packet in the source VLAN).

When the PFC receives the multicast packet, it is (conceptually) formatted as follows:

Layer 2 Frame Header		**Layer 3 IP Header**				**Data**	**FCS**
Destination	Source	Destination	Source	TTL	Checksum		
Group G1 MAC **Note** In this example, Destination B is a member of Group G1.	*Source A MAC*	*Group G1 IP*	*Source A IP*	*n*	*calculation1*		

The PFC rewrites the packet as follows:

- Changes the source MAC address in the Layer 2 frame header from the MAC address of the host to the MAC address of the RP (This is the burned-in MAC address of the system. This MAC address will be the same for all outgoing interfaces and cannot be modified. This MAC address can be displayed using the **show platform multicast statistics** command.)
- Decrements the IP header Time to Live (TTL) by one and recalculates the IP header checksum

The result is a rewritten IP multicast packet that appears to have been routed. The PFC replicates the rewritten packet onto the appropriate destination VLANs, where it is forwarded to members of IP multicast group G1.

After the PFC performs the packet rewrite, the packet is (conceptually) formatted as follows:

Frame Header		**IP Header**				**Data**	**FCS**
Destination	Source	Destination	Source	TTL	Checksum		
Group G1 MAC	*RP MAC*	*Group G1 IP*	*Source A IP*	*n–1*	*calculation2*		

Replication Modes

The Supervisor Engine 2T supports these replication modes:

- Ingress mode—The ingress module performs the replication for the egress interfaces on all modules.
- Egress mode (default)—Ingress multicast traffic is distributed over the fabric to the egress modules. The egress modules perform the replication for the egress interfaces.

The Supervisor Engine 2T performs egress-mode replication for ingress-only legacy switching modules, so that the presence of an ingress-only legacy switching module does not force a replication mode change.

Note Intranet and extranet MVPN are supported in egress and ingress replication mode.

Local Egress Replication Mode

DFC-equipped modules with dual switch-fabric connections host two packet replication engines, one per fabric connection. Each replication engine is responsible for forwarding packets to and from the interfaces associated with the switch-fabric connections. The interfaces that are associated with a switch-fabric connection are considered to be "local" from the perspective of the packet replication engine. Without local egress replication mode, both replication engines have the complete outgoing interface list for all modules, and the replication engines process and then drop traffic for nonlocal interfaces. The Supervisor Engine 2T provides local egress replication for CFC-equipped switching modules.

Local egress replication mode limits the outgoing interface list to only the local interfaces that each replication engine supports, which prevents unnecessary processing of multicast traffic.

In Cisco IOS Release 15.1SY, local egress replication mode is enabled by default.

PIM-SM hardware register support

The PIM-SM protocol requires the first-hop router for a multicast source to send a register packet to the Rendezvous Point (RP) when the source starts sending packets. On the Supervisor Engine 2T, the PIM control-plane uses the MFIB infrastructure to represent the PIM register tunnel as an interface and adds it to the outgoing interface list when PIM register packets are sent. When a new PIM RP is configured or learned, a PIM register tunnel interface is created and used for PIM register packets. The interface is deleted when a register-stop packet is received. On the RP, an additional interface is created and used to decapsulate the PIM register packet when it is received.

The Supervisor Engine 2T supports PIM register packet transmission and reception in hardware. PIM register packets are sent to the RP for the PIM registration process. CoPP can rate limit the PIM register packets sent to the RP for the PIM registration process.

PIM-SM hardware SPT-switchover support

SPT-switchover occurs in a PIM-SM network when the shortest path to the source diverges from the shortest path to the RP for a multicast group. During the transition from the shortest path tree to a source based tree, packets are received on both the shared and source tree and the multicast entry must be programmed to accept packets from two interfaces.

Hardware support is implemented with a multicast FIB dual-RPF mode. When a multicast FIB entry is programmed with a dual-RPF, packets received on the RPF towards the RP are forwarded and packets received on the RPF towards the source are sent to be processed in software for the PIM protocol to complete the SPT-switchover. After switching to the source tree, the multicast entry transitions back to a single RPF interface. To avoid excessive CPU utilization during the switchover process, you can configure CoPP to rate limit multicast packets sent to the RP during SPT-switchover.

Control Plane Policing (CoPP)

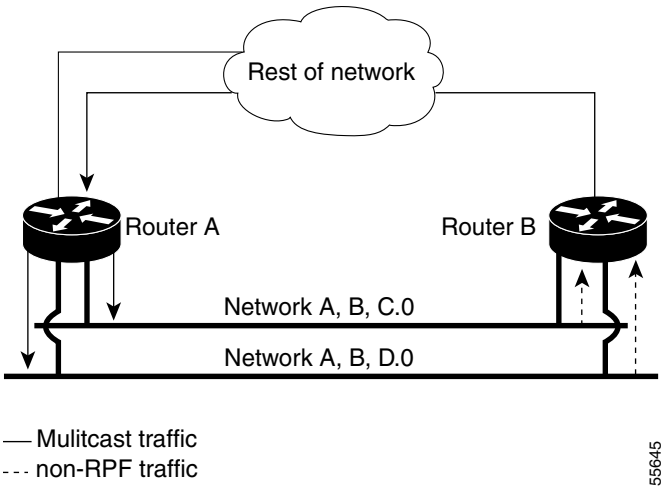
You can configure CoPP to protect the CPU from unnecessary or DoS traffic. With Cisco IOS Release 15.1SY, CoPP is configured and enabled by default. CoPP provides hardware rate limiting for the packets sent to the CPU for processing in software. Although multicast rate-limiters are still supported, CoPP is more efficient.

Note For any particular type of traffic, configure CoPP or a rate limiter, not both.

Non-RPF Traffic Processing

In a redundant configuration where multiple routers connect to the same LAN segment, only one router forwards the multicast traffic from the source to the receivers on the outgoing interfaces (see Figure 14-1). In this kind of topology, only the PIM designated router (PIM DR) forwards the data in the common VLAN, but the non-PIM DR receives the forwarded multicast traffic. The redundant router (non-PIM DR) must drop this traffic because it has arrived on the wrong interface and fails the RPF check. Traffic that fails the RPF check is called non-RPF traffic.

Figure 14-1 Redundant Multicast Router Configuration in a Stub Network



Non-RPF protection, which is enabled by default, keeps the CPU from being overwhelmed with non-RPF traffic while still allowing some packets to reach the CPU to support correct multicast routing protocol operation. The non-RPF protection feature uses a leak and drop mechanism: a non-RPF packet is leaked to the CPU, and subsequent non-RPF packets are dropped. The sequence repeats periodically.

Multicast RPF-fail packets that conform to the configured CoPP policy reach the CPU. Nonconforming packets are dropped. Rate limiting is configured in the CoPP policy.

Multicast Boundary

The multicast boundary feature allows you to configure an administrative boundary for multicast group addresses. By restricting the flow of multicast data packets, you can reuse the same multicast group address in different administrative domains.

You configure the multicast boundary on an interface. A multicast data packet is blocked from flowing across the interface if the packet's multicast group address matches the access control list (ACL) associated with the multicast boundary feature.

Multicast boundary ACLs can be processed in hardware by the Policy Feature Card (PFC), a Distributed Forwarding Card (DFC), or in software by the RP. The multicast boundary ACLs are programmed to match the destination address of the packet. These ACLs are applied to traffic on the interface in both directions (input and output).

To support multicast boundary ACLs in hardware, the switch creates new ACL TCAM entries or modifies existing ACL TCAM entries (if other ACL-based features are active on the interface). To verify TCAM resource utilization, enter the **show tcam counts ip** command.

If you configure the **filter-autorp** keyword, the administrative boundary also examines auto-RP discovery and announcement messages and removes any auto-RP group range announcements from the auto-RP packets that are denied by the boundary ACL.

IPv4 Bidirectional PIM

The PFC and DFCs support hardware forwarding of IPv4 bidirectional PIM groups. To support IPv4 bidirectional PIM groups, the PFC and DFCs support the designated forwarder (DF) mode. The designated forwarder is the router elected to forward packets to and from a segment for a IPv4 bidirectional PIM group. In DF mode, the switch accepts packets from the RPF and from the DF interfaces.

When the switch is forwarding IPv4 bidirectional PIM groups, the RPF interface is always included in the outgoing interface list of (*,G) entry, and the DF interfaces are included depending on IGMP/PIM joins.

If the route to the RP becomes unavailable, the group is changed to dense mode. Should the RPF link to the RP become unavailable, the IPv4 bidirectional PIM flow is removed from the hardware FIB.

For information on configuring IPv4 bidirectional PIM, see the "Configuring IPv4 Bidirectional PIM" section on page 14-26.

Supported Multicast Features

- Hardware-Supported IPv4 Layer 3 Features, page 14-9
- Unsupported IPv4 Layer 3 Features, page 14-10
- Hardware-Supported IPv6 Layer 3 Multicast Features, page 14-11
- Partially Hardware-Supported IPv6 Layer 3 Multicast Features, page 14-11
- Software-Supported IPv6 Layer 3 Multicast Features, page 14-11
- Unsupported IPv6 Layer 3 Multicast Features, page 14-12
- Hardware-Supported Layer 2 Common Multicast Features, page 14-12
- Unsupported Layer 2 Common Multicast Features, page 14-12
- Hardware-Supported Layer 2 Enterprise Multicast Features, page 14-13
- Unsupported Layer 2 Enterprise Multicast Features, page 14-13
- Hardware-Supported Layer 2 Metro Multicast Features, page 14-13
- Unsupported Layer 2 Metro Multicast Features, page 14-13

- Unsupported MPLS Multicast Features, page 14-14
- Hardware-Supported Security Multicast Features, page 14-14
- Software-Supported Security Multicast Features, page 14-14
- Unsupported Security Multicast Features, page 14-14

Hardware-Supported IPv4 Layer 3 Features

- Control plane policing (CoPP)
- Egress forced replication mode
- Egress replication local
- Egress replication mode
- HW assisted SPT switchover
- Input ACL logging
- Input and output ACL filtering
- IPv4 multicast over multipoint IPv4 GRE tunnel
- IPv4 multicast over P2P IPv4 GRE tunnel
- IPv4 multicast over P2P IPv4 GRE tunnel with tunnel endpoints in VRF
- IPv4 multicast over P2P IPv4 VRF GRE tunnel
- Load-Balancing of multicast packets on port-channels
- Multicast boundary
- Multicast Layer 3 forwarding on routed ports
- Multicast Layer 3 forwarding on subinterfaces
- Multicast Layer 3 forwarding on SVI
- Multicast load-splitting across parallel links
- Multicast VPN for IPv4 extranet support
- Multicast VPN for IPv4 intranet support
- Multicast VRF-lite
- MVPN over P2P IPv4 GRE tunnel
- Netflow accounting
- Non-RPF protection
- PIM Register decapsulation over IPv4
- PIM Register encapsulation over IPv4
- PIM-DM (S,G) forwarding
- PIM-SM (S,G) and (*,G) forwarding
- PIM-SSM
- QoS policing for ingress mode
- Rate limiters
- Statistics

- UDLR - unidirectional link routing
- URD - URL rendezvous directory
- Partially Hardware-Supported IPv4 Layer 3 Features
- Egress replication mode and QoS marking
- QoS marking for ingress mode
- Software-Supported IPv4 Layer 3 Features
- IGMPv3/v2/v1
- MET sharing
- MRM/mrinfo/mmon
- MSDP/MBGP
- Mtrace/Mping
- PGM router assist
- PGM router assist in VRF
- Platform Dependent MIB support
- Platform Independent MIB support
- SSM Mapping
- SSO/NSF

Unsupported IPv4 Layer 3 Features

- 6PE IPv6 over IPv4 infrastructure (using MDT tunnels)
- Destination IP NAT multicast
- MTR multicast ToS-based lookup
- Multicast stub (Supported in 12.2SX)
- Partial shortcut (Supported in 12.2SX)
- Service reflect
- Source IP NAT multicast
- Egress replication mode and QoS policing
- Output ACL logging
- QoS ingress or egress shaping
- QoS marking for multicast bridged frames undergoing routing
- DVMRP interoperability (supported in Release 12.2SX)
- ISSU/MDR
- MFIB consistency checker
- MFIB to HW consistency checker
- MTR multicast: separate RPF table for group range
- MTR multicast: separate URIB RPF table
- Multicast helper map (supported in Release12.2SX)

- RPF change tracking
- The **ip multicast rate-limit** command (supported in Release 12.2SX)
- The **ip multicast ttl-threshold** command (supported in Release 12.2SX)

Hardware-Supported IPv6 Layer 3 Multicast Features

- Control plane policing (CoPP)
- Egress forced replication mode
- Egress replication local
- Egress replication mode
- HW assisted SPT switchover
- Input ACL logging
- Input and output ACL filtering
- IPv6 Multicast over P2P IPv4 GRE/IP-in-IP tunnel (6over4)
- Load-Balancing of multicast packets on port-channels
- Multicast Layer 3 forwarding on routed ports
- Multicast Layer 3 forwarding on subinterfaces
- Multicast Layer 3 forwarding on SVI
- Multicast load-splitting across parallel links
- Netflow accounting
- Non-RPF protection
- PIM register decapsulation over IPv6
- PIM register encapsulation over IPv6
- PIM-SM (S,G) and (*,G) forwarding
- PIM-SSM
- QoS ingress mode marking
- QoS ingress mode policing
- Rate limiters
- Scope checking
- Statistics

Partially Hardware-Supported IPv6 Layer 3 Multicast Features

- Egress replication mode and QoS marking

Software-Supported IPv6 Layer 3 Multicast Features

- SSM mapping
- MET sharing
- MLDv1/v2

Unsupported IPv6 Layer 3 Multicast Features

- BIDIR PIM over P2P GRE tunnel
- Destination IP NAT multicast
- IPv4 multicast over P2P IPv6 GRE tunnel (4over6)
- IPv6 multicast over multipoint IPv4 GRE tunnel (6over4 mGRE)
- IPv6 multicast over multipoint IPv6 GRE tunnel
- IPv6 multicast over P2P IPv6 GRE tunnel
- IPv6 multicast over P2P IPv6 GRE tunnel with tunnel endpoints in VRF
- IPv6 multicast over P2P IPv6 VRF GRE tunnel
- MTR multicast: TOS based lookup
- Multicast VPN for IPv6 extranet support
- Multicast VPN for IPv6 intranet support
- Multicast VRF-lite
- MVPN over P2P IPv6 GRE tunnel
- PIM-DM (S,G) forwarding
- Source IP NAT multicast
- Egress replication mode and QoS policing
- QoS ingress and egress: shaping support
- MIB support
- Multicast boundary
- Multicast helper map
- Output ACL logging
- PGM router assist
- PGM router assist in VRF
- PIM-BIDIR
- QoS Marking for multicast bridged frames undergoing routing

Hardware-Supported Layer 2 Common Multicast Features

- NSF/SSO support for IGMP/PIM/MLD snooping

Unsupported Layer 2 Common Multicast Features

- ISSU/MDR support for IGMP/PIM/MLD snooping
- MIB support

Hardware-Supported Layer 2 Enterprise Multicast Features

- IGMPv2/v1 snooping - IP based constrain
- IGMPv2/v1 snooping - MAC based constrain
- IGMPv3 snooping with S,G constrain
- MLD v1 snooping - IP based constrain
- MLD v1 snooping - MAC based constrain
- MLD v2 snooping - IP based constrain
- MLD v2 snooping - MAC based constrain
- Multicast support for PVLAN over BD
- Optimized flooding for unknown IP multicast frames
- PIM snooping - IP based constrain
- PIM snooping - MAC based constrain
- IGMP snooping querier
- IGMPv3 snooping Explicit tracking
- MLD snooping querier
- PIM snooping - DR flooding

Unsupported Layer 2 Enterprise Multicast Features

- RGMP
- Source-Only detection
- Multicast Flood Protection
- CGMP compatibility mode for IGMP snooping
- CGMP redirect suppression

Hardware-Supported Layer 2 Metro Multicast Features

- Multicast VLAN Registration (MVR)

Unsupported Layer 2 Metro Multicast Features

- MLD v1/v2 snooping over Q-in-Q tagged frames
- Optimizied VPLS multicast constrains on LAN ports
- PIM snooping over Q-in-Q
- IGMPv3/v2/v1 snooping over Q-in-Q tagged frames
- MTP multicast optimization
- Multicast routing for BD with EOM

Unsupported MPLS Multicast Features

- Inter-AS IPv4 Multicast VPN using mLDP
- Inter-AS IPv6 Multicast VPN using mLDP
- IPv4 Multicast Traffic at the Edge (via Global routing table) using mLDP
- IPv4 Multicast Traffic at the Edge (via Global routing table) over a P2MP RSVP TE LSP
- IPv4 Multicast Traffic in a VRF over a P2MP RSVP TE LSP
- IPv4 Multicast Traffic in a VRF using mLDP
- IPv6 Multicast Traffic at the Edge (via Global routing table) using mLDP
- IPv6 Multicast Traffic at the edge (via Global routing table) over a P2MP RSVP TE LSP
- IPv6 Multicast Traffic in a VRF over a P2MP RSVP TE LSP
- IPv6 Multicast Traffic in a VRF using mLDP
- ISSU Support
- Link protection for P2MP TE LSPs (500 msec)
- Node protection for P2MP TE LSPs (500 msec)
- SSO/NSF Support
- Carrier Supporting Carrier (CSC) for IPv4 Multicast VPN using mLDP
- Carrier Supporting Carrier (CSC) for IPv6 Multicast VPN using mLDP
- Extranet support for IPv4 Multicast VPN for Label Switched Multicast
- Extranet support for IPv6 Multicast VPN for Label Switched Multicast
- Link protection for mLDP trees (500 msec)
- Node protection for mLDP trees (500 msec)
- MIB support

Hardware-Supported Security Multicast Features

- Multicast and service blade interaction
- P2P GRE tunnel and VPNSM/IPSEC SPA module interaction

Software-Supported Security Multicast Features

- IGMP Snooping filtering

Unsupported Security Multicast Features

- CTS LinkSecurity for multicast
- RBACL and IPv4/IPv6 multicast data packets
- CTS implicit tunnel for multicast
- GDOI key distribution

Default Settings for IPv4 Multicast Layer 3 Features

- Multicast routing: disabled globally.
- PIM routing: disabled on all interfaces.
- IP multicast Layer 3 switching: enabled when multicast routing is enabled and PIM is enabled on the interface.
- IP MFIB forwarding: enabled when PIM is enabled on the interface.

Internet Group Management Protocol (IGMP) snooping is enabled by default on all VLAN interfaces. If you disable IGMP snooping on an interface, multicast Layer 3 flows are still switched by the hardware. Bridging of the flow on an interface with IGMP snooping disabled causes flooding to all forwarding interfaces of the VLAN. For details on configuring IGMP snooping, see Chapter 15, "IGMP Snooping for IPv4 Multicast Traffic."

How to Configure IPv4 Multicast Layer 3 Features

- Enabling IPv4 Multicast Routing Globally, page 14-16
- Enabling IPv4 PIM on Layer 3 Interfaces, page 14-16
- Enabling IP Multicast Layer 3 Switching on Layer 3 Interfaces, page 14-16
- Enabling IP MFIB forwarding on Layer 3 Interfaces, page 14-17
- Configuring the Replication Mode, page 14-18
- Configuring Multicast Boundary, page 14-18
- Verifying Local Egress Replication, page 14-19
- Displaying IPv4 Multicast PIM-SM register tunnel information, page 14-20
- Displaying the IPv4 Multicast Routing Table, page 14-20
- Displaying IPv4 MRIB Information, page 14-21
- Displaying IPv4 MFIB Information, page 14-22
- Viewing Directly Connected Entries, page 14-23
- Displaying IPv4 Hardware Switching Information, page 14-24
- Displaying IPv4 CoPP Information, page 14-25
- Source-Specific Multicast with IGMPv3, IGMP v3lite, and URD, page 14-26
- Configuring IPv4 Bidirectional PIM, page 14-26
- Enabling IPv4 Bidirectional PIM Globally, page 14-27
- Configuring the Rendezvous Point for IPv4 Bidirectional PIM Groups, page 14-27
- Displaying IPv4 Bidirectional PIM Information, page 14-27
- Using IPv4 Debug Commands, page 14-31
- Redundancy for Multicast Traffic, page 14-31

Enabling IPv4 Multicast Routing Globally

You must enable IP multicast routing globally before you can enable IP multicast Layer 3 switching on Layer 3 interfaces.

To enable IP multicast routing globally, perform this task:

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

This example shows how to enable multicast routing globally:

```
Router(config)# ip multicast-routing
Router(config)#
```

Enabling IPv4 PIM on Layer 3 Interfaces

You must enable PIM on the Layer 3 interfaces before IP multicast Layer 3 switching functions on those interfaces.

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

	Command	Purpose
Step 1	`Router(config)# interface {{vlan vlan_ID} | {type slot/port}}`	Selects an interface to configure.
Step 2	`Router(config-if)# ip pim {dense-mode | sparse-mode | sparse-dense-mode}`	Enables IP PIM on a Layer 3 interface.

This example shows how to enable PIM on an interface using the default mode (**sparse-dense-mode**):

```
Router(config-if)# ip pim
```

This example shows how to enable PIM sparse mode on an interface:

```
Router(config-if)# ip pim sparse-mode
```

Note

- You must enable PIM on all participating Layer 3 interfaces before IP multicast Layer 3 switching will function. For information on configuring PIM on Layer 3 interfaces, see the "Enabling IPv4 PIM on Layer 3 Interfaces" section on page 14-16.
- PIM can be enabled on any Layer 3 interface, including VLAN interfaces.

Enabling IP Multicast Layer 3 Switching on Layer 3 Interfaces

IP multicast Layer 3 switching is enabled by default on the Layer 3 interface when you enable PIM on the interface. Perform this task only if you disabled IP multicast Layer 3 switching on the interface and you want to reenable it.

To enable IP multicast Layer 3 switching on a Layer 3 interface, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {{vlan vlan_ID} | {type slot/port}}`	Selects an interface to configure.
Step 2	`Router(config-if)# platform multicast forwarding ip`	Enables IP multicast Layer 3 switching on a Layer 3 interface.
Step 3	`Router(config-if)# exit`	Returns you to global configuration mode.
Step 4	`Router # platform ip multicast syslog`	(Optional) Enables display of multicast related syslog messages on console.

This example shows how to enable IP multicast Layer 3 switching on a Layer 3 interface:

```
Router(config-if)# platform multicast forwarding ip
Router(config-if)#
```

Enabling IP MFIB forwarding on Layer 3 Interfaces

Disabling MFIB forwarding on the interface is another way to disable IP multicast Layer 3 switching for an interface. By default MFIB forwarding in and out are enabled by when PIM is enabled on the interface. To enable MFIB forwarding on a Layer 3 interface, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {{vlan vlan_ID} | {type slot/port}}`	Selects an interface to configure.
Step 2	`Router(config-if)# ip mfib forwarding in`	Enables MFIB forwarding on a Layer 3 interface.
Step 3	`Router(config-if)# exit`	Returns you to global configuration mode.
Step 4	`Router # [no] platform ip multicast syslog`	(Optional) Enables display of multicast related syslog messages on console.

This example shows how to enable MFIB forwarding on a Layer 3 interface:

```
Router(config-if)# ip mfib forwarding in
Router(config-if)#
```

Configuring the Replication Mode

The default for Cisco IOS Release 15.1SY is egress replication mode. Egress replication mode is always supported because the Supervisor Engine 2T provides egress replication for ingress-only legacy switching modules. Modules installed or added do not constrain the replication mode. You can change the configured replication mode.

To configure the replication mode, perform this task:

Command	Purpose
`Router(config)# [no] platform ip multicast routing replication egress`	Configures the replication mode. • The **platform multicast routing replication egress** command configures egress replication mode. • The **no platform multicast routing replication egress** command configures ingress replication mode. • Changing the replication mode might interrupt traffic.

This example shows how to configure ingress replication mode:

```
Router(config)# no platform multicast routing replication egress
```

This example shows how to display the replication mode:

```
Router# show platform  multicast routing replication
Current mode of replication is Ingress
Configured mode of replication is Ingress

Slot                Multicast replication capability
 2                            Egress
 5                            Egress
```

Configuring Multicast Boundary

To configure a multicast boundary, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {{vlan` *vlan_ID*`} | {`*type slot/port*`} | {port-channel` *number*`}}`	Selects an interface to configure.
Step 2	`Router(config-if)# ip multicast boundary` *access_list* `[filter-autorp]`	Enables an administratively scoped boundary on an interface. • For *access_list*, specify the access list that you have configured to filter the traffic at this boundary. • (Optional) Specify **filter-autorp** to filter auto-RP messages at this boundary.

Note If you configure the **filter-autorp** keyword, the administrative boundary examines auto-RP discovery and announcement messages and removes any auto-RP group range announcements from the auto-RP packets that are denied by the boundary ACL. An auto-RP group range announcement is permitted and passed by the boundary only if all addresses in the auto-RP group range are permitted by the boundary ACL. If any address is not permitted, the entire group range is filtered and removed from the auto-RP message before the auto-RP message is forwarded.

The following example sets up a multicast boundary for all administratively scoped addresses:

```
Router (config)# access-list 1 deny 239.0.0.0 0.255.255.255
Router (config)# access-list 1 permit 224.0.0.0 15.255.255.255
Router (config)# interface gigabitethernet 5/2
Router (config-if)# ip multicast boundary 1
```

Verifying Local Egress Replication

DFC-equipped modules with dual switch-fabric connections host two packet replication engines, one per fabric connection. Each replication engine is responsible for forwarding packets to and from the interfaces associated with the switch-fabric connections. The interfaces that are associated with a switch-fabric connection are considered to be “local” from the perspective of the packet replication engine. When local egress replication mode is not enabled, both replication engines have the complete outgoing interface list for all modules, and the replication engines process and then drop traffic for nonlocal interfaces.

Local egress replication mode limits the outgoing interface list to only the local interfaces that each replication engine supports, which prevents unnecessary processing of multicast traffic.

Local egress replication is supported with the following software configuration and hardware:

- Egress replication mode.
- Dual fabric-connection DFC-equipped modules.
- CFC-equipped modules (functionality provided by the Supervisor Engine 2T).
- Members of Layer 3 EtherChannels and VLAN interfaces.

This example shows how to verify the replication engine selected for local egress replication:

```
Router# show platform multicast routing replication
Current mode of replication is Ingress
Configured mode of replication is Ingress

Slot                Multicast replication capability
 2                            Egress
 5                            Egress
```

Displaying IPv4 Multicast PIM-SM register tunnel information

To view the register tunnel interfaces associated with a PIM RP, enter the **show ip pim tunnel** command.

Command	Purpose
`Router# show ip pim rp mapping`	Displays PIM RP information.
`Router# show ip pim tunnel`	Displays PIM register encapsulation tunnel information on all routers. Displays additional PIM register decapsulation tunnel on the RP.

This example shows how to display the PIM register tunnel information:

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings

Group(s): 224.0.0.0/4, Static
    RP: 11.1.1.1 (?)

Router# show ip pim tunnel
Tunnel0
  Type  : PIM Encap
  RP    : 11.1.1.1*
  Source: 11.1.1.1
Tunnel1*
  Type  : PIM Decap
  RP    : 11.1.1.1*
  Source: -
```

Displaying the IPv4 Multicast Routing Table

To view a mroute entry, enter the **show ip mroute** command.

Command	Purpose
`Router# show ip mroute [hostname | group_number]`	Displays the IP multicast routing table.

This example shows how to display the IP multicast routing table:

```
Router# show ip mroute 225.1.1.1
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, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
```

```
(*, 225.1.1.1), 00:25:35/00:02:52, RP 11.1.1.1, flags: SJC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet1/4, Forward/Sparse-Dense, 00:21:43/00:02:52
    Vlan546, Forward/Sparse-Dense, 00:25:36/00:02:51

(22.2.2.1, 225.1.1.1), 00:25:36/00:01:49, flags: T
  Incoming interface: Vlan546, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet1/4, Forward/Sparse-Dense, 00:21:46/00:03:24
```

Displaying IPv4 MRIB Information

The **show ip mrib** command displays detailed information about IP MRIB. To display detailed MRIB information, perform one of these tasks:

Command	Purpose
Router# **show ip mrib client**	Displays the clients registered with MRIB.
Router# **show ip mrib route** [*hostname* | *group_number* | **summary** | **reserved**]	Displays the MRIB route information.

To view the MRIB clients, enter the **show ip mrib** client command. MFIB running on the PFC and each DFC must present as clients of the MRIB. This example shows how to display the MRIB clients:

```
Router# show ip mrib client
IP MRIB client-connections
MRIB Trans for MVRF #0     table:434    (connection id 1)
IPv4_mfib(0x57D354C8):6.642     (connection id 2)
IPv4_mfib(0x555FC7D8):1.362     (connection id 3)
```

This example shows how to display the MRIB table:

```
Router# show ip mrib route 225.1.1.1
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
    ET - Data Rate Exceeds Threshold,K - Keepalive,DDE - Data Driven Event
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, MD - mCAC Denied

(*,225.1.1.1) RPF nbr: 0.0.0.0 Flags: C
  Tunnel1 Flags: A
  GigabitEthernet1/4 Flags: F NS
  Vlan546 Flags: F NS

(22.2.2.1,225.1.1.1) RPF nbr: 0.0.0.0 Flags:
  Vlan546 Flags: A
  GigabitEthernet1/4 Flags: F NS
```

Displaying IPv4 MFIB Information

The **show ip mfib** command displays detailed information about IP MFIB. To display detailed MFIB information, perform one of these tasks:

Command	Purpose
Router# **show ip mfib interface** [*type name*]	Displays MFIB interface information
Router# **show ip mfib** [*hostname* | *group_number* | **global** | **verbose**]	Displays the MFIB route information.
Router# **show ip mfib summary**	Displays a summary of MFIB state
Router# **show ip mfib status**	Displays MFIB status
Router# **show ip mfib count**	Displays route and packet count data

This example shows how to display the MFIB interface information:

```
Router# show ip mfib interface
IPv4 Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
    Initialization State: Running
    Total signalling packets queued: 0
    Process Status: may enable - 3 - pid 642
    Tables 1/1/0 (active/mrib/io)

MFIB interface             status    CEF-based output
                                   [configured,available]
GigabitEthernet1/1         up      [yes       ,no       ]
GigabitEthernet1/2         up      [yes       ,no       ]
GigabitEthernet1/4         up      [yes       ,yes      ]
Loopback1                  up      [yes       ,yes      ]
Tunnel0                    up      [yes       ,yes      ]
Tunnel1                    up      [yes       ,no       ]
Vlan546                    up      [yes       ,yes      ]
```

This example shows how to display the MFIB table:

```
Router# show ip mfib 225.1.1.1
Entry Flags:    C - Directly Connected, S - Signal, IA - Inherit A flag,
                ET - Data Rate Exceeds Threshold, K - Keepalive
                DDE - Data Driven Event, HW - Hardware Installed
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
                MA - MFIB Accept
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   FS Pkt Count/PS Pkt Count
Default
 (*,225.1.1.1) Flags: C HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: 0/0/0
   Tunnel1 Flags: A
   GigabitEthernet1/4 Flags: F NS
     Pkts: 0/0
   Vlan546 Flags: F NS
     Pkts: 0/0
 (22.2.2.1,225.1.1.1) Flags: HW
   SW Forwarding: 0/0/0/0, Other: 37/0/37
```

```
   HW Forwarding:   536649628/234964/512/939858, Other: 0/0/0
   Vlan546 Flags: A
   GigabitEthernet1/4 Flags: F NS
     Pkts: 0/0
```

This example shows how to display the MFIB summary:

```
Router# show ip mfib summary
Default
 211 prefixes (211/0/0 fwd/non-fwd/deleted)
 343 ioitems (343/0/0 fwd/non-fwd/deleted)
 Forwarding prefixes: [101 (S,G), 108 (*,G), 2 (*,G/m)]
 Table id 0x0, instance 0x57D354C8
 Database: epoch 2
```

This example shows how to display the MFIB status:

```
Router# show ip mfib status
IPv4 Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
    Initialization State: Running
    Total signalling packets queued: 0
    Process Status: may enable - 3 - pid 642
    Tables 1/1/0 (active/mrib/io)
```

This example shows how to display the MFIB count:

```
Router# show ip mfib count
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:      Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Default
 211 routes, 108 (*,G)s, 2 (*,G/m)s
Group: 224.0.0.0/4
  RP-tree,
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
  RP-tree,
   SW Forwarding: 0/0/0/0, Other: 0/0/0
Group: 225.1.1.1
  RP-tree,
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: 0/0/0
  Source: 22.2.2.1,
   SW Forwarding: 0/0/0/0, Other: 37/0/37
   HW Forwarding:   38970288942/234961/512/939847, Other: 0/0/0
  Totals - Source count: 1, Packet count: 38970288942
```

Viewing Directly Connected Entries

This example shows how to display the directly connected subnet entries:

```
Router# show platform  hardware  cef | include receive
224    0.0.0.0/32            receive
225    255.255.255.255/32    receive
226    22.2.2.2/32           receive
227    22.2.2.0/32           receive
228    22.2.2.255/32         receive
229    10.10.10.10/32        receive
230    11.1.1.1/32           receive
231    11.1.1.0/32           receive
232    11.1.1.255/32         receive
```

```
3200   224.0.0.0/24          receive
198433 224.0.0.0/4           receive
```

Displaying IPv4 Hardware Switching Information

The **show platform hardware multicast routing ip** command displays detailed information about IP multicast Layer 3 switching. To display detailed IP multicast Layer 3 switching information, perform one of these tasks:

Command	Purpose
Router# **show platform hardware multicast routing ip control**	Displays Layer 3 IP multicast control entries.
Router# **show platform hardware multicast routing ip** [**source** *ip_address*] [**group** *ip_address* [**detail** | **verbose**]]	Displays IP multicast Layer 3 switching details for all interfaces.
Router# **show platform ip multicast summary**	Displays a summary of IP multicast Layer 3 switching information.

This example shows how to display the Layer 3 IP multicast control entries:

```
Router# show platform  hardware multicast routing ip control
IPv4 Multicast CEF Entries for VPN#0
Flags: C - Control, B - Bidir, c - CoPP ELIF, Q - QoS ELIF, n - Non-primary Input
Source          Destination/mask         RPF/DF      Flags  #packets     #bytes
Output LIFs/Info
+--------------+--------------------+----------------+------+-----------+----------------
--+---------------------------+
*                   224.0.0.0/24        -              C      -           -
*                   224.0.1.39/32       -              C      -           -
*                   224.0.1.40/32       -              C      -           -
Found 3 entries.
```

This example shows how to display the Layer 3 IP multicast switching information:

```
Router# show platform  hardware multicast routing ip source 22.2.2.1 group 225.1.1.1 de
IPv4 Multicast CEF Entries for VPN#0

(22.2.2.1, 225.1.1.1/32)
  FIBAddr: 0x20 IOSVPN: 0 RpfType:  SglRpfChk SrcRpf: Vl546
  CPx: 0 s_star_pri: 1 non-rpf drop: 0

  PIAdjPtr: 0x1C001 Format: IP rdt: off elif: 0xC5409
  fltr_en: off idx_sel/bndl_en: 0 dec_ttl: on mtu_idx: 2(1518)
  PV: 1 rwtype: MCAST_L3_REWRITE
  met3: 0x8000 met2: 0x0
  Packets: 0            Bytes: 0

  NPIAdjPtr: 0x1C002 Format: IP rdt: off elif: 0xC5409
  fltr_en: off idx_sel/bndl_en: 0 dec_ttl: off
  PV: 0 rwtype: NO_REWRITE
  smac_rwt: 0 ip_to_mac: 1
  Packets: 0            Bytes: 0
  MET offset: 0x8000
         OIF          AdjPtr      Elif        CR
    +-------------+----------+-----------+--------+
     EDT-2C001      0x2C001    0x8400A      6T1/T2
Found 1 entries.
```

This example shows how to display the Layer 3 IP multicast switching summary:

```
Router# show platform  hardware multicast routing ip summary
IPv4 Multicast CEF Entries Summary for VPN#0
 Slot     #shcut       #(S,G)       #(*,G)       #(*,G/m)       #Ctrl
+-----+-----------+-----------+-----------+-----------+-----------+
 6         203          101          101          1             3
```

Displaying IPv4 CoPP Information

The following commands can be used to check the multicast CoPP information:

Command	Purpose
`Router# show platform hardware multicast routing ip control`	Displays Layer 3 IP multicast control entries.
`Router# show policy-map control-plane input class` *class_name*	Displays class-map information for the control-plane policy.

This example shows how to display CoPP information:

```
Router# show platform  hardware  multicast  routing  ip control detail
IPv4 Multicast CEF Entries for VPN#0

(*, 224.0.0.0/24)
  FIBAddr: 0x2A0 IOSVPN: 0 RpfType: SkipRpf SrcRpf:
  CPx: 0 s_star_pri: 1 non-rpf drop: 0

  PIAdjPtr: 0x13110(IPv4 Control) Format: IP rdt: off elif: 0x9FC01
  fltr_en: off idx_sel/bndl_en: 0 dec_ttl: off mtu_idx: 0(9234)
  PV: 1 rwtype: NO_REWRITE
  smac_rwt: 0 ip_to_mac: 0

(*, 224.0.1.39/32)
  FIBAddr: 0x1E0 IOSVPN: 0 RpfType: SkipRpf SrcRpf:
  CPx: 0 s_star_pri: 1 non-rpf drop: 0

  PIAdjPtr: 0x13110(IPv4 Control) Format: IP rdt: off elif: 0x9FC01
  fltr_en: off idx_sel/bndl_en: 0 dec_ttl: off mtu_idx: 0(9234)
  PV: 1 rwtype: NO_REWRITE
  smac_rwt: 0 ip_to_mac: 0

(*, 224.0.1.40/32)
  FIBAddr: 0x1E2 IOSVPN: 0 RpfType: SkipRpf SrcRpf:
  CPx: 0 s_star_pri: 1 non-rpf drop: 0

  PIAdjPtr: 0x13110(IPv4 Control) Format: IP rdt: off elif: 0x9FC01
  fltr_en: off idx_sel/bndl_en: 0 dec_ttl: off mtu_idx: 0(9234)
  PV: 1 rwtype: NO_REWRITE
  smac_rwt: 0 ip_to_mac: 0
Found 3 entries.
```

```
Router# show policy-map control-plane input class class-copp-match-igmp

 Control Plane Interface

  Service-policy input: policy-default-autocopp

  Hardware Counters:

    class-map: class-copp-match-igmp (match-any)
      Match: access-group name acl-copp-match-igmp
      police :
        10000 pps 10000 limit 10000 extended limit
      Earl in slot 6 :
        0 packets
        5 minute offered rate 0 pps
        aggregate-forwarded 0 packets
                             action: set-discard-class-transmit
        exceeded 0 packets action: transmit
        aggregate-forward 0 pps exceed 0 pps

  Software Counters:

    Class-map: class-copp-match-igmp (match-any)
      7138 packets, 267084 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name acl-copp-match-igmp
        7138 packets, 267084 bytes
        5 minute rate 0 bps
      police:
          rate 10000 pps, burst 10000 packets
          conformed 7138 packets, 7138 bytes; action:
            set-discard-class-transmit 48
          exceeded 0 packets, 0 bytes; action:
            transmit
          conformed 0 pps, exceeded 0 pps
```

Source-Specific Multicast with IGMPv3, IGMP v3lite, and URD

For complete information and procedures about source-specific multicast (SSM) with IGMPv3, IGMP v3lite, and URL Rendezvous Directory (URD), see this URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_igmp/configuration/15-sy/imc-igmp-15-sy-book.html

Configuring IPv4 Bidirectional PIM

- Enabling IPv4 Bidirectional PIM Globally, page 14-27
- Configuring the Rendezvous Point for IPv4 Bidirectional PIM Groups, page 14-27
- Displaying IPv4 Bidirectional PIM Information, page 14-27

Enabling IPv4 Bidirectional PIM Globally

To enable IPv4 bidirectional PIM, perform this task:

Command	Purpose
`Router(config)# ip pim bidir-enable`	Enables IPv4 bidirectional PIM globally on the switch.

This example shows how to enable IPv4 bidirectional PIM on the switch:

```
Router(config)# ip pim bidir-enable
Router(config)#
```

Configuring the Rendezvous Point for IPv4 Bidirectional PIM Groups

To statically configure the rendezvous point for an IPv4 bidirectional PIM group, perform this task:

	Command	Purpose
Step 1	`Router(config)# ip pim rp-adress` *ip_address access_list* [**override**]	Statically configures the IP address of the rendezvous point for the group. When you specify the **override** option, the static rendezvous point is used.
Step 2	`Router(config)# access-list` *access-list* [**permit** | **deny**] *ip_address*	Configures an access list.
Step 3	`Router(config)# ip pim send-rp-announce` *type number* **scope** *ttl_value* [**group-list** access-list] [**interval** seconds] [**bidir**]	Configures the system to use auto-RP to configure groups for which the router will act as a rendezvous point (RP).
Step 4	`Router(config)# ip access-list standard` *access-list-name* **permit** | **deny** *ip_address*	Configures a standard IP access list.
Step 5	`Router(config)# platform ip multicast`	Enables hardware-supported IP multicast.

This example shows how to configure a static rendezvous point for an IPv4 bidirectional PIM group:

```
Router(config)# ip pim rp-address 10.0.0.1 10 bidir override
Router(config)# access-list 10 permit 224.1.0.0 0.0.255.255
Router(config)# ip pim send-rp-announce Loopback0 scope 16 group-list c21-rp-list-0 bidir
Router(config)# ip access-list standard c21-rp-list-0 permit 230.31.31.1 0.0.255.255
```

Displaying IPv4 Bidirectional PIM Information

To display IPv4 bidirectional PIM information, perform one of these tasks:

Command	Purpose
`Router# show ip pim rp mapping` [**in-use**]	Displays mappings between PIM groups and rendezvous points and shows learned rendezvous points in use.
`Router# show ip mfib`	Displays MFIB information for bidirectional PIM.
`Router# show platform hardware multicast routing ip`	Displays IP multicast Layer 3 switching details.

Command	Purpose
`Router# show platform software multicast routing cmrp info`	Displays information about the DF indices and DF masks allocated.
`Router# show platform ip multicast bidir`	Displays IPv4 bidirectional PIM information.

This example shows how to display information about the PIM group and rendezvous point mappings:

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP (Auto-RP)
This system is an RP-mapping agent
Group(s) 230.31.0.0/16
  RP 60.0.0.60 (?), v2v1, bidir
    Info source:60.0.0.60 (?), elected via Auto-RP
         Uptime:00:03:47, expires:00:02:11
  RP 50.0.0.50 (?), v2v1, bidir
    Info source:50.0.0.50 (?), via Auto-RP
         Uptime:00:03:04, expires:00:02:55
  RP 40.0.0.40 (?), v2v1, bidir
    Info source:40.0.0.40 (?), via Auto-RP
         Uptime:00:04:19, expires:00:02:38
```

This example shows how to display information in the IP multicast routing table that is related to IPv4 bidirectional PIM:

```
Router# show ip mroute bidirectional
(*,224.0.0.0/4), 00:17:18/-, RP 20.2.2.2, flags: B
  Bidir-Upstream: Loopback2, RPF nbr: 20.2.2.2
  Incoming interface list:
    TenGigabitEthernet3/8, Accepting/Sparse-Dense
    TenGigabitEthernet3/7, Accepting/Sparse-Dense
    GigabitEthernet1/12, Accepting/Dense
    GigabitEthernet1/1, Accepting/Sparse-Dense
    Port-channel2, Accepting/Sparse-Dense
    Loopback100, Accepting/Sparse-Dense
    Loopback10, Accepting/Sparse-Dense
    Loopback2, Accepting/Sparse-Dense

(*, 224.1.1.1), 00:17:18/00:02:26, RP 20.2.2.2, flags: BC
  Bidir-Upstream: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    TenGigabitEthernet3/8, Forward/Sparse-Dense, 00:17:17/00:02:26
```

This example shows how to display the MFIB table related to IPv4 bidirectional PIM:

```
Router# show ip mfib
Entry Flags:    C - Directly Connected, S - Signal, IA - Inherit A flag,
                ET - Data Rate Exceeds Threshold, K - Keepalive
                DDE - Data Driven Event, HW - Hardware Installed
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
                MA - MFIB Accept
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   FS Pkt Count/PS Pkt Count
Default
 (*,224.0.0.0/4) Flags: HW   ?- Indicates that Entry is installed in hardware
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: 0/0/0
   GigabitEthernet1/1 Flags: A
```

```
   GigabitEthernet1/12 Flags: A
   TenGigabitEthernet3/7 Flags: A
   TenGigabitEthernet3/8 Flags: A
   Port-channel2 Flags: A
   Loopback100 Flags: A
   Loopback10 Flags: A
   Loopback2 Flags: A F
     Pkts: 0/0
   Null0 Flags: A
  (*,224.1.1.1) Flags: IA HW
   SW Forwarding: 0/0/0/0, Other: 3/3/0
   HW Forwarding:   3357168/3000/100/2343, Other: 0/0/0 ?--- Hw Forwarding Statistics
   TenGigabitEthernet3/7 Flags: F
     Pkts: 0/0
   TenGigabitEthernet3/8 Flags: F
     Pkts: 0/0
```

This example shows how to display the hardware-switching table related to IPv4 bidirectional PIM:

```
Router# show platform hardware multicast routing ip group 224.0.0.0/4
IPv4 Multicast CEF Entries for VPN#0
Flags: C - Control, B - Bidir, c - CoPP ELIF, Q - QoS ELIF, n - Non-primary Input
Source          Destination/mask         RPF/DF      Flags  #packets      #bytes
Output LIFs/Info
+--------------+--------------------+---------------+------+-----------+----------------
--+--------------------------+
*                   224.0.0.0/4          0       B      0           0
*                   224.1.1.1/32         0       B      6539001     653900100
Te3/7, Te3/8 [2 oif(s)]
Found 2 entries.
```

This example shows how to display the DF-index and DF mask information related to IPv4 bidirectional PIM:

```
Router# show platform software multicast routing cmrp info

Replication Mode Information:
==============================
  repl_mode: Ingress; pending_repl_mode: Ingress;
  notify_repl_mode: Ingress; repl_mode_chng_in_prog: 0;
  repl_mode_notif_pending: 0

Resource Information:
======================
  fib_full_mask: 0x0; adj_full_mask: 0x0;
  met_full_mask: 0x0; met_unavail_mask: 0x0

Global HA Information:
=======================
  reconstruct_in_prog: 0; reconstruct_lc_mask: 0x0

Vrf Name: R; Vrf ID: 3; Df Idx Allocated: 8; mfib_sweep_mask: 0x0
================================================================================
  DF Idx Info for df_idx: 0
  ============================
  coll_obj: 0x530493CC; af:ipv4; df_state: USED
    DF Collection Obj Info
    ======================
    ref_count: 1; id_count: 4; app_data: 0x19D1D1A8; vrf_id: 3; df_idx: 0; cleanup: 0
    DF Set
    =======
    Tu100 (0x320004072), Tu108 (0x32000407A), Nu0 (0x32000407B), Tu3 (0x32000407F),
```

```
DF Idx Info for df_idx: 1
============================
coll_obj: 0x530493EC; af:ipv4; df_state: USED
  DF Collection Obj Info
  ======================
  ref_count: 1; id_count: 4; app_data: 0x19C3C740; vrf_id: 3; df_idx: 1; cleanup: 0
  DF Set
  =======
  Tu101 (0x320004073), Tu108 (0x32000407A), Nu0 (0x32000407B), Tu3 (0x32000407F),
DF Idx Info for df_idx: 2
============================
coll_obj: 0x5304936C; af:ipv4; df_state: USED
  DF Collection Obj Info
  ======================
  ref_count: 1; id_count: 4; app_data: 0x19D4D938; vrf_id: 3; df_idx: 2; cleanup: 0
  DF Set
  =======
  Tu102 (0x320004074), Tu108 (0x32000407A), Nu0 (0x32000407B), Tu3 (0x32000407F),
DF Idx Info for df_idx: 3
============================
coll_obj: 0x530492EC; af:ipv4; df_state: USED
  DF Collection Obj Info
  ======================
  ref_count: 1; id_count: 4; app_data: 0x19CE6338; vrf_id: 3; df_idx: 3; cleanup: 0
  DF Set
  =======
  Tu103 (0x320004075), Tu108 (0x32000407A), Nu0 (0x32000407B), Tu3 (0x32000407F),
DF Idx Info for df_idx: 4
============================
coll_obj: 0x5304930C; af:ipv4; df_state: USED
  DF Collection Obj Info
  ======================
  ref_count: 1; id_count: 4; app_data: 0x5C092894; vrf_id: 3; df_idx: 4; cleanup: 0
  DF Set
  =======
  Tu104 (0x320004076), Tu108 (0x32000407A), Nu0 (0x32000407B), Tu3 (0x32000407F),
DF Idx Info for df_idx: 5
============================
coll_obj: 0x530493AC; af:ipv4; df_state: USED
  DF Collection Obj Info
  ======================
  ref_count: 1; id_count: 4; app_data: 0x19D4D7FC; vrf_id: 3; df_idx: 5; cleanup: 0
  DF Set
  =======
  Tu105 (0x320004077), Tu108 (0x32000407A), Nu0 (0x32000407B), Tu3 (0x32000407F),
DF Idx Info for df_idx: 6
============================
coll_obj: 0x5304934C; af:ipv4; df_state: USED
  DF Collection Obj Info
  ======================
  ref_count: 1; id_count: 4; app_data: 0x19D4DC58; vrf_id: 3; df_idx: 6; cleanup: 0
  DF Set
  =======
  Tu106 (0x320004078), Tu108 (0x32000407A), Nu0 (0x32000407B), Tu3 (0x32000407F),
DF Idx Info for df_idx: 7
============================
coll_obj: 0x5304938C; af:ipv4; df_state: USED
  DF Collection Obj Info
  ======================
  ref_count: 1; id_count: 4; app_data: 0x5C09AD64; vrf_id: 3; df_idx: 7; cleanup: 0
  DF Set
  =======
  Tu107 (0x320004079), Tu108 (0x32000407A), Nu0 (0x32000407B), Tu3 (0x32000407F),
```

Using IPv4 Debug Commands

Table 14-1 describes IPv4 multicast Layer 3 switching debug commands that you can use to troubleshoot IP multicast Layer 3 switching problems.

Table 14-1 IP Multicast Layer 3 Switching Debug Commands

Command	Description
[no] debug platform software multicast routing cmrp {**event** | **error**} [**verbose**]	Debug CMRP related events and errors.
[no] debug platform software multicast routing edc server [**event** | **error**]	Debug errors and events for the egress distribution server component.
[no] debug platform software multicast routing edc client [**event** | **error**]	Debug errors and events for the egress distribution client component.
[no] debug platform software multicast routing hal [**event** | **error**]	Debug errors and events for the multicast hardware abstraction layer.
[no] debug platform software multicast routing cmfib [**event** | **error**]	Debug errors and events for the Constellation MFIB component.
[no] debug platform software met [**event** | **error** | **detail** | **all**]	Debug errors and events for MET manager.
[no] debug platform software filter *filter_id* {**ip** {**destination** | **source**} *ip_address* [*mask*] | **string** {**exclude** | **include**} *text_string*}	Turns on filtering for debug messages based on IPv4 destination address or source address or an input string.

Redundancy for Multicast Traffic

Redundancy for multicast traffic requires the following conditions:

- Unicast routing protocol such as OSPF or EIGRP:

  PIM uses RPF checks on the unicast routing table to determine the proper paths for multicast data to traverse. If a unicast routing path changes, PIM relies upon the unicast routing protocol (OSPF) to properly converge, so that the RPF checks used by PIM continue to work and show valid unicast paths to and from the source IP address of the server sourcing the multicast stream.

- PIM configured on all related Layer 3 interfaces:

  The unicast routing table is used to do path selection for PIM. PIM uses RPF checks to ultimately determine the shortest path tree (SPT) between the client (receiver VLAN) and the source (multicast VLAN). Therefore, the objective of PIM is to find the shortest unicast path between the receiver subnet and the source subnet. You do not need to configure anything else for multicast when the unicast routing protocol is working as expected and PIM is configured on all the Layer 3 links associated with the unicast routing protocol.

Tip For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum