Configuring Automatic Protection Switching on the Cisco ASR 903 Router

Automatic protection switching (APS) is a protection mechanism for SONET networks that enables SONET connections to switch to another SONET circuit when a circuit failure occurs. A protect interface serves as the backup interface for the working interface. When the working interface fails, the protect interface quickly assumes its traffic load.

This document contains the following sections:

Understanding Automatic Protection Switching

The protection mechanism used for this feature is "1+1, Bidirectional, nonrevertive" as described in the Bellcore publication "TR-TSY-000253, SONET Transport Systems; Common Generic Criteria, Section 5.3." In the 1+1 architecture, there is one working interface (circuit) and one protect interface, and the same payload from the transmitting end is sent to both the receiving ends. The receiving end decides which interface to use. The line overhead (LOH) bytes (K1 and K2) in the SONET frame indicate both status and action.

The protect interface is configured with the IP address of the router that has the working interface. The APS Protect Group Protocol, which runs on top of UDP, provides communication between the process controlling the working interface and the process controlling the protect interface. Using this protocol, interfaces can be switched because of a router failure, degradation or loss of channel signal, or manual intervention. In bidirectional mode, the receive and transmit channels are switched as a pair.

Two SONET/SDH connections are required to support APS. In a telco environment, the SONET/SDH circuits must be provisioned as APS. You must also provision the operation (for example, 1+1), mode (for example, bidirectional), and revert options (for example, no revert). If the SONET/SDH connections are homed on two separate routers (the normal configuration), an out of band (OOB) communications channel between the two routers needs to be set up for APS communication.

When configuring APS, we recommend that you configure the working interface first. Normal operation with 1+1 operation is to configure it as a working interface. Also configure the IP address of the interface being used as the APS OOB communications path.

APS uses Protect Group Protocol (PGP) between working and protect interfaces. The protect interface APS configuration should include an IP address of a loopback interface on the same router to communicate with the working interface using PGP. Using the PGP, POS interfaces can be switched in case of a degradation or loss of channel signal, or manual intervention. In bidirectional mode, the receive and transmit channels are switched as a pair.

In bidirectional APS the local and the remote connections negotiate the ingress interface to be selected for the data path. The egress interface traffic is not transmitted to both working and protect interfaces.

Inter Chassis Redundancy Manager

ICRM provides these capabilities for stateful MLPPP with MR-APS Inter-Chassis Redundancy implementation:

- Node health monitoring for complete node, PE, or box failure detection. ICRM also communicates failures to the applications registered with an ICRM group.
- Reliable data channels to transfer the state information.
- Detects active RP failure as node failure and notifies the controllers.

ICRM on the standby RP re-establishes the communication channel with peer node if the active RP fails.

For instructions on how to configure ICRM, see Configuring Stateful MLPPP with MR-APS Inter-Chassis Redundancy, page 5.

Limitations

The following limitations apply when using APS on the Cisco ASR 903 Router

- APS is not currently supported with CES.
- APS is not currently supported with ATM.
- APS is not currently supported with IMA.
- APS supports HDLC, PPP, and MLPPP encapsulation.
- ATM Layer 2 AAL0 and AAL5 encapsulation types are supported
- APS is only supported on MLP and serial interfaces on the OC-3 interface module.

Configuring Automatic Protection Switching Interfaces

The following sections describe how to configure APS interfaces:

- Configuring a Working Interface, page 3
- Configuring a Protect Interface, page 3

Note We recommend that you configure the working interface before the protected interface in order to prevent the protected interface from becoming the active interface and disabling the working interface.

Note For information about configuring optical interfaces for the first time, see the *Cisco ASR 903 Series Router Chassis Configuration Guide*.

Configuring a Working Interface

To configure a working interface, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **controller sonet** *slot* / *port-adapter* / *port*
2. **aps group** *group-number*
3. **aps working** *circuit-number*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**controller sonet** *slot* / *port-adapter* / *port* **Example:** `Router(config)# controller sonet 0/0/0`	Returns to controller configuration mode.
Step 2	**aps group** *group-number* **Example:** `Router(config-if)# aps group 2`	(Optional) Allows more than one protect/working interface group to be supported on a router. The APS group number must be greater than 1.
Step 3	**aps working** *circuit-number* **Example:** `Router(config-if)# aps working 1`	Configures this interface as a working interface. 1 is the only supported *circuit-number* value.
Step 4	**end** **Example:** Router(config-if)# end	Exits configuration mode.

Configuring a Protect Interface

To configure a protect interface, use the following commands beginning in global configuration mode.

SUMMARY STEPS

5. **controller sonet** *slot* / *port-adapter* / *port*
6. **aps protect** *circuit-number ip-address*

7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**controller sonet** *slot* / *port-adapter* / *port* **Example:** `Router(config)# controller sonet 0/0/0`	Returns to controller configuration mode.
Step 2	**aps group** *group-number* **Example:** `Router(config-if)# aps group 2`	(Optional) Allows more than one protect/working interface group to be supported on a router.
Step 3	**aps protect** *circuit-number ip-address* **Example:** `Router(config-if)# aps protect 1 7.7.7.7`	Configures the interface as a protect interface and specifies the IP address of the device that contains the working interface.
Step 4	**end** **Example:** `Router(config-if)# end`	Exits configuration mode.

Configuring Other APS Options

To configure the other APS options, use any of the following optional commands in interface configuration mode.

Command or Action	Purpose
aps authenticate *string* **Example:** `Router(config-if)# aps authenticate authstring`	(Optional) Configures the 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.
aps force *circuit-number* **Example:** `Router(config-if)# aps force 1`	(Optional) Manually switches the specified circuit to a protect interface, unless a request of equal or higher priority is in effect. For example, if the protect interface is configured as circuit 1, use the **aps force 1** command to set the protect interface to active.
aps group *group-number* **Example:** `Router(config-if)# aps group 2`	(Optional) Allows more than one protect/working interface group to be supported on a router.

Command or Action	Purpose
aps lockout *circuit-number* **Example:** `Router(config-if)# aps lockout 1`	(Optional) Prevents a working interface from switching to a protect interface. For example, if the protect interface is configured as circuit 1, use the **aps lockout 1** command to prevent the protect interface from becoming active.
aps manual *circuit-number* **Example:** `Router(config-if)# aps manual 0`	(Optional) Manually switches a circuit to a protect interface, unless a request of equal or higher priority is in effect. For example, if the working interface is configured as circuit 0, the command is applied as follows: • The **aps manual 0** command activates the working interface • The **aps manual 1** command activates the protect circuit. Applying the **no** form of the command removes the configuration and stops the router from sending K 1and K2 bytes on the interface.
aps revert *minutes* **Example:** `Router(config-if)# aps revert 10`	(Optional) Enables automatic switchover from the protect interface to the working interface after the working interface becomes available.
aps timers *seconds1 seconds2* **Example:** `Router(config-if)# aps timers 1 5`	(Optional) Specifies the following values: – *seconds1*—The time between hello packets. – *seconds2*—The time that the working interface can be down before the router switches to the protect interface.
aps unidirectional **Example:** `Router(config-if)# aps unidirectional`	(Optional) Configures a protect interface for unidirectional mode.

Configuring Stateful MLPPP with MR-APS Inter-Chassis Redundancy

The Cisco ASR 903 Router supports Stateful MLPPP with Inter-Chassis Redundancy. For information on how to configure this feature, see http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/wan_mlppp_mr_aps.html.

Monitoring and Maintaining APS

To provide information about system processes, the Cisco IOS software includes an extensive list of EXEC commands that begin with the word show, which, when executed, display detailed tables of system information. Following is a list of some of the common show commands for the APS feature.

To display the information described, use these commands in privileged EXEC mode.

Command or Action	Purpose
Router# **show aps**	Displays information about the automatic protection switching feature.
Router# **show controller sonet** *slot/ port-adapter/ port* Router# **show controllers pos**	Displays information about the hardware.
Router# **show interfaces**	Displays information about the interface.

For more information about these commands, see the *Cisco IOS Interface and Hardware Component Command Reference*.