Understanding APS Versions on POS Interfaces

Document ID: 16144

Contents

Introduction

This document describes the Protect Group Protocol (PGP), which is a key part of Packet Over SONET (POS) Automatic Protection Switching (APS) on Cisco routers and enterprise switches.

Prerequisites

Requirements

This document has no specific requirements.

Components Used

This document is not restricted to specific software and hardware versions.

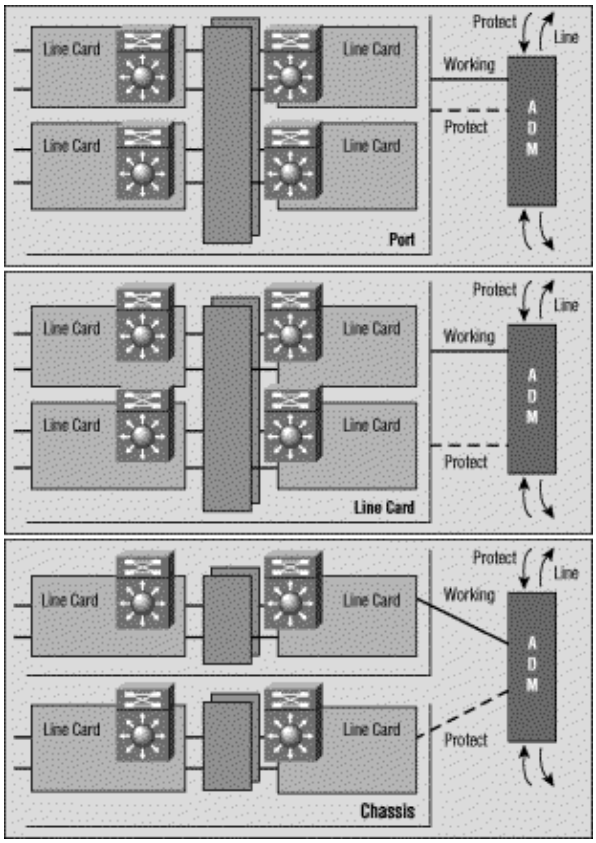
Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

PGP Overview

The Bellcore (now Telcordia) publication TR−TSY−000253, SONET Transport Systems; Common Generic Criteria, Section 5.3, defines Automatic Protection Switching (APS). The protection mechanism used for this feature has 1+1, architecture, in which a redundant line pair consists of a working line and a protection line.

This illustration shows possible SONET protection configurations. You can set up the Cisco POS protection scheme for situations where protect and working interfaces are different ports. These ports can be on the same router or on the same line card in the same router. These scenarios, however, provide protection for router interface or link failure. Most production deployments have working and protect interfaces on different routers. In such a two−router APS configuration, a protocol like PGP is required. PGP defines the protocol between the working and protect routers.



PGP Versions

As of Cisco IOS® Software Release 12.0(10)S, two versions of PGP are available. The working and protect routers must use the same PGP version and exchange negotiation messages using an out−of−band communications link. During negotiation, the protect router sends messages in multiple PGP versions, highest first. The working router ignores hellos with version numbers higher than its own and answers the others. Once the working router answers a hello message, it adopts that version number, and uses it in all subsequent replies.

In current Cisco IOS releases, the working and protect routers do not need to run the same IOS release. The working and protect routers can therefore be upgraded independently.

If Cisco IOS software detects a version mismatch, it prints log messages similar to this:

```
Sep 10 06:34:25.305 cdt: %SONET−3−MISVER: POS4/0: APS version mismatch.
WARNING: Loss of Working−Protect link can deselect both
protect and working interfaces. Protect router requires
software upgrade for full protection.
Sep 10 06:34:25.305 cdt: %SONET−3−APSCOMMEST: POS4/0:
Link to protect channel established − protocol version 0
Sep 10 06:34:33.257 cdt: %SONET−3−APSCOMMEST: POS4/0:
Link to protect channel established − protocol version 1
```

If this link experiences degraded performance and high packet loss, APS version negotiation between the working and protect routers fails. As a result, both routers adopt "down−rev" PGP versions. The problem results from corrupted negotiation messages. If the PGP communications link experiences high packet loss, the working router can miss the hello sent by the protect router with an advertised version number. If this happens, it might only see the subsequent down−rev message. This scenario causes both the working and protect routers to lock onto the lower version number. Cisco IOS Sofware Release 12.0(21)S avoids this problem by doing on−the−fly renegotiation as required.

If you are using a release prior to IOS Sofware Release 12.0(21)S and experience this problem, use this workaround to restore the normal PGP version. Do this once you have established a reliable link between the two routers:

1. Ensure that the working interface is selected. You can use the **aps force 0** command to do this.
2. Shut the protect interface. Leave it down long enough so that the working one declares that it has lost communications with the protect interface.
3. Use the **no shutdown** command on the protect interface to restart protocol negotiations.

PGP communication failures can occur due to any of these issues:

- Working router failure
- Protect router failure
- PGP channel failure

PGP channel failure can occur due to any of these issues:

- Traffic congestion
- Interface failure due to alarms
- Interface hardware failure

You can provide higher bandwidth interfaces for PGP in order to minimize congestion and avoid some PGP channel failures. The working router expects to receive *hellos* from the protect router every hello−interval. If the working router does not receive hellos for a time interval specified by the hold−interval, the working router assumes a PGP failure, and APS is suspended. Similarly, if the protect router does not receive hello acknowledgements from the working router before the hold−interval timer expires, it declares PGP failure and a switchover can occur.

Hello and Hold Timers

POS APS differs from "strict" SONET APS. POS APS supports additional configuration commands used to configure parameters of PGP.

You can use the **aps timers** command to change the hello timer and the hold timer. The hello timer defines the time between hello packets. The hold timer sets the time before the protect interface process declares a working interface's router to be down. By default, the hold time is greater than or equal to three times the hello time.

The following example specifies a hello time of two seconds and a hold time of six seconds on circuit 1 on POS interface 5/0/0:

```
router#configure terminal
router(config)#interface pos 5/0/0
router(config−if)#aps working 1
router(config−if)#aps timers 2 6
router(config−if)#end
```

As shown above, we have configured the **aps timers** command only on the protect interfaces.

You can configure the working and protect interfaces with unique hello and hold times. When working is in contact with a protect interface, it uses the timer values specified for the protect interface. When working is not in contact with a protect interface, it uses the hello and hold timers specified for the working interface.

Authentication

Another command supported only by POS APS is the **authentication** command, which enables authentication between the processes controlling the working and protect interfaces. Use this command to specify the string that must be present to accept any packet on a protect or working interface. Up to eight alphanumeric characters are accepted.

Contacting the Cisco TAC

If you need assistance with troubleshooting APS, contact the Cisco Technical Assistance Center (TAC). Please gather output from the following **show** commands on the routers with the protect and working interfaces:

- **show version**− Displays the configuration of the system hardware and the software version. This command also displays the names and sources of configuration files and the boot images.
- **show controller pos**− Displays information about the POS controllers.
- **show aps** − Displays information about the current automatic protection switching feature.

Related Information

- **Optical Technology Support Pages**
- **Technical Support − Cisco Systems**

Updated: Dec 15, 2005 Document ID: 16144