Informazioni sulle versioni APS sulle interfacce POS

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Convenzioni](#)
[Panoramica di PGP](#)
[Versioni PGP](#)
[Timer di saluto e attesa](#)
[Autenticazione](#)
[Come contattare Cisco TAC](#)
[Informazioni correlate](#)

Introduzione

Questo documento descrive il Protect Group Protocol (PGP), che è una parte chiave del POS (Packet Over SONET) Automatic Protection Switching (APS) su router Cisco e switch aziendali.

Prerequisiti

Requisiti

Questo documento non ha requisiti specifici.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

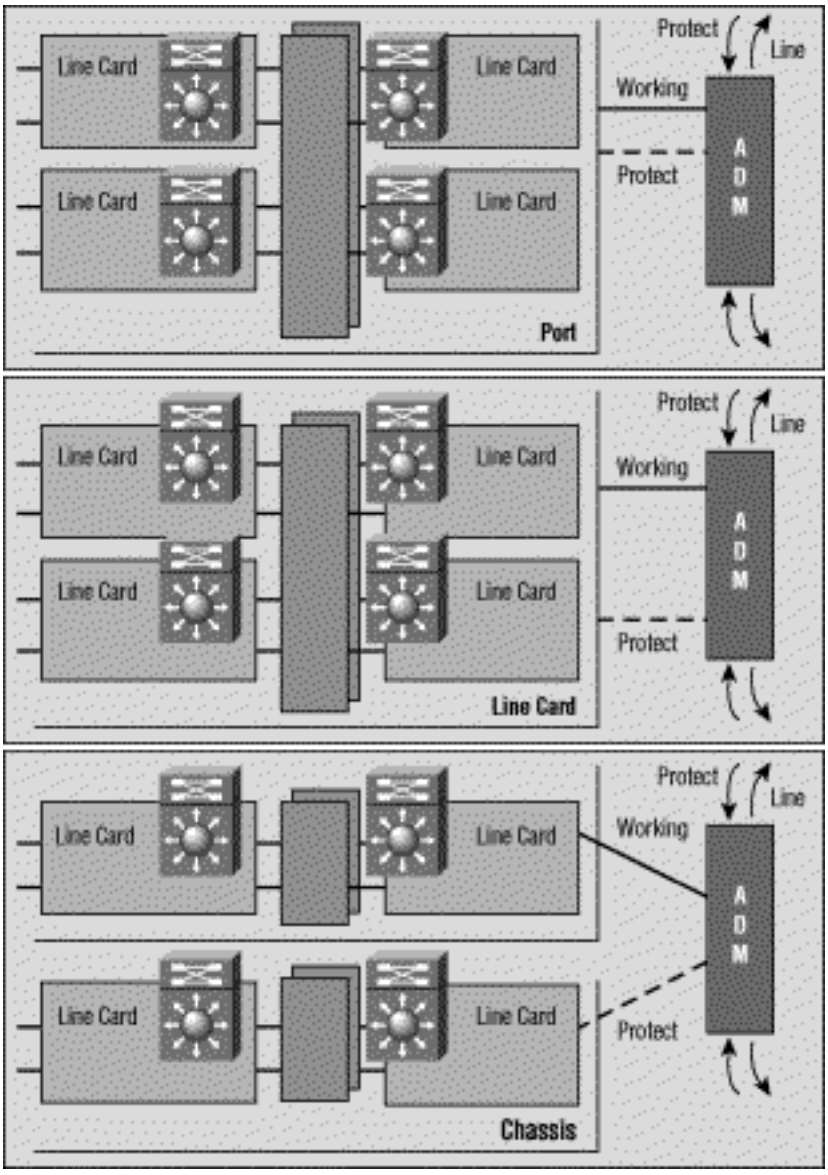
Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Panoramica di PGP

La pubblicazione di Bellcore (ora Telcordia) TR-TSY-000253, SONET Transport Systems; Common Generic Criteria, sezione 5.3, definisce la tecnologia Automatic Protection Switching

(APS). Il meccanismo di protezione utilizzato per questa funzione è basato sull'architettura 1+1, in cui una coppia di linee ridondanti è costituita da una linea di lavoro e una linea di protezione.

Nella figura vengono mostrate le possibili configurazioni di protezione SONET. È possibile configurare lo schema di protezione POS di Cisco in situazioni in cui le interfacce di protezione e di funzionamento sono porte diverse. Queste porte possono trovarsi sullo stesso router o sulla stessa scheda di linea nello stesso router. Questi scenari, tuttavia, forniscono protezione in caso di errore dell'interfaccia del router o del collegamento. La maggior parte delle installazioni di produzione dispone di interfacce funzionanti e protette su router diversi. In una configurazione APS a due router, è richiesto un protocollo come PGP. PGP definisce il protocollo tra i router funzionanti e i router di protezione.



Versioni PGP

A partire dal software Cisco IOS® versione 12.0(10)S, sono disponibili due versioni di PGP. I router funzionanti e protetti devono utilizzare la stessa versione PGP e scambiare messaggi di negoziazione utilizzando un collegamento di comunicazione fuori banda. Durante la negoziazione, il router di protezione invia i messaggi in più versioni PGP, la prima più alta. Il router funzionante ignora gli helper con numeri di versione superiori al proprio e risponde agli altri. Quando il router funzionante risponde a un messaggio di benvenuto, adotta il numero di versione e lo utilizza in tutte le risposte successive.

Nelle versioni Cisco IOS correnti, i router funzionanti e protettivi non devono eseguire la stessa versione IOS. I router funzionanti e protetti possono quindi essere aggiornati in modo indipendente.

Se il software Cisco IOS rileva una mancata corrispondenza delle versioni, visualizza messaggi di registro simili al seguente:

```
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 le prestazioni di questo collegamento risultano ridotte e il pacchetto viene perso in modo elevato, la negoziazione della versione APS tra i router funzionanti e i router di protezione non riuscirà. Di conseguenza, entrambi i router adottano le versioni "down-rev" PGP. Il problema è dovuto a messaggi di negoziazione danneggiati. Se il collegamento alle comunicazioni PGP subisce una perdita elevata di pacchetti, il router funzionante può perdere il saluto inviato dal router di protezione con un numero di versione pubblicizzato. In questo caso, è possibile che venga visualizzato solo il successivo messaggio di inversione. In questo scenario, i router attivi e quelli protetti vengono bloccati sul numero di versione inferiore. Il software Cisco IOS versione 12.0(21)S evita questo problema eseguendo una rinegoziazione immediata come richiesto.

Se si utilizza una versione precedente al software IOS versione 12.0(21)S e si verifica questo problema, utilizzare questa soluzione per ripristinare la versione PGP normale. Eseguire questa operazione dopo aver stabilito un collegamento affidabile tra i due router:

1. Accertatevi che l'interfaccia di lavoro sia selezionata. A tale scopo, è possibile utilizzare il comando **aps force 0**.
2. Chiudere l'interfaccia di protezione. Lasciare il pannello abbassato abbastanza a lungo da far sì che chi lavora dichiari di aver perso le comunicazioni con l'interfaccia di protezione.
3. Usare il comando **no shutdown** sull'interfaccia di protezione per riavviare le negoziazioni del protocollo.

Gli errori di comunicazione PGP possono essere causati da uno dei seguenti problemi:

- Errore del router funzionante
- Errore protezione router
- Errore del canale PGP

L'errore del canale PGP può essere causato da uno dei seguenti problemi:

- Congestione del traffico
- Errore dell'interfaccia a causa di allarmi
- Errore hardware dell'interfaccia

Èpossibile fornire interfacce con larghezza di banda maggiore per PGP per ridurre al minimo la congestione ed evitare alcuni errori del canale PGP. Il router funzionante si aspetta di ricevere *chiamate* di emergenza dal router di protezione a ogni intervallo di chiamata. Se il router operativo non riceve chiamate in attesa per un intervallo di tempo specificato dall'intervallo di attesa, assume un errore PGP e l'APS viene sospeso. Analogamente, se il router di protezione non riceve hello acknowledgement dal router funzionante prima della scadenza del timer dell'intervallo di

attesa, dichiara un errore PGP e può verificarsi un passaggio.

Timer di saluto e attesa

I POS AP si differenziano dai "strict" SONET AP. POS APS supporta comandi di configurazione aggiuntivi utilizzati per configurare i parametri di PGP.

Èpossibile utilizzare il comando **aps timers** per modificare il timer hello e il timer di attesa. Il timer hello definisce l'ora tra i pacchetti hello. Il timer di attesa imposta il tempo che deve trascorrere prima che il processo di protezione dell'interfaccia dichiari inattivo il router di un'interfaccia funzionante. Per impostazione predefinita, il tempo di attesa è maggiore o uguale a tre volte il tempo di benvenuto.

L'esempio seguente specifica un tempo hello di due secondi e un tempo di attesa di sei secondi sul circuito 1 sull'interfaccia 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
```

Come mostrato sopra, il comando **aps timers** è stato configurato solo sulle interfacce di protezione.

Èpossibile configurare le interfacce di lavoro e di protezione con tempi di attesa e di consegna univoci. Quando si lavora a contatto con un'interfaccia protetta, usa i valori del timer specificati per l'interfaccia protetta. Quando il lavoro non è a contatto con un'interfaccia di protezione, utilizza i timer per le chiamate in ingresso e in uscita specificati per l'interfaccia di lavoro.

Autenticazione

Un altro comando supportato solo da POS APS è il comando **authentication**, che abilita l'autenticazione tra i processi che controllano le interfacce attive e protette. Utilizzare questo comando per specificare la stringa che deve essere presente per accettare qualsiasi pacchetto su un'interfaccia di protezione o di lavoro. Sono accettati fino a otto caratteri alfanumerici.

Come contattare Cisco TAC

Per assistenza nella risoluzione dei problemi dei punti di accesso, contattare il Cisco Technical Assistance Center (TAC). Raccogliere l'output dai seguenti comandi **show** sui router con le interfacce di protezione e di lavoro:

- **show version**: restituisce la configurazione dell'hardware del sistema e la versione del software. Questo comando visualizza anche i nomi e le origini dei file di configurazione e delle immagini di avvio.
- **show controller pos**: visualizza le informazioni sui controller POS.
- **show ap**: visualizza le informazioni sulla funzione di commutazione della protezione automatica corrente.

Informazioni correlate

- Pagine di supporto per la tecnologia ottica
- Supporto tecnico – Cisco Systems