Compreendendo versões de APS em interfaces POS

Contents

Introduction

Este documento descreve o Protocolo de Grupo de Proteção (PGP - Protect Group Protocol), que é uma parte chave do Packet Over SONET (POS - Packet Over SONET) Automatic Protection Switching (APS - Automatic Protection Switching) em roteadores Cisco e switches empresariais.

Prerequisites

Requirements

Este documento não tem requisitos específicos.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Conventions

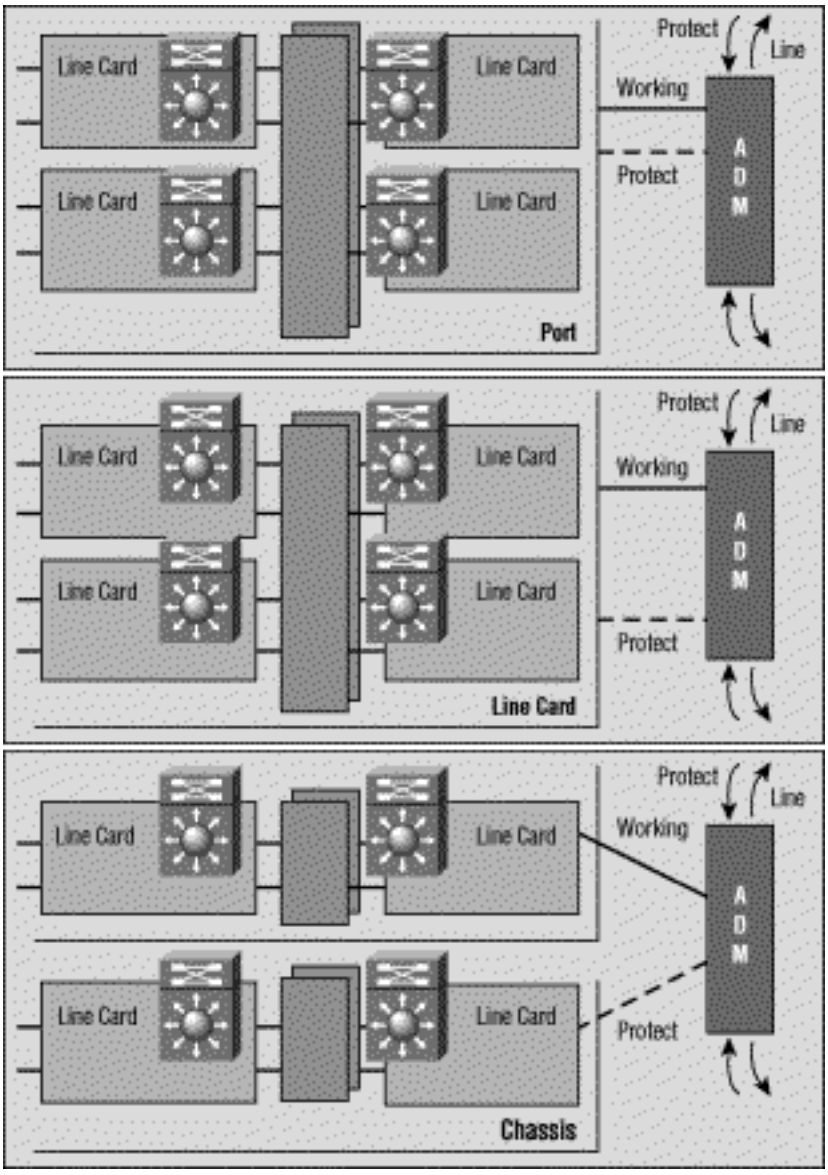
For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Visão geral de PGP

A publicação Bellcore (atualmente Telcordia) TR-TSY-000253, SONET Transport Systems; Common Generic Criteria, Seção 5.3, define Automatic Protection Switching (APS). O mecanismo

de proteção usado para esse recurso tem 1+1, arquitetura, na qual um par de linha redundante consiste em uma linha funcional e uma linha de proteção.

Esta ilustração mostra possíveis configurações de proteção SONET. Você pode configurar o esquema de proteção Cisco POS para situações em que as interfaces de proteção e de trabalho são portas diferentes. Essas portas podem estar no mesmo roteador ou na mesma placa de linha no mesmo roteador. Esses cenários, no entanto, fornecem proteção para a interface do roteador ou falha do link. A maioria das implantações de produção tem interfaces em funcionamento e de proteção em roteadores diferentes. Em uma configuração de APS de dois roteadores, um protocolo como o PGP é necessário. O PGP define o protocolo entre os roteadores em funcionamento e protege os roteadores.



Versões do PGP

A partir do Cisco IOS® Software Release 12.0(10)S, duas versões do PGP estão disponíveis. Os roteadores que trabalham e protegem devem usar a mesma versão do PGP e trocar mensagens de negociação usando um link de comunicação fora da banda. Durante a negociação, o roteador de proteção envia mensagens em várias versões de PGP, as mais altas primeiro. O roteador em funcionamento ignora saudações com números de versão superiores aos seus e responde aos outros. Quando o roteador em funcionamento responde uma mensagem de saudação, ele adota esse número de versão e o usa em todas as respostas subsequentes.

Nas versões atuais do Cisco IOS, os roteadores que funcionam e protegem não precisam executar a mesma versão do IOS. Os roteadores que funcionam e protegem podem, portanto, ser atualizados independentemente.

Se o software Cisco IOS detectar uma incompatibilidade de versão, ele imprimirá mensagens de log semelhantes a esta:

```
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
```

Se esse link apresentar desempenho reduzido e alta perda de pacotes, a negociação da versão APS entre os roteadores em funcionamento e de proteção falhará. Como resultado, ambos os roteadores adotam versões de PGP "down-rev". O problema resulta de mensagens de negociação corrompidas. Se o enlace de comunicação PGP sofrer uma alta perda de pacotes, o roteador em funcionamento pode perder o hello enviado pelo roteador de proteção com um número de versão anunciado. Se isso acontecer, ele poderá ver apenas a mensagem down-rev subsequente. Esse cenário faz com que os roteadores em funcionamento e de proteção se bloqueiem no número de versão mais baixo. O Cisco IOS Software Release 12.0(21)S evita esse problema ao fazer uma renegociação imediata conforme necessário.

Se você estiver usando uma versão anterior ao software IOS versão 12.0(21)S e tiver esse problema, use esta solução alternativa para restaurar a versão normal do PGP. Faça isso depois de estabelecer um link confiável entre os dois roteadores:

1. Verifique se a interface de trabalho está selecionada. Você pode usar o comando **aps force 0** para fazer isso.
2. Feche a interface de proteção. Deixe-o parado o suficiente para que o que está funcionando declare que ele perdeu as comunicações com a interface de proteção.
3. Use o comando **no shutdown** na interface de proteção para reiniciar negociações de protocolo.

Falhas de comunicação PGP podem ocorrer devido a qualquer um destes problemas:

- Falha no roteador em funcionamento
- Proteger falha do roteador
- falha de canal PGP

A falha do canal PGP pode ocorrer devido a qualquer um destes problemas:

- Congestionamento de tráfego
- Falha de interface devido a alarmes
- Falha de hardware de interface

Você pode fornecer interfaces de largura de banda mais alta para o PGP a fim de minimizar o congestionamento e evitar algumas falhas de canal do PGP. O roteador em funcionamento espera receber *saudações* do roteador de proteção a cada intervalo de saudação. Se o roteador em funcionamento não receber saudações para um intervalo de tempo especificado pelo intervalo de espera, o roteador em funcionamento assumirá uma falha de PGP e o APS será suspenso. Da mesma forma, se o roteador de proteção não receber confirmações de saudação do roteador em

funcionamento antes que o temporizador de intervalo de retenção expire, ele declarará uma falha de PGP e um switchover poderá ocorrer.

Timers de saudação e de espera

APS POS difere de APS SONET "rígidos". O POS APS suporta comandos de configuração adicionais usados para configurar parâmetros do PGP.

Você pode usar o comando **aps timers** para alterar o temporizador hello e o temporizador hold. O temporizador hello define o tempo entre os pacotes hello. O temporizador de espera define o tempo antes que o processo de interface de proteção declare o roteador de uma interface em funcionamento inativo. Por padrão, o tempo de espera é maior ou igual a três vezes o tempo de saudação.

O exemplo a seguir especifica um tempo de saudação de dois segundos e um tempo de espera de seis segundos no circuito 1 na interface 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 mostrado acima, configuramos o comando **aps timers** somente nas interfaces de proteção.

Você pode configurar as interfaces de trabalho e proteção com horários de saudação e espera exclusivos. Quando o trabalho está em contato com uma interface de proteção, ele usa os valores de temporizador especificados para a interface de proteção. Quando o trabalho não está em contato com uma interface de proteção, ele usa os temporizadores hello e hold especificados para a interface de trabalho.

Autenticação

Outro comando suportado somente pelo POS APS é o comando **authentication**, que permite a autenticação entre os processos que controlam as interfaces de trabalho e de proteção. Use este comando para especificar a cadeia de caracteres que deve estar presente para aceitar qualquer pacote em uma interface de proteção ou de trabalho. Até oito caracteres alfanuméricos são aceitos.

Entrando em contato com o Cisco TAC

Se precisar de assistência para solucionar problemas de APS, entre em contato com o Cisco Technical Assistance Center (TAC). Obtenha a saída dos seguintes comandos **show** nos roteadores com as interfaces de proteção e de trabalho:

- **show version** - Exibe a configuração do hardware do sistema e a versão do software. Esse comando também exibe os nomes e as origens dos arquivos de configuração e as imagens de inicialização.
- **show controller pos** - Exibe informações sobre os controladores POS.

- **show aps** - Exibe informações sobre o recurso de switching de proteção automática atual.

Informações Relacionadas

- Páginas de suporte de tecnologia ótica
- Suporte Técnico - Cisco Systems