



CHAPTER 12

Configuring InterVLAN Routing

This chapter describes how to configure the Multilayer Switch Feature Card (MSFC) for interVLAN routing on the Catalyst 6500 series switches.

**Note**

For complete syntax and usage for the commands that are used in this chapter, refer to the *Catalyst 6500 Series Switch Command Reference* publication.

This chapter consists of these sections:

- [Understanding How InterVLAN Routing Works, page 12-1](#)
- [Configuring InterVLAN Routing on the MSFC, page 12-2](#)

**Note**

Refer to the *FlexWAN Module Port Adapter Installation and Configuration Notes* for information about configuring routing on FlexWAN module interfaces.

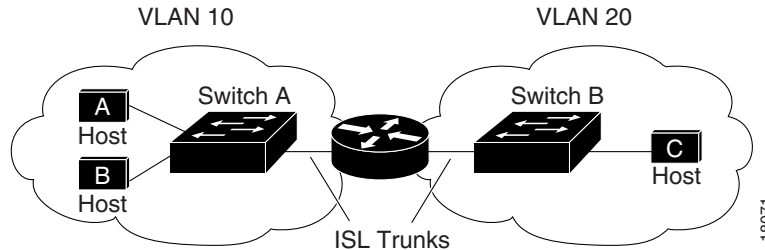
Understanding How InterVLAN Routing Works

The network devices in different VLANs cannot communicate with one another without a router to forward traffic between the VLANs. In most network environments, the VLANs are associated with individual networks or subnetworks.

For example, in an IP network, each subnetwork is mapped to an individual VLAN. In an IPX network, each VLAN is mapped to an IPX network number.

Configuring the VLANs helps to control the size of the broadcast domain and keeps the local traffic local. When an end station in one VLAN needs to communicate with an end station in another VLAN, interVLAN communication is required. This communication is provided by interVLAN routing. You configure one or more routers to route traffic to the appropriate destination VLAN.

[Figure 12-1](#) shows a basic interVLAN routing topology. Switch A is in VLAN 10 and Switch B is in VLAN 20. The router has an interface in each VLAN.

Figure 12-1 Basic InterVLAN Routing Topology

When Host A in VLAN 10 needs to communicate with Host B in VLAN 10, it sends a packet that is addressed to that host. Switch A forwards the packet directly to Host B without sending it to the router.

When Host A sends a packet to Host C in VLAN 20, Switch A forwards the packet to the router, which receives the traffic on the VLAN 10 interface. The router checks the routing table, determines the correct outgoing interface, and forwards the packet out the VLAN 20 interface to Switch B. Switch B receives the packet and forwards it to Host C.

Configuring InterVLAN Routing on the MSFC



Note

This section is for users who are familiar with Cisco IOS software and have some experience configuring Cisco IOS routing. If you are not familiar with configuring Cisco routing, refer to the Cisco IOS documentation on Cisco.com.

These sections describe how to configure interVLAN routing on the MSFC:

- [MSFC Routing Configuration Guidelines, page 12-2](#)
- [Configuring IP InterVLAN Routing on the MSFC, page 12-3](#)
- [Configuring IPX InterVLAN Routing on the MSFC, page 12-3](#)
- [Configuring AppleTalk InterVLAN Routing on the MSFC, page 12-4](#)
- [Configuring MSFC Features, page 12-5](#)

MSFC Routing Configuration Guidelines

This section describes the guidelines (which consists of two main procedures) for configuring interVLAN routing on the MSFC:

1. Create and configure VLANs on the switch and assign VLAN membership to switch ports. For more information, see [Chapter 11, “Configuring VLANs.”](#)
2. Create and configure VLAN interfaces for interVLAN routing on the MSFC. Configure a VLAN interface for each VLAN for which you want to route traffic.

The VLAN interfaces on the MSFC are virtual interfaces. However, you configure them the same as you do a physical router interface.

The MSFC3, MSFC2, MSFC2A, and MSFC support the same range of VLANs as the supervisor engine. MSFC3, MSFC2, and MSFC2A support up to 1,000 VLAN interfaces, and the MSFC supports up to 256 VLAN interfaces.

Configuring IP InterVLAN Routing on the MSFC

To configure interVLAN routing for IP, perform this task:

	Task	Command
Step 1	(Optional) Enable IP routing on the router ¹ .	Router(config)# ip routing
Step 2	(Optional) Specify an IP routing protocol ² .	Router(config)# router <i>ip_routing_protocol</i>
Step 3	Specify a VLAN interface on the MSFC.	Router(config)# interface <i>vlan-id</i>
Step 4	Assign an IP address to the VLAN.	Router(config-if)# ip address <i>n.n.n.n mask</i>
Step 5	Exit configuration mode.	Router(config-if)# Ctrl-Z

1. This step is necessary if you have multiple routers in the network.
2. This step is necessary if you enabled IP routing in Step 1. This step might include other commands, such as using the **network** router configuration command to specify the networks to route. Refer to the documentation for your router platform for detailed information on configuring routing protocols.

This example shows how to enable IP routing on the MSFC, create a VLAN interface, and assign the IP address to the interface:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip routing
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# interface vlan 100
Router(config-if)# ip address 10.1.1.1 255.0.0.0
Router(config-if)# ^Z
Router#
```

Configuring IPX InterVLAN Routing on the MSFC



Note

With Supervisor Engine 720 (MSFC3), IPX routing is done through the software.

To configure interVLAN routing for Internetwork Packet Exchange (IPX), perform this task:

Task	Command
Step 1 (Optional) Enable IPX routing on the router ¹ .	Router(config)# ipx routing
Step 2 (Optional) Specify an IPX routing protocol ² .	Router(config)# ipx router <i>ipx_routing_protocol</i>
Step 3 Specify a VLAN interface on the MSFC.	Router(config)# interface <i>vlan-id</i>
Step 4 Assign a network number to the VLAN ³ .	Router(config-if)# ipx network [<i>network</i> unnumbered] encapsulation <i>encapsulation-type</i>
Step 5 Exit configuration mode.	Router(config-if)# Ctrl-Z

1. This step is necessary if you have multiple routers in the network.
2. This step is necessary if you enabled IPX routing in Step 1. This step might include other commands, such as using the **network** router configuration command to specify the networks to route. Refer to the documentation for your router platform for detailed information on configuring routing protocols.
3. This step enables IPX routing on the VLAN. When you enable IPX routing on the VLAN, you can also specify an encapsulation type.

This example shows how to enable IPX routing on the MSFC, create a VLAN interface, and assign an IPX network address to the interface:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ipx routing
Router(config)# ipx router rip
Router(config-ipx-router)# network all
Router(config-ipx-router)# interface vlan100
Router(config-if)# ipx network 100 encapsulation snap
Router(config-if)# ^Z
Router#
```

Configuring AppleTalk InterVLAN Routing on the MSFC

To configure interVLAN routing for AppleTalk, perform this task:

Task	Command
Step 1 (Optional) Enable AppleTalk routing on the router ¹ .	Router(config)# appletalk routing
Step 2 Specify a VLAN interface on the MSFC.	Router(config)# interface <i>vlan-id</i>
Step 3 Assign a cable range to the VLAN.	Router(config-if)# appletalk cable-range <i>cable-range</i>
Step 4 Assign a zone name to the VLAN.	Router(config-if)# appletalk zone <i>zone-name</i>
Step 5 Exit configuration mode.	Router(config-if)# Ctrl-Z

1. This step is necessary if you have multiple routers in the network.

This example shows how to enable AppleTalk routing on the MSFC, create a VLAN interface, and assign an AppleTalk cable range and zone name to the interface:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# appletalk routing
Router(config)# interface vlan100
Router(config-if)# appletalk cable-range 100-100
Router(config-if)# appletalk zone Engineering
Router(config-if)# ^Z
Router#
```

Configuring MSFC Features

These sections describe the MSFC features:

- [Local Proxy ARP, page 12-5](#)
- [WCCP Layer 2 Redirection, page 12-5](#)
- [Autostate Feature, page 12-6](#)

Local Proxy ARP

With Release 12.1(2)E or later releases, the Local Proxy Address Resolution Protocol (ARP) allows the MSFC to respond to the ARP requests for the IP addresses within a subnet where normally no routing is required. With local proxy ARP enabled, the MSFC responds to all the ARP requests for the IP addresses within the subnet and forwards all traffic between the hosts in the subnet. Use this feature only on the subnets where the hosts are intentionally prevented from communicating directly by the configuration on the switch to which they are connected.

Local proxy ARP is disabled by default. Enter the **ip local-proxy-arp** interface configuration command to enable local proxy ARP on an interface. Enter the **no ip local-proxy-arp** interface configuration command to disable the feature. The Internet Control Message Protocol (ICMP) redirects are disabled on the interfaces where local proxy ARP is enabled.

WCCP Layer 2 Redirection



Note

Supervisor Engine 1 with the Policy Feature Card (PFC) supports this feature with Release 12.1(2)E or later releases. Supervisor Engine 2 with PFC2 supports this feature with Release 12.1(3a)E or later releases. WCCP Layer 2 redirection is not supported on Supervisor Engine 720 or Supervisor Engine 32.

Web Cache Communication Protocol (WCCP) Layer 2 redirection allows directly connected Cisco Cache Engines to use Layer 2 redirection, which is more efficient than Layer 3 redirection, through generic routing encapsulation (GRE). You can configure a directly connected Cache Engine to negotiate WCCP Layer 2 redirection. WCCP Layer 2 redirection requires no configuration on the MSFC. Enter the **show ip wccp web-cache detail** command to display which redirection method is in use for each cache. Follow these guidelines when using this feature:

- WCCP Layer 2 redirection sets the IP flow mask to full-flow mode.
- You can configure the Cisco Cache Engine software release 2.2 or later releases to use WCCP Layer 2 redirection.

- Layer 2 redirection takes place on the switch and is not visible to the MSFC. Entering the **show ip wccp web-cache detail** command on the MSFC displays statistics for only the first packet of a Layer 2 redirected flow, which provides an indication of how many flows, rather than packets, are using Layer 2 redirection. Entering the **show mls entries** command on the supervisor engine displays the other packets in the Layer 2 redirected flows.

Configure the Cisco IOS WCCP as described in the *Cisco IOS Configuration Fundamentals Configuration Guide* at this URL:

http://www.cisco.com/en/US/docs/ios/12_1/configfun/configuration/guide/fcd305.html

Autostate Feature

These MSFC autostate port-based modes are supported:

- [Normal Autostate Mode, page 12-6](#)
- [Autostate Exclude Mode, page 12-6](#)
- [Autostate Track Mode, page 12-7](#)

Normal Autostate Mode

Autostate shuts down (or brings up) the Layer 3 interfaces/subinterfaces on the MSFC and the Multilayer Switch Module (MSM) when the following port configuration changes occur on the switch:

- When the last port on a VLAN goes down, all the Layer 3 interfaces/subinterfaces on that VLAN shut down (are autostated) unless sc0 is on the VLAN or another router is in the chassis with an interface/subinterface in the VLAN.
- When the first port on the VLAN is brought back up, all the Layer 3 interfaces on that VLAN that were previously shut down are brought up.

The Catalyst 6500 series switch does not have knowledge of, or control over, the MSM or MSFC configuration (just as the switch does not have knowledge of, or control over, external router configurations). Autostate does not work on MSM or MSFC interfaces if the MSM or MSFC is not properly configured. For example, consider this MSM trunk configuration:

```
interface GigabitEthernet0/0/0.200
  encaps isl 200
  .
  .
```

In the example, the GigabitEthernet0/0/0.200 interface is not autostated if any of these configuration errors are made:

- VLAN 200 is not configured on the switch.
- Trunking is not configured on the corresponding Gigabit Ethernet switch port.
- Trunking is configured but VLAN 200 is not an allowed VLAN on that trunk.

Autostate Exclude Mode

Autostate exclude mode allows you to specify the ports to exclude from autostate. In normal autostate mode, the Layer 3 interfaces remain up if at least one port in the VLAN remains up. If you have appliances, such as load balancers or firewall servers that are connected to the ports in the VLAN, you can configure these ports to be excluded from the autostate feature to make sure that the forwarding SVI does not go down if these ports become inactive.

Autostate exclude mode affects all VLANs to which the port belongs and is supported on Ethernet, Fast Ethernet, and Gigabit Ethernet ports only.

**Note**

You cannot configure both autostate exclude mode and autostate track mode on the same port.

Autostate Track Mode

You can use autostate track mode to track key VLAN or port connections to the MSFC. When you configure the autostate track mode, the SVI stays up if any tracked connections remain up in the VLAN. Track mode requires that you define a global tracked VLAN group. The VLANs in this group will be tracked by MSFC autostate whether or not you define a member port to be tracked.

When you configure a VLAN and the ports to be tracked by autostate, the tracked SVIs remain down until at least one tracked Ethernet port in the VLAN moves to the Spanning Tree Protocol (STP) forwarding state. Conversely, tracked SVIs remain up if at least one tracked Ethernet port stays in the STP forwarding state.

Autostate track mode is supported on Ethernet, Fast Ethernet, and Gigabit Ethernet ports only.

**Note**

You cannot configure both autostate exclude mode and autostate track mode on the same port.

Configuring Autostate Exclude Mode

To configure autostate exclude mode, perform one of these tasks in privileged mode:

Task	Command
Configure autostate exclude mode.	set msfcautostate exclude <i>mod/port</i>
Clear the autostate configuration.	clear msfcautostate { all <i>mod/port</i> }

This example shows how to exclude a port from MSFC autostate:

```
Console> (enable) set msfcautostate exclude 3/1
Port 3/1 configured as excluded port
Console> (enable)
```

This example shows how to clear the autostate configuration:

```
Console> (enable) clear msfcautostate 3/1
MSFC autostate config cleared on excluded port 3/1
Console> (enable)
```

Configuring Autostate Track Mode

To configure autostate track mode, perform one of these tasks in privileged mode:

Task	Command
Configure autostate to track the specified VLANs.	set msfcautostate track [disable enable <i>vlan_list</i>]
Configure autostate to track the specified ports.	set msfcautostate track <i>mod/port_list</i>
Clear the autostate track mode configuration.	clear msfcautostate all <i>mod/port</i>

This example shows how to configure autostate to track VLANs 20, 21, 22, and 28:

```
Console> (enable) set msfcautostate track enable 20-22,28
Vlans 20-22,28 added to MSFC autostate track vlan group
Console> (enable)
```

This example shows how to configure autostate to track ports 1–5 on module 3:

```
Console> (enable) set msfcautostate track 3/1-5
Port 3/1-5 configured as tracked port
Console> (enable)
```

Displaying the Autostate Configuration

To display the current line protocol state determination for the MSM, perform this task in normal mode:

Task	Command
Display the current line protocol state determination for the MSM.	show msmautostate <i>mod</i>

This example shows how to display the current line protocol state determination for the MSM:

```
Console> show msmautostate
MSM Auto port state: enabled
Console>
```

To display the line protocol state determination for the MSFC, perform this task in privileged mode:

Task	Command
Display the line protocol state determination for the MSFC.	show msfcautostate

This example shows how to display the line protocol state determination for the MSFC:

```
Console> (enable) show msfcautostate
MSFC Auto port state: enabled
Excluded ports:
Tracked ports: 3/1-5
Tracked vlans: 20-22,28
Console> (enable)
```

To check which MSM interfaces are currently autostated, perform this task in enabled mode from the MSM prompt:

Task	Command
Check which MSM interfaces are currently autostated.	show autostate entries

This example shows how to check which MSM interfaces are currently autostated (shut down or brought up through autostate):

```
Router# show autostate entries
Port-channel1.5
Port-channel1.6
Port-channel1.4
Router#
```

Disabling Autostate

To disable autostate if you have an MSM installed, perform this task in privileged mode:

Task	Command
Disable autostate if you have an MSM installed.	set msmautostate disable

Autostate is enabled by default. This example shows how to disable autostate if you have an MSM installed:

```
Console> (enable) set msmautostate disable
MSM port auto state disabled.
Console> (enable)
```

To disable the line protocol state determination of the MSFC, perform this task in privileged mode:



Note

If you toggle (enable to disable and/or disable to enable) the **msfcautostate** command, you might have to use the **shutdown** and **no shutdown** commands to disable and then restart the VLAN and WAN interfaces on the MSFC to bring them back up. Unless there is a valid reason, the MSFC autostate feature should not be disabled.

Task	Command
Disable the line protocol state determination of the MSFC.	set msfcautostate disable

This example shows how to disable the line protocol state determination of the MSFC:

```
Console> (enable) set msfcautostate disable

MSM port auto state disabled.
Console> (enable)
```

