4 Configuring Unchannelized SONET/SDH Interfaces

This chapter provides information you need to configure unchannelized SONET/SDH interfaces.

Overview

The following line modules support unchannelized SONET/SDH interfaces:

- OC3 (dual port) line modules (OC3/STM1 only)
- OCx/STMx ATM line modules (OC3/STM1 and OC12/STM4)
- OCx/STMx POS line modules (OC3/STM1 and OC12/STM4)
- OC48 line modules (OC48/STM16)

For detailed specifications of these modules, see *ERX Installation and User Guide, Appendix B, Module Specifications*.

ERX Models

The ERX-700 series and the ERX-1410 system support the OC3 (dual port) and OCx/STMx line modules and associated I/O modules. The ERX-1440 system supports the OCx/STMx line modules and associated I/O modules, and the OC48 line module and its I/O module. The ERX-1440 system does not support the OC3 (dual port) line module and I/O module.

OC3 (Dual Port) Modules

The OC3 (dual port) line module pairs with OC3 I/O modules to deliver unchannelized OC3/STM1 ATM or POS operation via two line interfaces. I/O modules that support multimode or single-mode fiber via SC full duplex connectors are available.

Figure 4-1 shows the interface stack for OC3 (dual port) interfaces.

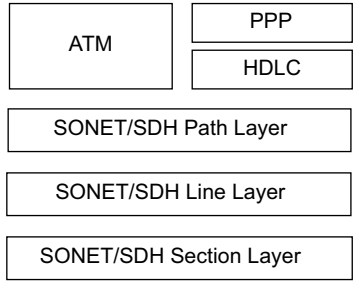

Figure 4-1 Stack for OC3 (dual port) interfaces

OCx/STMx ATM Line Modules

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

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

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

Figure 4-2 shows the interface stack for OCx/STMx ATM interfaces.

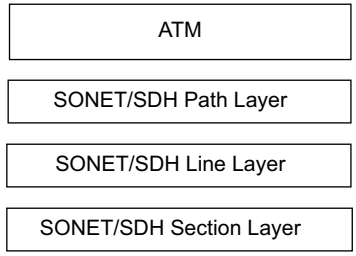

Figure 4-2 Interface stack for OCx/STMx ATM interfaces

OCx/STMx POS Line Modules

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

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

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

Figure 4-3 shows the interface stack for OCx/STMx POS interfaces.

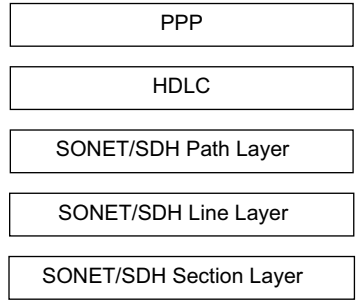

Figure 4-3 Interface stack for OCx/STMx POS and OC48/STM16 interfaces

OC48 Line Modules

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

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

The interface stack for the OC48/STM16 interfaces is the same as that for OCx/STMx POS interfaces (see Figure 4-3).

Higher-Level Protocols

See the release notes for information about the higher-level protocols that the interfaces described in this chapter support.

Exchanging Modules

If you replace an OC3 (dual port) line module and 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 *Replacing Line Modules* in *ERX System Basics Configuration Guide, Chapter 3, Managing Line Modules and SRP Modules*.

APS and MSP

The system supports APS and 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 the Release Notes.

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 system sends and receives data via both interfaces; however, in normal operation, only the signal on the working interface is used. if the signal on the primary interface fails, the system can use the signal on the protect interface. The process by which the system 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 the section *Numbering Schemes* later in this chapter.

Automatic Switchover

Provided you have not issued the **aps lockout** command for the protect interface, the system 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 system 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

The system supports *bidirectional* and *unidirectional* APS switching modes. By default, the system uses bidirectional mode, in which the system switches to the protect interface for both receipt and transmission of data, regardless of whether the signal failure is in the transmit or receive direction. In unidirectional mode, the system switches to the protect interface only for the direction in which signal failure occurs; for example, if there is a signal failure in the transmit direction, the system switches over to the protect interface for transmission but not receipt of data.

Reversion After Switchover

By default, if the system switches to the protect interface, it reverts to the working interface only if the protect interface subsequently fails. However, you can configure the system to revert to the working interface at a specified time after it recovers. This feature allows you to use the protect interface as a redundant connection that functions only when the working interface is not available.

Communication Methods

The system communicates with the remote device 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 4-1 and Table 4-2 show the meanings of the values of the K1 and K2 bytes.

Table 4-1 Explanation of K1 byte

Bit Value (87654321)	Meaning
Bits 8–5 represent the channel number.	
0	channel number of protect interface
0001–1110	channel number of working interface
Bits 4–1 represent a request.	
1111	Lockout of protection
1110	Forced switch
1101	High priority signal failure
1100	Low priority signal failure
1011	High priority signal degradation
1010	Low priority signal degradation
1001	Not used
1000	Manual switch
0111	Not used
0110	Wait-to-restore
0101	Not used
0100	Exercise
0011	Not used
0010	Reverse request
0001	Do not revert
0000	No request

Table 4-2 Explanation of K2 byte

Bit Value (87654321)	Meaning
Bits 8–5 represent the channel number.	
0	Channel number of protect interface
0001–1110	Channel number of working interface
Bit 4 indicates the type of redundancy.	
0	1+1 architecture
Bits 3–1 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)

References

Unchannelized SONET/SDH interfaces provide MIB support in accordance with RFC 2558 – Definitions of Managed Objects for the SONET/SDH Interface Type (March 1999)

For more information about APS/MSP, refer to the following documents:

- 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-09.txt (April 2003 expiration)

Numbering Schemes

When configuring or managing an interface, you must know the numbering scheme for identifying an interface. Unchannelized SONET/SDH interfaces use the *slot/port* format. Interfaces that support APS/MSP also use the APS/MSP *channel number*. These identifiers have the following definitions:

- *slot* – number of the slot in which the line module resides in the chassis.

  In the ERX-700 series, line module slots are numbered 2–6 (slots 0 and 1 are reserved for SRP modules). In an ERX-1400 series system, line module slots are numbered 0–5 and 8–13 (slots 6 and 7 are reserved for SRP modules).

- *port* – number of the port on the I/O module

  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.

- APS/MSP *channel number* – identifier of the working or protect (redundant) interface for configuration purposes. (See *APS and MSP*, earlier in this chapter.)

  The channel numbers of the working and protect interfaces are related to the number of the corresponding primary port. The channel number of the working interface is equal to the number of the corresponding primary port. The channel number of the protect interface is equal to the number of the corresponding primary port plus *n*, the number of active ports on the I/O module.

  For example, on an I/O module that provides one active port and one redundant port, if the primary port is labeled 0, the working interface has the channel number 0 and the protect interface has the channel number 1.

The following figures show the physical ports on the I/O modules described in this chapter. See *Chapter 1, Configuring Channelized T3 Interfaces*, for information on the ERX-700 series and the ERX-1400 series slot numbering.

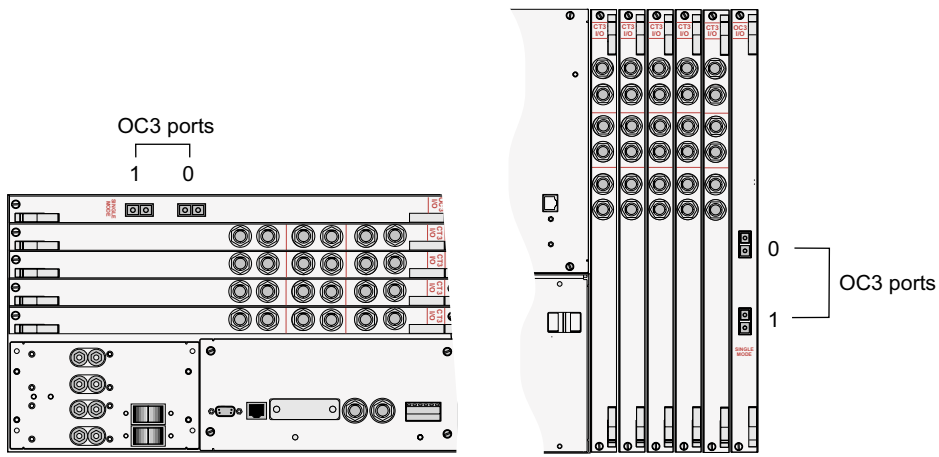

Figure 4-4 OC3 I/O modules in the ERX-700 series and the ERX-1410 system

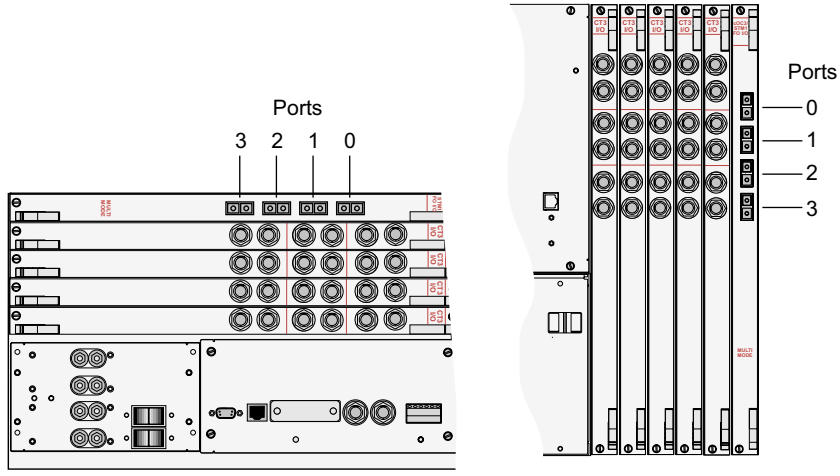

Figure 4-5 OC3-4 I/O modules in the ERX-700 series and the ERX-1400 series

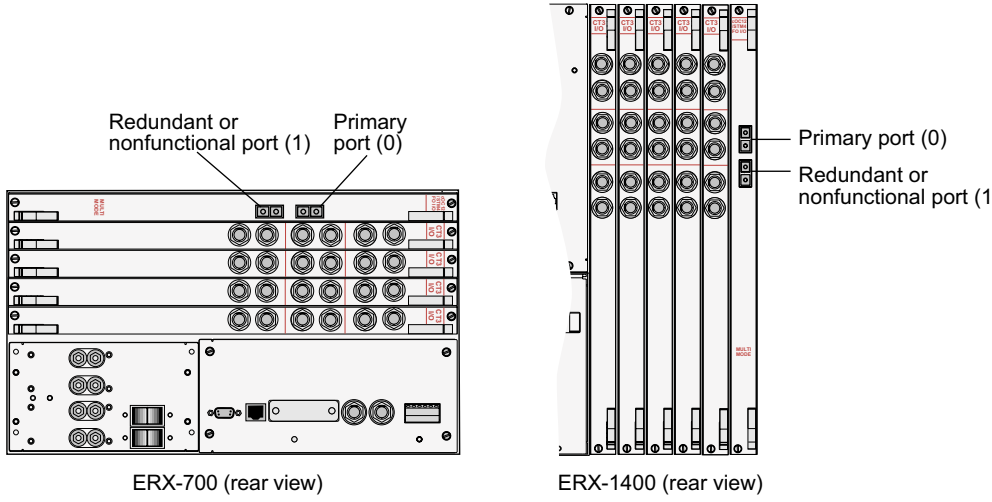

Figure 4-6 OC12 STM4 I/O modules in the ERX-700 series and the ERX-1400 series

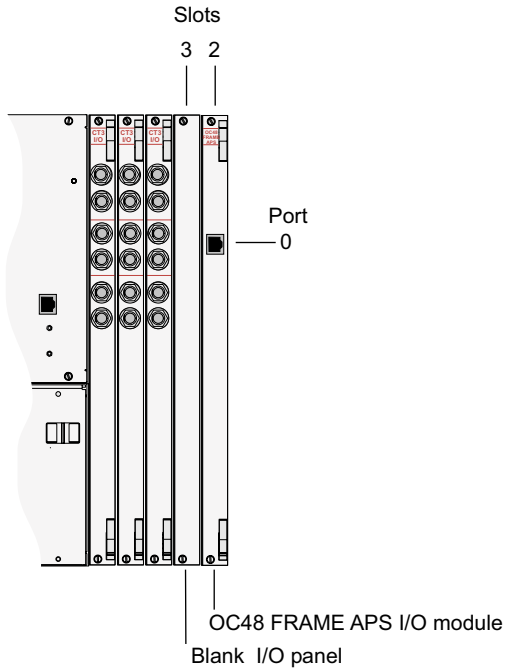

Figure 4-7 OC48 I/O modules in the ERX-1440 system

Configuring Interfaces

The first step to configuring an unchannelized SONET/SDH interface is to configure ATM or POS on the interface. For details on configuring POS and ATM, see *Chapter 10, Configuring ATM* and *Chapter 15, Configuring Packet over SONET.*

- On an OC3 (dual port) line module and an OC3 I/O module, you can configure either ATM or POS interfaces.
- On an OCx/STMx ATM line module and an OC3-4 or OC12 STM1 I/O module, you can only configure ATM interfaces.
- On an OCx/STMx POS line module and an OC3-4 or OC12 STM1 I/O module, you can only configure POS interfaces.
- On an OC48 line module and OC48 FRAME I/O module, you can only configure POS interfaces.

Configuring the SONET/SDH Layers

When you configure ATM or POS on an interface, you automatically configure parameters at the SONET/SDH layers. You do not need to configure the SONET/SDH layers separately. However, to provide compatibility with other SONET/SDH interfaces, you can:

1. Select a interface on which you want to configure SONET or SDH.
2. Specify a clock source for the interface.
3. Specify the type of interface: SONET or SDH.
4. 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 may 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 system'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 system's clock or the module's clock. You cannot configure some ports on the I/O module to use the system'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 system'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.
- Example

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

- There is no **no** version.

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 an interface.
- SONET/SDH interfaces are enabled by default.
- Example

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

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

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: *Configure the working interface before the protect interface. Otherwise the protect interface may assume the active role and, depending on the configuration, the system may prevent reversion to the working interface.*

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.
- By default, the primary port is not specified.
- Example

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

- 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.
- Specify one of the following keywords to indicate the alarm level:
  - sd-ber – alarm for signal degradation
  - sf-ber – alarm for signal failure
- Specify an integer *n* in the range 3–9, where *n* corresponds to a rate of 10^{-n} (10e-*n*) errors per second.
- Example

```
host1(config-controll)#threshold sf-ber 3
```

- Use the **no** version to restore the default, 6, for the specified alarm.

Configuring the Protect Interface

To configure the protect interface:

1. Select the interface.

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

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 system to revert to the working interface when it recovers.

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

6. (Optional) Specify that switchover should take 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 primary interface fails.
- You can only issue this command for the protect interface, not the working interface.
- Example

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

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

aps protect

- Use to configure an interface as a protect interface.
- You can only issue this command for the protect interface, not the working interface.
- Example

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

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

aps revert

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

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

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

aps unidirectional

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

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

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

```
host1(config-controller)#threshold sd-ber 5
```

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

```
host1(config-controller)#threshold sf-ber 7
```

threshold

- Use to set thresholds for the bit error rates associated with APS/MSP alarms.
- Specify one of the following keywords to indicate the alarm level:
  - sd-ber – alarm for signal degradation
  - sf-ber – alarm for signal failure
- Specify an integer *n* in the range 3–9 that corresponds to a bit error of 10^{-n} (10e-*n*).
- Example

```
host1(config-controller)#threshold sf-ber 3
```

- Use the **no** version to restore the default, 6, to the specified alarm.

Configuration Example

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

1 Configure the working interface.

```
host1(config)#controllerer sonet 3/0
host1(config-controller)#aps group boston
host1(config-controller)#aps working 1
host1(config-controller)#threshold sf-ber 3
```

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
```

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 protecting interface unless a request of equal or higher priority is in effect.
- This command has a higher priority than the following commands: **aps lockout**, **aps manual**, **aps protect**, **aps revert**
- You can only issue this command for the protect interface, not the working interface.
- Example

  ```
  host1(config-controll)#aps force
  ```

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

aps manual

- Use to switch from working interface to the protect interface unless a command of equal or higher priority is in effect.
- This command has a lower priority than the following commands: **aps force**, **aps lockout**, **aps protect**, **aps revert**
- The resulting configuration is not stored in NVS.
- You can only issue this command for the protect interface, not the working interface.
- Example

```
host1(config-controll)#aps manual
```

- 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 and sends an alarm indication signal (AIS) out toward the network.
  - **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 system and a SONET/SDH device at the other end of the line. This command defines:

- A message that the system sends from the specified interface to the SONET/SDH device at the other end of the line.
- A message that the system 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 system sends to or expects to receive from a SONET/SDH device connected to one of its SONET interfaces.
- Specify no path identifier for unchannelized SONET interfaces.
- Specify the keyword **msg** for a message that the system transmits for this path.
- Specify the keyword **exp-msg** to define a message that the system 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 system 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 Interfaces

You can monitor interface statistics and APS/MSP settings.

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 system 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

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

- There is no **no** version.

baseline path interface sonet

- Use to set a statistics baseline for the SONET/SDH path layer.
- The system 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

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

- There is no **no** version.

baseline section interface sonet

- Use to set a statistics baseline for the SONET/SDH section layer.
- The system 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

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

- 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
  - non channelized – unchannelized path
  - channelized – number of channels and speed for the interface
  - ifAdminStatus – configured status of the interface: up or down
  - snmp trap link-status – state of SNMP link status processing for the interface: enabled or disabled
  - Operational Status – physical state of the interface: up or down
  - 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:
  - module – internal clock is from the line module itself
  - chassis – internal clock is from the configured system clock
- Current section alarms – number of suspect bit patterns found in several consecutive frames in section layer
- Current line alarms – number of suspect bit patterns found in several consecutive frames in line layer
- Channel 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 controller: enabled or disabled
  - Operational Status – physical state of the controller: up or down
  - time since last status change: time the controller has been up or down
  - J1 transmit trace message – trace message sent to the remote device
  - J1 expected trace message – trace message expected from the remote device
- J1 received trace message – trace message received from the remote device

- Example 1

```
host1#show controllers sonet 4/0

oc3 4/0
non channelized
ifAdminStatus: up
snmp trap link-status: enabled
Operational Status: up
      time since last status change: 00:16:18
Loopback State: none
Mode: sonet
Timing source: internal module
Current section alarms: none
Current line alarms   : none

Channel configuration:
channel = 0, path = oc3, hierarchy = 1/1/1/0, current path
  alarms: none
 ifAdminStatus: up
 snmp trap link-status: disabled
 Operational Status: up
       time since last status change: 00:16:18
 J1 transmit trace message: hello
 J1 expected trace message: goodbye
 J1 received trace message: goodbye
```

show controllers sonet line | path | section

- Use to display statistics for the different layers in channelized SONET and SDH interfaces. Figure 4-2 and Figure 4-3 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.
- 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
    - Errored seconds – number of errored seconds encountered by a T1 or an E1 in an interval
    - Severely errored seconds – number of severely errored seconds encountered in an interval
    - Severely errored framing seconds – number of severely errored framing seconds encountered in an interval
    - Coding violations – number of coding violations encountered in an interval
    - Unavailable seconds – number of unavailable seconds encountered in an interval
  - › 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
  - › Last Far End Interval Counters - statistics for the remote connection associated with the SONET/SDH path in the previous 15-minute interval
- Example 1 – This example shows the MIB statistics for the path layer on interface 2/1.

```
host1#show controllers sonet 2/1 path

Channel number 1
Current Path Interval Counters
Current status                  = No Defect
Errored seconds                 = 0
Severly errored seconds         = 0
Coding violations               = 0
Unavailable seconds             = 248
```

```
Last Path Interval Counters
Errored seconds                  = 0
Severly errored seconds          = 0
Coding violations                = 0
Unavailable seconds              = 0
Current Far End Path Interval Counters
Errored seconds                  = 0
Severly errored seconds          = 0
Coding violations                = 0
Unavailable seconds              = 248

Far End Last Path Interval Counters
Errored seconds                  = 0
Severly errored seconds          = 0
Coding violations                = 0
Unavailable seconds              = 0
```

- Example 2 – This example shows the MIB statistics for the line layer on interface 2/1.

```
host1#show controllers sonet 2/1 line

Current Line Interval Counters
Current status                   = No Defect
Errored seconds                  = 0
Severly errored seconds          = 0
Coding violations                = 0
Unavailable seconds              = 190

Last Line Interval Counters
Errored seconds                  = 0
Severly errored seconds          = 0
Coding violations                = 0
Unavailable seconds              = 900

Current Far End Line Interval Counters
Errored seconds                  = 0
Severly errored seconds          = 0
Coding violations                = 0
Unavailable seconds              = 0

Far End Last Line Interval Counters
Errored seconds                  = 0
Severly errored seconds          = 0
Coding violations                = 0
Unavailable seconds              = 0
```

- Example 3 – This example shows the MIB statistics for the section layer on interface 2/1.

```
host1#show controllers sonet 2/1 section

Current Section Interval Counters
Current status                  = No Defect
Errored seconds                 = 0
Severly errored seconds         = 0
Severely errored framing seconds = 0
Coding violations               = 0

Last Section Interval Counters
Errored seconds                 = 0
Severly errored seconds         = 0
Severely errored framing seconds = 0
Coding violations               = 0
```

- Example 4 – This example illustrates the behavior of the **baseline section interface sonet** command. The examples show the MIB statistics of the section layer before and after the command is issued.

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

 Number of valid intervals - 0
 Time elapsed in current interval - 192

Current Section Interval Counters
Current status                  = No Defect
Errored seconds                 = 68
Severly errored seconds         = 68
Severely errored framing seconds = 2
Coding violations               = 4018

Total Section Counters
Errored seconds                 = 68
Severly errored seconds         = 68
Severely errored framing seconds = 2
Coding violations               = 4018

host1#baseline section interface sonet 2/0
host16#show controllers sonet 2/0 section total delta

Number of valid intervals - 0
Time elapsed in current interval - 209
```

```
Current Section Interval Counters
Current status                  = No Defect
Errored seconds                 = 68
Severly errored seconds         = 68
Severely errored framing seconds = 2
Coding violations               = 4018

Total Section Counters
Errored seconds                 = 0
Severly errored seconds         = 0
Severely errored framing seconds = 0
Coding violations               = 0
```

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.
- 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, 1–14 indicates a working interface.
  - ~ – interface is not currently active
  - Selected – interface is active
  - ~Selected – interface is not active
  - Bidirectional – system switches to the protect interface using the bidirectional switching mechanism
  - Unidirectional – system will switches to the protect interface using the unidirectional mode switching mechanism
  - Nonrevertive – system does not revert to the working interface when it recovers
  - Revertive – system 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

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

show aps group

- Use to display information about all APS/MSP groups or a specified APS/MSP group.
- Field descriptions
  - Current Conditions – current state of the group
  - Rx (K1/K2) – values of the received K1 and K2 bytes (see Table 4-1 and Table 4-2)
  - Tx (K1/K2) – values of the transmitted K1 and K2 bytes (see Table 4-1 and Table 4-2)
  - 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 three consecutive SONET/SDH frames out of the last twelve contain identical K1 bytes)
  - FEPLF – number of far-end protection line failures (signal failures detected on protect interface)
  - Aps channel - information about a specific APS channel
  - Current Conditions – current state of the interface
  - lockedOut – system is configured to prevent the protect interface from taking over if the primary interface fails.
  - SD – signal degradation is detected.
  - SF – signal failure is detected
  - switched – system 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 system has switched from the working interface to the protect interface
  - LastSwitchover – length of time that the working interface was active when the system last switched from the working interface to the protect interface; a value of zero indicates that the system has never switched to the protect interface or that this interface is the protect interface

- Examples

```
host1#show aps group
Aps group one
  Current Conditions: PSBF
  Rx(K1/K2): 00/00 Tx(K1/K2): c0/04
  Counters
    ModeMismatch = 0
    ChanMismatch = 0
    PSBF         = 1
    FEPLF        = 0
  Aps channel 0
    Current Conditions: SF
    Counters
      SignalDegrades = 0
      SignalFailures = 1
      Switchovers    = 0
      LastSwitchover = 0
  Aps channel 1
    Current Conditions: SF
    Counters
      SignalDegrades = 0
      SignalFailures = 1
      Switchovers    = 0
      LastSwitchover = 0
host1#show aps group one
Aps group one
  Current Conditions: PSBF
  Rx(K1/K2): 00/00 Tx(K1/K2): c0/04
  Counters
    ModeMismatch = 0
    ChanMismatch = 0
    PSBF         = 1
    FEPLF        = 0
```