Comprensión de las versiones APS en las interfaces POS

Contenido

Introducción

Este documento describe el protocolo protect group (PGP), que es una parte clave de Automatic Protection Switching (APS) del Packet Over SONET (POS) en los routeres Cisco y los switches Enterprise.

prerrequisitos

Requisitos

Este documento no tiene ningún requisito específico.

Componentes Utilizados

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

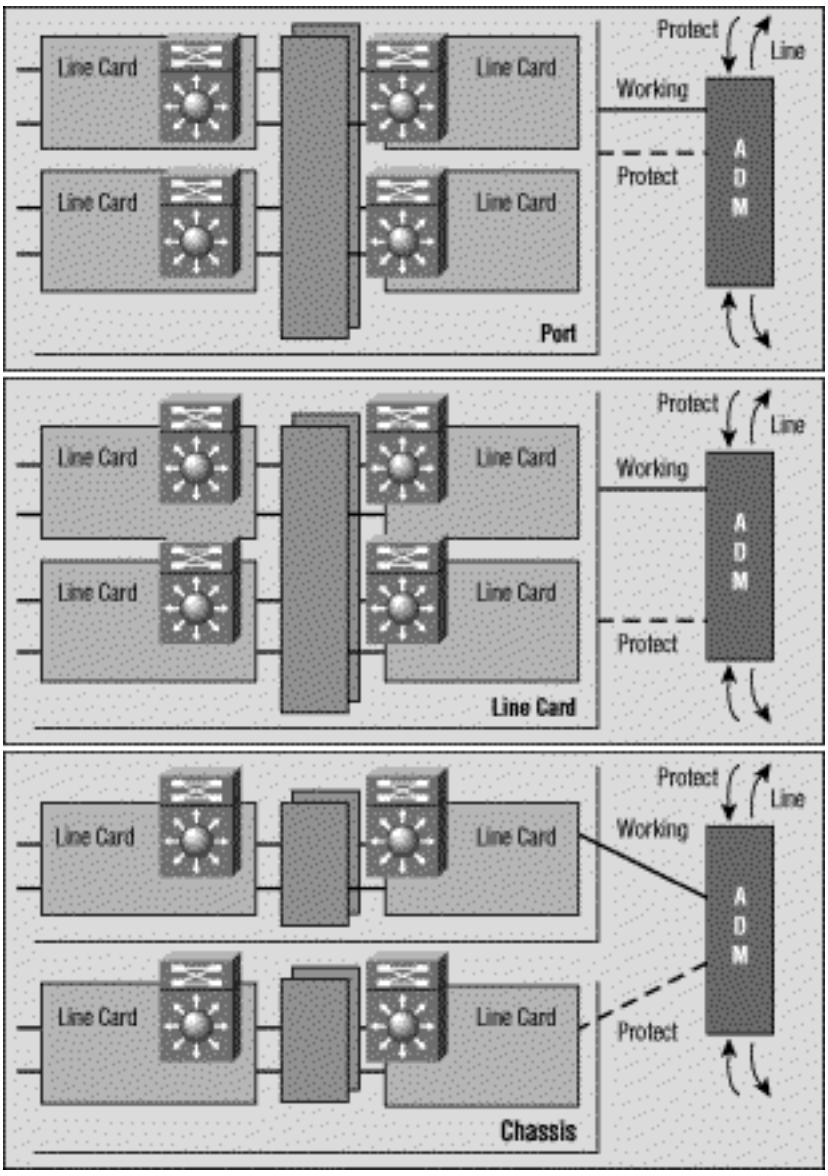
Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Información general de PGP

La publicación TR-TSY-000253 del Bellcore (ahora Telcordia), sistemas del transporte SONET; Los criterios genéricos comunes, la sección 5.3, definen el Automatic Protection Switching (APS). El mecanismo de protección usado para esta característica tiene 1+1, la arquitectura, en la cual un par de líneas redundantes consiste en una línea operativa y una línea de protección.

Este ejemplo muestra las configuraciones de la protección SONET posibles. Usted puede configurar el esquema de protección del POS de Cisco para las situaciones donde proteja y las interfaces en funcionamiento son diversos puertos. Estos puertos pueden estar en el mismo router o en el mismo linecard en el mismo router. Estos escenarios, sin embargo, proporcionan la protección para la interfaz del router o la falla de link. La mayoría de las implementaciones de producto tienen trabajo y protegen las interfaces en diverso Routers. En tal configuración APS del dos-router, un protocolo como el PGP se requiere. El PGP define el protocolo entre el funcionamiento y protege al Routers.



Versiones de PGP

A partir del Software Release 12.0(10)S de Cisco IOS®, dos versiones del PGP están disponibles. El funcionamiento y protege al Routers debe utilizar la misma versión de PGP e intercambiar los mensajes de negociación usando un enlace de comunicaciones fuera de banda. Durante la negociación, el router de la protección envía los mensajes en las versiones PGP múltiples, lo más arriba posible primero. El router en funcionamiento ignora el hellos con los números de la versión

más altos que sus los propio y contesta a los otros. Una vez que el router en funcionamiento contesta a un mensaje Hello Messages, adopta ese número de la versión, y lo utiliza en todas las respuestas subsiguientes.

En las versiones actuales del Cisco IOS, el funcionamiento y protege al Routers no necesita funcionar con la misma versión del IOS. El funcionamiento y protege al Routers se puede por lo tanto actualizar independientemente.

Si el Cisco IOS Software detecta una discordancía de la versión, imprime los mensajes del registro similares a esto:

```
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 el rendimiento disminuido y la alta pérdida del paquete, la negociación de la versión APS entre el funcionamiento y protege al Routers falla. Como consecuencia, ambo Routers adopta las versiones de PGP del “abajo revolución”. Los resultados del problema de los mensajes de negociación corrompidos. Si link de comunicaciones PGP experimenta un alto nivel de la pérdida del paquete, el router en funcionamiento puede faltar hola enviado por el router de la protección con un número de la versión de divulgación. Si sucede esto, puede ser que vea solamente el mensaje subsiguiente del abajo revolución. Este escenario causa a ambos el funcionamiento y protege al Routers para bloquear sobre el número de la versión inferior. El Cisco IOS Software Release 12.0(21)S evita este problema haciendo la renegociación simultánea como sea necesario.

Si usted está utilizando una versión antes de la versión de software IOS 12.0(21)S y experimenta este problema, utilice esta solución alternativa para restablecer la versión normal de PGP. Haga esto una vez que usted ha establecido un link confiable entre el dos Routers:

1. Asegúrese de que la interfaz en funcionamiento esté seleccionada. Usted puede utilizar el comando aps force 0 de hacer esto.
2. Cierre la interfaz de la protección. Déjela abajo suficientemente larga de modo que el trabajo declare que ha perdido las comunicaciones con la interfaz de la protección.
3. Utilice el comando no shutdown en la interfaz de la protección de recomenzar las negociaciones del protocolo.

Las fallas de comunicación PGP pueden ocurrir debido a ninguno de estos problemas:

- Error del router en funcionamiento
- Proteja la falla del router
- Error del canal PGP

El error del canal PGP puede ocurrir debido a ninguno de estos problemas:

- Congestión de tráfico
- Falla debido de la interfaz a las alarmas
- Falla de hardware de la interfaz

Usted puede proporcionar las interfaces del ancho de banda mayor para el PGP para minimizar la

congestión y evitar algunos errores del canal PGP. El router en funcionamiento espera recibir el *hellos del* router de la protección cada intervalo de saludo. Si el router en funcionamiento no recibe el hellos para un intervalo de tiempo especificado por el control-intervalo, el router en funcionamiento asume un error PGP, y se suspende el APS. Semejantemente, si el router de la protección no recibe hola los acuses de recibo del router en funcionamiento antes de que expire el temporizador del control-intervalo, declara que error PGP y un intercambio puede ocurrir.

Temporizadores hello y hold

El POS APS diferencia del SONET APS “estricto”. El POS APS apoya los comandos configuration adicionales usados para configurar los parámetros del PGP.

Usted puede utilizar el **comando aps timers** de cambiar el temporizador de saludo y al temporizador del control. El temporizador de saludo define el tiempo entre los paquetes de saludo. El temporizador del control fija el tiempo antes de que el proceso de la interfaz de la protección declare al router de una interfaz en funcionamiento estar abajo. Por abandono, el tiempo en espera es mayor o igual tres veces el tiempo de saludo.

El siguiente ejemplo especifica un tiempo de saludo de dos segundos y de un tiempo en 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 la protección.

Usted puede configurar el funcionamiento y proteger las interfaces con los saludos únicos y los tiempos en espera. Cuando el trabajo está en contacto con una interfaz de la protección, utiliza los valores del temporizador especificados para la interfaz de la protección. Cuando el trabajo no está en contacto con una interfaz de la protección, utiliza los temporizadores de espera y saludos especificados para la interfaz en funcionamiento.

Autenticación

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

Contacto con el TAC de Cisco

Si usted necesita la ayuda con el troubleshooting APS, entre en contacto el Centro de Asistencia Técnica de Cisco (TAC). Recolecte por favor la salida de los **comandos show** siguientes en el Routers con la protección y las interfaces en funcionamiento:

- **muestre que la versión** visualiza la configuración del hardware del sistema y de la versión de software. Este comando también visualiza los archivos de los nombres y de fuentes de la configuración y las imágenes del arranque de sistema.
- **muestre la** información de las visualizaciones **posición del regulador** sobre los controladores POS.
- **demostración aps** - Visualiza la información sobre la función de Automatic Protection Switching actual.

Información Relacionada

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