Configuring the OC-3c/STM-1, OC-12c/STM-4, and OC-48c/STM-16 SONET/SDH Optical Services Modules

This chapter describes the OC-3c/STM-1, OC-12c/STM-4, and OC-48c/STM-16 Packet over Synchronous Optical Network (SONET) (POS)/synchronous digital hierarchy (SDH) Optical Services Modules (OSMs).

This chapter consists of these sections:

Supported Features

These sections list the standard Cisco IOS POS and SDH features supported on the OC-3c/STM-1, OC-12c/STM-4, and OC-48c/STM-16 POS/SDH OSMs:

SONET/SDH Compliance

This section lists the SONET/SDH Compliance features:

- Bellcore GR-253-CORE
- ITU-T G.707, G.783, G.957, G.958
- 1+1 SONET Automatic Protection Switching (APS) as per G.783 Annex A
- 1+1 SDH Multiplex Section Protection (MSP) as per G.783 Annex A
- APS Reflector Mode

SONET/SDH Error, Alarm, and Performance Monitoring

This section lists supported SONET/SDH error, alarms, and performance monitoring:

- Signal failure bit error rate (SF-ber)
- Signal degrade bit error rate (SD-ber)
- Signal label payload construction (C2)
- Path trace byte (J1)
- Section:
  - Loss of signal (LOS)
  - Loss of frame (LOF)
  - Error counts for B1
  - Threshold crossing alarms (TCA) for B1
- Line:
  - Line alarm indication signal (LAIS)
  - Line remote defect indication (LRDI)
  - Line remote error indication (LREI)
  - Error counts for B2
  - Threshold crossing alarms (TCA) for B2
- Path:
  - Path alarm indication signal (PAIS)
  - Path remote defect indication (PRDI)
  - Path remote error indication (PREI)
  - Error counts for B3
  - Threshold crossing alarms (TCA) for B3
  - Loss of pointer (LOP)
  - New pointer events (NEWPTR)
  - Positive stuffing event (PSE)
  - Negative stuffing event (NSE)

SONET/SDH Synchronization

This section lists supported SONET/SDH synchronization:

- Local (internal) timing (for inter-router connections over dark fiber or WDM equipment)
- Loop (line) timing (for connecting to SONET/SDH equipment)
- +/- 20 ppm clock accuracy over full operating temperature

WAN Protocols

This section lists the supported WAN protocols:

- IETF RFC 1661, Point-to-Point Protocol (PPP)
- IETF RFC 1662, PPP in HDLC framing
- IETF RFC 2615, PPP over SONET/SDH with $1+x^{43}$ self-synchronous payload scrambling
- Cisco Protect Group Protocol over UDP/IP (Port 172) for APS and MSP
- Multiprotocol Label Switching (MPLS)

Note The 2-port OC-48c/STM-16 POS/DPT OSMs does support MPLS but does not support EoMPLS.

- Ethernet over Multiprotocol Label Switching (EoMPLS)
- Frame Relay

  Configure the POS interfaces for Frame Relay as described in the *Cisco IOS Wide-Area Networking Configuration Guide,* Release 12.1 under “Configuring Frame Relay” and in the *Cisco IOS Wide-Area Networking Command Reference,* Release 12.1 at these URLs:

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

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

  Configure traffic shaping for Frame Relay as described in the *Cisco IOS Quality of Service*

  Solutions Configuration Guide under “Configuring Distributed Traffic Shaping” at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt4/qcfdts.htm

  See the “Configuring Frame Relay and Frame Relay Traffic Shaping” section on page 3-17 for information about platform-specific configurations, commands, and limitations.

Note The 2-port OC-48c/STM-16 POS/DPT OSMs do not support Frame Relay.

Dynamic Packet Transport Protocol

The 2-port OC-48c/STM-16 POS/DPT OSMs (OSM-2OC48/1DPT) support these Dynamic Packet Transport (DPT) protocol features:

- DPT Spatial Reuse Protocol (SRP) MAC
- DPT SRP fairness algorithm (SRP-fa)
- DPT SRP intelligent protection switching (IPS)
- SRR (single ring recovery)

Bridging Control Protocol

Bridging Control Protocol (BCP) enables forwarding of Ethernet frames over SONET networks and provides a high-speed extension of enterprise LAN backbone traffic through a metropolitan area. The implementation of BCP on the OSMs includes support for IEEE 802.1D, IEEE 802.1Q Virtual LAN (VLAN), and high-speed switched LANs.

The following OSMs support BCP as defined in RFC 3518:

- OC-3 POS:
  - OSM-4OC3-POS-SI
  - OSM-4OC3-POS-SI+
  - OSM-8OC3-POS-SI, -SL
  - OSM-8OC3-POS-SI+, -SL+
  - OSM-16OC3-POS-SI, -SL
  - OSM-16OC3-POS-SI+
- OC-12 POS:
  - OSM-2OC12-POS-MM, -SI, -SL
  - OSM-2OC12-POS-MM+, -SI+
  - OSM-4OC12-POS-MM, -SI, -SL
  - OSM-4OC12-POS-SI+
- OC-48 POS:
  - OSM-1OC48-POS-SS, -SI, -SL
  - OSM-1OC48-POS-SS+, -SI+, -SL+
  - OSM-2OC48-POS/DPT-SS, -SI, -SL

Note For interoperability purposes, keep in mind that OSM POS interfaces with BCP configured can forward both Layer 2 and Layer 3 traffic at the same time, while POS interfaces on other Cisco platforms support only Layer 2 forwarding when BCP is enabled.

Figure 3-1 shows a topology where BCP is used to allow transparent forwarding of VLAN traffic over a SONET network.

Figure 3-1 BCP Topology in a SONET Network

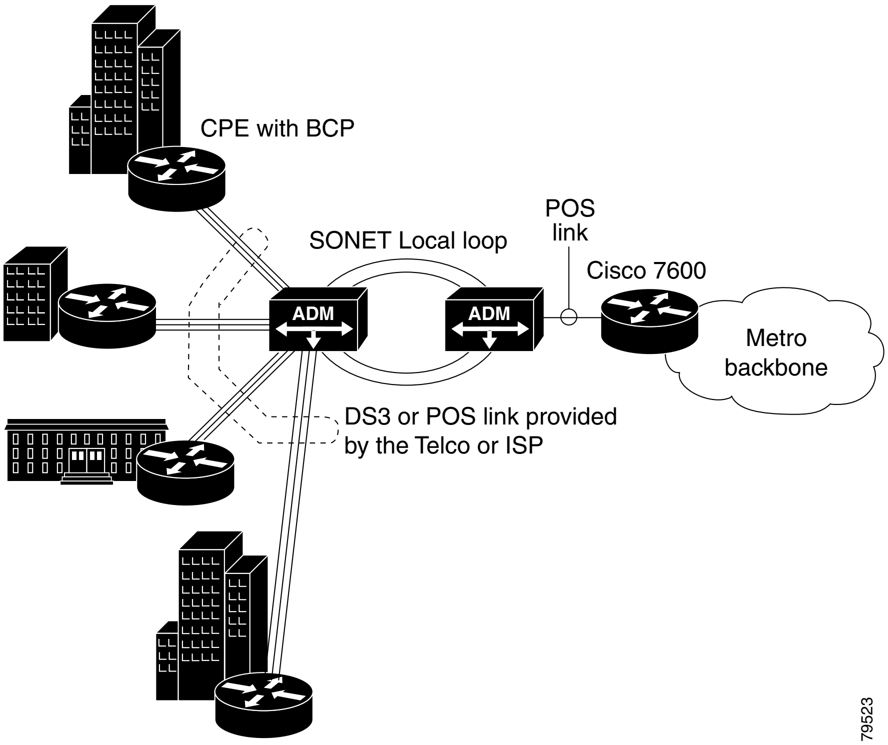
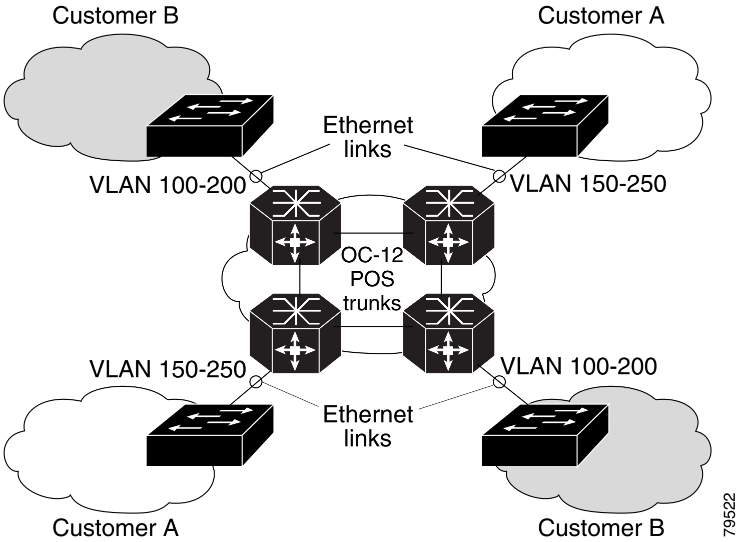


Figure 3-2 shows a topology where VLAN IDs are used to create VPNs for different customers and BCP is used to forward the VPN traffic over a SONET network.

Figure 3-2 BCP Topology in a VPN Network



For information on configuring BCP, see the "Configuring Bridging Control Protocol" section on page 3-22.

Quality of Service Support with BCP

Quality of Service (QoS) is supported on BCP links using the three experimental bits in a label to determine the priority of packets. To support QoS between LERs, you set the experimental bits in both the VC and tunnel labels. The experimental bits need to be set in the VC label because the tunnel label is popped at the penultimate router.

Routing and Scalability Protocols

This section lists the supported routing and scalability protocols:

- Distributed Cisco Express Forwarding (dCEF)
- WCCP v2
- With the Policy Feature Card 2 (PFC2) only, GRE encapsulated tunneling (supported in software)

Note Generic routing encapsulation (GRE) tunnel IP source and destination VRF membership is not supported with the **tunnel vrf** command.

Network Management

This section lists the supported network management features:

- Local (diagnostic) loopback
- Network loopback
- NetFlow Data Export
- IP over the Data Communications Channel (DCC)

Note The 2-port OC-48c/STM-16 POS/SDH OSMs do not support DCC.

- RFC 1595 performance statistics for timed intervals (current, 15 minute, multiple 15 minute, and 1-day intervals):
  - Regenerator section
  - Multiplex section
  - Path errored seconds
  - Severely errored seconds
  - Severely errored framed seconds

Quality of Service Protocols

This section lists the supported QoS features:

- 2,048 QoS queues per module (32 service classes and 64 DSCP queues/class)
- Class-based traffic shaping
- Differentiated Services Control Point (DSCP) classification

- IP precedence classification
- Class-based weighted fair queuing (CBWFQ)
- Low latency queuing (LLQ)
- Hierarchical traffic shaping for Frame Relay, HDLC, and PPP encapsulations.

Note The OC-48 POS/DPT modules do not support LLQ, CBWFQ, or DSCP classification. Class-based traffic shaping is supported for ingress traffic only.

Security Protocols

This section lists the supported security features:

- Standard and extended access control lists (ACL)
- Named, dynamic, reflexive, and time-based ACLs
- IPv4 NAT (supported in software)

Multiprotocol Label Switching

MPLS is supported on all Catalyst 6500 and Cisco 7600 series modules.

For information about platform-specific limitations and restrictions, and supported features, see Chapter 11, “Configuring Multiprotocol Label Switching on the Optical Services Modules.”

For information on MPLS and how to configure it on the OSMs, refer to the Multiprotocol Label Switching on Cisco Routers Feature Module at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/mpls4t.htm.

For general information on MPLS, refer to *Multiprotocol Label Switching* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/swprt3/index.htm

Understanding Packet-Over-SONET

Packet-over-SONET is a high-speed method of transporting IP traffic between two points. This technology combines the Point-to-Point Protocol (PPP) with SONET and Synchronous Digital Hierarchy (SDH) interfaces.

SONET is an octet-synchronous multiplex scheme defined by the American National Standards Institute (ANSI) standard (T1.1051988) for optical digital transmission at hierarchical rates from 51.840 Mbps to 2.5 Gbps (Synchronous Transport Signal, STS-1 to STS-48) and greater. SDH is an equivalent international standard for optical digital transmission at hierarchical rates from 155.520 Mbps (STM-1) to 2.5 gigabits per second (Gbps) (STM-16) and greater. SONET electrical specifications have been defined for single-mode fiber, multimode fiber, and CATV 75-ohm coaxial cable. The OC-3c/STM-1, OC-12c/STM-4, and OC-48c/STM-16 POS/SDH OSMs allow transmission over single-mode and multimode optical fiber at Optical Carrier 3, 12, and 48 (OC-3, OC-12, and OC-48) rates.

SONET/SDH transmission rates are integral multiples of 51.840 Mbps. The following transmission multiples are currently specified and commonly used:

- OC-3c/STM-1c—155.520 Mbps

- OC-12c/STM-4c—622.080 Mbps
- OC-48c/STM-16c—2488.320 Mbps

The POS specification (RFC 1619) describes the use of PPP encapsulation over SONET/SDH links. Because SONET/SDH is, by definition, a point-to-point circuit, PPP is well-suited for use over these links. PPP treats SONET/SDH transport as octet-oriented full-duplex synchronous links. PPP presents an octet interface to the physical layer. The octet stream is mapped into the SONET/SDH Synchronous Payload Envelope (SPE), with the octet boundaries aligned with the SPE octet boundaries. The PPP frames are located by row within the SPE payload. Because frames are variable in length, the frames are allowed to cross SPE boundaries.

The basic rate for POS is OC-3/STM-1, which is 155.520 Mbps. The available information bandwidth is 149.760 Mbps, which is the OC-3c/STM-1 SPE with section, line, and path overhead removed.

SONET Distance Limitations

The specification for optical fiber transmission defines two types of fiber: single-mode and multimode. Within the single-mode category, three transmission types are defined: short reach, intermediate reach, and long reach. Within the multimode category, only short reach is available.

For information on cable distance limitations and power budget, see
http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/hardware/osmodule/02prep.htm.

Configuring the Interfaces

This section describes how to configure the OC-3c/STM-1, OC-12c/STM-4, and OC-48c/STM-16 OSMs:

- Initial Configuration of the POS/SDH OSMs, page 3-9
- Configuring the Interface, page 3-9
- Customizing the POS/SDH OSM Configuration, page 3-10
- Using show Commands to Check System Status, page 3-12
- Configuring Automatic Protection Switching, page 3-13
- Configuring Frame Relay and Frame Relay Traffic Shaping, page 3-17
- Configuring Dynamic Packet Transport Protocol, page 3-20
- Configuring Bridging Control Protocol, page 3-22
- OC-3c/STM-1 POS Module Configuration Example, page 3-24

Initial Configuration of the POS/SDH OSMs

If you installed a new POS/SDH OSM or want to change the configuration of an existing interface, you must enter configuration mode by using the **configure** command in the privileged EXEC mode. Table 3-1 shows the default configuration of an enabled module. For more information, see the "Customizing the POS/SDH OSM Configuration" section on page 3-10.

Table 3-1 POS/SDH Module Configuration Default Values

Parameter	Configuration Command	Default Value
Keepalive	[**no**] **keepalive**	keepalive
Encapsulation	**encapsulation** [**hdlc** | **ppp** | **frame-relay**]	hdlc
Cisco Discovery Protocol (cdp)	[**no**] **cdp enable**	cdp enable
Maximum transmission unit (mtu)	[**no**] **mtu** *bytes*	4470 bytes
Framing	**pos framing** [**sdh** | **sonet**]	SONET OC-3c; OC-12c; OC-48c
Bandwidth	[**no**] **bandwidth** *kilobits*	155000; 622000; 2500000
SONET overhead	**pos flag** [**c2** *value* | **j0** *value* | **s1s0** *value* | **s1 ignore**]	c2 set to 0xcf; j0 set to 0xcc; s1s0 set to 0; s1 set to ignore the received s1 byte setting.
Loop internal	[**no**] **loop** [**internal** | **line**]	no loopback
POS SPE scrambling	[**no**] **pos scramble-atm**	no POS SPE scramble
Cyclic Redundancy Check	**crc** [**16** | **32**]	32
Clock source	**clock source** [**internal** | **line**]	line

Configuring the Interface

After you verify that the new POS/SDH OSM is installed correctly, use the **configure** command in the privileged EXEC mode to configure the new interface. Be prepared with the information you will need, such as the interface IP address.

The following procedure is for creating a basic configuration, which includes enabling an interface and specifying IP routing.

A Catalyst 6500 series switch and Cisco 7600 series router identifies an interface address by its module slot number and port number in the format *slot/port*. For example, the slot/port address of an interface on a 1-port OC-48c/STM-16 POS/SDH OSM installed in slot 4 is *4/1*. Even though the card contains only one port, you must use the *slot/port* notation.

Before using the **configure** command, you must enter the privileged level mode of the EXEC command interpreter by using the **enable** command. The system will prompt you for a password if one is set.

To configure the POS/SDH OSMs (press the **Return** key after each configuration step unless otherwise noted), perform this task:

	Command	Purpose
Step 1	`Router# show version`	Confirms that the system recognizes the module by entering the **show version** command.
Step 2	`Router# show interface`	Checks the status of each port by entering the **show interface** command.
Step 3	`Router# configure terminal`	Enters configuration mode and specifies that the console terminal will be the source of the configuration subcommands.
Step 4	`Router(config)# ip routing`	Enables IP routing by entering the **ip routing** command.
Step 5	`Router(config)# interface pos slot/port`	Specifies the new interface to configure by entering the **interface** command, followed by *type* and *slot/port*.
Step 6	`Router(config-if)# ip address ip-address mask [secondary]`	Assigns an IP address and subnet mask to the interface.
Step 7	`Router(config-if)# encapsulation encapsulation-type`	Verifies that HDLC encapsulation is correct for this interface; *encapsulation-type* is one of the keywords, **hdlc** or **ppp** or **frame-relay.**
Step 8	`Router(config-if)# clock source {line | internal}`	Verifies that the default value for the clock source is correct. The default value is *line*. Use it when clocking is derived from the network. The **clock source internal** command is typically used when two Cisco 7600 series routers or Catalyst 6500 series switches are connected back-to-back or are connected over dark fiber where no clocking is available. In either case, each device should have its clock source set to internal.
Step 9	`Router(config-if)# no shutdown`	Changes the interface state to up and enables the interface.
Step 10	`Router(config-if)# keepalive`	Turns on or off keepalive messages as desired. Keepalive messages are useful for encapsulated protocols such as HDLC. The keepalive default is on.
Step 11	`Router# copy running-config startup-config`	Writes the new configuration to memory.

Customizing the POS/SDH OSM Configuration

This section documents new platform-specific commands. Other commands used in OSM configuration are documented in the Cisco IOS Release 12.1 command reference publications.

You can change the default values of all POS/SDH OSM configuration parameters to match your network environment. Perform the tasks in the following sections if you need to customize the POS/SDH OSM configuration:

- Selecting a POS/SDH OSM Interface, page 3-11
- Configuring Framing, page 3-11
- Specifying SONET Overhead, page 3-11
- Configuring POS SPE Scrambling, page 3-11

Selecting a POS/SDH OSM Interface

An OC-3c/STM-1, OC-12c/STM-4, or OC-48c/STM-16 interface is referred to as **pos**, for packet-over-SONET, in the configuration commands. To select a specific POS interface, use the **interface pos** *slot/port* command in the configuration mode:

```
Router(config)# interface pos slot/port
```

Configuring Framing

The **pos framing** command allows you to set framing to SONET OC or SDH STM. The default is SONET.

```
Router(config-if)# pos framing [sdh|sonet]
```

Specifying SONET Overhead

The **pos flag** command allows you to specify values for the specific elements of the frame header.

```
Router(config-if)# pos flag [c2 value] [j0 value] [s1s0 value]
```

where

- **c2** is a path signal identifier, and *value* is one of the following:
  - 0xCF = PPP or HDLC (default)
  - 0x13 = ATM
- **j0** is the section trace byte, and *value* is 0x1 for interoperability with some SDH devices in Japan. The default value is 0xCC.
- **s1s0** is part of the payload pointer byte, and *value* is one of the following:
  - 0 = OC-3c (default)
  - 2 = AU-4

Configuring POS SPE Scrambling

The POS scrambling command allows you to scramble the POS SPE (synchronous payload envelope) payload. The default is no POS SPE scramble.

```
Router(config-if)#[no] pos scramble-atm
```

Using show Commands to Check System Status

Each OSM maintains information about its configuration, traffic, and errors. You can access this information by using the **show** commands.

Descriptions and examples of module and system status **show** commands follow:

- Use the **show interfaces** command and the **show interfaces pos** *slot/port* command to display information about the system interfaces. The following example illustrates the **show interface pos** *slot/port* command for port 1 of a module installed in slot 5:

```
Router# show interfaces pos 5/1
POS5/1 is administratively down, line protocol is down
  Hardware is Packet over SONET
  MTU 4470 bytes, BW 155000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation HDLC, crc 32, loopback not set, keepalive set (10 sec)
  Scramble disabled
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  queuing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
              0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 applique, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
...
(output truncated)
```

- Use the **show version** command to display the configuration of the system hardware (the number of each module type installed), the Cisco IOS software version, the names and sources of configuration files, and the boot images. The following example illustrates the **show version** command for a Catalyst 6509 switch:

```
Router# show version
WS-C6509 Software, Version NmpSW: 6.1(2)
Copyright (c) 1995-2001 by Cisco Systems
NMP S/W compiled on Jan 25 2001, 12:28:23
System Bootstrap Version: 6.1(2)
Hardware Version: 2.0 Model: WS-C6509 Serial #: SCA042101NG
Mod     Port    Model               Serial #        Versions
---     ----    ------------------- ----------- -----------------------------------
---
1       2       WS-X6K-SUP2-2GE     SAD044102J9     Hw : 1.1
                                                    Fw : 6.1(2)
                                                    Fw1: 6.1(3)
                                                    Sw : 6.1(2)
                                                    Sw1: 6.1(2)
                WS-F6K-PFC2         SAD04470KPP     Hw : 1.0
3       8       WS-X6408-GBIC       SAD03090264     Hw : 1.4
                                                    Fw : 4.2(0.24)VAI78
                                                    Sw : 6.1(2)
4       8       WS-X6408A-GBIC      SAD043500LE     Hw : 1.3
                                                    Fw : 5.4(2)
                                                    Sw : 6.1(2)
5       4       OSM-4OC12-POS-MM    SAD050202EJ     Hw : 0.101
                                                    Fw : 12.1(6.5)E1
                                                    Sw : 12.1(6.5)E1
```

```
6       24      WS-X6224-100FX-MT   SAD03040765     Hw : 1.2
                                                    Fw : 4.2(0.24)VAI78
                                                    Sw : 6.1(2)
9       48      WS-X6248            SAD03200773     Hw : 1.1
                                                    Fw : 4.2(0.24)VAI78
                                                    Sw : 6.1(2)
15      1       WS-F6K        SAD044803FK     Hw : 1.1
                                                    Fw : 12.1(3a)E4
                                                    Sw : 12.1(3a)E4
         DRAM                      FLASH                   NVRAM
Module   Total     Used    Free    Total   Used    Free    Total  Used   Free
------   -------   ------- ------- ------- ------- ------- -----  -----  -----
1      130944K     57316K  73628K  16384K  6647K   9737K   512K   302K   210K
Uptime is 2 days, 19 hours, 50 minutes
Console> (enable))
```

- Use the **show protocols** command to display the global (system-wide) and interface-specific status of any configured Level 3 protocol.
- Use the **show running-config** command to display the currently running configuration in RAM:

```
Router# show running-config
Building configuration...
Current configuration:
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname Maxwell
!
enable secret 5 $1$ZBC0$tJO8EeP3VI769LAw.3edJ1
enable password xxxx
!
ip host ray 172.27.136.253
ip host crusty 171.69.209.28
ip domain-name cisco.com
ip name-server 171.69.209.10
clock timezone EST -5
clock summer-time EDT recurring
!
interface POS0/0
 no ip address
 shutdown
 crc 32
!
interface POS0/1
 no ip address
 shutdown
 crc 32
!
(output truncated)
```

Configuring Automatic Protection Switching

Automatic protection switching (APS) allows switchover of packet-over-SONET (POS) circuits and is often required when connecting SONET equipment to telecommunications equipment. When APS is configured, a protect POS interface is brought into the SONET network from the intervening SONET equipment and the protect POS interface becomes the working POS interface on the circuit.

The protect interface is configured with the IP address of the router that has the working interface. The APS Protect Group Protocol provides communication between the process controlling the working interface and the process controlling the protect interface. When you use the APS Protect Group Protocol, POS interfaces can be switched in the event of a router failure, degradation or loss of channel signal, or manual intervention.

Two SONET connections are required to support APS. In a telecommuncations environment, the SONET circuits must be provisioned as APS. You must also provision the operation, mode, and revert options. If the SONET connections are homed on two separate routers (the normal configuration), an out-of-band (OOB) communications channel between the two routers needs to be set up for APS communication.

When configuring APS, we recommend that you configure the working interface first, along with the IP address of the interface being used as the APS OOB communications path.

Note To prevent the protected interface from becoming the active circuit and disabling the working circuit when it is discovered, configure the working interface before configuring the protected interface.

For more information on APS and configuration information for additional APS features, refer to the *Cisco IOS Interface Configuration Guide,* Release 12.1 at this URL:

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

Configuring the Working Interface

To configure the working interface, perform this task:

	Command	Purpose
Step 1	Router(config)# **interface pos** *slot/port*	Specifies the POS interface to be configured as the working interface and enters interface configuration mode.
Step 2	Router(config-controller)# **aps working** *circuit-number*	Configures this interface as a working interface.
Step 3	Router(config)# **end**	Exits configuration mode.
Step 4	Router# **show controllers pos** Router# **show interface pos** Router# **show aps** Router# **show aps controller**	Displays information about the POS controllers and interface so that you can verify that the interface is configured correctly.

Note If a router has two or more protect interfaces, the **aps group** command for each interface must precede the corresponding **aps protect** command.

Configuring the Protect Interface

To configure the protect interface, perform this task beginning in global configuration mode:

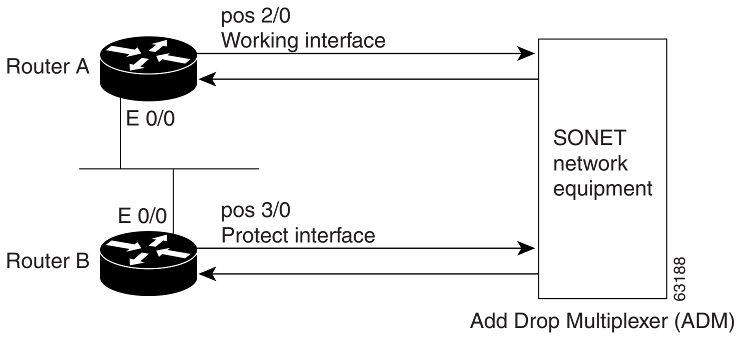
	Command	Purpose
Step 1	`Router(config)#` **`interface pos`** *`slot/port`*	Specifies the POS interface to be configured as the protect interface and enters interface configuration mode.
Step 2	`Router(config-if)#` **`aps protect`** *`circuit-number ip-address`*	Configures this interface as a protect interface. Specifies the IP address of the router that contains the working interface.
Step 3	`Router(config-if)#` **`end`**	Exits configuration mode.

Step 4	`Router#` **`show controllers pos`**
	`Router#` **`show interface pos`**
	`Router#` **`how aps`**
		Displays information about the POS controllers and interface so that you can verify that the interface is configured correctly.

Configuring Basic APS

The following example shows the configuration of APS on router A and router B (see Figure 3-3). In this example, router A is configured with the working interface, and router B is configured with the protect interface. If the working interface on router A becomes unavailable, the connection will automatically switch over to the protect interface on router B. The working and protect interfaces are configured at the controller level.

Figure 3-3 Basic APS Configuration



Step 1 On router A, which contains the working interface, use the following configuration:

```
Router# configure terminal
Router(config)# interface loopback 1
Router(config-if)# ip address 7.7.7.7 255.255.255.0
Router(config)# exit
Router(config)# interface pos 2/0
Router(config-if)# aps working 1
router(config-if)# pos ais-shut
Router(config-if)# end
Router#
```

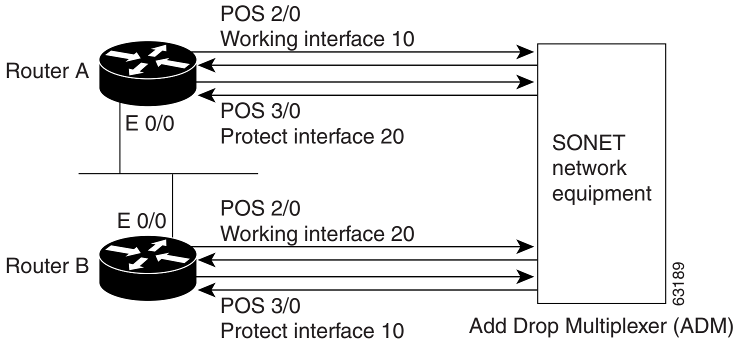
Step 2 On router B, which contains the protect interface, use the following configuration:

```
Router# configure terminal
Router(config)# interface loopback 2
Router(config-if)# ip address 7.7.7.6 255.255.255.0
Router(config)# exit
Router(config-if)# interface pos 3/0
Router(config-if)# aps protect 1 7.7.7.7
router(config-if)# pos ais-shut
Router(config-if)# end
Router#
```

Multiple APS Interface Configuration

To configure more than one protect/working interface, use the **aps group** command. The following example in Figure 3-4 shows the configuration of grouping more than one working/protect interface. In this example, router A is configured with a working interface and a protect interface, and router B is configured with a working interface and a protect interface. If the working interface 2/0 on router A becomes unavailable, the connection will switch over to the protect interface 3/0 on router B because they are both in APS group 10. Similarly, if the working interface 2/0 on router B becomes unavailable, the connection will switch over to the protect interface 3/0 on router A because they are both in APS group 20.

Figure 3-4 Multiple Working and Protect Interfaces Configuration



Note Configure the working interface before configuring the protect interface to avoid the protect interface from becoming the active circuit and disabling the working circuit when it is discovered.

Step 1 On router A, which contains the working interface for group 10 and the protect interface for group 20, use the following configuration:

```
router# configure terminal
router(config)# interface ethernet 0/0
router(config-if)# ip address 7.7.7.6 255.255.255.0
router(config-if)# exit
router(config)# interface POS 2/0
router(config-if)# aps group 10
router(config-if)# aps working 1
router(config-if)# exit
router(config)# interface POS 3/0
router(config-if)# aps group 20
router(config-if)# aps protect 1 7.7.7.7
router(config-if)# end
router#
```

Step 2 On router B, which contains the protect interface for group 10 and the working interface for group 20, use the following configuration:

```
router# configure terminal
router(config)# interface ethernet 0/0
router(config-if)# ip address 7.7.7.7 255.255.255.0
router(config-if)# exit
router(config)# interface POS 2/0
router(config-if)# aps group 20
router(config-if)# aps working 1
router(config-if)# exit
router(config)# interface POS 3/0
router(config-if)# aps group 10
router(config-if)# aps protect 1 7.7.7.6
router(config-if)# end
router#
```

Configuring Frame Relay and Frame Relay Traffic Shaping

This section describes Frame Relay configurations, platform-specific commands, and limitations:

- Frame Relay Limitations and Restrictions, page 3-18
- Frame Relay Traffic Shaping Configuration Example, page 3-18

Configure the interfaces for Frame Relay as described in the *Cisco IOS Wide-Area Networking Configuration Guide,* Release 12.1 under "Configuring Frame Relay" and in the *Cisco IOS Wide-Area Networking Command Reference,* Release 12.1 at these URLs:

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

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

Configure traffic shaping for Frame Relay as described in the *Cisco IOS Quality of Service*

Solutions Configuration Guide under "Configuring Distributed Traffic Shaping" at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt4/qcfdts.htm.

Frame Relay Limitations and Restrictions

The following limitations and restrictions apply to Frame Relay:

- Frame Relay is not supported on SVCs.
- IP addresses cannot be assigned to main interfaces configured for Frame Relay.
- Frame Relay is supported only on point-to-point connections.
- Frame Relay switching functionality is not supported. The Frame-Relay switching configuration is available only to configure the **frame-relay intf-type dce** option.
- Frame Relay Fragmentation and Compression is not supported.
- Only FIFO queuing is supported.
- DLCI is configurable on subinterfaces only and cannot be configured on the main interface.
- Only class-based traffic shaping is supported. The following commands are not supported:
  - Router(config-pmap-c)# **shape** [**average** | **peak**] *mean-rate* [[*burst-size*] [*excess-burst-size*]]
  - Router(config-pmap-c)# **priority** {*kbps* | **percent** *percent*} [*bytes*]
  - Router(config-pmap-c)# **fair-queue** *number-of-queues*
  - Router(config-map-class)# **frame-relay adaptive-shaping** [**becn** | **foresight**]
  - Router(config-map-class)# **frame-relay cir** {**in** | **out**} *bps*
  - Router(config-map-class)# **frame-relay** {**bc** | **be**} {**in** | **out**} *bits*
  - Router(config-map-class)# **frame-relay traffic-rate average** [**peak**]
  - Router(config-map-class)# **frame-relay priority-group** *list-number*
  - Router(config-map-class)# **frame-relay fragment** *fragment_size*
  - Router(config-if)# **frame-relay payload-compress packet-by-packet**
  - Router(config-if)# **frame-relay de-group** *group-number dlci*
  - Router# **show traffic-shape queue**

Frame Relay Traffic Shaping Configuration Example

To configure frame relay traffic shaping, perform this task:

	Command	Purpose
Step 1	`Router(config-pmap)# **class-map** [**match-all** | **match-any**]`	Creates a class map to be used for matching packets to a class you define and specifies the criteria to match on. Match criteria for classes can be based on IP DSCP or IP precedence.
Step 2	`Router(config-pmap)# **match**`	Identifies a match criterion.
Step 3	`Router(config)# **policy-map** *policy_map*`	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
Step 4	`Router(config-pmap)# **class** *class-name*`	Defines the classes you want the service policy to contain.
Step 5	`Router(config-pmap-c)# **shape average** *mean-rate* [burst-size]`	Shapes traffic to the indicated bit rate.

	Command	Purpose
Step 6	`Router(config)# map-class frame-relay map-class-name`	Specifies a map class to define quality of service (QoS) values.
Step 7	`Router(config-map-class)# no frame-relay adaptive-shaping`	Disables backward notification.
Step 8	`Router(config-map-class)# service-policy input policy-map`	Attaches the specified policy map to the input interface.
Step 9	`Router(config-map-class)# service-policy output policy-map`	Attaches the specified policy map to the output interface.
Step 10	`Router(config)# interface interface`	Specifies the interface to which the policy map will be applied.
Step 11	`Router(config-subif)# ip address ip_address mask`	Assigns an IP address to the subinterface.
Step 12	`Router(config-subif)# no cdp enable`	Disables CDP.
Step 13	`Router(config-subif)# frame-relay interface-dlci dlci`	Assigns a data link connection identifier (DLCI) to a specified Frame Relay subinterface.
Step 14	`Router(config-fr-dlci)# class class-name`	Specifies the name a predefined map-class which was defined with the **map-class frame-relay** command.

We recommend that you explicitly disable CDP on the subinterfaces. Should CDP be required on the subinterfaces, the input-queue depth may need to be adjusted. To accommodate the number of incoming CDP packets, configure the input-queue depth on the main interface to be slightly larger than the number of subinterfaces on which you have enabled CDP. The default input-queue depth is 75 and can be adjusted with the **hold-queue** interface command:

```
Router(config-if)# hold-queue 300 in
```

The following example shows a configuration that shapes the traffic for DLCI 18 to be 8 Mbps on both input and output traffic flows:

```
Router(config)# class-map match-all fr-classmap
Router(config-cmap)# match any
Router(config-cmap)# exit
Router(config)# policy-map fr-map
Router(config-pmap)# class fr-classmap
Router(config-pmap-c)# shape average 8000000 32000 32000
Router(config-pmap-c)# exit
Router(config)# map-class frame-relay fr-shaping
Router(config-map-class)# no frame-relay adaptive-shaping
Router(config-map-class)# service-policy input fr-pmap
Router(config-map-class)# service-policy output fr-pmap
Router(config-map-class)# exit
Router(config)# interface POS7/15.1 point-to-point
Router(config-subif)# ip address 72.0.0.1 255.255.0.0
Router(config-subif)# no cdp enable
Router(config-subif)# frame-relay interface-dlci 18
Router(config-fr-dlci)# class fr-shaping
Router(config-fr-dlci)# exit
```

Configuring Dynamic Packet Transport Protocol

Dynamic Packet Transport (DPT) is a packet ring technology that allows you to scale and distribute your Internet and IP services across a reliable optical packet ring infrastructure.

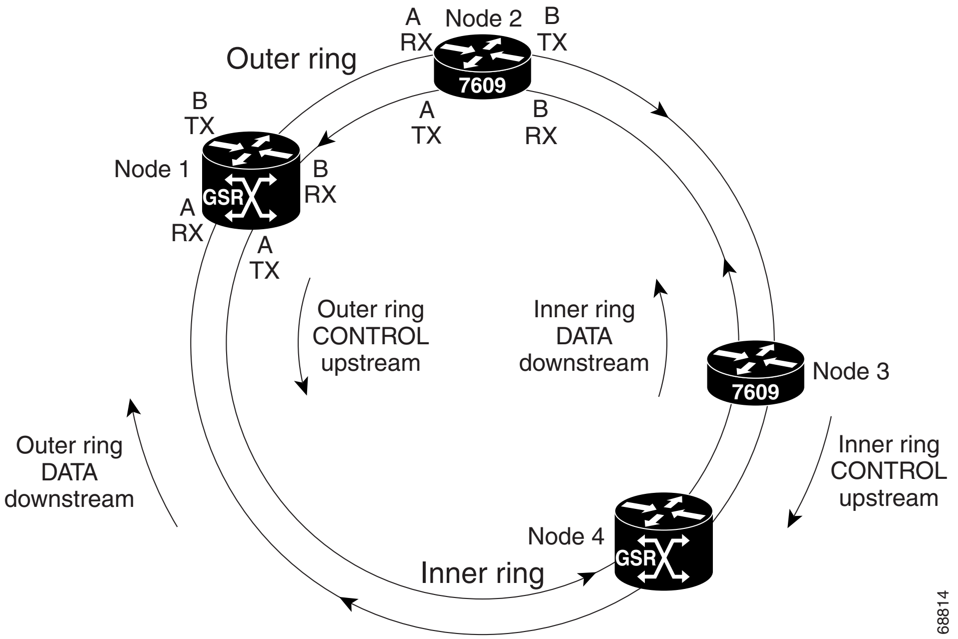
For general overview information for DPT, refer to the *Dynamic Packet Transport Feature Guide* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/srpapsgs.htm

The 2-port OC-48c/STM-16c OSM can be used as a 2-port POS/SDH uplink module or as a single-port DPT module. When the 2-port OC-48c/STM-16c OSM is used as a DPT module, one of the OC-48 interfaces functions as the Side-A interface and the other as the Side-B interface.

Figure 3-5 shows a DPT ring created with two 1-port OC-48c/STM-16c SRP modules installed in the Cisco 12000 series router and one 2-port OC-48c/STM-16c OSM installed in the Cisco 7600 series routers.

Figure 3-5 SRP/DPT Ring Example



To configure DPT on the 2-port OC-48c/STM-16 OSM, perform this task from configuration mode:

	Command	Purpose
Step 1	`Router(config)# hw-module slot 4 srp`	Converts the module to SRP/DPT mode.
Step 2	`Router(config)# interface srp 4/1`	Selects the SRP interface to be configured.
Step 3	`Router(config-if)# ip address 10.1.2.1 255.255.255.0`	Configures the IP address.
Step 4	`Router(config-if)# no cdp enable`	Disables CDP.
Step 5	`Router(config-if)# no shutdown`	Brings up the interface.
Step 6	`Router(config-if)# exit`	Exits interface configuration mode.

	Command	Purpose
Step 7	`Router(config)# exit`	Exits configuration mode.
Step 8	`Router# show interfaces srp 4 /1`	Displays interface configuration.

This example shows how to configure the 2-port OC-48c/STM-16c OSM for SRP/DPT mode.

```
Router(config)# hw-module slot 4 srp
```

Note Wait for the module in slot 4 to be configured to SRP/DPT mode and automatically reloaded. Continue with the configuration.

```
Router(config)# interface srp 4/1
Router(config-if)# ip address 10.1.2.1 255.255.255.0
Router(config-if)# no cdp enable
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
Router# show interfaces srp 4/1
SRP4/1 is up, line protocol is up
  Hardware is SRP, address is 00d0.01d7.4c0a (bia 00d0.01d7.4c0a)
  Internet address is 10.1.2.1/24
  MTU 4470 bytes, BW 2488000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 41/255
  Encapsulation SRP2,
  Side A: loopback not set
  Side B: loopback not set
     3 nodes on the ring   MAC passthrough not set
     Side A: not wrapped   IPS local: IDLE       IPS remote: IDLE
     Side B: not wrapped   IPS local: IDLE       IPS remote: IDLE
  Scramble enabled
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  queuing strategy: fifo
  Output queue :0/40 (size/max)
  Side A: 5 minutes output rate 0 bits/sec, 0 packets/sec
          5 minutes input rate 0 bits/sec, 0 packets/sec
  Side B: 5 minutes output rate 0 bits/sec, 0 packets/sec
          5 minutes input rate 0 bits/sec, 0 packets/sec
  L2 Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
  L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
  L3 out Switched: ucast: 0 pkt, 0 bytes
     360563 packets input, 286645033 bytes, 0 no buffer
     Received 0 broadcasts, 43 runts, 0 giants, 0 throttles
     50 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 7 abort
     847443 packets output, 34168034 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out
     Side A received errors:
        33 input errors, 0 CRC, 0 ignored,
        29 framer runts, 0 framer giants, 4 framer aborts,
        0 mac runts, 0 mac giants, 0 mac aborts
     Side B received errors:
        17 input errors, 0 CRC, 0 ignored,
        14 framer runts, 0 framer giants, 3 framer aborts,
        0 mac runts, 0 mac giants, 0 mac aborts
Router#
```

Configuring Bridging Control Protocol

When BCP is used to forward Ethernet frames over SONET no Layer 3 routing information needs to be exchanged, and the POS links function like Ethernet trunks carrying VLAN traffic over the existing reliable high-speed SONET network. BCP is not supported on DPT OSM.

Usage Guidelines and Restrictions

When configuring BCP, observe the following guidelines and restrictions.

- Each PXF complex supports only one instance of a VLAN. As a result, although more than one interface might be supported per PXF complex, the same VLAN cannot be configured on more than one interface per PXF complex. Depending on the particular POS OSM, each interface may share a PXF complex with other interfaces. For example, on a 4-port OC-12 POS OSM, port 1 and 2 share one PXF complex and port 3 and 4 share another PXF complex. If VLAN 400 is configured on port 1, that same VLAN cannot be configured on port 2. But VLAN 400 is allowed on either port 3 or port 4.

  Additionally, if you configure a given VLAN for BCP, then you cannot configure the same VLAN for any other bridging feature on an interface attached to the same PXF complex. This includes Frame Relay bridging as well as VPLS (Virtual Private LAN Service).
- In order for a POS interface to support bridging, the POS interface minimum MTU size should be 24 bytes larger than the VLAN interfaces and Ethernet interfaces MTU size. This accounts for 6 bytes of RFC 3518 header and 18 bytes of 802.1Q header.

  For example, if the MTU size on an ingress Ethernet port is 3000 bytes, the POS port MTU size should be at least 3024 bytes.

Quality of Service Support

OSMs use DSCP-based queuing and shaping, but because BCP does Layer 2 traffic forwarding, there is no DSCP value to look at. Instead, the 3-bit CoS field in the 802.1Q header is mapped to a 6-bit DSCP value.

When BCP is enabled, the CoS value in the 802.1Q header is mapped to the DSCP value in the IP header according to this default CoS to DSCP mapping:

CoS	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

For information about QoS on the Layer 3 OSM ports, see Chapter 9, “Configuring QoS on the Optical Services Modules.” For information on PFC2 QoS support, refer to the QoS chapter of the *Cisco 7600 Series Router Software Configuration Guide* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/qos.htm

To configure BCP, peform this task:

	Command	Purpose
Step 1	`Router(config)# **interface pos** *mod/port*`	Selects the interface.
Step 2	`Router(config-if)# **encapsulation ppp**`	Configures the interface for PPP encapsulation.

	Command	Purpose
Step 3	`Router(config-if)#` **`bridge-enable`**[1]	Enables BCP on the interface.
Step 4	`Router(config-if)#` **`switchport trunk`** `{`**`allowed`** `|` **`pruning vlan`** `{`**`add`** `|` **`all`** `|` **`except`** `|` **`remove`**`}}`	Configures the trunk characteristics.
Step 5	`Router(config-if)#` **`end`**	Exits configuration mode.
Step 6	`Router#` **`show interface pos`** *`mod/num`*	Displays interface configuration.

[1] Enter the **bridge-enable** command while the port is in shutdown state. If you enter the **bridge-enable** command while the port is in up state, enter the **shutdown** command followed by the **no shutdown** command in order to bring up BCP on the POS port.

In this example, BCP forwarding of all VLANs except for VLAN 400 is configured on a POS interface:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface pos 3/2
Router(config)# encapsulation ppp
Router(config-if)# bridge-enable
Router(config-if)# switchport trunk allowed vlan all
Router(config-if)# switchport trunk allowed vlan remove vlan 400
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# end
Router# show running-config interface pos 3/2
!
interface POS3/2
 ip address 2.2.2.2 255.255.255.0
 encapsulation ppp
  bridge-enable
 switchport
 switchport trunk allowed vlan 1-399,401-1005
 switchport mode trunk
 no cdp enable
end

Router# show interface pos 3/2 switchport
Name:Po3/2
Switchport:Enabled
Administrative Mode:trunk
Operational Mode:trunk
Administrative Trunking Encapsulation:dot1q
Operational Trunking Encapsulation:dot1q
Negotiation of Trunking:Off
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Administrative private-vlan host-association:none
Administrative private-vlan mapping:none
Operational private-vlan:none
Trunking VLANs Enabled:1-399,401-1005
Pruning VLANs Enabled:2-1001

Router# show interface pos 3/2 trunk

Port      Mode         Encapsulation  Status        Native vlan
Po3/2     on           802.1q         trunking      1

Port      Vlans allowed on trunk
Po3/2     1-399,401-1005

Port      Vlans allowed and active in management domain
Po3/2     1,31-32,34,91-92,100,500,1002-1005
```

```
Port      Vlans in spanning tree forwarding state and not pruned
Po3/2     31-32,34,91-92,100,1002-1005
```

OC-3c/STM-1 POS Module Configuration Example

The following is an example of configuration file commands for a Cisco 7600 series router (first router) with an OC-3c/STM-1 POS module in slot 3 connected back-to-back with a Cisco 7500 series router (second router) with a POS Interface Processor (POSIP) module in slot 3.

The configuration commands for the first router are as follows:

```
interface pos 3/1
ip address 10.1.2.3 255.0.0.0
clock source internal
no shutdown
no keepalive
no cdp enable
no ip mroute-cache
crc 32
```

The configuration commands for the second router are as follows:

```
interface pos 3/0/0
ip address 10.1.2.4 255.0.0.0
clock source internal
no shutdown
no keepalive
no cdp enable
crc 32
```

Configuring Multipoint Bridging

Multipoint bridging enables point-to-multipoint bridging for Frame Relay data-link connection identifiers (DLCIs). This feature allows the use of multiple DLCIs per VLAN for bridging on the following OSMs:

- 8-Port OC-3 POS
- 16-Port OC-3 POS
- 2-Port OC-12 POS
- 4-Port OC-12 POS:
- 1-Port OC-48 POS
- 2-Port OC-48 POS/DPT

Multipoint bridging allows service providers to add support for Ethernet-based Layer 2 services to the proven technology of their existing Frame Relay legacy networks. Customers can then use their current VLAN-based networks over the Frame Relay cloud. This also allows service providers to gradually update their core networks to the latest Gigabit Ethernet optical technologies, while still supporting their existing customer base.

Frame Relay interfaces use RFC 1490 bridging, which provides an encapsulation method to allow the transport of Ethernet frames over each type of Layer 2 network.

Note RFC 1490 has been obsoleted and superseded by RFC 2427, *Multiprotocol Interconnect over Frame Relay*. To avoid confusion, this document continues to use the original RFC numbers.

In Cisco IOS Release 12.2(18)SXE, multipoint bridging supports the following modes of operation:

- Raw (default)—Default bridging access mode, in which the bridged connection acts on and transmit bridge protocol data unit (BPDU) packets.
- Access—Access-only bridging access mode, in which the bridged connection does not act on or transmit BPDU packets.
- 802.1Q—Performs IEEE 802.1Q tagging to preserve the class of service (CoS) information from the Ethernet frames across the ATM network.
- 802.1Q Tunnel—IEEE 802.1Q tunneling mode, so that service providers can use one VLAN to support customers with multiple VLANs, as well as accept untagged frames.

Restrictions and Usage Guidelines

The following restrictions apply to the Multipoint Bridging feature:

- Supported only on Enhanced OSMs; non-enhanced OSMs are not supported.
- Multipoint bridging on Frame Relay interfaces supports only IETF encapsulation. Cisco encapsulation is not supported on when doing multipoint bridging.
- VLAN ID 1 is not available as a bridge domain for doing multipoint bridging.
- Multipoint bridging supports an absolute maximum of 60 VCs per each VLAN, and an absolute maximum number of VLANs per peer is 4096. We recommend configuring at most 30 VCs per VLAN, with at most 1024 VLANs per VC.

Prerequisites

The following prerequisites apply to Multipoint Bridging:

- VLANs must be manually added to the VLAN database, using the **vlan** command, to be able to use those VLANs in multipoint bridging.

Configuring Multipoint Bridging for Frame-Relay Interfaces

This section describes how to configure multipoint bridging on Frame-Relay interfaces. You can configure multipoint bridging on individual DLCI circuits. You can optionally add 802.1Q tagging or 802.1Q tunneling. To perform this configuration, use the following procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vlan** {*vlan-id* | *vlan-range*}
4. **interface** *iftype slot/port*
5. **no ip address**
6. **encapsulation frame-relay ietf**

Note The **encapulsulation frame-relay ietf** command does not work with Cisco encapsulation.

7. **mls qos trust** {**cos** | **dscp**}
8. **interface** *iftype slot/port.subinterface* {**multipoint** | **point-to-point**}
9. **mls qos trust** {**cos** | **dscp**}
10. **frame-relay interface-dlci** *dlci* [**ietf**]
11. **bridge-domain** *vlan-id* [**access** | **dot1q** | **dot1q-tunnel**] [**split-horizon**]
12. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**`vlan`** {*`vlan-id`* | *`vlan-range`*}
	Example:
	`Router(config)# vlan 2,5,10-12,20,25,4000`
	`Router(config-vlan)#`
		Adds the specified VLAN IDs to the VLAN database and enters VLAN configuration mode.
		• *vlan-id*—Specifies a single VLAN ID. The valid range is from 1 to 4094 (but VLAN 1 is not supported for multipoint bridging).
		• *vlan-range*—Specifies multiple VLAN IDs, as either a list or a range. The *vlan-range* can contain a list of the VLAN IDs, separated either by a comma (,), dash (-), or both.
		Note You must manually enter a VLAN ID into the VLAN database before you can use that VLAN for multipoint bridging.

	Command or Action	Purpose

Step 4	**`interface`** *`iftype slot/port`*
	Example:
	`Router(config)# interface pos 4/1`
	`Router(config-if)#`
		Enters configuration mode for the specified interface.

Step 5	**`no ip address`**
	Example:
	`Router(config-if)# no ip address`
	`Router(config-if)#`
		Removes the IP address, if any, that is configured on the interface.

Step 6	**`encapsulation frame-relay ietf`**
	Example:
	`Router(config-if)# encapsulation frame-relay ietf`
	`Router(config-if)#`
		Enables Frame Relay encapsulation on the interface, using IETF encapsulation. You must specify the **ietf** keyword either here or in Step 10 for each individual DLCI.
		Note Multipoint bridging does not support Cisco encapsulation using the **cisco** keyword.

	Note The **ietf** keyword is not available for a Frame Relay DLCI on a multipoint interface. If you want to configure a bridge-domain on a DLCI attached to a multipoint interface you must first enable Frame Relay encapsulation on the interface using IETF encapsulation.	

Step 7	**`mls qos trust`** `{`**`cos`** `|` **`dscp`**`}`
	Example:
	`Router(config-if)# mls qos trust cos`
	`Router(config-if)#`
		(Optional) Specifies the trusted state of the interface. The default state is untrusted, but can be changed with one of the following options:
		• **cos**—(Optional) Specifies that the CoS bits in incoming frames are trusted and derives the internal DSCP value from the CoS bits.
		• **dscp**—(Optional) Specifies that the ToS bits in the incoming packets contain a DSCP value.

Step 8	**`interface`** *`iftype slot/port.subinterface`* `{`**`multipoint`** `|` **`point-to-point`**`}`
	Example:
	`Router(config-if)# interface pos 4/1.21`
	`Router(config-subif)#`
		Enters configuration mode for the specified subinterface.

Step 9	**`mls qos trust`** `{`**`cos`** `|` **`dscp`**`}`
	Example:
	`Router(config-subif)# mls qos trust cos`
	`Router(config-subif)#`
		(Optional) Specifies the trusted state of the subinterface. The default state is untrusted, but can be changed with one of the following options:
		• **cos**—(Optional) Specifies that the CoS bits in incoming frames are trusted and derives the internal DSCP value from the CoS bits.
		• **dscp**—(Optional) Specifies that the ToS bits in the incoming packets contain a DSCP value.

	Command or Action	Purpose
Step 10	**frame-relay interface-dlci** *dlci* **Example:** Router(config-subif)# frame-relay interface-dlci 28 Router(config-fr-dlci)#	Creates the specified DLCI on the subinterface and enters DLCI configuration mode. • *dlci*—DLCI number to be used on the specified subinterface. **Note** This command includes other options that are not supported when using multipoint bridging.
Step 11	**bridge-domain** *vlan-id* [**access** | **dot1q** | **dot1q-tunnel**] [**split-horizon**] **Example:** Router(config-fr-dlci)# bridge-domain 100 dot1q-tunnel Router(config-fr-dlci)#	Enables RFC 1490 bridging to map a bridged VLAN to a PVC. The following options are supported: **Note** This command has additional options that are not supported in a multipoint bridging configuration. • *vlan-id*—Number of VLAN to be used in this bridging configuration. The valid range is from 2 to 4094 (but the VLAN ID must have been previously added to the VLAN database in Step 3). **Note** This is the default configuration; frames are not tagged with the dot1q header but STPs and BPDUs are transmitted. • **access**—Enables bridging access mode, so that the bridged connection does not act on or transmit BPDUs. • **dot1q**—(Optional) Terminates dot1q traffic. Also enables IEEE 802.1Q tagging to preserve the class of service (CoS) information from the Ethernet frames across the ATM network. Without this option, the COS values are not preserved. • **dot1q-tunnel**—(Optional) Enables IEEE 802.1Q tunneling mode, so that service providers can use one VLAN to support customers with multiple VLANs, as well as accept untagged frames. **Note** The **access**, **dot1q**, and **dot1q-tunnel** options are mutually exclusive. If you do not specify any of these options, the connection operates in “raw” bridging access mode, which is similar to **access**, except that the connection does act on and transmit BPDU packets. **Note** **split-horizon**—(Optional) Enables RFC 1490 split horizon mode to globally prevent bridging between PVCs in the same VLAN.
Step 12	**end** **Example:** Router(config-fr-dlci)# **end** Router#	Exits DLCI configuration mode and returns to privileged EXEC mode.

The following is an example of a Multipoint Bridging configuration on a Frame-Relay interface:

```
frame-relay switching
...
!
interface POS3/8
 no ip address
 encapsulation frame-relay ietf
 logging event link-status
 mls qos trust dscp
 clock source internal
 frame-relay intf-type dce
!
interface POS3/8.10 multipoint
 mls qos trust dscp
 frame-relay interface-dlci 120
  bridge-domain 100 dot1q-tunnel
 frame-relay interface-dlci 130
  bridge-domain 100 dot1q-tunnel
```

Configuring Strict Priority LLQ Support on POS Optical Service Modules

Starting with Cisco IOS Release 12.2(18)SXE, the Low Latency Queuing feature is changed for the Packet over SONET (POS) Optical Services Modules. With this change, priority queue policing is supported on these OSMs. Using Hierarchical Queuing Framework (HQF), the **police** command is combined with strict priority in a class on the OSM.

Note This command is supported on the OC-3 and OC-12 modules. It is not supported on the OC-48 modules. The **priority percent** *%* and **priority** *kbps* commands from previous releases are no longer supported on the OC-3 and OC-12 modules. However, these commands are still supported on the POS OC-48 OSM.

If a second priority police class is included in the policy, police must be configured first.

To configure strict priority LLQ support, perform the following tasks, starting in global configuration mode:

	Command or Action	Purpose

Step 1	`Router(config)# policy-map policy-name`
	Example:
	`Router(config)# policy-map policy11`
		Specifies the name of the policy map to be created or modified.

Step 2	`Router(config-pmap)# class class-name`
	Example:
	`Router(config)# class class204`
		Specifies the name of a predefined class included in the service policy.

	Command or Action	Purpose
Step 3	`Router(config-pmap-c)#` **`priority`** **Example:**`Router(config)# priority`	Configures the strict priority class.

Step 4	`Router(config-pmap-c)#` **`police`** *`rate`*
	
	Example:
	`Router(config-pmap-c) # police 1000000#`
		Sets the policing rate (in bps).

Examples

The following example shows a typical configuration and verification for the supported POS OSMs:

```
!
 Policy Map child-pos
   Class prec1
     priority
    police cir 1000000 bc 31250 be 31250 conform-action transmit exceed-action drop
   Class prec2
     bandwidth remaining 50 (%)
   Class prec3
     bandwidth remaining 30 (%)
   Class class-default
     bandwidth remaining 20 (%)
!
   Class class-default
     bandwidth 2200 (kbps)
     shape average 3000000 12000 12000
     service-policy child-pos
!
interface POS3/2
no ip address
encapsulation frame-relay
mls qos trust dscp
clock source internal
end
!
interface POS3/2.16 point-to-point
ip address 25.0.0.1 255.255.255.0
mls qos trust dscp
no cdp enable
frame-relay interface-dlci 16
service-policy output parent-pos
end
```

The following show command verifies the configuration:

```
Router #show policy interface pos3/2.16

POS3/2.16

 Service-policy output:parent-pos

   Class-map:class-default (match-any)
     0 packets, 0 bytes
     5 minute offered rate 0 bps, drop rate 0 bps
     Match:any
     Queueing
     queue limit 550 (packets)
     (queue depth/total drops/no-buffer drops) 0/0/0
     (pkts queued/bytes queued) 0/0
     bandwidth 2200 kbps
     shape (average) cir 3000000, bc 12000, be 12000
     target shape rate 3000000
     (shape parameter is rounded to 2944000 bps due to granularity)
       lower bound cir 0,  adapt to fecn 0

     Service-policy :child-pos

       Class-map:prec1 (match-all)
         0 packets, 0 bytes
         5 minute offered rate 0 bps, drop rate 0 bps
         Match:ip precedence 1
         Priority:b/w exceed drops:0
         police:
             cir 1000000 bps, bc 31250 bytes
           (Police cir is rounded to 983040 bps due to granularity)

       Class-map:prec2 (match-all)
         0 packets, 0 bytes
         5 minute offered rate 0 bps, drop rate 0 bps
         Match:ip precedence 2
         Queueing
         queue limit 150 (packets)
         (queue depth/total drops/no-buffer drops) 0/0/0
         (pkts queued/bytes queued) 0/0
         bandwidth remaining 50% (600 kbps)
         (bandwidth parameter is rounded to 504 kbps due to granularity)

       Class-map:prec3 (match-all)
         0 packets, 0 bytes
         5 minute offered rate 0 bps, drop rate 0 bps
         Match:ip precedence 3
         Queueing
         queue limit 90 (packets)
         (queue depth/total drops/no-buffer drops) 0/0/0
         (pkts queued/bytes queued) 0/0
         bandwidth remaining 30% (360 kbps)
         (bandwidth parameter is rounded to 300 kbps due to granularity)

       Class-map:class-default (match-any)
         0 packets, 0 bytes
         5 minute offered rate 0 bps, drop rate 0 bps
         Match:any
         Queueing
         queue limit 60 (packets)
         (queue depth/total drops/no-buffer drops) 0/0/0
         (pkts queued/bytes queued) 0/0
         bandwidth remaining 20% (240 kbps)
         (bandwidth parameter is rounded to 197 kbps due to granularity)
Router#
```