De betekenis van APS-versies op POS-interfaces

Inhoud

Inleiding

Dit document beschrijft het Protect Group Protocol (PGP), dat een essentieel deel is van Packet over SONET (POS) Automatic Protection Switching (APS) op Cisco-routers en ondernemingswitches.

Voorwaarden

Vereisten

Dit document bevat geen specifieke eisen.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

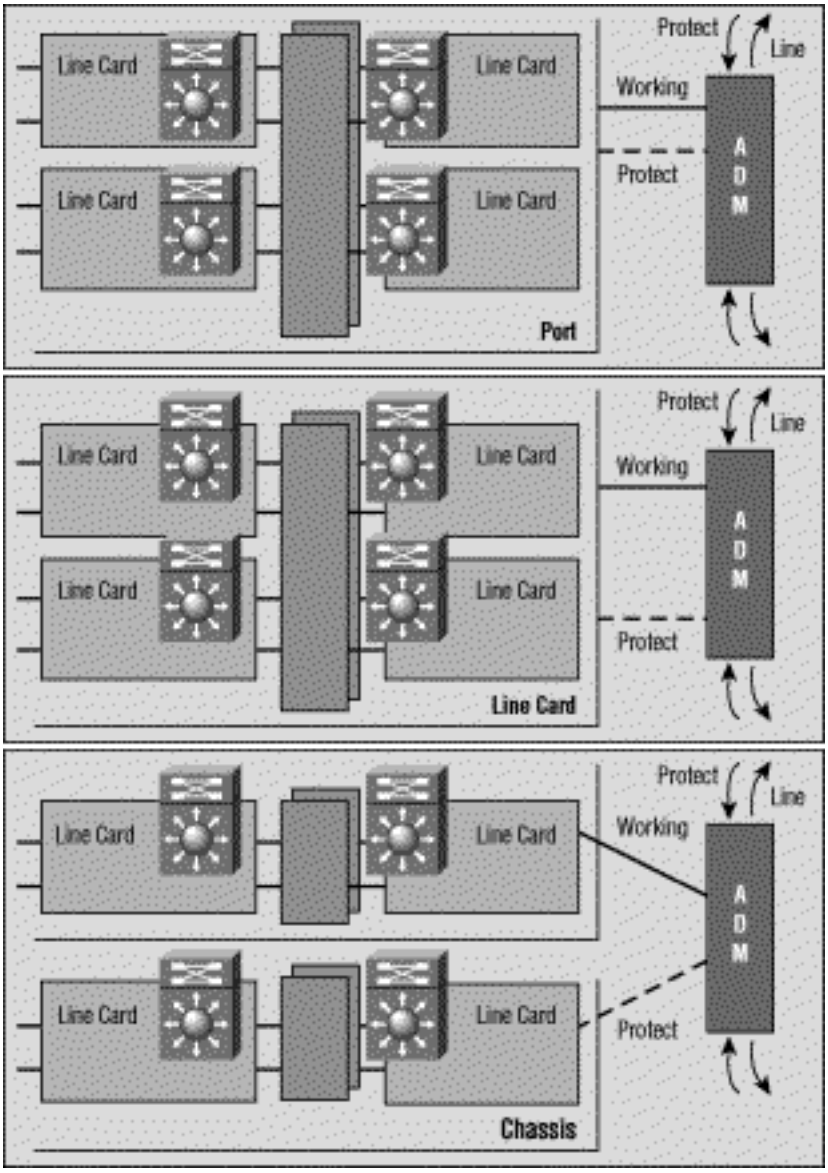
Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

PGP-Overzicht

de publicatie van Bellcore (nu Telcordia) TR-TSY-000253, SONET Transport Systems;

Gemeenschappelijke generieke criteria, paragraaf 5.3, definieert Automatic Protection Switching (APS). Het voor deze optie gebruikte beschermingsmechanisme heeft 1+1, architectuur, waarin een overbodig lijnpaar bestaat uit een werklijn en een beschermingslijn.

In deze illustratie worden mogelijke SONET-beveiligingsconfiguraties weergegeven. U kunt het Cisco POS-beveiligingsprogramma instellen voor situaties waarin security en werkende interfaces verschillende poorten zijn. Deze poorten kunnen op dezelfde router of op dezelfde lijnkaart in dezelfde router zijn. Deze scenario's bieden echter bescherming voor router interface- of verbindingsmislukking. De meeste productieimplementaties hebben werk- en beveiligingsinterfaces op verschillende routers. In zo een twee-router APS configuratie, is een protocol als PGP vereist. PGP definieert het protocol tussen de werknemers en beveiligingsrouters.



PGP-versies

Vanaf Cisco IOS® softwarerelease 12.0(10)S zijn twee versies van PGP beschikbaar. Het werken en beschermen van routers moet dezelfde PGP-versie gebruiken en onderhandelingsberichten uitwisselen via een out-of-band communicatielink. Tijdens onderhandeling, verstuurt de veiligheidsrouter berichten in meerdere PGP versies, het hoogste eerst. De werkrouter negeert hellos met versienummers hoger dan de eigen en antwoordt de anderen. Zodra de werkrouter een hallo bericht beantwoordt, adopteert het dat versienummer, en gebruikt het in alle daaropvolgende

antwoorden.

In huidige Cisco IOS releases hoeven de arbeiders- en beveiligingsrouters niet dezelfde IOS-release te gebruiken. Routers voor werken en beveiligen kunnen daarom onafhankelijk worden bijgewerkt.

Als Cisco IOS-software een fout-match van de versie detecteert, drukt deze log-berichten op deze manier af:

```
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
```

Als deze link verminderde prestaties en hoog pakketverlies ervaart, ontbreekt de APS-versieonderhandeling tussen de arbeiders en de beveiligingsrouters. Als resultaat hiervan, adopteren beide routers "Down-rev" PGP-versies. Het probleem vloeit voort uit gecorrumpeerde onderhandelingsboodschappen. Als de PGP-communicatie-link veel pakketverlies oplevert, kan de werkrouter de groeten niet ontvangen die door de beveiligingsrouter zijn verstuurd met een geadverteerd versienummer. Als dit gebeurt, ziet het alleen het volgende bericht omlaag. Dit scenario veroorzaakt zowel het werken als het beschermen van routers om op het lagere versienummer te vergrendelen. Cisco IOS-softwarerelease 12.0(21)S vermijdt dit probleem door indien nodig onmiddellijk opnieuw te onderhandelen.

Als u een release gebruikt vóór IOS-softwarerelease 12.0(21)S en dit probleem ervaart, gebruikt u deze werkmethode om de normale PGP-versie te herstellen. Doe dit zodra u een betrouwbaar verband tussen de twee routers hebt gelegd:

1. Zorg ervoor dat de werkinterface is geselecteerd. U kunt de **aps force 0** gebruiken om dit te doen.
2. Sluit de beveiligingsinterface. Laat het lang genoeg laag zodat de werkende verklaart dat het communicatie met de beveiligingsinterface heeft verloren.
3. Gebruik de opdracht **no shutdown** op de beveiligingsinterface om de protocolonderhandelingen opnieuw te starten.

PGP-communicatiestoornissen kunnen als gevolg van een van deze problemen optreden:

- Werkrouterstoring
- Bescherm routerfalen
- PGP-kanaalmislukking

PGP-kanaalstoring kan optreden als gevolg van een van deze problemen:

- Verkeerscongestie
- Interface-storing door alarm
- Fout in interface-hardware

U kunt hogere bandbreedte-interfaces voor PGP bieden om congestie te minimaliseren en sommige PGP-kanaalmislukkingen te voorkomen. De werkrouter verwacht *hellos* te ontvangen van de beschermde router elk hallo-interval. Als de werkrouter geen hellos ontvangt voor een tijdsinterval dat gespecificeerd is door het hold-interval, gaat de werkrouter uit van een PGP-

storing en wordt APS geschorst. Op dezelfde manier, als de beschermde router geen hallo nota's van de het werk router ontvangt alvorens de kloktijd verloopt, verklaart het PGP mislukking en kan een omschakeling voorkomen.

Hallo en Hold Timers

POS APS verschilt van "strikte" SONET APS. POS APS ondersteunt extra configuratieopdrachten die gebruikt worden om parameters van PGP te configureren.

U kunt de opdracht **aps timers** gebruiken om de gedag-timer en de timer voor de beelden te wijzigen. De hallo-timer definieert de tijd tussen hallo-pakketten. De timer voor de instellingen van de timer stelt de tijd in voordat het beveiligingsinterfaceproces de router van een werkinterface uitzet. Standaard is de wachttijd groter dan of gelijk aan drie keer de 'hallo'-tijd.

In het volgende voorbeeld wordt een hallo-tijd van twee seconden en een houdtijd van zes seconden gespecificeerd op circuit 1 op POS interface 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
```

Zoals hierboven aangegeven, hebben we de opdracht Taps-timers alleen op de beveiligingsinterfaces ingesteld.

U kunt het werk configureren en interfaces beveiligen met unieke hallo en houdtijden. Wanneer het werken in contact is met een beveiligingsinterface, gebruikt het de timer waarden die voor de beveiligingsinterface zijn gespecificeerd. Wanneer werken niet in contact is met een beveiligingsinterface, gebruikt het de hallo en houten timers die voor de werkinterface zijn opgegeven.

Verificatie

Een andere opdracht die alleen wordt ondersteund door POS APS is de **authenticatie** opdracht, die verificatie mogelijk maakt tussen de processen die de werking besturen en interfaces beveiligen. Gebruik deze opdracht om de string te specificeren die aanwezig moet zijn om pakje te accepteren op een beveiligings- of werkinterface. Tot acht alfanumerieke tekens worden geaccepteerd.

Contact met de Cisco TAC

Als u assistentie nodig hebt bij het oplossen van APS, neem dan contact op met het Cisco Technical Assistance Center (TAC). Verzamel uitvoer van de volgende **tonen** opdrachten op de routers met de beveiliging en werkinterfaces:

- **toon versie** - Hiermee geeft u de configuratie van de systeemhardware en de softwareversie weer. Deze opdracht geeft ook de namen en bronnen van configuratiebestanden en de laarsbeelden weer.

- **controller pos** - Hiermee geeft u informatie weer over de POS-controllers.
- **toont aps** - Informatie over de huidige automatische bescherming switching-functie.

Gerelateerde informatie

- Optische steunpagina's voor technologie
- Technische ondersteuning - Cisco-systemen