Chapter 3

Configuring Unchannelized OCx/STMx Interfaces

This chapter provides information you need to configure unchannelized SONET/SDH interfaces on E-series routers.

This chapter contains the following sections:

Overview

SONET/SDH interfaces are supported by the modules described in this chapter. This section describes features that are available with SONET/SDH interfaces.

APS and MSP

E-series routers support Automatic Protection Switching (APS) and Multiplex Section Protection (MSP) on selected I/O modules that provide SONET/SDH connections. This feature provides a redundant connection if a primary SONET/SDH connection fails.

For a list of I/O modules that support APS/MSP, see *ERX Module Guide*, *Appendix A*, *Module Protocol Support*.

NOTE: The E120 router and the E320 router do not support APS/MSP.

I/O modules that support APS/MSP have some ports designated for primary operation and other ports designated for redundant operation. For APS/MSP to work correctly, you must provide connections from a primary port and a corresponding redundant port to the remote device. The remote device must also support APS/MSP.

You configure a *working interface* on the primary port and a corresponding *protect interface* on the redundant port of the I/O module. The working interface provides the primary connection, and the protect interface provides the redundant connection.

The router sends and receives data through both interfaces; however, in normal operation, only the signal on the working interface is used. If the signal on the primary interface fails, the router can use the signal on the protect interface. The process by which the router switches to the protect interface is called *switchover*.

When you configure APS/MSP, you must assign a working interface and a corresponding protect interface to a unique group. This group establishes the relationship between the interfaces. Within the group, each interface is identified by an APS/MSP *channel number*. For information about identifying the channel number, see *Numbering Scheme* on page 76.

You must pair a working interface and its corresponding protect interface on an I/O module to form a valid linear APS 1 + 1 group. For example, on an I/O module that provides four working (primary) ports and four protect (redundant) ports, the working interface ports are numbered 0–3, and the protect interface ports are numbered 4–7. Table 7 lists the pairings required to form four valid APS 1 + 1 groups on this I/O module. Each working/protect port pair (for example, port 0 and port 4) forms a valid APS 1 + 1 group.

Table 7: Sample Pairings for Valid APS/MSP Groups

Pair This Working Port	With This Protect Port
0	4
1	5
2	6
3	7

Automatic Switchover

Provided you have not issued the **aps lockout** command for the protect interface, the router switches over to the protect interface if it detects signal failure. You can set the SONET/SDH alarms that determine signal failure and signal degradation.

Manual Switchover

When the router is running and you have configured the I/O module for APS/MSP, you can cause switchover by issuing the **aps force** or **aps manual** command.

Switching Mechanisms

E-series routers support both *bidirectional* and *unidirectional* APS switching modes. By default, the router uses bidirectional switching mode.

Bidirectional Switching Mode

In bidirectional switching mode, the router switches both ends of an APS pair to the same working interface or to the same protect interface when either end determines that a switch is required.

Possible reasons for initiating a bidirectional switch include:

- Detection of a signal failure
- Receipt of an **aps force** or **aps manual** command from the local end of an APS pair
- Reversion to the working interface after a failure has been corrected and the timeout value specified in the **aps revert** command has expired

The devices at both the local and remote ends of an APS pair must support bidirectional switching for the router to implement bidirectional switching mode. Otherwise, the router implements unidirectional switching mode at both ends of the APS pair.

The router detects support for bidirectional switching by interpreting the values of the K1 and K2 bytes in the SONET/SDH frame. For details about the meanings of the values of K1 and K2 bytes, see *Communication Methods* on page 70.

Unidirectional Switching Mode

In unidirectional switching mode, the router switches only one end of an APS pair to the working interface or to the protect interface when that end determines that a switch is required. Possible reasons for initiating a unidirectional switch are the same as those described in *Bidirectional Switching Mode* for initiating a bidirectional switch.

Reversion After Switchover

A failed interface automatically reverts from the protect interface to the working interface after the router detects that the working interface is operational and the timeout value specified in the **aps revert** command has expired. Reversion applies only to recovery from failures.

You can configure the router to revert to the working interface at a specified time after it recovers. This feature enables you to use the protect interface as a redundant connection that functions only when the working interface is not available.

Communication Methods

The router communicates with the remote device by using the K1 and K2 bytes in the line overhead of the SONET/SDH frame. The values of these bytes determine the switching and protect actions. Table 8 and Table 9 on page 71 list the meanings of the values of the K1 and K2 bytes. The bytes are defined in Telcordia document GR-253—Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria, Revision 3 (September 2000). See requirement objects R5-56 [179] and R5-58 [181] for information about bit ordering and meaning for the K1 byte; see R5-67 [190v2] for information about the K2 byte.

Table 8: Explanation of K1 Byte

Bit Value (12345678)	Meaning
Bits 1–4 represent a request.	
0000	No request
0001	Do not revert
0010	Reverse request
0011	Not used
0100	Exercise
0101	Not used
0110	Wait-to-restore
0111	Not used
1000	Manual switch
1001	Not used
1010	Low-priority signal degradation
1011	High-priority signal degradation
1100	Low-priority signal failure
1101	High-priority signal failure
1110	Forced switch
1111	Lockout of protection
Bits 5–8 represent the channel number.	
0	Channel number of protect interface
0001–1110	Channel number of working interface

Table 9: Explanation of K2 Byte

Bit Value (12345678)	Meaning
Bits 1–4 represent the channel number.	
0	Channel number of protect interface
0001–1110	Channel number of working interface
Bit 5 indicates the type of redundancy.	
0	1 + 1 architecture
Bits 6–8 indicate the switching mode.	
000– 011	Reserved for future use
100	Unidirectional mode
101	Bidirectional mode
110	Line remote defect indication (RDI)
111	Line alarm indication signal (AIS)

Higher-Level Protocols

See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the higher-level protocols that the interfaces described in this chapter support.

Platform Considerations

You can configure unchannelized SONET/SDH interfaces on the following E-series routers:

- E120 router
- E320 router
- ERX-1440 router
- ERX-1410 router
- ERX-710 router
- ERX-705 router
- ERX-310 router

This section describes the line modules and I/O modules that support SONET/SDH interfaces.

For detailed information about the modules that support SONET/SDH interfaces on ERX-14xx models, ERX-7xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the protocols and applications that SONET/SDH modules support.

For detailed information about the modules that support SONET/SDH interfaces on the E120 router and the E320 router:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the protocols and applications that SONET/SDH modules support.

OCx/STMx/DS3-ATM Line Modules

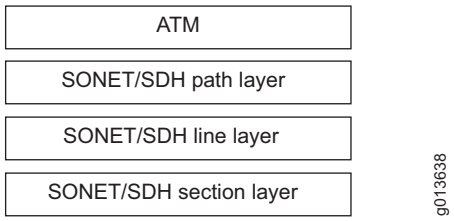
OCx/STMx/DS3-ATM line modules pair with OC3-4 I/O modules to deliver unchannelized OC3/STM1 ATM operation through four line interfaces.

OCx/STMx/DS3-ATM line modules pair with OC12 I/O modules to deliver unchannelized OC12/STM4 ATM operation through one line interface.

I/O modules that support single-mode (intermediate reach or long haul) or multimode operation through SC full duplex connectors are available. I/O modules that support SONET Automatic Protect Switching (APS) 1 + 1 redundancy and SDH Multiplex Section Protection (MSP) are also available.

Figure 5 shows the interface stack for OCx/STMx/DS3-ATM interfaces.

Figure 5: Interface Stack for OCx/STMx/DS3-ATM Interfaces



NOTE: For a detailed description of interface types and specifiers, see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*. For information about interfaces, see *JUNOSe System Basics Configuration Guide, Chapter 1, Planning Your Network*.

OCx/STMx POS Line Modules

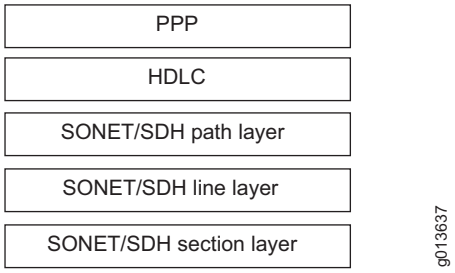
OCx/STMx POS line modules pair with OC3-4 I/O modules to deliver unchannelized OC3/STM1 POS operation through four line interfaces.

OCx/STMx POS line modules pair with OC12 I/O modules to deliver unchannelized OC12/STM4 POS operation through one line interface.

I/O modules that support single-mode (intermediate reach or long haul), or multimode operation through SC full duplex connectors are available. I/O modules that support APS/MSP are also available.

Figure 6 shows the interface stack for OCx/STMx POS interfaces.

Figure 6: Interface Stack for OCx/STMx POS and OC48/STM16 Interfaces



OC48 Line Modules

OC48 line modules pair with OC48 FRAME I/O modules to deliver unchannelized OC48/STM16 POS operation through one line interface.

The OC48 I/O module supports single-mode (intermediate reach or long haul) operation through an SC full duplex connector.

The interface stack for the OC48/STM16 interfaces is the same as that for OCx/STMx POS interfaces (Figure 6).

The OC48 line module can be installed in the router's turbo slots, numbered 2 and 4. When the OC48 line module is installed in a turbo slot, it spans slots 2–3 and 4–5. The bandwidth of slot 3 or slot 5 is used for a line module in slot 2 or slot 4 if that line module requires the turbo slot.

NOTE: If a line module is installed in slot 3 or slot 5, and the line module in slot 2 or 4 requires bandwidth, the system configures the line module it detects first. The state of the other line module is displayed in the **show version** command output as disabled (cfg error).

OC3/STM1 GE/FE Line Module

The OC3/STM1 GE/FE line module pairs with the OC3-2 GE APS I/O module to deliver unchannelized OC3/STM1 ATM operation through two line interfaces and Gigabit Ethernet operation through one line interface.

The OC3-2 GE APS I/O module uses a range of small form-factor pluggable transceivers (SFPs) to support different optical modes and cabling distances, and accepts up to three LC-style fiber-optic connectors. You can configure ports 0 and 1 for OC3/STM1 ATM interfaces; port 2 is reserved for a Gigabit Ethernet interface.

The interface stack for OC3/STM1 ATM interfaces on the OC3-2 GE APS I/O module is the same as for OCx/STMx/DS3-ATM interfaces. (See Figure 5 on page 72.)

For more information about configuring a Gigabit Ethernet interface on this I/O module, see *OC3-2 GE APS I/O Module* on page 171.

NOTE: The OC3-2 GE APS I/O module does not support APS in the current release.

ES2 4G Line Module

The E120 router and the E320 router support the ES2 4G LM. Other E-series routers do not support the ES2 4G LM. For more information about modules on the E120 router and the E320 router, see the *E120 and E320 Module Guide*.

The ES2 4G LM supports IOAs that support single-mode operation (intermediate reach or long haul). IOAs are available in a half-height size, which enables you to configure them in either of the two IOA bays that are available for each slot. For more information about installing IOAs, see the *E120 and E320 Hardware Guide*.

In the current release, the ES2 4G LM pairs with IOAs to provide OCx/STMx ATM, OCx/STMx POS, Gigabit Ethernet, 10-Gigabit Ethernet, and tunnel-service interfaces.

NOTE: For more information about configuring a Gigabit Ethernet interface or 10-Gigabit Ethernet interface, see *Chapter 5, Configuring Ethernet Interfaces*.

For more information about configuring a tunnel-service interface by using the Tunnel Server IOA, see *Chapter 6, Managing Tunnel-Service and IPSec-Service Interfaces*.

E120 Router Configuration

The 120 Gbps switch fabric of the E120 router allocates 10 Gbps of overall bandwidth to each line module slot. The line interface on the ES2 4G LM when installed in a 120 Gbps fabric configuration is 3.9 Gbps; you can achieve this rate with random packet sizes from 64–1518 bytes or a mixture of packet sizes that represent Internet mix traffic (IMIX).

E320 Router Configuration

The 100 Gbps switch fabric of the E320 router allocates 3.4 Gbps of overall bandwidth to each regular line module slot and 10 Gbps of overall bandwidth to each of the turbo slots (slots 2 and 4). The line interface on the ES2 4G LM when installed in a 100 Gbps fabric configuration is 3.4 Gbps; you can achieve this rate with packet sizes greater than 128 bytes.

The 320 Gbps switch fabric of the E320 router allocates 10 Gbps of overall bandwidth to each line module slot. The line interface on the ES2 4G LM when installed in a 320 Gbps fabric configuration is 3.9 Gbps; you can achieve this rate with random packet sizes from 64–1518 bytes or a mixture of packet sizes that represent Internet mix traffic (IMIX).

OCx/STMx ATM IOAs

The ES2 4G LM pairs with the ES2-S1 OC3-8 STM1 ATM IOA to deliver unchannelized OC3/STM1 ATM operation through eight line interfaces. You can install the ES2-S1 OC3-8 STM1 ATM IOA in both IOA bays.

The ES2 4G LM also pairs with the ES2-S1 OC12-2 STM4 ATM IOA to deliver unchannelized OC12/STM4 ATM operation through two line interfaces. You can install the ES2-S1 OC12-2 STM4 ATM IOA in both IOA bays.

The interface stack for both of these IOAs is the same as for OCx/STMx/DS3-ATM interfaces. (See Figure 5 on page 72.)

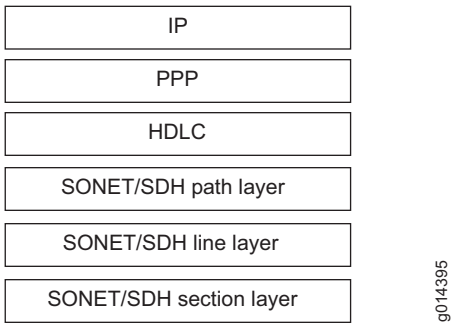
OCx/STMx POS IOAs

The ES2 4G LM pairs with the ES2-S1 OC12-2 STM4 POS IOA to deliver unchannelized OC12/STM4 POS operation through two line interfaces. You can install the ES2-S1 OC12-2 STM4 POS IOA in both IOA bays.

The ES2 4G LM also pairs with the ES2-S1 OC48 STM16 POS IOA to deliver unchannelized OC48/STM16 POS operation through one line interface. In the current release, you can install the ES2-S1 OC48 STM16 POS IOA in only one of the IOA bays per slot.

Figure 7 shows the interface stack for OCx/STMx POS interfaces on the ES2 4G LM.

Figure 7: Interface Stack for OCx/STMx POS Interfaces



Numbering Scheme

When configuring or managing an interface, you must know the numbering scheme for identifying an interface. The numbering scheme depends on the type of E-series router that you have.

ERX-7xx Models, ERX-14xx Models, and the ERX-310 Router

Use the *slot/port* format to identify unchannelized SONET/SDH interfaces. Interfaces that support APS/MSP also use the APS/MSP *channel number*.

- *slot*—Number of the slot in which the line module resides in the chassis.

  In ERX-7xx models, line module slots are numbered 2–6; slots 0 and 1 are reserved for SRP modules. In ERX-14xx models, line module slots are numbered 0–5 and 8–13; slots 6 and 7 are reserved for SRP modules. In an ERX-310 router, line module slots are numbered 1–2; slot 0 is reserved for the SRP module.

- *port*—Number of the port on the I/O module.

  On the OC3-2 GE APS I/O module, you can configure only unchannelized SONET/SDH interfaces on ports 0 and 1; port 2 is reserved for a Gigabit Ethernet interface.

  On I/O modules that support APS/MSP, each primary port has a corresponding redundant port. The number of the primary port, but not that of the redundant port, is used to identify the interface. The primary port is above the corresponding redundant port on the I/O modules.

  Primary port numbers range from 0 to *n–1*, where *n* is the total number of primary ports on the module. For example, if a module has one primary port, that port is labeled 0. On some I/O modules, redundant ports are labeled with a port number followed by the letter R. For example, port 3R is the redundant port for the primary port labeled 3. However, on some two-port modules, the primary port is labeled 0 and the redundant port is labeled 1.

  On I/O modules that support APS/MSP, the port numbers for the working (primary) interfaces are assigned the lower half of the numbered interfaces, whereas the port numbers for the protect (redundant) interfaces are assigned the upper half of the numbered interfaces. For example, on an I/O module that provides four primary ports and four redundant ports, the working interface ports are numbered 0–3 and the protect interface ports are numbered 4–7. Similarly, on an I/O module that provides one primary port and one redundant port, the working interface is port 0 and the protect interface is port 1.

- APS/MSP *channel number*—Identifier of the working or protect (redundant) interface for configuration purposes. (See *Bidirectional Switching Mode* on page 69.)

  The protect interface is always assigned channel number 0. The working interface is always assigned channel number 1.

See *Chapter 1, Configuring Channelized T3 Interfaces*, for information about slot numbering.

For information about installing line modules and I/O modules in ERX routers, see *ERX Hardware Guide, Chapter 4, Installing Modules*.

E120 Router and E320 Router

Use the *slot/adapter/port* format to identify unchannelized SONET/SDH interfaces.

NOTE: The E120 router and the E320 router do not support path channelization.

- *slot*—Number of the slot in which the line module resides in the chassis.

  In the E120 router, line module slots are numbered 0–5. In the E320 router, line module slots are numbered 0–5 and 11–16. For both routers, slots 6 and 7 are reserved for SRP modules; slots 8–10 are reserved for switch fabric modules (SFMs).

- *adapter*—number of the bay in which the I/O adapter (IOA) resides.

  This identifier applies to the E120 and E320 routers only. In the software, adapter 0 identifies the right IOA bay (E120 router) and the upper IOA bay (E320 router); adapter 1 identifies the left IOA bay (E120 router) and the lower IOA bay (E320 router).

- *port*—Number of the port on the IOA.

For information about installing line modules and IOAs in the E120 and E320 routers, see *E120 and E320 Hardware Guide, Chapter 4, Installing Modules*.

Interface Specifier

The configuration examples in this chapter use the format for ERX-7xx models, ERX-14xx models, and the ERX-310 router to specify a SONET/SDH interface. (The format is described in *Numbering Scheme* on page 76.)

For example, the following command specifies a SONET/SDH interface on port 0 of an I/O module in slot 0.

```
host1(config)#controller sonet 4/0
```

When you configure a SONET/SDH interface on an E120 router or an E320 router, you must include the adapter identifier as part of the interface specifier. For example, the following command specifies a SONET/SDH interface on port 0 of the IOA installed in the lower adapter bay (0) of slot 3.

```
host1(config)#controller sonet 3/0/0
```

For more information about interface types and specifiers on E-series models, see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*.

Exchanging Modules

If you replace an OC3 I/O module with an OCx/STMx line module and a corresponding OC3-4 I/O module or vice versa, you must erase the configuration of the existing modules. See **slot accept** in *JUNOSe System Basics Configuration Guide, Chapter 6, Managing Modules*.

On the E120 and E320 routers, if you replace an ES2-S1 OC3-8 STM1 ATM IOA with an ES2-S1 OC12 STM4 POS IOA, you must erase the configuration of the existing IOA. See **adapter accept** or **slot accept** in *JUNOSe System Basics Configuration Guide, Chapter 6, Managing Modules*.

References

For more information about MIB support for unchannelized SONET/SDH interfaces, see RFC 2558—Definitions of Managed Objects for the SONET/SDH Interface Type (March 1999).

For more information about APS/MSP, consult the following resources:

- Telcordia document GR-253—Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria, Revision 3 (September 2000)
- ITU-T G.783—Characteristics Of Synchronous Digital Hierarchy (SDH) Multiplexing Equipment Functional Blocks: Annex A – Multiplex Section Protection (MSP) Protocol, Commands And Operation (1990)
- Definitions of Managed Objects for SONET Linear APS Architectures—draft-ietf-atommib-sonetaps-mib-05.txt (November 2001 expiration)
- RFC 3498—Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures (March 2003)

Configuration Tasks

When configuring an unchannelized SONET/SDH interface, you first configure ATM or POS on the interface. For details on configuring POS and ATM, see *JUNOSe Link Layer Configuration Guide, Chapter 1, Configuring ATM,* and *JUNOSe Link Layer Configuration Guide, Chapter 6, Configuring Packet over SONET*.

- On an OCx/STMx/DS3-ATM line module with an OC3-4 or OC12 I/O module, you can configure only ATM interfaces.
- On an OCx/STMx POS line module with an OC3-4 or OC12 I/O module, you can configure only POS interfaces.
- On an OC48 line module with an OC48 FRAME I/O module, you can configure only POS interfaces.
- On an OC3/STM1 GE/FE line module with an OC3-2 GE APS I/O module, you can configure only ATM interfaces on ports 0 and 1.

- On an ES2 4G LM with an ES2-S1 OC12-2 STM4 POS IOA or an ES2-S1 OC48 STM16 POS IOA, you can configure only POS interfaces.
- On an ES2 4G LM with an ES2-S1 OC3-8 STM1 ATM IOA or an ES2-S1 OC12-2 STM4 ATM IOA, you can configure only ATM interfaces.

Configuring the SONET/SDH Layers

When you configure ATM or POS on an interface, you automatically configure default settings at the SONET/SDH layer. To modify the default settings:

1. Select an interface on which you want to configure SONET or SDH.
2. Specify the type of interface: SONET or SDH.
3. Specify a clock source for the interface.
4. (Optional) Assign a text description or an alias to the interface.
5. Disable processing of SNMP link status information for the section and line layers of the interface.
6. Enable processing of SNMP link status information for the path layer of the interface.
7. (Not recommended) Overwrite the automatic setting for the path signal label (C2) byte.
8. Configure the router to use remote defect indications (RDIs) at the path layer to determine the operational status of a path.
9. (MPLS fast reroute over SONET/SDH interfaces) Specify the time that the router waits to set an alarm when the router records a defect at the path layer.
10. (MPLS fast reroute over SONET/SDH interfaces) Specify the time that the router waits to set an alarm when the router records a defect at the line or section layer.
11. Shut down (disable) an interface.

clock source

- Use to configure the transmit clock source for the interface.
- In most cases, accept the default option, **line**. This setting allows the interface to derive the transmit clock from the received clock. In certain circumstances, it might be appropriate to generate a clock from one of the internal sources (options **module** or **chassis**).
- Specify the keyword **line** to use a transmit clock on the line's receive data stream.
- Specify the keywords **internal module** to use the line module's internal clock.
- Specify the keywords **internal chassis** to use the router's clock.

- On a cOC3/STM1 I/O module, you can configure some ports with internal clock sources and others with line clock sources. However, all ports with internal clock sources must use either the router's clock or the module's clock. You cannot configure some ports on the I/O module to use the router's clock and others to use the module's clock.
- To change the clock source of the ports on a cOC3/STM1 I/O module from the router's clock to the module's clock or vice versa, change the clock source of all ports firstly to the line setting, and then to the new internal clock setting.
- Example

  host1(config-controll)#**clock source internal module**

- Use the **no** version to revert to the default, **line**.

controller sonet

- Use to select an interface on which you want to configure SONET or SDH.
- Use the interface specifier in *slot/port:path-channel* format (ERX-14xx models, ERX-7xx models, and the ERX-310 router) or *slot/adapter/port* format (E120 router and E320 router). The E120 and E320 routers do not support path channelization, and therefore does not support the *path-channel* specifier.
- Example 1—Selects a SONET interface on ERX-14xx models, ERX-7xx models, or the ERX-310 router

  host1(config)#**controller sonet 4/0**

- Example 2—Selects an SONET interface on the E320 router

  host1(config)#**controller sonet 3/0/0**

- There is no **no** version.

description

- Use to assign a text description or an alias to an unchannelized SONET interface.
- You can use this command to help you identify the interface and keep track of interface connections.
- The description or alias can be a maximum of 64 characters.
- Use the **show controllers sonet** command to display the text description.
- Example

  host1(config-controll)#**description boston-sonet-interface**

- Use the **no** version to remove the text description or alias.

path description

- Use to assign a text description or an alias to an unchannelized SONET path.
- You can use this command to help you identify the interface and keep track of interface connections.
- The description or alias can be a maximum of 64 characters.

- Example

  host1(config-controll)#**path description westford**

- Use the **no** version to remove the description.

path overhead c2

- Use to overwrite the automatic setting for the path signal label (C2) byte.
- By default, the value of the C2 byte for the path is determined by the layers configured above the SONET/SDH interface and set automatically. The E-series router sets this default value in accordance with RFC 2558. (See *References* on page 78.)

CAUTION: Use this command only if you know that the automatic setting does not match the setting on the remote device. Otherwise, the remote device might send an unexpected value, and the router might lose data.

- Do not specify a path identifier for unchannelized SONET/SDH interfaces.
- Example

  host1(config-controll)#**path overhead c2 20**

- Use the **no** version to restore the default setting, in which the value of the C2 byte is determined by the layers configured above the SONET/SDH interface.

path shutdown

- Use to disable a path.
- Paths are enabled by default.
- Example

  host1(config-controll)#**path shutdown**

- Use the **no** version to restart a disabled path.

path snmp trap link-status

- Use to enable SNMP link-status processing for the path layer of the interface.
- The default is disabled.
- Do not specify a path identifier for unchannelized SONET/SDH interfaces.
- Example

  host1(config-controll)#**path snmp trap link-status**

- Use the **no** version to disable SNMP link status processing.

path trigger alarm prdi

- Use to configure the router to use remote defect indications (RDIs) at the path layer to determine the operational status of a path.
- Do not specify a path identifier for unchannelized SONET/SDH interfaces.
- Example

  host1(config-controll)#**path trigger alarm prdi**

- Use the **no** version to restore the default setting, in which the software uses loss of pointer and AIS defects at the path layer to determine the operational status of a path.

path trigger delay

- Use to set the time that the router waits to set an alarm when the router records a defect at the path layer.
- Change this value from the default only when you are using MPLS fast reroute over a SONET/SDH interface.
  - Specify a value of 0 milliseconds if the interface does not use APS/MSP or if you want MPLS to have priority over APS/MSP.
  - Specify a value of at least 100 milliseconds if this interface uses APS/MSP and you want APS/MSP to have priority over MPLS.
- Do not specify a path identifier for unchannelized SONET/SDH interfaces.
- Example

  host1(config-controll)#**path trigger delay msec 1000**

- Use the **no** version to restore the default setting, 2500 milliseconds.

sdh

- Use to specify that the interface supports SDH.
- Example

  host1(config-controller)#**sdh**

- Use the **no** version to revert to SONET operation on this interface.

shutdown

- Use to disable a SONET/SDH interface.
- SONET/SDH interfaces are enabled by default.
- Example

  host1 (config-controll)#**shutdown**

- Use the **no** version to restart a disabled interface.

snmp trap link-status

- Use to enable SNMP link-status processing for the section and line layers of the interface.
- The default is enabled.
- Example

  host1(config-controll)#**no snmp trap link-status**

- Use the **no** version to disable SNMP link status processing.

trigger delay

- Use to set the time that the router waits to set an alarm when the router records a defect at the line or section layer.
- Change this value from the default only when you are using MPLS fast reroute over a SONET/SDH interface.
  - Specify a value of 0 milliseconds if the interface does not use APS/MSP or if you want MPLS to have priority over APS/MSP.
  - Specify a value of at least 100 milliseconds if this interface uses APS/MSP and if you want APS/MSP to have priority over MPLS.
- Example

  host1(config-controll)#**trigger delay msec 1000**

- Use the **no** version to restore the default setting, 2500 milliseconds.

Configuring APS/MSP

For APS/MSP, you must configure a working interface and a corresponding protect interface. You must also assign each pair of working and protect interfaces to a unique group.

NOTE: Configuring the working interface before you configure the protect interface is not required. You can configure the working interface before or after you configure the protect interface.

NOTE: The E120 router and the E320 router does not support APS/MSP.

Configuring the Working Interface

To configure the working interface:

1. Select the interface.

   host1(config)#**controller sonet 4/0**

2. Specify the APS group to which the working and protect interfaces will belong.

   host1(config-controll)#**aps group boston**

3. Specify the interface as the working interface.

   host1(config-controll)#**aps working**

aps group

- Use to specify the group to which the working and protect interfaces will belong.
- Specify the name of the APS group.
- Example

  host1(config-controll)#**aps group boston**

- Use the **no** version to remove a group of APS interfaces.

aps working

- Use to specify the working interface.
- Optionally, you can specify 1 as the channel number for the working interface. Because the working interface is always assigned channel number 1, this is the only valid option.
- Examples

  host1(config-controll)#**aps working**
  host1(config-controll)#**aps working 1**

- Use the **no** version to prevent the interface from acting as a working interface.

threshold

- Use to set thresholds for the bit error rates associated with APS/MSP alarms.
- This command does not apply to the working interface. You can issue this command only for the protect interface.
- Specify one of the following keywords to indicate the alarm level:
  - **sd-ber**—Bit error rate that specifies signal degradation
  - **sf-ber**—Bit error rate that specifies signal failure
- Specify an integer *n* in one of the following ranges, where *n* corresponds to a rate of 10^{-n} (10e-*n*) errors per second.
  - For **sd-ber**, an integer in the range 5–9; the default value is 5
  - For **sf-ber**, an integer in the range 3–5; the default value is 3
- Example

  host1(config-controll)#**threshold sf-ber 4**

- Use the **no** version to restore the default, 5 (for **sd-ber**) or 3 (for **sf-ber**), for the specified alarm.

Configuring the Protect Interface

To configure the protect interface:

1. Select the interface.

   host1(config)#**controller sonet 4/1**

2. Specify the APS group to which the protect and working interfaces will belong.

   host1(config-controll)#**aps group boston**

3. Specify the protect interface.

   host1(config-controll)#**aps protect**

4. (Optional) Prevent the protect interface from taking over automatically if the working interface fails.

   host1(config-controll)#**aps lockout**

5. (Optional) Enable the router to revert to the working interface when it recovers.

   host1(config-controll)#**aps revert 7**

6. (Optional) Specify that switchover takes place in unidirectional mode.

   host1(config-controller)#**aps unidirectional**

aps group

- Use to specify the group to which the working and protect interfaces will belong.
- Specify the name of the APS group.
- Example

  host1(config-controll)#**aps group boston**

- Use the **no** version to remove a group of APS interfaces.

aps lockout

- Use to prevent the protect interface from taking over if the working interface fails.
- You can issue this command only for the protect interface, not for the working interface.
- The **aps lockout** command has a higher priority than the **aps force** command, **aps manual** command, a remote reversion request, a signal failure request, or a signal degradation.
- Optionally, you can specify 0 as the channel number for the protect interface. Because the protect interface is always assigned channel number 0, this is the only valid option.
- The resulting configuration is stored in NVS for SRP module or line module reloads and SNMP.

- Examples

  host1(config-controll)#**aps lockout**
  host1(config-controll)#**aps lockout 0**

- Use the **no** version to restore the default situation, in which the protect interface can take over if the working interface fails.

aps protect

- Use to configure an interface as a protect interface.
- You can issue this command only for the protect interface, not for the working interface.
- Optionally, you can specify 0 as the channel number for the protect interface. Because the protect interface is always assigned channel number 0, this is the only valid option.
- Examples

  host1(config-controll)#**aps protect**
  host1(config-controll)#**aps protect 0**

- Use the **no** version to remove the protect interface from the APS group.

aps revert

- Use to revert to the original working interface when it recovers.
- Specify the number of minutes in the range 5–7, after which the router will switch to the working interface.
- You can issue this command only for the protect interface, not for the working interface.
- Example

  host1(config-controll)#**aps revert 7**

- Use the **no** version to restore the default setting, in which the router does not revert to the working interface when it recovers.

aps unidirectional

- Use to specify that the router should switch to the protect interface using the unidirectional mode switching mechanism.
- You can issue this command only for the protect interface, not for the working interface.
- Example

  host1(config-controller)#**aps unidirectional**

- Use the **no** version to restore the default setting, bidirectional mode.

Configuring SONET/SDH Alarms

To configure the bit error rates that determine signal degradation and signal failure on the working interface:

1. Select the protect interface.

   host1(config)#**controller sonet 4/1**

2. Specify the bit error rate at which the router should generate an alarm indicating signal degradation.

   host1(config-controller)#**threshold sd-ber 6**

3. Specify the bit error rate at which the router should generate an alarm indicating signal failure and switch from the working interface to the protect interface.

   host1(config-controller)#**threshold sf-ber 5**

threshold

- Use to set thresholds for the bit error rates associated with APS/MSP alarms.
- You can issue this command only for the protect interface. It does not apply to the working interface.
- Specify one of the following keywords to indicate the alarm level:
  - **sd-ber**—Bit error rate that specifies signal degradation
  - **sf-ber**—Bit error rate that specifies signal failure
- Specify an integer *n* in one of the following ranges, where *n* corresponds to a rate of 10^{-n} (10e-*n*) errors per second.
  - For **sd-ber**, an integer in the range 5–9; the default value is 5
  - For **sf-ber**, an integer in the range 3–5; the default value is 3
- Example

  host1(config-controll)#**threshold sf-ber 4**

- Use the **no** version to restore the default, 5 (for **sd-ber**) or 3 (for **sf-ber**), for the specified alarm.

Configuration Example

The following example shows how to configure working and protect interfaces for APS/MSP.

1. Configure the working interface.

   host1(config)#**controller sonet 3/0**
   host1(config-controller)#**aps group boston**
   host1(config-controller)#**aps working 1**

2. Configure the protect interface.

```
host1(config-controller)#controller sonet 3/1
host1(config-controller)#aps group boston
host1(config-controller)#aps protect 0
host1(config-controller)#aps unidirectional
host1(config-controller)#aps revert 30
host1(config-controller)#threshold sf-ber 4
```

Configuring APS Event Collection

To configure line modules to deliver APS events to the necessary SNMP traps, issue the **aps events** command from Global Configuration mode.

aps events

- Use to enable line modules to deliver APS events to the necessary SNMP traps.
- Use the *list* variable to deliver the following types of APS events:
  - all—Configure notification of all APS events
  - channel-mismatch—Configure notification of APS channel mismatches
  - feplf—Configure notification of APS far-end protection line failures
  - mode-mismatch—Configure notification of APS mode mismatches
  - psbf—Configure notification of APS protection signal byte failures
  - switchover—Configure notification of APS switchovers
- Example

  ```
  host1(config)#aps events channel-mismatch
  ```

- Use the **no** version to disable the delivery of APS events from line modules to SNMP traps.

Manual Switching to a Redundant Port

To switch from the working interface to the protect interface manually, issue the **aps force** command or the **aps manual** command. The **aps force** command overrides any switchover settings you configured on the protect interface; the **aps manual** command does not override those settings.

aps force

- Use to switch from the working interface to the assigned protect interface unless a request of equal or higher priority is in effect.
- You can issue this command only for the protect interface, not for the working interface.
- The **aps force** command has a higher priority than the **aps manual** command, a remote reversion request, a signal failure request on a working channel, or a signal degradation request on a working channel.
- The resulting configuration is not stored in NVS for SRP module or line module reloads; however, it is stored in NVS for use with SNMP.

- You must specify one of the following channel numbers:
  - 0—Switches from the protect interface back to the working interface
  - 1—Switches from the working interface to the protect interface
- Examples

  host1(config-controll)#**aps force 0**
  host1(config-controll)#**aps force 1**

- Use the **no** version to revert to the original working interface.

aps manual

- Use to switch from the working interface to the protect interface unless a command of equal or higher priority is in effect.
- You can issue this command only for the working interface, not for the protect interface.
- The **aps manual** command has a higher priority than a remote reversion request.
- The resulting configuration is not stored in NVS for SRP module or line module reloads; however, it is stored in NVS for use with SNMP.
- You must specify one of the following channel numbers:
  - 0—Switches from the protect interface back to the working interface
  - 1—Switches from the working interface to the protect interface
- Examples

  host1(config-controll)#**aps manual 0**
  host1(config-controll)#**aps manual 1**

- Use the **no** version to revert to the original working interface.

Testing Interfaces

You can enable loopback tests at the SONET/SDH level. You can also test for connectivity between an interface and the SONET/SDH interface at the other end of the line.

Loopback Testing

To configure loopback testing at the SONET/SDH level, use the **loopback** command.

loopback

- Use to configure the type of loopback at the SONET/SDH layer.
- Specify one of the following options:
  - **local**—Loops the data back toward the router
  - **network**—Loops the data toward the network before the data reaches the frame.

- Example

  host1(config)#**controller sonet 4/0**
  host1(config-controller)#**loopback network**

- Use the **no** version to disable loopback.

Testing Connectivity

Use the **path overhead j1** command to check for connectivity between the router and a SONET/SDH device at the other end of the line. This command defines:

- A message that the router sends from the specified interface to the SONET/SDH device at the other end of the line.
- A message that the router expects to receive on the specified interface from the SONET/SDH device at the other end of the line.

When you define a message that the interface sends, you must monitor receipt of that message at the remote end.

When you define a message that the interface expects to receive, you should configure the remote device to transmit the same message to the interface. You can then use the **show controllers sonet** command to compare the expected and receive messages.

You must remove trace messages before you can change the port type from SONET to SDH or vice versa. Otherwise, you see the following error message:

```
% Cannot set port mode (path trace message is set)
```

path overhead j1

- Use to define messages that the router sends to or expects to receive from a SONET/SDH device connected to one of its SONET interfaces.
- Do not specify a path identifier for unchannelized SONET interfaces.
- Specify the keyword **msg** for a message that the router transmits for this path.
- Specify the keyword **exp-msg** to define a message that the router expects to receive on this path.
- Define a message of up to 62 characters for SONET or up to 15 characters for SDH.
- Configure the remote device to send the same message that the router expects to receive on this path. You can then compare the expected and received messages in the display of the **show controllers sonet** command.
- Example for unchannelized SONET interfaces:

  host1(config-controller)#**path overhead j1 msg hello**

- Use the **no** version to restore the default situation, in which all the characters in the transmitted or expected message are zeros.

Monitoring SONET/SDH Interfaces

You can monitor interface statistics and APS/MSP settings.

NOTE: The E120 router and E320 router output for **monitor** and **show** commands is identical to output from other E-series routers, except that the E120 and E320 router output also includes information about the adapter identifier in the interface specifier (*slot/adapter/port*).

Monitoring Interface Statistics

You can set statistics baselines for the section, line, and path layers using the **baseline interface sonet** commands.

To display statistics for SONET and SDH interfaces, use the **show controllers sonet** commands. Use the **delta** options to display statistics with the baseline subtracted.

baseline line interface sonet

- Use to set a statistics baseline for the SONET/SDH line layer.
- The router implements the baseline by reading and storing the MIB statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved.
- Use the **total** [**delta**] keywords with the **show controllers sonet line** command to view the baseline statistics.
- Example 1—Sets a baseline for SONET line layer interfaces on ERX-14xx models, ERX-7xx models, or the ERX-310 router

  host1#**baseline line interface sonet 2/0**

- Example 2—Sets a baseline for SONET line layer interfaces on the E320 router

  host1#**baseline line interface sonet 3/0/0**

- There is no **no** version.

baseline path interface sonet

- Use to set a statistics baseline for the SONET/SDH path layer.
- The router implements the baseline by reading and storing the MIB statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved.
- Use the **total** [**delta**] keywords with the **show controllers sonet path** command to view the baseline statistics.

- Example 1—Sets a baseline for SONET path layer interfaces on ERX-14xx models, ERX-7xx models, or the ERX-310 router

  host1#**baseline path interface sonet 2/0**

- Example 2—Sets a baseline for SONET path layer interfaces on the E320 router

  host1#**baseline path interface sonet 3/0/0**

- There is no **no** version.

baseline section interface sonet

- Use to set a statistics baseline for the SONET/SDH section layer.
- The router implements the baseline by reading and storing the MIB statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved.
- Use the **total** [**delta**] keywords with the **show controllers sonet section** commands to view the baseline statistics.
- Example 1—Sets a baseline for SONET section layer interfaces on ERX-14xx models, ERX-7xx models, or the ERX-310 router

  host1#**baseline section interface sonet 2/0**

- Example 2—Sets a baseline for SONET section layer interfaces on the E320 router

  host1#**baseline section interface sonet 3/0/0**

- There is no **no** version.

show controllers sonet

- Use to display the configuration for SONET and SDH interfaces.
- Field descriptions
  - Interface specifier in *slot/port* format (ERX-14xx models, ERX-7xx models, and the ERX-310 router) or *slot/adapter/port* format (E120 and E320 routers)
  - non channelized—Unchannelized path
  - channelized—Number of channels and speed for the interface
  - ifAdminStatus—Configured status of the interface: up or down
  - description—Configured description of the controller
  - snmp trap link-status—State of SNMP link-status processing for the section and line layers of the interface: enabled or disabled
  - alarms used for operational status calculation—Types of defects that the router uses to determine the operational status of the interface at the section and line layers
  - defect trigger soaking delay—Time that the router waits to set an alarm when the router records a defect at the section or line layer

- Operational Status—Physical state of the interface:
  - up—Interface is operational
  - down, failure alarm—Interface is not operational; type of defect that caused failure is specified
  - time since last status change—Time since the module was rebooted
- Loopback State—Type of loopback configured on the interface
- Mode—Type of interface: SONET or SDH
- Timing source—Type of clock source configured for the channel:
  - line—Internal clock is from the line module itself
  - chassis—Internal clock is from the configured router clock
- Receive FIFO Overruns—Number of times received FIFO was overrun
- Current section defects—Number of suspect bit patterns found in several consecutive frames in section layer
- Current line defects—Number of suspect bit patterns found in several consecutive frames in line layer
- Received SONET overhead—Section and line overhead bytes present in the receive side of the interface at any particular time
- Transmitted SONET overhead—Section and line overhead bytes present in the transmit side of the interface at any particular timeChannel configuration—Parameters for specific controllers. The actual parameters depend on the controller.
  - ifAdminStatus—State of the controller in the software configuration: up or down
  - snmp trap link-status—State of SNMP link status processing for the path layer: enabled or disabled
  - alarms used for operational status calculation—Types of defects that the router uses to determine the operational status of the interface at the path layer
  - defect trigger soaking delay—Time that the router waits to set an alarm when the router records a defect at the path layer
  - c2 byte—Setting of path signal byte: set by upper interface type (automatic setting) or configured value
  - Operational Status—Physical state of the controller: up, down, or lowerLayerDown
  - time since last status change: time the controller has been in the current physical state
- Received SONET Path overhead—Path overhead bytes present in the receive side of the interface at any particular time
- Transmitted SONET Path overhead—Path overhead bytes present in the transmit side of the interface at any particular time

- Example

```
host1#show controllers sonet 1/0

oc3 1/0
non channelized
ifAdminStatus: up
description: link1
snmp trap link-status: enabled
alarms used for operational status calculation: LOS LOF AIS RDI
defect trigger soaking delay: 2500 milliseconds
Operational Status: down, failure alarm: AIS
      time since last status change: 07:33:12
Loopback State: none
Mode: sonet
Timing source: line
Receive FIFO Overruns: 0, Framer stats: 0/0
Current section defects: none
Current line    defects: AIS


Received SONET overhead:
F1      :  n/a, J0      :  n/a, K1      : 0xFF, K2      : 0xFF, S1      : 0xFF
Transmitted SONET overhead:
F1      : 0x00, J0      : 0x01, K1      : 0x00, K2      : 0x00, S1      : 0x00

Channel configuration:
channel = 0, path = oc3, hierarchy = 1/0, current path defects: LowerLayerDefect
 ifAdminStatus: up
 snmp trap link-status: disabled
 alarms used for operational status calculation: LOP AIS
 defect trigger soaking delay: 2500 milliseconds
 c2 byte set by upper interface type
 Operational Status: lowerLayerDown
       time since last status change: 07:33:12


Received SONET Path overhead:
F2      :  n/a, Z3      :  n/a, Z4      :  n/a, C2      : 0xFF, C2Exp   : 0x00
Transmitted SONET Path overhead:
F2      : 0x00, Z3      : 0x00, Z4      : 0x00, C2      : 0x00
```

show controllers sonet line | path | section

- Use to display statistics for the different layers in channelized SONET and SDH interfaces. Figure 5 on page 72 and Figure 6 on page 73 show the layers in the interfaces.
- For definitions of the MIB statistics, see RFC 2558—Definitions of Managed Objects for the SONET/SDH Interface Type (March 1999).
- Specify an interface in *slot/port* format (ERX-14xx models, ERX-7xx models, and the ERX-310 router) or *slot/adapter/port* format (E120 and E320 routers).
- To view statistics for a layer, specify the type of layer.
- To view all statistics for all sessions, specify the **total** keyword.
- To view baselined statistics for all intervals, specify the **delta total** keywords.

- Field descriptions
  - Current Interval Counters—Statistics for the current 15-minute interval

    The following fields may appear in line, path, or section:

    - ES—Number of errored seconds encountered by a T1 or an E1 in an interval
    - SES—Number of severely errored seconds encountered in an interval
    - UAS—Number of unavailable seconds encountered in an interval
    - SEFS—Number of severely errored framing seconds encountered in an interval
    - (Code Violations)—Number of coding violations encountered in an interval (BIP-B1, BIP-B2, BIP-B3)
    - RDI—Number of remote defect indications
    - AIS—Number of alarm indication signals
    - BERR-SF—Number of bit error rate signal failures
    - BERR-SD—Number of bit error rate signal degrades
    - LOS—Number of loss of signal alarms
    - LOF—Number of loss of frame alarms
    - LOP—Number of loss of pointers
    - UNEQ—Number of unequipped alarms
    - PLM—Number of payload mismatchs
  - Last Interval Counters—Statistics for the previous 15-minute interval
  - Current Far End Interval Counters—Statistics for the remote connection associated with the SONET/SDH path in the current 15-minute interval
    - REI—Number of remote error indications
  - Far End Last Interval Counters—Statistics for the remote connection associated with the SONET/SDH path in the previous 15-minute interval
  - Total Interval Counters—Statistics for all intervals or baselined statistics
  - Total Far End Counters—Statistics for all remote connections associated with the SONET/SDH path
- Example 1—Shows the MIB statistics for the path layer on interface 1/0.

```
host1#show controllers sonet 1/0 path

Channel number 0

Number of valid intervals - 31
Time elapsed in current interval - 141
Current status                   = LowerLayerDefect

Current Path Interval Counters           Seconds      Counts        State
ES                                             0
SES                                            0
UAS                                          141
RDI                                          141           0       Active
AIS                                          141           0       Active
LOP                                            0           0       OK
```

```
UNEQ                                        0            0       OK
PLM                                       141            0       Active
BIP-B3  (Code Violation)                    0            0

Last Path Interval Counters             Seconds      Counts
ES                                          0
SES                                         0
UAS                                       900
RDI                                       900            0
AIS                                       900            0
LOP                                         0            0
UNEQ                                        0            0
PLM                                       900            0
BIP-B3  (Code Violation)                    0            0

Total Path Counters                     Seconds      Counts
ES                                          0
SES                                         0
UAS                                     27255
RDI                                     27255            0
AIS                                     27255            0
LOP                                         0            0
UNEQ                                        0            0
PLM                                     27255            0
BIP-B3  (Code Violation)                    0            0

Current Far End Path Interval Counters  Seconds      Counts
ES                                          0
SES                                         0
UAS                                       141
REI                                         0            0

Far End Last Path Interval Counters     Seconds      Counts
ES                                          0
SES                                         0
UAS                                       900
REI                                         0            0

Total Far End Path Counters             Seconds      Counts
ES                                          0
SES                                         0
UAS                                     27255
REI                                         0            0
```

- Example 2—Shows the MIB statistics for the line layer on interface 1/0.

```
host1#show controllers sonet 1/0 line

Number of valid intervals - 31
Time elapsed in current interval - 114
Current status                   = AIS

Current Line Interval Counters          Seconds      Counts       State
ES                                          0
SES                                         0
UAS                                       113
RDI                                         0            0       OK
AIS                                       113            0       Active
BERR-SF                                     0            0       OK
```

```
BERR-SD                                    0            0       OK
BIP-B2 (Code Violation)                    0            0

Last Line Interval Counters             Seconds      Counts
ES                                          0
SES                                         0
UAS                                       900
RDI                                         0            0
AIS                                       900            0
BERR-SF                                     0            0
BERR-SD                                     0            0
BIP-B2 (Code Violation)                     0            0

Total Line Counters                     Seconds      Counts
ES                                          0
SES                                         0
UAS                                     27227
RDI                                         0            0
AIS                                     27227            1
BERR-SF                                     0            0
BERR-SD                                     0            0
BIP-B2 (Code Violation)                     0            0

Current Far End Line Interval Counters  Seconds      Counts
ES                                          0
SES                                         0
UAS                                         0
REI                                         0            0

Far End Last Line Interval Counters     Seconds      Counts
ES                                          0
SES                                         0
UAS                                         0
REI                                         0            0

Total Far End Line Counters             Seconds      Counts
ES                                          0
SES                                         0
UAS                                        10
REI                                         0            0
```

- Example 3—Shows the MIB statistics for the section layer on interface 1/0.

```
host1#show controllers sonet 1/0 section

Number of valid intervals - 31
Time elapsed in current interval - 49
Current status                   = No Defect

Current Section Interval Counters       Seconds      Counts        State
ES                                          0
SES                                         0
SEFS                                        0
LOS                                         0            0       OK
LOF                                         0            0       OK
BIP-B1 (Code Violation)                     0            0

Last Section Interval Counters          Seconds      Counts
ES                                          0
SES                                         0
```

```
SEFS                                    0
LOS                                     0             0
LOF                                     0             0
BIP-B1 (Code Violation)                 0             0


Total Section Counters                Seconds       Counts
ES                                        1
SES                                       1
SEFS                                      0
LOS                                       0             0
LOF                                       0             0
BIP-B1 (Code Violation)                   1            16
```

- Example 4—Shows all statistics for all sessions for the section layer on interface 2/0.

```
host1#show controllers sonet 2/0 section total

Number of valid intervals - 31
Time elapsed in current interval - 244

Total Section Counters                Seconds       Counts
ES                                        1
SES                                       1
SEFS                                      0
LOS                                       0             0
LOF                                       0             0
BIP-B1 (Code Violation)                   1            16
```

Monitoring APS/MSP

You can use the **show aps** commands to monitor APS/MSP.

show aps

- Use to display information about interfaces on which APS/MSP is configured.
- Use the **all** keyword to display information from all APS/MSP groups. In the output, partially configured controllers are displayed with `none` and include only the group name.
- Field descriptions
  - sonet x/y—Location of the SONET/SDH interface
  - protect group—Name of the APS group that contains the working interface and the corresponding protect interface
  - channel—Number of the APS channel; 0 identifies the protect interface, 1 identifies the working interface
  - ~—Interface is not currently active
  - Selected—Interface is active
  - ~Selected—Interface is not active
  - Bidirectional—Router switches to the protect interface using the bidirectional switching mechanism
  - Unidirectional—Router switches to the protect interface using the unidirectional mode switching mechanism

- Nonrevertive—Router does not revert to the working interface when it recovers
- Revertive—Router reverts to the working interface when it recovers
- Disabled—APS/MSP is disabled on the interface
- Enabled—APS/MSP is enabled on the interface

- Example 1

```
host1#show aps
sonet 5/1 protect group one channel 0  ~Selected Unidirectional Nonrevertive
sonet 5/0 working group one channel 1   Selected Enabled
```

- Example 2

```
host1#show aps all
aps events: disabled
sonet 4/0 working group group-4 channel 1   Selected Enabled
sonet 4/1 protect group group-4 channel 0  ~Selected Unidirectional
Nonrevertive
sonet 2/0 working group group-2 channel 1   Selected Enabled
sonet 2/1 protect group group-2 channel 0  ~Selected Unidirectional
Nonrevertive
sonet 12/0
sonet 12/1
sonet 12/2 none    group partial-group
sonet 12/3
sonet 12/4
sonet 12/5
sonet 12/6
sonet 12/7
```

show aps group

- Use to display information about all APS/MSP groups or a specified APS/MSP group.
- Field descriptions
  - Aps group—Name of the APS group for which information is displayed
  - Current Conditions—Current state of the group
  - Rx (K1/K2)—Value, meaning, and channel number of the received K1 and K2 bytes (see Table 8 on page 70 and Table 9 on page 71)
  - Tx (K1/K2)—Value, meaning, and channel number of the transmitted K1 and K2 bytes (see Table 8 on page 70 and Table 9 on page 71)
  - Counters—Statistics for APS group
    - ModeMismatch—Number of differences detected in the local and remote switching mechanisms (unidirectional or bidirectional modes)
    - ChanMismatch—Number of differences detected between the number of the channel in the transmitted K1 byte and the number of the channel in the received K2 byte

        - PSBF—Number of protection switching byte failures detected (no 3 consecutive SONET/SDH frames out of the last 12 contain identical K1 bytes)
        - FEPLF—Number of far-end protection line failures (signal failures detected on protect interface)
    - Aps channel—Number, interface specifier (in *slot*/*port* format), and protect/working designation of the APS channel for which information is displayed
        - aps-protect—Identifies the protect interface
        - aps-working—Identifies the working interface
    - Current Conditions—Current state of the interface for this channel
        - lockedOut—Indicates that the router is configured to prevent the protect interface from taking over if the primary interface fails
        - SD—Indicates that signal degradation is detected
        - SF—Indicates that signal failure is detected
        - switched—Indicates that the router has switched from the working interface to the protect interface
    - Counters—Statistics for APS channel
        - SignalDegrades—Number of degraded signals detected
        - SignalFailures—Number of failed signals detected
        - Switchovers—Number of times the router has switched from the working interface to the protect interface
        - LastSwitchover—Length of time that the working interface was active when the router last switched from the working interface to the protect interface; a value of Not Applicable indicates that no switchovers have occurred
- Example

```
host1#show aps group
Aps group bos
  Current Conditions: PSBF
  Rx(K1/K2): 00/00, No Request on channel 0
  Tx(K1/K2): f0/05, Lockout of Protection on channel 0
  Counters
    ModeMismatch = 0
    ChanMismatch = 0
    PSBF         = 1
    FEPLF        = 0
  Aps channel 0  (5/4) (aps-protect)
    Current Conditions: SF
    Counters
      SignalDegrades = 0
      SignalFailures = 1
  Aps channel 1  (5/0) (aps-working)
    Current Conditions: None
    Counters
      SignalDegrades = 0
      SignalFailures = 0
      Switchovers    = 0
      LastSwitchover = Not Applicable
```