Introducción a las versiones de APS en las interfaces POS

Contenido

Introducción

Este documento describe el protocolo Protect Group Protocol (PGP), que es una parte clave de Packet Over SONET (POS) Automatic Protection Switching (APS) en routers Cisco y switches empresariales.

Prerequisites

Requirements

Este documento no tiene requisitos específicos.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

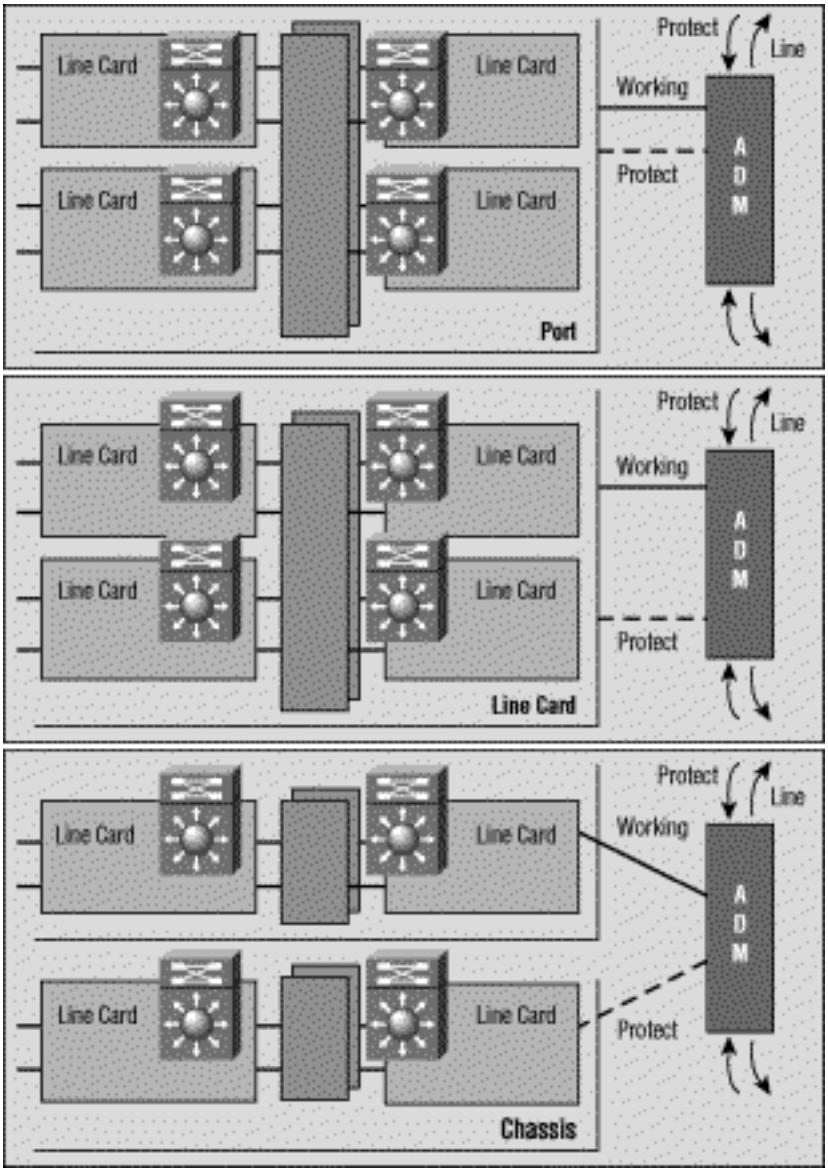
For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Información general de PGP

La publicación de Bellcore (ahora Telcordia) TR-TSY-000253, SONET Transport Systems;

Common Generic Criteria, Sección 5.3, define Automatic Protection Switching (APS). El mecanismo de protección utilizado para esta función tiene una arquitectura 1+1, en la que un par de línea redundante consta de una línea de trabajo y una línea de protección.

Esta ilustración muestra posibles configuraciones de protección SONET. Puede configurar el esquema de protección POS de Cisco para situaciones en las que las interfaces de protección y funcionamiento son puertos diferentes. Estos puertos pueden estar en el mismo router o en la misma tarjeta de línea en el mismo router. Estos escenarios, sin embargo, proporcionan protección para la interfaz del router o la falla del link. La mayoría de las implementaciones de producción tienen interfaces de trabajo y protección en diferentes routers. En una configuración APS de dos routers, se requiere un protocolo como PGP. PGP define el protocolo entre los routers que funcionan y los que protegen.



Versiones de PGP

A partir de Cisco IOS® Software Release 12.0(10)S, hay disponibles dos versiones de PGP. Los routers que trabajan y protegen deben utilizar la misma versión de PGP e intercambiar mensajes de negociación mediante un link de comunicaciones fuera de banda. Durante la negociación, el router de protección envía mensajes en varias versiones de PGP, la más alta primero. El router en funcionamiento ignora los saludos con números de versión superiores a los suyos y responde a los demás. Una vez que el router en funcionamiento responde un mensaje hello, adopta ese

número de versión y lo utiliza en todas las respuestas posteriores.

En las versiones actuales de Cisco IOS, los routers que funcionan y protegen no necesitan ejecutar la misma versión de IOS. Por lo tanto, los routers de funcionamiento y protección pueden actualizarse de forma independiente.

Si el software Cisco IOS detecta una discordancia de versión, imprime mensajes de registro similares a estos:

```
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
```

Si este link experimenta un rendimiento degradado y una alta pérdida de paquetes, la negociación de la versión APS entre los routers activos y protegidos falla. Como resultado, ambos routers adoptan versiones PGP "down-rev". El problema es resultado de mensajes de negociación dañados. Si el link de comunicaciones PGP experimenta una alta pérdida de paquetes, el router en funcionamiento puede perder el saludo enviado por el router de protección con un número de versión anunciado. Si esto sucede, es posible que sólo vea el siguiente mensaje down-rev. Esta situación hace que tanto los routers de trabajo como los de protección se bloqueen en el número de versión inferior. Cisco IOS Software Release 12.0(21)S evita este problema al realizar una renegociación sobre el terreno según sea necesario.

Si utiliza una versión anterior a la versión 12.0(21)S del software IOS y experimenta este problema, utilice esta solución alternativa para restaurar la versión PGP normal. Realice esto una vez que haya establecido un link confiable entre los dos routers:

1. Asegúrese de que la interfaz de trabajo esté seleccionada. Puede utilizar el comando **aps force 0** para hacer esto.
2. Cierre la interfaz de protección. Déjelo lo suficientemente inactivo para que el que trabaja declare que ha perdido comunicaciones con la interfaz de protección.
3. Utilice el comando **no shutdown** en la interfaz de protección para reiniciar las negociaciones del protocolo.

Los errores de comunicación de PGP pueden ocurrir debido a cualquiera de estos problemas:

- Falla del router en funcionamiento
- Proteger la falla del router
- falla del canal PGP

La falla del canal PGP puede ocurrir debido a cualquiera de estos problemas:

- Congestión del tráfico
- Falla de interfaz debido a alarmas
- Falla de hardware de interfaz

Puede proporcionar interfaces de ancho de banda más alto para PGP con el fin de minimizar la congestión y evitar algunas fallas de canales PGP. El router en funcionamiento espera recibir *saludos* del router de protección cada intervalo hello. Si el router en funcionamiento no recibe saludos durante un intervalo de tiempo especificado por el intervalo de espera, el router en

funcionamiento asume una falla PGP y APS se suspende. De manera similar, si el router de protección no recibe confirmaciones hello del router en funcionamiento antes de que caduque el temporizador de intervalo de espera, declara una falla de PGP y puede ocurrir un switchover.

Temporizadores hello y hold

POS APS difiere de SONET APS "estricto". POS APS admite comandos de configuración adicionales utilizados para configurar parámetros de PGP.

Puede utilizar el comando **aps timers** para cambiar el temporizador hello y el temporizador hold. El temporizador hello define el tiempo entre los paquetes hello. El temporizador de espera establece el tiempo antes de que el proceso de la interfaz de protección declare que el router de una interfaz en funcionamiento está inactivo. De forma predeterminada, el tiempo de espera es mayor o igual a tres veces el tiempo hello.

El siguiente ejemplo especifica un tiempo hello de dos segundos y un tiempo de espera de seis segundos en el circuito 1 en la interfaz POS 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
```

Como se muestra arriba, hemos configurado el comando **aps timers** solamente en las interfaces de protección.

Puede configurar las interfaces de trabajo y protección con tiempos de espera y hello únicos. Cuando trabaja en contacto con una interfaz de protección, utiliza los valores del temporizador especificados para la interfaz de protección. Cuando el trabajo no está en contacto con una interfaz de protección, utiliza los temporizadores hello y hold especificados para la interfaz de trabajo.

Autenticación

Otro comando soportado solamente por POS APS es el comando **authentication**, que habilita la autenticación entre los procesos que controlan las interfaces de trabajo y de protección. Utilice este comando para especificar la cadena que debe estar presente para aceptar cualquier paquete en una interfaz de protección o en funcionamiento. Se aceptan hasta ocho caracteres alfanuméricos.

Contacto con el TAC de Cisco

Si necesita ayuda para la resolución de problemas de APS, póngase en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC). Recopile resultados de los siguientes comandos **show** en los routers con las interfaces de protección y funcionamiento:

- **show version** - Muestra la configuración del hardware del sistema y la versión del software. Este comando también muestra los nombres y orígenes de los archivos de configuración y las

imágenes de inicio.
- **show controller pos**- Muestra información sobre los controladores POS.
- **show aps** - Muestra información sobre la función de conmutación de protección automática actual.

Información Relacionada

- Páginas de soporte de tecnología óptica
- Soporte Técnico - Cisco Systems