



SONET Controller Commands on the Cisco IOS XR Software

This module provides command line interface (CLI) commands for configuring SONET operation, using Layer 1 SONET transport technology, on the Cisco XR 12000 Series Router.

The configuration of the SONET controller includes SONET Automatic Protection Switch (APS), which is a feature offering recovery from fiber (external) or equipment (interface and internal) failures at the SONET line layer. You must configure a SONET controller before you can configure a Packet-over-SONET/SDH (POS) interface or a Spatial Reuse Protocol (SRP) interface.

All SONET-related configurations of a SONET-based physical port are grouped under the SONET controller configuration submenu. The SONET path-related configuration commands are grouped under the SONET path submenu.

- [ais-shut \(SONET\), page 3](#)
- [ais-shut \(SONET path\), page 5](#)
- [aps group, page 6](#)
- [aps group \(global\), page 9](#)
- [au, page 11](#)
- [authenticate \(PGP\), page 13](#)
- [b3-ber-prdi, page 15](#)
- [channel local, page 16](#)
- [channel remote, page 18](#)
- [clear counters sonet, page 20](#)
- [clock source \(SONET\), page 22](#)
- [controller \(SONET\), page 23](#)
- [delay clear, page 25](#)
- [delay trigger, page 26](#)
- [down-when-looped, page 27](#)
- [force, page 28](#)

- framing (SONET), page 30
- line delay clear, page 32
- line delay trigger, page 33
- lockout, page 34
- loopback (SONET), page 36
- manual, page 38
- mode (SONET), page 40
- overhead (SONET), page 42
- overhead (SONET path), page 44
- path delay clear, page 46
- path delay trigger, page 47
- path (SONET), page 48
- report (SONET), page 50
- report (SONET path), page 52
- revert, page 54
- scrambling disable (SONET path), page 56
- show aps, page 58
- show aps agents, page 60
- show aps group, page 62
- show controllers pos, page 65
- show controllers sonet, page 71
- show sonet-local trace frt, page 79
- shutdown (SONET), page 80
- signalling, page 82
- sts, page 84
- timers (APS), page 85
- threshold (SONET), page 87
- threshold (SONET path), page 89
- tug3, page 91
- uneq-shut (SONET path), page 93
- unidirectional, page 94
- width, page 96

ais-shut (SONET)

To enable automatic insertion of a line alarm indication signal (LAIS) in the sent SONET signal whenever the SONET port enters the administrative shutdown state, use the **ais-shut** command in SONET/SDH configuration mode. To disable automatic insertion of a LAIS, use the **no** form of this command.

ais-shut

no ais-shut

Syntax Description This command has no keywords or arguments.

Command Default This command is disabled by default; no AIS is sent.

Command Modes SONET/SDH configuration

Command History	Release	Modification
	Release 3.2	This command was introduced.

Usage Guidelines

When the line is placed in administrative shutdown state, use the **ais-shut** command to send a signal to downstream equipment that indicates that there is a problem with the line.

The **ais-shut** command is ignored if automatic protection switching (APS) is running for the corresponding port, because the setting must be enabled for proper APS operation.

For SONET ports that do not have hardware support for LAIS insertion, the **ais-shut** command is disabled.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples In the following example, the alarm indication is forced on the SONET OC-3 controller:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/0/CPU0:router(config-sonet)# ais-shut
```

Related Commands

Command	Description
show controllers sonet, on page 71	Displays information about the operational status of SONET layers.

ais-shut (SONET path)

To enable automatic insertion of path alarm indication signal (PAIS) in the sent SONET signal whenever the SONET path enters the administratively down state, use the **ais-shut** command in SONET/SDH path configuration mode. To disable automatic insertion of PAIS in the SONET signal, use the **no** form of this command.

ais-shut

no ais-shut

Syntax Description This command has no keywords or arguments.

Command Default This command is disabled by default; no AIS is sent.

Command Modes SONET/SDH path configuration

Command History	Release	Modification
	Release 3.2	This command was introduced.

Usage Guidelines Use the **ais-shut** command to enable automatic insertion of PAIS in the appropriate sent SONET path overhead whenever the corresponding SONET path enters the administratively down state.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples The following example shows the alarm indication being enabled on all paths:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# path
RP/0/0/CPU0:router(config-sonet-path)# ais-shut
```

Related Commands	Command	Description
	show controllers sonet , on page 71	Displays information about the operational status of SONET layers.

aps group

To manually switch an automatic protection switching (APS) channel, use the **aps group** command in EXEC configuration mode.

aps group *number* {**force**| **manual**} {**0**| **1**} {**disable**| **enable**}

Syntax Description

<i>number</i>	Number of the APS group. Range is from 1 to 255.
force	Sends a forced APS request at the local end of a SONET link with the assigned channel number.
manual	Sends a manual APS request at the local end of a SONET link with the assigned channel number, which is implemented when no other higher-priority user-initiated or automatic requests are in effect.
0	Specifies that the protect channel should be switched.
1	Specifies that the working channel should be switched.
disable	Stops sending the SONET K1/K2 bit pattern that informs the remote end to switch ports.
enable	Starts sending a SONET K1/K2 bit pattern to inform the remote end to switch ports.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

In a multirouter APS topology, a manual or force request is supported only on the protect router.

Specify **0** or **1** to identify on which channel the traffic should be stopped and switched to the other channel. Therefore, **force 0** or **manual 0** moves traffic from the protect to the working channel, and **force 1** or **manual 1** moves traffic from the working to the protect channel.

Use the **force** keyword to manually switch the traffic to a protect channel. For example, if you need to change the fiber connection, you can manually force the working channel to switch to the protect interface.

A forced switch can be used to override an automatic (Signal Failed Signal Degraded) or a manual switch request. A lockout request (using the **lockout** command) overrides a force request.



Note If a request of equal or higher priority is in effect, you cannot use the **force** keyword to initiate a forced APS request at the local end of the SONET link.

Use the **manual** keyword to manually switch the circuit to a protect channel. For example, you can use this feature when you need to perform maintenance on the working channel. If a protection switch is already up, you can also use the **manual** keyword to revert the communication link to the working channel before the wait to restore (WTR) time period has expired. The WTR time period is set by the **revert** command. Use the **no** form of this command to cancel the switch.

A manual switch request can be used to control which channel carries the traffic when no other higher-priority user-initiated or automatic requests are in effect.

The manual request has the lowest priority among all user-initiated or automatic requests. Any other such requests override a manual request.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following examples show how to use the **aps group** command in EXEC mode to force or manually switch traffic, and enable and disable sending of the K1/K2 bit pattern to signal the switchover to the remote end:

```
RP/0/0/CPU0:router# aps group 1 force 1 enable
RP/0/0/CPU0:router# aps group 1 force 1 disable
```

```
RP/0/0/CPU0:router# aps group 1 manual 1 enable
RP/0/0/CPU0:router# aps group 1 manual 1 disable
```

```
RP/0/0/CPU0:router# aps group 1 force 0 enable
RP/0/0/CPU0:router# aps group 1 force 0 disable
```

```
RP/0/0/CPU0:router# aps group 1 manual 0 enable
RP/0/0/CPU0:router# aps group 1 manual 0 disable
```

Related Commands

Command	Description
aps group (global), on page 9	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
lockout, on page 34	Overrides a manual or forced APS request at the local end of the SONET link and block the protect channel from receiving traffic.
revert, on page 54	Enables automatic switchover from the protect interface to the working interface after the working interface becomes available.

Command	Description
signalling, on page 82	Configures the K1K2 overhead byte signaling protocol used for APS.
show aps, on page 58	Displays the operational status for all configured SONET APS groups.

aps group (global)

To add an automatic protection switching (APS) group and enter APS group configuration mode, use the **aps group** command in global configuration mode. To remove a group, use the **no** form of this command.

aps group *number*

no aps group *number*

Syntax Description

<i>number</i>	Number of the group. Range is from 1 to 255.
---------------	--

Command Default

No APS groups are defined.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

An APS group contains one protect (P) SONET port and one working (W) SONET port. The working and protect ports can reside on the same logical channel (LC), on different LCs in the same router, or on different routers. One APS group must be configured for each protect port and its corresponding working ports.

Use the **aps group (global)** command to enter APS group configuration mode and configure APS connections with other SONET equipment.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to use the **aps group** command in global configuration mode to configure APS group 1 and enter APS group configuration mode:

```
RP/0/0/CPU0:router(config)# aps group 1
RP/0/0/CPU0:router(config-aps)#
```

Related Commands

Command	Description
aps group, on page 6	Manually switches an APS channel.
authenticate (PGP), on page 13	Configures the authentication string for the PGP message exchange between the protect and working routers.
channel local, on page 16	Assigns local SONET physical ports as SONET APS channels in the current APS group.
channel remote, on page 18	Assigns a port and interface that is physically located in a remote router as a SONET working or protect APS channel.
lockout, on page 34	Overrides a manual or forced APS request at the local end of the SONET link and block the protect channel from receiving traffic.
revert, on page 54	Enables automatic switchover from the protect interface to the working interface after the working interface becomes available.
signalling, on page 82	Configures the K1K2 overhead byte signaling protocol used for APS.
timers (APS), on page 85	Changes the time between hello packets and the time before the protect interface process declares a working interface router to be down.
unidirectional, on page 94	Configures a protect interface for unidirectional mode.
show aps, on page 58	Displays the operational status for all configured SONET APS groups.

au

To specify the administrative unit (AU) group number and enter the AU controller configuration mode, use the **au** command in SONET controller configuration mode.

au *number*

Syntax Description

<i>number</i>	Administrative unit group number in the range from 1 to 48.
---------------	---

Command Default

The default is 1.

Command Modes

SONET controller configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

The **au** command enables you to begin configuring the interface in the AU controller configuration mode, where you can configure tributary unit groups (TUGs), virtual containers (VCs), and DS3s, such as shown in the following path example:

STM-1 -> AU-4 -> TUG-3 -> VC-3 -> DS-3

One AU-4 path is equivalent to three AU-3 paths. An administrative unit type 4 (AU-4) consists of three STM-1s or one STM-3. An administrative unit type 3 (AU-3) consists of one STM-1.



Note

Use the **au** command to configure one of the AUGs available for your card. The **au** command is not used to configure the *type* of AU path that you are configuring, such as AU-3 or AU-4, but rather is used to identify one AU group number in the supported range for the card and AU type that you are configuring. For example, the 1-Port Channelized OC-48/STM-16 SPA supports 16 AU-4 groups. Therefore, you can specify a number between 1 and 16 for the **au** command to configure SDH AU-4 on that card. The 1-Port Channelized OC-3/STM-1 SPA supports 1 AUG for AU-4, so you would specify **au 1**.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to specify AU 1.

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/0/CPU0:router(config-sonet)# au 1
RP/0/0/CPU0:router(config-auPath)#
```

Related Commands

Command	Description
tug3, on page 91	Specifies the tributary unit group (TUG) number and enters the TUG3 controller configuration mode.

authenticate (PGP)

To configure the authentication string for the Protect Group Protocol (PGP) message exchange between the protect and working routers, use the **authenticate** command in APS group configuration mode. To revert to the default authentication string, use the **no** form of this command.

authenticate *string*

no authenticate *string*

Syntax Description

<i>string</i>	Authentication string that the router uses to authenticate PGP message exchange between protect or working routers. The maximum length of the string is eight alphanumeric characters. Spaces are not accepted.
---------------	---

Command Default

The default authentication string is "cisco."

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **authenticate** command to configure the authentication string for the PGP message exchange between the protect and working routers. Use the **no** form of this command to revert to the default authentication string.

The **authenticate** command applies only in multirouter automatic protection switching (APS) group configurations.

In multirouter APS topologies, the protect and working routers communicate with each other through the User Datagram Protocol (UDP)-based Pretty Good Privacy protocol. Each Pretty Good Privacy packet contains an authentication string used for packet validation. The authentication string on all routers involved in the same APS group operation must match for proper APS operation.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example enables authentication for APS group 1 in abctown:

```
RP/0/0/CPU0:router(config)# aps group 1
```

```
RP/0/0/CPU0:router(config-aps)# authenticate abctown
```

Related Commands

Command	Description
aps group (global), on page 9	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
channel local, on page 16	Assigns local SONET physical ports as SONET APS channels in the current APS group.
channel remote, on page 18	Assigns a port and interface that is physically located in a remote router as a SONET working or protect APS channel.
show aps, on page 58	Displays the operational status for all configured SONET APS groups.

b3-ber-prdi

To enable sending of a path-level remote defect indication (PRDI) when the bit error rate (BER) bit interleaved parity (BIP) B3 threshold is exceeded, use the **b3-ber-prdi** command in SONET/SDH path configuration mode. To disable sending a PRDI, use the **no** form of this command.

b3-ber-prdi

no b3-ber-prdi

Syntax Description This command has no keywords or arguments.

Command Default This command is disabled by default; a PRDI is not sent.

Command Modes SONET/SDH path configuration

Command History	Release	Modification
	Release 3.9.0	This command was introduced.

Usage Guidelines

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples The following example shows a PRDI enabled on all paths:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# path
RP/0/0/CPU0:router(config-sonet-path)# b3-ber-prdi
```

Related Commands	Command	Description
	path (SONET), on page 48	Enters SONET/SDH path configuration mode.
	show controllers sonet, on page 71	Displays information about the operational status of SONET layers.

channel local

To assign local SONET physical ports as SONET automatic protection switching (APS) channels in the current APS group, use the **channel local** command in APS group configuration mode. To return to the default setting, use the **no** form of this command.

channel {0|1} **local** [**preconfigure**] **sonet** *interface-path-id*

no channel {0|1} **local** [**preconfigure**] **sonet** *interface-path-id*

Syntax Description

{0 1}	Assigns a protect or working channel type. 0 is protect, 1 is working.
preconfigure	(Optional) Specifies a SONET preconfiguration. This keyword is used only when a modular services or line card is not physically installed in a slot.
sonet	Specifies a SONET interface type.
interface-path-id	Physical interface or virtual interface. Note Use the show controllers sonet command to see a list of all controllers currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

A SONET APS local channel is not assigned.

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack/slot/module/port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
 - *rack*: Chassis number of the rack.
 - *slot*: Physical slot number of the line card.
 - *module*: Module number. A physical layer interface module (PLIM) is always 0.
 - *port*: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

Use the **channel local** command to designate SONET physical ports as SONET APS channels in the current APS group. Use the **channel remote** command to assign channels that are physically located in a different router.

Preconfigured interfaces are supported.

If the protect channel is local, it must be assigned using a **channel** command *before* any of the working channels are assigned. The reason is that having only a working channel assigned is a valid configuration for a working router in a multirouter APS topology and further attempts to configure a local protect channel are rejected.

The interface type must be a SONET controller.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to configure SONET 0/2/0/2 as a local protect channel:

```
RP/0/0/CPU0:router(config)# aps group 1
RP/0/0/CPU0:router(config-aps)# channel 0 local SONET 0/2/0/2
```

Related Commands

Command	Description
aps group (global), on page 9	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
channel remote, on page 18	Assigns a port and interface that is physically located in a remote router as a SONET working or protect APS channel.
show aps, on page 58	Displays the operational status for all configured SONET APS groups.

channel remote

To assign a port and interface that is physically located in a remote router as a SONET working or protect automatic protection switching (APS) channel, use the **channel remote** command in APS group configuration mode. To return to the default setting, use the **no** form of this command.

channel {0|1} **remote** *ip-address*

no channel {0|1} **remote** *ip-address*

Syntax Description

{0 1}	Assigns a protect or working channel type. 0 is protect, 1 is working.
<i>ip-address</i>	Remote router IP address in A.B.C.D format.

Command Default

A SONET APS remote channel is not assigned.

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **channel remote** command to assign working or protect channels that are physically located in a different router.

Use the **channel local** command to assign channels in the local router.



Note

The **channel remote** command should not be used in single-router APS topologies.

The *IP address* of the remote router is required only if a working channel configured as the protect router contacts all working routers.

Specifying a remote protect channel is optional. If you do not specify a remote protect channel, the default value of 0.0.0.0 is used. The protect router is always the one that contacts the working router. The working router replies to the protect router using the source address extracted from the incoming messages as the destination address. If an address other than 0.0.0.0 (the default value) is specified, the working router always uses that address when sending messages to the protect router.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

In the following examples, a remote channel with IP address 192.168.1.1 is assigned as the working channel:

```
RP/0/0/CPU0:router(config)# aps group 1  
RP/0/0/CPU0:router(config-aps)# channel 1 remote 192.168.1.1
```

Related Commands

Command	Description
aps group (global), on page 9	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
channel local, on page 16	Assigns local SONET physical ports as SONET APS channels in the current APS group.
show aps, on page 58	Displays the operational status for all configured SONET APS groups.

clear counters sonet

To clear SONET counters for a specific SONET controller, use the **clear counters sonet** command in EXEC mode.

clear counters sonet *interface-path-id*

Syntax Description

<i>interface-path-id</i>	Physical interface or virtual interface.
Note	Use the show controllers sonet command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack/slot/module/port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
 - *rack*: Chassis number of the rack.
 - *slot*: Physical slot number of the line card.
 - *module*: Module number. A physical layer interface module (PLIM) is always 0.
 - *port*: Physical port number of the interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

Use the **clear counters sonet** command to clear SONET counters for a specific SONET controller.

Task ID

Task ID	Operations
sonet-sdh	read, write

Task ID	Operations
basic-services	read, write

Examples

The following example shows the SONET counters being cleared on the SONET interface:

```
RP/0/0/CPU0:router# clear counters sonet 0/1/0/0
```

Related Commands

Command	Description
show controllers sonet , on page 71	Displays information about the operational status of SONET layers.

clock source (SONET)

To set the clock source of the sent signal on SONET ports, use the **clock source** command in SONET/SDH configuration mode. To cancel a clock source setting, use the **no** form of this command.

clock source {**internal**| **line**}

no clock source {**internal**| **line**}

Syntax Description

internal	Specifies that the controller will clock its sent data from its internal clock.
line	Specifies that the controller will clock its sent data from a clock recovered from the receive data stream of the line. This is the default value.

Command Default

The clock source for the controller is **line**.

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **clock source** command to configure which reference clock is used by the sender.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

In the following example, the SONET controller is configured to clock its sent data from its internal clock:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# clock source internal
```

Related Commands

Command	Description
show controllers sonet , on page 71	Displays information about the operational status of SONET layers.

controller (SONET)

To enter SONET/SDH configuration mode so that you can configure a specific SONET controller, use the **controller (SONET)** command in global configuration mode. To return to the default state, use the **no** form of this command.

controller [**preconfigure**] **sonet** *interface-path-id*

no controller [**preconfigure**] **sonet** *interface-path-id*

Syntax Description

preconfigure	(Optional) Specifies a SONET preconfiguration. Use the preconfigure keyword only when a modular services card is not physically installed in a slot.
sonet	Enters the SONET configuration mode or configures the SONET port controller specified by <i>interface-path-id</i> .
<i>interface-path-id</i>	Physical interface or virtual interface. Note Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack/slot/module/port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
 - *rack*: Chassis number of the rack.
 - *slot*: Physical slot number of the line card.
 - *module*: Module number. A physical layer interface module (PLIM) is always 0.
 - *port*: Physical port number of the interface.

- If specifying a virtual interface, the number range varies, depending on interface type.

Use the **path (SONET)** command to enter SONET/SDH path configuration mode to specify other SONET options for a SONET path.

Task ID

Task ID	Operations
interface	read, write

Task ID**Examples**

The following example shows how to enter SONET/SDH configuration mode for the SONET controller in slot number 2:

```
RP/0/0/CPU0:router(config)# controller SONET 0/2/0/1
RP/0/0/CPU0:router(config-sonet)#
```

The following example shows how to configure the SONET controller path (0/2/0/1) to send a path-level remote defect indication (PRDI) when the bit error rate (BER) bit interleaved parity (BIP) B3 threshold is exceeded. :

```
RP/0/0/CPU0:router(config)# controller SONET 0/2/0/1 path b3-ber-prdi
RP/0/0/CPU0:router(config-sonet)#
```

Related Commands

Command	Description
path (SONET) , on page 48	Enters SONET/SDH path configuration mode.
show controllers sonet , on page 71	Displays information about the operational status of SONET layers.

delay clear

To configure the amount of time before a Synchronous Transport Signal (STS) path delay trigger alarm is cleared, use the **delay clear** command in STS path configuration mode. To return the command to its default setting, use the **no** form of this command.

delay clear *value*

no delay clear *value*

Syntax Description	<i>value</i>	Value, in milliseconds, before an STS path delay trigger alarm is cleared. The range is from 0 to 180000. The default is 10 seconds.
---------------------------	--------------	--

Command Default	The default is 10 seconds.
------------------------	----------------------------

Command Modes	STS path configuration
----------------------	------------------------

Command History	Release	Modification
	Release 3.8.0	This command was introduced.

Usage Guidelines

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples The following example shows how to specify that STS path delay trigger alarms should be cleared after 7000 milliseconds:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/3
RP/0/0/CPU0:router(config-sonet)# sts 1
RP/0/0/CPU0:router(config-stsPath)# delay clear 7000
```

Related Commands	Command	Description
	delay trigger , on page 26	Configures a time value for the STS path delay trigger.

delay trigger

To configure a time value for the Synchronous Transport Signal (STS) path delay trigger, use the **delay trigger** command in STS path configuration mode. To return the command to its default setting, use the **no** form of this command.

delay trigger *value*

no delay trigger *value*

Syntax Description	<i>value</i>
	Value, in milliseconds, for the STS path delay trigger. The range is from 0 through 60000. The default is 0 seconds, which means that there is no delay.

Command Default The default is 0 seconds, which means that there is no delay.

Command Modes STS path configuration

Command History	Release	Modification
	Release 3.8.0	This command was introduced.

Usage Guidelines If the timer for the STS path delay trigger expires, an alarm is declared.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples The following example shows how to set the STS path delay trigger to 6000 milliseconds:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/3
RP/0/0/CPU0:router(config-sonet)# sts 1
RP/0/0/CPU0:router(config-stsPath)# delay trigger 6000
```

Related Commands	Command	Description
	delay clear , on page 25	Configures the amount of time before a STS path delay trigger alarm is cleared.

down-when-looped

To configure a SONET controller to inform the system that it is down when loopback is detected, use the **down-when-looped** command in SONET/SDH configuration mode.

down-when-looped

Syntax Description

This command has no keywords or arguments.

Command Default

The default is disabled.

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced.

Usage Guidelines

This command does not have a **no** form.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to configure a SONET controller to inform the system that the associated line is down if a loopback is detected:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/0/CPU0:router(config-sonet)# down-when-looped

down-when-looped is a traffic-affecting operation
```

Related Commands

Command	Description
loopback (SONET) , on page 36	Configures the SONET controller for loopback mode.

force

To initiate a forced automatic protection switching (APS) request at the local end of the SONET link, use the **force** command in EXEC configuration mode.


Note

Effective with Cisco IOS XR Release 3.8.0, this command is replaced by the **aps group force** command. See the [aps group](#), on page 6 command for more information.

force {0|1}

Syntax Description

0 1	initiate a forced automatic protection switching (APS) request at the local end of the SONET link Assigned channel number. 0 = protect, 1 = working.
--------------	---

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.8.0	This command was replaced by the aps group command.

Usage Guidelines

Note

If a request of equal or higher priority is in effect, you cannot use the **force** command to initiate a forced APS request at the local end of the SONET link.

Use the **force** command to manually switch the traffic to a protect channel. For example, if you need to change the fiber connection, you can manually force the working channel to switch to the protect interface.

The **0** or **1** keyword (by default 1) identifies on which channel the traffic should be stopped and moved on the protect channel. The **force 1 command** moves traffic from the working channel to the protect channel; the **force 0 command** moves traffic from the protect channel back to the working channel.

A forced switch can be used to override an automatic (Signal Failed Signal Degraded) or a manual switch request. A lockout request (via the **lockout** command) overrides a force request.

In a multirouter APS topology, a force request is allowed only on the protect router.

This command remains in effect until it is unconfigured by using the **no** form of the command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to move traffic from the working channel back to the protect channel:

```
RP/0/0/CPU0:router(config)# aps group 1
RP/0/0/CPU0:router(config-aps)# force 1
```

Related Commands

Command	Description
lockout , on page 34	Overrides a manual or forced APS request at the local end of the SONET link and block the protect channel from receiving traffic.
manual , on page 38	Initiates a manual APS request at the local end of the SONET link.

framing (SONET)

To specify the framing used on the SONET controller, use the **framing** command in SONET/SDH configuration mode. To disable framing on the SONET controller, use the **no** form of this command.

framing {sdh|sonet}

no framing {sdh|sonet}

Syntax Description

sdh	Selects Synchronous Digital Hierarchy (SDH) framing. This framing mode is typically used in Europe.
sonet	Selects SONET framing. This is the default.

Command Default

The default framing on SONET controllers is **sonet**.

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **framing** command to select either SONET or SDH framing on the selected physical port, if supported. For physical ports that do not support either of these two options, the **framing** command is disabled.

Use the **no** form of this command to disable SONET or SDH framing on the SONET controller.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

In the following example, the SONET controller is configured for SDH framing:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# framing sdh
```

In the following example, the SONET controller is configured for SONET framing:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
```

```
RP/0/0/CPU0:router(config-sonet)# framing sonet
```

Related Commands

Command	Description
show controllers sonet, on page 71	Displays information about the operational status of SONET layers.

line delay clear

To configure the amount of time before a SONET/SDH line delay trigger alarm is cleared, use the **line delay clear** command in SONET controller configuration mode. To return the command to its default setting, use the **no** form of this command.

line delay clear *value*

no line delay clear

Syntax Description	<i>value</i>
	Value, in milliseconds, before a SONET/SDH line delay trigger alarm is cleared. The range is 1000 to 180000. The default is 10.

Command Default The default is 10.

Command Modes SONET controller configuration

Command History	Release	Modification
	Release 3.8.0	This command was introduced.

Usage Guidelines If the timer for the SONET/SDH line delay clear expires, an alarm is cleared.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples The following example shows how to specify that SONET/SDH line delay trigger alarms should be cleared after 4000 milliseconds:

```
RP/0/0/CPU0:router(config)# controller SONET 0/0/0/2
RP/0/0/CPU0:router(config-sonet)# line delay clear 4000
```

Related Commands	Command	Description
	line delay trigger , on page 33	Configures a time value for the SONET/SDH line delay trigger.

line delay trigger

To configure a time value for the SONET/SDH line delay trigger, use the **line delay trigger** command in SONET controller configuration mode. To return the command to its default setting, use the **no** form of this command.

line delay trigger *value*

no line delay trigger

Syntax Description	<i>value</i>	Value, in milliseconds, for the SONET/SDH line delay trigger. The range is 0 to 60000.
---------------------------	--------------	--

Command Default The default is 0, which means that there is no delay.

Command Modes SONET controller configuration

Command History	Release	Modification
	Release 3.8.0	This command was introduced.

Usage Guidelines If the timer for the SONET/SDH line delay trigger expires, an alarm is raised.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples The following example shows how to set the SONET/SDH line delay trigger to 3000 milliseconds:

```
RP/0/0/CPU0:router(config)# controller SONET 0/0/0/2
RP/0/0/CPU0:router(config-sonet)# line delay trigger 3000
```

Related Commands	Command	Description
	line delay clear , on page 32	Configures the amount of time before a SONET/SDH line delay trigger alarm is cleared.

lockout

To override a manual or forced APS request at the local end of the SONET link and block the protect channel from receiving traffic, use the **lockout** command in APS group configuration mode. To remove the lockout, use the **no** form of this command.

lockout [0]

no lockout [0]

Syntax Description

[0]	(Optional) Specifies blocking of the protect channel from a manual or forced APS request. This is the default.
-----	--

Command Default

The default is 0.

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

A lockout switch request can be used to override a force, an automatic (Signal Failed or Signal Degraded), or a manual switch request. No other request can override a lockout request; it has the highest possible priority. In a multirouter APS topology, a **lockout** request is allowed only on the protect router. This command remains in effect until it is unconfigured by using the **no** form of the command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to lock out or prevent the channel from switching to a protect router in the event that the working channel becomes unavailable:

```
RP/0/0/CPU0:router(config)# aps group 1
RP/0/0/CPU0:router(config-aps)# lockout 0
```

Related Commands

Command	Description
aps group (global), on page 9	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
aps group, on page 6	Manually switches an APS channel.

loopback (SONET)

To configure the SONET controller for loopback mode, use the **loopback** command in SONET/SDH configuration mode. To remove the loopback SONET command from the configuration file, use the **no** form of this command.

loopback {**internal**| **line**}

no loopback {**internal**| **line**}

Syntax Description

internal	Specifies that all the packets be looped back from the source.
line	Specifies that the incoming network packets be looped back to the SONET network.

Command Default

This command is disabled by default.

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

The SONET and Synchronous Digital Hierarchy (SDH) transport layers support two loopback operation modes for diagnostic purposes: internal and line. In the terminal (internal) loopback, the sent signal is looped back to the receiver. In the facility (line) loopback, the signal received from the far end is looped back and sent on the line. The two loopback modes cannot be active at the same time. In normal operation mode, neither of the two loopback modes is enabled.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

In the following example, all packets are looped back to the SONET controller:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# loopback internal
```

Related Commands

Command	Description
show controllers sonet, on page 71	Displays information about the operational status of SONET layers.

manual

To initiate a manual automatic protection switching (APS) request at the local end of the SONET link, use the **manual** command in APS group configuration mode. To cancel the switch, use the **no** form of this command.



Note

Effective with Cisco IOS XR Release 3.8.0, this command is replaced by the **aps group manual** command. See the [aps group, on page 6](#) command for more information.

manual *channel-number* {0|1}

no manual *channel-number* {0|1}

Syntax Description

<i>channel-number</i>	The assigned channel number: 0 = protect, 1 = working.
-----------------------	--

Command Default

No circuit is switched.

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.8.0	This command was replaced by the aps group command.

Usage Guidelines

Use the **manual** command to manually switch the circuit to a protect channel. For example, you can use this feature when you need to perform maintenance on the working channel. If a protection switch is already up, you can also use the **manual** command to revert the communication link to the working channel before the wait to restore (WTR) time period has expired. The WTR time period is set by the **revert** command. Use the **no** form of this command to cancel the switch.

A manual switch request can be used to control which channel carries the traffic when no other higher-priority user-initiated or automatic requests are in effect.

The **0** or **1** keyword identifies the channel from which the traffic should be moved on the protect channel:

- The **manual 1** command moves traffic on to the protect channel.
- The **manual 0** command moves traffic on to the working channel.

The manual request has the lowest priority among all user-initiated or automatic requests. Any other such requests override a manual request.

In a multirouter APS topology a **manual** request is allowed only on the protect router.

This command remains in effect until it is unconfigured by using the **no** form of the command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to move traffic on to the protect router:

```
RP/0/0/CPU0:router(config)# aps group 1
RP/0/0/CPU0:router(config-aps)# manual 1
```

Related Commands

Command	Description
force, on page 28	Initiates a forced APS request at the local end of the SONET link.
lockout, on page 34	Overrides a manual or forced APS request at the local end of the SONET link and block the protect channel from receiving traffic.

mode (SONET)

To set the mode of an STS path, AU path, T3 controller, or TUG3 controller, use the **mode** command in the applicable controller configuration mode. To disable the mode, use the **no** form of this command.

STS Controller Configuration Mode

```
mode {t3| vt15-t1| pos}
no mode {t3| vt15-t1| pos}
```

AU Controller Configuration Mode

```
mode {e3| t3| tug 3}
no mode {e3| t3| tug 3}
```

T3 Controller Configuration Mode

```
mode {e1| serial| t1}
no mode {e1| serial| t1}
```

TUG3 Controller Configuration Mode

```
mode {c12| c12-e1| e3| serial| t3}
no mode {c12| c12-e1| e3| serial| t3}
```

Syntax Description

t3	Specifies the mode of the port to be channelized as an AU3 or a TUG3 path carrying T3.
vt15-t1	Specifies the mode of the port to be channelized VT15-T1.
pos	Specifies the mode of the port to be channelized POS.
tug3	Specifies the mode of the port to be channelized TUG3.
e1	Specifies the mode of the port to be channelized E1.
serial	Specifies the mode of the port to be clear channel serial.
t1	Specifies the mode of the port to be channelized T1.
c12	Specifies the mode of the port to be channelized as a TUG3 path carrying TU-12.
c12-e1	Specifies the mode of the port to be channelized by TUG3 path carrying c12 to E1.
e3	Specifies the mode of the port to be channelized as an AU3 or a TUG3 path carrying E3.

Command Default No default behavior or values

Command Modes STS controller configuration
 AU controller configuration
 T3 controller configuration
 TUG3 controller configuration

Command History	Release	Modification
	Release 3.5.0	This command was introduced.

Usage Guidelines For channelized SPAs, you must use the **mode** command before you can configure any channelized controllers.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples The following example shows how to set the mode of a T3 controller to channelized T1:

```
RP/0/0/CPU0:router(config)# controller t3 0/1/0/0/1
RP/0/0/CPU0:router(config-t3)# mode t1
```

Related Commands	Command	Description
	width, on page 96	Sets the number of paths in a stream.

overhead (SONET)

To set the SONET overhead bytes in the frame header to a specific standards requirement, or to ensure interoperability with equipment from another vendor, use the **overhead** command in SONET/SDH configuration mode. To remove the setting of the SONET overhead bytes from the configuration file and restore the default condition, use the **no** form of this command.

overhead {j0| s1s0} *byte-value*

no overhead {j0| s1s0} *byte-value*

Syntax Description

j0	Sets the J0/C1 byte value in the SONET section overhead. For interoperability with Synchronous Digital Hierarchy (SDH) equipment in Japan, use the value 0x1. Default is 0xcc.
s1s0	Sets the SS bits value of the H1 byte in the SONET line overhead. Use the following values to tell the SONET transmission equipment the S1 and S0 bit: <ul style="list-style-type: none"> • For SONET mode, use 0 (this is the default). • For SDH mode, use 2. Range is from 0 to 3. Default is 0. Values 1 and 3 are undefined.
byte-value	Byte value to which the j1 or s1s0 keyword should be set. Range is from 0 to 255.

Command Default

byte-value: 0x01 (j0)

byte-value: 0 (s1s0)

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **overhead** command to set the SONET overhead bytes in the frame header to a specific standards requirement.

Use the **no** form of this command to remove the setting of the SONET overhead bytes from the configuration file and restore the default condition.

For the **j0** keyword, the value that you use for the trace byte depends on the type of equipment being used. For the **s1s0** keyword, the value that you use depends on whether you are using the SONET or SDH mode. For SONET mode, use the value 0 (the default). For SDH mode, use the value 2.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to set the SS bits value of the H1 byte in the SONET line overhead to 2 for SDH:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/1
RP/0/0/CPU0:router(config-sonet)# overhead s1s0 2
```

The following example shows how to set the SS bits value of the H1 byte in the SONET line overhead to 0 for SONET:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/1
RP/0/0/CPU0:router(config-sonet)# overhead s1s0 0
```

overhead (SONET path)

To set the SONET path overhead bytes in the frame header to a specific standards requirement or to ensure interoperability with equipment from another vendor, use the **overhead** command in SONET/SDH path configuration mode. To remove the setting of the SONET path overhead bytes from the configuration file and restore the system to its default condition, use the **no** form of this command.

overhead {*c2 byte-value*| **expected-trace** *LINEascii-text*| **j1** *ascii-value*}

no overhead {*c2 byte-value*| **expected-trace** *LINEascii-text*| **j1** *ascii-value*}

Syntax Description

c2 <i>byte-value</i>	Specifies Synchronous Transport Signal (STS) synchronous payload envelope (SPE) content (C2) byte. The transmitted c2 value is automatically set to 0xCF for unscrambled payload and 0x16 for scrambled payload. If c2 is configured to a user-specified value, the user-specified value is always applied regardless of scrambling. Replace the <i>byte-value</i> argument with the byte value to which the c2 keyword should be set. Range is from 0 to 255. Default value is 0.
j1 <i>ascii-value</i>	Configures the SONET path trace (j1) buffer. Replace the <i>ascii-value</i> argument with a text string that describes the SONET path trace buffer. Default is a 64-byte path trace ASCII message, which includes default information such as router name, (Layer 2 —POS) interface name, and IP address, if applicable.
expected-trace <i>LINE</i> <i>ascii-text</i>	Configures the SONET/SDH path trace. The trace monitoring feature allows a node to perform trace monitoring by using the SONET/SDH capabilities. Replace the <i>LINE</i> with the expected trace message Replace the <i>ascii-text</i> argument with a text string that describes the SONET path trace buffer. Default is a 64-byte path trace ASCII message, which includes default information such as router name, (Layer 2 —POS) interface name, and IP address, if applicable. the <i>LINE</i> is the expected trace message which should match else ptim mismatch would be reported

Command Default

byte-value: 0xCF

byte-value: 0

Command Modes

SONET/SDH path configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

The SONET standards permit or require user access for configuration of some bytes or bits in the SONET path overhead. Use the **overhead** command to set the SONET path overhead bytes in the frame header to a specific standards requirement. Use the **no** form of this command to remove the setting of the SONET path overhead bytes from the configuration file and restore the system to its default condition.

Use the **c2** keyword to configure the desired C2 byte value in the SONET path overhead.

Use the **j1** keyword to configure a user-defined path trace message in the j1 bytes of the SONET path overhead. For the **j1** keyword, use the default message or insert your own message that has a maximum of 62 characters. If no user-defined message is configured, a default message is automatically generated, containing the router name, the controller name, its IP address, and the values of the sent and received K1 and K2 bytes in the SONET line overhead.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to set the STS SPE C2 byte in the SONET path frame header:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# path
RP/0/0/CPU0:router(config-sonet-path)# overhead c2 0x13
```

Related Commands

Command	Description
scrambling disable (SONET path), on page 56	Disables payload scrambling on a SONET path.

path delay clear

To configure the amount of time before a SONET/SDH path delay trigger alarm is cleared, use the **path delay clear** command in SONET controller configuration mode. To return the command to its default setting, use the **no** form of this command.

path delay clear *value*

no path delay clear

Syntax Description	<i>value</i>
	Value, in milliseconds, before a SONET/SDH path delay trigger alarm is cleared. The range is 1000 to 180000. The default is 10 seconds.

Command Default The default is 10 seconds.

Command Modes SONET controller configuration

Command History	Release	Modification
	Release 3.8.0	This command was introduced.

Usage Guidelines

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples The following example shows how to specify that SONET/SDH path delay trigger alarms should be cleared after 7000 milliseconds:

```
RP/0/0/CPU0:router(config)# controller SONET 0/0/0/1
RP/0/0/CPU0:router(config-sonet)# path delay clear 7000
```

Related Commands	Command	Description
	path delay trigger , on page 47	Configures a time value for the SONET/SDH path delay trigger.

path delay trigger

To configure a time value for the SONET/SDH path delay trigger, use the **path delay trigger** command in SONET controller configuration mode. To return the command to its default setting, use the **no** form of this command.

path delay trigger *value*

no path delay trigger

Syntax Description	<i>value</i>	Value, in milliseconds, for the SONET/SDH path delay trigger. The range is 0 to 60000.
---------------------------	--------------	--

Command Default The default is 0, which means that there is no delay.

Command Modes SONET controller configuration

Command History	Release	Modification
	Release 3.8.0	This command was introduced.

Usage Guidelines If the timer for the SONET/SDH path delay trigger expires, an alarm is declared.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples The following example shows how to set the SONET/SDH path delay trigger to 6000 milliseconds:

```
RP/0/0/CPU0:router(config)# controller SONET 0/0/0/1
RP/0/0/CPU0:router(config-sonet)# path delay trigger 6000
```

Related Commands	Command	Description
	path delay clear , on page 46	Configures the amount of time before a SONET/SDH path delay trigger alarm is cleared.

path (SONET)

To enter SONET/SDH path configuration mode, use the **path** command in SONET controller configuration mode.

path

Syntax Description This command has no keywords or arguments.

Command Default No default behavior or values

Command Modes SONET controller configuration

Command History	Release	Modification
	Release 3.2	This command was introduced.

Usage Guidelines

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples The following example shows how to access SONET path submode from SONET controller configuration mode:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/0/CPU0:router(config-sonet)# path
```

Related Commands	Command	Description
	ais-shut (SONET path), on page 5	Enables automatic insertion of PAIS in the sent SONET signal whenever the SONET path enters the administratively down state.
	b3-ber-prdi, on page 15	Enables sending of a PRDI when the BER bit interleaved parity (BIP) B3 threshold is exceeded.
	delay clear, on page 25	Configures the amount of time before a STS path delay trigger alarm is cleared.

Command	Description
delay trigger , on page 26	Configures a time value for the STS path delay trigger.
overhead (SONET path) , on page 44	Sets the SONET path overhead bytes in the frame header to a specific standards requirement or to ensure interoperability with equipment from another vendor.
report (SONET path) , on page 52	Configures whether or not selected SONET alarms are logged to the console for a SONET path controller.
scrambling disable (SONET path) , on page 56	Disables payload scrambling on a SONET path.
threshold (SONET path) , on page 89	Sets the bit error rate (BER) threshold values of the specified alarms for a SONET path.
uneq-shut (SONET path) , on page 93	Enables automatic insertion of P-UNEQ code (0x00) in the sent SONET path overhead C2 byte.

report (SONET)

To permit selected SONET alarms to be logged to the console for a SONET controller, use the **report** command in SONET/SDH configuration mode. To disable logging of select SONET alarms, use the **no** form of this command.

report [b1-tca| b2-tca| lais| lrdi| sd-ber| sf-ber| slof| slos]

no report [b1-tca| b2-tca| lais| lrdi| sd-ber| sf-ber| slof| slos]

Syntax Description

b1-tca	(Optional) Reports bit 1 (B1) bit error rate (BER) threshold crossing alert (TCA) errors.
b2-tca	(Optional) Reports bit 2 (B2) BER TCA errors.
lais	(Optional) Reports line alarm indication signal (LAIS) errors.
lrdi	(Optional) Reports line remote defect indication errors.
sd-ber	(Optional) Reports signal degradation BER errors.
sf-ber	(Optional) Reports signal failure BER errors.
slof	(Optional) Reports section loss of frame (SLOF) errors.
slos	(Optional) Reports section loss of signal (SLOS) errors.

Command Default

Alarms from the following keywords are reported by default:

- b1-tca
- b2-tca
- sf-ber
- slof
- slos

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Reporting an alarm means that the alarm can be logged to the console, but it is no guarantee that it is logged. SONET alarm hierarchy rules dictate that only the most severe alarm of an alarm group is reported. Whether an alarm is reported or not, you can check the current state of masked alarm, a problem indication that is a candidate for an alarm, by displaying the “Masked Alarms” line in the **show controllers sonet** command output.

For B1, the bit interleaved parity (BIP) error report is calculated by comparing the BIP-8 code with the BIP-8 code that is extracted from the B1 byte of the following frame. Differences indicate that section-level bit errors have occurred.

For B2, the BIP error report is calculated by comparing the BIP-8/24 code with the BIP-8 code that is extracted from the B2 byte of the following frame. Differences indicate that line-level bit errors have occurred.

Path AIS is sent by line terminating equipment to alert the downstream path terminating equipment (PTE) that it has detected a defect on its incoming line signal.

Path loss of pointer (LOP) is reported as a result of an invalid pointer (H1, H2) or an excess number of new data flag enabled indications.

SLOF is detected when an error-framing defect on the incoming SONET signal persists for 3 microseconds.

SLOS is detected when an all-zeros pattern on the incoming SONET signal is observed. This defect might also be reported if the received signal level drops below the specified threshold.

To determine the alarms that are reported on the controller, use the **show controllers sonet** command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to enable the reporting of line AIS alarms on the path controller:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/1
RP/0/0/CPU0:router(config-sonet)# report lais
```

Related Commands

Command	Description
show controllers sonet , on page 71	Displays information about the operational status of SONET layers.

report (SONET path)

To configure whether or not selected SONET alarms are logged to the console for a SONET path controller, use the **report** command in SONET/SDH path configuration mode. To disable or re-enable the logging of select SONET alarms, use the **no** form of this command.

report [b3-tca| pais| plop| pplm| prdi| ptim]

no report [b3-tca| pais| plop| pplm| prdi| ptim]

Syntax Description

b3-tca	(Optional) Reports bit 3 (B3) bit error rate (BER) threshold crossing alert (TCA) errors.
pais	(Optional) Reports path alarm indication signal (PAIS) errors.
plop	(Optional) Reports path loss of pointer (PLOP) errors.
pplm	(Optional) Reports path payload mismatch (PPLM) defect errors.
prdi	(Optional) Reports path remote defect indication (PRDI) errors.
ptim	(Optional) Reports path trace identity mismatch (PTIM) defect errors.

Command Default

Alarms from the following keywords are reported:

- b3-tca
- plop

Command Modes

SONET/SDH path configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Reporting an alarm means that the alarm can be logged to the console, but it is no guarantee that it is logged. SONET alarm hierarchy rules dictate that only the most severe alarm of an alarm group is reported. Whether an alarm is reported or not, you can view the current state of a masked alarm, a problem indication that is a candidate for an alarm, by inspecting the “Masked Alarms” line displayed in the **show controllers sonet** command output.

For B3, the bit interleaved parity (BIP) error report is calculated by comparing the BIP-8 code with the BIP-8 code that is extracted from the B3 byte of the following frame. Differences indicate that path-level bit errors have occurred.

Path AIS is sent by line-terminating equipment to alert the downstream path-terminating equipment (PTE) that it has detected a defect on its incoming line signal.

Path LOP is reported as a result of an invalid pointer (H1, H2) or an excess number of new data flag enabled indications.

To determine the alarms that are reported on the controller, use the **show controllers sonet** command.

All report commands accept the default option. The default reporting values are determined based upon the SONET standards specifications and are clearly identified in the corresponding command's help string.

**Note**

The reporting of B3 BER TCA errors and path LOP errors is enabled by default.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

In the following example, reporting of path PAIS alarms is enabled:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# path
RP/0/0/CPU0:router(config-sonet-path)# report pais
```

Related Commands

Command	Description
show controllers sonet , on page 71	Displays information about the operational status of SONET layers.

revert

To enable automatic switchover from the protect interface to the working interface after the working interface becomes available, use the **revert** command in APS configuration mode. To disable automatic switchover, use the **no** form of this command.

revert *minutes*

no revert *minutes*

Syntax Description

<i>minutes</i>	Number of minutes until the circuit is switched back to the working interface after the working interface is available.
----------------	---

Command Default

minutes: 0

Automatic switchover is disabled.

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **revert** command to enable and disable revertive APS operation mode, if needed. The revertive APS operation mode of the routers should be matched with the APS operation mode of the connected SONET equipment. Use the **no** form of this command to disable automatic switchover.

The revertive APS operation mode is the recommended operation mode because it offers better traffic protection during various possible software failures and upgrade or downgrade scenarios.

The *minutes* argument indicates how many minutes will elapse until automatic protection switching (APS) decides to switch traffic back from protect to working after the condition that caused an automatic (Signal Failed or Signal Degrade) switch to protect disappears. A value of 0 (default) disables APS revertive mode.

In a multirouter APS topology, the **revert** command is allowed only on the protect router.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to enable APS to revert to the protect or working channel after 5 minutes have elapsed:

```
RP/0/0/CPU0:router(config)# aps group 1  
RP/0/0/CPU0:router(config-aps)# revert 5
```

Related Commands

Command	Description
aps group (global), on page 9	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
show aps, on page 58	Displays the operational status for all configured SONET APS groups.

scrambling disable (SONET path)

To disable payload scrambling on a SONET path, use the **scrambling disable** command in SONET/SDH path configuration mode. To enable payload scrambling after it has been disabled, use the **no** form of this command.

scrambling disable

no scrambling disable

Syntax Description This command has no keywords or arguments.

Command Default The default is enable (SONET payload scrambling is on).

Command Modes SONET/SDH path configuration

Command History	Release	Modification
	Release 3.2	This command was introduced.

Usage Guidelines SONET payload scrambling applies a self-synchronous scrambler (x43+1) to the synchronous payload envelope (SPE) of the controller to ensure sufficient bit transition density. Both ends of the connection must be configured using SONET path scrambling.

If the hardware payload scrambling support is not user-configurable, or is not supported, the **scrambling disable** command may be rejected.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples In the following example, scrambling is disabled for the path:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# path
RP/0/0/CPU0:router(config-sonet-path)# scrambling disable
```

Related Commands

Command	Description
show controllers sonet, on page 71	Displays information about the operational status of SONET layers.

show aps

To display the operational status for all configured SONET automatic protection switching (APS) groups, use the **show aps** command in EXEC mode.

show aps

Syntax Description This command has no keywords or arguments.

Command Default No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced.

Usage Guidelines Use the **show aps** command to display operational status for all configured SONET APS groups. Displaying the SONET APS operational data is considered of lower priority than the APS operation itself. Because the information is collected from several sources scattered across the various nodes involved, there is a small probability that some states will change while the command is being run. The command should be reissued for confirmation before decisions are made based on the results displayed.

Task ID	Task ID	Operations
	sonet-sdh	read

Examples The following is sample output from the **show aps** command:

```
RP/0/0/CPU0:router# show aps
APS Group 1:
Protect ch 0 (SONET3_0):Enabled
  SONET framing, SONET signalling, bidirectional, revertive (300 sec)
  Rx K1:0x21 (Reverse Request - Working)
    K2:0x15 (bridging Working, 1+1, bidirectional)
  Tx K1:0x81 (Manual Switch - Working)
    K2:0x15 (bridging Working, 1+1, bidirectional)
Working ch 1 (SONET2_0):Disabled
  Rx K1:0x00 (No Request - Null)
    K2:0x00 (bridging Null, 1+1, non-aps)
  Tx K1:0x00 (No Request - Null)
    K2:0x00 (bridging Null, 1+1, non-aps)
```

```

APS Group 3:
PGP:protocol version: native 2 adopted 2
PGP:Authentication "cisco", hello timeout 1 sec, hold timeout 3 sec
Protect ch 0 (SONET3_1):Disabled
  SONE_T framing, SONE_T signalling, bidirectional, non-revertive
  Rx K1:0x00 (No Request - Null)
     K2:0x05 (bridging Null, 1+1, bidirectional)
  Tx K1:0x00 (No Request - Null)
     K2:0x05 (bridging Null, 1+1, bidirectional)
Working ch 1 (192.168.1.1):Enabled
APS Group 49:
Protect ch 0 (SONET0_2_0_0):Disabled
  SONE_T framing, SONE_T signalling, unidirectional, non-revertive
  Rx K1:0x00 (No Request - Null)
     K2:0x00 (bridging Null, 1+1, non-aps)
  Tx K1:0x00 (No Request - Null)
     K2:0x04 (bridging Null, 1+1, unidirectional)
Working ch 1 (SONET0_2_0_1):Enabled
  SONE_T framing, unidirectional
  Rx K1:0x00 (No Request - Null)
     K2:0x00 (bridging Null, 1+1, non-aps)
  Tx K1:0x00 (No Request - Null)
     K2:0x00 (bridging Null, 1+1, non-aps)
APS Group 6:
PGP:protocol version: native 2 adopted 2
PGP:Authentication "cisco", hello timeout 1 sec, hold timeout 3 sec
Protect ch 0 (192.168.3.2 - auto):Disabled
Working ch 1 (SONET6_0):Enabled
  Rx K1:0x00 (No Request - Null)
     K2:0x00 (bridging Null, 1+1, non-aps)
  Tx K1:0x00 (No Request - Null)
     K2:0x00 (bridging Null, 1+1, non-aps)

```

Table 1: show aps Field Descriptions

Field	Description
APS Group	Assigned number of the APS group. Range is from 1 through 255.
Protect ch	Number and address of the protect channel interface.
Working ch	Number and address of the working channel interface.

Related Commands

Command	Description
show aps agents , on page 60	Displays the status of the APS WP distributed communication subsystem.
show aps group , on page 62	Displays information about the APS groups.

show aps agents

To display the status of the automatic protection switching (APS) working to protect (WP) distributed communication subsystem, use the **show aps agents** command in EXEC mode.

show aps agents

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **show aps agents** command to display the status of the APS WP distributed communication subsystem.

The WP communication is critical for the APS functionality. The **show aps agents** command is typically used as a debugging aid for unexpected or unusual APS operation.

Displaying the APS operational data is considered of lower priority than the APS operation itself. Because the information is collected from several sources scattered across the various nodes involved, there is a small probability that some states will change while the command is being run.

The command should be reissued for confirmation before decisions are made based on the results displayed.

Task ID

Task ID	Operations
sonet-sdh	read

Examples

The following is sample output from the **show aps agents** command:

```
RP/0/0/CPU0:router# show aps agents

SONET APS Manager working-Protect (WP) connections:
Remote peer (192.168.3.2 - auto) is up:
  Group 6 [P.Ch0] 192.168.3.2 === Manager --- SONET6_0 (node6) --- [W.Ch1]
Remote peer (10.1.1.1) is up:
  Group 3 [W.Ch1] 192.168.1.1 === Manager --- SONET3_1 (node3) --- [P.Ch0]
Local agent (node2) is up:
  Group 1 [W.Ch1] --- SONET2_0 --- SONET3_0 (node3) --- [P.Ch0]
Local agent (node3) is up:
  Group 1 [P.Ch0] --- SONET3_0 --- SONET2_0 (node2) --- [W.Ch1]
```

```

Group 3 [P.Ch0] --- SONE3_1 --- Manager === 192.168.1.1 [W.Ch1]
Group 5 [P.Ch0] --- SONE3_2 --- SONE3_3 (node3) --- [W.Ch1]
Group 5 [W.Ch1] --- SONE3_3 --- SONE3_2 (node3) --- [P.Ch0]
Local agent (node6) is up:
Group 6 [W.Ch1] --- SONE6_0 --- Manager === 192.168.3.2 [P.Ch0]

```

Table 2: show aps agents Field Descriptions

Field	Description
Remote peer	IP address of the remote Protect Group Protocol (PGP) peer for the working router in an APS group. An IP address of 0.0.0.0 indicates a dynamically discovered PGP peer not yet contacted, shown on working routers only. (The protect router contacts the working router.)
Local agent	Node name of the local agent, such as (node2).
Group	The interface location or IP address of the SONET APS group. Internal WP communication channel segments are represented as "---" if the segment is operational or "-/-" if the connection is broken. PGP segments are represented as "===" if operational or "==" if broken.

Related Commands

Command	Description
show aps , on page 58	Displays the operational status for all configured SONET APS groups.

show aps group

To display information about the automatic protection switching (APS) groups, use the **show aps group** command in EXEC mode.

show aps group [*number*]

Syntax Description

<i>number</i>	(Optional) The assigned group number.
---------------	---------------------------------------

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

The **show aps group** command displays information about APS groups, and is useful if multiple APS groups are configured.

Displaying the APS operational data is considered of lower priority than the APS operation itself. Because the information is collected from several sources scattered across the various nodes involved, there is a small probability that some states will change while the command is being run.

The command should be reissued for confirmation before decisions are made based on the results displayed.

Task ID

Task ID	Operations
sonet-sdh	read

Examples

The following is sample output from the **show aps group** command:

```
RP/0/0/CPU0:router# show aps group 3
APS Group 3:
PGP:Authentication "cisco", hello timeout 1 sec, hold timeout 3 sec
Protect ch 0 (SONET3 1):Admin Down, Disabled
SONET framing, SONET signalling, bidirectional, non-revertive
Rx K1:0x00 (No Request - Null)
   K2:0x05 (bridging Null, 1+1, bidirectional)
Tx K1:0x00 (No Request - Null)
   K2:0x05 (bridging Null, 1+1, bidirectional)
```

Working ch 1 (192.168.1.1):Admin Down, Enabled

Table 3: show aps group Field Descriptions

Field	Description
APS Group	<p>Group number assigned to the displayed APS group. For each channel in the group, the following information is displayed:</p> <ul style="list-style-type: none"> • Authentication string • Hello timer value • Hold timer value • Role of the channel (working or protect) • Channel number • Name of the assigned physical port • Channel status (Enabled, Disabled, Admin Down, Signal Fail, Signal Degraded, or Not Contacted) • Group-related information (for protect channels only) that includes: <ul style="list-style-type: none"> ◦ Framing of the SONET port ◦ Kilobytes signaling protocol ◦ Unidirectional or bidirectional APS mode ◦ APS revert time, in seconds (in revertive operation mode only)
Rx	Received error signaling bytes and their APS decoded information.
Tx	Sent error signaling bytes and their APS decoded information.
Working ch	IP address of the corresponding Protect Group Protocol (PGP) peer.

The information displayed for the channels local to the routers is identical to the channel information displayed for single-router APS groups.

Related Commands

Command	Description
show aps, on page 58	Displays the operational status for all configured SONET APS groups.
show aps agents, on page 60	Displays the status of the APS WP distributed communication subsystem.

show controllers pos

To display information on the Packet-over-SONET/SDH (POS) controllers, use the **show controllers pos** command in EXEC mode.

```
show controllers pos interface-path-id [all framer {internal|register|statistics}| internal] [begin line|
exclude line| file filename| include line]
```

Syntax Description

<i>interface-path-id</i>	Physical interface or virtual interface. Note Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
all	(Optional) Displays information for all POS interface controllers.
framer	(Optional) Displays all POS framer information.
internal	(Optional) Displays all POS internal information.
register	(Optional) Displays the POS framer registers.
statistics	(Optional) Displays the POS framer cumulative counters.
begin line	(Optional) Displays information beginning with the line that includes the regular expression given by the <i>line</i> argument.
exclude line	(Optional) Displays information excluding all lines that contain regular expressions that match the <i>line</i> argument.
file filename	(Optional) Saves the configuration to the designated file. For more information on which standard filenames are recognized, use the question mark (?) online help function.
include line	(Optional) Displays only those lines that contain the regular expression given by the <i>line</i> argument.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack/slot/module/port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
 - *rack*: Chassis number of the rack.
 - *slot*: Physical slot number of the line card.
 - *module*: Module number. A physical layer interface module (PLIM) is always 0.
 - *port*: Physical port number of the interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

The information displayed is generally useful for diagnostic tasks performed by technical support personnel only.

Task ID

Task ID	Operations
interface	read

Examples

The following is sample output from the **show controllers pos** command:

```
RP/0/0/CPU0:router# show controllers POS 0/3/0/2
Port Number          : 2
Interface            : POS0/3/0/2
Ifhandle             : 0x1380120
CRC                  : 32
MTU                  : 4474
Port Bandwidth Kbps : 2488320
Admin state          : Up
Driver Link state    : Up

Bundle member        : No
Bundle MTU           : 4474
Bundle Adminstate    : Up
```

The following is sample output from the **show controllers pos all** command:

```
RP/0/0/CPU0:router# show controllers POS 0/3/0/2 all
Port Number          : 2
Interface            : POS0/3/0/2
Ifhandle             : 0x1380120
CRC                  : 32
MTU                  : 4474
Port Bandwidth Kbps : 2488320
Admin state          : Up
Driver Link state    : Up

Bundle member        : No
Bundle MTU           : 4474
```

Bundle Adminstate : Up

POS Driver Internal Cooked Stats Values for port 2

```
=====
Rx Statistics                               Tx Statistics
-----
Total Bytes:      1200                      Total Bytes:      0
Good Bytes:       1200                      Good Bytes:       0
Good Packets:     25                        Good Packets:     0
Aborts:           0                         Aborts:           0
FCS Errors:       0                         Min-len errors:  0
Runts:            0                         Max-len errors:  0
FIFO Overflows:  0                         FIFO Underruns:  0
Giants:           0
Drops:            0
```

Sky4402 asic #2 registers:

```
0x000 general_cntrl                0x00
0x002 sys_intf_cntrl_1            0x06
0x003 sys_intf_cntrl_2            0x00
0x004 JTAG3                        0x10
0x005 JTAG2                        0x10
0x006 JTAG1                        0x10
0x007 JTAG0                        0x2f
0x010 active_led                  0x01
0x011 gpio_port_mode              0x01
0x012 gpio_port_fault             0x00
0x013 gpio_port_data              0x58
0x015 gpio_port_cntrl             0x3f
0x017 gpio_port_transition        0x00
0x019 gpio_port_intr_mask        0xff
0x01b gpio_port_intr              0x3f
0x01c master_intr_status          0x00
0x01d master_mask                 0x00
0x020 interrupt_4                 0x04
0x021 interrupt_3                 0x00
0x022 interrupt_2                 0x00
0x023 interrupt_1                 0x00
0x024 status_4                    0x04
0x025 status_3                    0x00
0x026 status_2                    0x0c
0x027 status_1                    0x80
0x028 mask_4                       0x07
0x029 mask_3                       0x03
0x02a mask_2                       0x1c
0x02b mask_1                       0x8f
0x02d link_state_cntrl            0x80
0x041 diag                         0x00
0x042 stcks                        0x03
0x043 short_frame_cntrl           0x00
0x0c0 ror_ram_c2                   0x16
0x0c1 ror_ram_g1                   0x00
0x0c2 ror_ram_f2                   0x00
0x0c3 ror_ram_h4                   0x00
0x0c4 ror_ram_z3                   0x00
0x0c5 ror_ram_z4                   0x00
0x0c6 ror_ram_z5                   0x00
0x0c7 ror_ram_db_c2               0x16
0x0c8 ror_ram_db_g1               0x00
0x142 tor_ram_c2                   0x16
0x143 tor_ram_g1                   0x00
0x144 tor_ram_f2                   0x00
0x145 tor_ram_h4                   0x00
0x146 tor_ram_z3                   0x00
0x147 tor_ram_z4                   0x00
0x148 tor_ram_z5                   0x00
0x170 tor_ram_s1                   0x00
0x171 tor_ram_e2                   0x00
```

show controllers pos

```

0x172 tor_ram_e1          0x00
0x173 tor_ram_f1          0x00
0x174 tor_ram_k1          0x00
0x175 tor_ram_k2          0x00
0x177 tor_ram_z2          0x00
0x180 rsp_cntrl_1         0x00
0x181 rsp_cntrl_2         0x02
0x184 rtop_f1_ovrhd       0x00
0x185 rtop_k1_ovrhd       0x00
0x186 rtop_k2_ovrhd       0x00
0x187 rtop_s1_ovrhd       0x00
0x188 rtop_e1_ovrhd       0x00
0x189 rtop_e2_ovrhd       0x00
0x18a rtop_deb_s1_ovrhd   0x00
0x18c rtop_b1_mismatch_cnt_u 0x00
0x18d rtop_b1_mismatch_cnt_l 0x00
0x190 rtop_b2_mismatch_cnt_u 0x00
0x191 rtop_b2_mismatch_cnt_l 0x00
0x194 rtop_rei_l_cnt_u    0x00
0x195 rtop_rei_l_cnt_l    0x00
0x198 rtop_ber_thresh_u   0x00
0x199 rtop_ber_thresh_l   0x00
0x19a rtop_ber_leak_u     0x00
0x19b rtop_ber_leak_l     0x00
0x19c rtop_ber_delay_u    0x00
0x19d rtop_ber_delay_l    0x00
0x1c0 rpop_signal_lbl_c2  0x16
0x1c2 rpop_valid_ptr_u    0x02
0x1c3 rpop_valid_ptr_l    0x0a
0x1c4 rpop_b3_mismatch_cnt_u 0x00
0x1c5 rpop_b3_mismatch_cnt_l 0x00
0x1c8 rpop_rei_p_cnt_u    0x00
0x1c9 rpop_rei_p_cnt_l    0x00
0x1cc rpop_ber_thresh_u   0x00
0x1cd rpop_ber_thresh_l   0x00
0x1ce rpop_ber_leak_u     0x00
0x1cf rpop_ber_leak_l     0x00
0x1d0 rpop_ber_delay_u    0x00
0x1d1 rpop_ber_delay_l    0x00
0x200 rpp_cntrl_1         0x11
0x201 rpp_cntrl_2         0x03
0x202 rpp_cntrl_3         0x3e
0x203 rpp_cntrl_4         0x00
0x204 rpp_cntrl_5         0x00
0x208 rpp_max_pkt_len_u   0x08
0x209 rpp_max_pkt_len_l   0xbd
0x20a rpp_min_pkt_len     0x04
0x244 tpp_inter_pkt_u     0x00
0x245 tpp_inter_pkt_l     0x00
0x246 tpp_idle_cell_hdr   0x00
0x247 tpp_idle_cell_filldata 0x00
0x248 tpp_cntrl           0x04
0x280 tpog_cntrl          0x20
0x2c0 ttog_cntrl          0x00
0x2c2 ttog_ovrhd_src_1    0x00
0x2c3 ttog_ovrhd_src_2    0x00
0x2c9 ttog_ovrhd_fill     0x00

```

Table 4: show controllers pos Field Descriptions

Field	Description
Cisco POS ASIC Register Dump (Receive)	Header for display of the contents of the receive ASIC1 register log.
asic mode	Address in hex of the ASIC mode flag.

Field	Description
error source	Address in hex of the error source flag.
error mask	Address in hex of the error mask flag.
error detail 1	Address in hex of the error detail 1 flag.
error detail 2	Address in hex of the error detail 2 flag.
rx offset	Address in hex of the receive offset.
Channel Modes	Location in hex of the channel mode flag.
Port 0:	Port 0 (the first port) statistics display.
Port 1:	Port 1 (the second port) statistics display.
Port 2:	Port 2 (the third port) statistics display.
Port 3:	Port 3 (the fourth port) statistics display.
Runt Threshold	Limit in packets set for runts on the specified port.
Tx Delay	Transmit delay that has been set for the specified port.
Cisco POS ASIC Register Dump (Transmit)	Header for display of the contents of the transmit ASIC register log.
POS Driver Internal Cooked Stats Values for port 0	Statistics relating to the specified POS port (POS port 0).
Rx Statistics	Receive statistics for the indicated POS port.
Total Bytes	Total number of bytes, including data and MAC encapsulation, received by the system.
Good Bytes	Number of bytes received without errors.
Good Packets	Number of packets received without errors.
Aborts	Number of receive bytes that have been aborted
FCS Errors	Number of FCS2 errors that have been received.
Runts	Number of received packets that are discarded because they are smaller than the minimum packet size of the medium.
FIFO Overflows	Number of received packets that exceeded the FIFO stack limit.

Field	Description
Giants	Number of received packets that are discarded because they exceed the maximum packet size of the medium.
Drops	Number of received packets that have been dropped from the system.
Tx Statistics	Transmit statistics for the indicated POS port.
Total Bytes	Total number of bytes, including data and MAC encapsulation, sent by the system.
Good Bytes	Number of bytes sent without errors.
Good Packets	Number of packets sent without errors.
Aborts	Number of sent bytes that have been aborted.
Min-len errors	Minimum queue length violations.
Max-len errors	Maximum queue length violations.
FIFO Underruns	First-in, first-out, a buffering scheme where the first byte of data entering the buffer is the first byte retrieved by the CPU. FIFO underruns reports the number of times that the transmitter has been running faster than the router can handle.

[1 2](#)

¹ 1. application-specific integrated circuit

² 2. frame check sequence

show controllers sonet

To display information about the operational status of SONET layers, use the **show controllers sonet** command in EXEC mode.

```
show controllers sonet interface-path-id {all| framers| internal-state}
```

Syntax Description

<i>interface-path-id</i>	Physical interface or virtual interface. Note Use the show interfaces command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
all	Displays all information.
framers	Displays framer information.
internal-state	Displays internal SONET state.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For the *interface-path-id* argument, use the following guidelines:

- If specifying a physical interface, the naming notation is *rack/slot/module/port*. The slash between values is required as part of the notation. An explanation of each component of the naming notation is as follows:
 - *rack*: Chassis number of the rack.
 - *slot*: Physical slot number of the line card.
 - *module*: Module number. A physical layer interface module (PLIM) is always 0.
 - *port*: Physical port number of the interface.
- If specifying a virtual interface, the number range varies, depending on interface type.

Use the **show controllers sonet** command to display information about the operational status of SONET layers on a particular SONET port.

If the manageability PIE is not installed, you can use the **show controllers sonet** command to display the counters for the current 15 minutes only without history data. However, the SONET MIB is still available but is limited to the current bucket of data. History data is still available only when the manageability PIE is loaded. The **show controllers sonet** command is available at any time to display current data, and history data is stored in the line card rather than in the history bucket.

Task ID

Task ID	Operations
interface	read

Examples

The following is sample output from the **show controllers sonet** command:

```
RP/0/0/CPU0:router# show controllers sonet 0/1/2/1
Port SONET0/1/2/1:
Status: Up
Loopback: None
SECTION
  LOF = 0          LOS   = 0          BIP(B1) = 0
LINE
  AIS = 0          RDI   = 1          FEBE = 0          BIP(B2) = 0
PATH
  AIS = 0          RDI   = 0          FEBE = 0          BIP(B3) = 0
  LOP = 0          NEWPTR = 0        PSE  = 0          NSE   = 0
  PLM = 0          TIM   = 0
Line delays trigger:      0 ms clear: 10000 ms
Path delays trigger:     0 ms clear: 10000 ms
Last clearing of "show controllers SONET" counters never
Detected Alarms: None
Asserted Alarms: None
Mask for Detected->Asserted: None
Detected Alerts: None
Reported Alerts: None
Mask for Detected->Reported: None
Alarm reporting enabled for: SLOS SLOF SF_BER PLOP
Alert reporting enabled for: B1-TCA B2-TCA B3-TCA
Framing: SONET
SPE Scrambling: Enabled
C2 State: Stable  C2_rx = 0x16 (22)  C2_tx = 0x16 (22) / Scrambling Derived
S1S0(tx): 0x0  S1S0(rx): 0x0 / Framing Derived
PATH TRACE BUFFER : STABLE
  Remote hostname : P1 CRS-8
  Remote interface: POS0/1/4/0
  Remote IP addr  : 0.0.0.0
APS
No APS Group Configured
Protect Channel 0  DISABLED
Rx(K1/K2) : 0x00/0x00
Tx(K1/K2) : 0x00/0x00
Remote Rx(K1/K2): 01/0  Remote Tx(K1/K2): 01/0
```

```

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

Optics type: OC48 SR/STM16 I-16
Clock source: internal (actual) internal (configured)
Rx S1: 0xf Tx S1: 0x50

Optical Power Monitoring (accuracy: +/- 1dB)
Rx power = 0.3162 mW, -5.0 dBm
Tx power = 0.2883 mW, -5.4 dBm
Tx laser current bias = 17.2 mA

```

Table 5: show controllers sonet Field Descriptions

Field	Description
Port	Slot number of the POS interface.
Status	Displays whether the link associated with the specified port is up or down.
Loopback	Loopback identifier, if applicable.
LOF	Section loss of frame is detected when a severely error-framing (SEF) defect on the incoming SONET signal persists for 3 milliseconds.
LOS	Section loss of signal is detected when an all-zeros pattern on the incoming SONET signal lasts 19(+3) microseconds or longer. This defect might also be reported if the received signal level drops below the specified threshold.
BIP	<p>Bit interleaved parity error reported.</p> <ul style="list-style-type: none"> • For B1, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B1 byte of the following frame. Differences indicate that section-level bit errors have occurred. • For B2, the bit interleaved parity error report is calculated by comparing the BIP-8/24 code with the BIP-8 code extracted from the B2 byte of the following frame. Differences indicate that line-level bit errors have occurred. • For B3, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B3 byte of the following frame. Differences indicate that path-level bit errors have occurred.

Field	Description
AIS	<p>Alarm indication signal.</p> <ul style="list-style-type: none"> Line alarm indication signal is sent by the STE1 to alert the downstream LTE2 that a LOS or LOF defect has been detected on the incoming SONET section. Path alarm indication signal is sent by the LTE to alert the downstream PTE3 that it has detected a defect on its incoming line signal.
RDI	<p>Remote defect indication.</p> <ul style="list-style-type: none"> Line remote defect indication is reported by the downstream LTE when it detects LOF4, LOS5, or AIS6. Path remote defect indication is reported by the downstream PTE when it detects a defect on the incoming signal.
FEBE	<p>Far-end block errors.</p> <ul style="list-style-type: none"> Line far-end block error (accumulated from the M0 or M1 byte) is reported when the downstream LTE detects BIP7 (B2) errors. Path far-end block error (accumulated from the G1 byte) is reported when the downstream PTE detects BIP (B3) errors.
LOP	<p>Path loss of pointer is reported as a result of an invalid pointer (H1, H2) or an excess number of NDF8 enabled indications.</p>
NEWPTR	<p>Inexact count of the number of times the SONET framer has validated a new SONET pointer value (H1, H2).</p>
PSE	<p>Inexact count of the number of times the SONET framer has detected a positive stuff event in the received pointer (H1, H2).</p>
NSE	<p>Inexact count of the number of times the SONET framer has detected a negative stuff event in the received pointer (H1, H2).</p>
PLM	<p>Payload label mismatch. A different payload-specific functionality than the provisioned functionality is reported. For example, 02 to E0, or FD to FE.</p>

Field	Description
TIM	Trace identifier mismatch. Reported TIM defects that occur primarily as a result of provisioning errors; for example, incorrect cross-connections in the network.
Line delays trigger	Line triggers delayed and cleared, in milliseconds.
Path delays trigger	Path triggers delayed and cleared, in milliseconds.
Last clearing of "show controllers SONET" counters	When the counters associated with the show controllers sonet command were last cleared.
Detected/Asserted Alarms	Any alarms detected by the controller are displayed here. Alarms are as follows: <ul style="list-style-type: none"> • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
Mask for Detected -> Asserted	Masked alarms for the asserted alarm. For example, when SLOS is asserted, all low-level alarms are masked and are listed in this section of the output.
Detected Alerts	List of alerts that are detected.
Reported Alerts	List of reported alerts, such as B1-TCA B2-TCA B3-TCA, sent to the application layer.
Mask for Detected -> Reported	List of masked alerts for asserted alarms that are reported.
Alarm reporting enabled for	Types of alarms that generate an alarm message.
Alert reporting enabled for	Types of alarms that generate an alert message.
Framing	Type of framing enabled on the controller.
SPE Scrambling	Status of synchronous payload envelope (SPE) scrambling: Enabled, Disabled.
C2 State	Value extracted from the SONET path signal label byte (C2).

Field	Description
S1S0(tx)	Two S bits received in the last H1 byte.
PATH TRACE BUFFER	SONET path trace buffer is used to communicate information regarding the remote hostname, interface name/number, and IP address. This use of the J1 (path trace) byte is proprietary to Cisco.
Remote hostname	Name of the remote host.
Remote interface	Interface of the remote host.
Remote IP addr	IP address of the remote host.
APS	Configuration status of the APS feature
APS Group	Indicates whether or not an APS group is configured.
Protect Channel 0	Indicates whether or not channel 0 is protected.
Rx(K1/K2)/Tx(K1/K2)	Contents of the received and transmitted K1 and K2 bytes at the local end in an APS configuration.
Remote Rx(K1/K2)/Tx(K1/K2)	Contents of the received and transmitted K1 and K2 bytes at the remote end in an APS configuration.
BER thresholds	List of the bit error rate (BER) thresholds you configured with the threshold (SONET) command.
TCA thresholds	List of threshold crossing alarms (TCA) you configured with the threshold (SONET) command.
Optics type	Type of small form-factor pluggable (SFP) used in the associated port.
Tx laser current bias	Measured laser bias current, in milliamps (mA). The valid range is 0 through 131 mA.
Clock source	Actual and configured clock source.
Optical Power Monitoring	Power status of the SONET controller.
Tx laser current bias	Current information, in milliamps (mA), in the transmit direction.

[3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#)

The following is sample output from the **show controllers sonet** command with the **framers** option:

```
RP/0/0/CPU0:router# show controllers sonet 0/1/2/1 framers

Common Regs
reg[0]                Master Reset and Identity 0x01
reg[1]                Master Cfg 0000
reg[3]                Master Clock Monitors 0x37
reg[100]              Master Intr Status 1 0000
reg[101]              Master Intr Status Ch 0-7 0000
reg[102]              Master Intr Status Ch 8-15 0000
reg[1000]             Master Clock Source Cfg 0000
reg[1001]             Master DCC Interface Cfg 1 0x0f
reg[1002]             Master DCC Interface Cfg 2 0000
reg[1004]             APS Cfg and Status 0000
reg[1005]             APS FIFO Cfg and Status 0x0f
reg[1006]             APS Intr Status 1 0000
reg[1007]             APS Intr Status 2 0000
reg[1008]             APS Reset Ctrl 0000
reg[1010]             TUL3 Interface Cfg 0x80
reg[1011]             TUL3 Intr Status/Enable 1 0000
reg[1012]             TUL3 Intr Status/Enable 2 0000
reg[1013]             TUL3 ATM Level 3 FIFO Cfg 0x03
reg[1014]             TUL3 ATM Level 3 Signal Label 0x01
reg[1015]             TUL3 POS Level 3 FIFO Low Water Mark 0x15
reg[1016]             TUL3 POS Level 3 FIFO High Water Mark 0x17
reg[1017]             TUL3 POS Level 3 Signal Label 0000
reg[1018]             TUL3 burst 0x0f
--More--
```

The following is sample output from the **show controllers sonet** command with the **internal-state** keyword:

```
RP/0/0/CPU0:router# show controllers sonet 0/1/2/1 internal-state

Interface(layer)      admin_up  if_state
-----
SONET0/1/2/1         up       up
(SONET Section)      up       up
(SONET Line)         up       up
(SONET Path)         up       up
SonetPath0/1/2/1    up       up
  POS0/1/2/1         up       up
```

Table 6: show controllers sonet Field Descriptions

Field	Description
Interface (layer)	Slot number of the POS interface.

- 3 1. section terminating equipment
4 2. line terminating equipment
5 3. path terminating equipment
6 4. loss of frame
7 5. loss of synchronization
8 6. alarm indication signal
9 7. bit interleaved parity
10 8. new data flag
11

Field	Description
admin_up	Whether the interface and its associated layers are in the admin-up state.
if_state	Whether the interface and its associated layers are in the up or down state.

show sonet-local trace frr

To display the alarms associated with Fast Re-Route (FRR) for all nodes or for a specific node, use the **show sonet-local trace frr** command in EXEC mode.

```
show sonet-local trace frr location node-id
```

Syntax Description

location <i>node-id</i>	Full path location of the node. For more information about the syntax for the router, use the question mark (?) online help function.
--------------------------------	--

Command Default

Displays the FRR alarms for all nodes on the router.

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
cisco-support	read

Examples

The following example shows how to display the FRR alarms for a specific node:

```
RP/0/0/CPU0:router# show sonet-local trace frr location 0/1/0/0
```

The following example shows how to display the FRR alarms for all nodes on the router:

```
RP/0/0/CPU0:router# show sonet-local trace frr
```

Related Commands

Command	Description
show controllers sonet , on page 71	Displays information about the operational status of SONET layers.

shutdown (SONET)

To disable SONET controller processing, use the **shutdown** command in SONET/SDH configuration mode. To bring back up a SONET controller and enable SONET controller processing, use the **no form of this** command.

shutdown

no shutdown

Syntax Description This command has no keywords or arguments.

Command Default The SONET controller is up, and SONET controller processing is enabled.

Command Modes SONET/SDH configuration

Command History	Release	Modification
	Release 3.2	This command was introduced.

Usage Guidelines Use the **shutdown** command to shut down a SONET controller and disable SONET controller processing. Use the **no shutdown** command to bring back up a SONET controller and enable SONET controller processing. The SONET controller must be brought up for the proper operation of the Layer 2 interface. The Layer 2 interface has a separate **shutdown** command available, which does not operate on the SONET controller's administrative state.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples The following example shows how to bring down the SONET controller and disable SONET controller processing:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/2
RP/0/0/CPU0:router(config-sonet)# shutdown
```

Related Commands

Command	Description
show controllers sonet, on page 71	Displays information about the operational status of SONET layers.

signalling

To configure the K1K2 overhead byte signaling protocol used for automatic protection switching (APS), use the **signalling** command in APS group configuration mode. To reset APS signaling to the default, use the **no** form of this command.

signalling {sonet|sdh}

no signalling {sonet|sdh}

Syntax Description

sonet	Sets signaling to SONET.
sdh	Sets signaling to Synchronous Digital Hierarchy (SDH).

Command Default

SONET signaling is set by default.

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

By default, APS uses the signaling mode matching the framing mode. The **signalling** command may be required, depending upon the transport equipment capabilities, only on “transition” links interconnecting SONET and SDH networks.

In a multirouter APS topology, the **signalling** command is allowed only on the protect router.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to reset the signaling protocol from the default SONET value to SDH:

```
RP/0/0/CPU0:router(config)# aps group 1
```

```
RP/0/0/CPU0:router(config-aps)# signalling sdh
```

The following example sets the signaling to SONET:

```
RP/0/0/CPU0:router(config)# aps group 1  
RP/0/0/CPU0:router(config-aps)# signalling sonet
```

Related Commands

Command	Description
aps group (global), on page 9	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
show aps group, on page 62	Displays information about the APS groups.

sts

To specify the Synchronous Transport Signal (STS) path and enter the STS controller configuration mode, use the **sts** command in SONET controller configuration mode.

sts number

Syntax Description

<i>number</i>	STS path number. The range varies by the type of line card.
---------------	---

Command Default

No default behavior or values

Command Modes

SONET controller configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to specify STS 1:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/0/CPU0:router(config-sonet)# sts 1
RP/0/0/CPU0:router(config-stsPath)#
```

Related Commands

Command	Description
au , on page 11	Specifies the administrative unit (AU) group number and enters the AU controller configuration mode.

timers (APS)

To change the time between hello packets and the time before the protect interface process declares a working interface router to be down, use the **timers** command in APS group configuration mode. To return to the default timers, use the **no** form of this command.

timers *hello-seconds hold-seconds*

no timers

Syntax Description

<i>hello-seconds</i>	Number of seconds to wait before sending a hello packet (hello timer). Range is from 1 through 255 seconds. Default is 1 second.
<i>hold-seconds</i>	Number of seconds to wait to receive a response from a hello packet before the interface is declared down (hold timer). Range is from 1 through 255 seconds. Default is 3 seconds.

Command Default

hello-seconds: 1

hold-seconds: 3

Command Modes

APS group configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **timers** command to change the time between hello packets and the time before the protect interface process declares a working interface router to be down.

The hello time, in seconds, represents the interval between the periodic message exchange between the Protect Group Protocol (PGP) peers. The hold time, in seconds, represents the maximum interval starting with the first failed periodic message after which, if no successful exchange takes place, the PGP link is declared dead. If the Hello timer is X seconds and Hold Timer is configured as Y seconds (where, $X < Y$), then the PGP link down announcement happens in a minimum of $Y - X$ seconds and maximum of Y seconds.

If many multirouter APS groups are configured and the CPU load or the User Datagram Protocol (UDP) traffic associated with the PGP communication is considered too high, then the hello interval should be increased.

Increasing the hold time is suggested if the PGP link is flapping. The possible causes include high route processor (RP) CPU load, high traffic, or high error rates on the links between the working and the protect routers.

We recommend that you have a hold time at least three times longer than the hello time (allowing three or more consecutive failed periodic message exchange failures).

The **timers** command is typically used only on the protect router. After the PGP connection is established, the working router learns about the timer settings from the protect router and automatically adjusts accordingly, regardless of its own timer configuration.

The **timers** command is meaningful only in multirouter automatic protection switching (APS) topologies and is ignored otherwise.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to configure APS group 3 with the hello timer at 2 seconds and the hold timer at 6 seconds:

```
RP/0/0/CPU0:router(config)# aps group 3
RP/0/0/CPU0:router(config-aps)# timers 2 6
```

Related Commands

Command	Description
aps group (global), on page 9	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
show aps group, on page 62	Displays information about the APS groups.

threshold (SONET)

To set the bit error rate (BER) threshold values of the specified alarms for a SONET controller, use the **threshold** command in SONET/SDH configuration mode. To remove the setting of the threshold from the configuration file and restore the default condition, use the **no** form of this command.

threshold {**b1-tca**|**b2-tca**|**sd-ber**|**sf-ber**} *bit-error-rate*

no threshold {**b1-tca**|**b2-tca**|**sd-ber**|**sf-ber**} *bit-error-rate*

Syntax Description

b1-tca	Sets the B1 BER threshold crossing alarm (TCA). Range is from 3 through 9. Default is 10e-6.
b2-tca	Sets the B2 BER threshold crossing alarm (TCA). Range is from 3 through 9. Default is 10e-6.
sd-ber	Sets the signal degrade BER threshold. Range is from 3 through 9. Default is 10e-6.
sf-ber	Sets the signal failure BER threshold. Range is from 3 through 9. Default is 10e-3.
bit-error-rate	BER from 3 to 9 (10 to the minus <i>x</i>).

Command Default

b1-tca: 10e-6
b2-tca: 10e-6
sd-ber: 10e-6
sf-ber: 10e-3

Command Modes

SONET/SDH configuration

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

For B1, the bit interleaved parity (BIP) error report is calculated by comparing the BIP-8 code with the BIP-8 code that is extracted from the B1 byte of the following frame. Differences indicate that section-level bit errors have occurred.

For B2, the BIP error report is calculated by comparing the BIP-8/24 code with the BIP-8 code that is extracted from the B2 byte of the following frame. Differences indicate that line-level bit errors have occurred.

Signal failure BER and signal degrade BER are sourced from B2 BIP-8 error counts (as is B2-TCA). The **b1-tca** and **b2-tca** keywords print only a log message to the console (if reports for them are enabled).

To determine the BER thresholds configured on the controller, use the **show controllers sonet** command.

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to configure thresholds on the SONET controller:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# threshold sd-ber 8
RP/0/0/CPU0:router(config-sonet)# threshold sf-ber 4
RP/0/0/CPU0:router(config-sonet)# threshold b1-tca 4
```

Related Commands

Command	Description
report (SONET), on page 50	Permits selected SONET alarms to be logged to the console for a SONET controller.
show controllers sonet, on page 71	Displays information about the operational status of SONET layers.

threshold (SONET path)

To set the bit error rate (BER) threshold values of the specified alarms for a SONET path, use the **threshold** command in SONET/SDH path configuration mode. To remove the setting of the SONET path threshold from the configuration file and restore the default condition, use the **no** form of this command.

threshold b3-tca *bit-error-rate*

no threshold b3-tca *bit-error-rate*

Syntax Description	Command	Description
	b3-tca	Sets the B3 BER threshold crossing alarm (TCA). Default is 6.
	<i>bit-error-rate</i>	BER from 3 to 9 (10 to the minus <i>x</i>).

Command Default **b3-tca: 6**

Command Modes SONET/SDH path configuration

Command History	Release	Modification
	Release 3.2	This command was introduced.

Usage Guidelines

For B3, the bit interleaved parity (BIP) error report is calculated by comparing the BIP-8 code with the BIP-8 code that is extracted from the B3 byte of the following frame. Differences indicate that path-level bit errors have occurred.

In addition to BIP errors detected at the local end in the receive direction, B3 error counts detected in the G1 byte (P-REI or P-FEBE) by the far-end SONET equipment are returned.

The **b3-tca** keyword prints only a log message to the console (if reports for them are enabled).

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples

In the following example, the BER is set to 4:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/1
RP/0/0/CPU0:router(config-sonet)# path
RP/0/0/CPU0:router(config-sonet-path)# threshold b3-tca 4
```

Related Commands

Command	Description
report (SONET), on page 50	Permits selected SONET alarms to be logged to the console for a SONET controller.
show controllers sonet, on page 71	Displays information about the operational status of SONET layers.

tug3

To specify the tributary unit group (TUG) number and enter the TUG3 controller configuration mode, use the **tug3** command in SONET controller configuration mode.

tug3 *number*

Syntax Description

<i>number</i>	The tributary unit group (TUG) number. The ranges are: <ul style="list-style-type: none"> • AU4—The only value is 1. • AU3—The range is 1 to 3.
---------------	---

Command Default

The default is 1.

Command Modes

SONET controller configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

The **tug3** command enables you to begin configuring the interface in the TUG3 controller configuration mode, where you can configure virtual containers (VCs) and DS3s:

STM1 -> AU4 -> TUG3 -> VC-3 -> DS3

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to specify tug3 1.

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/0
RP/0/0/CPU0:router(config-sonet)# au 1
RP/0/0/CPU0:router(config-auPath)# tug3 1
RP/0/0/CPU0:router(config-tug3Path)#
```

Related Commands

Command	Description
au, on page 11	Specifies the administrative unit (AU) group number and enters the AU controller configuration mode.

uneq-shut (SONET path)

To enable automatic insertion of P-UNEQ code (0x00) in the sent SONET path overhead C2 byte, use the **uneq-shut** command in SONET/SDH path configuration mode. To disable this feature, use the **no** form of this command.

uneq-shut

no uneq-shut

Syntax Description This command has no keywords or arguments.

Command Default Automatic insertion is enabled.

Command Modes SONET/SDH path configuration

Command History	Release	Modification
	Release 3.2	This command was introduced.

Usage Guidelines Use the **uneq-shut** command to disable automatic insertion of P-UNEQ code in the sent SONET path overhead C2 byte whenever the SONET path enters the administratively down state.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples In the following example, automatic insertion of P-UNEQ code is disabled in the sent SONET path overhead C2 byte:

```
RP/0/0/CPU0:router(config)# controller sonet 0/2/0/2
RP/0/0/CPU0:router(config-sonet)# path
RP/0/0/CPU0:router(config-sonet-path)# uneq-shut
```

unidirectional

To configure a protect interface for unidirectional mode, use the **unidirectional** command in APS group configuration mode. To restore the default setting, bidirectional mode, use the **no** form of this command.

unidirectional

no unidirectional

Syntax Description This command has no keywords or arguments.

Command Default Bidirectional mode is the default mode for the protect interface.

Command Modes APS group configuration

Command History	Release	Modification
	Release 3.2	This command was introduced.

Usage Guidelines Use the **unidirectional** command to configure a protect interface for unidirectional mode. Use the **no** form of this command to restore the default setting.

The unidirectional or bidirectional automatic protection switching (APS) operation mode of the routers should be matched with the APS operation mode of the connected SONET equipment.



Note

We recommend using bidirectional APS mode when it is supported by the interconnecting SONET equipment. When the protect interface is configured as unidirectional, the working and protect interfaces must cooperate to switch the transmit and receive SONET channel in a bidirectional fashion. Cooperation occurs automatically when the SONET network equipment is in bidirectional mode.

In a multirouter APS topology, the **unidirectional** command is allowed only on the protect router.

Task ID	Task ID	Operations
	sonet-sdh	read, write

Examples The following example shows how to configure an APS group for unidirectional mode:

```
RP/0/0/CPU0:router(config)# aps group 1
```

```
RP/0/0/CPU0:router(config-aps)# unidirectional
```

Related Commands

Command	Description
aps group (global), on page 9	Adds an automatic protection switching (APS) group and enter APS group configuration mode.
show aps, on page 58	Displays the operational status for all configured SONET APS groups.

width

To set the number of paths in a stream, use the **width** command in the STS or AU controller configuration mode.

width *number*

Syntax Description

number Number of STS streams that are concatenated. The possible values are:

- 1—Indicating one STS stream
- 3—Indicating three STS streams (STS-3c)
- 12—Indicating concatenation of 12 STS streams (STS-12c)
- 48—Indicating concatenation of 48 STS streams (STS-48c)

Widths 3, 12, and 48 are configured on STS paths at natural boundaries, which coincide with the following path numbers:

- 1, 4, 7, 10, and so on, for STS-3c
- 1, 13, 25, and 37 for STS-12c
- 1 for STS-48c

Command Default

The default is 1.

Command Modes

SONET controller configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operations
sonet-sdh	read, write

Examples

The following example shows how to specify a width of 3:

```
RP/0/0/CPU0:router(config)# controller sonet 0/1/0/0  
RP/0/0/CPU0:router(config-sonet)# sts 1  
RP/0/0/CPU0:router(config-stsPath)# width 3
```

Related Commands

Command	Description
mode (SONET), on page 40	Sets the mode of an STS path, AU path, T3 controller, or TUG3 controller.

width