



CHAPTER 13

Configuring the POS SPAs

This chapter provides information about configuring the Packet over SONET (POS) shared port adapters (SPAs) on the Catalyst 6500 Series switch. This chapter includes the following sections:

- [Configuration Tasks, page 13-1](#)
- [Verifying the Interface Configuration, page 13-18](#)
- [Configuration Examples, page 13-18](#)

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.

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 xliv](#).

Configuration Tasks

This section describes how to configure POS SPAs and includes information about verifying the configuration.

It includes the following topics:

- [Required Configuration Tasks, page 13-2](#)
- [Specifying the Interface Address on a SPA, page 13-3](#)
- [Modifying the Interface MTU Size, page 13-4](#)
- [Modifying the POS Framing, page 13-5](#)
- [Modifying the Keepalive Interval, page 13-7](#)
- [Modifying the CRC Size, page 13-7](#)
- [Modifying the Clock Source, page 13-8](#)
- [Modifying SONET Payload Scrambling, page 13-9](#)
- [Configuring the Encapsulation Type, page 13-10](#)
- [Configuring APS, page 13-11](#)
- [Configuring POS Alarm Trigger Delays, page 13-12](#)
- [Configuring SDCC, page 13-15](#)

- [Configuring Layer 2 Internetworking Features on POS SPAs, page 13-16](#)
- [Saving the Configuration, page 13-17](#)
- [Shutting Down and Restarting an Interface on a SPA, page 13-18](#)

Required Configuration Tasks

This section lists the required configuration steps to configure the POS SPAs. 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.

To configure the POS SPAs, perform this task:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# interface pos <i>slot/subslot/port</i>	Specifies the POS interface to configure and enters interface configuration mode, where: • <i>slot/subslot/port</i>—Specifies the location of the interface. See the “Specifying the Interface Address on a SPA” section on page 13-3.
Step 3	Router(config-if)# ip address <i>ip-address mask [secondary]</i>	Sets a primary or secondary IP address for an interface, where: • <i>ip-address</i>—Specifies the IP address for the interface. • <i>mask</i>—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.
Step 4	Router(config-if)# pos framing {sonet sdh}	(As Required) Specifies the POS framing type, where: • sonet—Enables Synchronous Optical Network Framing for optical carrier (OC) rates. This is the default. • sdh—Enables Synchronous Digital Hierarchy framing for synchronous transfer mode (STM) rates. The POS framing type must be configured to be the same on both ends of the POS link.
Step 5	Router(config-if)# mtu bytes	(As Required) Configures the maximum transmission unit (or packet size) for an interface, where: • <i>bytes</i>—Specifies the maximum number of bytes for a packet. The default is 4470 bytes.

	Command	Purpose
Step 6	Router(config-if)# keepalive [<i>period</i> [<i>retries</i>]]	(As Required) Specifies the frequency at which the Cisco IOS software sends messages to the other end of the link, to ensure that a network interface is alive, where: <i>period</i>—Specifies the time interval in seconds for sending keepalive packets. The default is 10 seconds. <i>retries</i>—Specifies the number of times that the device will continue to send keepalive packets without response before bringing the interface down. The default is 5 retries. The keepalive must be configured to be the same on both ends of the POS link.
Step 7	Router(config-if)# crc [16 32]	(As Required) Specifies the length of the cyclic redundancy check (CRC), where: 16—Specifies a 16-bit length CRC. This is the default. 32—Specifies a 32-bit length CRC. The CRC size must be configured to be the same on both ends of the POS link.
Step 8	Router(config-if)# clock source { line internal }	(As Required) Specifies the clock source for the POS link, where: line—The link uses the recovered clock from the line. This is the default. internal—The link uses the internal clock source.
Step 9	Router(config-if)# encapsulation <i>encapsulation-type</i>	(As Required) Specifies the encapsulation method used by the interface, where: <i>encapsulation-type</i>—Can be HDLC, PPP, or Frame Relay. The default encapsulation is HDLC. The encapsulation must be configured to be the same on both ends of the POS link. Note: The POS SPAs on the Cisco 7600 SIP-600 do not support Frame Relay.
Step 10	Router(config-if)# pos scramble-atm	(As Required) Enables SONET payload scrambling. The default configuration is SONET payload scrambling disabled. The SONET payload scrambling must be configured to be the same on both ends of the POS link.
Step 11	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.

For more information about identifying slots and subslots, see the [“Identifying Slots and Subslots for SIPs, SSCs, and SPAs” section on page 4-2](#).

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 three bytes of payload size, 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, for an Ethernet packet, 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).

Interface MTU Configuration Guidelines

When configuring the interface MTU size on the POS SPAs, consider the following guidelines:

- If you are also using MPLS, be sure that the **mpls mtu** command is configured for a value less than or equal to the interface MTU.
- If you change the interface MTU size, the giant counter increments when the interface receives a packet that exceeds the MTU size that you configured, plus an additional 88 bytes for overhead, and an additional 2 or 4 bytes for the configured cyclic redundancy check (CRC).

For example, with a maximum MTU size of 9216 bytes, the giant counter increments:

- For a 16-bit CRC (or FCS), when receiving packets larger than 9306 bytes (9216 + 88 + 2).
- For a 32-bit CRC, when receiving packets larger than 9308 bytes (9216 + 88 + 4).

- The Frame Relay Local Management Interface (LMI) protocol requires that all permanent virtual circuit (PVC) status reports fit into a single packet. Using the default MTU of 4470 bytes, this limits the number of data-link connection identifiers (DLCIs) to 890. The following formula demonstrates how to determine the maximum DLCIs for a configured interface MTU:
 - Maximum DLCIs = (MTU bytes – 20)/(5 bytes per DLCI)
 - Maximum DLCIs for the default MTU = (4470 – 20)/5 = 890 DLCIs per interface

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 <i>bytes</i>	Configures the maximum packet size for an interface, where: • <i>bytes</i>—Specifies the maximum number of bytes for a packet. The default is 4470 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 pos** privileged EXEC command and observe the value shown in the MTU field.

The following example shows an MTU size of 4470 bytes for interface port 0 (the first port) on the SPA installed in subslot 1 of the SIP that is located in slot 2 of the Catalyst 6500 Series switch:

```
Router# show interfaces pos 2/1/0
POS2/1/0 is up, line protocol is up (APS working - active)
  Hardware is Packet over Sonet
  Internet address is 10.1.1.1/24
  MTU 4470 bytes, BW 155000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255.
.
.
.
```

Modifying the POS Framing

POS framing can be specified as SONET (Synchronous Optical Network) or SDH (Synchronous Digital Hierarchy). SONET and SDH are a set of related standards for synchronous data transmission over fiber-optic networks. SONET is the United States version of the standard published by the American National Standards Institute (ANSI). SDH is the international version of the standard published by the International Telecommunications Union (ITU).

To modify the POS framing, perform this task in interface configuration mode:

Command	Purpose
Router(config-if)# pos framing {sonet sdh}	Specifies the POS framing type, where: • sonet—Enables Synchronous Optical Network framing for optical carrier (OC) rates. This is the default. • sdh—Enables Synchronous Digital Hierarchy framing for synchronous transfer mode (STM) rates. The POS framing type must be configured to be the same on both ends of the POS link.

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

Verifying the POS Framing

To verify the POS framing, use the **show controllers pos** privileged EXEC command and observe the value shown in the Framing field. The following example shows that POS framing mode is set to SONET for the first interface (0) on the POS SPA installed in subslot 2 of a SIP installed in chassis slot 3:

```
Router# show controllers pos 3/2/0
POS3/2/0
SECTION
LOF = 0 LOS = 0 BIP(B1) = 0
LINE
AIS = 0 RDI = 0 FEBE = 0 BIP(B2) = 0
PATH
AIS = 0 RDI = 0 FEBE = 0 BIP(B3) = 0
PLM = 0 UNEQ = 0 TIM = 0 TIU = 0
LOP = 0 NEWPTR = 0 PSE = 0 NSE = 0

Active Defects: None
Active Alarms: None
Alarm reporting enabled for: SF SLOS SLOF B1-TCA B2-TCA PLOP B3-TCA

Framing: SONET
APS

COAPS = 0 PSBF = 0
State: PSBF_state = False
Rx(K1/K2): 00/00 Tx(K1/K2): 00/00
Rx Synchronization Status S1 = 00
S1S0 = 00, C2 = CF
Remote aps status (none); Reflected local aps status (none)
CLOCK RECOVERY
RDOOL = 0
State: RDOOL_state = False
PATH TRACE BUFFER: STABLE
Remote hostname : sip-sw-7600-2
Remote interface: POS3/2/1
Remote IP addr : 0.0.0.0
Remote Rx(K1/K2): 00/00 Tx(K1/K2): 00/00

BER thresholds: SF = 10e-3 SD = 10e-6
TCA thresholds: B1 = 10e-6 B2 = 10e-6 B3 = 10e-6
```

Clock source: internal

Modifying the Keepalive Interval

When the keepalive feature is enabled, a keepalive packet is sent at the specified time interval to keep the interface active. The keepalive interval must be configured to be the same on both ends of the POS link.

To modify the keepalive interval, perform this task in interface configuration mode:

Command	Purpose
Router(config-if)# keepalive [<i>period</i> [<i>retries</i>]]	Specifies the frequency at which the Cisco IOS software sends messages to the other end of the link, to ensure that a network interface is alive, where: • <i>period</i>—Specifies the time interval in seconds for sending keepalive packets. The default is 10 seconds. • <i>retries</i>—Specifies the number of times that the device will continue to send keepalive packets without response before bringing the interface down. The default is 5 retries.

To disable keepalive packets, use the **no** form of this command.

Verifying the Keepalive Interval

To verify the keepalive interval, use the **show interfaces pos** privileged EXEC command and observe the value shown in the Keepalive field.

The following example shows that keepalive is enabled for interface port 0 on the POS SPA installed in the SIP that is located in slot 2 of the Catalyst 6500 Series switch:

```
Router# show interfaces pos 2/0/0
  Hardware is Packet over Sonet
  Internet address is 10.1.1.1.2
  MTU 9216 bytes, BW 622000 Kbit, DLY 100 usec, reliability 255/255, txload 1/255,
  rxload 1/255
    Keepalive set (10 sec)
  .
  .
  .
```

Modifying the CRC Size

CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data. The CRC size indicates the length in bits of the FCS.

The CRC size must be configured to be the same on both ends of the POS link.

To modify the CRC size, perform this task in interface configuration mode:

Command	Purpose
Router(config-if)# crc [16 32]	(As Required) Specifies the length of the cyclic redundancy check (CRC), where: • 16—Specifies a 16-bit length CRC. This is the default. • 32—Specifies a 32-bit length CRC. The CRC size must be configured to be the same on both ends of the POS link.

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

Verifying the CRC Size

To verify the CRC size, use the **show interfaces pos** privileged EXEC command and observe the value shown in the CRC field.

The following example shows that the CRC size is 16 for interface port 0 on the POS SPA installed in the SIP that is located in slot 2 of the Catalyst 6500 Series switch:

```
Router# show interfaces pos 2/0/0
  Hardware is Packet over Sonet
  Internet address is 10.1.1.2.1
  MTU 9216 bytes, BW 622000 Kbit, DLY 100 usec, reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
.
.
.
```

Modifying the Clock Source

A clock source of internal specifies that the interface clocks its transmitted data from its internal clock. A clock source of line specifies that the interface clocks its transmitted data from a clock recovered from the line's receive data stream.

For information about the recommended clock source settings for POS switch interfaces, refer to *Configuring Clock Settings on POS Router Interfaces* at the following URL:

http://www.cisco.com/en/US/tech/tk482/tk607/technologies_tech_note09186a0080094bb9.shtml

To modify the clock source, perform this task in interface configuration mode:

Command	Purpose
Router(config-if)# clock source {line internal}	Specifies the clock source for the POS link, where: • line—The link uses the recovered clock from the line. This is the default. • internal—The link uses the internal clock source.

To return to the default clock source, use the **no** form of this command.

Verifying the Clock Source

To verify the clock source, use the **show controllers pos** privileged EXEC command and observe the value shown in the Clock source field.

The following example shows that the clock source is internal for interface port 0 on the POS SPA installed in subslot 0 of the SIP that is located in slot 2 of the Catalyst 6500 Series switch:

```
Router# show controllers pos 2/0/0
POS2/0/0
SECTION
LOF = 0 LOS = 1 BIP(B1) = 7
LINE
AIS = 0 RDI = 1 FEBE = 20 BIP(B2) = 9
PATH
AIS = 0 RDI = 0 FEBE = 0 BIP(B3) = 5
PLM = 0 UNEQ = 0 TIM = 0 TIU = 0
LOP = 0 NEWPTR = 0 PSE = 0 NSE = 0

Active Defects: None
Active Alarms: None

Alarm reporting enabled for: SF SLOS SLOF B1-TCA LAIS LRDI B2-TCA PAIS PLOP PRDI PUNEQ
B3-TCA RDOOL

APS

COAPS = 2 PSBF = 0
State: PSBF_state = False
Rx(K1/K2): 00/00 Tx(K1/K2): 00/00
Rx Synchronization Status S1 = 00
S1S0 = 02, C2 = CF
CLOCK RECOVERY
RDOOL = 0
State: RDOOL_state = False
PATH TRACE BUFFER: STABLE
Remote hostname : RouterTester. Port 102/1
Remote interface:
Remote IP addr :
Remote Rx(K1/K2): / Tx(K1/K2): /

BER thresholds: SF = 10e-5 SD = 10e-6
TCA thresholds: B1 = 10e-6 B2 = 10e-6 B3 = 10e-6

Clock source: internal
.
.
.
```

Modifying SONET Payload Scrambling

SONET payload scrambling applies a self-synchronous scrambler (x43+1) to the Synchronous Payload Envelope (SPE) of the interface to ensure sufficient bit transition density.

The default configuration is SONET payload scrambling disabled.

SONET payload scrambling must be configured to be the same on both ends of the POS link.

To modify SONET payload scrambling, perform this task in interface configuration mode:

Command	Purpose
Router(config-if)# pos scramble-atm	Enables SONET payload scrambling.

To disable SONET payload scrambling, use the **no** form of this command.

Verifying SONET Payload Scrambling

To verify SONET payload scrambling, use the **show interfaces pos** privileged EXEC command and observe the value shown in the Scramble field.

The following example shows that SONET payload scrambling is disabled for interface port 0 on the POS SPA installed in subslot 0 of the SIP that is located in slot 2 of the Catalyst 6500 Series switch:

```
Router# show interfaces pos 2/0/0
  Hardware is Packet over Sonet
  Internet address is 10.0.0.1/24
  MTU 9216 bytes, BW 622000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive not set
  Scramble disabled
.
.
.
```

Configuring the Encapsulation Type

By default, the POS interfaces support High-Level Data Link Control (HDLC) encapsulation. The encapsulation method can be specified as HDLC, Point-to-Point Protocol (PPP) or Frame Relay. The encapsulation type must be configured to be the same on both ends of the POS link.

To modify the encapsulation method, perform this task in interface configuration mode:

Command	Purpose
Router(config-if)# encapsulation <i>encapsulation-type</i>	Specifies the encapsulation method used by the interface, where: <i>encapsulation-type</i>—Can be HDLC, PPP, or Frame Relay. The default is HDLC.

Verifying the Encapsulation Type

To verify the encapsulation type, use the **show interfaces pos** privileged EXEC command and observe the value shown in the Encapsulation field.

The following example shows the encapsulation type is HDLC for port 0 on the POS SPA installed in subslot 0 of the SIP that is located in slot 2 of the Catalyst 6500 Series switch:

```
Router# show interfaces pos 2/0/0
  Hardware is Packet over Sonet
  Internet address is 10.0.0.1/24
  MTU 9216 bytes, BW 622000 Kbit, DLY 100 usec,
```

```

reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, crc 16, loopback not set
  Keepalive not set
  Scramble disabled
.
.
.

```

Configuring APS

Automatic protection switching (APS) allows switchover of POS circuits in the event of circuit failure and is often required when connecting SONET equipment to telco equipment. APS refers to the method of using a protect POS interface in the SONET network as the backup for a working POS interface. When the working interface fails, the protect interface quickly assumes its traffic load. Depending on the configuration, the two circuits may be terminated in the same switch, or in different switches.

For more information about APS, refer to *A Brief Overview of Packet Over SONET APS* at the following URL:

http://www.cisco.com/en/US/tech/tk482/tk607/technologies_tech_note09186a0080093eb5.shtml

To configure the working POS interface, perform this task in interface configuration mode:

Command	Purpose
Router(config-if)# aps working <i>circuit-number</i>	Configures a POS interface as a working APS interface, where: <i>circuit-number</i>—Specifies the circuit number associated with this working interface.

To remove the POS interface as a working interface, use the **no** form of this command.

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

Command	Purpose
Router(config-if)# aps protect <i>circuit-number ip-address</i>	Configures a POS interface as a protect APS interface, where: <i>circuit-number</i>—Specifies the number of the circuit to enable as a protect interface. <i>ip-address</i>—Specifies the IP address of the switch that has the working POS interface.

To remove the POS interface as a protect interface, use the **no** form of this command.

Verifying the APS Configuration

To verify the APS configuration or to determine if a switchover has occurred, use the **show aps** command.

The following is an example of a switch configured with a working interface. In this example, POS interface 0/0/0 is configured as a working interface in group 1, and the interface is selected (that is, active).

```
Router# show aps
POS0/0/0 working group 1 channel 1 Enabled Selected
```

The following is an example of a switch configured with a protect interface. In this example, POS interface 2/1/1 is configured as a protect interface in group 1. The output also shows that the working channel is located on the switch with the IP address 10.0.0.1 and that the interface currently selected is enabled.

```
Router# show aps
POS2/1/1 APS Group 1: protect channel 0 (inactive)
Working channel 1 at 10.0.0.1 (Enabled)
  SONEt framing; SONEt APS signalling by default
  Remote APS configuration: (null)
.
.
.
```

Configuring POS Alarm Trigger Delays

A trigger is an alarm that when activated causes the line protocol to go down. The POS alarm trigger delay helps to ensure uptime of a POS interface by preventing intermittent problems from disabling the line protocol. The POS alarm trigger delay feature delays the setting of the line protocol to down when trigger alarms are received. If the trigger alarm was sent because of an intermittent problem, the POS alarm trigger delay can prevent the line protocol from going down when the line protocol is functional.

Line-Level and Section-Level Triggers

The **pos delay triggers line** command is used for POS switch interfaces connected to internally protected Dense Wavelength Division Multiplexing (DWDM) systems. This command is invalid for interfaces that are configured as working or protect APS. Normally, a few microseconds of line- or section-level alarms brings down the link until the alarm has been clear for ten seconds. If you configure holdoff, the link-down trigger is delayed for 100 milliseconds. If the alarm stays up for more than 100 milliseconds, the link is brought down. If the alarm clears before 100 milliseconds, the link remains up.

The following line- and section-level alarms are triggers, by default, for the line protocol to go down:

- Line alarm indication signal (LAIS)
- Section loss of signal (SLOS)
- Section loss of frame (SLOF)

You can use the **pos delay triggers line** command to delay a down trigger of the line protocol on the interface. You can set the delay from 50 to 10000 milliseconds. The default delay is 100 milliseconds.

To configure POS line- or section-level triggers, perform this task beginning in interface configuration mode:

	Command	Purpose
Step 1	Router(config-if)# pos delay triggers line <i>ms</i>	Specifies a delay for setting the line protocol to down when a line-level trigger alarm is received, where: <i>ms</i>—Specifies the delay in milliseconds. The default delay is 100 milliseconds.
Step 2	Router(config-if)# pos threshold { b1-tca b2-tca b3-tca sd-ber sf-ber } <i>rate</i>	Configures the POS bit error rate (BER) threshold values of the specified alarms, where: b1-tca rate—Specifies the B1 BER threshold crossing alarm. The default is 6. b2-tca rate—Specifies the B2 BER threshold crossing alarm. The default is 6. b3-tca rate—Specifies the B3 BER threshold crossing alarm. The default is 6. sd-ber rate—Specifies the signal degrade BER threshold. The default is 6. sf-ber rate—Specifies the signal failure BER threshold. The default is 3. <i>rate</i>—Specifies the bit error rate from 3 to 9 (10e-n). The default varies by the type of threshold that you configure.
Step 3	Router(config-if)# pos ais-shut	Sends a line alarm indication signal (AIS-L) to the other end of the link after a shutdown command has been issued to the specified POS interface. AIS-L is also known as LAIS when alarm-related output is generated using the show controllers pos command. By default, the AIS-L is not sent to the other end of the link. Stops transmitting the AIS-L by issuing either the no shutdown or the no pos ais-shut commands.

To disable alarm trigger delays, use the **no** form of the **pos delay triggers line** command.

To determine which alarms are reported on the POS interface, and to display the BER thresholds, use the **show controllers pos** command.

Path-Level Triggers

To configure various path alarms as triggers and to specify an activation delay between 50 and 10000 milliseconds, use the **pos delay triggers path** command. The default delay value is 100 milliseconds. The following path alarms are not triggers by default. You can configure these path alarms as triggers and also specify a delay:

- Path alarm indication signal (PAIS)
- Path remote defect indication (PRDI)
- Path loss of pointer (PLOP)

- sd-ber (signal degrade [SD] bit error rate [BER])
- sf-ber (signal failure [SF] BER)
- b1-tca (B1 BER threshold crossing alarm [TCA])
- b2-tca (B2 BER TCA)
- b3-tca (B3 BER TCA)

The **pos delay triggers path** command can also bring down the line protocol when the higher of the B2 and B3 error rates is compared with the signal failure (SF) threshold. If the SF threshold is crossed, the line protocol of the interface goes down.

To configure POS path-level triggers, perform this task in interface configuration mode:

Command	Purpose
Router(config-if)# pos delay triggers path <i>ms</i>	Specifies that path-level alarms should act as triggers and specifies a delay for setting the line protocol to down when a path-level trigger alarm is received, where: • <i>ms</i>—Specifies the delay in milliseconds. The default delay is 100 milliseconds.

To disable path-level triggers, use the **no** form of this command.

Verifying POS Alarm Trigger Delays

To verify POS alarm trigger delays, use the **show controllers pos** privileged EXEC command and observe the values shown in the Line alarm trigger delay and Path alarm trigger delay fields.

The following example shows the POS alarm trigger delays for interface port 0 on the POS SPA installed in the SIP that is located in slot 2 of the Catalyst 6500 Series switch:

```
Router# show controllers pos 2/0/0 details
POS2/0/0
SECTION
LOF = 0 LOS = 1 BIP(B1) = 5
LINE
AIS = 0 RDI = 1 FEBE = 5790 BIP(B2) = 945
PATH
AIS = 0 RDI = 0 FEBE = 0 BIP(B3) = 5
PLM = 0 UNEQ = 0 TIM = 0 TIU = 0
LOP = 1 NEWPTR = 0 PSE = 0 NSE = 0

Active Defects: None
Active Alarms: None
Alarm reporting enabled for: SF SLOS SLOF B1-TCA B2-TCA PLOP B3-TCA

Line alarm trigger delay = 100 ms
Path alarm trigger delay = 100 ms
.
.
.
```

Configuring SDCC

Before any management traffic can traverse the section data communication channel (SDCC) links embedded in the POS SPA overhead, the SDCC interfaces must be configured and activated.



Note

SDCC is not supported by the 1-Port OC-48c/STM-16 POS SPA on the Cisco 7600 SIP-400 and is not supported by any POS SPAs on the Cisco 7600 SIP-600.

SDCC Configuration Guidelines

When configuring SDCC on a POS SPA, consider the following guidelines:

- SDCC must be enabled on the main POS interfaces.
- SDCC can be configured on up to two interfaces of the 4-Port OC-3c/STM-1 POS SPA.
- SDCC supports only HDLC and PPP encapsulation, not Frame Relay.

SDCC Configuration Task

To configure the POS SPAs for SDCC, perform this task:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# interface pos <i>slot/subslot/port</i>	Specifies the POS interface to configure and enters interface configuration mode, where: • <i>slot/subslot/port</i>—Specifies the location of the interface. See the “Specifying the Interface Address on a SPA” section on page 13-3.
Step 3	Router(config-if)# sdcc enable	Enables SDCC on the interface.
Step 4	Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.
Step 5	Router(config)# interface sdcc <i>slot/subslot/port</i>	Specifies the SDCC interface and enters interface configuration mode, where: • <i>slot/subslot/port</i>—Specifies the location of the interface. See the “Specifying the Interface Address on a SPA” section on page 13-3.

	Command	Purpose
Step 6	Router(config-if)# ip address <i>ip-address</i> <i>mask</i> [secondary]	Sets a primary or secondary IP address for an interface, where: <i>ip-address</i>—Specifies the IP address for the interface. <i>mask</i>—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.
Step 7	Router(config-if)# no shutdown	Enables the interface.

Verifying the SDCC Interface Configuration

To verify the SDCC interface, use the **show interfaces sdcc** privileged EXEC command and observe the value shown in the Hardware is field.

The following example shows the SDCC interface port 1 on the POS SPA installed in subslot 0 of the SIP that is located in slot 5 of the Catalyst 6500 Series switch:

```
Router# show interfaces sdcc 5/0/1
SDCC5/0/1 is up, line protocol is up
  Hardware is SDCC
    Internet address is 10.14.14.14/8
    MTU 1500 bytes, BW 155000 Kbit, DLY 20000 usec,
        reliability 5/255, txload 1/255, rxload 1/255
    Encapsulation HDLC, crc 16, loopback not set
    Keepalive not set
    Last input 00:01:24, output never, output hang never
    Last clearing of 'show interface' counters 00:01:30
    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
    5 packets input, 520 bytes, 0 no buffer
        Received 0 broadcasts (0 IP multicast)
        0 runs, 0 giants, 0 throttles
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    5 packets output, 520 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 output buffer failures, 0 output buffers swapped out
        0 carrier transitions
```

Configuring Layer 2 Internetworking Features on POS SPAs

This section provides information about the Layer 2 internetworking features that are supported by the POS SPAs on the Catalyst 6500 Series switch.

Configuring Multipoint Bridging

Multipoint bridging (MPB) enables the connection of multiple ATM PVCs, Frame Relay PVCs, BCP ports, and WAN Gigabit Ethernet subinterfaces into a single broadcast domain (virtual LAN), together with the LAN ports on that VLAN. This feature enables service providers to add support for Ethernet-based Layer 2 services to the proven technology of their existing ATM and Frame Relay legacy networks. Customers can then use their current VLAN-based networks over the ATM or Frame Relay cloud. This feature also allows service providers to gradually update their core networks to the latest Gigabit Ethernet optical technologies, while still supporting their existing customer base.

For MPB configuration guidelines and restrictions and feature compatibility tables, see the [“Configuring Multipoint Bridging”](#) section on page 4-17 of Chapter 4, “Configuring the SIPs and SSC.”

Configuring the Bridging Control Protocol

The 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 SPAs includes support for IEEE 802.1D, IEEE 802.1Q Virtual LAN (VLAN), and high-speed switched LANs.

For BCP configuration guidelines and restrictions and feature compatibility tables, see the [“Configuring PPP Bridging Control Protocol Support”](#) section on page 4-18 of Chapter 4, “Configuring the SIPs and SSC.”

Configuring Virtual Private LAN Service (VPLS) and Hierarchical VPLS

VPLS enables geographically separate LAN segments to be interconnected as a single bridged domain over a packet switched network, such as IP, MPLS or hybrid of both bridging techniques.

VPLS with EoMPLS uses an MPLS-based provider core, where the PE routers have to cooperate to forward customer Ethernet traffic for a given VPLS instance in the core. VPLS uses 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 VPLS and H-VPLS configuration guidelines and restrictions and feature compatibility tables, see the [Configuring Virtual Private LAN Service \(VPLS\)](#), page 4-23 of Chapter 4, “Configuring the SIPs and SSC.”

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 more information about managing 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 then enters the interface into an administratively down state.

If you are preparing for an OIR of a SPA, it is not necessary to independently shut down each of the interfaces prior to deactivation of the SPA. You do not need to independently restart any interfaces on a SPA after OIR of a SPA or SIP. For more information about performing an OIR for a SPA, see the [“Preparing for Online Insertion and Removal of SIPs, SSCs, and SPAs”](#) section on page 5-3.

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

Besides using the **show running-configuration** command to display your Catalyst 6500 Series switch configuration settings, you can use the **show interfaces pos** and **show controllers pos** commands to get detailed information on a per-port basis for your POS SPAs.

Verifying Per-Port Interface Status

To find detailed interface information on a per-port basis for the POS SPAs, use the **show interfaces pos** command. For a description of the command output, see the *Catalyst 6500 Series Cisco IOS Command Reference, 12.2SX*.

Monitoring Per-Port Interface Statistics

To find detailed alarm and error information on a per-port basis for the POS SPAs, use the **show controllers pos** command. For a description of the command output, see the *Catalyst 6500 Series Cisco IOS Command Reference, 12.2SX*.

Configuration Examples

This section includes the following examples for configuring a POS SPA installed in a Catalyst 6500 Series switch:

- [Basic Interface Configuration Example, page 13-19](#)
- [MTU Configuration Example, page 13-19](#)
- [POS Framing Configuration Example, page 13-20](#)

- [Keepalive Configuration Example, page 13-20](#)
- [CRC Configuration Example, page 13-20](#)
- [Clock Source Configuration Example, page 13-21](#)
- [SONET Payload Scrambling Configuration Example, page 13-21](#)
- [Encapsulation Configuration Example, page 13-21](#)
- [APS Configuration Example, page 13-21](#)
- [POS Alarm Trigger Delays Configuration Example, page 13-23](#)
- [SDCC Configuration Example, page 13-23](#)

Basic Interface Configuration Example

The following example shows how to enter global configuration mode to enter global configuration mode to specify the interface that you want to configure, configure an IP address for the interface, enable the interface, and save the configuration. This example configures interface port 0 (the first port) of the SPA located in subslot 0 of the SIP that is installed in slot 2 of the Catalyst 6500 Series switch:

```
!Enter global configuration mode
!
Router# configure terminal
!
! Specify the interface address
!
Router(config)# interface pos 2/0/0
!
! Configure an IP address
!
Router(config-if)# ip address 192.168.50.1 192.255.255.0
!
! Enable the interface
!
Router(config-if)# no shutdown
!
! Save the configuration to NVRAM
!
Router(config-if)# exit
Router# copy running-config startup-config
```

MTU Configuration Example

The following example sets the MTU to 4470 bytes on interface port 1 (the second port) of the SPA located in the bottom subslot (1) of the SIP that is installed in slot 2 of the Catalyst 6500 Series switch:

```
!Enter global configuration mode
!
Router# configure terminal
!
! Specify the interface address
!
Router(config)# interface pos 2/1/1
!
! Configure MTU
!
Router(config-if)# mtu 4470
```

POS Framing Configuration Example

The following example shows how to change from the default POS framing of SONET to SDH:

```
!Enter global configuration mode
!
Router# configure terminal
!
! Specify the interface address
!
Router(config)# interface pos 2/1/1
! (The default pos framing is sonet)
!
!Modify the framing type
!
Router(config-if)# pos framing sdh
```

Keepalive Configuration Example

The following example shows how to change from the default keepalive period of 10 seconds to 20 seconds:

```
!Enter global configuration mode
!
Router# configure terminal
!
! Specify the interface address
!
Router(config)# interface pos 2/1/1
!
! Configure keepalive 20
!
Router(config-if)# keepalive 20
```

CRC Configuration Example

The following example shows how to change the CRC size from 32 bits to the default 16 bits for POS SPAs:

```
!Enter global configuration mode
!
Router# configure terminal
!
! Specify the interface address
!
Router(config)# interface pos 2/1/1
!
! Configure crc 16
!
Router(config-if)# crc 16
```

Clock Source Configuration Example

The following example shows how to change from the default clock source of internal to line:

```
!Enter global configuration mode
!
Router# configure terminal
!
! Specify the interface address
!
Router(config)# interface pos 2/1/1
!
! Configure the clock source
!
Router(config-if)# clock source line
```

SONET Payload Scrambling Configuration Example

The following example shows how to change from a default SONET payload scrambling of disabled to enabled:

```
!Enter global configuration mode
!
Router# configure terminal
!
! Specify the interface address
!
Router(config)# interface pos 2/1/1
!
! Configure the SONET payload scrambling
!
Router(config-if)# pos scramble-atm
```

Encapsulation Configuration Example

The following example shows how to change from the default encapsulation method of HDLC to PPP:

```
!Enter global configuration mode
!
Router# configure terminal
!
! Specify the interface address
!
Router(config)# interface pos 2/1/1
!
! Configure ppp
!
Router(config-if)# encapsulation ppp
```

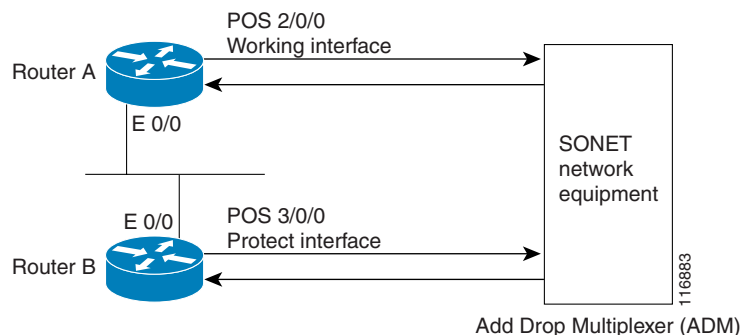
APS Configuration Example

The following example shows the configuration of APS on router A and router B ([Figure 13-1](#)), and how to configure more than one protect or working interface on a router by using the **aps group** command.

**Note**

In the following figure, the devices with the ATM SPAs are shown as Cisco 7600 series routers, but they can also be Catalyst 6500 series switches.

Figure 13-1 Basic APS Configuration



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 loopback interface is used as the interconnect. The **aps group** command is used even when a single protect group is configured.

The following example shows how to configure Router A for this scenario:

```
!Enter global configuration mode
!
Router# configure terminal
!
! Configure a loopback interface as the protect interconnect path
!
Router(config)# interface loopback 1
Router(config-if)# ip address 10.10.10.10 255.0.0.0

! Configure the POS interface address for the APS working interface
!
Router(config)# interface pos 2/0/0
!
! Configure the POS interface IP address and other interface parameters
!
Router(config-if)# ip address 172.16.1.8 255.255.0.0
Router(config-if)# no ip directed-broadcast
Router(config-if)# no keepalive
Router(config-if)# crc 32
!
! Configure the APS group number by which to associate APS interfaces
!
Router(config-if)# aps group 1
!
! Configure a circuit number for the APS working interface
!
Router(config-if)# aps working 1
```

The following example shows how to configure Router B for this scenario:

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

```

! Configure the POS interface address for the APS protect interface
!
Router(config)# interface pos 3/0/0
!
! Configure the POS interface IP address and other interface parameters
!
Router(config-if)# ip address 172.16.1.9 255.255.0.0
Router(config-if)# no ip directed-broadcast
Router(config-if)# no keepalive
Router(config-if)# crc 32
!
! Configure the APS group number by which to associate APS interfaces
!
Router(config-if)# aps group 1
!
! Configure a circuit number for the protect interface and an IP address for the router
! that has the APS working interface. In this case, the loopback interface address is
! used.
!
Router(config-if)# aps protect 1 10.10.10.10

```

POS Alarm Trigger Delays Configuration Example

The following example shows how to change POS line-level and path-level alarm trigger delays from the default of 100 milliseconds to 200 milliseconds:

```

!Enter global configuration mode
!
Router# configure terminal
!
! Specify the interface address
!
Router(config)# interface pos 2/1/1
!
Router(config-if)# pos delay triggers line 200
Router(config-if)# pos delay triggers path 200

```

SDCC Configuration Example



Note

SDCC is not supported by the 1-Port OC-48c/STM-16 POS SPA on the Cisco 7600 SIP-400 and is not supported by any POS SPAs on the Cisco 7600 SIP-600.

The following example shows how to configure an SDCC interface:

```

!Enter global configuration mode
!
Router# configure terminal
!
! Specify the POS interface
!
Router(config)# interface pos 5/0/1
!
! Enable SDCC on the POS interface
!
Router(config-if)# sdcc enable
!
! Exit interface configuration mode and return to

```

```
! global configuration mode
!
Router(config-if# exit
!
! Specify the SDCC interface
!
Router(config)# interface sdcc 5/0/1
!
! Specify the IP address
!
Router(config-if)# ip address 10.14.14.14. 255.0.0.0
!
! Enable the interface
!
Router(config-if)# no shutdown
```