Présentation des versions d'APS sur les interfaces POS

Contenu

Introduction

Ce document décrit le protocole PGP (Protect Group Protocol), qui est un élément clé de la commutation de protection automatique (APS) Packet Over SONET (POS) sur les routeurs Cisco et les commutateurs d'entreprise.

Conditions préalables

Conditions requises

Ce document n'a aucune exigence spécifique.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

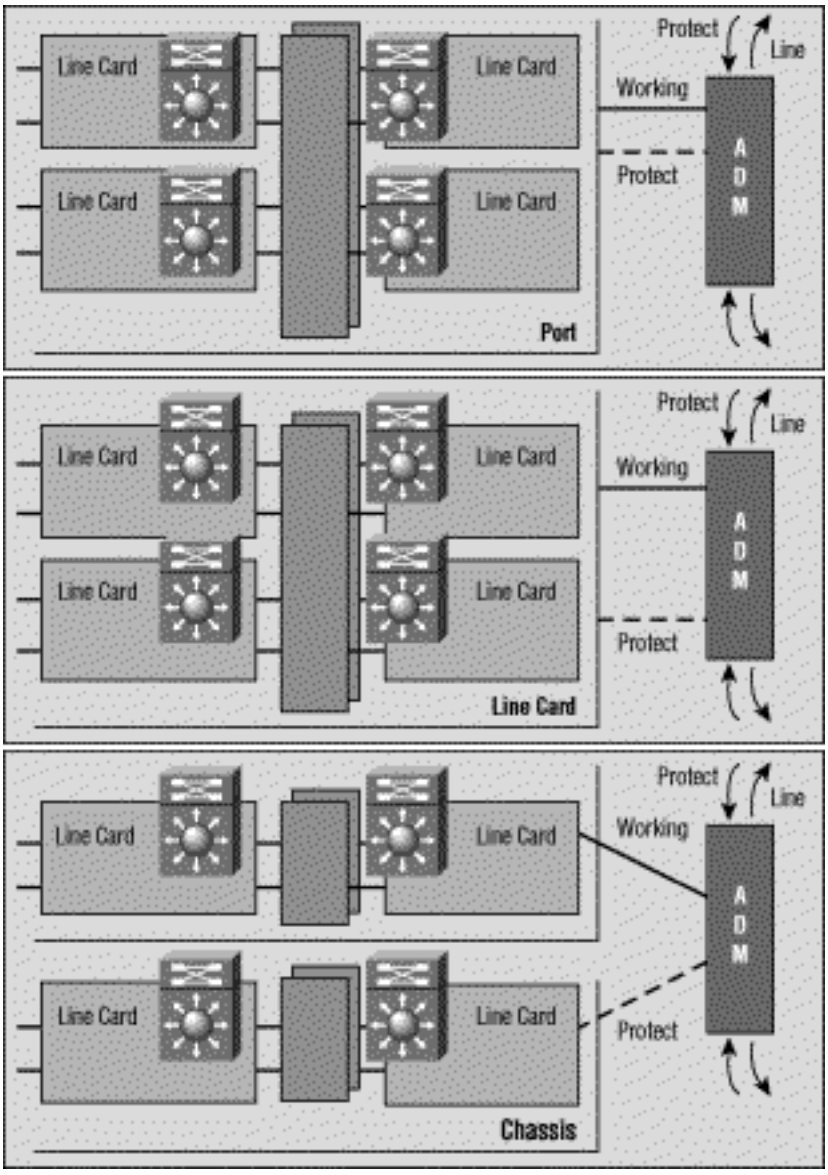
For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Présentation de PGP

La publication de Bellcore (aujourd'hui Telcordia) TR-TSY-000253, SONET Transport Systems ; Common Generic Criteria, Section 5.3, définit la commutation à protection automatique (APS). Le

mécanisme de protection utilisé pour cette fonctionnalité a une architecture 1+1, dans laquelle une paire de lignes redondantes se compose d'une ligne de travail et d'une ligne de protection.

Cette illustration présente les configurations de protection SONET possibles. Vous pouvez configurer le système de protection Cisco POS pour les situations où les interfaces de protection et de travail sont des ports différents. Ces ports peuvent se trouver sur le même routeur ou sur la même carte de ligne sur le même routeur. Ces scénarios offrent toutefois une protection contre les défaillances de l'interface du routeur ou de la liaison. La plupart des déploiements de production ont des interfaces de travail et de protection sur différents routeurs. Dans une telle configuration APS à deux routeurs, un protocole tel que PGP est requis. Le protocole PGP définit le protocole entre les routeurs actifs et protège les routeurs.



Versions PGP

Depuis la version 12.0(10)S du logiciel Cisco IOS®, deux versions de PGP sont disponibles. Les routeurs actifs et protégés doivent utiliser la même version PGP et échanger des messages de négociation à l'aide d'une liaison de communication hors bande. Au cours de la négociation, le routeur de protection envoie des messages dans plusieurs versions PGP, en premier lieu le plus élevé. Le routeur actif ignore les paquets Hello dont les numéros de version sont supérieurs aux siens et répond aux autres. Une fois que le routeur actif a répondu à un message Hello, il adopte ce numéro de version et l'utilise dans toutes les réponses suivantes.

Dans les versions actuelles de Cisco IOS, les routeurs de travail et de protection n'ont pas besoin d'exécuter la même version d'IOS. Les routeurs de travail et de protection peuvent donc être mis à niveau indépendamment.

Si le logiciel Cisco IOS détecte une incompatibilité de version, il imprime les messages de journal de la même manière que ceci :

```
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 cette liaison présente des performances dégradées et une perte de paquets élevée, la négociation de version APS entre les routeurs fonctionnant et protégeant échoue. Par conséquent, les deux routeurs adoptent des versions PGP « down-rev ». Le problème provient de messages de négociation corrompus. Si la liaison de communication PGP subit une perte de paquets élevée, le routeur opérationnel peut manquer le Hello envoyé par le routeur de protection avec un numéro de version annoncé. Si cela se produit, il se peut qu'il ne voit que le message down-rev suivant. Ce scénario entraîne le fonctionnement et la protection des routeurs pour qu'ils se verrouillent sur le numéro de version inférieur. Le logiciel Cisco IOS Version 12.0(21)S évite ce problème en renégociant à la volée selon les besoins.

Si vous utilisez une version antérieure au logiciel IOS Version 12.0(21)S et que vous rencontrez ce problème, utilisez cette solution de contournement pour restaurer la version PGP normale. Effectuez cette opération une fois que vous avez établi une liaison fiable entre les deux routeurs :

1. Assurez-vous que l'interface de travail est sélectionnée. Vous pouvez utiliser la commande **aps force 0** pour cela.
2. Fermez l'interface de protection. Laisser le câble hors tension suffisamment longtemps pour que le routeur actif déclare avoir perdu les communications avec l'interface de protection.
3. Utilisez la commande **no shutdown** sur l'interface de protection pour redémarrer les négociations de protocole.

Des échecs de communication PGP peuvent se produire en raison de l'un de ces problèmes :

- Échec du routeur de travail
- Protection contre les défaillances du routeur
- Échec du canal PGP

Une défaillance du canal PGP peut se produire en raison de l'un de ces problèmes :

- Empêcher le trafic
- Panne d'interface due aux alarmes
- Panne matérielle de l'interface

Vous pouvez fournir des interfaces de bande passante plus élevée pour PGP afin de minimiser l'encombrement et d'éviter certaines défaillances de canaux PGP. Le routeur actif attend de recevoir *des paquets Hello* du routeur de protection à chaque intervalle Hello. Si le routeur actif ne reçoit pas d'HELLO pendant un intervalle de temps spécifié par l'intervalle de conservation, le routeur actif suppose une défaillance PGP et l'APS est suspendu. De même, si le routeur de protection ne reçoit pas d'accusés de réception Hello du routeur actif avant l'expiration du

compteur d'intervalle d'attente, il déclare une défaillance PGP et un basculement peut se produire.

Minuteurs Hello et Hold

POS APS diffère de SONET APS « strict ». POS APS prend en charge des commandes de configuration supplémentaires utilisées pour configurer les paramètres de PGP.

Vous pouvez utiliser la commande **aps timers** pour modifier le compteur Hello et le compteur d'attente. Le minuteur Hello définit le délai entre les paquets Hello. Le compteur d'attente définit la durée avant que le processus de protection de l'interface déclare le routeur d'une interface opérationnelle hors service. Par défaut, le temps d'attente est supérieur ou égal à trois fois le temps Hello.

L'exemple suivant spécifie un délai Hello de deux secondes et un délai d'attente de six secondes sur le circuit 1 sur l'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
```

Comme indiqué ci-dessus, nous avons configuré la commande **aps timers** uniquement sur les interfaces de protection.

Vous pouvez configurer les interfaces de travail et de protection avec des temps d'attente et d'attente uniques. Lorsque vous travaillez en contact avec une interface de protection, elle utilise les valeurs de minuteur spécifiées pour l'interface de protection. Lorsque le travail n'est pas en contact avec une interface de protection, il utilise les minuteurs Hello et de mise en attente spécifiés pour l'interface de travail.

Authentification

Une autre commande prise en charge uniquement par POS APS est la commande **authentication**, qui active l'authentification entre les processus contrôlant les interfaces de travail et de protection. Utilisez cette commande pour spécifier la chaîne qui doit être présente pour accepter tout paquet sur une interface de protection ou de travail. Jusqu'à huit caractères alphanumériques sont acceptés.

Contacter le TAC Cisco

Si vous avez besoin d'aide pour le dépannage d'APS, contactez le centre d'assistance technique Cisco (TAC). Recueillez les résultats des commandes **show** suivantes sur les routeurs avec les interfaces de protection et de travail :

- **show version** - Affiche la configuration du matériel système et de la version du logiciel. Cette commande affiche également les noms et les sources des fichiers de configuration et les images de démarrage.
- **show controller pos** - Affiche des informations sur les contrôleurs POS.

- **show aps** - Affiche des informations sur la fonction de commutation de protection automatique actuelle.

Informations connexes

- Pages de soutien de la technologie optique
- Support technique - Cisco Systems