SONET-Trigger

Inhalt

Einführung

Ein Trigger ist ein Ereignis, das die Rolle der *Ursache* in der Ursache-Wirkung-Beziehung in einer SONET-Schnittstelle (Synchronous Optical Network) in IOS erfüllt. Manchmal können Sie den Befehl **POS-Verzögerungs-Trigger** verwenden. In anderen Fällen empfiehlt Cisco, den Befehl **POS-Verzögerungs-Trigger** nicht zu verwenden, insbesondere wenn Sie versuchen, strenge Service Level Agreements (SLAs) zu erfüllen. Service Provider verkaufen differenzierte Service Level basierend auf bestimmten Vereinbarungen. Die Vereinbarungen betreffen die interne Weiterleitung, den Schutz oder die Priorisierung des Kundendatenverkehrs durch das Netzwerk. Mithilfe dieser Befehle können Anbieter Netzwerke so konfigurieren, dass sie die Service-Vereinbarungen erfüllen.

In diesem Dokument werden die Trigger für Schnittstellenaktivierungs- und -

abschaltungsereignisse untersucht. In diesem Dokument wird auch die Bereitstellung von Packet Over SONET (POS) erläutert. Darüber hinaus werden SLAs und Konvergenzzeiten auf Layer 3 berücksichtigt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Ereignisse, die eine POS-Schnittstelle auslösen

In diesem Abschnitt werden die Ereignisse beschrieben, durch die eine POS-Schnittstelle deaktiviert wird, und die zugehörigen Befehle aufgeführt.

Abschnitt- und Leitungsebenen-Trigger

Die Liste der Trigger in diesem Abschnitt bezieht sich auf die *SONET-Transportsysteme* GR-253-CORE*: Allgemeine* Spezifikation *allgemeiner Kriterien*:

- Section Loss of Signal (SLOS) (Signalverlust (SLOS)): Die Spezifikation gibt an, dass mindestens 2,5 us und höchstens 100 us (6.2.1.1.1) erkannt werden müssen.
- Section Loss of Frame (SLOF) (Abschnitt-Verlust von Rahmen (SLOF)): Die Spezifikation gibt an, dass Sie dies in mindestens 3 ms (oder 24 aufeinander folgenden fehlerhaften Framing-Pattern) erkennen müssen (6.2.1.1.2).
- Alarm Indication Signal - Line (AIS-L) - AIS-L muss ggf. innerhalb von 125 ms nach der Erkennung ausgesendet werden. Ein Gerät muss den Empfang von AIS-L erkennen, wenn das Gerät 5 aufeinander folgende Frames erkennt, wobei die Bits 6,7 und 8 von K2 auf 111 (6.2.1.2.1) festgelegt sind.
- SD-BER (Signal Degrade Bit Error Rate) - SD-BER ist ein Auslöser nur für Schnittstellen mit Automatic Protection Switching (APS) (gebunden an die B2 BER-Berechnung).
- Signal Failure Bit Error Rate (SF-BER) - SF-BER ist ein Auslöser für APS- und Nicht-APS-Schnittstellen (gebunden an die B2-BER-Berechnung).
- Remote Defect Indication - Line (RDI-L) - RDI-L ist kein Auslöser für POS oder APS. (RDI-L

ist jedoch ein Auslöser für MPLS FRR) (Abschnitt 5.3.3.1).

Weitere Informationen zu den in dieser Liste erwähnten Abschnitten finden Sie auf der Telcordia Information SuperStore Website.

Zugehörige Befehle

Die **PoS-Verzögerung löst für n ms** den Befehl **line *n* aus, der LOS/LOF/AIS sperrt, bevor der Befehl die Leitung auslöst:**

Wenn Sie den Befehl ohne numerischen Wert konfigurieren, beträgt die Verzögerungszeit standardmäßig 100 ms. Sie können Line-Trigger für alle POS-Schnittstellen verwenden, die keine APS-Ports sind. Sie können Line-Trigger nicht für Schnittstellen verwenden, die am APS teilnehmen, da Line-Trigger den APS-Betrieb stören. Der Befehl **POS-Delay-Trigger *n* ermöglicht** nicht, dass die Leitung auf den kurzen LOS, der von einem intern geschützten Dense Wavelength-Division Multiplexing (DWDM)-Gang stammt, abgeschaltet wird, sobald ein interner DWDM-Schutzschalter auftritt. Wenn der Defekt während der Holdoff-Zeit auftritt, ist es so, als wäre der Fehler nie aufgetreten.

Die **PoS-Verzögerung löst den Befehl line** (**line**) aus, der jede Aktion aufgrund des Fehlers auslöst (außer den Zähler für Fehler zu erhöhen), bis die angegebene Holdoff-Periode endet.

Wenn Sie diesen Befehl nicht aktivieren, werden APS und Link Down von den oben genannten SONET-Fehlern sofort im Route Processor (RP) ausgelöst.

Pfad-Trigger

Diese spezifischen PATH-Level-Defekte initiieren eine Statusänderung nur, wenn Sie **PoS-Verzögerung** aktiviert haben**, um** den **Pfad** der Schnittstelle **auszulösen**:

- AIS-P - Dieser Fehler muss innerhalb von 125 ms nach der Erkennung des Fehlers, der zum AIS-P führt, ausgelöst werden. Der Path Terminating Equipment (PTE) muss diesen Fehler erkennen, wenn die H1- und H2-Byte für einen STS-Pfad alle 1s für drei aufeinander folgende Frames enthalten. Konkordierte Pfade müssen nur die ersten H1- und H2-Byte beobachten. Weitere Informationen finden Sie in Abschnitt 6.2.1.2.2 von R6-175 und R6-176.
- RDI-P: Wenn RDI-P vorhanden ist, muss der Fehler innerhalb von 10 Frames erkannt werden. Siehe 6.2.1.3.2 von R6-221.
- B3-TCA (Schwellenwert-Crossing-Alarme) für B3 - Dieser Alarm ist an die Berechnung der B3 Binary Synchronous Communications (Bisync) IP (BIP) gebunden.
- LOP-P (Path Loss of Pointer) (wenn die IOS-Version CSCdx58021 enthält) - Siehe Abschnitt 6.2.1.1.3 von GR-253.

Weitere Informationen zu den in dieser Liste erwähnten Abschnitten finden Sie auf der Telcordia Information SuperStore Website.

Related-Befehl

Der **PoS-Delay-Befehl löst Pfade *<msec>*** aktiviert das Link-Down-Triggering bei AIS-P-, RDI-P- und exzessiven B3-Fehlern. Standardmäßig ist das Link-Down-Triggering für Pfadfehler deaktiviert.

Der Befehl gibt auch eine Haltezeit zwischen 0 und 511 ms an (der Standardwert ist 100 ms).

Pfadauslösungsfehler (AIS-P, RDI-P), die vor dem Ende der Haltephase behoben werden, führen nicht zu Auslösen. Wenn Sie diesen Befehl nicht explizit auf einer POS-Schnittstelle konfiguriert haben, werden bei Verarbeitung der PATH-Level-Fehler keine Aktionen ausgeführt. Im Gegensatz zu den Line-Triggern lassen APS-Schnittstellen Pfadauslöser zu, da Path-Trigger die Aktivität von APS auf Postenebene nicht beeinträchtigen. Path-Trigger konnten in Versionen vor Cisco IOS® Software Release 12.0(28)S nicht mit APS konfiguriert werden. Es wurden Pfadauslöser hinzugefügt, um das Auf-/Abwärtsverhalten der POS-Schnittstellen bei der Verbindung mit SONET-Netzwerken zu beschleunigen. Dies ermöglichte eine schnellere Layer-3-Konvergenz bei Remote-Fehlern.

Zusammenfassung des CLI-Verhaltens der POS-Trigger

In dieser Tabelle sind die POS-Trigger-Bedingungen und die zugehörigen Ergebnisse aufgeführt:

Bedingung	Ergebnis
Wenn Sie keine explizite Beziehung zu POS-Triggern konfiguriert haben.	Auslöser auf Postenebene werden sofort verarbeitet.
Wenn Sie den Befehl **POS-Verzögerung** konfiguriert haben**, löst dies den** Befehl **line aus**.	Auslöser auf Postenebene werden nach einer Verzögerung von 100 ms verarbeitet.
Wenn Sie den Befehl **POS-Verzögerung** konfiguriert haben**, löst dies den Befehl line *x* aus**.	Auslöser auf Postenebene werden nach *x* msecs verarbeitet, wobei *x* zwischen 0 und 511 liegt.
Wenn Sie keine explizite Beziehung zu Path-Triggern konfiguriert haben.	Pfadauslöser werden nicht verarbeitet, und es werden keine Maßnahmen ergriffen.
Wenn Sie den Befehl **POS-Verzögerung** konfiguriert haben**, löst er den** Befehl **path aus**.	Auslöser auf Pfadebene werden nach einer Verzögerung von 100 ms verarbeitet.
Wenn Sie den Befehl **pos delay** konfiguriert haben**, löst der Befehl path *x* aus**.	Auslöser auf Pfadebene werden nach *x* msecs verarbeitet, wobei *x* zwischen 0 und 511 liegt.

Debouncing von SONET-Alarmen

SONET-Alarme, die aus Defekten resultieren, werden 10 Sekunden (10.5 +-.5) nach Beseitigung des Mangels gehalten.

Handhabung von Fehlern

In IOS ändern die POS-Karten ihren LINE-Status aufgrund verschiedener Trigger über zwei allgemeine Methoden zur Fehlerbearbeitung. Dies hängt zwar von der spezifischen Konfiguration der Schnittstelle ab (APS oder Nicht-APS), im Allgemeinen gibt es jedoch zwei Arten von

Ausfällen:

- Verwaltete
- Nicht verwaltet

Sie müssen die in diesem Dokument verwendeten Begriffe zur Handhabung von Warnmeldungen verstehen:

- Defect (Fehler): Der Fehlerzustand, der von der Hardware erkannt wird.
- Failure (Fehler): Ein Fehler, der für die erforderlichen ~2,5 Sekunden abgefangen wurde und dann über die SONET-4-ALARM-Nachrichten gemeldet wird. Ein Defekt, der einen Auslöser darstellt, wird nicht eingetrocknet.
- Unmanaged Failure (Nicht verwaltete Fehler): Ereignisse wie LOS, LOF usw. werden vom SONET-Framer durch einen definierten Satz von Parametern erkannt und müssen nicht berechnet werden. Es liegt entweder ein Fehler vor, der durch die Hardware geltend gemacht wird, oder es liegt kein Fehler vor. Hard Failure wie diese werden im Allgemeinen durch Interrupts gehandhabt. LOS, LOF, AIS-L und in Sonderfällen AIS-P und RDI-P werden sofort geltend gemacht. Diese sind abhängig vom Framer und den definierten Regeln, um diese Fehler zu erkennen. Diese Fehler wirken sich sofort aus. Sie können den Router jedoch anweisen, die Geltendmachung dieses Fehlers als Fehler zu verzögern. Es gibt zwei Timer, die den Verzögerungswert bestimmen, **POS-Verzögerungsauslöse [path | Leitung]** und Carrier-Verzögerung. Diese werden später im Dokument behandelt.
- Verwaltete Alarme - Ereignisse wie TCAs und SD/SF-BER-Berechnungen. Diese erfordern eine gewisse Berechnung, um festzustellen, ob sie vorhanden sind, sich im Anstieg oder im Rückgang befinden usw. Zum Beispiel kann es kein LOS geben, das seine "LOS-ness" aus Sicht des Routers erhöht. Sie können jedoch eine BER-Obergrenze festlegen, die entweder steigt oder abnimmt; die getroffenen Maßnahmen können unterschiedlich sein. Weiche Fehler wie BER und TCA müssen berechnet werden, da sie von einer Reihe von Faktoren abhängen, z. B. von Schwellenwerten, die ein Benutzer konfigurieren kann, Bitrate und der maximalen Anzahl von IP-Übertragungen (CVs) (da sie sich für B1, B2 und B3 unterscheiden). Diese Ausfälle dauern auch länger, da die Hardware für die Grenzkontrollstellen abgefragt wird, und auch, weil diese Art von Fehlern allmählich auftreten und sich im Laufe der Zeit anhäufen. Es ist auch richtig, dass Sie im Allgemeinen nicht von 0-IP-Adresse direkt zu einer Signalherabstufung (SD) oder einem Signalfehler (SF) wechseln, ohne dass eine andere Art von schwerwiegenden Ausfällen im Netzwerk vorliegt. Diese Defekte treten im Vergleich zu den schweren Ausfällen langsamer auf.

Im Folgenden wird ein allgemeiner Ansatz für grundlegende Berechnungen beschrieben, der die Berechnung der BER beschreibt:

Nach jedem Neustart der Berechnungen und bis BER_Period Required_BER_Period erreicht (das Integrationsfenster ist nicht vollständig bereitgestellt), fungiert der Algorithmus als integrierter bzw. durchschnittlicher Wert:

- BER_Period = BER_Period + 1 Sek.
- Current_IP_IP = Current_BIP + BIP_new.
- Current_BER = Current_BIP/BER_Period.

Nachdem BER_Period Required_BER_Period erreicht hat (das Integrationsfenster wurde vollständig bereitgestellt und beginnt, zu schieben), funktioniert der Algorithmus als undichte Zelle eins:

- BER_Period = Required_BER_Period.
- Current_IP_IP = Current_IP_IP + IP_new - Current_BER * 1 sec.
- Current_BER = Current_BIP/BER_Period.

Der Required_BER_Period wird anhand der Leitungsrate und des konfigurierten BER-Schwellenwerts ermittelt, die den Standards entsprechen (siehe Abbildung 5-5, Switch Initiation Time Criteria, GR-253). Sie ist jedoch auf eine Sekunde begrenzt, unsere Abtastrate.

Somit wird bei jeder Umfrage das BER_Period (Integrationsfenster) verschoben, und bei jeder Umfrage wird eine neue BER berechnet. Wenn Current_BER jemals über einen festgelegten Grenzwert hinausgeht, wird der entsprechende Fehler sofort im gleichen Umfrage- oder Berechnungsintervall ausgelöst, und die Antwort wird minimal gehalten. Wir wiederholen diese Berechnungen jede Sekunde und prüfen, ob eines der drei Ereignisse aufgetreten ist:

- Die BER fällt immer noch in denselben Bereich. Es gibt keine neuen Maßnahmen.
- Die BER ist wieder gestiegen und hat einen SD- oder SF-Schwellenwert (für B2) überschritten. Melden Sie einen neuen Alarm an.
- Die GVO ist unter einen GVO-Grenzwert gefallen. Löschen Sie den Alarm.

Für die Assertion einer TCA oder SD/SF müssen Sie nur warten, bis Sie in diesem entsprechenden Polling-Intervall eine Grenze überschritten haben. Überprüfen Sie zum Zeitpunkt der Berechnung, ob die Current_BER einen Grenzwert überschritten hat, und wenn dies der Fall ist, können Sie den Alarm sofort per Software bestätigen.

Dies ist gültig, weil, wenn die Current_BER groß genug ist, um den Alarm zunächst auszulösen, die Bedingung am Ende der BER_Period immer noch wahr ist. Dies basiert darauf, wie die Werte definiert und im Verhältnis zum Berechnungsfenster verglichen werden.

Wenn Sie einen Alarm löschen, müssen Sie bis zum Ende des Berechnungsfensters BER_Period warten. Dadurch wird sichergestellt, dass im letzten Teil des Fensters keine neuen Grenzkontrollstellen angesammelt werden, die einen Schwellenwert überschreiten könnten.

Hinweis: Laut GR-253 sind sowohl SD-BER als auch SF-BER eng an die B2-Grenzkontrollstelle gebunden. Die aktuellen Standardschwellenwerte sind:

- BER-Schwellenwerte - SF = 10e-3 SD = 10e-6
- TCA-Schwellenwerte - B1 = 10e-6 B2 = 10e-6 B3 = 10e-6

Hinweis: Engine2 OC-48-Karten haben folgende Standardschwellenwerte:

- BER-Schwellenwerte - SF = 10e-4 SD = 10e-6
- TCA-Schwellenwerte - B1 = 10e-6 B2 = 10e-6 B3 = 10e-6

Wenn Sie möchten, dass der B3-TCA-Pfad-Trigger ähnlich wie SF aussieht, muss der B3-Grenzwert auf den gleichen Grenzwert (10e-3) festgelegt werden. Sie können dies über den Befehl **poS threshold b3-tca 3** an der Eingabeaufforderung `router(config-if)#` tun.

Hinweis: Da das Abfrageintervall eine Sekunde beträgt, wird der TCA- oder SD/SF-Fehler erst nach einer Mindestzeit erkannt und ausgelöst. Aufgrund der kumulierten Anzahl von TCA/SD/SF treten bei diesen Ausfällen auch bei typischen Ausfällen schnell andere Ausfälle auf. Dadurch wird ein Gleichgewicht zwischen der Prozessorauslastung des Routers und der Leistung aufrechterhalten. Das Abfrageintervall kann nicht konfiguriert werden.

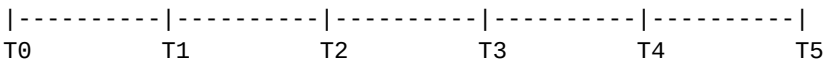
Auslöser in Aktion

Dieser Abschnitt enthält Hintergrundinformationen zur Untersuchung der Interaktion einiger benutzerdefinierbarer Tasten in IOS:

Die **PoS-Verzögerungsauslöse [Leitung | path]** Befehl verzögert die Meldung und Aktion eines Fehlers kurz.

Die POS-Verzögerungsleitung ist die Haltezeit, bevor auf einen Leitungsalarm reagiert wird. Der Standardwert ist eine sofortige Reaktion, d. h. **POS-Verzögerungsauslöser Leitung *0*.** Wenn Sie die **POS-Verzögerungsleitung** ohne Wert direkt konfigurieren, wird der Standardwert von 100 ms berücksichtigt. Dies ermöglicht eine sofortige oder verzögerte Reaktion, basierend auf dem gewünschten Effekt. Bei einer dieser Konfigurationen wird der Fehler erst dann als aktiver Alarm angezeigt, wenn der Holdoff-Zeitraum abgelaufen ist.

Zeitplan:



Hier:

- t0 - Zeit, zu der der Fehler auftritt.
- t1 - Zeit, zu der die Hardware den Fehler erkennt.
- t2 - Zeit, zu der der Fehler als Fehler gemeldet wird.
- t2-t3: Zeit, die für konfigurierte Trigger abgehalten wird.
- t3-t4: Zeit, für die Sie aufgrund einer Carrier-Verzögerung warten.
- t4 - Zeit, zu der die Schnittstelle in IOS tatsächlich ausfällt.
- t5: Zeit, zu der eine beliebige Adjacency für ein Routing-Protokoll ausfällt.

Untersuchen Sie die Zeitleiste, um zu beobachten, wie die verschiedenen Knöpfe zu verschiedenen Ergebnissen zu erreichen.

Der Befehl **post delay löggers** beeinflusst die Dauer zwischen t2 und t3 und verbirgt den Fehler in der Tat vor IOS, bis der Holdoff-Zeitraum abgelaufen ist. Natürlich, wenn der Fehler beseitigt wird, bevor Sie zu erreichen t3, nichts passiert, und es ist, als wäre nichts passiert. Der Standardwert für Line- und Path-Trigger beträgt 100 ms, der Bereich liegt zwischen 0 und 511 ms. Pfadauslöser sind nicht aktiviert (d. h. sie ergreifen keine Maßnahmen), es sei denn, der **Pfad für** die **POS-Verzögerung** wird zuerst konfiguriert. **POS-Verzögerungsauslösungspfad** ist die Haltezeit, bevor auf einen Pfadalarm reagiert wird. Der Standardwert ist keine Reaktion. Wenn Sie den **POS-Verzögerungspfad** direkt ohne Wert konfigurieren, wird der Standardwert 100 ms automatisch zugewiesen. Dazu gehören AIS-P, RDI-P und B3-TCA. Diese Funktionalität wurde durch CSCds82814 (ca. 12.0(15.5)S/ST) hinzugefügt.

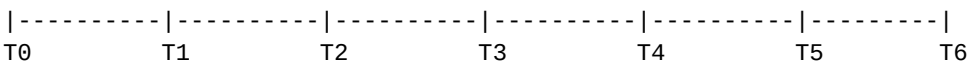
"Carrier-Delay" ist die Haltezeit zwischen dem Ende der POS-Verzögerungszeit und dem Herunterfahren der IOS-Schnittstelle. Der Standardwert ist 2000 ms. Die Carrier-Verzögerung ist die Zeit zwischen t3 (wenn IOS einen Fehler erkennt) und t4 (wenn die Schnittstelle ausfällt). Standardmäßig ist dieser Wert auf 2 Sekunden festgelegt und kann für msec-Werte konfiguriert werden. Wie die Zeitleiste anzeigt, handelt es sich um eine Zusatzfunktion neben den SONET-Pegel-Holdoff-Timern. Es verhält sich genauso wie die POS-Trigger - wenn der Alarm vor Ende der Holdoff-Periode gelöscht wird, wird die Schnittstelle nicht deaktiviert. Allerdings gibt es hier ein Dilemma. Der SONET-Debouncing-Timer löscht den Fehler nicht, bevor die Carrier-Verzögerung aktiviert wird, es sei denn, die Carrier-Verzögerung ist groß (weit über 10 Sekunden). Dies führt zu einer Situation, in der die Carrier-Verzögerung fast immer aktiviert wird und daher bei

Bereitstellung mit PoS-Schnittstellen als relativ klein angesehen werden muss. Die Carrier-Verzögerung wird ebenfalls hinzugefügt, nachdem der Alarm gelöscht wurde, bevor die Schnittstelle ebenfalls deklariert wird. Daher können Sie den Wert der Carrier-Verzögerung zweimal zählen, bevor die Schnittstelle wieder verfügbar ist.

Bei einigen Schnittstellen und physischen Medien ist dies hilfreich. Bei POS-Schnittstellen gibt es jedoch eine Reihe von Triggern und Timern, die Sie verwenden können, und kombiniert, um den gewünschten Effekt zu erzielen, ohne Carrier-Verzögerung eine solche wichtige Rolle zu übernehmen. Ein Carrier Delay-Wert von 0-8 ms ist ein guter Ausgangspunkt für Kunden, die diese Knöpfe selbst testen möchten. Im Allgemeinen ist eine gute Strategie, den Befehl **POS-Verzögerungs-Trigger** zu verwenden, um alle Probleme zu absorbieren und den gewünschten Holdoff-Effekt bereitzustellen. Die Carrier-Verzögerung kann gering gehalten werden, um die Auswirkungen zu minimieren.

Der oben erwähnte SONET-Debounce-Timer wird auf 10 Sekunden (+/- 0,5 Sekunden) eingestellt und ist für GR-253 erforderlich, um sicherzustellen, dass ein Flapping-Zeitraum von weniger als 10 Sekunden nicht eintritt. Der Timer beginnt, nachdem der Fehler gelöscht wurde. Der Timer wird zurückgesetzt, wenn ein anderes Defektereignis auftritt, bevor das Zeitgeberfenster abgelaufen ist.

Zeitplan:



Hier:

- t0: Defect wird gelöscht.
- t0 - Debounce-Timer wird gestartet.
- t4 - t0 + 10sec (daher muss der Fehler klar sein, wenn zwischen t0 und t4 keine neuen Fehler auftreten).

Wenn ein Ereignis vor t4 (sagen Sie) bei t2 auftritt (dies kann ein weiterer Fehler oder ein Wiederauftreten desselben Fehlertyps sein), wird der Zeitgeber angehalten, bis dieser neue Fehler gelöscht wird. Bei t3 startet der Timer erneut, wenn keine aktiven Fehler vorliegen, und zählt für die ~10 Sekunden. Wenn keine neuen Ereignisse aufgetreten sind, löschen Sie den Alarm bei t5, und starten Sie dann den Carrier Delay Timer. Wenn die Carrier-Verzögerung bei t6 gelöscht wurde, rufen Sie die Schnittstelle erneut auf.

Anhand dieser Informationen sollte der Kunde besser verstehen können, wie die POS-Schnittstellen auf verschiedene SONET/SDH-Bedingungen reagieren. Dadurch kann das Gerät genauer entsprechend dem vom Kunden beabsichtigten Verhalten konfiguriert werden.

Warum Trigger verwenden?

In diesem Abschnitt wird erläutert, wann Sie die **POS-Verzögerungs-Trigger** verwenden müssen **[line | path]**, und wenn Sie es nicht verwenden dürfen.

Hier sind die Szenarien, in denen Sie keine **POS-Verzögerungsauslöser** verwenden dürfen. Es gibt mehrere Szenarien:

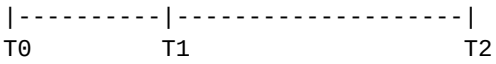
- Sie können keine Line Trigger für APS-konfigurierte Schnittstellen verwenden. Versionen vor der Cisco IOS Software, Version 12.0(28)S, boten nicht einmal die Verwendung von Path-Triggern.
- Wenn Sie explizit nicht möchten, dass PATH-Level-Defekte die Schnittstelle deaktivieren, können Sie diese Trigger nicht verwenden.
- Wenn Sie möchten, dass Auslöser auf Postenebene die Schnittstelle ohne Verzögerung deaktivieren, können Sie diesen Befehl nicht verwenden.

Im Folgenden sind die Szenarien aufgeführt, in denen Sie den Befehl **POS-Verzögerungsauslöser** verwenden können:

- Wenn Sie die Wirkung eines Defekts auf der Postenebene vorübergehend abhalten möchten.
- Damit PATH-Level-Defekte die Schnittstelle sofort deaktivieren können.
- Um PATH-Level-Defekte zu aktivieren, wird die Schnittstelle deaktiviert, aber einige Holdoff-Elemente sind enthalten.

SLAs und POS-Trigger

In diesem Zeitrahmen erfahren Sie:



- Time t=0 (t0): Wenn der Fehler erkannt wird.
- Zeit t2 - Die erforderliche SLA-Wiederherstellungszeit.
- Time t1 (Zeit t1): Alle Holdoff-Meldungen aus der **POS-Verzögerung lösen den** konfigurierten Befehl aus (der Standardwert für LINE ist 0 und der Standardwert für PATH ist nicht aktiviert).
- X ist der Holdoff-Wert (also X = der Wert von t1).
- Y ist die Zeit, die für die Wiederherstellung des Service auf Layer 3 benötigt wird.

Theorem

Manchmal können Sie den Befehl **POS-Verzögerungs-Trigger** verwenden, in anderen Fällen jedoch nicht, insbesondere wenn Sie versuchen, strenge Service Level Agreements (SLAs) zu erfüllen.

Postulaten

- Wenn Y > (t2-t1) für einen beliebigen Wert von t1 verwendet wird, ist ein Holdoff keine gute Idee, da Sie Ihr SLA nicht einhalten können, wenn Sie ein Holdoff konfigurieren.
- Wenn Y <= (t2-t1), können Sie die Implementierung eines Holdoffs in Betracht ziehen. Wenn die Dauer des Ausfalls kleiner als (t1-t0) ist, können Sie den Ausfall abbrechen, da Sie keine Router-Ressourcen nutzen müssen und das gewünschte SLA erfüllen können. Wenn der Fehler in der vergangenen Zeit t1 besteht, können Sie das SLA auch dann einhalten, wenn Sie einige Zeit verlieren, bevor Sie die Wiederherstellung auf IP-Ebene starten.

Sie müssen einige Kenntnisse über das zugrunde liegende Transportnetzwerk und die Konvergenzzeiten des Layer-3-Netzwerks besitzen, um die Werte kennen zu können, die Sie in diesen Formeln verwenden können. Sie müssen auch einige Tests durchführen.

So funktionieren die Trigger:

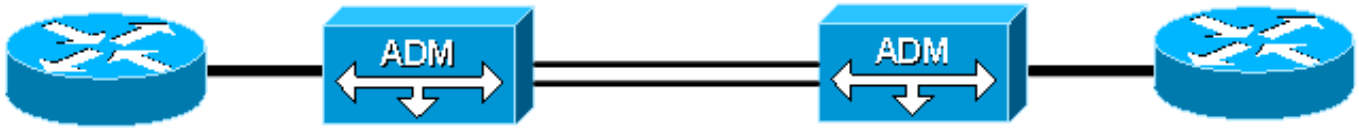
- Die **PoS-Verzögerung löst die Befehlszeile *n*** für *n* ms aus, bevor die Befehlszeile auslöst. Der Standardwert ist 100 ms. Sie können diesen Befehl auf jeder POS-Schnittstelle verwenden, die nicht zum APS gehört. Der Befehl **POS-Verzögerung löst den Befehl line *n* aus und** ermöglicht nicht, dass die Leitung auf den kurzen LOS, der von intern geschützten DWDM-Geräten stammt, abgeschaltet wird, wenn ein interner DWDM-Schutzschalter auftritt. Wenn der Defekt während der Holdoff-Zeit auftritt, ist es so, als wäre der Fehler nie aufgetreten.
- Der Befehl **POS-Verzögerung löst** alle Aktionen aufgrund des Fehlers aus (außer den Zähler für Fehler zu erhöhen), bis die angegebene Haltezeit endet.Wenn Sie diesen Befehl nicht aktivieren, werden APS und Link Down im RP sofort ausgelöst.

Bereitstellung von SONET-Triggern

In diesem Abschnitt wird die Bereitstellung von SONET-Triggern beschrieben.

Geschütztes SONET-Netzwerk: Keine APS auf den Routern

Abbildung 1: Internes geschütztes SONET-Netzwerk



Das SONET-Netzwerk verfügt über einen internen Schutz, d. h. ein Ausfall innerhalb des SONET-Netzwerks löst einen gewissen Schutz-Switch aus, um den Service sehr schnell wiederherzustellen. Daher müssen Sie überlegen, ob Sie die Schnittstelle deaktivieren und Layer 3 benachrichtigen möchten. In den meisten Fällen sehen die Router, wenn ein Schutzschalter innerhalb des SONET-Netzwerks auftritt, eine kurze Leitung oder einen kurzen Pfad AIS, während das Netzwerk Wiederherstellungsmaßnahmen ergreift. Dies tritt jedoch nur auf, wenn der Ausfall einen Hop von einem der Router entfernt auftritt. Das SONET-Netzwerk kann möglicherweise mehrere NEs im Durchmesser haben. Beide Router erkennen LINE-Ausfälle nur als PATH-Ausfälle. In diesem Fall sollten Sie Pfad- und Zeilenebenenauslöser in Betracht ziehen, wenn Sie einen Holdoff benötigen.

Um diese Entscheidung zu treffen, müssen Sie die damit verbundenen Kosten mit beiden Ansätzen verstehen. Als Netzwerkbetreiber müssen Sie folgende Fragen berücksichtigen:

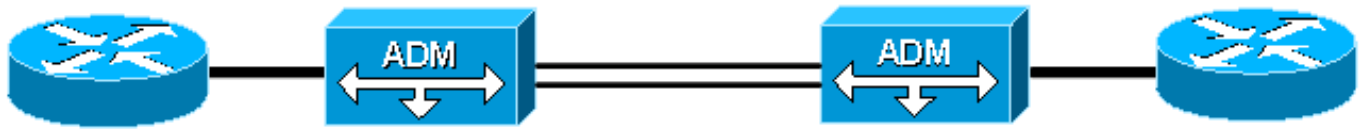
- Reicht die Konvergenz des Netzwerks schnell aus? Andernfalls ist dieser Ansatz nicht geeignet.
- Wie wirkt sich das Routing bei einem solchen Fehler aus? Ist der Einfluss auf den Router so groß, dass die Leistung unter ein akzeptables Niveau sinkt?

Letztlich müssen Sie entscheiden, ob Sie einen potenziellen ca. 60-msec-Treffer ignorieren können oder ob Sie ein solches Ereignis lieber umgehen möchten. Wenn Sie den Treffer ignorieren können, müssen Sie angeben, wie viel von einem "Fudge-Faktor" hinzugefügt werden soll, weil Sie diesen Fehler nicht nur abhalten wollen, um mehrere Millisekunden zu wenige zu warten, und damit die Korrekturmaßnahme verzögern.

In diesem Szenario sind **POS-Verzögerungslöse** wahrscheinlich ausreichend **Zeilen** und **Pfad**. Berücksichtigen Sie darüber hinaus Werte von mindestens 60 ms, wenn ein Holoff gerechtfertigt ist. Wenn das Netzwerk breit genug ist und Sie sofort auf Fehler auf Leitungs- und Pfadebene reagieren möchten, müssen Sie keine Trigger auf Leitungsebene konfigurieren. Sie müssen jedoch den **Pfade** für **PoS-Verzögerungen** konfigurieren, um die sofortige Verarbeitung von PATH-Level-Fehlern zu ermöglichen.

Internes, ungeschütztes SONET-Netzwerk

Abbildung 2: Internes ungeschütztes SONET-Netzwerk

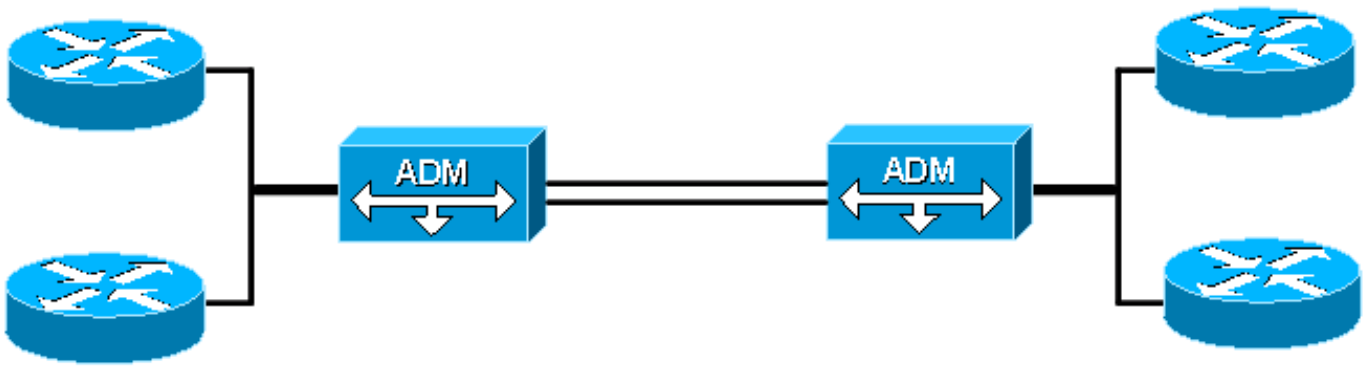


In einem ungeschützten SONET-Netzwerk gehen Sie mit den gleichen Risiken wie im ersten Szenario und noch ein paar mehr vor. Wenn das Netzwerk groß genug ist, können die Router im Falle eines Ausfalls möglicherweise keinen Fehler auf LINE-Ebene erkennen, da alle Fehler gefiltert werden. Auf den Routern werden PFAD-Level-Defekte nach oben und unten angezeigt. In einigen Situationen, in denen im Netzwerk ein Ausfall auftritt, erkennt der Router daher nur Ereignisse auf PATH-Ebene, und es besteht keine End-to-End-Kontinuität zwischen den Routern. Noch schlimmer ist, dass auf SONET-Ebene keine Wiederherstellung erfolgt, um diese Situation zu beheben.

In diesem Szenario müssen Sie Path-Trigger konfigurieren, damit die Router an beiden Enden auf einen PATH-Fehler stoßen, selbst wenn die Router keine Holoff-Auswirkungen haben möchten. Wenn Sie Path-Trigger konfiguriert haben, müssen Sie als Netzwerkbetreiber überprüfen, ob es besser ist, eine Layer 3-Wiederherstellung abzuhalten oder auszulösen.

Geschütztes oder ungeschütztes SONET-Netzwerk

Abbildung 3: Internes ungeschütztes SONET-Netzwerk

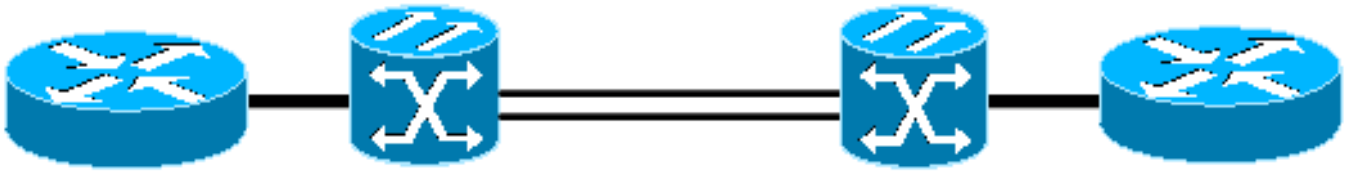


In Cisco IOS Software Release 12.0(28)S können Sie PATH-Trigger auf APS-Schaltungen aktivieren. Wenn Sie APS auf den lokalen oder Remote-Routern bereitstellen, verursacht ein APS-Switch, dass die Remote-Router Working and Protect einen kurzen Fehler auf PFAD-Ebene erkennen. Bei einem kleinen Triggerwert werden die Schnittstellen deaktiviert, und diese Situation ist nicht wünschenswert. Eine Schnittstelle, die ausfällt, verzögert die Servicewiederherstellung, die bereits durchgeführt wird. Ein kurzzeitiger Ausfall in der Cloud kann auch die Servicewiederherstellung verzögern. Das Auftreten eines persistenten PATH-Level-Fehlers weist

jedoch darauf hin, dass der Schaltungsschutz (entweder innerhalb des Netzwerks oder am anderen Ende) die Verbindung nicht wiederherstellen konnte. In diesem Fall müssen die APS-Router Maßnahmen ergreifen und eine Routing-Neukonvergenz initiieren. Sie können Verzögerungswerte für den Pfad von >= 100 ms konfigurieren. Wenn bei dieser Konfiguration ein persistenter Fehler entweder im SONET-Netzwerk oder am Remote-Ende auftritt, bringen die Router beide APS-Schnittstellen in den Zustand der Verbindung. Aus diesem Grund initiieren die Router eine schnellere Umleitung und Wiederherstellung des Service.

Geschütztes DWDM-Netzwerk

Abbildung 4: Geschütztes DWDM-Netzwerk



In diesem Szenario müssen keine Path-Trigger verwendet werden, da das DWDM-Netzwerk nicht auf der Ebene des SONET-Protokolls beteiligt ist. Der Router erkennt Fehler auf ABSCHNITT- oder LINE-Ebene.

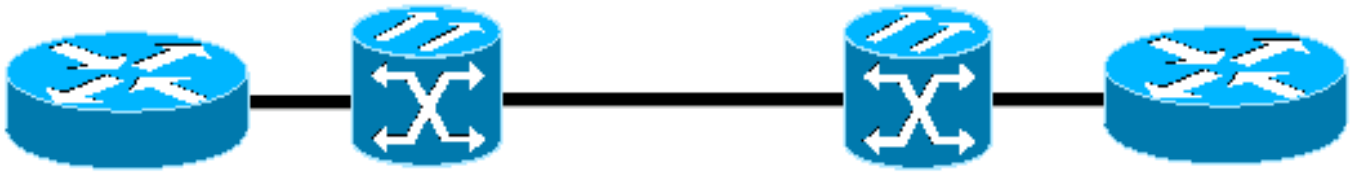
Da das DWDM-Netzwerk intern geschützt ist, wird bei einem Ausfall des Netzwerks in Kürze eine Wiederherstellung durchgeführt. Der Router erkennt in der Regel sehr kurze LOS-, LOF- oder Grenzwertüberschreitungswerte (Burst of BIP Error, LOF).

Daher müssen Sie nur entscheiden, ob ein Holdoff in diesem Netzwerk wünschenswert ist.

Der Befehl **POS-Verzögerung löst** den Befehl **line** aus, wenn Sie eine Verzögerung auswählen.

Ungeschütztes DWDM-Netzwerk

Abbildung 5: Ungeschütztes DWDM-Netzwerk



Wenn sich ein ungeschütztes DWDM-Netzwerk im Transport befindet, müssen Sie alle Fehler in den Routern beheben. In dieser Situation ermöglicht die Standardkonfiguration eine sofortige Reaktion auf Fehler, die bei einem der Router auftreten, da das DWDM nicht am SONET-Protokoll beteiligt ist. Wenn Sie diesen Effekt wünschen, ist die Standardkonfiguration für keine konfigurierten POS-Trigger geeignet.

Wenn Sie einen Holdoff benötigen, genügt der Befehl **pos delay löst den** Befehl **line aus**, um diese Funktionalität bereitzustellen.

Back-to-Back-Verbindungen für Router

Abbildung 6: Router im Back-to-Back-Modus verbunden

Zwei Router, die Back-to-Back zwischen zwei POS-Schnittstellen verbunden sind, müssen wie im letzten Szenario funktionieren. Sie können Ausfälle sofort an jedem Router sehen, da es keine zwischengeschalteten Geräte gibt, die auf dem SONET-Overhead betrieben werden oder Teile des SONET-Signals beenden.

Eine interessante Situation ist, wenn R1 S-LOS sieht und R2 sowohl L-RDI als auch P-RDI, da R1 sowohl LTE (Line Terminating Equipment) als auch PTE (Path Terminating Equipment) ist. Da L-RDI explizit die Ausführung einer Aktion nach Erhalt untersagt, wird die Schnittstelle durch R2 nicht gelöscht. Dieses Problem kann möglicherweise dazu führen, dass eine Schnittstelle von R1 ausgefallen ist, die Schnittstelle von R2 jedoch immer noch aktiv ist und Datenverkehr weiterleitet. Natürlich bietet jedes Layer-2-Keepalive (wie High-Level Data Link Control (HDLC)) Timeout und deklariert die Verbindung, in der Regel in 30 Sekunden, basierend auf den konfigurierten Timern. Einige Betreiber deaktivieren diese Layer-2-Keepalives jedoch und können dies nicht verhindern. Um dieses Problem zu beheben, können Sie verschiedene Ansätze verfolgen, und jeder Ansatz behandelt dies aus einer anderen Perspektive, wie hier erläutert:

- Aktivieren von Path-Triggern - Wenn P-RDI eine Schnittstelle bei aktivierten Path-Triggern deaktiviert, können Sie diese Methode verwenden, um eine schnelle Antwort zu geben und die Schnittstelle zu verwerfen. Der interessante Punkt ist, dass L-RDI die P-RDI im normalen Betrieb nach GR-253 verdeckt. Wenn die POS-Trigger auf der Fehlerebene behandelt werden, werden die Trigger vor der Warnmeldungsmaskierung verarbeitet, und die Schnittstelle fällt weiterhin entsprechend der konfigurierten Verzögerungszeit ab.
- Aktivieren von Layer-2-Keepalives (Layer-2-Keepalives aktivieren): Diese Option bewirkt, dass die Schnittstelle auf R2 das Zeitlimit überschreitet, nachdem 3 Keepalives verpasst wurden. Dies beträgt in der Regel insgesamt 30 Sekunden (3 x 10), und Cisco empfiehlt diese Option im Allgemeinen nicht, um die schnelle Link-Konvergenz zu optimieren.
- Aktivieren eines Link-State-Routing-Protokolls - Wenn die Schnittstelle auf R1 aufgrund des S-LOS deaktiviert wird, wird sofort eine Link-State-Meldung gesendet. Auch wenn die Schnittstelle auf R2 noch aktiv sein kann, wird SPF ausgeführt, wenn die Meldung zum Verbindungsstatus im gesamten Bereich empfangen wird, und die Verbindung wird aus der Topologie entfernt, da die Verbindung die Prüfung der bidirektionalen Konnektivität nicht besteht. Dies verhindert, dass das Netzwerk versucht, dieses Simplex-Szenario zu durchlaufen.

Remote-Benachrichtigung basierend auf Signalqualität

Wenn Sie zwei Router entweder Back-to-Back- oder über ein SONET-Netzwerk verbinden, deckt die bereitgestellte OAM-Architektur die Erkennung der meisten Fehlerszenarien ab.

In der Regel gibt es lokale Benachrichtigungen und Remote-Benachrichtigungen. Wenn jedoch

eine große Anzahl von Grenzwertüberschreitungsfehlern (SD, SF oder B3-TCA) einen Schwellenwert überschreitet, wird keine Benachrichtigung per Fernzugriff gesendet, um anzuzeigen, dass diese Bedingung aufgetreten ist. Wenn Sie also Multi Protocol Label Switching (MPLS) Fast Re-Route-Schutz verwenden, aktiviert kein Trigger einen sofortigen Schutz-Switch. Der Datenverkehr wird weiterhin blockiert, bis hinreichender Datenverkehr verloren geht und entweder Layer-2-Keepalives für die Verbindung oder Nachbarbeziehungen zwischen IGP-Peers (Interior Gateway Protocol) ausfällt. Manchmal tritt dies nie auf und wird weiterhin den Datenverkehr erpressen.

Zur Bewältigung dieses Szenarios führt CSCec85117 den Befehl **po-action b3-ber prdi** in die Befehlsstruktur POS und SONET ein.

Mit diesem Befehl kann der Operator die Schnittstelle so konfigurieren, dass eine P-RDI gesendet wird, wenn der B3-Grenzwert überschritten wurde. Mit dieser Option können Sie die gesamte Verbindung unabhängig von der Topologie optimal überwachen. Wenn der **Pfade für die PoS-Verzögerung** auf den Routern aktiviert ist, aktiviert der Befehl **b3-ber prdi** die **PoS-Aktion** die heruntergekommene Verbindung (und das entsprechende FRR- oder Routing-Update). Dadurch wird der schwarze Löcher-Effekt auf beschädigte Links vermieden.

Um die Empfindlichkeit dieser Aktion zu ändern, stellen Sie die b3-tca wie folgt ein:

```
router(config-if)# pos threshold b3-tca ?
```

Der angegebene Wert ist die exponentielle Komponente für die BER-Berechnung (z. B. **der pos threshold b3-tca 3** legt die B3-TCA auf eine Rate von 1 x 10^-3 fest).

Zugehörige Informationen

- Telcordia Information SuperStore
- Technischer Support und Dokumentation - Cisco Systems