Présentation des versions d'APS sur les interfaces POS

Contenu

Introduction

Ce document décrit le groupe Protocol (PGP) de protection, qui est une partie principale de Fonction Automatic Protection Switching (APS) de Paquet sur SONET (POS) sur des Routeurs et des commutateurs de la gamme Enterprise de Cisco.

Conditions préalables

Conditions requises

Ce document n'a aucune condition requise spécifique.

Composants utilisés

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

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Aperçu PGP

La publication TR-TSY-000253 de Bellcore (maintenant Telcordia), systèmes de transport SONET

; Les critères génériques communs, la section 5.3, définit le Fonction Automatic Protection Switching (APS). Le mécanisme de protection utilisé pour cette caractéristique a 1+1, l'architecture, en laquelle paire de lignes redondant se compose d'une ligne fonctionnante et d'une ligne de protection.

Cette illustration affiche des configurations possibles de protection SONET. Vous pouvez installer le schéma de protection de POS de Cisco pour des situations où protégez et en fonctionnant des interfaces soyez différents ports. Ces ports peuvent être sur le même routeur ou sur le même linecard dans le même routeur. Ces scénarios, cependant, assurent la protection pour la panne d'interface de routeur ou de lien. La plupart des déploiements de production ont fonctionner et protègent des interfaces sur différents Routeurs. Dans une telle configuration du deux-routeur aps, un protocole comme le PGP est exigé. Le PGP définit le protocole entre le fonctionnement et protège des Routeurs.

Versions PGP

En date de la version de logiciel 12.0(10)S de Cisco IOS®, deux versions de PGP sont disponibles. Le fonctionnement et protègent des Routeurs doit utiliser la même version PGP et permuter des messages de négociation utilisant une liaison hors bande. Pendant la négociation, le routeur de protection l'envoie message dans de plusieurs versions PGP, le premier le plus élevé. Le routeur fonctionnant ignore des hellos avec le supérieur à de numéros de version ses propres moyens et répond aux autres. Une fois que le routeur fonctionnant répond à un message Hello, il adopte ce numéro de version, et l'utilise dans toutes les réponses ultérieures.

Dans des releases en cours de Cisco IOS, le fonctionnement et protègent des Routeurs n'a pas besoin d'exécuter la même release IOS. Le fonctionnement et protègent des Routeurs peut donc être mis à jour indépendamment.

Si le logiciel de Cisco IOS détecte une non-concordance de version, il imprime des messages de log semblables à 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 ce lien éprouve la représentation et la perte de paquets dégradées de haute, la négociation de version aps entre le fonctionnement et protègent des Routeurs échoue. En conséquence, les deux Routeurs adoptent des versions PGP de « vers le bas-Rév ». Les résultats de problème des messages corrompus de négociation. Si la liaison PGP éprouve la perte de paquets élevée, le routeur fonctionnant peut manquer bonjour envoyé par le routeur de protection avec un numéro de version annoncé. Si ceci se produit, il pourrait seulement voir le message ultérieur de vers le bas-Rév. Ce scénario entraîne le fonctionnement et protège des Routeurs pour verrouiller sur le numéro de version inférieur. Le Logiciel Cisco IOS version 12.0(21)S évite ce problème en faisant la renégociation en marche au besoin.

Si vous utilisez une version avant la version de logiciel d'IOS Software 12.0(21)S et rencontrez ce problème, employez ce workaround pour restaurer la version normale PGP. Faites ceci une fois que vous avez établi un lien fiable entre les deux Routeurs :

1. Assurez-vous que l'interface fonctionnante est sélectionnée. Vous pouvez utiliser la commande de l'**aps force 0** de faire ceci.
2. Fermez l'interface de protection. Laissez-le vers le bas assez long de sorte que fonctionnant déclare qu'il a perdu des transmissions avec l'interface de protection.
3. N'utilisez l'**aucune commande shutdown** sur l'interface de protection de redémarrer des négociations de protocole.

Les pannes de communication PGP peuvent se produire en raison de l'un de ces questions :

- Fonctionner la panne de routeur
- Protégez la panne de routeur
- Panne de canal PGP

La panne de canal PGP peut se produire en raison de l'un de ces questions :

- Embouteillages
- Panne d'interface due aux alarmes
- Défaillance matérielle d'interface

Vous pouvez fournir des interfaces de bande passante élevée pour le PGP afin de réduire l'encombrement et éviter quelques pannes de canal PGP. Le routeur fonctionnant compte recevoir des *hellos du* routeur de protection chaque intervalle Hello. Si le routeur fonctionnant ne reçoit pas des hellos pour un intervalle de temps spécifié par l'attente-intervalle, le routeur fonctionnant assume une panne PGP, et des aps est interrompus. De même, si le routeur de protection ne reçoit pas bonjour des accusés de réception du routeur fonctionnant avant que le temporisateur d'attente-intervalle expire, il déclare que panne PGP et un basculement peut se produire.

Bonjour et temporisateurs d'attente

Le POS aps diffère de SONET « strict » aps. Le POS aps prend en charge des commandes de configuration supplémentaire utilisées pour configurer des paramètres de PGP.

Vous pouvez utiliser l'**aps timers** commandez de changer le minuteur Hello et le temporisateur d'attente. Le minuteur Hello définit le temps entre bonjour les paquets. Le temporisateur d'attente place le temps avant que le processus d'interface de protection déclare le routeur d'une interface fonctionnante être en baisse. Par défaut, la durée d'attente est supérieur ou égal à trois fois l'intervalle Hello.

L'exemple suivant spécifie un intervalle Hello de deux secondes et d'une durée d'attente de six secondes sur le circuit 1 sur l'interface 5/0/0 de POS :

```
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 affiché ci-dessus, nous avons configuré la commande d'**aps timers** seulement sur les interfaces de protection.

Vous pouvez configurer le fonctionnement et protéger des interfaces avec le seuls bonjour et durées d'attente. Quand fonctionner est en contact avec une interface de protection, il utilise les valeurs de temporisateur spécifiées pour l'interface de protection. Quand fonctionner n'est pas en contact avec une interface de protection, il utilise bonjour et des temporisateurs d'attente spécifiés pour l'interface fonctionnante.

Authentification

Une autre commande prise en charge seulement par le POS aps est l'**authentication command**, qui active l'authentification entre les processus contrôlant le fonctionnement et protège des interfaces. Utilisez cette commande de spécifier la chaîne qui doit être présente pour recevoir n'importe quel paquet sur une protection ou une interface de fonctionner. Jusqu'à huit caractères alphanumériques sont reçus.

Contacter Cisco TAC

Si vous avez besoin de l'assistance avec le dépannage aps, entrez en contact avec le centre d'assistance technique Cisco (TAC). Veuillez recueillir la sortie des **commandes show** suivantes sur les Routeurs avec la protection et les interfaces de fonctionner :

- **affichez que la version** affiche la configuration du matériel système et de la version de logiciel. Cette commande affiche également les noms et les sources des fichiers de configuration et des images de démarrage.
- affiche des informations **position de show controller** au sujet des contrôleurs de POS.
- **show aps** - Affiche des informations au sujet de la caractéristique automatique en cours de commutation de protection.

Informations connexes

- Pages de support technologique Optiques
- Support technique - Cisco Systems