CHAPTER 10

Configuring the Fast Ethernet and Gigabit Ethernet SPAs

This chapter provides information about configuring the 4-Port Fast Ethernet SPA, 8-Port Fast Ethernet SPA, 1-Port 10-Gigabit Ethernet SPA, 2-Port Gigabit Ethernet SPA, 5-Port Gigabit Ethernet SPA, and 10-Port Gigabit Ethernet SPA on the Catalyst 6500 Series switch. It includes the following sections:

For more information about the commands used in this chapter, see the *Catalyst 6500 Series Cisco IOS Command Reference, 12.2SX* publication. Also refer to the related Cisco IOS Release 12.2 software command reference and master index publications. For more information about accessing these publications, see the "Related Documentation" section on page xlv.

For information about managing your system images and configuration files, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2* and *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* publications.

Configuration Tasks

This section describes how to configure the Fast Ethernet and Gigabit Ethernet SPAs and includes information about verifying the configuration.

This section includes the following topics:

Required Configuration Tasks

This section lists the required configuration steps to configure the Fast Ethernet and Gigabit Ethernet SPAs. The commands in the section are applicable for both Fast Ethernet and Gigabit Ethernet SPAs; however, the examples below are for configuring a Gigabit Ethernet SPA. If you are configuring a Fast Ethernet SPA, replace the **gigabitethernet** command with the **fastethernet** command.

Some of the required configuration commands implement default values that might be appropriate for your network. If the default value is correct for your network, then you do not need to configure the command. These commands are indicated by "(As Required)" in the Purpose column.

Note Cisco Discovery Protocol (CDP) is disabled by default on the Cisco 7600 SIP-400 interfaces.

To configure the Fast Ethernet or Gigabit Ethernet SPAs, perform this task:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.

Step 2	`Router(config)# interface fastethernet` *slot/subslot/port*`[.`*subinterface-number*`]`
	or
	`Router(config)# interface gigabitethernet` *slot/subslot/port*`[.`*subinterface-number*`]`
	or
	`Router(config)# interface tengigabitethernet` *slot/subslot/port*`[.`*subinterface-number*`]`
		Specifies the Fast Ethernet, Gigabit Ethernet, or the 10-Gigabit Ethernet interface to configure, where:
		• *slot*/*subslot*/*port*—Specifies the location of the interface. See the "Specifying the Interface Address on a SPA" section on page 10-4.
		• *.subinterface-number*—(Optional) Specifies a secondary interface (subinterface) number.

	Command	Purpose
Step 3	`Router(config-if)# ip address [ip-address mask {secondary} | dhcp {client-id interface-name}{hostname host-name}]`	Sets a primary or secondary IP address for an interface that is using IPv4, where: • *ip-address*—Specifies the IP address for the interface. • *mask*—Specifies the mask for the associated IP subnet. • **secondary**—(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. • **dhcp**—Specifies that IP addresses will be assigned dynamically using DHCP. • **client-id** *interface-name*—Specifies the client identifier. The *interface-name* sets the client identifier to the hexadecimal MAC address of the named interface. • **hostname** *host-name*—Specifies the hostname for the DHCP purposes. The *host-name* is the name of the host to be placed in the DHCP option 12 field. **Note** The DHCP options with this command are not available for all Gigabit Ethernet SPAs and Fast Ethernet SPAs.
Step 4	`Router(config)# ip accounting mac-address {input | output}`	(Optional) Enables MAC address accounting. MAC address accounting provides accounting information for IP traffic based on the source and destination MAC addresses of the LAN interfaces, where: • **input**—Specifies MAC address accounting for traffic entering the interface. • **output**—Specifies MAC address accounting for traffic leaving the interface.
Step 5	`Router(config-if)# mtu bytes`	(As Required) Specifies the maximum packet size for an interface, where: • *bytes*—Specifies the maximum number of bytes for a packet. The default is 1500 bytes.

	Command	Purpose
Step 6	`Router(config-if)# standby [group-number] ip [ip-address [secondary]]`	(Required for HSRP Configuration Only) Creates (or enables) the HSRP group using its number and virtual IP address, where: • (Optional) *group-number*—The group number on the interface for which HSRP is being enabled. The range is 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number. • (Optional on all but one interface if configuring HSRP) *ip-address*—The virtual IP address of the hot standby switch interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces. • (Optional) **secondary**—The IP address is a secondary hot standby switch interface. If neither switch is designated as a secondary or standby switch and no priorities are set, the primary IP addresses are compared and the higher IP address is the active switch, with the next highest as the standby switch. This command enables HSRP but does not configure it further. For additional information on configuring HSRP, see the "Configuring Hot Standby Router Protocol" section of the Cisco IP Configuration Guide, Release 12.2.
Step 7	`Router(config-if)# no shutdown`	Enables the interface.

Specifying the Interface Address on a SPA

SPA interface ports begin numbering with 0 from left to right. Single-port SPAs use only the port number 0. To configure or monitor SPA interfaces, you need to specify the physical location of the SIP, SPA, and interface in the CLI. The interface address format is *slot*/*subslot*/*port*, where:

- *slot*—Specifies the chassis slot number in the Catalyst 6500 Series switch where the SIP is installed.
- *subslot*—Specifies the secondary slot of the SIP where the SPA is installed.
- *port*—Specifies the number of the individual interface port on a SPA.

The following example shows how to specify the first interface (0) on a SPA installed in the first subslot of a SIP (0) installed in chassis slot 3:

```
Router(config)# interface serial 3/0/0
```

This command shows a serial SPA as a representative example; however, the same *slot*/*subslot*/*port* format is similarly used for other SPAs (such as ATM and POS) and other non-channelized SPAs.

Modifying the MAC Address on the Interface

The Gigabit Ethernet SPAs use a default MAC address for each port that is derived from the base address that is stored in the electrically erasable programmable read-only memory (EEPROM) on the backplane of the Catalyst 6500 Series switch.

To modify the default MAC address of an interface to some user-defined address, perform this task in interface configuration mode:

Command	Purpose
`Router(config-if)# mac-address` *ieee-address*	Modifies the default MAC address of an interface to some user-defined address, where: • *ieee-address*—Specifies the 48-bit Institute of Electrical and Electronics Engineers (IEEE) MAC address written as a dotted triple of four-digit hexadecimal numbers (*xxxx.yyyy.zzzz*).

To return to the default MAC address on the interface, use the **no** form of the command.

Verifying the MAC Address

To verify the MAC address of an interface, use the **show interfaces gigabitethernet** privileged EXEC command and observe the value shown in the "address is" field.

The following example shows that the MAC address is 000a.f330.2e40 for interface 1 on the SPA installed in subslot 0 of the SIP installed in slot 2 of the Catalyst 6500 Series switch:

```
Router# show interfaces gigabitethernet 2/0/1
GigabitEthernet2/0/1 is down, line protocol is down
  Hardware is GigEther SPA, address is 000a.f330.2e40 (bia 000a.f330.2e40)
  Internet address is 2.2.2.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full-duplex, 1000Mb/s, link type is force-up, media type is SX
  output flow-control is on, input flow-control is on
(Additional output removed for readability)
```

Obtaining MAC Address Accounting Statistics

The **ip accounting mac-address** [**input** | **output**] command can be entered to enable MAC address accounting on an interface.

After MAC address accounting is enabled, MAC address statistics can be obtained by entering the **show interfaces mac-accounting** command.

Configuring HSRP

Hot Standby Router Protocol (HSRP) provides high network availability because it routes IP traffic from hosts without relying on the availability of any single switch. HSRP is used in a group of switches for selecting an active switch and a standby switch. (An *active switch* is the switch of choice for routing packets; a *standby switch* is a switch that takes over the switching duties when an active switch fails, or when preset conditions are met).

HSRP is enabled on an interface by entering the **standby** [*group-number*] **ip** [*ip-address* [**secondary**]] command. The **standby** command is also used to configure various HSRP elements. This document does not discuss more complex HSRP configurations. For additional information on configuring HSRP, see the "Configuring Hot Standby Router Protocol" section of the Cisco IP Configuration Guide, Release 12.2.

In the following HSRP configuration, standby group 2 on GigabitEthernet port 2/1/0 is configured at a priority of 110 and is also configured to have a preemptive delay should a switchover to this port occur.

```
Router(config)# interface GigabitEthernet 2/1/0
Router(config-if)# standby 2 ip 120.12.1.200
Router(config-if)# standby 2 priority 110
Router(config-if)# standby 2 preempt
```

Verifying HSRP

To display HSRP information, use the **show standby** command in EXEC mode:

```
Router# show standby
Ethernet0 - Group 0
Local state is Active, priority 100, may preempt
Hellotime 3 holdtime 10
Next hello sent in 0:00:00
Hot standby IP address is 198.92.72.29 configured
Active router is local
Standby router is 198.92.72.21 expires in 0:00:07
Standby virtual mac address is 0000.0c07.ac00
Tracking interface states for 2 interfaces, 2 up:
UpSerial0
UpSerial1
```

Modifying the Interface MTU Size

The Cisco IOS software supports three different types of configurable maximum transmission unit (MTU) options at different levels of the protocol stack:

- Interface MTU—Checked by the SPA on traffic coming in from the network. Different interface types support different interface MTU sizes and defaults. The interface MTU defines the maximum packet size allowable (in bytes) for an interface before drops occur. If the frame is smaller than the interface MTU size, but is not smaller than the minimum frame size for the interface type (such as 64 bytes for Ethernet), then the frame continues to process.
- IP MTU—Can be configured on a subinterface and is used by the Cisco IOS software to determine whether fragmentation of a packet takes place. If an IP packet exceeds the IP MTU size, then the packet is fragmented.
- Tag or Multiprotocol Label Switching (MPLS) MTU—Can be configured on a subinterface and allows up to six different labels, or tag headers, to be attached to a packet. The maximum number of labels is dependent on your Cisco IOS software release.

Different encapsulation methods and the number of MPLS MTU labels add additional overhead to a packet. For example, Subnetwork Access Protocol (SNAP) encapsulation adds an 8-byte header, dot1q encapsulation adds a 2-byte header, and each MPLS label adds a 4-byte header (*n* labels x 4 bytes).

For the Fast Ethernet and Gigabit Ethernet SPAs on the Catalyst 6500 Series switch, the default MTU size is 1500 bytes. When the interface is being used as a Layer 2 port, the The maximum configurable MTU is 9216 bytes. The SPA automatically adds an additional 38 bytes to the configured MTU size to accommodate some of the additional overhead.

Interface MTU Configuration Guidelines

When configuring the interface MTU size on a Fast Ethernet and Gigabit Ethernet SPA on a Catalyst 6500 Series switch, consider the following guidelines:

- The default interface MTU size accommodates a 1500-byte packet, plus 38 additional bytes to cover the following additional overhead:
  - Layer 2 header—14 bytes
  - SNAP header—8 bytes
  - Dot1q header—4 bytes
  - 2 MPLS labels—8 bytes
  - CRC—4 bytes

Note Depending on your Cisco IOS software release, a certain maximum number of MPLS labels are supported. If you need to support more than two MPLS labels, then you need to increase the default interface MTU size.

- If you are using MPLS, be sure that the **mpls mtu** command is configured for a value less than or equal to the interface MTU.
- If you are using MPLS labels, then you should increase the default interface MTU size to accommodate the number of MPLS labels. Each MPLS label adds 4 bytes of overhead to a packet.

Interface MTU Guidelines for Layer 2 Ports

On Layer 2 ports, it is important to understand the concept of the jumbo MTU. The jumbo MTU can be configured using the **system jumbomtu** command, although this command is only supported in the following situations:

- The port is a member of a Layer 2 EtherChannel.
- The new MTU size on the Layer 2 port is less than the currently configured maximum MTU for the port.

Note Fast Ethernet SPAs cannot function as Layer 2 ports.

Interface MTU Configuration Task

To modify the MTU size on an interface, perform this task in interface configuration mode:

Command	Purpose
`Router(config-if)# mtu bytes`	Configures the maximum packet size for an interface, where: • *bytes*—Specifies the maximum number of bytes for a packet. The default is 1500 bytes and the maximum configurable MTU is 9216 bytes.

To return to the default MTU size, use the **no** form of the command.

Verifying the MTU Size

To verify the MTU size for an interface, use the **show interfaces gigabitethernet** privileged EXEC command and observe the value shown in the MTU field.

The following example shows an MTU size of 1500 bytes for interface port 1 (the second port) on the Gigabit Ethernet SPA installed in the top subslot (0) of the SIP that is located in slot 2 of the Catalyst 6500 Series switch:

```
Router# show interfaces gigabitethernet 2/0/1
GigabitEthernet2/0/1 is down, line protocol is down
  Hardware is GigEther SPA, address is 000a.f330.2e40 (bia 000a.f330.2e40)
  Internet address is 2.2.2.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
```

Configuring the Encapsulation Type

By default, the interfaces on the Fast Ethernet and Gigabit Ethernet SPAs support Advanced Research Projects Agency (ARPA) encapsulation. They do not support configuration of service access point (SAP) or SNAP encapsulation for transmission of frames; however, the interfaces will properly receive frames that use SAP and SNAP encapsulation.

The only other encapsulation supported by the SPA interfaces is IEEE 802.1Q encapsulation for virtual LANs (VLANs).

Configuring Autonegotiation on an Interface

Fast Ethernet and Gigabit Ethernet interfaces use a connection-setup algorithm called *autonegotiation.* Autonegotiation allows the local and remote devices to configure compatible settings for communication over the link. Using autonegotiation, each device advertises its transmission capabilities and then agrees upon the settings to be used for the link.

For the Fast Ethernet and Gigabit Ethernet interfaces on the Catalyst 6500 Series switch, flow control is autonegotiated when autonegotiation is enabled. Autonegotiation is enabled by default.

The following guidelines should be followed regarding autonegotiation:

- If autonegotiation is disabled on one end of a link, it must be disabled on the other end of the link. If one end of a link has autonegotiation disabled while the other end of the link does not, the link will not come up properly on both ends.
- Autonegotiation is not supported on the 10-Port Gigabit Ethernet SPA on the Cisco 7600 SIP-600.
- Flow control can be configured separately of autonegotiation when Ethernet SPAs are installed in a SIP-600.
- Flow control is enabled by default.
- Flow control will be on if autonegotiation is disabled on both ends of the link.
- Flow control cannot be disabled on a Fast Ethernet SPA.

Disabling Autonegotiation

Autonegotiation is automatically enabled and can be disabled on the Fast Ethernet interfaces on the Cisco 7600 SIP-200, and the Gigabit Ethernet interfaces on the Cisco 7600 SIP-400 or Cisco 7600 SIP-600. During autonegotiation, advertisement for flow control, speed, and duplex is advertised. If the Gigabit Ethernet interface is connected to a link that has autonegotiation disabled, autonegotiation should either be reenabled on the other end of the link or disabled on the Fast Ethernet or Gigabit Ethernet SPA if possible. Both ends of the link will not come up properly if only one end of the link has disabled autonegotiation.

Note Speed and duplex configurations are negotiated using autonegotiation. However, the only values that are negotiated are 100 Mbps for speed and full-duplex for duplex for Fast Ethernet SPAs, and 1000 Mbps for speed and full-duplex for duplex for Gigabit Ethernet SPAs. From a user's perspective, these settings are not negotiated, but are enabled using autonegotiation.

To disable autonegotiation on Fast Ethernet or Gigabit Ethernet SPAs, perform this task in interface configuration mode. Autonegotiation cannot be disabled on the 1-Port 10-Gigabit Ethernet SPA and 10-Port Gigabit Ethernet SPA when used in a SIP-400.

	Command	Purpose
Step 1	`Router(config-if)# no negotiation auto`	Disables autonegotiation on a Fast Ethernet SPA interface on the Cisco 7600 SIP-200 or a Gigabit Ethernet SPA interfaces on the Cisco 7600 SIP-400. No advertisement of flow control occurs.
Step 2	`Router(config-if)# speed nonegotiate`	Disables autonegotation of speed. This command first became available for SPAs when run in the SIP-600 and is not available in many setups.

Enabling Autonegotiation

Autonegotiation is automatically enabled and cannot be disabled (autonegotiation for the 10-Port Gigabit Ethernet SPA can be disabled when the SPA is installed in a SIP-600). During autonegotiation, advertisement and configuration of flow control, speed, and duplex occurs (flow control configuration is possible independently of autonegotiation when the Gigabit Ethernet SPA is installed in a SIP-600.

See the Configuring Flow Control for an Ethernet SPA Interface in a SIP-600, page 10-20). To reenable autonegotiation on a Fast Ethernet or Gigabit Ethernet interface, perform this task in interface configuration mode:

	Command	Purpose
Step 1	`Router(config-if)# negotiation auto`	Enables autonegotiation on a Fast Ethernet SPA interface on a Cisco 7600 SIP-200 or a Gigabit Ethernet SPA interfaces on the Cisco 7600 SIP-400. Advertisement of flow control occurs.
Step 2	`Router(config-if)# no speed nonegotiate`	Reenables autonegotation of speed. This command first became available for SPAs when run in the SIP-600 and is not available in many setups.

Configuring an Ethernet VLAN

For information on configuring Ethernet VLANs, see the "Creating or Modifying an Ethernet VLAN" section of the "Configuring VLANs" chapter in the *Cisco IOS Software Configuration Guide, Release 12.2(33)SXH and Later Releases*.

Configuring a Subinterface on a VLAN

You can configure subinterfaces on the Fast Ethernet SPA interfaces and Gigabit Ethernet SPA interfaces on a VLAN using IEEE 802.1Q encapsulation. Cisco Discovery Protocol (CDP) is disabled by default on the 2-Port Gigabit Ethernet SPA interfaces and subinterfaces on the Cisco 7600 SIP-400.

Note On any Cisco 7600 SIP-600 Ethernet port subinterface using VLANs, a unique VLAN ID must be assigned. This VLAN ID cannot be in use by any other interface on the Catalyst 6500 Series switch.

To configure a SPA subinterface on a VLAN, perform this task beginning in interface configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface fastethernet` *slot/subslot/port.subinterface-number* or `Router(config)# interface gigabitethernet` *slot/subslot/port.subinterface-number* or `Router(config)# interface tengigabitethernet` *slot/subslot/port.subinterface-number*	Specifies the Fast Ethernet, Gigabit Ethernet or 10-Gigabit Ethernet interface to configure, where: • *slot/subslot/port*—Specifies the location of the interface. See the "Specifying the Interface Address on a SPA" section on page 10-4. • *.subinterface-number*—Specifies a secondary interface (subinterface) number.
Step 2	`Router(config-subif)# encapsulation dot1q` *vlan-id*	Defines the encapsulation format as IEEE 802.1Q ("dot1q"), where *vlan-id* is the number of the VLAN (1–4095).
Step 3	`Router(config-if)# ip address` *ip-address mask* [**secondary**]	Sets a primary or secondary IP address for an interface, where: • *ip-address*—Specifies the IP address for the interface. • *mask*—Specifies the mask for the associated IP subnet. • **secondary**—(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

Verifying Subinterface Configuration on a VLAN

To verify the configuration of a subinterface and its status on the VLAN, use the **show vlans** privileged EXEC command.

The following example shows the status of subinterface number 1 on port 0 on the SPA in VLAN number 200:

```
Router# show vlans
VLAN ID:200 (IEEE 802.1Q Encapsulation)

Protocols Configured:         Received:       Transmitted:
          IP                  0                  14

VLAN trunk interfaces for VLAN ID 200:

GigabitEthernet4/1/0.1 (200)

      IP:12.200.21.21

      Total 0 packets, 0 bytes input
      Total 2 packets, 120 bytes output
```

Configuring Layer 2 Switching Features

The Catalyst 6500 Series switch supports simultaneous, parallel connections between Layer 2 Ethernet segments. After you review the SPA-specific guidelines described in this document, then refer to the "Configuring Layer 2 Ethernet Interfaces" section of the *Cisco IOS Software Configuration Guide, Release 12.2(33)SXH and Later Releases* for more information about configuring the Layer 2 Switching features.

Configuring MPLSoGRE and mVPNoGRE

The MPLS over generic routing encapsulation (MPLSoGRE) and multicast virtual private network over generic routing encapsulation (mVPNoGRE) provides a mechanism to send unicast and multicast packets across a non-MPLS network. This is accomplished by creating a GRE tunnel across the non-MPLS network. When MPLS (unicast VRF) or mVPN (multicast VRF) packets are sent across the non-MPLS network, they are encapsulated within a GRE packet and transverse the non-MPLS network through the GRE tunnel. Upon receiving the GRE packet at the other side of the non-MPLS network, it removes the GRE header and forwards the inner MPLS or unicast VRF or mVPN packet to its final destination.

Note For mVPNoGRE, there is one outer packet and two inner packets. The outer packet is unicast GRE. The first inner packet is multicast GRE (mVPN). The second inner packet is normal (customer) multicast.

Note MPLSoGRE and mVPNoGRE are not supported on Fast Ethernet SPAs on the Cisco 7600 SIP-200.

MPLSoGRE Support

MPLSoGRE supports the following features:

- PE-to-PE tunneling of VRF unicast and multicast packets.
- IPv4 on CE-facing interfaces.
- IPv4 on core-facing interfaces.
- GRE 4-byte headers (no option fields).
- Non-dedicated physical interface supporting both tunneled and non-tunneled traffic.
- Only a single route for the tunnel between the Cisco 7600 SIP-400 physical interface or subinterface and the IP cloud may exist.
- No software imposed limit on the maximum number of tunnels. The SIP-400 supports a maximum number of 128 tunnels. Tunnel traffic can be routed through SIP-400 main interfaces or subinterfaces.

MPLSoGRE Restrictions

The following are not supported with MPLSoGRE:

- Ingress/egress features are not supported on the tunnel interface; they are supported on the physical interface or subinterface.
- GRE options: sequencing, checksum, key, source route.

- Some tunnel options: carry security options of client packet, Unidirectional Link Routing, Mobile IP path MTU discovery.
- The Cisco 7600 SIP-400 physical interface or subinterface used for the tunnel endpoint may not be used to transport native MPLS or its variations (for example, AToMoMPLS, EoMPLS, FRoMPLS, and PPPoMPLS).
- IPv6.
- Advanced features such as Carrier Supporting Carrier (CSC) and Inter-Autonomous Systems (Inter-AS).
- Multiple tunnels on the same Cisco 7600 SIP-400 interface or subinterfaces.

PE-to-PE Tunneling

MPLSoGRE and mVPNoGRE use the provider edge to provider edge (PE-to-PE) tunneling variation. This feature provides a scalable way to connect multiple customer networks across a non-MPLS network.by multiplexing traffic destined to multiple customer networks through a single GRE tunnel.

On each side of the non-MPLS network, each customer edge (CE) switch is assigned a VPN routing and forwarding (VRF) number by the PE switch. The IP networks behind the CE switches are learned by the PE switch through a routing protocol such as BGP, OSPF or RIP. Routes to these networks are then stored in the VRF routing table for that CE switch.

The PE switch on one side of the non-MPLS network is learned by the PE switch on the other side of the non-MPLS network though a routing protocol running within the non-MPLS network. Routes between the PE switches are stored in the main or default routing table.

Routes of the customer networks behind the PE switch are learned by the other PE switch through BGP and are not known to the non-MPLS network. This is accomplished by defining a static route to BGP neighbor (the other PE switch) through a GRE tunnel across the non-MPLS network. When routes are learned from the BGP neighbor, they will have the next-hop of the GRE tunnel and all customer network traffic will be sent using the GRE tunnel.

GRE Tunnel Attached to a Cisco 7600 SIP-400 Interface or Subinterface

For the Catalyst 6500 Series switch to perform the MPLS and mVPN processing and have the Cisco 7600 SIP-400 perform the GRE processing, a GRE tunnel must be attached to a Cisco 7600 SIP-400 MPLS and PIM (multicast) enabled interface or subinterface. The Catalyst 6500 Series switch views the Cisco 7600 SIP-400 main interface or subinterface as an MPLS or PIM interface so MPLS and mVPN processing is performed, and provides the Cisco 7600 SIP-400 with the correlation information needed to perform GRE processing.

Tunnel Interface Configuration

The **ip pim sparse-mode** command is not configured on the tunnel interface. It is automatically configured on the Cisco 7600 SIP-400 interface or subinterface when a tunnel is attached to the interface or subinterface.

The tunnel source IP address is the IP address of the Cisco 7600 SIP-400 interface or subinterface. The following example illustrates the tunnel interface configuration on the Catalyst 6500 Series switch:

```
Router(config)# interface Tunnel1
Router(config-if)# ip address 8.0.0.1 255.0.0.0
Router(config-if)# mpls label protocol ldp
Router(config-if)# tag-switching ip
Router(config-if)# tunnel source 6.0.0.1
Router(config-if)# tunnel destination 7.0.0.1
```

Configuring AToM over GRE

MPLS over generic routing encapsulation (MPLSoGRE) encapsulates MPLS packets inside IP tunnels, creating a virtual point-to-point link across non-MPLS networks. This allows users of primarily MPLS networks to continue to use existing non-MPLS legacy networks until migration to MPLS is possible. Any Transport over MPLS over GRE (AToMoGRE) includes support for the following transports:

- ATM over MPLS
- Frame Relay over MPLS (FRoMPLS)
- High-Level Data Link Control (HDLC) over MPLS
- Scalable Ethernet over MPLS (EoMPLS)
- Circuit Emulation over Packet (CEoP)
- Hardware-based EoMPLS

AToMoGRE is supported in Cisco IOS Release 12.2(33)SXI or later releases, and is supported only on the following hardware:

- Cisco 7600 SIP-400, 5-Port Gigabit Ethernet SPA, 2-Port Gigabit Ethernet SPA (core facing)
- ATM SPA (such as 2-Port OC-3c/STM-1 ATM SPA, 4-Port OC-3c/STM-1 ATM SPA, 1-Port OC-12c/STM-4 ATM SPA, 1-Port OC-48c/STM-16 ATM SPA), CEoP SPA (such as 24-Port Channelized T1/E1/J1 CEoP SPA) with inverse multiplexing (IMA) support, and all Ethernet interfaces
- Supervisor 32, Supervisor 720, or RSP720

AToMoGRE supports the following features:

- Provider edge (PE)-to-PE, provider (P)-to-PE, and P-to-P tunneling of MPLS packets (see Figure 10-1, Figure 10-2, and Figure 10-3).

Figure 10-1 PE-to-PE GRE Tunnel

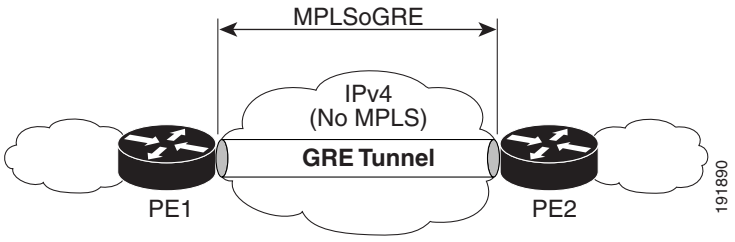


Figure 10-2 P-to-PE GRE Tunnel

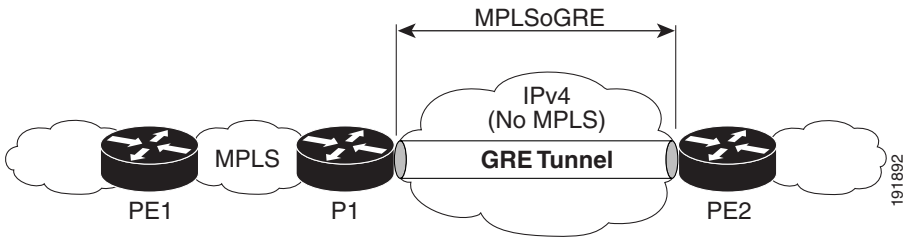
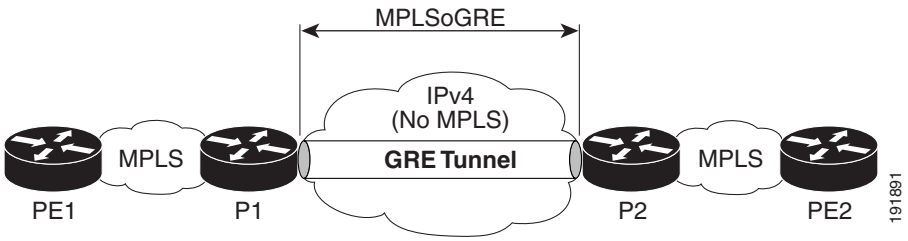


Figure 10-3 P-to-P GRE Tunnel



- IPv4 on customer edge (CE) facing interfaces.
- IPv4 on core facing interfaces.
- GRE 4-byte headers (no option fields).
- Nondedicated physical interface supporting both tunneled and nontunneled traffic.
- Multiple routes for the tunnel between the Cisco 7600 SIP-400 physical interface or subinterface and the IP cloud may exist. The routing protocol will pick only one route for MPLSoGRE traffic.
- No software-imposed limit on the maximum number of tunnels. The Cisco 7600 SIP-400 supports a maximum number of 128 tunnels. Tunnel traffic can be routed through Cisco 7600 SIP-400 main interfaces or subinterfaces.
- The Cisco 7600 SIP-400 physical interface or subinterface used for the tunnel endpoint can be used to carry native MPLS and AToMoMPLS and its variations: hardware-based EoMPLS, FRoMPLS, PPPoMPLS, HDLCoMPLS, Scalable EoMPLS, and CEoP.

AToMoGRE Configuration Guidelines

The following guidelines apply to AToMoGRE:

- Ingress and egress features are not supported on the tunnel interface; they are supported on the physical interface or subinterface.
- Unsupported GRE options are sequencing, checksum, key, and source route.
- Unsupported tunnel options are Carry Security Options of Client Packet, Unidirectional Link Routing, and Mobile IP Path MTU Discovery.
- The Cisco 7600 SIP-400 physical interface or subinterface used for the tunnel endpoint cannot be used to carry software-based EoMPLS and VPLS. Advanced features such as Carrier Supporting Carrier (CSC) and Inter-Autonomous Systems (Inter-AS) are not supported.
- AToM over GRE cannot be combined with the AToM Tunnel Select feature.

Configuring the Cisco 7600 SIP-400 Interface or Subinterface

Two configuration commands are required for configuring a Cisco 7600 SIP-400 interface or subinterface. The keywords of the commands may change based on input from the parser policy, but their placement and parameters remain the same. To configure the interface or subinterface, perform this task:

	Command	Purpose
Step 1	`Router(config-subif)# tunnel-interface tunnel-name`	Attaches a GRE tunnel to a Cisco 7600 SIP-400 subinterface. If the Cisco 7600 SIP-400 interface supports subinterfaces, the command will be available in subinterface configuration mode. If the Cisco 7600 SIP-400 interface does *not* support subinterfaces, the command is only available in interface configuration mode.
Step 2	`Router(config-subif)# ip route a.b.c.d e.f.g.h [i.j.k.l]`	Defines IP traffic that should be tunneled. This will normally be the IP address of the BGP neighbor. This command is only available in a submode of the **tunnel-interface** command. *a.b.c.d* is the IP address. *e.f.g.h* is the IP mask. *i.j.k.l* is the IP address of the next-hop switch.

The following example shows the commands to configure the MPLSoGRE and mVPNoGRE feature on a Cisco 7600 SIP-400 interface or subinterface. However, this example uses a Cisco 7600 SIP-400 interface that does *not* support subinterfaces:

```
Router# configure terminal
Router(config)# int pos2/0/0
Router(config-if)# tunnel-interface tu1
Router(config-if-ti)# ip route 4.0.0.1 255.255.255.255
Router(config-if-ti)# exit
Router(config-if)# end
Router#
```

When **tunnel-interface** is configured on the Cisco 7600 SIP-400 interface or subinterface, **ip pim sparse-mode** and **tag-switching ip** are automatically added to the interface. A static route to IP address contained on the **ip route** command is internally created. The following example shows the output of a **show running interface** after adding or configuring **tunnel-interface**. However, this example uses a Cisco 7600 SIP-400 interface that does *not* support subinterfaces:

```
Router# show run int pos2/0/0
!
interface POS2/0/0
 ip address 6.0.0.1 255.0.0.0
 ip pim sparse-mode
 no keepalive
 tunnel-interface Tunnel1
    ip route 4.0.0.1 255.255.255.255
    exit-tunnel-interface
 tag-switching ip
 clock source internal
end
```

Note You do not need to configure a static route (globally or on the tunnel) to the BGP neighbor on the Catalyst 6500 Series switch. This is automatically done by the **ip route** command under the **tunnel-interface** command on the Cisco 7600 SIP-400 interface or subinterface.

Displaying Unicast Routes

The display of unicast routes (Main Routing Table) shows the next hop for the BGP neighbor to be the Cisco 7600 SIP-400 interface or subinterface. On a switch that natively supports this feature, the next hop for the BGP neighbor is the tunnel interface.

The following example shows the output from the **show ip route** command:

```
Router# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     17.0.0.0/32 is subnetted, 1 subnets
O       17.0.0.2 [110/3] via 6.0.0.2, 00:09:55, POS2/0/0
     2.0.0.0/32 is subnetted, 1 subnets
C       2.0.0.1 is directly connected, Loopback0
     3.0.0.0/32 is subnetted, 1 subnets
O       3.0.0.1 [110/2] via 6.0.0.2, 00:09:55, POS2/0/0
S    64.0.0.0/8 [1/0] via 172.18.20.1
     4.0.0.0/32 is subnetted, 2 subnets
S       4.0.0.1 is directly connected, POS2/0/0
O       4.0.0.3 [110/3] via 6.0.0.2, 00:09:55, POS2/0/0
C    6.0.0.0/8 is directly connected, POS2/0/0
```

Displaying Multicast Routes

The display of multicast routes (groups) shows the output interface for the 239.0.0.0/8 group to be the Cisco 7600 SIP-400 interface or subinterface. On a switch that natively supports this feature, the output interface is the tunnel interface.

The following example shows the output from the **show ip mroute** command:

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

(2.0.0.1, 239.1.1.1), 00:02:02/00:03:02, flags: sTZ
  Incoming interface: Loopback0, RPF nbr 0.0.0.0, RPF-MFD
  Outgoing interface list:
    POS2/0/0, Forward/Sparse, 00:00:58/00:03:02, H

(4.0.0.1, 239.1.1.1), 00:00:58/00:02:02, flags: sTIZ
  Incoming interface: POS2/0/0, RPF nbr 8.0.0.2, RPF-MFD
  Outgoing interface list:
    MVRF vpn1, Forward/Sparse, 00:00:58/00:02:02, H
```

Displaying Tunnel-to-Interface Mappings

The **show cwan mplsogre** command displays the tunnel-to-interface mappings. The following example illustrates the output of the **show cwan mplsogre** command, which displays the tunnel-to-interface mappings:

```
Router# show cwan mplsogre
POS2/0/0
  Tunnel1 is attached
    Interface
      VLAN: 1022, STATE: UP
      IP Address: 6.0.0.1          IP Mask: 255.0.0.0
    Tunnel
      VLAN: 1017, STATE: UP
      IP Address: 8.0.0.1          IP Mask: 255.0.0.0
      Src Address: 6.0.0.1, Dst Address: 7.0.0.1
      Static Routes to Tunnel: 1
        IP Address: 4.0.0.1          IP Mask: 255.255.255.255
```

Scalable EoMPLS

As of the 12.2(33)SXH release, scalable EoMPLS now allows a Cisco 7600 SIP-400-based linecard to face the CE. This configuration allows the platform to scale the number of EoMPLS VCs that it can support from 4 K to 12 K. When AToM **xconnect** commands are placed on Cisco 7600 SIP-400 subinterfaces, the linecard performs AToM imposition and disposition. The supervisor engine performs only MPLS switching on traffic from these interfaces. Additionally, configuring **xconnect** commands on Cisco 7600 SIP-400 subinterfaces will not consume globally significant VLANs on a per xconnect basis. This change also provides the ability to support FRR on EoMPLS VCs with the same model as other CEF/MFI-based AToM configurations.

To achieve this scalability, Cisco 7600 SIP-400 must be the CE-facing linecard as opposed to the current model of a LAN linecard facing the CE. With Cisco 7600 SIP-400 configured for scalable EoMPLS, any linecard capable of switching MPLS packets may be core facing.

On a Supervisor Engine 720, configuring EoMPLS under a non-VLAN interface is considered hardware-based EoMPLS. Configuring EoMPLS on a VLAN interface is considered to be software-based MPLS. Configuring EoMPLS on Cisco 7600 SIP-400 subinterfaces is considered to be Scalable EoMPLS.

Configuring Flow Control Support on the Link

Flow control is turned on or off based on the result of the autonegotiation on the Cisco 7600 SIP-400. On the Cisco 7600 SIP-600, flow control can be configured independently of autonegotiation. For information on this process, see the "Configuring Autonegotiation on an Interface" section on page 10-8.

This section discusses the following topics:

Verifying Flow Control Status for an Ethernet SPA Interface on a SIP-200

The following example shows how to verify that flow control pause frames are being transmitted and received for a Fast Ethernet SPA on the Cisco 7600 SIP-200:

```
Router# show hw sub 2 counter mac
    Show counters info for Subslot 2:
    port:0
    good_octets_received: 2046026640038
    bad_octets_received: 0
    good_frames_received: 31969140675
    bad_frames_received: 0
    broadcast_frames_received: 2
    multicast_frames_received: 3562
    good_octets_sent: 1373554315151
    good_frames_sent: 22892514199
    broadcast_frames_sent: 0
    multicast_frames_sent: 0
    mac_transfer_error: 0
    excessive_collision: 0
    unrecog_mac_control_received: 0
    fc_sent: 11232431
    good_fc_received: 0
    rx_over_flow_events: 234082101
    undersize: 0
    fragments: 0
    oversize: 0
    jabber: 0
    mac_rcv_error: 0
    bad_crc: 0
    collisions: 0
    late_collision: 0
    rate_limit_dropped: 0
    tx_fifo_full_packet_drops : 0
    spi4_rx_frames: 2814271686
    spi4_tx_frames: 1328805298
```

Verifying Flow Control Status for an Ethernet SPA Interface on a SIP-400

To verify flow control status on a Gigabit Ethernet interface on a SPA, use the **show interfaces gigabitethernet** privileged EXEC command and view the "output flow-control is" and "input flow-control is" output lines to see if input and output flow control is on or off. The "pause input" and "pause output" counters of the output of this command can be used to view the number of pause frames sent or received by the interface.

The following example shows that zero pause frames have been transmitted and received by the MAC device for interface port 1 (the second port) on the SPA located in subslot 0 of the SIP that is installed in slot 2 of the Catalyst 6500 Series switch:

```
Router# show interfaces gigabitethernet 2/0/1
GigabitEthernet2/0/1 is down, line protocol is down
  Hardware is GigEther SPA, address is 000a.f330.2e40 (bia 000a.f330.2e40)
  Internet address is 2.2.2.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full-duplex, 1000Mb/s, link type is force-up, media type is SX
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 03:18:49, output 03:18:44, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

```
1703 packets input, 638959 bytes, 0 no buffer
Received 23 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 1670 multicast, 0 pause input
1715 packets output, 656528 bytes, 0 underruns
0 output errors, 0 collisions, 4 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
```

Configuring Flow Control for an Ethernet SPA Interface in a SIP-600

On the Cisco 7600 SIP-600, flow control can be configured on Ethernet SPA interfaces by entering the **flowcontrol send** command to configure the interface to transmit pause frames or the **flowcontrol receive** command to configure the interface to receive pause frames.

To configure flow control on an Ethernet interface, perform this task in interface configuration mode:

	Command	Purpose
Step 1	`Router(config-if)# flowcontrol send {desired | off | on}`	Enables transmission of outgoing pause frames. The following options can be configured with this command: • **desired**—Allows, but does not require, outgoing pause frames to leave the interface. • **off**—Disables transmission of outgoing pause frames. • **on**—Enables transmission of outgoing pause frames.
Step 2	`Router(config-if)# flowcontrol receive {desired | off | on}`	Enables the interface to receive incoming pause frames. The following options can be configured with this command: • **desired**—Allows, but does not require, the interface to receive incoming pause frames. • **off**—Does not allow incoming pause frames to enter the interface. • **on**—Allows incoming pause frames to enter the interface.

Note When a user configures flow control for either the transmit or receive direction, it is automatically enabled for both transmit and receive directions simultaneously.

Fast Ethernet SPAs have flow control enabled by default and it cannot be disabled.

Configuring EtherChannels

An EtherChannel bundles individual Ethernet links into a single logical link that provides the aggregate bandwidth of up to eight physical links.

Note EtherChannel is only supported on the 10-Port Gigabit Ethernet SPA and the 1-Port 10-Gigabit Ethernet SPA on the Cisco 7600 SIP-600. EtherChannel is not supported on the 2-Port Gigabit Ethernet SPA on the Cisco 7600 SIP-400 or on a Fast Ethernet SPA on the Cisco 7600 SIP-200.

For additional information on EtherChannels, see the "Configuring EtherChannels" section in the "Configuring Layer 3 and Layer 2 EtherChannel" chapter of the *Cisco IOS Software Configuration Guide, Release 12.2(33)SXH and Later Releases*.

Configuring H-VPLS

Hierarchal Virtual Private LAN Services (H-VPLS) use the provider core to join multiple attachment circuits together to simulate a virtual bridge that connects the multiple attachment circuits together. From a customer point of view, there is no topology for VPLS. All of the CE devices appear to connect to a logical bridge emulated by the provider core.

For more information on VPLS and H-VPLS feature, refer to the "Configuring Virtual Private LAN Service (VPLS)" section on page 4-23.

The H-VPLS feature works similarly on the Gigabit Ethernet SPAs as the OSM modules on the Cisco 7600 series router. For information about configuring VPLS and H-VPLS on the SIPs, refer to the "Virtual Private LAN Services on the Optical Services Modules" section of the *OSM Configuration Note* for the Cisco 7600 series router at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SR_OSM_config/mpls.html#wp1423607

Note H-VPLS is not available on Fast Ethernet SPAs.

H-VPLS Restrictions

In addition to the restrictions listed in the "Restrictions for VPLS" section in the *OSM Configuration Note* for the Cisco 7600 series router, the following restrictions apply to all transport types under H-VPLS:

- Split Horizon can be disabled, but should only be used for hub-and-spoke configurations.
- Hub-and-spoke and H-VPLS are supported.
- The Catalyst 6500 Series switch supports a maximum of 60 peer PEs and a maximum of 32,000 VCs.

Configuring Ethernet Operations, Administration, and Maintenance

In Cisco IOS Release 12.2(33)SXI and later releases, the Gigabit Ethernet SPAs support Operations, Administration, and Maintenance (OAM) as defined by IEEE 802.3ah, *Ethernet in the First Mile*. IEEE 802.3ah operates on a single point-to-point link between two devices using slow protocol packets called OAM protocol data units (OAMPDUs) that are never forwarded.

IEEE 802.3ah defines five functional areas, of which the Gigabit Ethernet SPAs on the Catalyst 6500 Series switch support the following three:

- OAM discovery—Supports identification of OAM support and capabilities on a peer device.
- Link monitoring—Provides event notification and link information. It also supports polling and response (but not writing) of the 802.3ah MIB.
- Remote failure indication—Supports informing a peer device that the receive path is down. This requires support of unidirectional operation on the link.

Ethernet OAM Configuration Guidelines

When configuring Ethernet OAM on the SPAs, consider the following guidelines:

- On Gigabit Ethernet links, the unidirectional fault signaling support in OAM and the autonegotiation capabilities of Gigabit Ethernet (IEEE 802.3z) are mutually exclusive. You must disable autonegotiation for OAM fault signaling to be sent over unidirectional links.
- Ethernet OAM requires point-to-point links where OAMPDUs are created and terminated.
- When configuring Ethernet OAM interface modes, consider the following guidelines:
  - At least one of the peer interfaces must be in active mode.
  - The peer interfaces either can be both in active mode, or one can be in active mode and the other in passive mode.
  - You can change Ethernet OAM modes without disabling OAM.
- When using templates to configure Ethernet OAM interfaces, consider the following guidelines:
  - If you use a template to configure common or global OAM characteristics and apply it to an interface, you can override any of the configuration statements in the template by configuring the same command at the interface with a different value.
  - You can define multiple templates to create different sets of link-monitoring characteristics.
  - You can only apply one template to any single Ethernet OAM interface.
- Table 10-1 provides information about where the OAM features for SPA interfaces are supported.

Table 10-1 Ethernet OAM Feature Compatibility by SIP and SPA Combination

Feature	Cisco 7600 SIP-200	Cisco 7600 SIP-400	Cisco 7600 SIP-600
• OAM discovery • Link monitoring • Remote failure indication (Dying Gasp only)	Not supported.	In Cisco IOS Release 12.2(33)SXI: • 2-Port Gigabit Ethernet SPA	In Cisco IOS Release 12.2(33)SXI: • 1-Port 10-Gigabit Ethernet SPA • 5-Port Gigabit Ethernet SPA • 10-Port Gigabit Ethernet SPA
Remote loopback	Not supported.	Not supported.	Not supported.
MIB variable retrieval	Not supported.	Not supported.	Not supported.

Ethernet OAM Configuration Tasks

The following sections describe the Ethernet OAM configuration tasks:

- Enabling OAM on an Interface, page 10-23 (required)
- Enabling and Disabling a Link-Monitoring Session, page 10-25 (optional)
- Starting and Stopping Link-Monitoring Operation, page 10-25 (optional)
- Configuring Link-Monitoring Options, page 10-26 (optional)
- Configuring Remote Failure Indication Actions, page 10-33 (optional)
- Configuring Global Ethernet OAM Options Using a Template, page 10-34 (optional)
- Verifying Ethernet OAM Configuration, page 10-35

Enabling OAM on an Interface

OAM is disabled on an interface by default. When you enable OAM on an interface, the interface automatically advertises to the remote peer that it supports link-monitoring during OAM discovery. Link-monitoring support must be agreed upon by the peer interfaces for monitoring to operate across the link.

Once link-monitoring support is achieved between the peer interfaces, the interface will start the link-monitoring operation, send event OAMPDUs when errors occur locally, and interpret event OAM PDUs received by the remote peer.

You do not need to explicitly configure link-monitoring support, or start the link-monitoring operation on the link unless you have previously disabled monitoring support or operation on the interface.

To enable OAM features on a Gigabit Ethernet interface, perform this task beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface` *type slot/subslot/port*	Specifies the Ethernet SPA interface, where: • *type*—Specifies the type of Ethernet interface, such as **gigabitethernet** or **tengigabitethernet**. • *slot/subslot/port*—Specifies the location of the interface. See the "Specifying the Interface Address on a SPA" section on page 10-4. **Note** Ethernet OAM can be defined on a main Gigabit Ethernet interface only, not on subinterfaces.
Step 2	`Router(config-if)# ethernet oam [max-rate` *oampdus* `| min-rate` *num-seconds* `| mode {active | passive} | timeout` *seconds*`]`	Enables OAM on a Gigabit Ethernet interface, where: • **max-rate** *oampdus*—(Optional) Specifies the maximum number of OAMPDUs that can be sent per second as an integer in the range of 1 to 10. The default is 10. • **min-rate** *num-seconds*—(Optional) Specifies the number of seconds (in the range 1–10) during which at least one OAMPDU must be sent. The default is 1 second. • **mode** {**active** | **passive**}—(Optional) Specifies the client mode for OAM discovery and link negotiation, where: – **active**— Specifies that the interface initiates OAMPDUs for protocol negotiation as soon as the interface becomes active. This is the default. At least one of the OAM peers must be configured in active mode. – **passive**—Specifies that the interface waits in a listening mode to receive an incoming OAMPDU for protocol negotiation from a peer. The passive interface begins sending OAMPDUs once it receives OAMPDUs from the peer.

Command	Purpose
	Note If you configure an interface in passive mode, then you must be sure that the peer is in active mode for successful OAM operation. • **timeout** *seconds*—Specifies the amount of time, in seconds (in the range 2–30), after which a device declares its OAM peer to be nonoperational and resets its state machine. The default is 5 seconds.

Enabling and Disabling a Link-Monitoring Session

The OAM peer interfaces must establish a link-monitoring session before the actual operation of link-monitoring can begin. If you have enabled OAM on the interface, and have not explicitly disabled link-monitoring support on the interface, then you do not need to explicitly configure link-monitoring support on the interface to establish a session.

The **ethernet oam link-monitor supported** command automatically runs in the background when you configure the **ethernet oam** interface configuration command. Be sure that at least one of the Ethernet OAM peers is configured for active mode so that a session can be established.

To explicitly configure and enable a link-monitoring session on an interface, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# ethernet oam link-monitor supported`	Enables link-monitoring support on an Ethernet OAM interface.

To disable a link-monitoring session on an interface, perform this task in interface configuration mode:

Command	Purpose
`Router(config-if)# no ethernet oam link-monitor supported`	Disables link-monitoring support on an Ethernet OAM interface.

Starting and Stopping Link-Monitoring Operation

If a link-monitoring session is established among the Ethernet OAM peer interfaces, then sending and receiving of Event Notification OAMPDUs can begin between the peers. This link-monitoring operation across the link automatically starts when you enable OAM on the interface.

The **ethernet oam link-monitor on** command automatically runs in the background when you configure the **ethernet oam** interface configuration command.

You can stop and restart the operation of link-monitoring (or the sending and receiving of Event Notification OAMPDUs on a link). Stopping a link-monitoring operation is not the same thing as disabling link-monitoring support. When you stop a link-monitoring operation, the interface is still configured to support link-monitoring with its peer, but just is not actively sending and receiving Event Notification OAMPDUs.

To explicitly configure and start a link-monitoring operation on an interface, perform this task in interface configuration mode:

Command	Purpose
`Router(config-if)# ethernet oam link-monitor on`	Starts link-monitoring on an Ethernet OAM interface.

To stop a link-monitoring operation on an interface, perform this task in interface configuration mode:

Command	Purpose
`Router(config-if)# no ethernet oam link-monitor on`	Stops link-monitoring on an Ethernet OAM interface.

Configuring Link-Monitoring Options

When OAM link-monitoring is active, Event Notification OAMPDUs are sent to a remote OAM client when errors are detected locally. You can configure certain windows and thresholds to define when these error event notifications are triggered. If you do not modify the link-monitoring options, default values are used for the window periods and low thresholds.

The Gigabit Ethernet SPAs support the following types of error events as defined by IEEE 802.3ah:

- Errored Symbol Period (errored symbols per second)—This event occurs when the number of symbol errors during a specified period exceeds a threshold. These are coding symbol errors (for example, a violation of 4B/5B coding).
- Errored Frame (errored frames per second)—This event occurs when the number of frame errors during a specified period exceeds a threshold.
- Errored Frame Period (errored frames per N frames)—This event occurs when the number of frame errors within the last N frames exceeds a threshold.
- Errored Frame Seconds Summary (errored seconds per M seconds)—This event occurs when the number of errored seconds (one second intervals with at least one frame error) within the last M seconds exceeds a threshold.

Cisco Systems adds the following types of vendor-specific error events:

- Receive CRC (errored frames per second)—This event occurs when the number of frames received with CRC errors during a specified period exceeds a threshold.
- Transmit CRC (errored frames per second)—This event occurs when the number of frames transmitted with CRC errors during a specified period exceeds a threshold.

The link-monitoring options can be configured in a global template that can be applied to one or more interfaces, and also can be explicitly configured at the interface.

Specifying Errored Symbol Period Link-Monitoring Options

The errored symbol period link-monitoring options include the ability to specify the number of symbols to be tracked or counted for errors, and the high and low thresholds for triggering the Errored Symbol Period Link Event.

To specify errored symbol period link-monitoring options, perform this task in interface configuration or template configuration mode:

Command	Purpose
`Router(config-if)# ethernet oam link-monitor symbol-period window` *million-symbol-units*	(Optional) Specifies the number of symbols (in the range 1–65535, as a multiple of 1 million symbols) to be included in the error counting according to the specified thresholds. The default window unit is 100, or 100 million symbols.
`Router(config-if)# ethernet oam link-monitor symbol-period threshold low` *low-symbols*	(Optional) Specifies the low errored symbol threshold as a number of symbol errors (in the range 0–65535). If the number of error symbols in the window period is equal to or greater than *low-symbols*, then the Errored Symbol Period Link Event will be generated. The default low threshold is 0 symbols.
`Router(config-if)# ethernet oam link-monitor symbol-period threshold high {none | high-symbols}`	(Optional) Specifies the high errored symbol threshold as a number of error symbols (in the range 1–65535). If the number of error symbols in the window period is equal to or greater than *high-symbols*, then a user defined action will be triggered. There is no default for the high threshold, so you must explicitly configure a value to enable it. For more information about configuring a user-defined action, see "Specifying a High-Threshold Action" section on page 10-32.

Specifying Errored Frame Link-Monitoring Options

The errored frame link-monitoring options include the ability to specify a period of time during which frame errors are tracked or counted, and the high and low thresholds for triggering the Errored Frame Link Event. The Gigabit Ethernet SPAs on the Catalyst 6500 Series switch count general frame errors, such as CRC errors and corrupted packets, as errored frames.

To specify errored frame link-monitoring options, perform this task in interface configuration or template configuration mode:

Command	Purpose
`Router(config-if)# ethernet oam link-monitor frame window` *100-millisecond-units*	(Optional) Specifies a period of time (in the range 10–600, as a multiple of 100 milliseconds) during which error-counting occurs according to the specified thresholds. The default window unit is 10, or 1000 milliseconds.

Command	Purpose
`Router(config-if)# ethernet oam link-monitor frame threshold low low-frames`	(Optional) Specifies the low error frame threshold as a number of frames (in the range 0–65535). If the number of error frames in the window period is equal to or greater than *low-frames*, then the Errored Frame Link Event will be generated. The default low threshold is 0 frame errors.
`Router(config-if)# ethernet oam link-monitor frame threshold high {none | high-frames}`	(Optional) Specifies the high error frame threshold as a number of error frames (in the range 1–65535). If the number of error frames in the window period is equal to or greater than *high-frames*, then a user-defined action will be triggered. There is no default for the high threshold, so you must explicitly configure a value to enable it. Use the **none** keyword to disable the high threshold. For more information about configuring a user-defined action, see "Specifying a High-Threshold Action" section on page 10-32.

Specifying Errored Frame Period Link-Monitoring Options

The errored frame period link-monitoring options include the ability to specify the number of error frames to be tracked or counted for errors, and the high and low thresholds for triggering the Errored Frame Period Link Event. The Gigabit Ethernet SPAs on the Catalyst 6500 Series switch count general frame errors, such as CRC errors and corrupted packets, as errored frames.

To specify errored frame period link-monitoring options, perform this task in interface configuration or template configuration mode:

Command	Purpose
`Router(config-if)# ethernet oam link-monitor frame-period window 10000-frame-units`	(Optional) Specifies the number of frames (in the range 1000–65535, as a multiple of 10000 frames) to be included in the error counting according to the specified thresholds. The default window unit is 1000, or 10000000 frames.

Command	Purpose
`Router(config-if)# ethernet oam link-monitor frame-period threshold low` *low-frames*	(Optional) Specifies the low error frame threshold as a number of frames (in the range 0–65535). If the number of error frames in the window period is equal to or greater than *low-frames*, then the Errored Frame Period Link Event will be generated. The default low threshold is 0 frame errors.
`Router(config-if)# ethernet oam link-monitor frame-period threshold high {none | high-frames}`	(Optional) Specifies the high error frame threshold as a number of frames (in the range 1–65535). If the number of error frames in the window period is equal to or greater than *high-frames*, a user defined action will be triggered. There is no default for the high threshold, so you must explicitly configure a value to enable it. Use the **none** keyword to disable the high threshold. For more information about configuring a user-defined action, see "Specifying a High-Threshold Action" section on page 10-32.

Specifying Errored Frame Seconds Summary Link-Monitoring Options

The errored frame seconds summary link-monitoring options include the ability to specify a period of time during which tracking of a number of errored-seconds periods (one-second intervals with at least one frame error) occurs, and the high and low thresholds for triggering the Errored Frames Seconds Summary Link Event.

To specify errored frame seconds summary link-monitoring options, perform this task in interface configuration or template configuration mode:

Command	Purpose
`Router(config-if)# ethernet oam link-monitor frame-seconds window` *100-millisecond-units*	(Optional) Specifies a period of time (in the range 100–9000, as a multiple of 100 milliseconds) during which tracking of an errored-seconds period occurs according to the specified thresholds. The default window unit is 100, or 10000 milliseconds.

Command	Purpose
`Router(config-if)# ethernet oam link-monitor frame-seconds threshold low` *low-errored-seconds*	(Optional) Specifies the low errored seconds threshold as a number of errored seconds (in the range 0–900). If the number of errored seconds in the window period is equal to or greater than *low-errored-seconds*, then the Errored Frame Seconds Summary Link Event will be generated. The default low threshold is 0 error seconds.
`Router(config-if)# ethernet oam link-monitor frame-seconds threshold high {none | high-errored-seconds}`	(Optional) Specifies the high errored seconds threshold as a number of errored seconds (in the range 1–900). If the number of errored seconds in the window period is equal to or greater than *high-errored-seconds*, then a user defined action will be triggered. There is no default for the high threshold, so you must explicitly configure a value to enable it. Use the **none** keyword to disable the high threshold. For more information about configuring a user-defined action, see "Specifying a High-Threshold Action" section on page 10-32.

Specifying Receive CRC Link-Monitoring Options

The receive CRC link-monitoring options include the ability to specify a period of time during which tracking of frames received with CRC occurs, and the high and low thresholds for triggering the error. Receive CRC link-monitoring is a Cisco-specific implementation and is only locally significant to the Ethernet OAM interface on the Catalyst 6500 Series switch.

To specify receive CRC link-monitoring options, perform this task in interface configuration or template configuration mode:

Command	Purpose
`Router(config-if)# ethernet oam link-monitor receive-crc window` *100-millisecond-units*	(Optional) Specifies a period of time (in the range 10–1800, as a multiple of 100 milliseconds) during which tracking of frames received with CRC errors occurs according to the specified thresholds. The default window unit is 10, or 1000 milliseconds.

Command	Purpose
`Router(config-if)# ethernet oam link-monitor receive-crc threshold low low-frames`	(Optional) Specifies the low CRC threshold as a number of frames (in the range 0–65535). If the number of frames received with CRC errors in the window period is equal to or greater than *low-frames*, then the Receive CRC error will be generated. The default low threshold is 1 frame.
`Router(config-if)# ethernet oam link-monitor receive-crc threshold high {none | high-frames}`	(Optional) Specifies the high CRC threshold as a number of frames (in the range 1–65535). If the number of frames received with CRC errors in the window period is equal to or greater than *high-frames*, a user-defined action will be triggered. There is no default for the high threshold, so you must explicitly configure a value to enable it. Use the **none** keyword to disable the high threshold. For more information about configuring a user-defined action, see "Specifying a High-Threshold Action" section on page 10-32.

Specifying Transmit CRC Link-Monitoring Options

The transmit CRC link-monitoring options include the ability to specify a period of time during which tracking of frames transmitted with CRC occurs, and the high and low thresholds for triggering the error. Transmit CRC link-monitoring is a Cisco-specific error event and is only locally significant to the Ethernet OAM interface on the Catalyst 6500 Series switch.

To specify transmit CRC link-monitoring options, perform this task in interface configuration or template configuration mode:

Command	Purpose
`Router(config-if)# ethernet oam link-monitor transmit-crc window 100-millisecond-units`	(Optional) Specifies a period of time (in the range 10–1800, as a multiple of 100 milliseconds) during which tracking of frames received with CRC errors occurs according to the specified thresholds. The default window unit is 10, or 1000 milliseconds.

Command	Purpose
`Router(config-if)# ethernet oam link-monitor transmit-crc threshold low` *low-frames*	(Optional) Specifies the low CRC threshold as a number of frames (in the range 0–65535). If the number of frames transmitted with CRC errors in the window period is equal to or greater than *low-frames*, then the Receive CRC error will be generated. The default low threshold is 1 frame.
`Router(config-if)# ethernet oam link-monitor transmit-crc threshold high {none | high-frames}`	(Optional) Specifies the high CRC threshold as a number of frames (in the range 1–65535). If the number of frames transmitted with CRC errors in the window period is equal to or greater than *high-frames*, a user defined action will be triggered. There is no default for the high threshold, so you must explicitly configure a value to enable it. Use the **none** keyword to disable the high threshold. For more information about configuring a user-defined action, see "Specifying a High-Threshold Action" section on page 10-32.

Specifying a High-Threshold Action

When you configure high thresholds for OAM link-monitoring, you can specify an action to be taken when the high threshold is exceeded.

When configuring high-threshold actions, consider the following guidelines:

- There is no default action.
- If you configure a high threshold but do not configure any corresponding action, only a message appears on the syslog and no other action is taken on the interface.
- If you want to associate different high-threshold actions for different kinds of link-monitoring functions, you can use configuration templates. However, only one configuration template can be applied to any Ethernet OAM interface.
- Only one high-threshold action can be configured for any Ethernet OAM interface.

To configure an action when a high threshold for an error is exceeded on an Ethernet OAM interface, use the following command in interface configuration or template configuration mode:

Command	Purpose
`Router(config-if)# ethernet oam link-monitor high-threshold action {error-disable-interface | failover}`	(Optional) Configures the action when a high-threshold error is exceeded, where: • **error-disable-interface**—Shuts down the Ethernet OAM interface. • **failover**—(EtherChannel interface only) Configures the interface for an automatic failover of traffic from one port in an EtherChannel to another port in the same EtherChannel when one of the ports in the channel exceeds the high error threshold within the specified interval. The port failover only occurs if there is at least one operational port available in the EtherChannel. The failed port will be put into an error disable state. If the failed port is the last port in the EtherChannel, the port will not be put into an error disable state and continues to pass traffic regardless of the type of errors being received. Single, nonchanneling ports go into the error disable state when the error threshold is exceeded within the specified interval.

Configuring Remote Failure Indication Actions

When an RFI event occurs locally, the local client sends an Information OAMPDU to its peer with a bit selected that indicates the type of failure. The Gigabit Ethernet SPAs on the Catalyst 6500 Series switch process all of the following types of Remote Failure Indication (RFI) conditions as defined by IEEE 802.3ah:

- Critical Event—This type of RFI is sent when an unspecified critical event has occurred. These events are vendor specific, and the failure indication might be sent immediately and continuously.
- Dying Gasp—This type of RFI is sent when an unrecoverable condition (for example, a power failure) has occurred. The conditions for a Dying Gasp RFI are vendor specific, and the failure indication might be sent immediately and continuously. The Gigabit Ethernet SPAs on the Catalyst 6500 Series switch generate a Dying Gasp RFI when an interface is error-disabled or administratively shut down. This is the only type of RFI that the Gigabit Ethernet SPAs on the Catalyst 6500 Series switch generate.
- Link Fault—This type of RFI is sent when a loss of signal is detected by the receiver (for example, a peer's laser is malfunctioning). A link fault is sent once per second in the Information OAMPDU. The link fault RFI applies only when the physical sublayer is capable of independent transmit and receive.

When the Gigabit Ethernet SPAs receive an OAMPDU with an RFI bit selected, a syslog message is created providing the failure reason, as shown in the following example:

```
%ETHERNET_OAM-SP-6-RFI: The client on interface Gi1/1 has received a remote failure
indication from its remote peer (failure reason = remote client administratively turned
off)
```

You can configure a response, or action, by the local client to shut down the OAM interface when it receives Information OAMPDUs with a Dying Gasp RFI bit selected.

To configure an error disable action for the local Ethernet OAM interface, use the following command in interface configuration or template configuration mode:

Command	Purpose
`Router(config-if)# ethernet oam remote-failure dying-gasp action error-disable-interface`	(Optional) Specifies that the local Ethernet OAM interface is shut down upon receipt of an Information OAMPDU from its peer that indicates a Dying Gasp.

Configuring Global Ethernet OAM Options Using a Template

Create configuration templates when you have a common set of link-monitoring or remote-failure characteristics that you want to apply to multiple Ethernet OAM interfaces. Templates simplify Ethernet OAM interface configuration.

Although you can configure multiple configuration templates, only one template can be associated with any single Ethernet OAM interface. You can override any commands defined within a template by explicitly configuring the same command (that is predefined by the template) in interface configuration mode.

To configure global Ethernet OAM interface options using a template, use the following command beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# template` *template-name*	Creates or selects a template and enters template configuration mode, where *template-name* is an up to 32-character string defining the name of the template.
Step 2	`Router(config-template)# ethernet oam link-monitor` *command* or `Router(config-template)# ethernet oam remote-failure` *command*	Specify one or more **ethernet oam** configuration commands. Repeat this step for the number of commands that you want to configure. For information about link-monitoring commands, see the "Configuring Link-Monitoring Options" section on page 10-26.
Step 3	`Router(config-template)# exit`	Exit template configuration mode and return to global configuration mode.

	Command	Purpose
Step 4	`Router(config)# interface type slot/subslot/port`	Specifies the Ethernet SPA interface, where: • *type*—Specifies the type of Ethernet interface, such as **gigabitethernet** or **tengigabitethernet**. • *slot*/*subslot*/*port*—Specifies the location of the interface. See the "Specifying the Interface Address on a SPA" section on page 10-4. **Note** Ethernet OAM only can be defined on a main Gigabit Ethernet interface, not on subinterfaces.
Step 5	`Router(config-if)# source template template-name`	Attaches the template called *template-name* and applies the set of configuration commands defined by the named template to the specified interface.

Verifying Ethernet OAM Configuration

To verify the Ethernet OAM configuration, perform this task in privileged EXEC configuration mode:

Command	Purpose
`Router# show ethernet oam discovery [interface type slot/subslot/port]`	Displays information about OAM functions negotiated during the OAM discovery phase of establishing an OAM session, where: • *type*—Specifies the type of Ethernet interface, such as **gigabitethernet** or **tengigabitethernet**. • *slot*/*subslot*/*port*—Specifies the location of the interface. See the "Specifying the Interface Address on a SPA" section on page 10-4.
`Router# show ethernet oam statistics [interface type slot/subslot/port]`	Displays statistics for information OAMPDUs and local and remote faults, where: • *type*—Specifies the type of Ethernet interface, such as **gigabitethernet** or **tengigabitethernet**. • *slot*/*subslot*/*port*—Specifies the location of the interface. See the "Specifying the Interface Address on a SPA" section on page 10-4.

Command	Purpose
`Router# show ethernet oam status [interface type slot/subslot/port]`	Displays information about the link-monitoring configuration and status on the local OAM client, where: • *type*—Specifies the type of Ethernet interface, such as **gigabitethernet** or **tengigabitethernet**. • *slot*/*subslot*/*port*—Specifies the location of the interface. See the "Specifying the Interface Address on a SPA" section on page 10-4.
`Router# show ethernet oam summary`	Displays information about the OAM session with the remote OAM client, where: • *type*—Specifies the type of Ethernet interface, such as **gigabitethernet** or **tengigabitethernet**. • *slot*/*subslot*/*port*—Specifies the location of the interface. See the "Specifying the Interface Address on a SPA" section on page 10-4.

This section includes the following topics:

Verifying an OAM Session

To verify an OAM session, use the **show ethernet oam summary** command.

The following example shows that the local OAM client is established on the second Gigabit Ethernet SPA interface (1) located in subslot 1 of the SIP installed in chassis slot 6 of the Catalyst 6500 Series switch (Gi6/1/1).

The local client interface is in session with a remote client with MAC address 0012.7fa6.a700 and organizationally unique identifier (OUI) 00000C, which is the OUI for Cisco Systems. The remote client is in active mode, and has established capabilities for link-monitoring and remote loopback for the OAM session.

```
Router# show ethernet oam summary
Symbols:          * - Master Loopback State,  # - Slave Loopback State
Capability codes: L - Link Monitor,  R - Remote Loopback
                  U - Unidirection,  V - Variable Retrieval

  Local                         Remote
Interface       MAC Address     OUI     Mode    Capability

  Gi6/1/1       0012.7fa6.a700 00000C active   L R
```

Verifying OAM Discovery Status

To verify OAM Discovery status on the local client and remote peer, use the **show ethernet oam discovery** command as shown in the following example:

```
Router# show ethernet oam discovery interface gigabitethernet6/1/1

GigabitEthernet6/1/1
```

```
Local client
------------
  Administrative configurations:
    Mode:              active
    Unidirection:      not supported
    Link monitor:      supported (on)
    Remote loopback:   not supported
    MIB retrieval:     not supported
    Mtu size:          1500

  Operational status:
Port status:       operational
    Loopback status:   no loopback
    PDU permission:    any
    PDU revision:      1

Remote client
-------------
  MAC address: 0030.96fd.6bfa
  Vendor(oui): 0x00 0x00 0x0C (cisco)

  Administrative configurations:
    Mode:              active
    Unidirection:      not supported
    Link monitor:      supported
    Remote loopback:   not supported
    MIB retrieval:     not supported
    Mtu size:          1500
```

Verifying Information OAMPDU and Fault Statistics

To verify statistics for information OAMPDUs and local and remote faults, use the **show ethernet oam statistics** command as shown in the following example:

```
Router# show ethernet oam statistics interface gigabitethernet6/1/1

GigabitEthernet6/1/1
Counters:
---------
Information OAMPDU Tx                   : 588806
  Information OAMPDU Rx                   : 988
  Unique Event Notification OAMPDU Tx     : 0
  Unique Event Notification OAMPDU Rx     : 0
  Duplicate Event Notification OAMPDU TX  : 0
  Duplicate Event Notification OAMPDU RX  : 0
  Loopback Control OAMPDU Tx              : 1
  Loopback Control OAMPDU Rx              : 0
  Variable Request OAMPDU Tx              : 0
  Variable Request OAMPDU Rx              : 0
  Variable Response OAMPDU Tx             : 0
  Variable Response OAMPDU Rx             : 0
  Cisco OAMPDU Tx                         : 4
  Cisco OAMPDU Rx                         : 0
  Unsupported OAMPDU Tx                   : 0
  Unsupported OAMPDU Rx                   : 0
  Frames Lost due to OAM                  : 0

Local Faults:
-------------
  0 Link Fault records
  2 Dying Gasp records
    Total dying gasps       : 4
    Time stamp              : 00:30:39
```

```
    Total dying gasps       : 3
    Time stamp              : 00:32:39

  0 Critical Event records

Remote Faults:
--------------
  0 Link Fault records
  0 Dying Gasp records
  0 Critical Event records

Local event logs:
-----------------
  0 Errored Symbol Period records
  0 Errored Frame records
  0 Errored Frame Period records
  0 Errored Frame Second records

Remote event logs:
------------------
  0 Errored Symbol Period records
  0 Errored Frame records
  0 Errored Frame Period records
  0 Errored Frame Second records
```

Verifying Link-Monitoring Configuration and Status

To verify link-monitoring configuration and status on the local client, use the **show ethernet oam status** command. The highlighted "Status" field in the following example shows that link-monitoring status is supported and enabled (on).

```
Router# show ethernet oam status interface gigabitethernet6/1/1

GigabitEthernet6/1/1
General
-------
  Mode:                  active
  PDU max rate:          10 packets per second
  PDU min rate:          1 packet per 1 second
  Link timeout:          5 seconds
  High threshold action: no action

Link Monitoring
---------------
  Status: supported (on)

  Symbol Period Error
    Window:              1 million symbols
    Low threshold:       1 error symbol(s)
    High threshold:      none

  Frame Error
    Window:              10 x 100 milliseconds
    Low threshold:       1 error frame(s)
    High threshold:      none
Frame Period Error
    Window:              1 x 100,000 frames
    Low threshold:       1 error frame(s)
    High threshold:      none

  Frame Seconds Error
    Window:              600 x 100 milliseconds
    Low threshold:       1 error second(s)
    High threshold:      none
```

Verifying Status of the Remote OAM Client

To verify the status of a remote OAM client, use the **show ethernet oam summary** and **show ethernet oam status** commands.

To verify the remote client mode and capabilities for the OAM session, use the **show ethernet oam summary** command and observe the values in the Mode and Capability fields. The following example shows that the local client (local interface Gi6/1/1) is connected to the remote client:

```
Router# show ethernet oam summary
Symbols:          * - Master Loopback State,  # - Slave Loopback State
Capability codes: L - Link Monitor,  R - Remote Loopback
                  U - Unidirection,  V - Variable Retrieval

  Local                         Remote
Interface       MAC Address     OUI     Mode    Capability

  Gi6/1/1       0012.7fa6.a700 00000C active   L R
```

Configuring QoS Features on Ethernet SPAs

For information about the QoS features supported by the Ethernet SPAs, see the "Configuring QoS Features on a SIP" section on page 4-33 of Chapter 4, "Configuring the SIPs and SSC."

QoS Configuration Guidelines for the Ethernet SPA

For Fast Ethernet SPAs and the 2-Port Gigabit Ethernet SPA, the following QoS behavior applies:

- In both the ingress and egress directions, all QoS features calculate packet size similarly to how packet size calculation is performed by the FlexWAN and Enhanced FlexWAN modules on the Catalyst 6500 Series switch.
- Specifically, all features consider the IEEE 802.3 Layer-2 headers and the Layer-3 protocol payload. The CRC, interframe gap, and preamble are not included in the packet size calculations.

Note For Fast Ethernet SPAs, QoS cannot change the speed of an interface (for example, Fast Ethernet SPAs cannot change QoS settings whenever an interface speed is changed between 100 Mbps to 10 Mbps). When the speed is changed, the user must also adjust the QoS setting accordingly.

Saving the Configuration

To save your running configuration to nonvolatile random-access memory (NVRAM), perform this task in privileged EXEC configuration mode:

Command	Purpose
`Router# copy running-config startup-config`	Writes the new configuration to NVRAM.

For information about managing your system image and configuration files, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2* and *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* publications.

Shutting Down and Restarting an Interface on a SPA

You can shut down and restart any of the interface ports on a SPA independently of each other. Shutting down an interface stops traffic and enters the interface into an administratively down state.

There are no restrictions for online insertion and removal (OIR) on Fast Ethernet or Gigabit Ethernet SPAs. Fast Ethernet and Gigabit Ethernet SPAs can be removed from a SIP at any time. SIPs populated with any type of SPAs can be removed from the switch at any time.

If you are preparing for an OIR of a SPA, you do not need to independently shut down each of the interfaces prior to deactivation of the SPA. The **hw-module subslot shutdown** command automatically stops traffic on the interfaces and deactivates them along with the SPA in preparation for OIR.

You also do not need to independently restart any interfaces on a SPA after OIR of a SPA or SIP.

To shut down an interface on a SPA, perform this task in interface configuration mode:

Command	Purpose
`Router(config-if)# shutdown`	Disables an interface.

To restart an interface on a SPA, perform this task in interface configuration mode:

Command	Purpose
`Router(config-if)# no shutdown`	Restarts a disabled interface.

Verifying the Interface Configuration

In addition to using the **show running-configuration** command to display your switch configuration settings, you can use the **show interfaces gigabitethernet** command to get detailed information on a per-port basis for your Gigabit Ethernet SPAs, and use the **show interfaces fastethernet** command to get detailed information on a per-port basis for your Fast Ethernet SPAs.

Verifying Per-Port Interface Status

To find detailed interface information on a per-port basis for the Fast Ethernet and Gigabit Ethernet SPAs, use the **show interfaces fastethernet** and **show interfaces gigabitethernet** commands, respectively. For a description of the command output, see the *Catalyst 6500 Series Cisco IOS Command Reference, Release 12.2SX*.

The following example provides sample output for interface port 1 on the SPA located in the top subslot (0) of the SIP that is installed in slot 2 of the Catalyst 6500 Series switch:

```
Router# show interfaces gigabitethernet 2/0/1
GigabitEthernet2/0/1 is down, line protocol is down
  Hardware is GigEther SPA, address is 000a.f330.2e40 (bia 000a.f330.2e40)
  Internet address is 2.2.2.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full-duplex, 1000Mb/s, link type is force-up, media type is SX
  output flow-control is on, input flow-control is on
```

```
ARP type: ARPA, ARP Timeout 04:00:00
Last input 03:18:49, output 03:18:44, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   1703 packets input, 638959 bytes, 0 no buffer
   Received 23 broadcasts (0 IP multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog, 1670 multicast, 0 pause input
   1715 packets output, 656528 bytes, 0 underruns
   0 output errors, 0 collisions, 4 interface resets
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier, 0 PAUSE output
   0 output buffer failures, 0 output buffers swapped out
```

Configuration Examples

This section includes the following configuration examples:

Basic Interface Configuration Example

The following example shows how to enter global configuration mode to specify the interface that you want to configure, configure an IP address for the interface, and save the configuration. This example configures interface port 1 on the SPA that is located in subslot 0 of the SIP, that is installed in slot 3 of the Catalyst 6500 Series switch:

```
!Enter global configuration mode
!
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
!
! Specify the interface address
!
Router(config)# interface gigabitethernet 3/0/1
!
! Configure an IP address
!
Router(config-if)# ip address 192.168.50.1 255.255.255.0
!
! Start the interface
!
Router(config-if)# no shutdown
!
! Save the configuration to NVRAM
!
Router(config-if)# exit
Router# copy running-config startup-config
```

MAC Address Configuration Example

The following example changes the default MAC address on the interface to 1111.2222.3333:

```
!Enter global configuration mode
!
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
!
! Specify the interface address
!
Router(config)# interface gigabitethernet 3/0/1
!
! Modify the MAC address
!
Router(config-if)# mac-address 1111.2222.3333
```

MTU Configuration Example

The following example sets the interface MTU to 9216 bytes:

Note The SPA automatically adds an additional 38 bytes to the configured interface MTU size.

```
!Enter global configuration mode
!
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
!
! Specify the interface address
!
Router(config)# interface gigabitethernet 3/0/1
!
! Configure the interface MTU
!
Router(config-if)# mtu 9216
```

VLAN Configuration Example

The following example creates subinterface number 268 on SPA interface port 2 (the third port), and configures the subinterface on the VLAN with ID number 268 using IEEE 802.1Q encapsulation:

Note The SPA does not support ISL encapsulation.

```
!Enter global configuration mode
!
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
!
! Specify the interface address
!
Router(config)# interface gigabitethernet 3/0/1.268
!
! Configure dot1q encapsulation and specify the VLAN ID
!
Router(config-subif)# encapsulation dot1q 268
```

MPLSoGRE and mVPNoGRE Configuration Example

The following example shows how to configure the MPLSoGRE and mVPNoGRE feature on a Cisco 7600 SIP-400 interface or subinterface; however, this example uses a Cisco 7600 SIP-400 interface that does *not* support subinterfaces:

```
! Enter global configuration mode.
!
Router# configure terminal
! Enter configuration commands, one per line. End with CNTL/Z.
!
! Specify the Gigabit Ethernet interface to configure.
!
Router(config)# interface gigabitethernet 2/0/0
! Attach a GRE Tunnel to a Cisco 7600 SIP-400 subinterface.
!
Router(config-if)# tunnel-interface tu1
! Define the IP traffic that should be tunneled.
!
Router(config-if-ti)# ip route 10.0.0.1 255.255.255.0
Router(config-if-ti)# exit
```

When **tunnel-interface** is configured on the Cisco 7600 SIP-400 interface or subinterface, **ip pim sparse-mode** and **tag-switching ip** are automatically added to the interface. A static route to IP address contained on the **ip route** command is internally created. The following example shows the output of the **show running interface** command after adding or configuring **tunnel-interface**; however, this example uses a Cisco 7600 SIP-400 interface that does *not* support subinterfaces:

```
Router# show running interface gigabitethernet 2/0/0
!
interface gigabitethernet2/0/0
 ip address 10.1.0.1 255.255.255.0
 ip pim sparse-mode
 no keepalive
 tunnel-interface Tunnel1
    ip route 10.11.0.1 255.255.255.0
```

```
   exit-tunnel-interface
 tag-switching ip
 clock source internal
end
```

Note You do not need to configure a static route (globally or on the tunnel) to the BGP neighbor on the Catalyst 6500 Series switch. This is automatically done by the **ip route** command under the **tunnel-interface** command on the Cisco 7600 SIP-400 interface or subinterface.

The following example illustrates the tunnel interface configuration on the Catalyst 6500 Series switch:

```
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip pim sparse-dense-mode
 mpls ip
 tunnel source 22.22.22.22
 tunnel destination 44.44.44.44
```

EoMPLS Configuration Example

The following example shows how to configure software-based EoMPLS:

```
! Enter global configuration mode.
!
Router# configure terminal
! Enter configuration commands, one per line. End with CNTL/Z.
Router# vlan 101
!
Router(config)# interface VLAN101
Router(config-if)# xconnect 7.7.7.7 73829 encapsulation MPLS
!
Router(config)# interface gigabitethernet 4/1/0.1
Router(config-subif)# encapsulation dot1Q 100
```

The following example shows the commands to configure Scalable EoMPLS (only for a Cisco 7600 SIP-400 Ethernet interface):

```
Router(config)# interface GigabitEthernet 1/2/1
Router(config-if)# no ip address
Router(config-if)# no cdp enable
!
Router(config-if)# interface GigabitEthernet 1/2/1.2
Router(config-subif)# encapsulation dot1Q 2
Router(config-subif)# xconnect 5.5.5.5 20002 encapsulation mpls
!
[Snip ...]
!
Router(config-if)# interface GigabitEthernet 1/2/1.4095
Router(config-subif)# encapsulation dot1Q 4095
Router(config-subif)# xconnect 5.5.5.5 24095 encapsulation mpls
```

The following example shows how to configure hardware EoMPLS (other Ethernet interfaces):

```
Router(config)# interface GigabitEthernet 1/1
Router(config-if)# no ip address
Router(config-if)# no cdp enable
!
Router(config-subif)# interface GigabitEthernet 1/1.2
```

```
Router(config-subif)# encapsulation dot1Q 2
Router(config-subif)# xconnect 5.5.5.5 10002 encapsulation mpls
!
[Snip ...]
Router(config)# interface GigabitEthernet 1/1.3095
Router(config-subif)# encapsulation dot1Q 3095
Router(config-subif)# xconnect 5.5.5.5 13095 encapsulation mpls
!
```

Changing the Speed of a Fast Ethernet SPA Configuration Example

The following example shows how to change the speed of a Fast Ethernet SPA:

Note In order to change the speed of a Fast Ethernet SPA, you must disable autonegotiation.

```
Router# show run interface fastethernet 5/0/1
Building configuration...
Current configuration : 86 bytes
!
! Disable Autonegotiation
!
interface FastEthernet5/0/1
ip address 10.1.0.2 255.255.0.0
negotiation auto
end
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/0/1
Router(config-if)# no negotiation auto
Router(config-if)# speed 10
Router(config-if)# end
Router# show run interface fastethernet 5/01
Building configuration...
Current configuration : 112 bytes
!
interface FastEthernet 5/0/1
ip address 10.1.0.2 255.255.0.0
speed 10
duplex full
no negotiation auto
end
Router# show interface fastethernet 5/0/1
FastEthernet5/0/1 is up, line protocol is up
Hardware is FastEthernet SPA, address is 000a.8b3e.cc00 (bia 000a.8b3e.cc00)
Internet address is 10.1.0.2/16
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not supported
Full-duplex, 10Mb/s
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:04, output 00:00:04, output hang never
Last clearing of "show interface" counters 1d00h
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
```

```
1608 packets input, 547102 bytes, 0 no buffer
Received 1 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog
0 input packets with dribble condition detected
1606 packets output, 548403 bytes, 0 underruns

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 5/0/1
Router(config-if)# speed 100
Router(config-if)# end
Router#
*Apr 25 21:10:36: %SYS-5-CONFIG_I: Configured from console by console
Router# show interface fastethernet 5/0/1
FastEthernet5/0/1 is down, line protocol is down
Hardware is FastEthernet SPA, address is 000a.8b3e.cc00 (bia 000a.8b3e.cc00)
Internet address is 10.1.0.2/16
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not supported
Full-duplex, 100Mb/s
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:23, output 00:00:22, output hang never
Last clearing of "show interface" counters 1d00h
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1608 packets input, 547102 bytes, 0 no buffer
Received 1 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
```