SONET APS Commands on Cisco IOS XR Software

This module describes the commands used to configure SONET automatic protection switching (APS).

The SONET APS is a feature offering recovery from fiber (external) or equipment (interface and internal) failures at the SONET line layer.

aps group

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

number	Number of the group. Range is from 1 through 255.

Defaults

No groups exist

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **aps group** command to enter APS group configuration mode and configure APS connections with other SONET equipment. Use the **no** form of this command to remove a group.

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.

Examples

The following example shows how the **aps group** command is used to configure APS group 1 and enter APS group configuration mode:

```
RP/0/RP0/CPU0:router(config)# aps group 1
```

Related Commands

Command	Description
show aps	Displays SONET APS group operational status.

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

string	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.

Defaults

Authentication is always disabled by using the string **cisco**

Command Modes

APS group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Examples

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

```
RP/0/RP0/CPU0:router(config)# aps group 1

RP/0/RP0/CPU0:router(config-aps)# authenticate abctown
```

Related Commands

Command	Description
channel local	Assigns a port and interface local to the router as a SONET APS channel.
channel remote	Assigns a port and interface that is physically located in a remote router as a SONET APS channel.
show aps	Displays SONET APS group operational status.

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 *channel-number* {**0** | **1**} **local** {**sonet** | **preconfigure**} *type instance*

no channel *channel-number* {**0** | **1**} **local** {**sonet** | **preconfigure**} *type instance*

Syntax Description

channel-number	Assigned channel number: **0** = protect, **1** = working.
sonet	Configures SONET port controllers.
preconfigure	Specifies a SONET preconfiguration. This keyword is used only when a modular services or line card is not physically installed in a slot.
type	Interface type. For more information, use the question mark (**?**) online help function.
instance	Either a physical interface instance or a virtual interface instance: • Physical interface instance. Naming notation is *rack/slot/module/port* and a slash between values is required as part of the notation. – *rack*: Chassis number of the rack. – *slot*: Physical slot number of the modular services card or line card. – *module*: Module number. A physical layer interface module (PLIM) is always 0. – *port*: Physical port number of the interface. • Virtual interface instance. Number range will vary depending on interface type. For more information about the syntax for the router, use the question mark (**?**) online help function.

Defaults

A SONET APS local channel is not assigned

Command Modes

APS group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 will be rejected.

The interface type must be a SONET controller.

Examples

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

```
RP/0/RP0/CPU0:router(config)# aps group 1

RP/0/RP0/CPU0:router(config-aps)# channel 0 local SONET 0/2/0/2
```

Related Commands

Command	Description
channel remote	Assigns a port and interface that is physically located in a remote router as a SONET APS channel.
show aps	Displays SONET APS group operational status.

channel remote

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

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

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

Syntax Description

channel-number {**0** | **1**}	Assigned channel number. Replace the *channel-number* argument with a number that identifies the channel. Enter **0** to designate the channel as protect channel, or **1** to designate the channel as a working channel.
ip-address	Remote router IP address in A.B.C.D format.

Defaults

A SONET APS remote channel is not assigned

Command Modes

APS group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 it is not used, 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.

Examples

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

```
RP/0/RP0/CPU0:router(config)# aps group 1

RP/0/RP0/CPU0:router(config-aps)# channel 1 remote 192.168.1.1
```

Related Commands

Command	Description
channel local	Assigns a port and interface local to the router as a SONET APS channel.
show aps	Displays SONET APS group operational status.

force

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

force *channel-number* {**0** | **1**}

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

Syntax Description

channel-number	The assigned channel number. **0** = protect, **1** = working.

Defaults

No default behavior or values

Command Modes

APS group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Examples

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

```
RP/0/RP0/CPU0:router(config)# aps group 1

RP/0/RP0/CPU0:router(config-aps)# force 1
```

Related Commands

Command	Description
lockout	Initiates an APS lockout switch request at the local end of the SONET link.
manual	Initiates an APS manual switch request at the local end of the SONET link.

lockout

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

lockout *channel-number* {**0** | **1**}

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

Syntax Description

channel-number	(Optional) The assigned channel number. **0** = protect, **1** = working. Default is **0**.

Defaults

The default is **0**

Command Modes

APS group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The optional **0** or **1** keyword (by default **0**) identifies the channel from which the traffic should not be moved on the protect channel:

- The **lockout 1** command keeps traffic away from the working router.
- The **lockout 0** command keeps traffic away from the protect router.

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.

Examples

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

```
RP/0/RP0/CPU0:router(config)# aps group 1

RP/0/RP0/CPU0:router(config-aps)# lockout 1
```

Related Commands

Command	Description
force	Initiates an APS force switch request at the local end of the SONET link.
manual	Initiates an APS manual switch request at the local end of the SONET link.

manual

To initiate a forced 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.

manual *channel-number* {**0** | **1**}

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

Syntax Description

channel-number	The assigned channel number: **0** = protect, **1**= working.

Defaults

No circuit is switched

Command Modes

APS group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Examples

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

```
RP/0/RP0/CPU0:router(config)# aps group 1

RP/0/RP0/CPU0:router(config-aps)# manual 1
```

Related Commands

Command	Description
force	Initiates an APS force switch request at the local end of the SONET link.
lockout	Initiates an APS lockout switch request at the local end of the SONET link.

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

Syntax Description

minutes	Number of minutes until the circuit is switched back to the working interface after the working interface is available.

Defaults

minutes = **0**

Automatic switchover is disabled

Command Modes

APS group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Examples

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

```
RP/0/RP0/CPU0:router(config)# aps group 1

RP/0/RP0/CPU0:router(config-aps)# revert 5
```

Related Commands

Command	Description
show aps	Displays SONET APS group operational status.

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 arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Examples

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

```
RP/0/RP0/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
    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):Enabled
APS Group 5:
  Protect ch 0 (SONET3_2):Disabled
    SONET framing, SONET signalling, unidirectional (auto), non-revertive
    Rx K1:0x00 (No Request - Null)
       K2:0x04 (bridging Null, 1+1, unidirectional)
    Tx K1:0x00 (No Request - Null)
       K2:0x05 (bridging Null, 1+1, bidirectional)
  Working ch 1 (SONET3_3):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)
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 17 describes the significant fields shown in the display.

Table 17 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	Displays the status of the APS WP distributed communication subsystem.
show aps group	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 arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Examples

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

```
RP/0/RP0/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] --- SONET3_1 --- Manager === 192.168.1.1 [W.Ch1]
  Group 5   [P.Ch0] --- SONET3_2 --- SONET3_3 (node3) --- [W.Ch1]
  Group 5   [W.Ch1] --- SONET3_3 --- SONET3_2 (node3) --- [P.Ch0]
Local agent (node6) is up:
  Group 6   [W.Ch1] --- SONET6_0 --- Manager === 192.168.3.2 [P.Ch0]
```

Table 18 describes the significant fields shown in the display.

Table 18 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	Displays SONET APS group operational status.

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

number	(Optional) The assigned group number.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Examples

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

```
RP/0/RP0/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 19 describes the significant fields shown in the display.

Table 19 show aps group Field Descriptions

Field	Description
APS Group	Group number assigned to the displayed APS group. For each channel in the group, the following information is displayed: • 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: – 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	Displays SONET APS group operational status.
show aps agents	Displays the status of the APS WP distributed communication subsystem.

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).

Defaults

SONET signaling is set by default

Command Modes

APS group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Examples

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

```
RP/0/RP0/CPU0:router(config)# aps group 1

RP/0/RP0/CPU0:router(config-aps)# signalling sdh
```

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

hello-seconds	Number of seconds to wait before sending a hello packet (hello timer). Range is from 1 through 255 seconds. Default is 1 second.
hold-seconds	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.

Defaults

hello-seconds: 1

hold-seconds: 3

Command Modes

APS group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 interval starting with the first failed periodic message after which, if no successful exchange takes place, the PGP link is declared dead.

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.

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/RP0/CPU0:router(config)# aps group 3

RP/0/RP0/CPU0:router(config-aps)# timers 2 6
```

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 arguments or keywords.

Defaults

Bidirectional mode

Command Modes

APS group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Examples

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

```
RP/0/RP0/CPU0:router(config)# aps group 1

RP/0/RP0/CPU0:router(config-aps)# unidirectional
```

Related Commands

Command	Description
show aps	Displays SONET APS group operational status.