

# Configuring Multilayer Switching

---

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

---

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

---

This chapter consists of these sections:

- Understanding How MLS Works on page 42-1
- Software and Hardware Requirements on page 42-8
- Default MLS Configuration on page 42-9
- Configuration Guidelines and Restrictions on page 42-9
- Configuring MLS on the Router on page 42-12
- Configuring MLS on the Switch on page 42-19
- MLS Implementation Examples on page 42-30
- MLS Configuration Examples on page 42-37

## Understanding How MLS Works

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

- MLS Overview on page 42-2
- MLS Components on page 42-2
- MLS Flows on page 42-2
- MLS Cache on page 42-3
- Layer 3-Switched Packet Rewrite on page 42-3
- MLS Operation on page 42-4

- Standard and Extended Access Lists on page 42-5
- Flow Masks on page 42-6
- Packet Export Rate on page 42-8

## MLS Overview

MLS provides high-performance hardware-based Layer 3 switching for Catalyst 5000 and 2926G series LAN switches. MLS switches unicast IP data packet flows between subnets using advanced application-specific integrated circuit (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 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.

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

---

**Note** For more information about NDE, see Chapter 43, “Configuring NetFlow Data Export.”

---

In addition, 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 MLS, see the “Using Debug Commands on the MLS Router” section on page 42-19.

## MLS Components

An MLS network topology consists of these components:

- Multilayer Switching-Switching Engine (MLS-SE)—Catalyst 2926G series switch, or Catalyst 5000 series switch with the NFFC or NFFC II. The MLS-SE provides Layer 3 LAN-switching services.
- Multilayer Switching-Route Processor (MLS-RP)—A Catalyst 5000 series Route Switch Module (RSM) or an externally connected Cisco 7500, 7200, 4500, or 4700 series router with software that supports MLS. The MLS-RP provides Cisco IOS-based multiprotocol routing, network services, and central configuration and control for the switches.
- Multilayer Switching Protocol (MLSP)—The protocol running between the MLS-SE and MLS-RP to enable MLS.

## 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.

The NFFC (or NFFC II) maintains a Layer 3 switching table (MLS cache) for the 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. When the Layer 3-switching entry for a flow ages out, the flow statistics can be exported to a flow collector application.

## MLS Cache

The MLS-SE maintains a cache for MLS flows and maintains statistics for each flow. 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 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 MLS router interfaces (which determines the flow mask). See the “Flow Masks” section on page 42-6 for additional information.

---

## 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.

---

**Note** The Catalyst 5000 series 24-port 10/100BaseTX and 12-port 100BaseFX Backbone Fast Ethernet switching modules (WS-X5225R and WS-X5201R) have onboard hardware that performs the packet rewrite, optimizing MLS performance. This optimization is also used on the Catalyst 2926G series switch ports.

---

---

**Note** There are slot restrictions when using MLS with the Gigabit Ethernet (WS-X5403) switching module. You must install the switching module in specific slots in the Catalyst 5000 series switches to maximize MLS operation. Refer to the *Catalyst 5000 Series Module Installation Guide* for details.

---

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
MLS-RP MAC	Host A MAC	Host B IP	Host A IP				

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 saved 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 <sup>1</sup>	Checksum <sup>2</sup>	Data	Checksum
Host B MAC	MLS-RP MAC	Host B IP	Host A IP				

- 1 The IP header TTL value is decremented by 1.
- 2 The IP header checksum is recalculated.

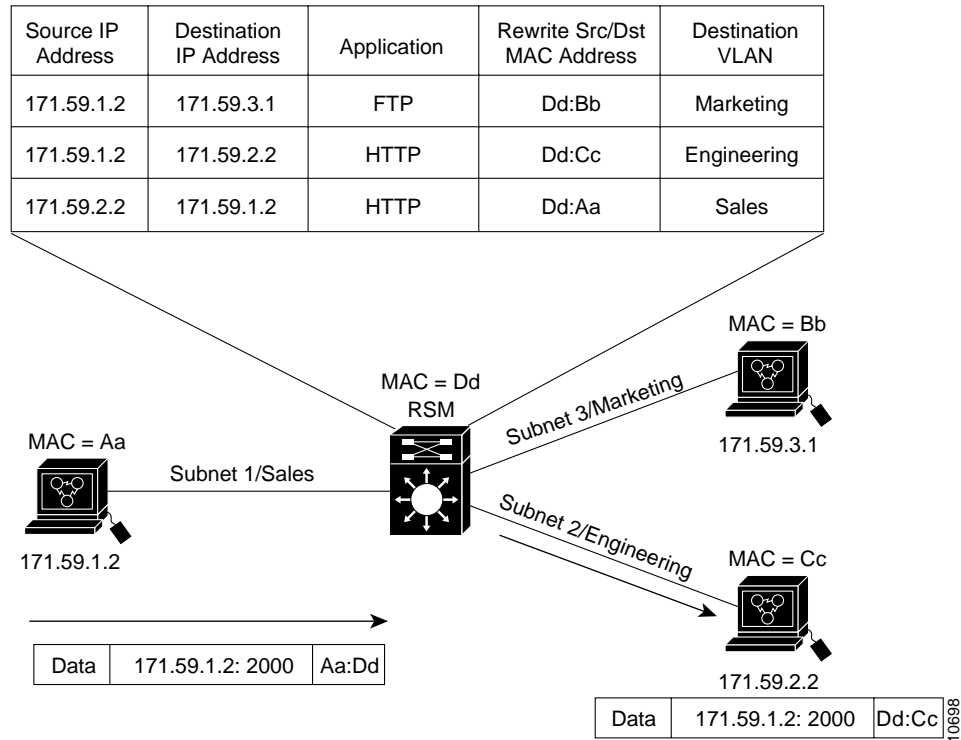
## MLS Operation

Figure 42-1 shows a simple 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 42-1). 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 42-1 MLS Example Topology



## Standard and Extended Access Lists

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

MLS allows you to enforce access lists on every packet of the flow without compromising MLS performance. When you enable 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 MLS switching path automatically on the MLS-SE. The techniques for handling route and access list changes apply to both the RSM and 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.

## Flow Masks

The MLS-SE uses flow mask modes to determine how MLS entries are created. The flow mask mode is based on the access lists configured on the MLS router interfaces. The MLS-SE learns the flow mask through MLSP messages from each MLS-RP for which the MLS-SE is performing Layer 3 switching.

These sections describe how the flow mask modes work:

- Flow Mask Modes on page 42-6
- Flow Mask Mode and show mls entry Command Output on page 42-6

### Flow Mask Modes

An MLS-SE supports only one flow mask (the most specific one) for all MLS-RPs that are Layer 3 switched. 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 mode. Depending on the current mode, some fields in the flow record might not have values. Unsupported fields are filled with a zero (0).

The three flow mask modes are as follows:

- destination-ip mode—The least-specific flow mask mode. 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 router interfaces.
- source-destination-ip mode—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 interfaces.
- ip-flow mode—The most-specific flow mask mode. 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 interfaces.

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

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

In destination-ip mode, 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)

```

In source-destination-ip mode, 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
          Last   Used
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
10.19.28.11    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)

```

In ip-flow mode, because a separate MLS entry is created for every ip-flow, details are shown 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)
```

## 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

MLS requires these software and hardware versions:

- Supervisor engine software—Software release 4.1(1) or later
- Cisco IOS router software—IOS release 11.3(2)WA4(4) or later
- Catalyst 2926G series switch or a Catalyst 5000 series switch with Supervisor Engine III, III FSX, or III FLX module with a NetFlow Feature Card (NFFC) or NFFC II
- Route Switch Module (RSM) or Cisco 7500, 7200, 4500, or 4700 series router
- (Optional) Catalyst 5000 series 24-port 10/100BaseTX and 12-port 100BaseFX Backbone Fast Ethernet switching modules (WS-X5225R and WS-X5201R)—These switching modules have onboard hardware that optimizes MLS performance (this optimization is also used in the Catalyst 2926G series switches)

## Default MLS Configuration

Table 42-1 shows the default MLS configuration.

**Table 42-1 Default MLS Configuration**

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

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

## Configuration Guidelines and Restrictions

These sections describe configuration guidelines that apply when configuring MLS:

- General Configuration Guidelines on page 42-9
- External Routers on page 42-10
- Access Lists on page 42-10
- MLS Interaction with Other Features on page 42-11
- Maximum Transmission Unit Size on page 42-11
- Restrictions on Using IP Router Commands with MLS Enabled on page 42-12

## General Configuration Guidelines

Follow these general guidelines when configuring MLS:

- When you enable MLS, the RSM or externally attached router continues to handle all non-IP protocols while offloading the switching of IP packets to the MLS-SE.
- Do not confuse MLS with the NetFlow switching supported by Cisco routers. MLS uses both the RSM or directly attached external router and the MLS-SE. With 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, 4500, and 4700 series) for MLS when they are externally attached to the switch. You can make the attachment with multiple Ethernet connections (one per subnet) or by using Fast or Gigabit Ethernet with Inter-Switch Link (ISL) encapsulation.
- You can connect end hosts through any media (Ethernet, Fast Ethernet, ATM, and Fiber Distributed Data Interface [FDDI]) but the connection between the external router and the switch must be through standard 10/100 Ethernet interfaces or ISL links.

## Access Lists

Access lists affect MLS as follows:

- Input access lists—Router interfaces with input access lists cannot participate in MLS. If you configure an input access list on an interface, 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 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 MLS.

- Access list impact on flow masks—Access lists impact the flow mask mode advertised to the MLS-SE by an MLS-RP. When there is no access list on any MLS-RP interface, the flow mask mode is destination-ip (the least specific) by default. When there is a standard access list on any of the MLS-RP interfaces, the mode is source-destination-ip by default. When there is an extended access list on any of the MLS-RP interfaces, the mode is ip-flow (the most specific) by default. You can specify the minimum flow mask using the **set mls flow** command.
- Reflexive access lists—Router interfaces with reflexive access lists cannot participate in Layer 3 switching.

## MLS Interaction with Other Features

Other Cisco IOS software features affect MLS as follows:

- IP accounting—Enabling IP accounting on an 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 43, “Configuring NetFlow Data Export.”

---

- Data encryption—MLS is disabled on an interface when the data encryption feature is configured on the interface.
- Policy route-map—MLS is disabled on an interface when a policy route-map is configured on the interface.
- TCP intercept—With MLS interfaces enabled, the Transmission Control Protocol (TCP) intercept feature (enabled in global configuration mode) might not work properly. When you enable the TCP intercept feature, the following message displays:  

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

## Maximum Transmission Unit Size

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

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

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

If you attempt to enable 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 MLS Enabled

When you enable some IP processes on an interface, you will disable MLS on the interface. Table 42-2 shows the affected commands.

**Table 42-2 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 MLS on this MLS-RP.
<b>ip security</b> (all forms of this command)	Disables MLS on the interface.
<b>ip tcp compression-connections</b>	Disables MLS on the interface.
<b>ip tcp header-compression</b>	Disables MLS on the interface.

## Configuring MLS on the Router

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

- Enabling MLSP on the Router on page 42-13
- Adding an MLS Interface to a VTP Domain on page 42-13
- Assigning a VLAN ID to a Router Interface on page 42-14
- Enabling MLS on a Router Interface on page 42-14
- Specifying a Router Interface as a Management Interface on page 42-14
- Removing a Router Interface as a Management Interface on page 42-15
- Disabling MLS on a Router Interface on page 42-15
- Clearing a VLAN ID from a Router Interface on page 42-15
- Removing an MLS Interface from a VTP Domain on page 42-16
- Removing an MLS Interface from the Null Domain on page 42-16
- Disabling MLSP on the Router on page 42-17
- Monitoring MLS on the Router on page 42-17
- Using Debug Commands on the MLS Router on page 42-19

---

**Note** The interface-specific commands in these sections apply only to Ethernet, Fast Ethernet, and VLAN interfaces on the Catalyst RSM/VIP2 or directly-attached external router.

---



---

**Note** For information on configuring VLAN interfaces on the RSM, see Chapter 39, “Configuring InterVLAN Routing.”

---

After you perform the steps in this section to configure the router, see the “Configuring MLS on the Switch” section on page 42-19.

## Enabling MLSP on the Router

To use MLS in your network, you must globally enable MLSP, the protocol that runs between the MLS-SE and the MLS-RP.

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

Task	Command
Globally enable MLSP on the router.	Router(config)# <b>mls rp ip</b>

This example shows how to enable MLSP on the router:

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

## Adding an MLS Interface to a VTP Domain

---

**Note** Perform this configuration task only if the switch is in a VTP domain.

---

Determine which router interfaces you will use as MLS interfaces and add those interfaces to the same VTP domain as the switches. A switch can be in only one VTP domain and you must add the MLS interfaces to the same domain.

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



**Caution** Perform this task before you enter any other MLS interface commands on the MLS interface (specifically, the **mls rp ip** or **mls rp management-interface** commands). Entering 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 MLS interface into a domain other than the null domain, you must clear the MLS interface configuration before you can add it to another VTP domain (for more information, see the “Removing an MLS Interface from the Null Domain” section on page 42-16).

On ISL interfaces, enter the **mls rp vtp-domain** command on the primary interface. All subinterfaces on the primary interface inherit the VTP domain assigned to the primary interface.

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

Task	Command
Add an MLS interface to a VTP domain.	Router(config-if)# <b>mls rp vtp-domain</b> [ <i>domain_name</i> ]

This example shows how to add an 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) or ISL-encapsulated interfaces.

---

The MLS interface must have a VLAN ID configured before you can enable it for MLS. Removing the VLAN ID from an interface disables MLS for the interface.

The assigned interface must be either an Ethernet or Fast Ethernet interface with no subinterfaces.

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

Task	Command
Assign a VLAN ID to an MLS interface.	Router(config-if)# <b>mls rp vlan-id</b> [vlan_id_num]

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

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

## Enabling MLS on a Router Interface

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

Task	Command
Specify a router interface for MLS.	Router(config-if)# <b>mls rp ip</b>

This example shows how to enable 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, MLSP packets will not be sent or received.

Every switch participating in 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 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.	Router(config-if)# <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.	Router(config-if)#no mls rp management-interface

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 MLS on a Router Interface

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

Task	Command
Remove a router interface from MLS.	Router(config-if)#no mls rp ip

This example shows how to disable 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) or ISL-encapsulated interfaces.

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

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

Task	Command
Remove a VLAN ID from an MLS interface.	Router(config-if)#no mls rp vlan-id [vlan_id_num]

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

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

## Removing an MLS Interface from a VTP Domain

To remove an interface from one VTP domain and add it to another, perform this task in interface configuration mode:

Task	Command
<b>Step 1</b> Remove an interface from a VTP domain if you have not already entered the <b>mls rp ip</b> or <b>mls rp management-interface</b> commands on the interface.	Router(config-if)# <b>no mls rp vtp-domain</b> [domain_name]
<b>Step 2</b> Add the interface to a new VTP domain.	Router(config-if)# <b>mls rp vtp-domain</b> [domain_name]

This example shows how to remove an interface from a VTP domain and add it to another VTP domain if you have not already entered the **mls rp ip** or **mls rp management-interface** commands on the interface:

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

## Removing an MLS Interface from the Null Domain

If you entered either the **mls rp ip** command or the **mls rp management-interface** command on the interface before you assigned the interface to a VTP domain, the interface will be in the null domain.

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

Task	Command
<b>Step 1</b> Remove an interface from the null domain.	Router(config-if)# <b>no mls rp ip</b> Router(config-if)# <b>no mls rp management-interface</b> Router(config-if)# <b>no mls rp vtp-domain</b> [domain_name]
<b>Step 2</b> Add the interface to a new VTP domain.	Router(config-if)# <b>mls rp vtp-domain</b> [domain_name]

This example shows how to remove an interface from 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 MLSP on the Router

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

Task	Command
Globally disable MLSP on the router.	Router(config)# <b>no mls rp ip</b>

This example shows how to disable MLSP on the router:

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

## Monitoring MLS on the Router

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

- 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 MLS

To display detailed MLS information on the router, perform one of these tasks:

Task	Command
Show MLS details for all interfaces.	<b>show mls rp</b> <i>[interface]</i>
Show 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 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:
```

## Configuring MLS on the Router

---

```
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 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 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 MLS Router

Table 42-3 describes MLS-related debug commands that you can use to troubleshoot MLS problems on the router.

---

**Note** To turn off any of the debug commands listed in Table 42-3, use the **no** form of the command.

---

**Table 42-3**      **MLS Debug Commands**

Command	Description
<b>debug mls rp events</b>	Displays a run-time sequence of events for the MLSP.
<b>debug mls rp packets</b>	Displays packet contents (in verbose and hexadecimal formats) for MLSP messages.
<b>debug mls rp error</b>	Displays error messages related to MLS.
<b>debug mls rp ip</b>	Turns on IP-related events for MLS, including route purging and changes of access lists and flow masks.
<b>debug mls rp locator</b>	Identifies which switch is switching a particular flow by using MLS explorer packets.
<b>debug mls rp all</b>	Turns on all MLS debugging events.

## Configuring MLS on the Switch

MLS is enabled by default on Catalyst 5000 and 2926G series switches. If the MLS-RP is an RSM installed in the Catalyst 5000 series 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 MLS aging time
- You want to enable NDE

These sections describe how to configure MLS on the switch:

- Enabling MLS on the Switch on page 42-20
- Specifying Routers to Participate in MLS on page 42-20
- Specifying MLS Aging-Time Value on page 42-21
- Specifying MLS Fast Aging Time and Packet Threshold Values on page 42-22
- Setting the Minimum MLS Flow Mask on page 42-22
- Removing Routers from Participation in MLS on page 42-23
- Disabling MLS on the Switch on page 42-23
- Displaying CAM Entries on the Switch on page 42-24
- Displaying MLS Information on page 42-24
- Displaying MLS Cache Entries on page 42-25
- Clearing MLS Cache Entries on page 42-28

- Displaying MLS Statistics on page 42-28
- Clearing MLS Statistics on page 42-30
- Displaying MLS Debug Information on page 42-30

---

**Note** For information on configuring VLANs on the switch, refer to Chapter 10, “Configuring VLANs.”

---

## Enabling MLS on the Switch

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

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

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

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

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

## Specifying Routers to Participate in MLS

If the MLS-RP is an external router, you must specify the IP address of the MLS-RP to participate in 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 MLS automatically and is included in the inclusion list (provided the RSM is running the correct Cisco IOS software version). If you physically remove the RSM or disable MLS on the RSM, the RSM is removed from the inclusion list.

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

---

**Note** Before specifying a router to participate in 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 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 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 MLS.

---

This example shows how to identify the MLS-RP IP address on the router, how to specify the MLS-RP to participate in 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 MLS Aging-Time Value

The 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 (less than 1 percent) are sent to the router. To help keep the size of the MLS cache down, enable MLS fast aging, as described in the “Specifying MLS Fast Aging Time and Packet Threshold Values” section on page 42-22.

---

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

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

This example shows how to set the MLS aging time:

```

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

```

## Specifying MLS Fast Aging Time and Packet Threshold Values

To help keep the MLS cache size below 32K, enable MLS fast aging time. The 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 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 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 MLS fast aging time and packet threshold, perform this task in privileged mode:

Task	Command
Specify the 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 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 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 42-6.

For example, if you do not configure access lists on any MLS-RP, then the 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 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** This command purges all existing shortcuts in the MLS cache and affects the number of active shortcuts on the MLS-SE. Exercise care when using this command.

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

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

This example shows how to set the minimum 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 MLS

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

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

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

This example shows how to remove a router from the 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 MLS on the Switch

When you disable 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 MLS, you lose the statistics for existing cache entries—they are not exported.

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

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

This example shows how to disable 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 51.0.0.3
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 MLS Information

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

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

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

This example shows how to display 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 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 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 42-6.

---

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

- Displaying All MLS Entries on page 42-26
- Displaying MLS Entries for a Specific Destination Address on page 42-26
- Displaying Entries for a Specific Source Address on page 42-26
- Displaying Entries for a Specific IP Flow on page 42-27
- Displaying Entries for a Specific MLS-RP on page 42-27

### 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)
    
```

### Displaying MLS Entries for a Specific Destination Address

To display MLS entries for a specific destination IP address, perform this task in privileged mode:

Task	Command
Show MLS entries for the specified destination IP address.	<b>show mls entry destination [ip_addr]</b>

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

```

Console> (enable) show mls entry destination 172.20.22.14/24
Destination IP      Source IP      Port DstPrt  SrcPrt Destination Mac      Vlan
Port
-----
----
MLS-RP 172.20.25.1:
172.20.22.14       172.20.25.10  TCP  6001    Telnet  00-60-70-6c-fc-22    4    2/1
MLS-RP 172.20.27.1:
172.20.22.16       172.20.27.139 TCP  6008    Telnet  00-60-70-6c-fc-24    4    2/3
      ..
      ..
Console> (enable)
    
```

### Displaying Entries for a Specific Source Address

To display MLS entries for a specific source IP address, perform this task in privileged mode:

Task	Command
Show MLS entries for the specified source IP address.	<b>show mls entry source [ip_addr]</b>

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

```

Console> (enable) show mls entry source 10.0.2.15
Destination IP  Source IP      Port DstPrt SrcPrt Destination Mac  Vlan Port
-----
MLS-RP 51.0.0.3:
51.0.0.2      10.0.2.15    TCP  Telnet  37819  00-e0-4f-15-49-ff 51  1/9
51.0.0.2      10.0.2.15    ICMP                00-e0-4f-15-49-ff 51  1/9
Console> (enable)

```

### Displaying Entries for a Specific IP Flow

The **show mls entry flow** command displays MLS entries for a specific IP flow. The *protocol* argument can be **tcp**, **udp**, **icmp**, or a decimal number for other protocol families. The *src\_port* and *dst\_port* arguments specify the protocol ports if the protocol is TCP or User Datagram Protocol (UDP). A value of zero (0) for *src\_port* and *dst\_port* or *protocol* is treated as a wildcard and all entries are displayed (unspecified options are treated as wildcards). If the protocol selected is not TCP or UDP, set the *src\_port* and *dst\_port* to 0 or no flows will be displayed.

To display MLS entries for a specific IP flow (when the switch flow mask mode is ip-flow), perform this task in privileged mode:

Task	Command
Show entries for a specific IP flow (when the switch flow mask mode is ip-flow).	<b>show mls entry flow</b> [ <i>protocol src_port dst_port</i> ]

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</b> <i>ip_addr</i>

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</b> [ <i>ip_addr_spec</i> ] <b>source</b> [ <i>ip_addr_spec</i> ] <b>flow</b> [ <i>protocol src_port dst_port</i> ] [ <b>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 520, and TCP destination port 320:

```
Console> (enable) clear mls entry destination 172.20.26.22 source 172.20.22.113 flow
tcp 520 320
Console> (enable)
```

## Displaying MLS Statistics

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

- Displaying MLS Statistics by Protocol on page 42-28
- Displaying Statistics for MLS-RPs on page 42-29
- Displaying Statistics for MLS Cache Entries on page 42-29

### Displaying MLS Statistics by Protocol

The **show mls statistics protocol** command displays 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 MLS statistics by protocol, perform this task in privileged mode:

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

This example shows how to display 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 MLS statistics for MLS-RPs. If you do not specify a particular MLS-RP, statistics for all MLS-RPs are displayed.

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

Task	Command
Show 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> ] [ <b>noalias</b> ]

This example shows how to display 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 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</b> <i>protocol 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 MLS Statistics

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

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

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

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

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

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

## Displaying MLS Debug Information

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

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

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

## MLS Implementation Examples

These sections provide examples that show the interaction between switches and routers necessary to perform MLS. All examples assume Host A and Host B are on different VLANs.

- Basic MLS Implementation on page 42-31
- Packets Traversing a Single Router between Two Hosts on page 42-33
- Destination Host Connected to a Switch Through a Router on page 42-34
- Source Host Connected to a Switch Through a Router on page 42-34
- Source and Destination Hosts Connected to a Switch Through Different Routers on page 42-35
- Source Host Connected to a Switch Through an FDDI Ring on page 42-36
- Source Host Connected to a Switch Through an ATM Cloud on page 42-36
- Unsupported Topologies on page 42-37

---

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

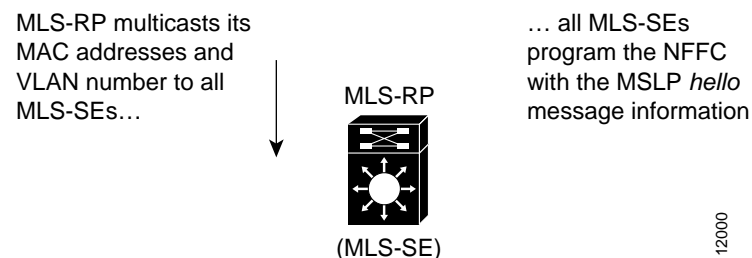
---

## Basic MLS Implementation

This section provides a step-by-step description of 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 MLS initialization, the MLS-SE is programmed with the MLS-RP MAC address and its associated VLAN number (see Figure 42-2).

**Figure 42-2** MLS Implementation: Step 1



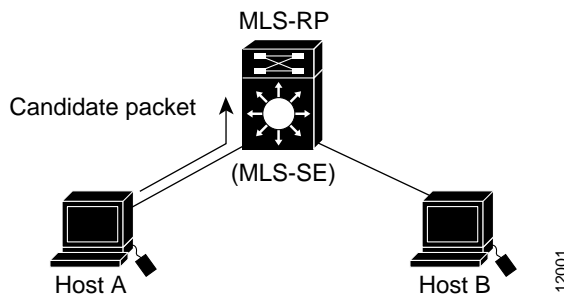
**Step 2** In Figure 42-3, Host A and Host B are located on different VLANs. Host A initiates a data transfer to Host B. When Host A sends the first packet to the MLS-RP, the MLS-SE recognizes this packet as a *candidate packet* for Layer 3 switching because the MLS-SE has learned the MLS-RP's destination 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 42-3 MLS Implementation: Step 2**

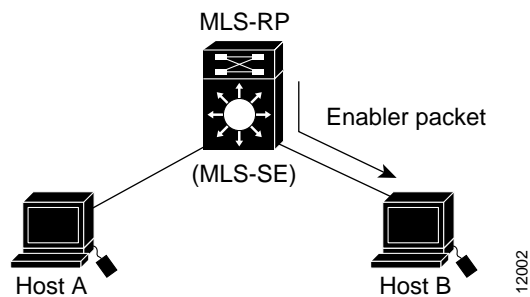
Because the Catalyst switch has learned the MAC and VLAN information of the MLS-RP, the switch starts the MLS process for the Layer 3 flow contained in this packet, the *candidate packet*



**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 42-4).

**Figure 42-4 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 42-5).

**Note** 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.

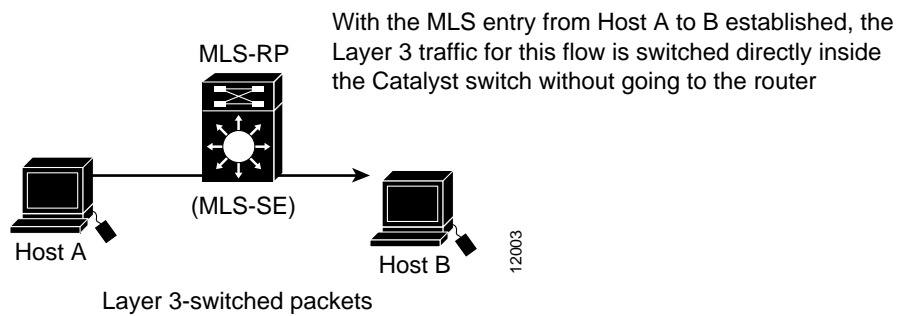
The resultant packet format and protocol behavior is identical to that of a packet routed by the RSM or external Cisco router.

---

**Note** For more information on the packet rewrite process, see the “Layer 3-Switched Packet Rewrite” section on page 42-3.

---

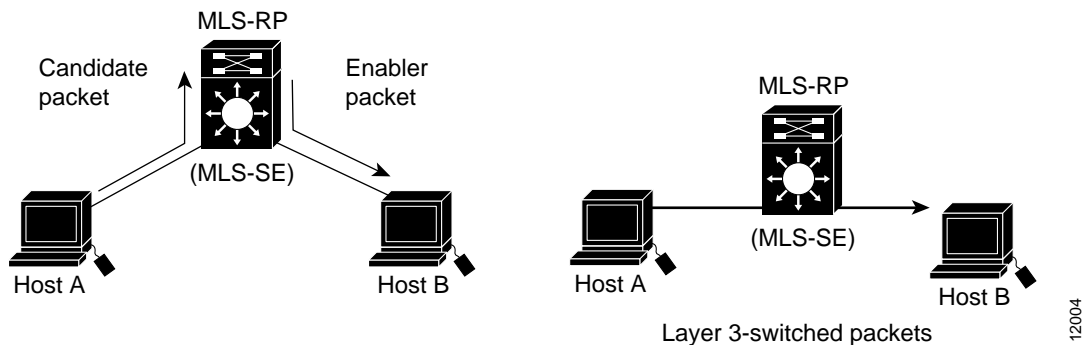
**Figure 42-5 MLS Implementation: Step 4**



## Packets Traversing a Single Router between Two Hosts

In Figure 42-6, 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 Layer 3 switched directly by the switch, bypassing the router.

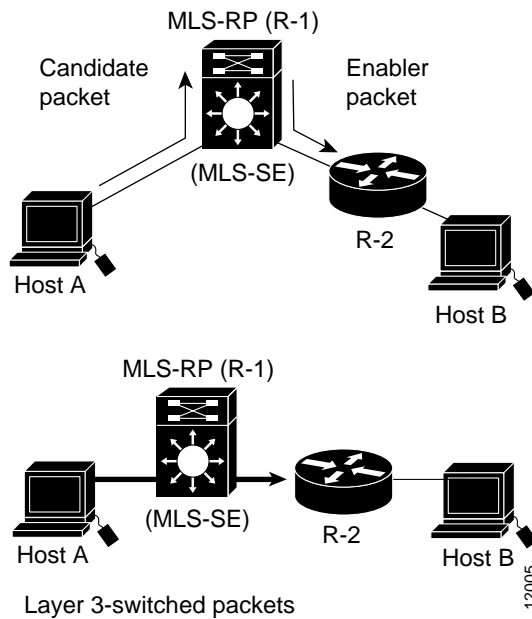
**Figure 42-6 Packets Traversing a Single Router Between Two Hosts**



## Destination Host Connected to a Switch Through a Router

In Figure 42-7, 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 Layer 3 switched directly by the switch. However, Router R-2 still routes the packets.

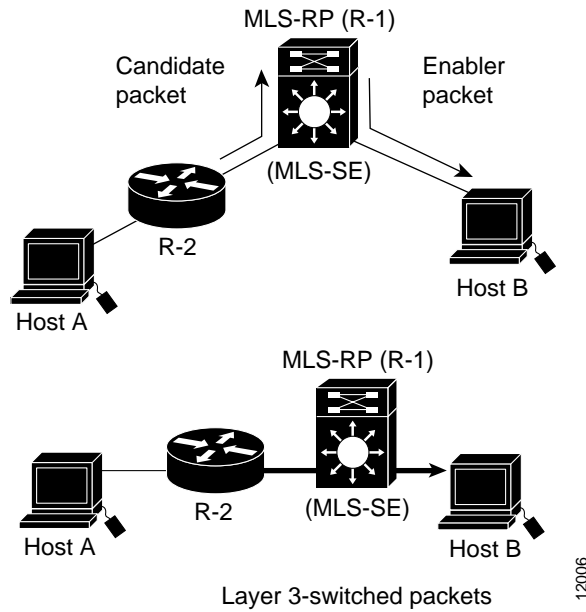
**Figure 42-7 Destination Host Connected to a Switch Through a Router**



## Source Host Connected to a Switch Through a Router

In Figure 42-8, 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 Layer 3 switched directly by the switch to the destination host.

**Figure 42-8 Source Host Connected to a Switch Through a Router**

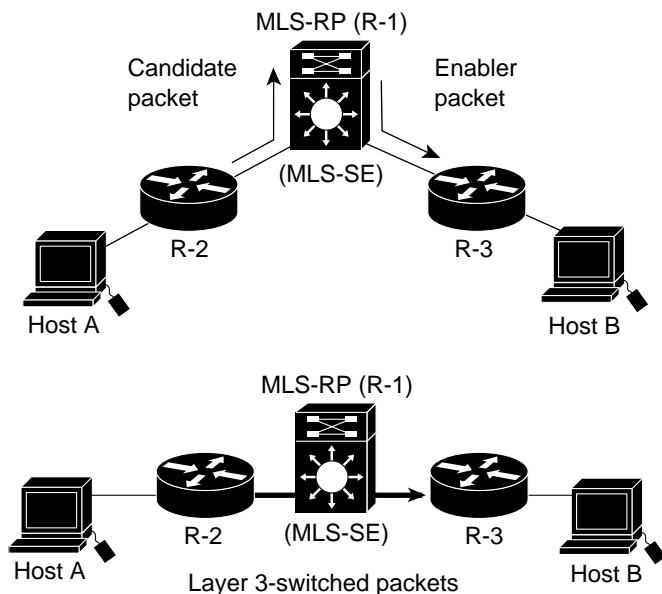


12006

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

In Figure 42-9, 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, Layer 3 switched directly by the switch to Router R-3, and then routed by Router R-3 to the destination host.

**Figure 42-9 Source and Destination Hosts Connected to a Switch Through Different Routers**

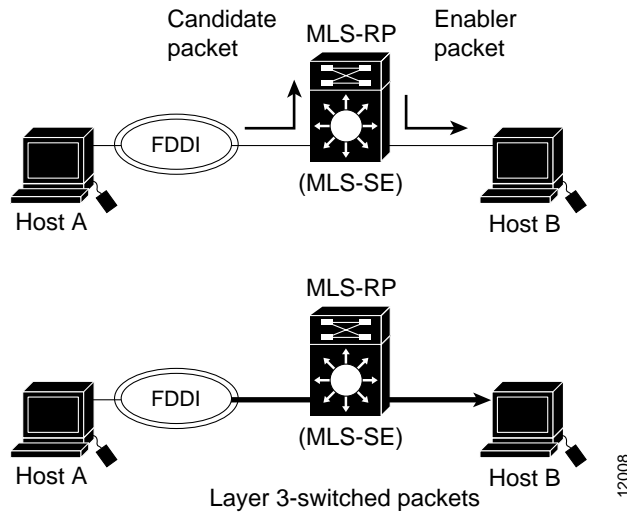


12007

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

In Figure 42-10, the path from Host A to Host B is through a 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 a FDDI VLAN by the switch, translated to an Ethernet VLAN, and then Layer 3 switched directly by the switch to the destination host.

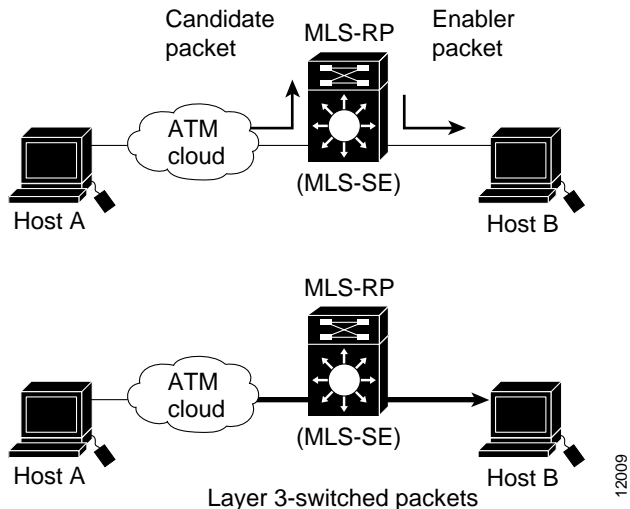
**Figure 42-10 Source Host Connected to Switch Through FDDI Ring**



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

In Figure 42-11, 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 Layer 3 switched directly by the switch to the destination host.

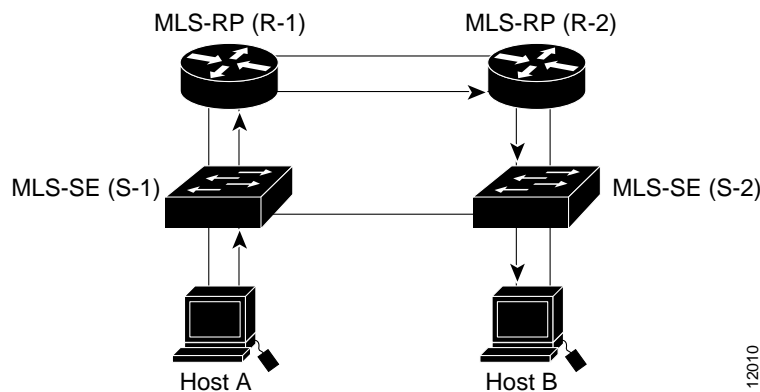
**Figure 42-11 Source Host Connected to Switch Through ATM Cloud**



## Unsupported Topologies

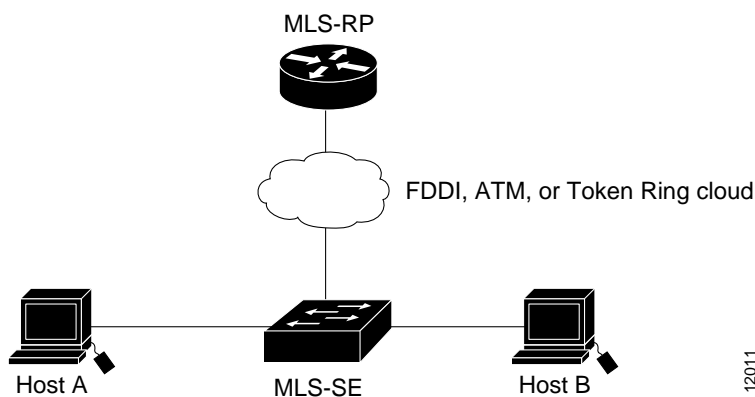
In Figure 42-12, the routed path from Host A to Host B traverses Switch S-1, Routers R-1 and R-2, and Switch S-2. Layer 3 switching is not possible because the candidate packet creates an entry in the MLS cache on Switch S-1, but the enabler packet is forwarded to Router R-2 rather than to Switch S-1. 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 42-12 Unsupported Topologies (Example 1)**



In Figure 42-13, Layer 3 switching is not possible because MLSP is not supported over FDDI, ATM, and Token Ring media.

**Figure 42-13 Unsupported Topologies (Example 2)**



## MLS Configuration Examples

These sections show different example MLS configurations. In these examples, VLAN interfaces 1 and 3 are in the VTP domain Engineering. The management interface is configured on the VLAN 1 interface. Only information relevant to MLS is shown in these configurations.

- Router Configuration with No Access Lists on page 42-38
- Router Configuration with Standard Access List on page 42-39

- Router Configuration with Extended Access List on page 42-39
- Switch Configuration on page 42-40

### Router Configuration with No Access Lists

In this example configuration, no access lists are configured on the RSM VLAN interfaces. Therefore, the flow mask mode is destination-ip.

```
Router# write terminal
Building configuration...

Current configuration:
.
.
.
mls rp ip

interface Vlan1
 ip address 172.20.26.56 255.255.255.0
 mls rp vtp-domain Engineering
 mls rp management-interface
 mls rp ip

interface Vlan2
 ip address 128.6.2.73 255.255.255.0

interface Vlan3
 ip address 128.6.3.73 255.255.255.0
 mls rp vtp-domain Engineering
 mls rp ip
.
.
end
Router#
Router# show mls rp
multilayer switching is globally enabled
mls id is 0006.7c71.8600
mls ip address 172.20.26.56
mls flow mask is destination-ip

number of domains configured for mls 1
vlan domain name: Engineering
  current flow mask: destination-ip
  current sequence number: 82078006
  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: 02:54:21
  keepalive timer expires in 11 seconds
  retry timer not running
  change timer not running

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

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

    mac 0006.7c71.8600
      vlan id(s)
      1      3
```

```

router currently aware of following 1 switch(es):
  switch id 00e0.fe4a.aeff
Router#

```

## Router Configuration with Standard Access List

In this example configuration, a standard access list is configured on the RSM VLAN 3 interface. Therefore, the flow mask mode is source-destination-ip.

```

.
interface Vlan3
 ip address 128.6.3.73 255.255.255.0
 ip access-group 2 out
 mls rp vtp-domain Engineering
 mls rp ip
.

Router# show mls rp
multilayer switching is globally enabled
mls id is 0006.7c71.8600
mls ip address 172.20.26.56
mls flow mask is source-destination-ip

number of domains configured for mls 1
vlan domain name: Engineering
  current flow mask: source-destination-ip
  current sequence number: 82078007
  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: 02:57:31
  keepalive timer expires in 4 seconds
  retry timer not running
  change timer not running

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

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

  mac 0006.7c71.8600
  vlan id(s)
  1      3

router currently aware of following 1 switch(es):
  switch id 00e0.fe4a.aeff

Router#

```

## Router Configuration with Extended Access List

In this example configuration, an extended access list is configured on the RSM VLAN 3 interface. Therefore, the flow mask mode is ip-flow.

```

.
interface Vlan3
 ip address 128.6.3.73 255.255.255.0
 ip access-group 101 out
 mls rp vtp-domain Engineering
 mls rp ip
.

```

```
Router# show mls rp
multilayer switching is globally enabled
mls id is 0006.7c71.8600
mls ip address 172.20.26.56
mls flow mask is ip-flow

number of domains configured for mls 1
vlan domain name: Engineering
  current flow mask: ip-flow
  current sequence number: 82078009
  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: 03:01:52
  keepalive timer expires in 3 seconds
  retry timer not running
  change timer not running

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

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

  mac 0006.7c71.8600
    vlan id(s)
    1      3

router currently aware of following 1 switch(es):
  switch id 00e0.fe4a.aeff

Router#
```

## Switch Configuration

This example configuration shows the switch MLS configuration with NDE enabled.

```
.
#mls
set mls enable
set mls agingtime 256
set mls agingtime fast 0 0
set mls nde flow destination 10.0.2.25/255.255.255.0
set mls nde 171.69.194.140 8000
set mls nde enable
.
```