APS-Versionen auf POS-Schnittstellen

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Konventionen](#)
[PGP - Übersicht](#)
[PGP-Versionen](#)
[Hello- und Hold-Timer](#)
[Authentifizierung](#)
[Kontaktaufnahme mit dem Cisco TAC](#)
[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird das Protect Group Protocol (PGP) beschrieben, das eine zentrale Komponente von Packet Over SONET (POS) Automatic Protection Switching (APS) auf Cisco Routern und Enterprise Switches darstellt.

Voraussetzungen

Anforderungen

Dieses Dokument enthält keine spezifischen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

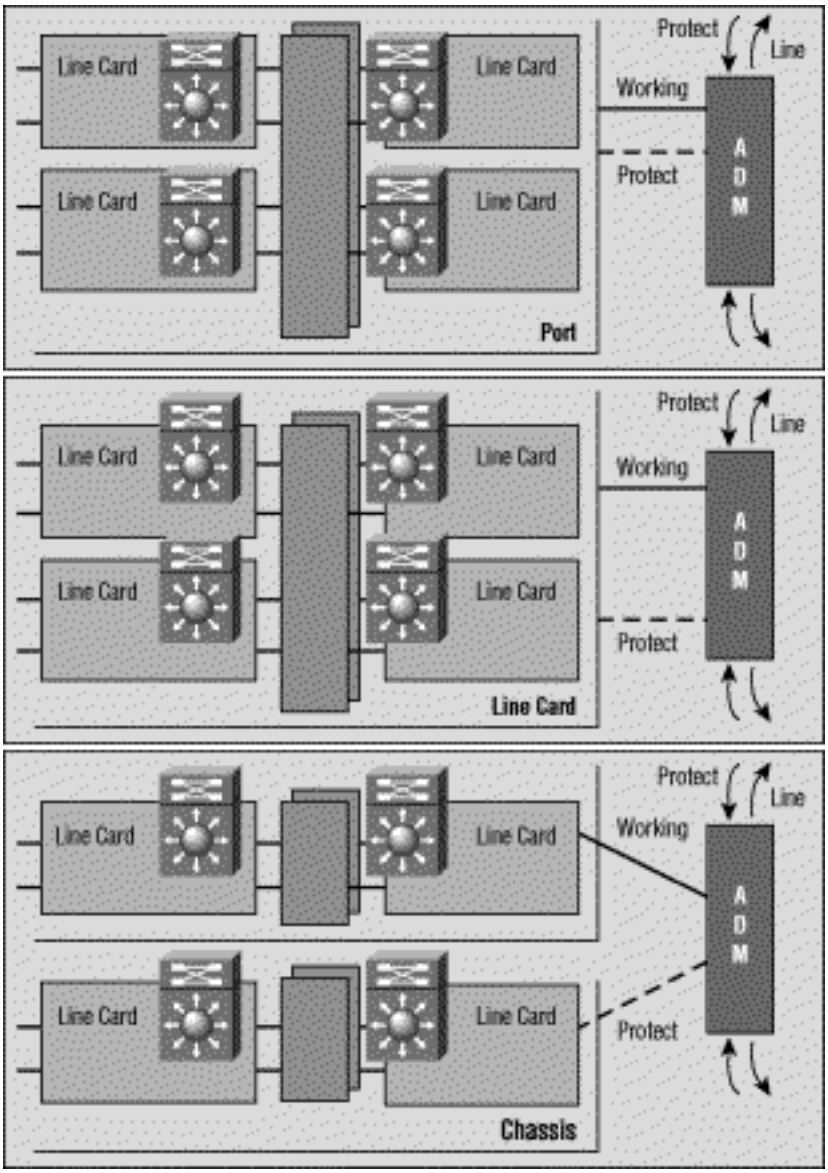
Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

PGP - Übersicht

Bellcore (jetzt Telcordia) veröffentlicht TR-TSY-00253, SONET Transport Systems; Common Generic Criteria, Abschnitt 5.3, definiert Automatic Protection Switching (APS). Der für diese Funktion verwendete Schutzmechanismus hat eine 1+1-Architektur, in der ein redundantes

Leitungspaar aus einer Arbeitsleitung und einer Schutzleitung besteht.

Diese Abbildung zeigt mögliche SONET-Schutzkonfigurationen. Sie können das Cisco POS-Schutzschema für Situationen einrichten, in denen sich Schutz- und Arbeitsschnittstellen auf unterschiedlichen Ports befinden. Diese Ports können sich auf demselben Router oder auf derselben Linecard im selben Router befinden. Diese Szenarien bieten jedoch Schutz für Router-Schnittstellen oder Verbindungsausfälle. Die meisten Produktionsbereitstellungen verfügen über funktionierende und geschützte Schnittstellen auf verschiedenen Routern. Bei einer solchen APS-Konfiguration mit zwei Routern ist ein Protokoll wie PGP erforderlich. PGP definiert das Protokoll zwischen den aktiven Routern und den geschützten Routern.



PGP-Versionen

Ab der Cisco IOS® Softwareversion 12.0(10)S sind zwei Versionen von PGP verfügbar. Die Netzwerk- und Protect-Router müssen dieselbe PGP-Version verwenden und über eine Out-of-Band-Kommunikationsverbindung Verhandlungsnachrichten austauschen. Während der Aushandlung sendet der Protect-Router Meldungen in mehreren PGP-Versionen, die höchste Priorität haben. Der funktionierende Router ignoriert Hellos mit höheren Versionsnummern als die eigenen und antwortet auf die anderen. Sobald der funktionierende Router eine Hello-Nachricht beantwortet hat, übernimmt er diese Versionsnummer und verwendet sie in allen nachfolgenden Antworten.

In aktuellen Cisco IOS-Versionen müssen die Router für Arbeit und Schutz nicht dieselbe IOS-Version ausführen. Die Arbeits- und Schutzrouter können daher unabhängig aktualisiert werden.

Wenn die Cisco IOS-Software eine Versionskonflikt erkennt, werden Protokollmeldungen ähnlich der folgenden ausgegeben:

```
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
```

Wenn bei dieser Verbindung die Leistung beeinträchtigt und ein hoher Paketverlust auftritt, schlägt die APS-Versionsaushandlung zwischen den funktionierenden Routern und den Schutzroutern fehl. Daher verwenden beide Router "Downrev"-PGP-Versionen. Das Problem resultiert aus beschädigten Verhandlungsnachrichten. Wenn bei der PGP-Kommunikationsverbindung ein hoher Paketverlust auftritt, kann der funktionierende Router das vom Protect-Router gesendete Hello mit einer angegebenen Versionsnummer verpassen. In diesem Fall wird möglicherweise nur die nachfolgende Downrev-Meldung angezeigt. Dieses Szenario bewirkt, dass sowohl die funktionierenden als auch die geschützten Router an der unteren Versionsnummer festgehalten werden. Cisco IOS Software Release 12.0(21)S vermeidet dieses Problem, indem es bei Bedarf direkt verhandelt.

Wenn Sie eine Version verwenden, die älter als die IOS-Softwareversion 12.0(21)S ist und dieses Problem auftritt, verwenden Sie diese Problemumgehung, um die normale PGP-Version wiederherzustellen. Führen Sie diese Schritte aus, sobald eine zuverlässige Verbindung zwischen den beiden Routern hergestellt wurde:

1. Stellen Sie sicher, dass die funktionierende Schnittstelle ausgewählt ist. Sie können dazu den Befehl **aps force 0** verwenden.
2. Schließen Sie die Schutzschnittstelle. Lassen Sie es so lange ausfallen, dass der funktionierende erklärt, dass er die Kommunikation mit der Schutzschnittstelle verloren hat.
3. Verwenden Sie den Befehl **no shutdown** auf der Protect-Schnittstelle, um Protokollverhandlungen neu zu starten.

PGP-Kommunikationsfehler können aufgrund eines der folgenden Probleme auftreten:

- Fehler beim funktionierenden Router
- Schutz von Router-Fehlern
- PGP-Kanalfehler

Ein PGP-Kanalausfall kann aufgrund eines der folgenden Probleme auftreten:

- Verkehrsstaus
- Schnittstellenfehler aufgrund von Alarmen
- Schnittstellenhardwarefehler

Sie können Schnittstellen mit höherer Bandbreite für PGP bereitstellen, um Überlastungen zu minimieren und PGP-Kanalausfälle zu vermeiden. Der funktionierende Router erwartet in jedem Hello-Intervall *Hellos* vom Protect-Router. Wenn der funktionierende Router während eines durch das Halteintervall festgelegten Zeitraums keine Hellos empfängt, geht der funktionierende Router von einem PGP-Ausfall aus, und der APS wird ausgesetzt. Wenn der Protect-Router keine Hello-

Bestätigungen vom funktionierenden Router empfängt, bevor der Hold-Intervall-Timer abläuft, deklariert er PGP-Fehler und es kann zu einem Switchover kommen.

Hello- und Hold-Timer

POS APS unterscheidet sich von "strikten" SONET APS. POS APS unterstützt zusätzliche Konfigurationsbefehle zum Konfigurieren von PGP-Parametern.

Sie können den Befehl **aps timers** verwenden, um den Hello-Timer und den Hold-Timer zu ändern. Der Hello-Timer definiert die Zeit zwischen Hello-Paketen. Der Hold-Timer legt die Zeit fest, bevor der Prozess der Protect-Schnittstelle erklärt, dass der Router einer funktionierenden Schnittstelle ausgefallen ist. Standardmäßig ist die Haltezeit größer oder gleich dreimal so hoch wie die Hello-Zeit.

Im folgenden Beispiel wird eine Hello-Zeit von zwei Sekunden und eine Haltezeit von sechs Sekunden auf Circuit 1 an der POS-Schnittstelle 5/0/0 angegeben:

```
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
```

Wie oben gezeigt, wurde der Befehl **aps timers** nur auf den Protect-Schnittstellen konfiguriert.

Sie können die Arbeits- und Schutzschnittstellen mit eindeutigen Hello- und Haltezeiten konfigurieren. Wenn die Arbeit mit einer Schutzschnittstelle in Berührung kommt, werden die für die Schutzschnittstelle angegebenen Timer-Werte verwendet. Wenn bei der Arbeit keine Schutzschnittstelle verwendet wird, werden die Hello- und Hold-Timer verwendet, die für die Arbeitsschnittstelle angegeben sind.

Authentifizierung

Ein weiterer nur von POS APS unterstützter Befehl ist der **Authentifizierungsbefehl**, der die Authentifizierung zwischen den Prozessen ermöglicht, die die Arbeits- und Schutzschnittstellen steuern. Verwenden Sie diesen Befehl, um die Zeichenfolge anzugeben, die vorhanden sein muss, um ein beliebiges Paket auf einer Schutz- oder Arbeitsschnittstelle zu akzeptieren. Es werden bis zu acht alphanumerische Zeichen akzeptiert.

Kontaktaufnahme mit dem Cisco TAC

Wenn Sie Hilfe bei der Fehlerbehebung von APS benötigen, wenden Sie sich an das Cisco Technical Assistance Center (TAC). Sammeln Sie die Ausgabe der folgenden **show**-Befehle auf den Routern mit den Schutz- und Arbeitsschnittstellen:

- **show version**: Zeigt die Konfiguration der Systemhardware und die Softwareversion an. Mit diesem Befehl werden auch die Namen und Quellen der Konfigurationsdateien sowie die Boot-Images angezeigt.
- **show controller pos**: Zeigt Informationen über die POS-Controller an.

- **Anzeigen von aps** - Zeigt Informationen über die aktuelle automatische Schutzschalter-Umschaltfunktion an.

Zugehörige Informationen

- Support-Seiten für optische Technologie
- Technischer Support - Cisco Systems