# Configuring IP Multicast Layer 3 Switching

This chapter describes how to configure IP multicast Layer 3 switching on the Catalyst 6500 series switches.

**Note** For more information on the syntax and usage for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

**Note** In this chapter, the term "PFC" refers to either a PFC2 or a PFC1, except when specifically differentiated, and the term "MSFC" refers to either an MSFC2 or an MSFC1, except when specifically differentiated.

# Understanding How IP Multicast Layer 3 Switching Works

These sections describe how IP multicast Layer 3 switching works:

# IP Multicast Layer 3 Switching Overview

Policy Feature Card 2 (PFC2) 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 PFC2. 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 PFC2 and the DFCs support hardware switching of (*,G) state flows. PFC1, PFC2, and the DFCs support rate limiting of non-RPF traffic.

Policy Feature Card 1 (PFC1) provides Layer 3 switching of IP multicast flows with Multilayer Switching (MLS) using the NetFlow and hardware replication tables.

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

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

PFC1, PFC2, 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 21, "Configuring IGMP Snooping").

# Multicast Layer 3 Switching Cache

PFC1, PFC2, and the DFCs maintain Layer 3 switching information in one or more hardware tables as follows:

- PFC1 populates the Layer 3 flow as {source IP, IP group, ingress-interface/VLAN} in the NetFlow cache. It also stores the Layer 3 rewrite information and a pointer to a list of outgoing interfaces (such as replication entries) for the flow. If a flow does not match these parameters, it is considered a NetFlow miss and is bridged on the incoming port based on the Layer 2 lookup.

- PFC2 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 systems with PFC1, the maximum switching cache size is 128K entries and is shared by all Layer 3 switching processes on the switch (such as IP unicast MLS and Internetwork Packet Exchange [IPX] MLS). However, a cache exceeding 32K entries increases the probability that a flow will not be switched by the PFC and will get forwarded to the MSFC.

In systems with PFC1 or PFC2, the MSFC 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 MSFC ages out, the MSFC deletes the entry and forwards the updated information to the PFC. In systems with DFCs, flows are populated symmetrically on all DFCs and on PFC2.

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:

- Clearing the multicast routing table (using the **clear ip mroute** command) clears all multicast Layer 3 switching cache entries.

- Disabling IP multicast routing on the MSFC (using the **no ip multicast-routing** command) purges all multicast Layer 3 switching cache entries on the PFC.

- Disabling multicast Layer 3 switching on an individual interface basis (using the **no mls ip multicast** command) causes flows that use this interface as the RPF interface to be routed only by the MSFC in software.

# IP Multicast Layer 3 Switching Flow Mask

IP multicast Layer 3 switching with PFC1 supports only the multicast source-destination-VLAN flow mask. PFC1 maintains one multicast Layer 3 switching cache entry for each {source IP, destination group IP, source VLAN}. The multicast source-destination-VLAN flow mask differs from the IP unicast MLS source-destination-ip flow mask in that, for IP multicast Layer 3 switching, the source VLAN is included as part of the entry. The source VLAN is the multicast RPF interface for the multicast flow. Flows are based on the IP address of the source device, the destination IP multicast group address, and the source VLAN. The MSFC uses the RPF interface to send a unicast packet back to the source.

# Layer 3-Switched Multicast Packet Rewrite

✎ **Note**    Only ARPA rewrites are supported for IP multicast packets. Subnetwork Address Protocol (SNAP) rewrites are not supported.

When a multicast packet is Layer 3 switched from a multicast source to a destination multicast group, PFC1 performs a packet rewrite based on information learned from the MSFC and stored in the Layer 3 switching cache. In the case of PFC2 and the DFCs, the packet rewrite is based on information learned from the MSFC2 and is stored in the adjacency table. The format of the packet rewrite is the same for PFC1, PFC2, and DFCs.

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 formatted (conceptually) 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 MSFC (this MAC address is stored in the multicast Layer 3 switching cache entry for the flow)

- 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 formatted (conceptually) as follows:

| Frame Header | | IP Header | | | | Data | FCS |
|---|---|---|---|---|---|---|---|
| Destination | Source | Destination | Source | TTL | Checksum | | |
| *Group G1 MAC* | *MSFC 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 MSFC and is software forwarded on those outgoing interfaces that are not multilayer switched.

These sections describe partially and completely switched flow:

- Partially Switched Flows with PFC1 or PFC2, page 18-4
- Partially Switched Flows with PFC2, page 18-5
- Completely Switched Flows, page 18-5

## Partially Switched Flows with PFC1 or PFC2

If your system has a PFC1 or PFC2 installed, a flow might be partially switched instead of completely switched in these situations:

- The switch is configured as a member of the IP multicast group (using the **ip igmp join-group** command) on the RPF interface of the multicast source.

- 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]).

- The multicast TTL threshold is configured on an outgoing interface for the flow (using the **ip multicast ttl-threshold** command).

- The multicast helper is configured on the RPF interface for the flow, and multicast to broadcast translation is required.

- The outgoing interface is a generic routing encapsulation (GRE) Distance Vector Multicast Routing Protocol (DVMRP) tunnel interface.

- The maximum transmission unit (MTU) of the RPF interface is greater than the MTU of any outgoing interface.

- If Network Address Translation (NAT) is configured on an interface, and source address translation is required for the outgoing interface.

### Partially Switched Flows with PFC2

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 Layer 3 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 MSFC interface in that VLAN, freeing the MSFC 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 MSFC. The MSFC 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

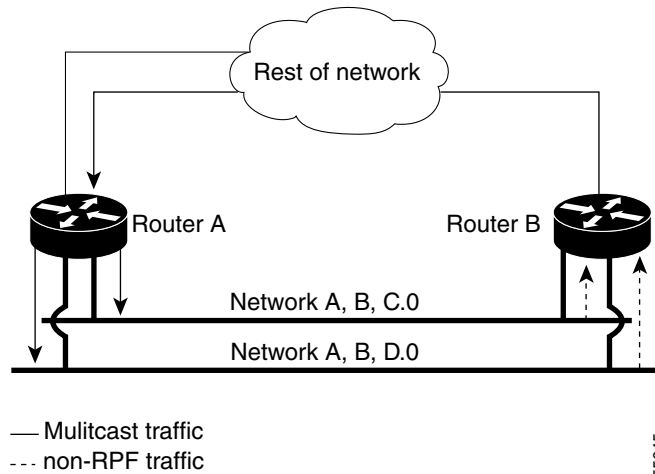These sections describe non-RPF traffic processing:

- Non-RPF Traffic Overview, page 18-5
- Filtering of RPF Failures for Stub Networks, page 18-6
- Rate Limiting of RPF Failure Traffic, page 18-6

### 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 18-1). 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 Catalyst 6500 series switch processes non-RPF traffic in hardware on the PFC by filtering (dropping) or rate limiting the non-RPF traffic.

*Figure 18-1   Redundant Multicast Router Configuration in a Stub Network*



— Mulitcast traffic
--- non-RPF traffic

## Filtering of RPF Failures for Stub Networks

PFC1, PFC2, 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-or NetFlow-based rate limiting to rate-limit 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 18-14.

## Rate Limiting of RPF Failure Traffic

Rate limiting of packets that fail the RPF check (non-RPF packets) drops most non-RPF packets in hardware. According to the multicast protocol specification, the router needs to see the non-RPF packets for the PIM assert mechanism to work, so all non-RPF packets cannot be dropped in hardware. To support the PIM assert mechanism, the PFC leaks a percentage of the non-RPF flow packets to the MSFC.

These sections describe two modes of RPF failure rate limiting:

- NetFlow-Based Rate Limiting of RPF Failures, page 18-7
- CEF-Based Rate Limiting of RPF Failures, page 18-7

**Note**    PFC2 and the DFCs support both rate-limiting modes. CEF-based rate limiting of RPF failures is the default on systems with PFC2 and for DFCs. NetFlow-based rate limiting of RPF failures is the only rate limiting mode supported with PFC1.

### NetFlow-Based Rate Limiting of RPF Failures

With NetFlow-based rate limiting of RPF failures, a NetFlow entry is created for each non-RPF flow. When a non-RPF packet arrives, the MSFC communicates information about the group, the source, and the interface on which the packet arrived to the PFC. The PFC then installs a NetFlow entry and bridges the packet to all ports in the VLAN, excluding the internal router port.

The PFC checks for non-RPF traffic every 2 seconds. An entry is kept for a maximum of 20 seconds if non-RPF traffic exists.

To configure NetFlow-based rate limiting of RPF failures, see the "Enabling NetFlow-Based Rate Limiting of RPF Failures" section on page 18-12.

### CEF-Based Rate Limiting of RPF Failures

PFC2 and the DFCs support both CEF-based rate limiting of RPF failures and NetFlow-based rate limiting of RPF failures. In the CEF-based mode, the PFC2 or the DFC drops non-RPF packets instead of bridging them to the MSFC2. To support the PIM assert mechanism, CEF-based rate limiting works in 10-second intervals. For a short duration in each 10-second interval, packets are leaked to the MSFC. During the remainder of each 10-second interval, the non-RPF packets are dropped in hardware. CEF-based rate limiting of RPF failures is enabled by default on systems with PFC2 and on the DFCs and does not require any user configuration.

For information on configuring CEF-based rate limiting of RPF failures, see the "Enabling CEF-Based Rate Limiting of RPF Failures" section on page 18-13.

# Default IP Multicast Layer 3 Switching Configuration

Table 18-1 shows the default IP multicast Layer 3 switching configuration.

*Table 18-1    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 |
| CEF-based rate limiting | Enabled globally (PFC2 only) |
| Netflow-based rate limiting | Disabled 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 hardware switched. 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 21, "Configuring IGMP Snooping."

# IP Multicast Layer 3 Switching Configuration Guidelines and Restrictions

These sections describe IP Multicast Layer 3 switching configuration restrictions:

- PFC2 with MSCF2, page 18-8
- PFC1 with MSFC or MSCF2, page 18-8
- PFC1 and PFC2 General Restrictions, page 18-9
- Unsupported Features, page 18-9

## PFC2 with MSCF2

In systems with PCF2 and MSFC2, 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).
- If the SPT bit for the flow is cleared when running PIM sparse mode for the interface or group.
- 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).

## PFC1 with MSFC or MSCF2

In systems with PFC1 and MSFC or MSFC2, IP multicast Layer 3 switching is not provided for an IP multicast flow in the following situations:

- For IP multicast groups that fall into these ranges (where * is in the range 0 to 255):

  224.0.0.* through 239.0.0.*
  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 interfaces of the VLAN. All 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 flows that are forwarded on the multicast-shared tree (that is, {*,G,*} forwarding) when the interface or group is running PIM sparse mode.

- If the SPT bit for the flow is cleared when running PIM sparse mode for the interface or group.

- For packets that require fragmentation and packets with IP options. However, packets in the flow that do not specify IP options are Layer 3 switched.

- For source traffic received on tunnel interfaces (such as MBONE traffic).

## PFC1 and PFC2 General Restrictions

Input ACL deny is not applied by the hardware ACL engine when the Layer 2 entry corresponding to the Layer 3 flow does not exist in the Layer 2 forwarding table. The ACL will be applied by the MSFC software.

## 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 IP 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 18-10
- Enabling IP Multicast Routing Globally, page 18-10
- Enabling IP PIM on Layer 3 Interfaces, page 18-10
- Enabling IP Multicast Layer 3 Switching on Layer 3 Interfaces, page 18-11
- Configuring the Layer 3 Switching Global Threshold, page 18-11
- Enabling Installation of Directly Connected Subnets, page 18-12
- Enabling NetFlow-Based Rate Limiting of RPF Failures, page 18-12
- Enabling CEF-Based Rate Limiting of RPF Failures, page 18-13
- Enabling Shortcut-Consistency Checking, page 18-13
- Configuring ACL-Based Filtering of RPF Failures, page 18-14
- Displaying RPF Failure Rate-Limiting Information, page 18-14
- Displaying IP Multicast Layer 3 Hardware Switching Summary, page 18-14
- Displaying the IP Multicast Routing Table, page 18-16
- Displaying IP Multicast Layer 3 Switching Statistics, page 18-17
- Using Debug Commands, page 18-18
- Clearing IP Multicast Layer 3 Switching Statistics, page 18-19

**Note**    With Release 12.1(11b)E and later, when you are in configuration mode you can enter EXEC mode-level commands by entering the **do** keyword before the EXEC mode-level 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), refer to this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtssm5t.htm

# Enabling IP 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, refer to these publications:

- *Cisco IOS IP and IP Routing Configuration Guide*, Release 12.1, at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/index.htm

- *Cisco IOS IP and IP Routing Command Reference*, Release 12.1, at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_r/index.htm

To enable IP multicast routing globally, perform this task:

| Command | Purpose |
|---------|---------|
| Router(config)# **ip multicast-routing** | Enables IP multicast routing globally. |
| Router(config)# **no ip multicast-routing** | Disables IP multicast routing globally. |

This example shows how to enable multicast routing globally:

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

# Enabling IP 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. |
| | Router(config-if)# **no ip pim** [**dense-mode** \| **sparse-mode** \| **sparse-dense-mode**] | Disables IP PIM on a Layer 3 interface. |

1. *type* = **ethernet**, **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
Router(config-if)#
```

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

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

# 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 IP PIM on Layer 3 Interfaces" section on page 18-10.

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)# **no mls ip multicast** | Disables IP multicast Layer 3 switching on a Layer 3 interface. |

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

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 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 MSFC, which 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. |
| Router(config)# **no mls ip multicast threshold** | Reverts to the default 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. (subnet/mask, 224/4) entries installed in the hardware FIB allows both (*,G) flows to remain completely hardware-switched flows, and new, directly connected sources to be learned correctly. Installing 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. |
| Router(config)# **no mls ip multicast connected** | Disables installation of directly connected subnets. |

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

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

# Enabling NetFlow-Based Rate Limiting of RPF Failures

You can enable NetFlow-based rate limiting of RPF failures globally and on a per-Layer 3 interface basis. When enabled on a global level, the feature is automatically enabled on all eligible Layer 3 interfaces.

**Note**    To enable NetFlow-based rate limiting of RPF failures on a PFC2, you must first disable CEF-based rate limiting of RPF failures, which is enabled by default.

To enable NetFlow-based rate limiting of RPF failures, perform this task:

| | Command | Purpose |
|---|---|---|
| Step 1 | Router(config)# **mls ip multicast non-rpf netflow** | Enables NetFlow-based rate limiting of RPF failures globally. |
| | Router(config)# **no mls ip multicast non-rpf netflow** | Disables NetFlow-based rate limiting of RPF failures globally. |
| Step 2 | Router(config)# **interface** {{**vlan** *vlan_ID*} \| {*type*[1] *slot/port*} \| {**port-channel** *channel_ID*}} | Selects the Layer 3 interface to be configured. |

| | Command | Purpose |
|---|---|---|
| **Step 3** | Router(config-if)# **mls ip multicast non-rpf netflow** | Enables NetFlow-based rate limiting of RPF failures on the Layer 3 interface. |
| | Router(config-if)# **no mls ip multicast non-rpf netflow** | Disables NetFlow-based rate limiting of RPF failures on the Layer 3 interface. |

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

This example shows how to enable NetFlow-based rate limiting of non-RPF failures globally:

```
Router(config)# mls ip multicast non-rpf netflow
Router(config)#
```

# Enabling CEF-Based Rate Limiting of RPF Failures

CEF-based rate limiting of RPF failures is enabled by default on systems with PFC2. CEF-based rate limiting of RPF failures can be configured globally only.

To enable CEF-based rate limiting of RPF failures, perform this task:

| Command | Purpose |
|---|---|
| Router(config)# **mls ip multicast non-rpf cef** | Enables CEF-based rate limiting of RPF failures globally. |
| Router(config)# **no mls ip multicast non-rpf cef** | Disables CEF-based rate limiting of RPF failures globally. |

This example shows how to enable CEF-based rate limiting of RPF failures globally:

```
Router(config)# mls ip multicast non-rpf CEF
Router(config)#
```

# Enabling Shortcut-Consistency Checking

When you enable the shortcut-consistency checking feature, the multicast route table and the multicast-hardware entries are 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 mintues.

To enable shortcut-consistency checking, perform this task:

| Command | Purpose |
|---|---|
| Router(config)# **mls ip multicast consistency-check** | Enables shortcut-consistency checking. |
| Router(config)# **no mls ip multicast consistency-check** *num* | Restores the default. |

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. |
| | Router(config-if)# **no mls ip multicast stub** | Disables ACL-based filtering of RPF failures on an interface. |

1.  *type* = **ethernet**, **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#
```

# Displaying IP 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 MSFC 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* = **ethernet**, **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


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#
```

# Displaying the IP 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** [*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 the flow is completely hardware switched. The H flag indicates the flow is hardware switched on the outgoing interface.

# Displaying IP 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 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* = **ethernet**, **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#
```

## Using Debug Commands

Table 18-2 describes IP multicast Layer 3 switching-related debug commands that you can use to troubleshoot IP multicast Layer 3 switching problems.

*Table 18-2   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. |

*Table 18-2    IP Multicast Layer 3 Switching Debug Commands (continued)*

| Command | Description |
|---|---|
| [**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** | Turns on MDSS-related events. |
| [**no**] **debug mdss all** | Turns on all MDSS messages. |

1.  MDSS = Multicast Distributed Switching Services

# Clearing IP 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 MSFC, the VLAN, the multicast group address, or the multicast traffic source. For an example of the **show mls ip multicast statistics** command, see the .