

# Configuring IP Multilayer Switching

---

This chapter describes how to configure IP Multilayer Switching (MLS) on the Catalyst 5000 family and 2926G series switches.

---

**Note** For complete syntax and usage information for the IOS commands used in this chapter, refer to the software documentation for your router platform. For complete syntax and usage information for the switch commands used in this chapter, refer to the *Command Reference* for your switch.

---

This chapter consists of these sections:

- Understanding How IP MLS Works, page 5-1
- Software and Hardware Requirements, page 5-8
- Default IP MLS Configuration, page 5-9
- Configuration Guidelines and Restrictions, page 5-9
- Configuring IP MLS on the Router, page 5-12
- Configuring IP MLS on the Switch, page 5-18
- IP MLS Supported Network Topologies, page 5-29
- IP MLS Unsupported Network Topologies, page 5-33
- IP MLS Examples, page 5-35

## Understanding How IP MLS Works

These sections provide an overview of IP MLS and describe how IP MLS works:

- IP MLS Overview, page 5-2
- IP MLS Components, page 5-2
- IP MLS Flows, page 5-2
- Layer 3 MLS Cache, page 5-3
- Flow Masks, page 5-3
- Layer 3-Switched Packet Rewrite, page 5-5
- IP MLS Operation, page 5-6

- Standard and Extended Access Lists, page 5-7
- Packet Export Rate, page 5-8

## IP MLS Overview

IP MLS provides high-performance hardware-based Layer 3 switching for Catalyst 5000 family and 2926G series LAN switches. IP MLS switches unicast IP data packet flows between IP subnets using advanced ASIC switching hardware, offloading processor-intensive packet routing from network routers.

The packet forwarding function is moved onto Layer 3 switches whenever a partial or complete switched path exists between two hosts. Packets that do not have a partial or complete switched path to reach their destinations are still forwarded in software by routers. Standard routing protocols, such as Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol (RIP), and Intermediate System-to-Intermediate System (IS-IS), are used for route determination.

IP MLS allows you to debug and trace flows in your network. You can identify which switch is handling a particular flow by using MLS explorer packets. The explorer packets aid you in path detection and troubleshooting. For complete information on debugging IP MLS, see the “Using Debug Commands on the IP MLS Router” section on page 5-17.

In addition, IP MLS provides traffic statistics you can use to identify traffic characteristics for administration, planning, and troubleshooting. IP MLS uses NetFlow Data Export (NDE) to export flow statistics.

---

**Note** For more information about NDE, see Chapter 8, “Configuring NetFlow Data Export.”

---

## IP MLS Components

An IP MLS network topology consists of these components:

- Multilayer Switching-Switching Engine (MLS-SE)—Catalyst 5000 family switch with Supervisor Engine III or III F with the NetFlow Feature Card (NFFC) or NFFC II, or Supervisor Engine II G or III G, or a Catalyst 2926G series switch. The MLS-SE provides Layer 3 LAN-switching services.
- Multilayer Switching-Route Processor (MLS-RP)—A Catalyst 5000 family Route Switch Module (RSM) or Route Switch Feature Card (RSFC), or an externally connected Cisco 7500, 7200, 4700, 4500, or 3600 series router with software that supports IP MLS. The MLS-RP provides Cisco IOS-based multiprotocol routing and network services.

## IP MLS Flows

Layer 3 protocols, such as IP and Internetwork Packet Exchange (IPX), are connectionless—they deliver every packet independently of every other packet. However, actual network traffic consists of many end-to-end conversations, or flows, between users or applications.

A flow is a unidirectional sequence of packets between a particular source and destination that share the same protocol and transport-layer information. Communication from a client to a server and from the server to the client are separate flows. For example, Telnet traffic transferred from a particular source to a particular destination comprises a separate flow from File Transfer Protocol (FTP) packets between the same source and destination.

Flows are based only on Layer 3 addresses, which allow IP traffic from multiple users or applications to a particular destination to be carried on a single flow if only the destination IP address is used to identify a flow.

## Layer 3 MLS Cache

The NFFC (or NFFC II) maintains a Layer 3 switching table (the Layer 3 MLS cache) for Layer 3 switched flows. The cache also includes entries for traffic statistics that are updated in tandem with the switching of packets. After the MLS cache is created, packets identified as belonging to an existing flow can be Layer 3-switched based on the cached information. The MLS cache maintains flow information for all active flows.

An MLS cache entry is created for the initial packet of each flow. Upon receipt of a packet that does not match any flow currently in the MLS cache, a new IP MLS entry is created.

The state and identity of the flow are maintained while packet traffic is active; when traffic for a flow ceases, the entry ages out. You can configure the aging time for MLS entries kept in the MLS cache. If an entry is not used for the specified period of time, the entry ages out and statistics for that flow can be exported to a flow collector application.

The maximum MLS cache size is 128K. However, an MLS cache larger than 32K increases the probability that a flow will not be switched by the MLS-SE and will get forwarded to the router.

---

**Note** The number of active flows that can be stored in the MLS cache depends on the type of access lists configured on IP MLS router interfaces (which determines the flow mask). See the “Flow Masks” section on page 5-3 for additional information.

---

## Flow Masks

The MLS-SE uses flow masks to determine how MLS entries are created. The flow mask is based on the access lists configured on the MLS-RP (router) interfaces. The MLS-SE learns the flow mask through Multilayer Switching Protocol (MLSP) messages from each MLS-RP for which the MLS-SE is performing Layer 3 switching. MLSP is the protocol running between the MLS-SE and MLS-RP to enable MLS.

These sections describe how the flow mask modes work:

- Flow Mask Modes, page 5-3
- Flow Mask Mode and show mls entry Command Output, page 5-4

### Flow Mask Modes

An MLS-SE supports only one flow mask (the most specific one) for all MLS-RPs that are Layer 3 switched by that MLS-SE. If the MLS-SE detects different flow masks from different MLS-RPs for which it is performing Layer 3 switching, it changes its flow mask to the most specific flow mask detected.

When the MLS-SE flow mask changes, the entire MLS cache is purged. When an MLS-SE exports cached entries, flow records are created based on the current flow mask. Depending on the current flow mask, some fields in the flow record might not have values.

**Note** On a switch with Supervisor Engine III or III F with the NFFC II, and on the Supervisor Engine II G and III G, no values are displayed for the “Last Used” IP address and port fields in the **show mls entry** command output. A “0” or “-” is displayed.

The three flow masks are as follows:

- **destination-ip**—The least-specific flow mask. The MLS-SE maintains one MLS entry for each destination IP address. All flows to a given destination IP address use this MLS entry. This mode is used if there are no access lists configured on any of the MLS-RP interfaces.
- **source-destination-ip**—The MLS-SE maintains one MLS entry for each source and destination IP address pair. All flows between a given source and destination use this MLS entry regardless of the IP protocol ports. This mode is used if there is a standard access list on any of the MLS-RP interfaces.
- **ip-flow**—The most-specific flow mask. The MLS-SE creates and maintains a separate MLS cache entry for every IP flow. An ip-flow entry includes the source IP address, destination IP address, protocol, and protocol ports. This mode is used if there is an extended access list on any of the MLS-RP interfaces.

### Flow Mask Mode and show mls entry Command Output

This section describes how the flow mask impacts the screen output of the **show mls entry** command.

With the destination-ip flow mask, the source IP, protocol, and source and destination port fields show the details of the last packet that was Layer 3 switched using the MLS cache entry.

This example shows how the **show mls entry** command output appears in destination-ip mode:

```

Console> (enable) show mls entry
      Last Used          Last   Used
Destination IP  Source IP      Port DstPrt SrcPrt Destination Mac  Vlan Port
-----
MLS-RP 10.20.6.161:
10.19.6.2      10.19.26.9    UDP  6009   69     00-10-0b-16-98-00 250 1/1-2
10.19.22.8     10.19.2.1     TCP  6001   Telnet 00-00-00-00-00-08 22   4/6
10.19.2.1      10.19.22.8    TCP  6008   Telnet 00-10-0b-16-98-00 250 1/1-2
10.19.27.10    10.19.7.3     TCP  6003   20     00-00-00-00-00-10 27   4/8
10.19.28.11    10.19.8.4     UDP  6004   DNS    00-00-00-00-00-11 28   4/9
10.19.26.9     10.19.6.2     UDP  6002   69     00-00-00-00-00-09 26   4/7
10.19.7.3      10.19.27.10   TCP  6010   FTP    00-10-0b-16-98-00 250 1/1-2
MLS-RP 132.68.9.10:
10.19.86.12    10.19.85.7    TCP  6007   SMTP   00-00-00-00-00-12 86   4/10
10.19.85.7     10.19.86.12   TCP  6012   WWW    00-00-00-00-00-07 85   4/5
MLS-RP 10.20.6.82:
10.19.63.13    10.19.73.14   TCP  6014   Telnet 00-00-00-00-00-13 63   4/11
10.19.73.14    10.19.63.13   TCP  6013   FTP    00-00-00-00-00-14 73   4/12
Console> (enable)
    
```

With the source-destination-ip flow mask, the protocol, source port, and destination port fields show the details of the last packet that was Layer 3 switched using the MLS cache entry.

This example shows how the **show mls entry** command output appears in source-destination-ip mode:

```

Console> (enable) show mls entry

```

Destination IP	Source IP	Last		Used		Destination Mac	Vlan	Port
		Port	DstPrt	SrcPrt				
-----								
MLS-RP 10.20.6.161:								
10.19.26.9	10.19.6.2	UDP	6002	69		00-00-00-00-00-09	26	4/7
10.19.28.11	10.19.8.4	UDP	6004	DNS		00-00-00-00-00-11	28	4/9
10.19.6.2	10.19.26.9	UDP	6009	69		00-10-0b-16-98-00	251	1/1-2
10.19.2.1	10.19.22.8	TCP	6008	Telnet		00-10-0b-16-98-00	251	1/1-2
10.19.27.10	10.19.7.3	TCP	6003	20		00-00-00-00-00-10	27	4/8
10.19.22.8	10.19.2.1	TCP	6001	Telnet		00-00-00-00-00-08	22	4/6
10.19.7.3	10.19.27.10	TCP	6010	FTP		00-10-0b-16-98-00	251	1/1-2
MLS-RP 132.68.9.10:								
10.19.85.7	10.19.86.12	TCP	6012	WWW		00-00-00-00-00-07	85	4/5
10.19.86.12	10.19.85.7	TCP	6007	SMTP		00-00-00-00-00-12	86	4/10
MLS-RP 10.20.6.82:								
10.19.63.13	10.19.73.14	TCP	6014	Telnet		00-00-00-00-00-13	63	4/11
10.19.73.14	10.19.63.13	TCP	6013	FTP		00-00-00-00-00-14	73	4/12

```

Console> (enable)

```

With the ip-flow flow mask, details are shown for every flow because a separate MLS entry is created for every flow.

This example shows how the **show mls entry** command output appears in ip-flow mode:

```

Console> (enable) show mls entry

```

Destination IP	Source IP	Port	DstPrt	SrcPrt	Destination Mac	Vlan	Port
-----							
MLS-RP 10.20.6.161:							
10.19.26.9	10.19.6.2	UDP	6002	69	00-00-00-00-00-09	26	4/7
10.19.6.2	10.19.26.9	UDP	6009	69	00-10-0b-16-98-00	251	1/1-2
10.19.22.8	10.19.2.1	TCP	6001	Telnet	00-00-00-00-00-08	22	4/6
10.19.2.1	10.19.22.8	TCP	6008	Telnet	00-10-0b-16-98-00	251	1/1-2
10.19.27.10	10.19.7.3	TCP	6003	20	00-00-00-00-00-10	27	4/8
10.19.28.11	10.19.8.4	UDP	6004	DNS	00-00-00-00-00-11	28	4/9
10.19.7.3	10.19.27.10	TCP	6010	FTP	00-10-0b-16-98-00	251	1/1-2
MLS-RP 132.68.9.10:							
10.19.86.12	10.19.85.7	TCP	6007	SMTP	00-00-00-00-00-12	86	4/10
10.19.85.7	10.19.86.12	TCP	6012	WWW	00-00-00-00-00-07	85	4/5
MLS-RP 10.20.6.82:							
10.19.63.13	10.19.73.14	TCP	6014	Telnet	00-00-00-00-00-13	63	4/11
10.19.73.14	10.19.63.13	TCP	6013	FTP	00-00-00-00-00-14	73	4/12

```

Console> (enable)

```

## Layer 3-Switched Packet Rewrite

When a packet is Layer 3 switched from a source host to a destination host, the switch (MLS-SE) performs a packet rewrite based on information learned from the router (MLS-RP) and stored in the MLS cache.

If Host A and Host B are on different virtual LANs (VLANs) and Host A sends a packet to the MLS-RP to be routed to Host B, the MLS-SE recognizes that the packet was sent to the Media Access Control (MAC) address of the MLS-RP. The MLS-SE checks the MLS cache and finds the entry matching the flow in question.

When the MLS-SE receives the packet, it is formatted as follows:

Frame Header		IP Header				Payload	
Destination	Source	Destination	Source	TTL	Checksum	Data	Checksum
<i>MLS-RP MAC</i>	<i>Host A MAC</i>	<i>Host B IP</i>	<i>Host A IP</i>	<i>n</i>	<i>calculation1</i>		

The MLS-SE rewrites the Layer 2 frame header, changing the destination MAC address to the MAC address of Host B and the source MAC address to the MAC address of the MLS-RP (these MAC addresses are stored in the MLS cache entry for this flow). The Layer 3 IP addresses remain the same, but the IP header Time to Live (TTL) is decremented and the checksum is recomputed. The MLS-SE rewrites the switched Layer 3 packets so that they appear to have been routed by a router.

The MLS-SE forwards the rewritten packet to Host B’s VLAN (the destination VLAN is stored in the MLS cache entry) and Host B receives the packet.

After the MLS-SE performs the packet rewrite, the packet is formatted as follows:

Frame Header		IP Header				Payload	
Destination	Source	Destination	Source	TTL	Checksum	Data	Checksum
<i>Host B MAC</i>	<i>MLS-RP MAC</i>	<i>Host B IP</i>	<i>Host A IP</i>	<i>n+1</i>	<i>calculation2</i>		

---

**Note** Some Catalyst 5000 family switching modules have onboard hardware that performs the packet rewrite, maximizing IP MLS performance. This performance enhancement is also used on the Catalyst 2926G series switch ports. To determine whether a port supports packet rewrite, use the **show port capabilities** command. If the port does not support inline rewrite, the packet rewrite is done in the supervisor engine.

---

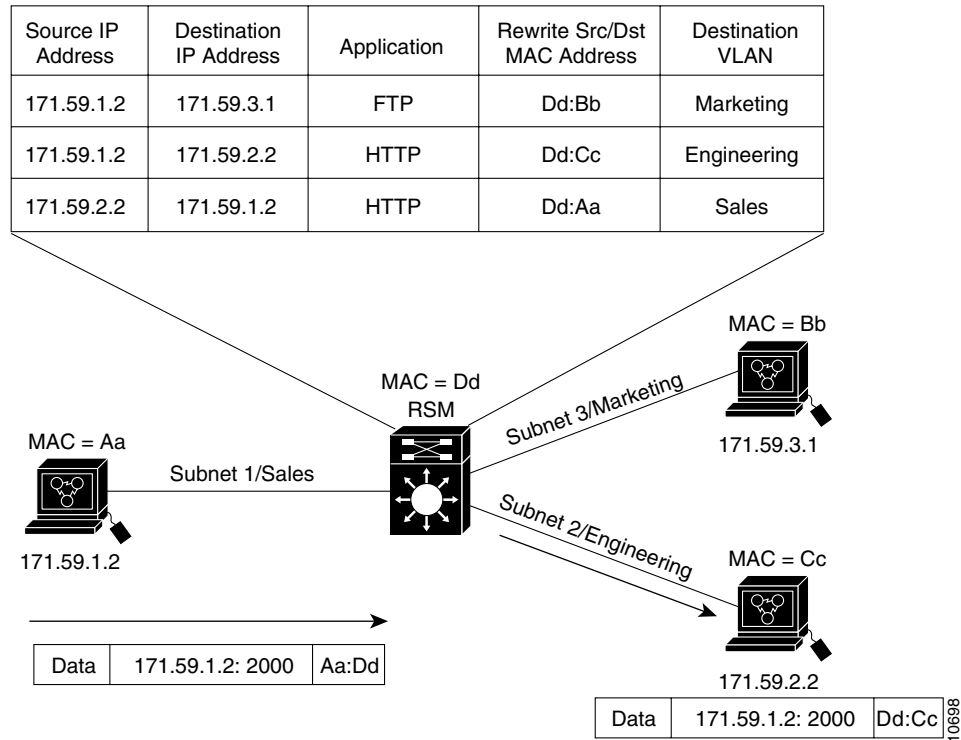
## IP MLS Operation

Figure 5-1 shows a simple IP MLS network topology. In this example, Host A is on the Sales VLAN (IP subnet 171.59.1.0), Host B is on the Marketing VLAN (IP subnet 171.59.3.0), and Host C is on the Engineering VLAN (IP subnet 171.59.2.0).

When Host A initiates an FTP file transfer to Host B, an MLS entry for this flow is created (this entry is the first item in the MLS cache shown in Figure 5-1). The MLS-SE stores the MAC addresses of the MLS-RP and Host B in the MLS entry when the MLS-RP forwards the first packet from Host A through the switch to Host B. The MLS-SE uses this information to rewrite subsequent packets from Station A to Station B.

Similarly, a separate MLS entry is created in the MLS cache for the HTTP traffic from Host A to Host C, and for the HTTP traffic from Host C to Host A. The destination VLAN is stored as part of each MLS entry so that the correct VLAN identifier is used when encapsulating traffic on trunk links.

Figure 5-1 IP MLS Example Topology



## Standard and Extended Access Lists

**Note** Router interfaces with input access lists cannot participate in IP MLS. However, you can translate any input access list to an output access list to provide the same effect on the interface.

IP MLS allows you to enforce access lists on every packet of the flow without compromising IP MLS performance. When you enable IP MLS, the MLS-SE handles standard and extended access list permit traffic at wire speed.

**Note** Access list deny traffic is always handled by the MLS-RP, not the MLS-SE.

Route topology changes and the addition or modification of access lists are reflected in the IP MLS switching path automatically on the MLS-SE. The techniques for handling route and access list changes apply to the RSM and to directly attached external routers.

For example, when Station A wants to communicate with Station B, it sends the first packet to the MLS-RP. If an access list is configured on the MLS-RP to deny access from Station A to Station B, the MLS-RP receives the packet, checks the access list to see if the packet flow is permitted, and discards the packet based on the access list. Because the first packet for this flow does not return from the MLS-RP, an MLS cache entry is not established by the MLS-SE.

If a flow is already being Layer 3 switched by the MLS-SE and the access list is created on the MLS-RP, the MLS-SE learns of the change through MLSP and immediately enforces security for the affected flow by purging it from the MLS cache. New flows are created based on the restrictions imposed by the access list.

Similarly, when the MLS-RP detects a routing topology change, the appropriate MLS cache entries are deleted in the MLS-SE. New flows are created based on the new topology.

## Packet Export Rate

---

**Note** Packets are exported only when NDE is enabled.

---

Export rates for MLS entries depend on the traffic pattern; there is no typical packet rate. The worst-case packet export rate occurs when all existing MLS entries are purged due to an event such as a route change. The MLS entries are exported at a burst rate of 1,213 datagrams of 27 flows each.

## Software and Hardware Requirements

IP MLS requires these software and hardware versions:

- Supervisor engine software release 4.1(1) or later
- Cisco IOS router software:
  - IOS release 12.0(3c)W5(8a) or later on the Route Switch Feature Card (RSFC)
  - IOS release 12.0(3c)W5(8) or later on the MLS-RP if running MLS over ATM media
  - IOS release 12.0(2) or later on Cisco 3600 series routers
  - IOS release 11.3(2)WA4(4) or later and IOS release 12.0(1) or later on the Route Switch Module (RSM), or Cisco 7500, 7200, 4700, and 4500 series routers
- If running MLS over ATM media, Catalyst 5000 family ATM module software release 11.3(8)WA4(11) or later, or release 12.0(3c)W5(10) or later
- Hardware:
  - Catalyst 2926G series switch, or a Catalyst 5000 family switch with Supervisor Engine II G or III G, or Supervisor Engine III or III F with a NetFlow Feature Card (NFFC) or NFFC II
  - RSM, RSFC, or external Cisco 7500, 7200, 4700, 4500, or 3600 series router
  - Catalyst 5000 family ATM module and a router with an ATM interface if running MLS over ATM media
  - (Optional) Inline-rewrite capable switching modules—These switching modules have onboard hardware that maximizes IP MLS performance (this performance enhancement is also used in the Catalyst 2926G series switches). Use the **show port capabilities** command to determine if your hardware supports inline rewrite.

---

**Note** When using IP MLS with the Gigabit Ethernet (WS-X5403) switching module, you must install the module in specific slots in the Catalyst 5000 family switches to maximize IP MLS operation. Refer to the *Catalyst 5000 Family Module Installation Guide* for details.

---

## Default IP MLS Configuration

Table 5-1 shows the default IP MLS configuration.

**Table 5-1 Default IP MLS Configuration**

Feature	Default Value
IP MLS enable state	Enabled
Participating routers	None <sup>1</sup>
IP MLS aging-time	256 seconds
IP MLS fast aging-time	0 seconds (no fast aging)
IP MLS fast aging-time packet threshold	0 packets
Minimum IP MLS flow mask	Varies depending on router access list configuration

<sup>1</sup> If an RSM is installed in the switch, the device is automatically included as a participating IP MLS router.

## Configuration Guidelines and Restrictions

These sections describe configuration guidelines that apply when configuring IP MLS:

- General Configuration Guidelines, page 5-9
- External Routers, page 5-9
- Access Lists, page 5-10
- IP MLS Interaction with Other Features, page 5-10
- Maximum Transmission Unit Size, page 5-11
- Restrictions on Using IP Router Commands with IP MLS Enabled, page 5-11

## General Configuration Guidelines

Follow these general guidelines when configuring IP MLS:

- When you enable IP MLS, the RSM or externally attached router continues to handle all non-IP-unicast traffic while offloading the routing of IP packets to the MLS-SE.
- Do not confuse IP MLS with the NetFlow switching supported by Cisco routers. MLS uses both the RSM or directly attached external router and the MLS-SE. With IP MLS, you are not required to use NetFlow switching on the RSM or directly attached external router; any switching path on the RSM or directly attached external router will work (process, fast, optimum, and so on).

## External Routers

Follow these guidelines when using an external router:

- We recommend one directly attached external router per switch to ensure that the MLS-SE caches the appropriate flow information from both sides of the routed flow.

- You can use Cisco high-end routers (Cisco 7500, 7200, 4700, and 4500 series) for IP MLS when they are externally attached to the switch. You can make the attachment in any of these configurations:
  - Fast or Gigabit Ethernet interface with Inter-Switch Link (ISL) or IEEE 802.1Q encapsulation on multiple subinterfaces (one per subnet)
  - ATM interface with LANE encapsulation on multiple subinterfaces (one per subnet)
  - Multiple Ethernet interfaces (one per subnet)
- You can connect end hosts through any media (Ethernet, Fast Ethernet, ATM, Fiber Distributed Data Interface [FDDI], or Token Ring) but the connection between the external router and the switch must be through standard Ethernet, Fast Ethernet, or Gigabit Ethernet interfaces, ISL trunk links, IEEE 802.1Q trunk links, or ATM LANE trunk links.

## Access Lists

Access lists affect IP MLS as follows:

- Input access lists—Input access lists are supported with IP MLS in Cisco IOS release 12.0(2) and later.

Prior to IOS release 12.0(2), input access lists are not supported with IP MLS and router interfaces with input access lists cannot participate in IP MLS. No packets destined for that interface are Layer 3 switched, even if the flow is not filtered by the access list. Existing flows for that interface are purged, and no new flows are cached.

---

**Note** You can translate input access lists to output access lists to provide the same effect on the interface.

---

- Output access lists—When an output access list is first applied to an interface, the MLS cache entries for that interface are purged. Entries associated with other interfaces are not affected; they follow their normal aging or purging procedures.

Applying an output access list that uses the **log**, **precedence**, **tos**, or **establish** options prevents the interface from participating in IP MLS.
- Access list impact on flow masks—Access lists impact the flow mask advertised to the MLS-SE by an MLS-RP. You can specify the minimum flow mask using the **set mls flow** command. For more information, see the “Flow Masks” section on page 5-3.
- Reflexive access lists—Router interfaces with reflexive access lists cannot participate in Layer 3 switching.

## IP MLS Interaction with Other Features

Other Cisco IOS software features affect IP MLS as follows:

- IP accounting—Enabling IP accounting on an IP MLS-enabled interface disables the IP accounting functions on that interface.

---

**Note** To collect statistics for the Layer 3-switched traffic, enable NDE. For information on configuring NDE, see Chapter 8, “Configuring NetFlow Data Export.”

---

- Data encryption—IP MLS is disabled on an interface when the data encryption feature is configured on the interface.
- Policy route-map—Policy routing is supported with IP MLS in Cisco IOS release 12.0(3) and later. Enter the **[no] mls rp ip route-map** global configuration command to allow policy routing in conjunction with IP MLS. IP MLS cannot function on interfaces that are configured to policy route based on packet length.

In Cisco IOS releases prior to release 12.0(3), IP MLS is disabled on an interface when a policy route-map is configured on the interface.

- TCP intercept—With IP MLS interfaces enabled, the TCP intercept feature (enabled in global configuration mode) might not work properly. When you enable TCP intercept, the following message displays:  

```
Command accepted, interfaces with mls might cause inconsistent behavior.
```
- Network Address Translation (NAT)—IP MLS is disabled on an interface when NAT is configured on the interface.
- Committed access rate (CAR)—IP MLS is disabled on an interface when CAR is configured on the interface.

## Maximum Transmission Unit Size

The maximum transmission unit (MTU) for an IP MLS interface must be the default Ethernet MTU, 1500 bytes.

To change the MTU on an IP MLS-enabled interface, you must first disable IP MLS on the interface (enter the **no mls rp ip** command on the interface). If you attempt to change the MTU with IP MLS enabled, the following message displays:

```
Need to turn off the mls router for this interface first.
```

If you attempt to enable IP MLS on an interface that has an MTU value other than the default value, the following message displays:

```
mls only supports interfaces with default mtu size
```

## Restrictions on Using IP Router Commands with IP MLS Enabled

When you enable some IP processes on an interface, you will disable IP MLS on the interface. Table 5-2 shows the affected commands.

**Table 5-2 IP Router Command Restrictions**

Command	Behavior
<b>clear ip route</b>	Clears all MLS cache entries for all switches performing Layer 3 switching for this MLS-RP.
<b>ip routing</b>	The <b>no</b> form purges all MLS cache entries and disables IP MLS on this MLS-RP.
<b>ip security</b> (all forms of this command)	Disables IP MLS on the interface.
<b>ip tcp compression-connections</b>	Disables IP MLS on the interface.
<b>ip tcp header-compression</b>	Disables IP MLS on the interface.

## Configuring IP MLS on the Router

These sections describe how to configure one or more routers for IP MLS. Depending upon your configuration, you might not have to perform all the steps in the procedure.

- Enabling IP MLS on the Router, page 5-12
- Adding an IP MLS Interface to a VTP Domain, page 5-12
- Assigning a VLAN ID to a Router Interface, page 5-13
- Enabling IP MLS on a Router Interface, page 5-14
- Specifying a Router Interface as a Management Interface, page 5-14
- Removing a Router Interface as a Management Interface, page 5-14
- Disabling IP MLS on a Router Interface, page 5-15
- Clearing a VLAN ID from a Router Interface, page 5-15
- Removing an Interface from a VTP Domain (Including the Null Domain), page 5-15
- Disabling IP MLS on the Router, page 5-16
- Monitoring IP MLS on the Router, page 5-16
- Using Debug Commands on the IP MLS Router, page 5-17

---

**Note** For information on configuring interVLAN routing on the RSM and external routers, see Chapter 3, “Configuring InterVLAN Routing.”

---

For information on configuring IP MLS on the switch, see the “Configuring IP MLS on the Switch” section on page 5-18.

## Enabling IP MLS on the Router

To use IP MLS, you must globally enable IP MLS on the router.

To enable IP MLS globally on the MLS-RP, perform this task in global configuration mode:

Task	Command
Globally enable IP MLS on the router.	<b>mls rp ip</b>

This example shows how to enable IP MLS globally on the router:

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

## Adding an IP MLS Interface to a VTP Domain

---

**Note** Perform this configuration task only if the switch is a VTP server or client.

---

Determine which router interfaces you will use as IP MLS interfaces and add those interfaces to the same VTP domain as the MLS-SE.

To view the VTP configuration on the switch, including the VTP domain name, enter the **show vtp domain** command on the switch.



**Caution** Perform this task before you enter any other IP MLS interface commands on the IP MLS interface (specifically, the **mls rp ip** interface command or **mls rp management-interface** interface command). Entering IP MLS interface commands on an interface prior to putting the interface into a VTP domain places the interface in the null domain. To put the IP MLS interface into a domain other than the null domain, you must clear the IP MLS interface configuration before you can add it to another VTP domain (for more information, see the “Removing an Interface from a VTP Domain (Including the Null Domain)” section on page 5-15).

On ISL or 802.1Q trunk links, enter the **mls rp vtp-domain** command on the primary interface (not on the individual subinterfaces). All subinterfaces on the primary interface inherit the VTP domain assigned to the primary interface.

To add an IP MLS interface to a VTP domain, perform this task in interface configuration mode:

Task	Command
Add an IP MLS interface to a VTP domain.	<b>mls rp vtp-domain</b> [domain_name]

This example shows how to add an IP MLS interface to a VTP domain:

```
Router(config-if)#mls rp vtp-domain engineering
Router(config-if)#
```

## Assigning a VLAN ID to a Router Interface

**Note** This task is not required for RSM VLAN interfaces (virtual interfaces), ISL-encapsulated interfaces, and 802.1Q-encapsulated interfaces.

**Note** Make sure you add the interface to a VTP domain *before* performing this task. For more information, see the “Adding an IP MLS Interface to a VTP Domain” section on page 5-12.

In these configurations, the IP MLS interface must have a VLAN ID configured before you can enable it for IP MLS:

- ATM interface with LANE encapsulation and multiple subinterfaces (one per subnet/VLAN)
- Ethernet, Fast Ethernet, or Gigabit Ethernet interface with no subinterfaces. (one physical interface per subnet/VLAN)

To assign a VLAN ID to an IP MLS interface, perform this task in interface configuration mode:

Task	Command
Assign a VLAN ID to an IP MLS interface.	<b>mls rp vlan-id</b> [vlan_id_num]

This example shows how to assign a VLAN ID to an IP MLS interface:

```
Router(config-if)#mls rp vlan-id 23
Router(config-if)#
```

## Enabling IP MLS on a Router Interface

---

**Note** Make sure you add the interface to a VTP domain *before* performing this task. For more information, see the “Adding an IP MLS Interface to a VTP Domain” section on page 5-12.

---

To enable IP MLS on a specific router interface, perform this task in interface configuration mode:

Task	Command
Specify a router interface for IP MLS.	<b>mls rp ip</b>

This example shows how to enable IP MLS on a router interface:

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

## Specifying a Router Interface as a Management Interface

MLSP packets are sent and received through the management interface. You must specify at least one router interface as a management interface. If you do not specify a management interface, IP MLS will not function.

Every switch participating in IP MLS must have an active port in at least one VLAN that has a corresponding router interface configured as a management interface. If the VLAN to which the management interface belongs does not span the whole IP MLS network, you must configure multiple management interfaces such that each switch has an active port in a VLAN with a management interface.

To specify a router interface as a management interface, perform this task in interface configuration mode:

Task	Command
Specify an interface as the management interface.	<b>mls rp management-interface</b>

This example shows how to specify a router interface as a management interface:

```
Router(config-if)#mls rp management-interface
Router(config-if)#
```

## Removing a Router Interface as a Management Interface

To remove a router interface as a management interface, perform this task in interface configuration mode:

Task	Command
Remove an interface as the management interface.	<b>no mls rp management-interface</b>

This example shows how to remove a router interface as a management interface:

```
Router(config-if)#no mls rp management-interface
Router(config-if)#
```

## Disabling IP MLS on a Router Interface

To disable IP MLS on a specific router interface, perform this task in interface configuration mode:

Task	Command
Remove a router interface from IP MLS.	<b>no mls rp ip</b>

This example shows how to disable IP MLS on a router interface:

```
Router(config-if)#no mls rp ip
Router(config-if)#
```

## Clearing a VLAN ID from a Router Interface

---

**Note** This task does not apply for RSM VLAN interfaces (virtual interfaces), ISL-encapsulated interfaces, and 802.1Q-encapsulated interfaces.

---

Removing the VLAN ID from an interface disables IP MLS for the interface.

To clear a VLAN ID from an IP MLS interface, perform this task in interface configuration mode:

Task	Command
Remove a VLAN ID from an IP MLS interface.	<b>no mls rp vlan-id [vlan_id_num]</b>

This example shows how to clear a VLAN ID from an IP MLS interface:

```
Router(config-if)#no mls rp vlan-id 23
Router(config-if)#
```

## Removing an Interface from a VTP Domain (Including the Null Domain)

To remove an interface from a VTP domain (including the null domain) and add it to another domain, perform this task in interface configuration mode:

Task	Command
<b>Step 1</b> Clear the IP MLS configuration on the interface, if necessary.	<b>no mls rp ip</b> <b>no mls rp management-interface</b>
<b>Step 2</b> Remove the interface from the VTP domain.	<b>no mls rp vtp-domain [domain_name]</b>
<b>Step 3</b> Add the interface to a new VTP domain.	<b>mls rp vtp-domain [domain_name]</b>

This example shows how to remove an interface from one VTP domain (including the null domain) and add it to another VTP domain:

```
Router(config-if)#no mls rp ip
Router(config-if)#no mls rp management-interface
Router(config-if)#no mls rp vtp-domain engineering
Router(config-if)#mls rp vtp-domain wbu
Router(config-if)#
```

## Disabling IP MLS on the Router

To disable IP MLS on the router, perform this task in global configuration mode:

Task	Command
Globally disable IP MLS on the router.	<b>no mls rp ip</b>

This example shows how to disable IP MLS on the router:

```
Router(config)#no mls rp ip
Router(config)#
```

## Monitoring IP MLS on the Router

The **show mls rp** command displays IP MLS details, including specific information about MLSP. The output of the **show mls rp** command includes:

- IP MLS status (enabled or disabled) for switch interfaces and subinterfaces
- Flow mask used by this device when creating Layer 3-switching entries for the router
- Current settings for the keepalive timer, retry timer, and retry count
- MLSP-ID used in MLSP messages
- List of interfaces in all VTP domains that are enabled for IP MLS

To display detailed IP MLS information on the router, perform one of these tasks in privileged mode:

Task	Command
Show IP MLS details for all interfaces.	<b>show mls rp</b> <i>[interface]</i>
Show IP MLS interfaces for a specific VTP domain.	<b>show mls rp vtp-domain</b> <i>[domain_name]</i>

This example shows how to display details about IP MLS on the router:

```
Router# show mls rp
multilayer switching is globally enabled
mls id is 00e0.fefc.6000
mls ip address 10.20.26.64
mls flow mask is ip-flow

vlan domain name: WBU
current flow mask: ip-flow
current sequence number: 80709115
current/maximum retry count: 0/10
current domain state: no-change
current/next global purge: false/false
current/next purge count: 0/0
domain uptime: 13:03:19
keepalive timer expires in 9 seconds
retry timer not running
change timer not running
fcp subblock count = 7

1 management interface(s) currently defined:
vlan 1 on Vlan1
```

```

7 mac-vlan(s) configured for multi-layer switching:

  mac 00e0.fefc.6000
  vlan id(s)
    1   10   91   92   93   95   100

router currently aware of following 1 switch(es):
  switch id 0010.1192.b5ff

Router#

```

This example shows how to display IP MLS information about a specific interface (in this case, interface vlan 10):

```

Router# show mls rp interface vlan 10
mls active on Vlan10, domain WBU
Router#

```

This example shows how to show detailed information about IP MLS interfaces in a specific VTP domain:

```

Router# show mls rp vtp-domain WBU
vlan domain name: WBU
  current flow mask: ip-flow
  current sequence number: 80709115
  current/maximum retry count: 0/10
  current domain state: no-change
  current/next global purge: false/false
  current/next purge count: 0/0
  domain uptime: 13:07:36
  keepalive timer expires in 8 seconds
  retry timer not running
  change timer not running
  fcp subblock count = 7

1 management interface(s) currently defined:
  vlan 1 on Vlan1

7 mac-vlan(s) configured for multi-layer switching:

  mac 00e0.fefc.6000
  vlan id(s)
    1   10   91   92   93   95   100

router currently aware of following 1 switch(es):
  switch id 0010.1192.b5ff

Router#

```

## Using Debug Commands on the IP MLS Router

Table 5-3 describes IP MLS-related debug commands that you can use to troubleshoot IP MLS problems on the router.

**Table 5-3 IP MLS Debug Commands**

Command	Description
[no] debug mls rp events	Displays a run-time sequence of events for MLSP.
[no] debug mls rp packets	Displays packet contents (in verbose and hexadecimal formats) for MLSP messages.
[no] debug mls rp error	Displays error messages related to MLS.

Command	Description
[no] debug mls rp ip	Turns on IP-related events for MLS, including route purging and changes of access lists and flow masks.
[no] debug mls rp locator	Identifies which switch is switching a particular flow by using MLS explorer packets.
[no] debug mls rp all	Turns on all MLS debugging events.

## Configuring IP MLS on the Switch

IP MLS is enabled by default on Catalyst 5000 family and 2926G series switches. If the MLS-RP is an RSM installed in the Catalyst 5000 family switch chassis, you do not need to configure the switch. You only need to configure the switch in these circumstances:

- You have an external router as the MLS-RP (this is always the case with the Catalyst 2926G series switches)
- You want to change the IP MLS aging time
- You want to enable NDE

These sections describe how to configure IP MLS on the switch:

- Enabling IP MLS on the Switch, page 5-19
- Specifying Routers to Participate in IP MLS, page 5-19
- Specifying IP MLS Aging-Time Value, page 5-20
- Specifying IP MLS Fast Aging Time and Packet Threshold Values, page 5-20
- Setting the Minimum IP MLS Flow Mask, page 5-21
- Removing Routers from Participation in IP MLS, page 5-21
- Disabling IP MLS on the Switch, page 5-22
- Displaying CAM Entries on the Switch, page 5-22
- Displaying IP MLS Information, page 5-23
- Displaying IP MLS Cache Entries, page 5-24
- Clearing MLS Cache Entries, page 5-26
- Displaying IP MLS Statistics, page 5-27
- Clearing IP MLS Statistics, page 5-28
- Displaying IP MLS Debug Information, page 5-29

---

**Note** For information on configuring VLANs on the switch, refer to the “Configuring VTP and VLANs on the Switch” section on page 3-3.

---

For information on configuring IP MLS on the router, see the “Configuring IP MLS on the Router” section on page 5-12.

## Enabling IP MLS on the Switch

When you enable IP MLS on the switch, the switch (MLS-SE) starts to process MLSP messages from the MLS-RPs and starts Layer 3 switching. IP MLS is enabled by default on the MLS-SE.

To enable IP MLS on the switch, perform this task in privileged mode:

Task	Command
<b>Step 1</b> Enable IP MLS on the switch.	<b>set mls enable</b>
<b>Step 2</b> Verify that IP MLS is enabled.	<b>show mls [noalias]</b>

This example shows how to enable IP MLS on the switch and verify the configuration:

```
Console> (enable) set mls enable
Multilayer switching is enabled
Console> (enable)
```

## Specifying Routers to Participate in IP MLS

If the MLS-RP is an external router, you must specify the IP address of an interface on the MLS-RP to participate in IP MLS. The MLS-SE does not process MLSP messages from external routers that have not been included as MLS-RPs.

If an RSM is installed in the switch, it participates in IP MLS automatically and is included in the inclusion list (provided the device is running the correct Cisco IOS software version). If you physically remove the RSM or if you disable IP MLS on the RSM, the device is removed from the inclusion list.

On the Catalyst 2926G series switches, you must specify at least one external router to participate in IP MLS.

---

**Note** Before specifying a router to participate in IP MLS, enter the **show mls rp** command on the router to identify the MLS-RP IP address. Use the displayed address when you enter the **set mls include ip\_addr** command on the switch.

---

To specify a router to participate in IP MLS, perform this task in privileged mode:

Task	Command
<b>Step 1</b> On the switch, specify the IP address of the MLS-RP to participate in IP MLS.	<b>set mls include [ip_addr]</b>
<b>Step 2</b> Verify the configuration.	<b>show mls include</b>

---

**Note** You can specify the IP addresses of multiple MLS-RPs on the same command line. Up to 16 MLS-RPs can be selected to participate in IP MLS.

---

This example shows how to identify the MLS-RP IP address on the router, how to specify the MLS-RP to participate in IP MLS, and how to verify the configuration:

```
Console> (enable) set mls include 170.170.2.1
Multilayer switching is enabled for router 170.170.2.1
Console> (enable) show mls include
```

```
Included MLS-RP
-----
170.67.2.13
170.67.2.12
Console> (enable)
```

### Specifying IP MLS Aging-Time Value

The IP MLS aging time applies to all MLS cache entries. Any MLS entry that has not been used for *agingtime* seconds is aged out. The default is 256 seconds.

You can configure the aging time in the range of 8 to 2032 seconds in 8-second increments. Any aging-time value that is not a multiple of 8 seconds is adjusted to the closest one. For example, a value of 65 is adjusted to 64 and a value of 127 is adjusted to 128.

Other events might cause MLS entries to be purged, such as routing changes or a change in link state (MLS-SE link down).

---

**Note** We recommend that you keep the number of MLS entries in the MLS cache below 32K. If the number of MLS entries is more than 32K, some flows are sent to the router. To help keep the size of the MLS cache down, enable IP MLS fast aging, as described in the “Specifying IP MLS Fast Aging Time and Packet Threshold Values” section on page 5-20.

---

To specify the IP MLS aging time, perform this task in privileged mode:

Task	Command
Specify the IP MLS aging time for an MLS cache entry.	<b>set mls agingtime</b> [ <i>agingtime</i> ]

This example shows how to set the IP MLS aging time:

```
Console> (enable) set mls agingtime 512
Multilayer switching aging time set to 512
Console> (enable)
```

### Specifying IP MLS Fast Aging Time and Packet Threshold Values

To help keep the MLS cache size below 32K, enable IP MLS fast aging time. The IP MLS fast aging time applies to MLS entries that have no more than *pkt\_threshold* packets switched within *fastagingtime* seconds after it is created. A typical cache entry that is removed is the entry for flows to and from a Domain Name Server (DNS) or TFTP server; the entry might never be used again after it is created. Detecting and aging out these entries saves space in the MLS cache for other data traffic.

The default *fastagingtime* value is 0 (no fast aging). You can configure the *fastagingtime* value to 32, 64, 96, or 128 seconds. Any *fastagingtime* value that is not configured exactly as the indicated values is adjusted to the closest one. You can configure the *pkt\_threshold* value to 0, 1, 3, 7, 15, 31, or 63 packets.

If you need to enable IP MLS fast aging time, initially set the value to 128 seconds. If the size of the MLS cache continues to grow over 32K, decrease the setting until the cache size stays below 32K. If the cache continues to grow over 32K, decrease the normal IP MLS aging time.

Typical values for *fastagingtime* and *pkt\_threshold* are 32 seconds and 0 packets (no packets switched within 32 seconds after the entry is created).

To specify the IP MLS fast aging time and packet threshold, perform this task in privileged mode:

Task	Command
Specify the IP MLS fast aging time and packet threshold for an MLS cache entry.	<b>set mls agingtime fast</b> <i>[fastagingtime]</i> <i>[pkt_threshold]</i>

This example shows how to set the IP MLS fast aging time to 32 seconds with a packet threshold of 0 packets:

```
Console> (enable) set mls agingtime fast 32 0
Multilayer switching fast aging time set to 32 seconds for entries with no more than 0
packets switched.
Console> (enable)
```

## Setting the Minimum IP MLS Flow Mask

You can set the minimum granularity of the flow mask for the MLS cache on the MLS-SE. The actual flow mask used will be at least of the granularity specified by this command. For information on how the different flow masks work, see the “Flow Masks” section on page 5-3.

For example, if you do not configure access lists on any MLS-RP, then the IP MLS flow mask on the MLS-SE is destination-ip by default. However, you can force the MLS-SE to use the source-destination-ip flow mask by setting the minimum IP MLS flow mask using the **set mls flow destination-source** command. If an extended access list is configured on MLS-RP, then the flow mask is changed to ip-flow, which is a more granular flow mask than the configured source-destination-ip flow mask.



**Caution** Be careful when using this command. This command purges all existing shortcuts in the MLS cache and affects the number of active shortcuts on the MLS-SE.

To specify the minimum IP MLS flow mask, perform this task in privileged mode:

Task	Command
Specify the minimum IP MLS flow mask.	<b>set mls flow</b> { <b>destination</b>   <b>destination-source</b>   <b>full</b> }

This example shows how to set the minimum IP MLS flow mask to destination-source-ip:

```
Console> (enable) set mls flow destination-source
Configured flow mask is set to destination-source flow.
Console> (enable)
```

## Removing Routers from Participation in IP MLS

To remove a router from the list of routers participating in IP MLS, perform this task in privileged mode:

Task	Command
Remove an MLS-RP from participation in IP MLS.	<b>clear mls include</b> <i>[ip_addr]</i> <b>[all]</b>

---

**Note** You cannot remove an RSM or RSFC installed in the switch from the inclusion list using the **clear mls include** command. To remove an RSM or RSFC from the inclusion list, you must disable IP MLS on the RSM or RSFC or physically remove the RSM or RSFC from the switch.

---

This example shows how to remove a router from the IP MLS inclusion list on the switch:

```
Console> (enable) clear mls include stargate
Multilayer switching is disabled for router 170.20.15.1 (Stargate)
Console> (enable)
```

## Disabling IP MLS on the Switch

When you disable IP MLS on the switch, the MLS-SE does not process any MLSP messages from any MLS-RPs, and all existing MLS cache entries are purged.

---

**Note** If NDE is enabled and you disable IP MLS, you lose the statistics for existing cache entries. The flow statistics are not exported.

---

To disable IP MLS on the switch, perform this task in privileged mode:

Task	Command
<b>Step 1</b> Disable IP MLS on the switch.	<b>set mls disable</b>
<b>Step 2</b> Verify that IP MLS is disabled.	show mls

This example shows how to disable IP MLS on the switch:

```
Console> (enable) set mls disable
Multilayer switching is disabled
Console> (enable)
```

## Displaying CAM Entries on the Switch

The **show cam** command displays the content-addressable memory (CAM) entries associated with a specific MAC address. If the MAC address belongs to an MLS-RP, an “R” is appended to the MAC address.

If you specify a VLAN number, only those CAM entries corresponding to that VLAN number are displayed. If a VLAN is not specified, entries for all VLANs are displayed.

The **show cam mlsrp** command displays entries in the forwarding table for the specified MLS-RP.

To display CAM entries on the switch, perform one of these tasks:

Task	Command
• Show CAM entries by MAC address.	<b>show cam</b> [ <i>mac_addr</i> ] [ <i>vlan</i> ]
• Show CAM entries for a router.	<b>show cam mlsrp</b> [ <i>ip_addr</i> ] [ <i>vlan</i> ]

This example shows how to display the CAM entries on the switch:

```

Console> (enable) show cam 00-10-29-8a-4c-00
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.

VLAN  Dest MAC/Route Des  Destination Ports or VCs / [Protocol Type]
-----
10     00-10-29-8a-4c-00R  9/1                               IP
51     00-10-29-8a-4c-00R  9/1                               IP
52     00-10-29-8a-4c-00R  9/1                               IP
53     00-10-29-8a-4c-00#  9/1                               IP
54     00-10-29-8a-4c-00#  9/1                               IP
Total Matching CAM Entries Displayed = 5
Console> (enable)

```

This example shows how to display CAM entries for the specified MLS-RP:

```

Console> (enable) show cam mlsrp 10.1.1.3
VLAN Destination MAC      Destination Ports or VCs  Xtag Status
-----
52     00-10-29-8a-4c-00R  9/1                       5  H
51     00-10-29-8a-4c-00R  9/1                       5  H
10     00-10-29-8a-4c-00R  9/1                       5  H
Total Matching CAM Entries Displayed = 3
Console> (enable)

```

## Displaying IP MLS Information

The **show mls** command displays IP MLS information and MLS-RP-specific information. The **show mls rp** command displays MLS-RP-specific information for the specified MLS-RP.

To display IP MLS information on the switch, perform one of these tasks:

Task	Command
• Show general IP MLS information and router-specific information for all MLS-RPs.	<b>show mls [noalias]</b>
• Show router-specific information for a specified MLS-RP.	<b>show mls rp [ip_addr] [noalias]</b>

This example shows how to display IP MLS information on the switch:

```

Console> (enable) show mls
Multilayer switching enabled
Multilayer switching aging time = 256 seconds
Multilayer switching fast aging time = 0 seconds, packet threshold = 1
Destination-ip flow
Total packets switched = 101892
Active entries = 2153
Netflow data export enabled
Netflow data export configured for port 8010 on host 10.0.2.15
Total packets exported = 20

MLS-RP IP    MLS-RP ID      Xtag  MLS-RP MAC-Vlans
-----
172.20.25.2 0000808cece0  2     00-00-80-8c-ec-e0 1-20
          00-00-80-8c-ec-e1 21-30
          00-00-80-8c-ec-e2 31-40
          00-00-80-8c-ec-e3 41-50
          00-00-80-8c-ec-e4 51-60

```

```
172.20.27.1 0000808c1214 3 00-00-80-8c-12-14 1-20,31-40
00-00-80-8c-12-15 21-30
00-00-80-8c-12-16 41-50
```

Console> (enable)

This example shows how to display IP MLS information for a specific MLS-RP:

```
Console> (enable) show mls rp 172.20.25.2
MLS-RP IP    MLS-RP ID      Xtag  MLS-RP MAC-Vlans
-----
172.20.25.2 0000808cece0  2     00-00-80-8c-ec-e0 1-20
00-00-80-8c-ec-e1 21-30
00-00-80-8c-ec-e2 31-40
00-00-80-8c-ec-e3 41-50
00-00-80-8c-ec-e4 51-60
```

Console> (enable)

## Displaying IP MLS Cache Entries

---

**Note** For a description of how the flow mask mode affects the screen displays when showing MLS entries, see the “Flow Mask Mode and show mls entry Command Output” section on page 5-4.

---

These sections describe how to display MLS cache entries on the switch:

- Displaying All MLS Entries, page 5-24
- Displaying MLS Entries for a Specific Destination Address, page 5-25
- Displaying Entries for a Specific Source Address, page 5-25
- Displaying Entries for a Specific IP Flow, page 5-25
- Displaying Entries for a Specific MLS-RP, page 5-26

### Displaying All MLS Entries

To display all MLS entries on the switch, perform this task in privileged mode:

Task	Command
Show all MLS entries.	<b>show mls entry</b>

This example shows how to display all MLS entries on the switch:

```
Console> (enable) show mls entry
Last Used      Last      Used
Destination IP Source IP   Port DstPrt SrcPrt Destination Mac  Vlan Port
-----
MLS-RP 10.20.6.161:
10.19.6.2      10.19.26.9  UDP 6009 69    00-10-0b-16-98-00 250 1/1-2
10.19.26.9     10.19.6.2  UDP 6002 69    00-00-00-00-00-09 26  4/7
MLS-RP 132.68.9.10:
10.19.86.12   10.19.85.7  TCP 6007  SMTP 00-00-00-00-00-12 86  4/10
10.19.85.7    10.19.86.12 TCP 6012  WWW  00-00-00-00-00-07 85  4/5
MLS-RP 10.20.6.82:
10.19.63.13   10.19.73.14 TCP 6014  Telnet 00-00-00-00-00-13 63  4/11
10.19.73.14   10.19.63.13 TCP 6013  FTP  00-00-00-00-00-14 73  4/12
Console> (enable)
```



This example shows how to display MLS entries for a specific IP flow:

```

Console> (enable) show mls entry flow tcp 23 37819
Destination IP   Source IP       Port DstPrt SrcPrt Destination Mac   Vlan Port
-----
MLS-RP 51.0.0.3:
10.0.2.15      51.0.0.2       TCP  37819  Telnet 08-00-20-7a-07-75 10   3/1
Console> (enable)
    
```

### Displaying Entries for a Specific MLS-RP

To display MLS entries for a specific MLS-RP, perform this task in privileged mode:

Task	Command
Show MLS entries for the specified MLS-RP.	<b>show mls entry rp <i>ip_addr</i></b>

This example shows how to display MLS entries for a specific MLS-RP:

```

Console> (enable) show mls entry rp 172.20.27.1
Destination IP   Source IP       Port DstPrt SrcPrt Destination Mac   Vlan Port
-----
MLS-RP 172.20.27.1:
172.20.22.16    172.20.27.139 TCP  DNS    DNS    00-60-70-6c-fc-24 4    2/3
172.20.21.17    172.20.27.138 TCP  7001   7003   00-60-70-6c-fc-25 3    2/4
Console> (enable)
    
```

### Clearing MLS Cache Entries

The **clear mls entry** command removes specific MLS cache entries on the switch. The **all** keyword clears all MLS entries. The **destination** and **source** keywords specify the source and destination IP addresses. The destination and source *ip\_addr\_spec* can be a full IP address or a subnet address in the format *ip\_subnet\_addr*, *ip\_addr/subnet\_mask*, or *ip\_addr/subnet\_mask\_bits*.

The **flow** keyword specifies the following additional flow information:

- Protocol family (*protocol*)—Specify **tcp**, **udp**, **icmp**, or a decimal number for other protocol families. A value of zero (0) for *protocol* is treated as a wildcard and entries for all protocols are cleared (unspecified options are treated as wildcards).
- TCP or UDP source and destination port numbers (*src\_port* and *dst\_port*)—If the protocol you specify is TCP or UDP, specify the source and destination TCP or UDP port numbers. A value of zero (0) for *src\_port* or *dst\_port* is treated as a wildcard, and entries for all source or destination ports are cleared (unspecified options are treated as wildcards). For other protocols, set the *src\_port* and *dst\_port* to 0, or no entries will be cleared.

To clear an MLS entry, perform this task in privileged mode:

Task	Command
Clear an MLS entry on the switch.	<b>clear mls entry destination [<i>ip_addr_spec</i>] source [<i>ip_addr_spec</i>] flow [<i>protocol src_port dst_port</i>] [all]</b>

This example shows how to clear MLS entries with destination IP address 172.20.26.22:

```

Console> (enable) clear mls entry destination 172.20.26.22
Console> (enable)
    
```

This example shows how to clear MLS entries with destination IP address 172.20.22.113, TCP source port 1652, and TCP destination port 23:

```
Console> (enable) clear mls entry destination 172.20.26.22 source 172.20.22.113 flow
tcp 1652 23
Console> (enable)
```

## Displaying IP MLS Statistics

These sections describe how to display a variety of IP MLS statistics:

- Displaying IP MLS Statistics by Protocol, page 5-27
- Displaying Statistics for MLS-RPs, page 5-27
- Displaying Statistics for MLS Cache Entries, page 5-28

### Displaying IP MLS Statistics by Protocol

The **show mls statistics protocol** command displays IP MLS statistics by protocol (such as Telnet, FTP, and WWW). The **protocol** keyword functions only if the flow mask mode is ip-flow. Use the **show mls** command to see the current flow mask.

To display IP MLS statistics by protocol, perform this task in privileged mode:

Task	Command
Show IP MLS statistics by protocol (only if IP MLS is in ip-flow mode).	<b>show mls statistics protocol</b>

This example shows how to display IP MLS statistics by protocol:

```
Console> (enable) show mls statistics protocol
Protocol  TotalFlows  TotalPackets  Total Bytes
-----  -
Telnet    900         630           4298
FTP       688         2190          3105
WWW       389         42679         623686
SMTP      802         4966          92873
X         142         2487          36870
DNS       1580        52            1046
Others    82          1             73
Total    6583        53005         801951
Console> (enable)
```

### Displaying Statistics for MLS-RPs

The **show mls statistics rp** command displays IP MLS statistics for MLS-RPs. If you do not specify a particular MLS-RP, statistics for all MLS-RPs are displayed.

To display IP MLS statistics for MLS-RPs, perform this task in privileged mode:

Task	Command
Show IP MLS statistics for MLS-RPs. If a particular MLS-RP is not specified, statistics for all MLS-RPs are shown.	<b>show mls statistics rp</b> [ <i>ip_addr</i> ] [ <i>noalias</i> ]

This example shows how to display IP MLS statistics for all MLS-RPs:

```

Console> (enable) show mls statistics rp
Total packets switched = 212540292
Active shortcuts = 2000
Total packets exported= 1889

MLS-RP IP           MLS-RP ID           Total switched
                    packets      bytes
-----
10.20.26.64        00e0fefc6000        7877192 803473584
Console> (enable)
    
```

### Displaying Statistics for MLS Cache Entries

The **show mls statistics entry** command displays IP MLS statistics for MLS cache entries. Specify the destination IP address, source IP address, protocol, and source and destination ports to see specific MLS cache entries.

A value of zero (0) for *src\_port* or *dst\_port* is treated as a wildcard, and all statistics are displayed (unspecified options are treated as wildcards). If the protocol specified is not TCP or UDP, set the *src\_port* and *dstprt* to 0 or no statistics will be displayed.

To display statistics for MLS cache entries, perform this task in privileged mode:

Task	Command
Show statistics for MLS cache entries. If a specific MLS cache entry is not specified, all statistics are shown.	<b>show mls statistics entry</b> [ <b>destination</b> <i>ip_addr_spec</i> ] [ <b>source</b> <i>ip_addr_spec</i> ] [ <b>flow protocol</b> <i>src_port dst_port</i> ]

This example shows how to display statistics for a particular MLS cache entry:

```

Console> (enable) show mls statistics entry destination 92.1.0.219
Destination IP  Source IP      Port DstPrt  SrcPrt  Stat-Pkts  Stat-Bytes
-----
MLS-RP 10.20.26.64:
92.1.0.219      10.1.0.219      ICMP -      -      511      52122
Console> (enable)
    
```

### Clearing IP MLS Statistics

The **clear mls statistics** command clears the following statistics on the switch:

- Total packets switched
- Total packets exported (for NDE)

To clear IP MLS statistics on the switch, perform this task in privileged mode:

Task	Command
Clear IP MLS statistics on the switch.	<b>clear mls statistics</b>

This example shows how to clear IP MLS statistics on the switch:

```

Console> (enable) clear mls statistics
Console> (enable)
    
```

## Displaying IP MLS Debug Information

The **show mls debug** command displays IP MLS debug information that you can send to your technical support representative for analysis if necessary.

To display IP MLS debug information on the switch, perform this task:

Task	Command
Display IP MLS debug information that you can send to your technical support representative.	<b>show mls debug</b>

## IP MLS Supported Network Topologies

IP MLS requires specific network topologies to function correctly. These sections describe the supported topologies:

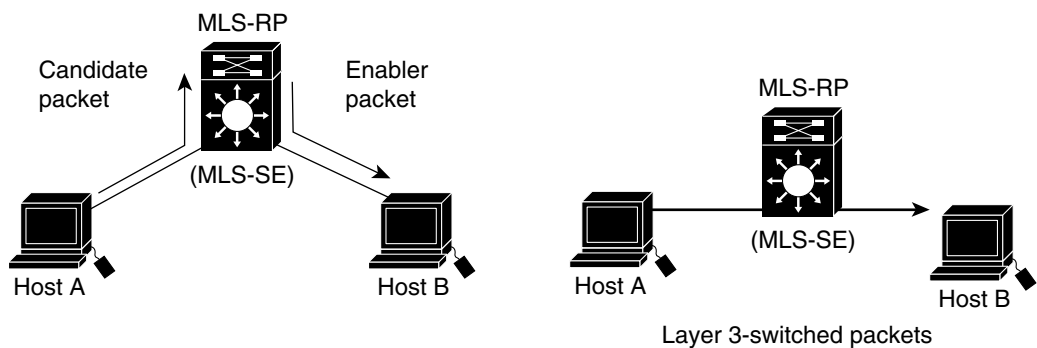
- Packets Traversing a Single Router between Two Hosts, page 5-29
- Destination Host Connected to a Switch Through a Router, page 5-30
- Source Host Connected to a Switch Through a Router, page 5-30
- Source and Destination Hosts Connected to a Switch Through Different Routers, page 5-31
- Source Host Connected to a Switch Through an FDDI Ring, page 5-32
- Source Host Connected to a Switch Through an ATM Cloud, page 5-33

**Note** The MLS-RPs in the illustrations represent either an RSM or an externally attached Cisco router.

## Packets Traversing a Single Router between Two Hosts

In Figure 5-2, the path from Host A to Host B is through a single router. After the MLS cache entry is created for this flow, packets from Host A to Host B are multilayer switched directly by the switch, bypassing the router.

**Figure 5-2** Packets Traversing a Single Router Between Two Hosts

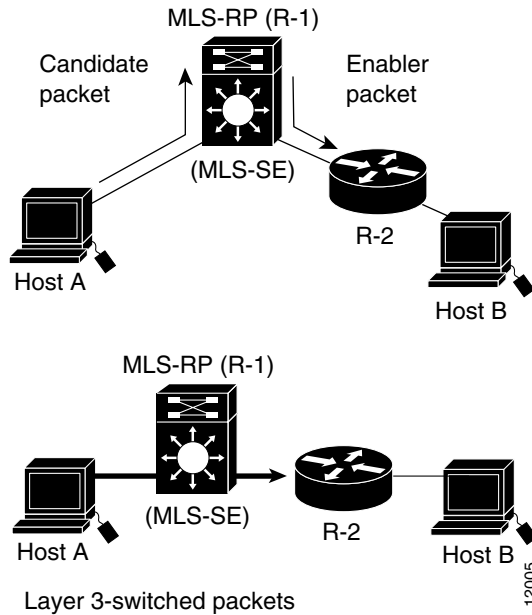


12004

## Destination Host Connected to a Switch Through a Router

In Figure 5-3, the path from Host A to Host B is through two routers. Router R-2 is located between the switch and the destination host (Host B). After the MLS cache entry is created for this flow, packets from Host A to Host B are multilayer switched directly by the switch. However, Router R-2 still routes the packets.

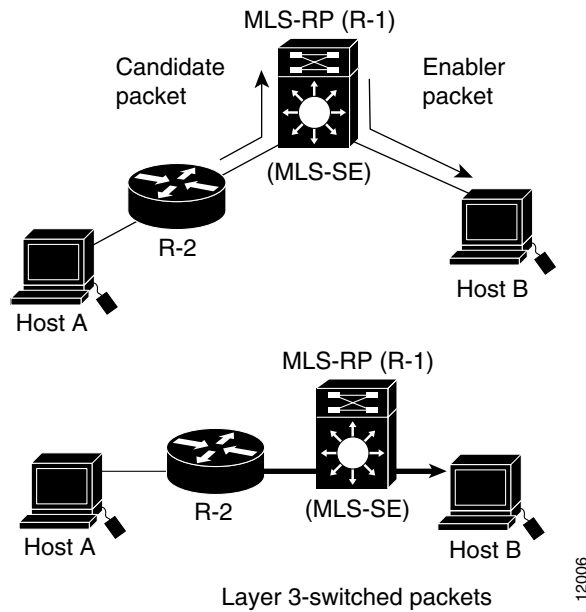
**Figure 5-3 Destination Host Connected to a Switch Through a Router**



## Source Host Connected to a Switch Through a Router

In Figure 5-4, the path from Host A to Host B is through two routers. Router R-2 is located between the source host (Host A) and the switch. After the MLS cache entry is created for this flow, packets from Host A to Host B are routed by Router R-2 and then multilayer switched directly by the switch to the destination host.

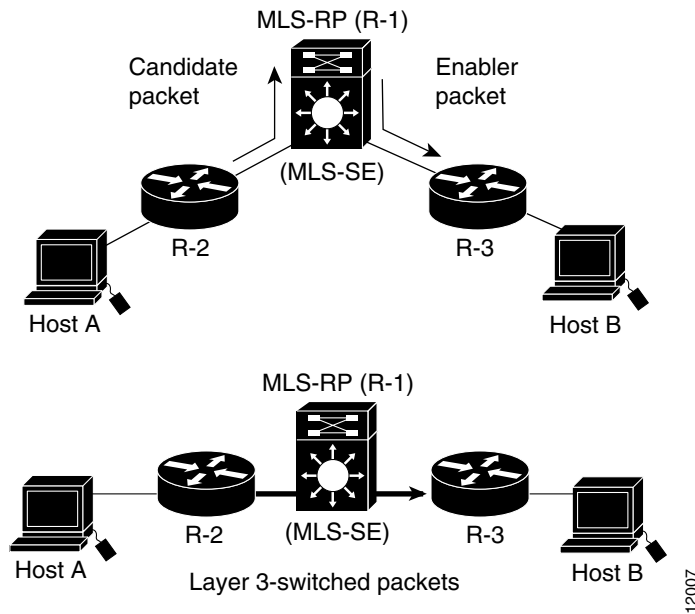
**Figure 5-4 Source Host Connected to a Switch Through a Router**



## Source and Destination Hosts Connected to a Switch Through Different Routers

In Figure 5-5, the path from Host A to Host B is through three routers. Router R-2 is located between the source host (Host A) and the switch. Router R-3 is located between the switch and the destination host (Host B). After the MLS cache entry is created for this flow, packets from Host A to Host B are routed by Router R-2, multilayer switched directly by the switch to Router R-3, and then routed by Router R-3 to the destination host.

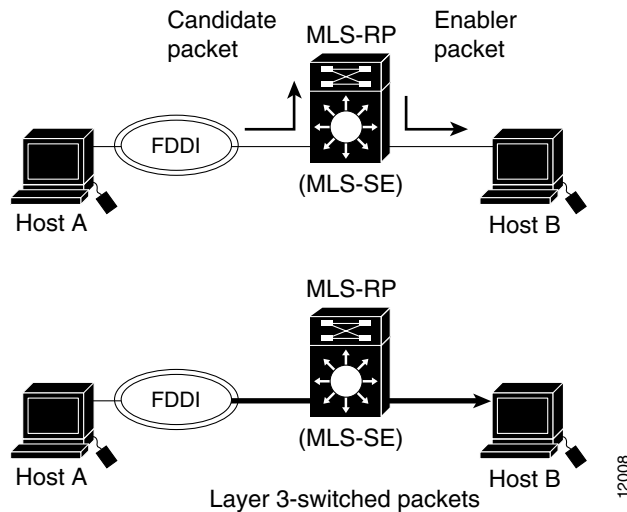
**Figure 5-5 Source and Destination Hosts Connected to a Switch Through Different Routers**



## Source Host Connected to a Switch Through an FDDI Ring

In Figure 5-6, the path from Host A to Host B is through an FDDI ring and one router. After the MLS cache entry is created for this flow, packets from Host A to Host B are received on an FDDI VLAN by the switch, translated to an Ethernet VLAN, and then multilayer switched directly by the switch to the destination host.

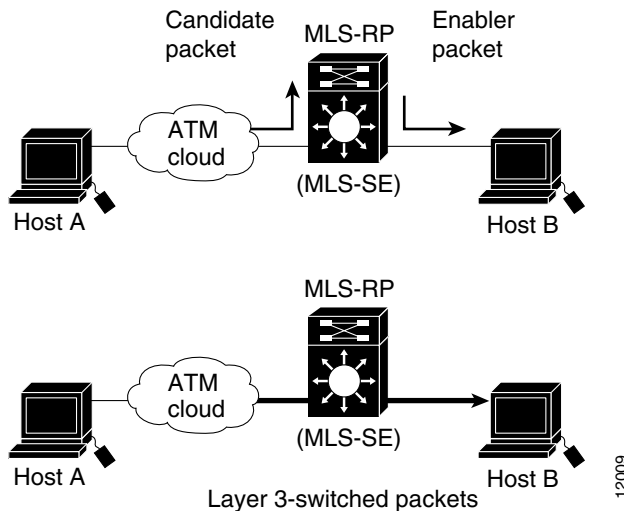
**Figure 5-6 Source Host Connected to Switch Through FDDI Ring**



## Source Host Connected to a Switch Through an ATM Cloud

In Figure 5-7, the path from Host A to Host B is through an ATM cloud and one router. After the MLS cache entry is created for this flow, packets from Host A to Host B are received as cells on the ATM LAN Emulation (LANE) module, translated to Ethernet frames, and then multilayer switched directly by the switch to the destination host.

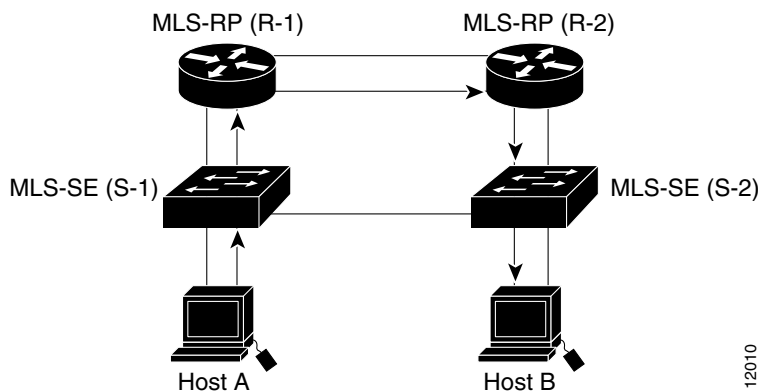
**Figure 5-7 Source Host Connected to Switch Through ATM Cloud**



## IP MLS Unsupported Network Topologies

IP MLS does not support some network topologies. In Figure 5-8, the routed path from Host A to Host B traverses Switch S-1, Routers R-1 and R-2, and Switch S-2. Layer 3 switching is not possible because the candidate packet creates an entry in the MLS cache on Switch S-1, but the enabler packet is forwarded to Router R-2 rather than to Switch S-1. The entry created in the MLS cache for the candidate packet times out because no enabler packet returns to the switch. In this topology, Routers R-1 and R-2 forward all packets between Hosts A and Host B.

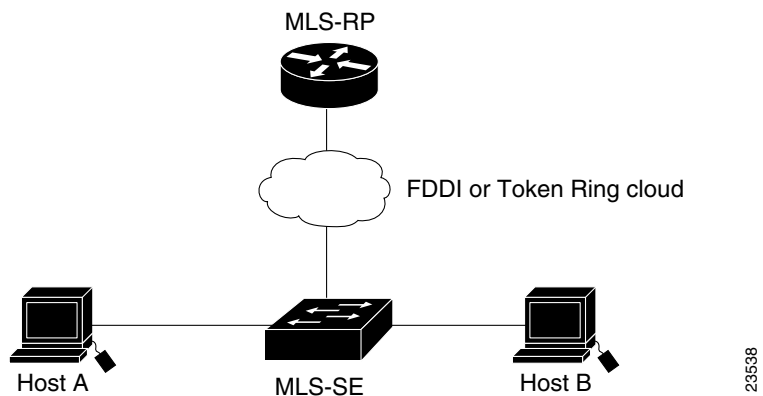
**Figure 5-8 Unsupported Topologies—Incomplete MLS Cache Entry**



In Figure 5-9, Layer 3 switching is not possible because MLSP is not supported over FDDI and Token Ring media.

In addition, MLSP is supported over ATM media only with Cisco IOS software release 12.0(3)W5(8) or later on the MLS-RP.

**Figure 5-9** Unsupported Topologies—MLSP Over FDDI or Token Ring



23538

## IP MLS Examples

These sections contain example IP MLS implementations:

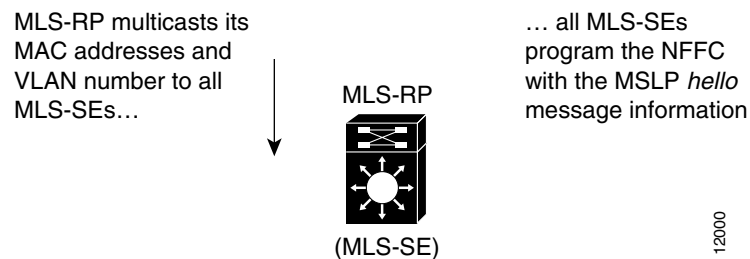
- Basic IP MLS Implementation, page 5-35
- IP MLS With Cisco 7505 Over IEEE 802.1Q, page 5-37

## Basic IP MLS Implementation

This section provides a step-by-step description of IP MLS implementation.

- Step 1** The MLSP informs the switch of the MLS-RP MAC addresses used on different VLANs and the MLS-RP's routing and access-list changes. Through this protocol, the MLS-RP multicasts its MAC and VLAN information to all MLS-SEs. When the MLS-SE hears the MLSP hello message indicating an IP MLS initialization, the MLS-SE is programmed with the MLS-RP MAC address and its associated VLAN number (see Figure 5-10).

**Figure 5-10 IP MLS Implementation: Step 1**



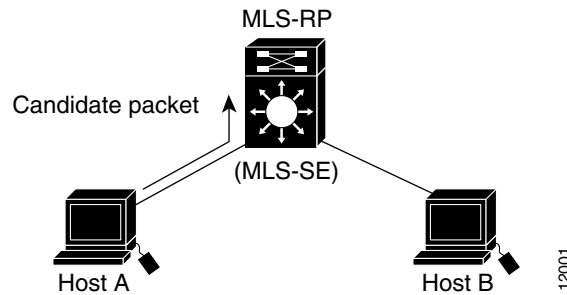
- Step 2** In Figure 5-11, Host A and Host B are located on different VLANs. Host A initiates a data transfer to Host B. When Host A sends the first packet to the MLS-RP, the MLS-SE recognizes this packet as a *candidate packet* for Layer 3 switching because the MLS-SE has learned the MLS-RP's destination MAC address and VLAN through MLSP. The MLS-SE learns the Layer 3 flow information (such as the destination address, source address, and protocol port numbers), and forwards the first packet to the MLS-RP. A partial MLS entry for this Layer 3 flow is created in the MLS cache.

The MLS-RP receives the packet, looks at its route table to determine how to forward the packet, and applies services such as access control lists and class of service (COS) policy.

The MLS-RP rewrites the MAC header adding a new destination MAC address (Host B's) and its own MAC address as the source.

**Figure 5-11 IP MLS Implementation: Step 2**

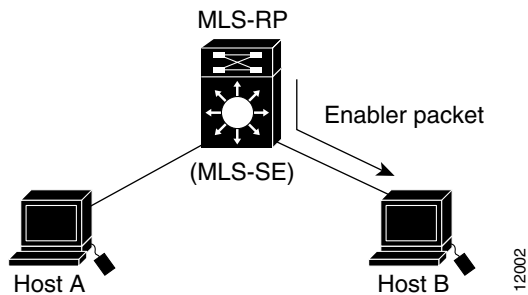
Because the Catalyst switch has learned the MAC and VLAN information of the MLS-RP, the switch starts the MLS process for the Layer 3 flow contained in this packet, the *candidate packet*



**Step 3** The MLS-RP routes the packet to the destination host. When the switch receives the packet, the MLS-SE recognizes that the source MAC address belongs to the MLS-RP, and that the flow information for the packet matches the flow for which the candidate entry was created. The MLS-SE considers this packet an *enabler packet* and completes the MLS entry in the MLS cache (see Figure 5-12).

**Figure 5-12 IP MLS Implementation: Step 3**

The MLS-RP routes this packet to Host B. Because the MLS-SE has learned both this MLS-RP and the Layer 3 flow in this packet, it completes the MLS entry in the MLS cache. The first routed packet is called the *enabler packet*



**Step 4** After the MLS entry has been completed, all Layer 3 packets in the same flow from the source host to the destination host are Layer 3 switched directly by the switch, bypassing the router (see Figure 5-13).

**Note** IP MLS is unidirectional. A separate Layer 3-switched path is created for traffic from Host B to Host A.

After the Layer 3-switched path is established, the MLS-SE rewrites the packet from the source host before it is forwarded to the destination host. The rewritten information includes the MAC addresses, encapsulations (when applicable), and some Layer 3 information.

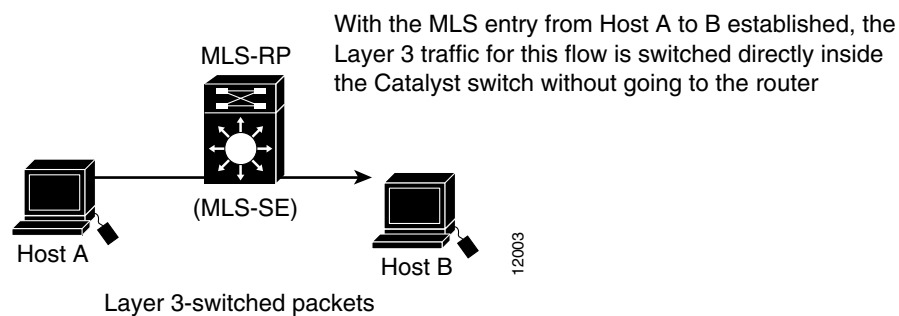
The resultant packet format and protocol behavior is identical to that of a packet routed by the RSM or external Cisco router.

---

**Note** For more information on the packet rewrite process, see the “Layer 3-Switched Packet Rewrite” section on page 5-5.

---

**Figure 5-13 IP MLS Implementation: Step 4**



## IP MLS With Cisco 7505 Over IEEE 802.1Q

This example consists of these sections:

- Example Network Topology, page 5-37
- Operation before IP MLS, page 5-38
- Operation after IP MLS, page 5-39
- Router Configuration, page 5-39
- Switch A Configuration, page 5-40
- Switch B Configuration, page 5-41
- Switch C Configuration, page 5-41

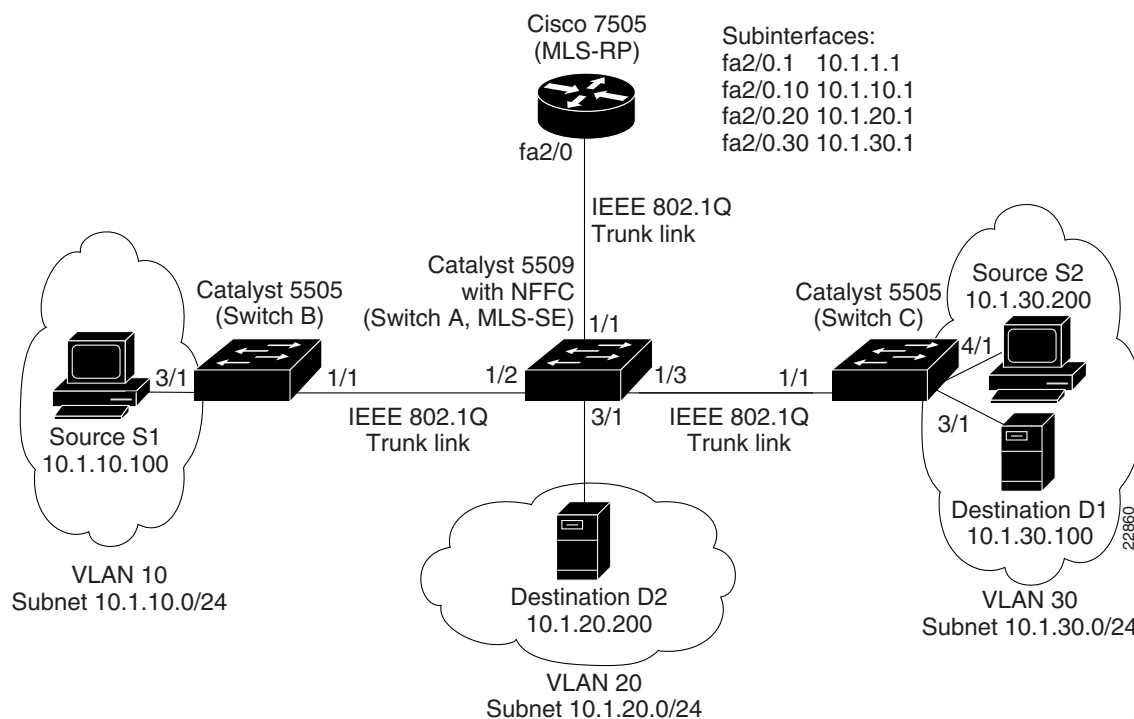
### Example Network Topology

Figure 5-14 shows an IP MLS example network topology using three Catalyst 5000 family switches and a Cisco 7505 router, all interconnected using IEEE 802.1Q trunk links. The network is configured as follows:

- There are four VLANs (IP subnetworks):
  - VLAN 1 (management VLAN), subnet 10.1.1.0/24
  - VLAN 10, subnet 10.1.10.0/24
  - VLAN 20, subnet 10.1.20.0/24
  - VLAN 30, subnet 10.1.30.0/24

- The MLS-RP is a Cisco 7505 router with a Fast Ethernet interface (interface fastethernet2/0)
- The subinterfaces on the router interface have these IP addresses:
  - fastethernet2/0.1–10.1.1.1 255.255.255.0
  - fastethernet2/0.10–10.1.10.1 255.255.255.0
  - fastethernet2/0.20–10.1.20.1 255.255.255.0
  - fastethernet2/0.30–10.1.30.1 255.255.255.0
- A standard output access list is configured on subinterface fastethernet2/0.20 (the interface in VLAN 20) on the MLS-RP
- Switch A, the MLS-SE, is a Catalyst 5509 switch with Supervisor Engine III and the NFFC
- Switch B and Switch C are Catalyst 5505 switches
- Switch A is the VTP server in domain “Corporate”
- Switch B and Switch C are VTP clients

**Figure 5-14 IP MLS With Cisco 7505 Over IEEE 802.1Q Example Network**



### Operation before IP MLS

Before IP MLS is implemented, when the source host S1 (on VLAN 10) transmits traffic destined for destination server D1 (on VLAN 30), Switch B forwards the traffic (based on the Layer 2 forwarding table) to Switch A over the 802.1Q trunk link. Switch A forwards the packet to the router over the 802.1Q trunk.

The router receives the packet on the VLAN 10 subinterface, checks the destination IP address, and routes the packet to the VLAN 30 subinterface. Switch A receives the routed packet and forwards it to Switch C. Switch C receives the packet and forwards it to destination server D1. This process is repeated for each packet in the flow between source host S1 and destination server D1.

When source host S2 sends traffic to destination server D2, Switch C forwards the packets over the 802.1Q trunk to Switch A. Switch A forwards the packet to the MLS-RP, which receives it on the VLAN 30 subinterface. Because the standard access list configured on the outgoing VLAN 20 subinterface denies all traffic from VLAN 30, the router drops the traffic to Destination D2 from Source S2. Any subsequent traffic from Source S2 for Destination D2 also reaches the router and is dropped.

## Operation after IP MLS

After IP MLS is implemented, when the source host S1 (on VLAN 10) transmits traffic destined for destination server D1 (on VLAN 30), Switch B forwards the traffic (based on the Layer 2 forwarding table) to Switch A (the MLS-SE) over the 802.1Q trunk link. When the first packet enters Switch A, a candidate flow entry is established in the MLS cache. Switch A forwards the packet to the MLS-RP over the 802.1Q trunk.

The MLS-RP receives the packet on the VLAN 10 subinterface, checks the destination IP address, and routes the packet to the VLAN 30 subinterface. Switch A receives the routed packet (the enabler packet) and completes the flow entry in the MLS cache for destination IP address 10.1.30.100. Switch A forwards the packet to Switch C, where it is forwarded to destination server D1.

Subsequent packets destined for IP address 10.1.30.100 are multilayer switched by the MLS-SE based on the flow entry in the MLS cache. For example, subsequent packets in the flow from source host S1 are forwarded by Switch B to Switch A (the MLS-SE). The MLS-SE determines that the packets are part of the established flow, rewrites the packet headers, and switches the packets directly to Switch C, bypassing the router.

When source host S2 sends traffic to destination server D2, Switch C forwards the packets over the 802.1Q trunk to Switch A. Switch A forwards the candidate packet to the MLS-RP, which receives it on the VLAN 30 subinterface. Because the standard access list configured on the outgoing VLAN 20 subinterface denies all, traffic from VLAN 30, the router drops the traffic to Destination D2 from Source S2.

Switch A never receives the enabler packet for the flow on VLAN 20 and no MLS cache entry is completed for the flow. Any subsequent traffic from Source S2 for Destination D2 also reaches the router and is dropped.

---

**Note** Because there is a standard access list configured on one of the IP MLS interfaces, the MLS-SE must use the source-destination-ip flow mask for all MLS cache entries.

---

## Router Configuration

This example shows how to configure the router (MLS-RP):

```
Cisco7505#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cisco7505(config)#mls rp ip
Cisco7505(config)#access-list 1 deny 10.1.30.0 0.0.0.255
Cisco7505(config)1#access-list 1 permit any
Cisco7505(config)#interface fastethernet 2/0
Cisco7505(config-if)#full-duplex
```

```

Cisco7505(config-if)#mls rp vtp-domain Corporate
Cisco7505(config-if)#interface fastethernet2/0.1
Cisco7505(config-subif)#encapsulation dot1q 1
Cisco7505(config-subif)#ip address 10.1.1.1 255.255.255.0
Cisco7505(config-subif)#mls rp ip
Cisco7505(config-subif)#mls rp management-interface
Cisco7505(config-subif)#interface fastethernet2/0.10
Cisco7505(config-subif)#encapsulation dot1q 10
Cisco7505(config-subif)#ip address 10.1.10.1 255.255.255.0
Cisco7505(config-subif)#mls rp ip
Cisco7505(config-subif)#interface fastethernet2/0.20
Cisco7505(config-subif)#encapsulation dot1q 20
Cisco7505(config-subif)#ip address 10.1.20.1 255.255.255.0
Cisco7505(config-subif)#ip access-group 1 out
Cisco7505(config-subif)#mls rp ip
Cisco7505(config-subif)#interface fastethernet2/0.30
Cisco7505(config-subif)#encapsulation dot1q 30
Cisco7505(config-subif)#ip address 10.1.30.1 255.255.255.0
Cisco7505(config-subif)#mls rp ip
Cisco7505(config-subif)#^Z
Cisco7505#

```

## Switch A Configuration

---

**Note** In some IOS software releases, traffic on the IEEE 802.1Q native VLAN is not routed. The default native VLAN on Catalyst switches is VLAN 1. If your IOS software release does not route traffic on the native VLAN and you want to route traffic on VLAN 1, change the native VLAN on the switch-to-router trunk link to an unused VLAN. In the Switch A, Switch B, and Switch C configuration examples, the native VLAN on all of the 802.1Q trunk links is set to an unused VLAN, VLAN 5.

---

This example shows how to configure Switch A (MLS-SE):

```

SwitchA> (enable) set vtp domain Corporate mode server
VTP domain Corporate modified
SwitchA> (enable) set vlan 5
Vlan 5 configuration successful
SwitchA> (enable) set vlan 10
Vlan 10 configuration successful
SwitchA> (enable) set vlan 20
Vlan 20 configuration successful
SwitchA> (enable) set vlan 30
Vlan 30 configuration successful
SwitchA> (enable) set port name 1/1 Router Link
Port 1/1 name set.
SwitchA> (enable) set trunk 1/1 on dot1q
Port(s) 1/1 trunk mode set to on.
Port(s) 1/1 trunk type set to dot1q.
SwitchA> (enable) set port name 1/2 SwitchB Link
Port 1/2 name set.
SwitchA> (enable) set trunk 1/2 desirable dot1q
Port(s) 1/2 trunk mode set to desirable.
Port(s) 1/2 trunk type set to dot1q.
SwitchA> (enable) set port name 1/3 SwitchC Link
Port 1/3 name set.
SwitchA> (enable) set trunk 1/3 desirable dot1q
Port(s) 1/3 trunk mode set to desirable.
Port(s) 1/3 trunk type set to dot1q.

```

```

SwitchA> (enable) set vlan 5 1/1-3
VLAN 5 modified.
VLAN 1 modified.
VLAN Mod/Ports
-----
5      1/1-3

SwitchA> (enable) set mls enable
IP Multilayer switching is enabled.
SwitchA> (enable) set mls include 10.1.1.1
IP Multilayer switching enabled for router 10.1.1.1.
SwitchA> (enable) set port name 3/1 Destination D2
Port 3/1 name set.
SwitchA> (enable) set vlan 20 3/1
VLAN 20 modified.
VLAN 1 modified.
VLAN Mod/Ports
-----
20     3/1

SwitchA> (enable)

```

## Switch B Configuration

This example shows how to configure Switch B:

```

SwitchB> (enable) set port name 1/1 SwitchA Link
Port 1/1 name set.
SwitchB> (enable) set vlan 5 1/1
VLAN 5 modified.
VLAN 1 modified.
VLAN Mod/Ports
-----
5      1/1

SwitchB> (enable) set port name 3/1 Source S1
Port 3/1 name set.
SwitchB> (enable) set vlan 10 3/1
VLAN 10 modified.
VLAN 1 modified.
VLAN Mod/Ports
-----
10     3/1

SwitchB> (enable)

```

## Switch C Configuration

This example shows how to configure Switch C:

```

SwitchC> (enable) set port name 1/1 SwitchA Link
Port 1/1 name set.
SwitchC> (enable) set vlan 5 1/1
VLAN 5 modified.
VLAN 1 modified.
VLAN Mod/Ports
-----
5      1/1

SwitchC> (enable) set port name 3/1 Destination D1
Port 3/1 name set.

```

```
SwitchC> (enable) set vlan 30 3/1
VLAN 30 modified.
VLAN 1 modified.
VLAN Mod/Ports
-----
30    3/1

SwitchC> (enable) set port name 4/1 Source S2
Port 4/1 name set.
SwitchC> (enable) set vlan 30 4/1
VLAN 30 modified.
VLAN 1 modified.
VLAN Mod/Ports
-----
30    3/1
      4/1

SwitchC> (enable)
```