CHAPTER 15

Configuring the POS SPAs

This chapter provides information about configuring the Packet over SONET (POS) shared port adapters (SPAs) on the Cisco 7600 series router. This chapter includes the following sections:

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

For more information about the commands used in this chapter, refer to the *Cisco IOS Software Releases 12.2SR Command Reference*s and to the *Cisco IOS Software Releases 12.2SX Command References*. Also refer to the related Cisco IOS Release 12.2 software command reference and master index publications. For more information, see the "Related Documentation" section on page 47.

Configuration Tasks

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

It includes the following topics:

- Shutting Down and Restarting an Interface on a SPA, page 15-15

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 Cisco 7600 series router where the SIP is installed.
- *subslot*—Specifies the secondary slot of the SIP where the SPA is installed.
- *port*—Specifies the number of the individual interface port on a SPA.

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

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

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

Modifying the 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, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# **mtu** *bytes*	Configures the maximum packet size for an interface, where: • *bytes*—Specifies the maximum number of bytes for a packet. The default is 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 Cisco 7600 series router:

```
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, use the following command in interface configuration mode:

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, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# **keepalive** [*period* [*retries*]]	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: • *period*—Specifies the time interval in seconds for sending keepalive packets. The default is 10 seconds. • *retries*—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.

Note If keepalives are enabled and you are trying to configure line loopback on a POS interface, the keepalive protocol will fail and periodically reset the interface based on the keepalive timeout and cause Layer 1 errors on the other end of the link that is trying to do the loopbacks.

You can avoid this by using the **no keepalive** command on the POS interface that is configured for line loopback. The side that is not in line loopback detects that its keepalive is being looped back and functions properly. An interface configured for internal loopback also functions properly with keepalives enabled.

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 Cisco 7600 series router:

```
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, use the following command 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 Cisco 7600 series router:

```
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 router 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, use the following command 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 Cisco 7600 series router:

```
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, use the following command 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 Cisco 7600 series router:

```
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, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# **encapsulation** *encapsulation-type*	Specifies the encapsulation method used by the interface, where: • *encapsulation-type*—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 Cisco 7600 series router:

```
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 mechanism 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 router, or in different routers.

The performance enhancement of PPP/MLPPP APS does not impact the original PPP/MLPPP scalability on Cisco 7600.

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, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# **aps working** *circuit-number*	Configures a POS interface as a working APS interface, where: • *circuit-number*—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, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# **aps protect** *circuit-number ip-address*	Configures a POS interface as a protect APS interface, where: • *circuit-number*—Specifies the number of the circuit to enable as a protect interface. • *ip-address*—Specifies the IP address of the router 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 router 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 router 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 router 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 router 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 issue 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, use the following commands beginning in interface configuration mode:

	Command	Purpose
Step 1	Router(config-if)# **pos delay triggers line** *ms*	Specifies a delay for setting the line protocol to down when a line-level trigger alarm is received, where: • *ms*—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**} *rate*	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. • *rate*—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

You can issue the **pos delay triggers path** command to configure various path alarms as triggers and to specify an activation delay between 50 and 10000 milliseconds. 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, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# **pos delay triggers path** *ms*	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: • *ms*—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 Cisco 7600 series router:

```
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.

SDCC Configuration Guidelines

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

- SDCC must be enabled on the main POS interfaces.
- SDCC supports only HDLC and PPP encapsulation, not Frame Relay.

SDCC Configuration Task

To configure the POS SPAs for SDCC, complete the following steps:

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 Cisco 7600 series router:

```
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 runts, 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
```

- The default mode for all SPA interfaces is POS. To change between POS and SRP modes, you must shut down the SPA interface.
- Whenever you change modes on a POS SPA, the SPA automatically reloads.
- To change the SRP mate configuration, you must shut down the SPA interfaces.
- You cannot configure subinterfaces on an SRP interface.
- To distinguish between the two rings, one is referred to as the "inner" ring and the other as the "outer" ring. SRP operates by sending data packets in one direction (downstream) and sending the corresponding control packets in the opposite direction (upstream) on the other fiber. An SRP node uses SRP side A to receive (RX) outer ring data and transmit (TX) inner ring data. The node uses SRP side B to receive (RX) inner ring data and transmit (TX) outer ring data. Side A on one node connects to Side B on an adjacent SRP node.

  For configuration of SRP on POS SPAs in multiple slots on the same SIP, the lower-numbered slot and subslot combination hosts the SRP interface and becomes "Side A" of the SRP interface. The slot number of the side-A interface must be lower than the slot location of the SRP mate (side B) interface.
- To configure SRP options, you must specify the slot and subslot location of the side-A interface, in addition to a port number.

SRP Mode Configuration Guidelines

When enabling SRP mode, consider the following guidelines:

- **hw-module subslot srp** command You only need to configure the **hw-module subslot srp** command on the host SRP interface—not on the mate SRP interface.
- The host SRP interface becomes "Side A" of the SRP interface. When configuring SPAs that are installed in different slots on the same SIP for SRP, the slot number of the side-A interface must be lower than the slot location of the SRP mate (side B) interface. Also, you must specify the side-A interface location for configuration of any SRP options.
- The SIP reads the information it receives from the hardware cable mating to validate the mate cable connectivity with your software configuration.
- When you change the SPA mode, the SPA automatically reloads.

Saving the Configuration

To save your running configuration to nonvolatile random-access memory (NVRAM), use the following command 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.

To shut down an interface on a SPA, use the following command in interface configuration mode:

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

To restart an interface on a SPA, use the following command 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 Cisco 7600 series router 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

The following example provides sample output for interface port 0 (the first port) on the SPA located in the subslot 0 of the SIP that is installed in slot 3 of the Cisco 7600 series router:

```
Router# show interfaces pos 3/0/0
POS3/0/0 is up, line protocol is up
  Hardware is Packet over Sonet
  MTU 4470 bytes, BW 622000 Kbit, DLY 100 usec,
     reliability 194/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, crc 16, loopback not set
  Keepalive set (10 sec)
  Scramble disabled
  LMI enq sent  18, LMI stat recvd 0, LMI upd recvd 0
  LMI enq recvd 1473, LMI stat sent  1473, LMI upd sent  0, DCE LMI up
  LMI DLCI 1023  LMI type is CISCO  frame relay DCE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/256, broadcasts sent/dropped 2223/1, interface
broadcasts 1977
  Last input 00:00:05, output 00:00:05, output hang never
  Last clearing of "show interface" counters 04:46:02
  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
     47019 packets input, 163195100 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
```

```
14332 runts, 925 giants, 0 throttles
         0 parity
17820 input errors, 1268 CRC, 0 frame, 0 overrun, 0 ignored, 10 abort
49252 packets output, 170900767 bytes, 0 underruns
0 output errors, 0 applique, 2 interface resets
0 output buffer failures, 0 output buffers swapped out
3 carrier transitions.
```

Monitoring Per-Port Interface Statistics

The following is sample output from the **show controllers pos** command on a Cisco 7600 series router for POS interface 4/3/0 (which is the interface for port 0 of the SPA in subslot 3 of the SIP in chassis slot 4):

```
Router# show controllers pos 4/3/0
POS4/3/0
SECTION
  LOF = 0          LOS    = 0                            BIP(B1) = 65535
LINE
  AIS = 0          RDI    = 0          FEBE = 65535      BIP(B2) = 16777215
PATH
  AIS = 0          RDI    = 0          FEBE = 65535      BIP(B3) = 65535
  PLM = 0          UNEQ   = 0          TIM  = 0          TIU     = 0
  LOP = 0          NEWPTR = 3          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 = 1          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 : woodson
  Remote interface: POS3/0/0
  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
```

Configuration Examples

This section includes the following examples for configuring a POS SPA installed in a Cisco 7600 series router:

- Basic Interface Configuration Example, page 15-17
- MTU Configuration Example, page 15-17

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 Cisco 7600 series router:

```
!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 Cisco 7600 series router:

```
!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

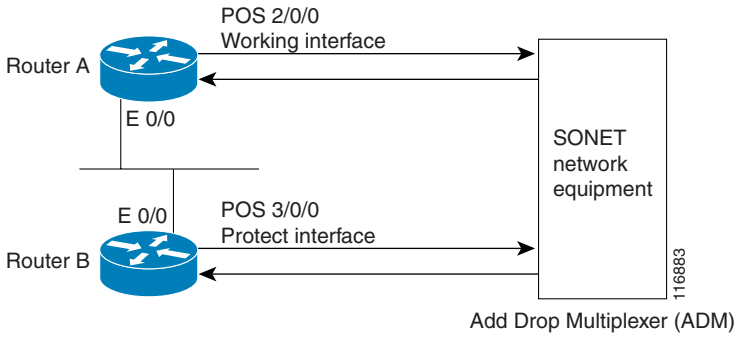
The following example shows how to change from the default encapsulation method of HDLC to PPP:

```
!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, and how to configure more than one protect or working interface on a router by using the **aps group** command. See Figure 15-1.

Figure 15-1 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

```
Router(config-if)# exit
Router(config))# hw-module subslot 1/0 srp mate 1/1
!
! Configure an SRP interface
!
Router(config)# interface srp 1/0/0
Router(config-if)# mac-address 0003.0003.0003
Router(config-if)# ip address 10.4.4.1 255.255.255.0
Router(config-if)# no ip directed-broadcast
Router(config-if)# ipv6 address 10:4:4::1/64
Router(config-if)# service-policy output parent
```