Configuring IPv4 Multicast Layer 3 Switching

This chapter describes how to configure IPv4 multicast Layer 3 switching in Cisco IOS Release 12.2SX.

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

- The Cisco IOS Master Command List, at this URL:

  http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

- The Release 12.2 publications at this URL:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html

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

This chapter consists of these sections:

- Understanding IPv4 Multicast Layer 3 Switching, page 37-1
- Understanding IPv4 Bidirectional PIM, page 37-9
- Default IPv4 Multicast Layer 3 Switching Configuration, page 37-9
- IPv4 Multicast Layer 3 Switching Configuration Guidelines and Restrictions, page 37-10
- Configuring IPv4 Multicast Layer 3 Switching, page 37-11
- Configuring IPv4 Bidirectional PIM, page 37-24

Understanding IPv4 Multicast Layer 3 Switching

These sections describe how IPv4 multicast Layer 3 switching works:

- IPv4 Multicast Layer 3 Switching Overview, page 37-2

- Multicast Layer 3 Switching Cache, page 37-2
- Layer 3-Switched Multicast Packet Rewrite, page 37-3
- Partially and Completely Switched Flows, page 37-4
- Non-RPF Traffic Processing, page 37-5
- Multicast Boundary, page 37-8
- Understanding IPv4 Bidirectional PIM, page 37-9

IPv4 Multicast Layer 3 Switching Overview

The Policy Feature Card (PFC) provides Layer 3 switching for IP multicast flows using the hardware replication table and hardware Cisco Express Forwarding (CEF), which uses the forwarding information base (FIB) and the adjacency table on the PFC. In systems with Distributed Forwarding Cards (DFCs), IP multicast flows are Layer 3 switched locally using Multicast Distributed Hardware Switching (MDHS). MDHS uses local hardware CEF and replication tables on each DFC to perform Layer 3 switching and rate limiting of reverse path forwarding (RPF) failures locally on each DFC-equipped switching module.

The PFC and the DFCs support hardware switching of (*,G) state flows. The PFC and the DFCs support rate limiting of non-RPF traffic.

Multicast Layer 3 switching forwards IP multicast data packet flows between IP subnets using advanced application-specific integrated circuit (ASIC) switching hardware, which offloads processor-intensive multicast forwarding and replication from network routers.

Layer 3 flows that cannot be hardware switched are still forwarded in the software by routers. Protocol Independent Multicast (PIM) is used for route determination.

The PFC and the DFCs all use the Layer 2 multicast forwarding table to determine on which ports Layer 2 multicast traffic should be forwarded (if any). The multicast forwarding table entries are populated in conjunction with Internet Group Management Protocol (IGMP) snooping (see Chapter 38, “Configuring IGMP Snooping for IPv4 Multicast Traffic”).

Multicast Layer 3 Switching Cache

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 route processor (RP) updates its multicast routing table and forwards the new information to the PFC whenever it receives traffic for a new flow. In addition, if an entry in the multicast routing table on the RP ages out, the RP deletes the entry and forwards the updated information to the PFC. In systems with DFCs, flows are populated symmetrically on all DFCs and on the PFC.

The Layer 3 switching cache contains flow information for all active Layer 3-switched flows. After the switching cache is populated, multicast packets identified as belonging to an existing flow can be Layer 3 switched based on the cache entry for that flow. For each cache entry, the PFC maintains a list of outgoing interfaces for the IP multicast group. From this list, the PFC determines onto which VLANs traffic from a given multicast flow should be replicated.

These commands affect the Layer 3 switching cache 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 multicast Layer 3 switching on an individual interface basis using the **no mls ipmulticast** command, flows that use this interface as the RPF interface are routed only by the RP in software.

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[1]	*Source A MAC*	*Group G1 IP*	*Source A IP*	*n*	*calculation1*		

1. In this example, Destination B is a member of Group G1.

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 mls 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*		

Partially and Completely Switched Flows

When at least one outgoing Layer 3 interface for a given flow is multilayer switched and at least one outgoing interface is not multilayer switched, that flow is considered partially switched. When a partially switched flow is created, all multicast traffic belonging to that flow still reaches the RP and is forwarded by software on those outgoing interfaces that are not multilayer switched.

These sections describe partially and completely switched flow:

- Partially Switched Flows, page 37-4
- Completely Switched Flows, page 37-5

Partially Switched Flows

A flow might be partially switched instead of completely switched in these situations:

- If the switch is configured as a member of the IP multicast group on the RPF interface of the multicast source (using the **ip igmp join-group** command).
- During the registering state, if the switch is the first-hop router to the source in PIM sparse mode (in this case, the switch must send PIM-register messages to the rendezvous point [RP]).
- If the multicast TTL threshold is configured on an outgoing interface for the flow (using the **ip multicast ttl-threshold** command).
- If the multicast helper is configured on the RPF interface for the flow, and multicast to broadcast translation is required.
- If the outgoing interface is a generic routing encapsulation (GRE) tunnel interface.
- If the outgoing interface is a Distance Vector Multicast Routing Protocol (DVMRP) tunnel interface.
- If Network Address Translation (NAT) is configured on an interface and source address translation is required for the outgoing interface.
- Flows are partially switched if any of the outgoing interfaces for a given flow are not Layer 3 switched.

(S,G) flows are partially switched instead of completely switched in these situations:

- (S,G) flows are partially switched if the (S,G) entry has the RPT-bit (R bit) set.
- (S,G) flows are partially switched if the (S,G) entry does not have the SPT bit (T flag) set and the Prune bit (P flag) set.

(*,G) flows are partially switched instead of completely switched in these situations:

- (*,G) flows are partially switched on the last-hop leaf router if the shared-tree to shortest-path-tree (SPT) threshold is not equal to infinity. This allows the flow to transition from the SPT.
- (*,G) flows are partially switched if at least one (S,G) entry has the same RPF as a (*,g) entry but any of these is true:
  - The RPT flag (R bit) is not set.
  - The SPT flag (T bit) is not set.
  - The Prune-flag (P bit) is not set.
- (*,G) flows are partially switched if a DVMRP neighbor is detected on the input interface of a (*,G) entry.
- (*,G) flows are partially switched if the interface and mask entry is not installed for the RPF-interface of a (*,G) entry and the RPF interface is not a point-to-point interface.

- In PFC2 systems, (*,G) flows will be partially switched on the last-hop leaf router if the shared-tree to shortest-path-tree (SPT) threshold is not equal to infinity. This allows the flow to transition from SPT.

Note With a PFC2, flows matching an output ACL on an outgoing interface are routed in software.

Completely Switched Flows

When all the outgoing interfaces for a given flow are Layer 3 switched, and none of the above situations apply to the flow, that flow is considered completely switched. When a completely switched flow is created, the PFC prevents multicast traffic bridged on the source VLAN for that flow from reaching the RP interface in that VLAN, freeing the RP of the forwarding and replication load for that flow.

One consequence of a completely switched flow is that multicast statistics on a per-packet basis for that flow cannot be recorded. Therefore, the PFC periodically sends multicast packet and byte count statistics for all completely switched flows to the RP. The RP updates the corresponding multicast routing table entry and 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.

Non-RPF Traffic Processing

These sections describe non-RPF traffic processing:

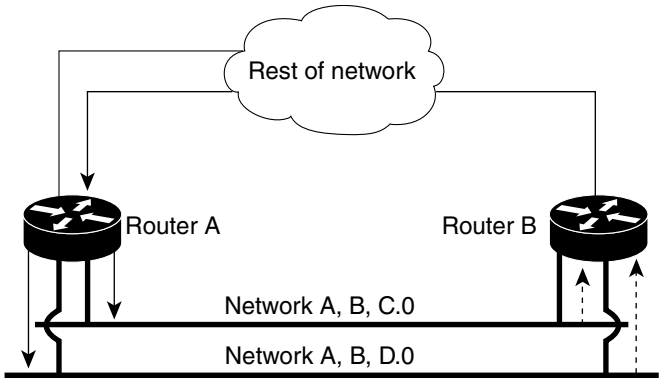
- Non-RPF Traffic Overview, page 37-5
- Filtering of RPF Failures for Stub Networks, page 37-8
- Rate Limiting of RPF Failure Traffic, page 37-8

Non-RPF Traffic Overview

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 37-1). 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.

The PFC hardware processes non-RPF traffic by filtering (dropping) or rate limiting the non-RPF traffic.

Figure 37-1 Redundant Multicast Router Configuration in a Stub Network



The conflicting requirements for the non-RPF traffic in the PFC3 prevent the majority of traffic from reaching the RP. However, leaking some packets to the RP ensures that correct protocol operations are met by using the hardware NetFlow table on the PFC3. By default, the NetFlow non-RPF traffic handling is enabled on the Supervisor Engine 720, and it cannot be disabled.

When the first non-RPF packet for an existing multicast FIB table entry is received, a matching (S,G) FIB TCAM entry for the packet is found; however, the RPF check is mismatched so a non-RPF NetFlow entry for the multicast entry is created in the NetFlow table. The packet is then bridged to the non-RPF VLAN and the RP for further processing.

The NetFlow search engine removes all of the non-RPF NetFlow entries from the hardware every 20 seconds. The next non-RPF packet received for a FIB TCAM entry triggers the creation of a non-RPF NetFlow entry while bridging the packet to the RP CPU. This operation results in only a single packet for each non-RPF NetFlow entry which will be bridged to the RP CPU approximately every 20 seconds, regardless of the rate of the various multicast traffic flows passing through the system.

Note The non-RPF NetFlow entries are created only for PIM-SM, PIM-DM, and SSM multicast FIB entries. Because the Bidir PIM does not use the PIM assert mechanism, non-RPF NetFlow entries are never created for Bidir PIM FIB entries.

In addition to the 20-second periodic timer, any non-RPF NetFlow entries that remain unused for more than 2 seconds are automatically purged to conserve NetFlow table resources. To view details of the multicast non-RPF entries in the NetFlow table, use the **show mls netflow ip multicast rpf-fail** command from the SP console.

This example shows how to display RPF fail information:

```
Router (config)# mls netflow ip multicast rpf-fail
Source      Destination    RPF      #packets   #bytes     Type
+---------+--------------+--------+-----------+--------+--------------------------
10.14.1.60   225.0.0.158   Vl19        2          92       NRPF
10.14.1.68   225.0.1.110   Vl19        2          92       NRPF
10.14.1.60   225.0.1.102   Vl19        2          92       NRPF
10.14.1.137  225.0.0.235   Vl19      121        5566       NRPF
10.14.1.135  225.0.0.233   Vl19      122        5612       NRPF
10.14.1.127  225.0.0.225   Vl19      122        5612       NRPF
10.14.1.124  225.0.0.222   Vl19      122        5612       NRPF
10.14.1.81   225.0.1.123   Vl19        2          92       NRPF
10.14.1.67   225.0.1.109   Vl19        2          92       NRPF
```

```
10.14.1.41   225.0.1.83    Vl19        2           92        NRPF
```

If the NetFlow table is full when the system attempts to create a new non-RPF NetFlow entry, the packet is bridged in the VLAN and is also forwarded to a reserved adjacency that punts the packet to the RP CPU. By default, the traffic sent to this adjacency entry is not rate limited. To protect the RP CPU from excess non-RPF packets, rate limit the traffic sent to this adjacency by using the **mls rate limit multicast non-rpf rate burst** command. You can check whether the NetFlow table is full by using the **show mls netflow table contention summary** command.

Filtering of RPF Failures for Stub Networks

The PFC and the DFCs support ACL-based filtering of RPF failures for sparse mode stub networks. When you enable the ACL-based method of filtering RPF failures by entering the **mls ip multicast stub** command on the redundant router, the following ACLs automatically download to the PFC and are applied to the interface you specify:

```
access-list 100 permit ip A.B.C.0 0.0.0.255 any
access-list 100 permit ip A.B.D.0 0.0.0.255 any
access-list 100 permit ip any 224.0.0.0 0.0.0.255
access-list 100 permit ip any 224.0.1.0 0.0.0.255
access-list 100 deny ip any 224.0.0.0 15.255.255.255
```

The ACLs filter RPF failures and drop them in hardware so that they are not forwarded to the router.

Use the ACL-based method of filtering RPF failures only in sparse mode stub networks where there are no downstream routers. For dense mode groups, RPF failure packets have to be seen on the router for the PIM assert mechanism to function properly. Use CEF-based or NetFlow-based rate limiting to limit the rate of RPF failures in dense mode networks and sparse mode transit networks.

For information on configuring ACL-based filtering of RPF failures, see the "Configuring ACL-Based Filtering of RPF Failures" section on page 37-18.

Rate Limiting of RPF Failure Traffic

When you enable rate limiting of packets that fail the RPF check (non-RPF packets), most non-RPF packets are dropped in hardware. According to the multicast protocol specification, the router needs to receive the non-RPF packets for the PIM assert mechanism to function properly, so all non-RPF packets cannot be dropped in hardware.

When a non-RPF packet is received, a NetFlow entry is created for each non-RPF flow.

When the first non-RPF packet arrives, the PFC bridges the packet to the RP and to any bridged ports and creates a NetFlow entry that contains source, group, and ingress interface information, after which the NetFlow entry handles all packets for that source and group, sending packets only to bridged ports and not to the RP.

To support the PIM assert mechanism, the PFC periodically forwards a percentage of the non-RPF flow packets to the RP. The first packets for directly connected sources in PIM sparse mode are also rate-limited and are processed by the CPU. By default, rate limiting of RPF failures is disabled .

The non-RPF hardware rate limiter offers an alternative method for handling the non-RPF multicast traffic. You can enable the traffic-handling method by using the **mls rate-limit multicast non-rpf** command. The configured rate represents the aggregate of all non-RPF traffic punted to the RP CPU. We recommend that you enable the rate limiter when the NetFlow table is full. By default, the rate limiter is disabled.

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.

Understanding IPv4 Bidirectional PIM

The PFC3 supports hardware forwarding of IPv4 bidirectional PIM groups. To support IPv4 bidirectional PIM groups, the PFC3 implements a new mode called 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 37-24.

Default IPv4 Multicast Layer 3 Switching Configuration

Table 37-1 shows the default IP multicast Layer 3 switching configuration.

Table 37-1 Default IP Multicast Layer 3 Switching Configuration

Feature	Default Value
ACL for stub networks	Disabled on all interfaces
Installing of directly connected subnet entries	Enabled globally
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
Shortcut consistency checking	Enabled

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 38, "Configuring IGMP Snooping for IPv4 Multicast Traffic."

IPv4 Multicast Layer 3 Switching Configuration Guidelines and Restrictions

These sections describe IP Multicast Layer 3 switching configuration restrictions:

- Restrictions, page 37-10
- Unsupported Features, page 37-10

Restrictions

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 224.0.2.* to 239.*.*.*.

  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.
- For source traffic received on tunnel interfaces (such as MBONE traffic).
- 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.
- For IPv4 bidirectional PIM entries when a DF interface or RPF interface is a tunnel.
- GRE tunnel encapsulation and de-encapsulation for multicast packets is handled in software.
- Supervisor Engine 32 does not support egress multicast replication and cannot detect the multicast replication mode.

Unsupported Features

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.

Configuring IPv4 Multicast Layer 3 Switching

These sections describe how to configure IP multicast Layer 3 switching:

- Source-Specific Multicast with IGMPv3, IGMP v3lite, and URD, page 37-11
- Enabling IPv4 Multicast Routing Globally, page 37-11
- Enabling IPv4 PIM on Layer 3 Interfaces, page 37-12
- Enabling IP Multicast Layer 3 Switching on Layer 3 Interfaces, page 37-13
- Configuring the Replication Mode, page 37-13
- Enabling Local Egress Replication, page 37-15
- Configuring the Layer 3 Switching Global Threshold, page 37-16
- Enabling Installation of Directly Connected Subnets, page 37-17
- Specifying the Flow Statistics Message Interval, page 37-17
- Configuring IPv4 Bidirectional PIM, page 37-24
- Setting the IPv4 Bidirectional PIM Scan Interval, page 37-25
- Enabling Shortcut-Consistency Checking, page 37-17
- Configuring ACL-Based Filtering of RPF Failures, page 37-18
- Displaying RPF Failure Rate-Limiting Information, page 37-18
- Configuring Multicast Boundary, page 37-19
- Displaying IPv4 Multicast Layer 3 Hardware Switching Summary, page 37-19
- Displaying the IPv4 Multicast Routing Table, page 37-22
- Displaying IPv4 Multicast Layer 3 Switching Statistics, page 37-23
- Displaying IPv4 Bidirectional PIM Information, page 37-26
- Using IPv4 Debug Commands, page 37-28
- Clearing IPv4 Multicast Layer 3 Switching Statistics, page 37-28
- Redundancy for Multicast Traffic, page 37-29

Note When you are in configuration mode you can enter EXEC mode commands by entering the **do** keyword before the EXEC mode command.

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

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

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

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.

For complete information and procedures, see these publications:

- *Cisco IOS IP and IP Routing Configuration Guide*, Release 12.2, at this URL:
  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/fipr_c.html
- *Cisco IOS IP and IP Routing Command Reference*, Release 12.1, at this URL:
  http://www.cisco.com/en/US/docs/ios/12_2/ipaddr/command/reference/fipras_r.html

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*[1] *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.

1. *type* = **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

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
```

Enabling IP Multicast Layer 3 Switching Globally

To enable hardware switching of multicast routes globally on your system, perform this task:

	Command	Purpose
Step 1	`Router(config)# mls ip multicast`	Globally enables hardware switching of multicast routes.
Step 2	`Router# show mls ip multicast`	Displays MLS IP multicast configuration.

This example shows how to globally enable hardware switching of multicast routes:

```
Router(config)# mls ip multicast
Router(config)#
```

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.

PIM can be enabled on any Layer 3 interface, including VLAN interfaces.

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 37-12.

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[1] slot/port}}`	Selects an interface to configure.
Step 2	`Router(config-if)# mls ip multicast`	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 # [no] mls ip multicast syslog`[2]	(Optional) Enables display of multicast related syslog messages on console.

1. *type* = **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

2. This command is only available in IOS Software Release 12.2SXI and later, and is disabled by default.

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

```
Router(config-if)# mls ip multicast
Router(config-if)#
```

Configuring the Replication Mode

Note Supervisor Engine 32 and the Cisco ME 6500 Series Ethernet switches support only ingress replication mode.

The Supervisor Engine 720 and Supervisor Engine 720-10GE support the **egress** keyword. Support for the **egress** keyword is called "Multicast Enhancement - Replication Mode Detection" in the release notes and Feature Navigator.

By default, the switch automatically detects the replication mode based on the switching modules installed in the system. If all switching modules are capable of egress replication, the switch uses egress-replication mode. If the switch detects switching modules that are not capable of egress

replication, the replication mode automatically changes to ingress replication. You can override this action by entering the **mls ip multicast replication-mode egress** command so that the switch continues to work in egress-replication mode even if there are fabric-enabled modules installed that do not support egress replication. You can also configure the switch to operate only in ingress-replication mode.

If the switch is functioning in automatic detection mode, and you install a switching module that cannot perform egress replication, the following occurs:

- The switch reverts to ingress mode
- A system log is generated

If the switch is functioning in forced egress mode, a system log is created that will display the presence of modules that are not capable of egress replication mode.

Note

- If you configure forced egress mode in a switch that has fabric-enabled modules that are not capable of egress replication, you must make sure that these modules are not sourcing or receiving multicast traffic.
- Egress mode is not compatible with QoS or SPAN. When QoS is configured, egress replication can result in the incorrect COS or DSCP marking. When SPAN is configured, egress replication can result in multicast packets not being sent to the SPAN destination port. If you are using QoS or SPAN and your switching modules are capable of egress replication, enter the **mls ip multicast replication-mode ingress** command to force ingress replication.
- During a change from egress- to ingress-replication mode, traffic interruptions may occur because the shortcuts will be purged and reinstalled. To avoid interruptions in traffic forwarding, enter the **mls ip multicast replication-mode ingress** command in global configuration mode. This command forces the system to operate in ingress-replication mode.
- The **no** form of the **mls ip multicast replication-mode ingress** command restores the system to automatic detection mode.

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

	Command	Purpose
Step 1	`Router(config)# mls ip multicast replication-mode [egress | ingress]`	Specifies the replication mode.
Step 2	`Router# show mls ip multicast capability`	Displays the configured replication mode.
Step 3	`Router# show mls ip multicast summary`	Displays the replication mode and if automatic detection is enabled or disabled.

This example shows how to enable the replication mode:

```
Router (config)# mls ip multicast replication-mode egress
Router# show mlp ip multicast capability
Current mode of replication is Ingress
Configured replication mode is Egress

Slot           Multicast replication capability
    2                       Egress
    3                       Egress
    4                       Ingress
    5                       Egress
    6                       Egress
```

```
Router# show mls ip multicast summary
4 MMLS entries using 656 bytes of memory
Number of partial hardware-switched flows:2
Number of complete hardware-switched flows:2

Directly connected subnet entry install is enabled
Current mode of replication is Ingress
Auto-detection of replication mode is enabled
Consistency checker is enabled
Router (config)#
```

Enabling Local Egress Replication

Note Supervisor Engine 32 and the Cisco ME 6500 Series Ethernet switches support only ingress replication mode.

With a Supervisor Engine 720 or Supervisor Engine 720-10GE, you can unconditionally enable local egress replication. This feature is called “Multicast enhancement - egress replication performance improvement” in the release notes and Feature Navigator.

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:

- IPv4 egress replication mode.
- Dual fabric-connection DFC-equipped modules.
- All releases can provide local egress replication on Layer 3-routed interfaces and subinterfaces that are not members of an EtherChannel.
- Releases earlier than Release 12.2(33)SXI cannot provide local egress replication on members of Layer 3 EtherChannels or on VLAN interfaces.
- Release 12.2(33)SXI and later releases add local egress replication support for members of Layer 3 EtherChannels and VLAN interfaces.

The local egress replication feature is not supported for the following internal VLANs:

- Egress internal VLAN
- Partial-shortcut internal VLAN
- Internal VLAN for Multicast VPN Multicast Distribution Tree (MDT) tunnel
- Point-to-point tunnel internal VLAN
- QoS internal VLAN

Note The local egress replication feature is not supported with IPv6 multicast or in a system that has a mix of IPv4 and IPv6 multicast enabled.

To enable local egress replication, perform this task:

	Command	Purpose
Step 1	`Router(config)# mls ip multicast egress local`	Enables local egress replication. **Note** This command requires a system reset for the configuration to take effect.
Step 2	`Router # reload`	Reloads the system.
Step 3	`Router# show mls ip multicast capability` `Router# show mls cef ip multicast detail`	Displays the configured replication mode.

This example shows how to enable local egress replication:

```
Router (config)# mls ip multicast egress local
Router (config)# exit
Router # reload
Router # show mls ip multicast capability
Current mode of replication is Ingress
Configured replication mode is Egress
Egress Local is Enabled
Slot Multicast replication capability Egress Local
2 Egress No
3 Egress Yes
4 Ingress No
5 Egress No
6 Egress No
```

Configuring the Layer 3 Switching Global Threshold

You can configure a global multicast rate threshold (specified in packets per second) below which all multicast traffic is routed by the RP. This configuration prevents creation of switching cache entries for low-rate Layer 3 flows.

Note This command does not affect flows that are already being routed. To apply the threshold to existing routes, clear the route and let it reestablish.

To configure the Layer 3 switching threshold, perform this task:

Command	Purpose
`Router(config)# mls ip multicast threshold` *ppsec*	Configures the IP MMLS threshold.

This example shows how to configure the Layer 3 switching threshold to 10 packets per second:

```
Router(config)# mls ip multicast threshold 10
Router(config)#
```

Enabling Installation of Directly Connected Subnets

In PIM sparse mode, a first-hop router that is the designated router for the interface may need to encapsulate the source traffic in a PIM register message and unicast it to the rendezvous point. To prevent new sources for the group from being learned in the routing table, the (*,G) flows should remain as completely hardware-switched flows. When (subnet/mask, 224/4) entries are installed in the hardware, the FIB allows both (*,G) flows to remain completely hardware-switched flows, and new, directly connected sources to be learned correctly. The installation of directly connected subnets is enabled globally by default. One (subnet/mask, 224/4) is installed per PIM-enabled interface.

To view FIB entries, enter the **show mls ip multicast connected** command.

To enable installation of directly connected subnets, perform this task:

Command	Purpose
`Router(config)# mls ip multicast connected`	Enables installation of directly connected subnets.

This example shows how to enable installation of directly connected subnets:

```
Router(config)# mls ip multicast connected
Router(config)#
```

Specifying the Flow Statistics Message Interval

By default, the switch processor (SP) forwards flow statistics messages to the route processor (RP) every 25 seconds. The messages are forwarded in batches, and each batch of messages contains statistics for 25 percent of all flows. If you leave the interval at the default of 25 seconds, it will take 100 seconds to forward statistics for all flows to the RP.

To specify how often flow statistics messages forwarded from the SP to the RP, perform this task:

Command	Purpose
`Router(config)# mls ip multicast flow-stat-timer` *num*	Specifies how the SP forwards flow statistics messages to the RP.

This example shows how to configure the SP to forward flow statistics messages to the RP every 10 seconds:

```
Router(config)# mls ip multicast flow-stat-timer 10
Router(config)#
```

Enabling Shortcut-Consistency Checking

When you enable the shortcut-consistency checking feature, the multicast route table and the multicast-hardware entries are checked for consistency, and any inconsistencies are corrected. You can view inconsistencies by entering the **show mls ip multicast consistency-check** command.

If consistency checking is enabled, the multicast route table will be scanned every two seconds and a full scan is completed within 4 minutes.

To enable shortcut-consistency checking, perform this task:

Command	Purpose
`Router(config)# mls ip multicast consistency-check`	Enables shortcut-consistency checking.

This example shows how to enable the hardware shortcut-consistency checker:

```
Router (config)# mls ip multicast consistency-check
Router (config)#
```

Configuring ACL-Based Filtering of RPF Failures

When you configure ACL-based filtering of RPF failures, ACLs that filter RPF failures in hardware are downloaded to the hardware-based ACL engine and applied on the interface you specify.

To enable ACL-based filtering of RPF failures on an 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)# mls ip multicast stub`	Enables ACL-based filtering of RPF failures on an interface.

1. *type* = **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

Displaying RPF Failure Rate-Limiting Information

To display RPF failure rate-limiting information, perform this task:

Command	Purpose
`Router# show mls ip multicast summary`	Displays RPF failure rate-limiting information.

This example shows how to display RPF failure rate-limiting information:

```
Router# show mls ip multicast summary
10004 MMLS entries using 1280464 bytes of memory
Number of partial hardware-switched flows:4
Number of complete hardware-switched flows:10000
Router#
```

Configuring Multicast Boundary

To configure a multicast boundary, 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 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.

1. *type* = **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

Note In releases earlier than 12.2(33)SXI, the switch creates an empty ACL (with implicit deny any any) even though the ACL is not preconfigured. However, from 12.2(33)SXI or later releases, if the ACL is not preconfigured, the **ip multicast boundary** command will not create an empty ACL (with implicit deny any any).

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
```

Displaying IPv4 Multicast Layer 3 Hardware Switching Summary

Note The **show interface statistics** command does not display hardware-switched packets, only packets switched by software.

The **show ip pim interface count** command displays the IP multicast Layer 3 switching enable state on IP PIM interfaces and the number of packets received and sent on the interface.

To display IP multicast Layer 3 switching information for an IP PIM Layer 3 interface, perform one of these tasks:

Command	Purpose
`Router# show ip pim interface [{{vlan vlan_ID} | {type[1] slot/port} | {port-channel number}}] count`	Displays IP multicast Layer 3 switching enable state information for all RP IP PIM Layer 3 interfaces.
`Router# show ip interface`	Displays the IP multicast Layer 3 switching enable state on the Layer 3 interfaces.

1. *type* = **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

These examples show how to display the IP PIM configuration of the interfaces:

```
Router# show ip pim interface count

State:* - Fast Switched, D - Distributed Fast Switched
      H - Hardware Switching Enabled
Address          Interface          FS  Mpackets In/Out
10.15.1.20       GigabitEthernet4/8 * H 952/4237130770
10.20.1.7        GigabitEthernet4/9 * H 1385673757/34
10.25.1.7        GigabitEthernet4/10* H 0/34
10.11.1.30       FastEthernet6/26   * H 0/0
10.37.1.1        FastEthernet6/37   * H 0/0
1.22.33.44       FastEthernet6/47   * H 514/68
```

The "*" flag indicates that this interface can be fast switched and the "H" flag indicates that this interface is hardware switched. The "In" flag indicates the number of multicast packet bytes that have been received on the interface. The "Out" flag indicates the number of multicast packet bytes that have been forwarded from this interface.

```
Router# show ip mroute count
IP Multicast Statistics
56 routes using 28552 bytes of memory
13 groups, 3.30 average sources per group
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)

Group:224.2.136.89, Source count:1, Group pkt count:29051
  Source:132.206.72.28/32, Forwarding:29051/-278/1186/0, Other:85724/8/56665
Router#
```

Note The -tive counter means that the outgoing interface list of the corresponding entry is NULL, and this indicates that this flow is still active.

This example shows how to display the IP multicast Layer 3 switching configuration of interface VLAN 10:

```
Router# show ip interface vlan 10
Vlan10 is up, line protocol is up
  Internet address is 10.0.0.6/8
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.1 224.0.0.2 224.0.0.13 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
```

```
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are never sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Fast switching turbo vector
  IP Normal CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
IP multicast multilayer switching is enabled
IP mls switching is enabled
Router#
```

This example shows how to display the IP multicast Layer 3 switching configuration of Gigabit Ethernet interface 1/2:

```
Router# show interfaces gigabitEthernet 1/2
GigabitEthernet1/2 is up, line protocol is up (connected)
  Hardware is C6k 1000Mb 802.3, address is 0001.c9db.2441 (bia 0001.c9db.2441)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
  Last clearing of "show interface" counters 00:05:13
  ….
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 10000 bits/sec, 1 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     284 packets input, 113104 bytes, 0 no buffer
     Received 284 broadcasts (284 multicast)
     0 runts, 41 giants, 0 throttles
     41 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     198 packets output, 14732 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Router#
```

Displaying the IPv4 Multicast Routing Table

The **show ip mroute** command displays the IP multicast routing table.

To display the IP multicast routing table, perform this task:

Command	Purpose
Router# **show ip mroute partical-sc** [*hostname* | *group_number*]	Displays the IP multicast routing table and the hardware-switched interfaces.

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

```
Router# show ip mroute 230.13.13.1
IP Multicast Routing Table
Flags:D - Dense, S - Sparse, s - SSM Group, C - Connected, L - Local,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT, M - MSDP created entry, X - Proxy Join Timer Running
       A - Advertised via MSDP, U - URD, I - Received Source Specific Host
           Report
Outgoing interface flags:H - Hardware switched
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode

(*, 230.13.13.1), 00:16:41/00:00:00, RP 10.15.1.20, flags:SJC
  Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20
  Outgoing interface list:
 GigabitEthernet4/9, Forward/Sparse-Dense, 00:16:41/00:00:00, H

(*, 230.13.13.2), 00:16:41/00:00:00, RP 10.15.1.20, flags:SJC
 Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD
  Outgoing interface list:
    GigabitEthernet4/9, Forward/Sparse-Dense, 00:16:41/00:00:00, H

(10.20.1.15, 230.13.13.1), 00:14:31/00:01:40, flags:CJT
 Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD
  Outgoing interface list:
    GigabitEthernet4/9, Forward/Sparse-Dense, 00:14:31/00:00:00, H
(132.206.72.28, 224.2.136.89), 00:14:31/00:01:40, flags:CJT
  Incoming interface:GigabitEthernet4/8, RPF nbr 10.15.1.20, RPF-MFD
 Outgoing interface list:Null
Router#
```

Note The RPF-MFD flag indicates that the flow is completely switched by the hardware. The H flag indicates the flow is switched by the hardware on the outgoing interface.

Displaying IPv4 Multicast Layer 3 Switching Statistics

The **show mls ip multicast** 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 mls ip multicast group** *ip_address* [**interface** *type slot/port* | **statistics**]	Displays IP multicast Layer 3 switching group information.
Router# **show mls ip multicast interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*} | {**port-channel** *number*}} [**statistics** | **summary**]	Displays IP multicast Layer 3 switching details for all interfaces.
Router# **show mls ip multicast source** *ip_address* [**interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*} | {**port-channel** *number*}} | **statistics**]	Displays IP multicast Layer 3 switching source information.
Router# **show mls ip multicast summary**	Displays a summary of IP multicast Layer 3 switching information.
Router# **show mls ip multicast statistics**	Displays IP multicast Layer 3 switching statistics.

1. *type* = **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to display information on a specific IP multicast Layer 3 switching entry:

```
Router# show mls ip multicast group 10.1.0.11
Multicast hardware switched flows:
Total shortcut installed: 0
```

This example shows how to display IP multicast group information:

```
Router# show mls ip multicast group 230.13.13.1 source 10.20.1.15
Multicast hardware switched flows:
(10.20.1.15, 230.13.13.1) Incoming interface:Gi4/8, Packets switched:0
Hardware switched outgoing interfaces:Gi4/9
RPF-MFD installed

Total hardware switched flows :1
Router#
```

This example shows how to display IP multicast Layer 3 switching information for VLAN 10:

```
Router# show mls ip multicast interface vlan 10
Multicast hardware switched flows:
(10.1.0.15, 224.2.2.15) Incoming interface: Vlan10, Packets switched: 0
Hardware switched outgoing interfaces:
MFD installed: Vlan10

(10.1.0.19, 224.2.2.19) Incoming interface: Vlan10, Packets switched: 1970
Hardware switched outgoing interfaces:
MFD installed: Vlan10

(10.1.0.11, 224.2.2.11) Incoming interface: Vlan10, Packets switched: 0
Hardware switched outgoing interfaces:
MFD installed: Vlan10

(10.1.0.10, 224.2.2.10) Incoming interface: Vlan10, Packets switched: 2744
Hardware switched outgoing interfaces:
MFD installed: Vlan10
```

```
(10.1.0.17, 224.2.2.17) Incoming interface: Vlan10, Packets switched: 3340
Hardware switched outgoing interfaces:
MFD installed: Vlan10

(10.1.0.13, 224.2.2.13) Incoming interface: Vlan10, Packets switched: 0
Hardware switched outgoing interfaces:
```

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

```
Router# show mls ip multicast statistics
MLS Multicast Operation Status:
MLS Multicast configuration and state:
    Router Mac: 00e0.b0ff.7b00, Router IP: 33.0.33.24
    MLS multicast operating  state: ACTIVE
    Shortcut Request Queue size 4
    Maximum number of allowed outstanding messages: 1
    Maximum size reached from feQ: 3096
    Feature Notification sent: 1
    Feature Notification Ack received: 1
    Unsolicited Feature Notification received: 0
    MSM sent: 205170
    MSM ACK received: 205170
    Delete notifications received: 0
    Flow Statistics messages received: 35211
MLS Multicast statistics:
    Flow install Ack: 996508
    Flow install Nack: 1
    Flow update Ack: 1415959
    Flow update Nack: 0
    Flow delete Ack: 774953
    Complete flow install Ack: 958469
Router#
```

Configuring IPv4 Bidirectional PIM

These sections describe how to configure IPv4 bidirectional protocol independent multicast (PIM):

- Enabling IPv4 Bidirectional PIM Globally, page 37-24
- Configuring the Rendezvous Point for IPv4 Bidirectional PIM Groups, page 37-25
- Setting the IPv4 Bidirectional PIM Scan Interval, page 37-25
- Displaying IPv4 Bidirectional PIM Information, page 37-26

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)# mls ip multicast`	Enables MLS 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
```

Setting the IPv4 Bidirectional PIM Scan Interval

You can specify the interval between the IPv4 bidirectional PIM RP Reverse Path Forwarding (RPF) scans.

To set the IPv4 bidirectional PIM RP RPF scan interval, perform this task:

Command	Purpose
`Router(config)# mls ip multicast bidir gm-scan-interval interval`	Specifies the IPv4 bidirectional PIM RP RPF scan interval; valid values are from 1 to 1000 seconds. The default is 10 seconds.

This example shows how to set the IPv4 bidirectional PIM RP RPF scan interval:

```
Router(config)# mls ip multicast bidir gm-scan-interval 30
Router(config)#
```

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 mls ip multicast rp-mapping** [*rp_address*]	Displays PIM group to active rendezvous points mappings.
Router# **show mls ip multicast rp-mapping gm-cache**	Displays information based on the group/mask ranges in the RP mapping cache.
Router# **show mls ip multicast rp-mapping df-cache**	Displays information based on the DF list in RP mapping cache.
Router# **show mls ip multicast bidir**	Displays IPv4 bidirectional PIM information.
Router# **show ip mroute**	Displays information about the multicast routing table.

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
    (*, 225.1.3.0), 00:00:02/00:02:57, RP 3.3.3.3, flags:BC
      Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
      Outgoing interface list:
        GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:02/00:00:00,H
        Vlan30, Forward/Sparse-Dense, 00:00:02/00:02:57, H

    (*, 225.1.2.0), 00:00:04/00:02:55, RP 3.3.3.3, flags:BC
      Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
      Outgoing interface list:
        GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:04/00:00:00,H
        Vlan30, Forward/Sparse-Dense, 00:00:04/00:02:55, H

    (*, 225.1.4.1), 00:00:00/00:02:59, RP 3.3.3.3, flags:BC
      Bidir-Upstream:GigabitEthernet2/1, RPF nbr 10.53.1.7, RPF-MFD
      Outgoing interface list:
        GigabitEthernet2/1, Bidir-Upstream/Sparse-Dense, 00:00:00/00:00:00,H
        Vlan30, Forward/Sparse-Dense, 00:00:00/00:02:59, H
```

This example show how to display information related to a specific multicast route. In the output below, the arrow in the margin points to information about a partical short cut:

```
Router# show ip mroute 239.1.1.2 4.4.4.4
IP Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags:H - Hardware switched
 Timers:Uptime/Expires
 Interface state:Interface, Next-Hop or VCD, State/Mode

(4.4.4.4, 239.1.1.2), 1d02h/00:03:20, flags:FTZ
 Incoming interface:Loopback0, RPF nbr 0.0.0.0, Partial-SC
  Outgoing interface list:
    Vlan10, Forward/Sparse-Dense, 1d02h/00:02:39 (ttl-threshold 5)
```

This example shows how to display the entries for a specific multicast group address:

```
Router# show mls ip multicast group 230.31.31.1
Multicast hardware switched flows:
(*, 230.31.31.1) Incoming interface:Vlan611, Packets switched:1778
Hardware switched outgoing interfaces:Vlan131 Vlan151 Vlan415 Gi4/16 Vlan611
RPF-MFD installed
```

This example shows how to display PIM group to active rendezvous points mappings:

```
Router# show mls ip multicast rp-mapping
State:H - Hardware Switched, I - Install Pending, D - Delete Pending, Z - Zombie

RP Address      State       RPF            DF-count    GM-count
60.0.0.60       H           Vl611                 4           1
```

This example shows how to display information based on the group/mask ranges in the RP mapping cache:

```
Router# show mls ip multicast rp-mapping gm-cache
State:H - Hardware Switched, I - Install Pending, D - Delete Pending,
       Z - Zombie

RP Address     State       Group           Mask            State         Packet/Byte-count
60.0.0.60      H           230.31.0.0      255.255.0.0     H             100/6400
```

This example shows how to display information about specific MLS IP multicasting groups:

```
Router# show mls ip multicast rp-mapping df-cache
State:H - Hardware Switched, I - Install Pending, D - Delete Pending, Z - Zombie

RP Address      State        DF             State
60.0.0.60       H           Vl131           H
60.0.0.60       H           Vl151           H
60.0.0.60       H           Vl415           H
60.0.0.60       H           Gi4/16          H
```

Using IPv4 Debug Commands

Table 37-2 describes IPv4 multicast Layer 3 switching debug commands that you can use to troubleshoot IP multicast Layer 3 switching problems.

Table 37-2 IP Multicast Layer 3 Switching Debug Commands

Command	Description
[no] **debug mls ip multicast events**	Displays IP multicast Layer 3 switching events.
[no] **debug mls ip multicast errors**	Turns on debug messages for multicast MLS-related errors.
[no] **debug mls ip multicast group** *group_id group_mask*	Turns on debugging for a subset of flows.
[no] **debug mls ip multicast messages**	Displays IP multicast Layer 3 switching messages from and to hardware switching engine.
[no] **debug mls ip multicast all**	Turns on all IP multicast Layer 3 switching messages.
[no] **debug mdss errors**	Turns on MDSS[1] error messages.
[no] **debug mdss events**	Displays MDSS-related events for debugging.
[no] **debug mdss events mroute-bidir**	Displays IPv4 bidirectional PIM MDSS events for debugging.
[no] **debug mdss all**	Displays all MDSS messages.
[no] **debug ip pim df** *ip_address*	Displays the DF election for a given rendezvous point for debug purposes.

1. MDSS = Multicast Distributed Switching Services

Clearing IPv4 Multicast Layer 3 Switching Statistics

To clear IP multicast Layer 3 switching statistics, perform this task:

Command	Purpose
Router# **clear mls ip multicast statistics**	Clears IP multicast Layer 3 switching statistics.

This example shows how to clear IP multicast Layer 3 switching statistics:

```
Router# clear mls ip multicast statistics
```

The **show mls multicast statistics** command displays a variety of information about the multicast flows being handled by the PFC. You can display entries based on any combination of the participating RP, the VLAN, the multicast group address, or the multicast traffic source. For an example of the **show mls ip multicast statistics** command, see the "Displaying IPv4 Multicast Layer 3 Switching Statistics" section on page 37-23.

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