Disparadores SONET

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Eventos que desactivan una interfaz POS](#)
[Desencadenadores de nivel de línea y sección](#)
[Disparadores de Trayectoria](#)
[Resumen del comportamiento CLI de POS Triggers](#)
[Retirada de alarmas SONET](#)
[Gestión de defectos](#)
[Disparadores en acción](#)
[¿Por qué utilizar los desencadenadores?](#)
[Disparadores de SLA y POS](#)
[Teorema](#)
[Postulados](#)
[Implementación de disparadores SONET](#)
[Red SONET protegida: No hay APS en los routers](#)
[Red SONET interna no protegida](#)
[Red SONET protegida o desprotegida](#)
[Red DWDM protegida](#)
[Red DWDM no protegida](#)
[Routers conectados adosados](#)
[Notificación remota basada en la calidad de la señal](#)
[Información Relacionada](#)

Introducción

Un disparador es cualquier evento que cumple la función de *causa* en la relación causa-efecto en una interfaz de red óptica sincrónica (SONET) en IOS. A veces, puede utilizar el comando **pos delay triggers**. En otras ocasiones, Cisco recomienda que no utilice el comando **pos delay triggers**, especialmente cuando intente cumplir los Acuerdos de nivel de servicio (SLA) estrictos. Los proveedores de servicios venden niveles de servicio diferenciados según determinados acuerdos. Los acuerdos tratan de cómo la red enruta, protege o prioriza el tráfico del cliente internamente. Estos comandos ayudan a los proveedores a ajustar las redes para cumplir los acuerdos de servicio.

Este documento examina los desencadenadores que se relacionan con los eventos de interfaz activo y inactivo. Este documento también explica cómo implementar Packet Over SONET (POS)

y considera los SLA y los tiempos de convergencia en la Capa 3.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Eventos que desactivan una interfaz POS

Esta sección describe los eventos que desactivan una interfaz POS y enumera los comandos relacionados.

Desencadenadores de nivel de línea y sección

La lista de desencadenadores en esta sección se refiere a los *sistemas de transporte de red óptica sincrónica (SONET)* GR-253-CORE*:* Especificación *de criterios genéricos comunes*:

- Pérdida de señal de sección (SLOS): la especificación indica que debe detectar no menos de 2,5 us y no más de 100 us (6.2.1.1.1).
- Pérdida de trama de sección (SLOF): la especificación indica que debe detectarlo en un mínimo de 3 ms (o 24 patrones de trama con errores consecutivos) (6.2.1.1.2).
- Señal de indicación de alarma - Línea (AIS-L): AIS-L debe enviarse cuando proceda, dentro de los 125 usec de detección. Un dispositivo debe detectar la recepción de AIS-L si el dispositivo ve 5 tramas consecutivas donde los bits 6,7 y 8 de K2 están configurados en 111 (6.2.1.2.1).
- Tasa de error de bits de degradación de la señal (SD-BER): SD-BER es un disparador sólo en interfaces con conmutación de protección automática (APS) (vinculada al cálculo de B2 BER).
- Tasa de error de bit de fallo de señal (SF-BER): SF-BER es un disparador tanto para las interfaces APS como para las interfaces que no son APS (atadas al cálculo de B2 BER).
- Indicación de defecto remoto - Línea (RDI-L): RDI-L no es un disparador para POS o APS. (Sin embargo, RDI-L es un disparador para MPLS FRR) (sección 5.3.3.1).

Para obtener más información sobre las secciones mencionadas en esta lista, vea el sitio web del Telcordia Information SuperStore .

Comandos relacionados

El **retardo pos dispara la línea *n*** el comando apaga LOS/LOF/AIS para n ms antes de que el comando active la línea hacia abajo:

Si configura el comando sin ningún valor numérico, el tiempo de retraso es de 100 ms de forma predeterminada. Puede utilizar disparadores de línea en cualquier interfaz POS que no sea APS. No puede utilizar disparadores de línea en las interfaces que participan en APS, porque los disparadores de línea interfieren con el funcionamiento de APS. El comando **pos delay dispara la línea *n*** no permite que la línea caiga en el breve LOS que proviene del equipo de multiplexación por división de longitud de onda densa (DWDM) protegido internamente, desde el momento en que se produce un switch de protección DWDM interno. Si el defecto se elimina durante el período de retención, es como si nunca hubiera ocurrido.

El comando **pos delay dispara la línea** detiene cualquier acción basada en el defecto (excepto para aumentar el contador de defectos) hasta que finaliza el período de retención especificado.

Si no activa este comando, los APS y el link descendente de los defectos SONET anteriores se activan inmediatamente en el Procesador de ruta (RP).

Disparadores de Trayectoria

Estos defectos de nivel de PATH específicos inician un cambio de estado solamente si ha habilitado la **trayectoria de disparadores de retardo pos** en la interfaz:

- AIS-P: este defecto se debe provocar dentro de los 125 usec a partir de la detección del defecto que resulta en el AIS-P. El equipo de terminación de trayecto (PTE) debe detectar este defecto cuando los bytes H1 y H2 para una ruta STS contienen todos 1 para 3 tramas consecutivas. Las trayectorias concatenadas necesitan observar solamente los primeros bytes H1 y H2. Para más información, ver sección 6.2.1.2.2 de R6-175 y R6-176.
- RDI-P: si el RDI-P está presente, el defecto se debe detectar en 10 tramas. Véase 6.2.1.3.2 de R6-221.
- B3-TCA (alarmas de cruce de umbral) para B3: esta alarma está vinculada al cálculo de la IP binaria de comunicaciones sincrónicas (Bisync) (BIP) de B3.
- LOP-P (Pérdida de Trayectoria del Puntero) (si la versión de IOS incluye CSCdx58021)—Vea la sección 6.2.1.1.3 de GR-253.

Para obtener más información sobre las secciones mencionadas en esta lista, vea el sitio web del Telcordia Information SuperStore .

Comando relacionado

El comando **pos delay triggers path *<msec>*** habilita el desencadenado de link en AIS-P, RDI-P y errores B3 excesivos. De forma predeterminada, el desencadenado de link para los errores de trayectoria está desactivado.

El comando también especifica un tiempo de espera entre 0 y 511 ms (el valor predeterminado es 100 ms). Los defectos de activación de la ruta (AIS-P, RDI-P) que se eliminan antes del final del

período de espera no provocan el desencadenamiento. Cuando no ha configurado explícitamente este comando en una interfaz POS, no se produce ninguna acción si se procesan los defectos del nivel PATH. A diferencia de los disparadores de línea, las interfaces APS permiten disparadores de trayecto, porque los disparadores de trayecto no interfieren con la actividad de nivel de línea de APS. No se permitió configurar los desencadenadores de ruta con APS en versiones anteriores a la versión 12.0(28)S del software Cisco IOS®. Se agregaron desencadenadores de ruta para acelerar el comportamiento ascendente/descendente del link de las interfaces POS cuando se conectaban a redes SONET. Esto permitió una convergencia de nivel 3 más rápida en presencia de errores remotos.

Resumen del comportamiento CLI de POS Triggers

Esta tabla enumera las condiciones del disparador POS y los resultados asociados:

Condición	Resultado
Si no ha configurado nada relacionado explícitamente con los disparadores POS.	Los disparadores de nivel de línea se procesan inmediatamente.
Si ha configurado el comando **pos delay triggers line**.	Los disparadores de nivel de línea se procesan después de una demora de 100 ms.
Si ha configurado el comando **pos delay triggers line** *x*.	Los disparadores de nivel de línea se procesan después de *x* msecs, donde *x* está entre 0 y 511.
Si no ha configurado nada relacionado explícitamente con los desencadenadores de trayecto.	Los desencadenadores de trayecto no se procesan y no se realiza ninguna acción.
Si ha configurado el comando **pos delay triggers path**.	Los disparadores de nivel de trayecto se procesan después de un retraso de 100 ms.
Si ha configurado el comando **pos delay triggers path** *x*.	Los desencadenadores de nivel de trayecto se procesan después de *x* msecs, donde *x* está entre 0 y 511.

Retirada de alarmas SONET

Las alarmas SONET que resultan de defectos se mantienen durante 10 segundos (10,5 +-,5) después de que se borra el defecto.

Gestión de defectos

En IOS, las tarjetas POS cambian su estado LINE debido a diferentes disparadores, a través de dos medios generales para el procesamiento de defectos. Aunque esto depende de la configuración específica de la interfaz (APS o no APS), en general hay dos tipos de fallas:

- Gestionado
- No administrado

Debe entender los términos específicos para el manejo de alarmas que este documento utiliza:

- Defecto: la condición de falla que reconoce el hardware.
- Fallo: defecto que se ha empapado durante los ~2.5 segundos necesarios y que se informa a través de los mensajes SONET-4-ALARM. Cualquier defecto que sea un disparador no se empapará.
- Fallas no administradas: eventos como LOS, LOF, etc. El marco SONET los detecta un conjunto definido de parámetros y no requiere cálculo alguno. Hay un defecto presente y afirmado por el hardware o no hay defecto. Los fallos difíciles como estos, en general, se manejan mediante interrupciones. LOS, LOF, AIS-L y, en casos especiales, AIS-P y RDI-P se reafirman inmediatamente. Éstos dependen del framer y de las reglas definidas para detectar cada uno de estos defectos. El efecto de estos defectos es inmediato. Sin embargo, puede indicar al router que retrase la afirmación de este defecto como una falla. Hay dos temporizadores que determinan el valor de demora, **pos delay triggers [path | line]** y retraso del transportista. Estas cuestiones se abordan más adelante en el documento.
- Alarmas administradas: eventos como TCA y cálculos de SD/SF-BER. Éstos requieren algún cálculo para determinar si están presentes, están en aumento o disminuyen, etc. Por ejemplo, no puede tener un LOS que aumente su "LOS-ness" desde la perspectiva del router. Sin embargo, puede tener BER que está aumentando o disminuyendo; las medidas adoptadas pueden ser diferentes. Las fallas de software, como BER y TCA, necesitan algún cálculo, porque dependen de una serie de factores, por ejemplo, umbrales que un usuario puede configurar, velocidad de bits y número máximo de CV BIP (porque son diferentes para B1, B2 y B3). Estos fallos también tardan más en detectarse, porque el hardware se sondea para los contadores BIP y también porque estos tipos de defectos son de naturaleza gradual y se acumulan con el tiempo. También es cierto que, en general, no pasa de 0 BIP directamente a una degradación de la señal (SD) o a una falla de señal (SF) sin que haya ningún otro tipo de fallo duro en la red. Estos defectos son más lentos cuando se comparan con los fallos duros.

Este es un enfoque generalizado de los cálculos básicos que describe cómo calcular la BER:

Después de cada reinicio de los cálculos y hasta que BER_Period alcance Required_BER_Period (la ventana de integración no está completamente implementada), el algoritmo funciona estrictamente como uno que integra o promedia:

- BER_Period = BER_Period + 1 s.
- Current_BIP = Current_BIP + BIP_new.
- Current_BER = Current_BIP/BER_Period.

Después de que BER_Period alcance Required_BER_Period (la ventana de integración se implementó completamente y comienza a deslizarse), el algoritmo funciona como una cubeta con fuga uno:

- BER_Period = Required_BER_Period.
- Current_BIP = Current_BIP + BIP_new - Current_BER * 1 s.
- Current_BER = Current_BIP/BER_Period.

El valor Required_BER_Period se determina basándose únicamente en la velocidad de línea y el umbral BER configurado, siguiendo los estándares (consulte la figura 5-5, Criterios de tiempo de inicio del switch, GR-253). Sin embargo, se limita a 1 segundo, nuestra tasa de muestreo.

Por lo tanto, BER_Period (ventana de integración) se mueve con cada sondeo y se calcula un nuevo BER con cada sondeo. Si Current_BER supera un límite definido, se produce el defecto adecuado inmediatamente durante el mismo intervalo de sondeo o cálculo y se mantiene la respuesta mínima. Repetimos estos cálculos cada segundo y comprobamos si se ha producido uno de los tres eventos siguientes:

- La BER aún se encuentra dentro del mismo rango. No hay ninguna acción nueva.
- BER ha aumentado nuevamente y ha cruzado un umbral SD o SF (para B2). Levante una nueva alarma.
- BER ha disminuido por debajo de un umbral BER. Limpia la alarma.

Para la afirmación de una TCA o SD/SF, debe esperar sólo hasta que haya superado un límite en ese intervalo de sondeo respectivo. En el momento del cálculo, verifique si Current_BER ha cruzado un umbral y, si lo ha hecho, puede continuar y afirmar la alarma inmediatamente a través del software.

Esto es válido porque, si Current_BER es lo suficientemente grande como para activar la alarma inicialmente, la condición sigue siendo cierta al final del BER_Period. Esto se basa en cómo se definen y comparan los valores en relación con la ventana de cálculo.

Cuando borra una alarma, debe esperar hasta el final de la ventana de cálculo BER_Period. Esto es para asegurarse de que no se acumulen nuevos BIP durante la última parte de la ventana que podría mantenerle por encima de un umbral.

Nota: Según GR-253, SD-BER y SF-BER están estrictamente ligados al conteo de BIP B2. Los umbrales predeterminados actuales son:

- umbrales BER: SF = 10e-3 SD = 10e-6
- Umbrales TCA: B1 = 10e-6 B2 = 10e-6 B3 = 10e-6

Nota: Las tarjetas OC-48 Engine2 tienen estos umbrales predeterminados:

- umbrales BER: SF = 10e-4 SD = 10e-6
- Umbrales TCA: B1 = 10e-6 B2 = 10e-6 B3 = 10e-6

Si desea que el disparador de Trayectoria de TCA B3 se active de forma similar a SF, el umbral B3 se debe establecer en el mismo umbral, 10e-3. Puede hacerlo a través del comando **pos threshold b3-tca 3** en la indicación `router(config-if)#`.

Nota: Dado que el intervalo de sondeo es de un segundo, ese es el tiempo mínimo en el que notaremos y aumentaremos el defecto de TCA o SD/SF. Además, debido a la naturaleza acumulada del TCA/SD/SF, estos tipos de fallas se acompañan de otros fallos cuando ocurren rápidamente en fallas típicas. Esto mantiene un equilibrio entre la utilización y el rendimiento del procesador del router. No se puede configurar el intervalo de sondeo.

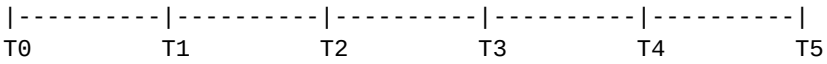
Disparadores en acción

Esta sección proporciona información básica para examinar la interacción de algunos de los diversos botones ajustables del usuario en IOS:

Los **disparadores de retraso pos [line | path]** retrasa brevemente la notificación y la acción de un defecto.

La línea de disparador de retraso POS es el tiempo de espera antes de reaccionar a una alarma de línea. El valor predeterminado es la reacción inmediata, lo que significa que la **línea del disparador de retraso pos *0***. Si configura directamente la **línea disparadora de retraso pos** sin ningún valor, se tendrá en cuenta el valor predeterminado de 100 ms. Esto permite una respuesta inmediata o retardada, basada en el efecto deseado. Con cualquiera de estos dos configurados, el defecto no aparece como alarma activa hasta que el período de retención haya terminado.

Línea de tiempo:



Aquí:

- t0: tiempo en el que se produce el defecto.
- t1: tiempo en el que el hardware detecta el defecto.
- t2: tiempo en el que se informa del defecto como una falla.
- t2-t3: tiempo que se detiene para cualquier disparador configurado.
- t3-t4: tiempo durante el cual se espera debido al retraso del portador.
- t4: tiempo en el que la interfaz realmente se desactiva en IOS.
- t5: tiempo en el que se desactiva cualquier adyacencia para un protocolo de ruteo.

Examine la cronología para observar cómo ajustar los diferentes mandos para lograr varios resultados.

El comando **post delay triggers** afecta la duración entre t2 y t3 y, en efecto, oculta el defecto del IOS hasta que el período de retención haya terminado. Por supuesto, si el defecto se borra antes de alcanzar t3, no ocurre nada, y es como si nada hubiera pasado. El valor predeterminado para los desencadenadores de línea y ruta es de 100 ms y el intervalo es de 0 a 511 ms. Los desencadenadores de trayecto no están habilitados (es decir, no realizan ninguna acción) a menos que la **trayectoria de disparadores de retardo pos** se configure primero. **pos delay trigger path** es el tiempo de espera antes de reaccionar a una alarma de trayectoria. El default no es una reacción. Si configura directamente **pos delay trigger path** sin ningún valor, el valor predeterminado de 100 ms se asignará automáticamente. Esto incluye AIS-P, RDI-P y B3-TCA. Esta funcionalidad se agregó a través de CSCds82814 (alrededor de 12.0(15.5)S/ST).

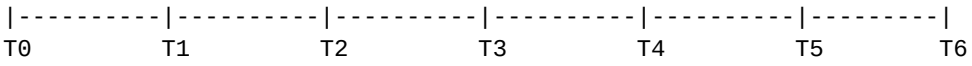
Carrier-delay es el tiempo de espera entre el final del tiempo de espera del retraso POS y desactivará la interfaz IOS. El valor predeterminado es 2000 ms. El retraso de la portadora es el tiempo entre t3 (cuando IOS detecta una falla) y t4 (cuando la interfaz se desactiva). De forma predeterminada, se establece en 2 segundos y se puede configurar para valores msec. Como indica la línea de tiempo, es una función aditiva sobre los temporizadores de retención de nivel SONET. Se comporta de la misma manera que los disparadores POS - si la alarma se despeja antes del final del período de retención, la interfaz no se desactiva. Sin embargo, aquí hay un enigma. El temporizador de rebote SONET no borra el defecto antes de que se active el retraso de la portadora, a menos que el retardo de portadora sea grande (mucho más de 10 segundos). Esto da lugar a una situación en la que el retraso de la portadora se activa casi siempre y, por lo tanto, debe considerarse bastante pequeño cuando se implementa con interfaces POS. El retraso de la portadora también se agrega después de que se borra la alarma, antes de que se declare la interfaz también. Por lo tanto, puede contar el valor del retraso del portador dos veces antes de que la interfaz vuelva a funcionar.

Con algunas interfaces y medios físicos esto es útil. Sin embargo, con las interfaces POS hay un

número de activadores y temporizadores que puede utilizar y combinar para crear el efecto deseado, sin que el transportista tarde en asumir un rol tan importante. Un valor de retraso de portadora de 0-8 mseg es un buen punto de partida para que los clientes lo consideren cuando prueben estos botones por su cuenta. En general, una buena estrategia es utilizar el comando **pos delay triggers** para absorber cualquier problema y proporcionar el efecto de retención deseado. El retraso de la portadora puede mantenerse pequeño para minimizar su impacto.

El temporizador de eliminación de rebote SONET mencionado anteriormente se establece en 10 segundos (+/-.5sec) y GR-253 lo requiere para asegurarse de que no se produzca un período de inestabilidad inferior a 10 segundos. El temporizador comienza después de que se borra el defecto. El temporizador se reinicia si se produce otro evento de defecto antes de que la ventana del temporizador haya caducado.

Línea de tiempo:



Aquí:

- t0: el defecto se borra.
- t0: se inicia el temporizador de rebote.
- t4—t0 + 10sec (por lo tanto, la falla debe borrarse si no se producen nuevos defectos entre t0 y t4).

Si un evento ocurre antes de t4, (digamos, a t2) (podría ser otro defecto o una repetición del mismo tipo de defecto), el temporizador se detiene hasta que se borra este nuevo defecto. En t3, el temporizador se inicia de nuevo, cuando no hay defectos activos, y cuenta durante los ~10 segundos. Si no se detecta ningún evento nuevo, borre la alarma en t5 y luego inicie el temporizador de retraso del portador. Cuando se haya borrado el retraso de la portadora en t6, vuelva a activar la interfaz.

Esta información debería permitir al cliente entender con mayor claridad cómo reaccionan las interfaces POS a diversas condiciones SONET/SDH. Esto permite que el equipo se configure con mayor precisión según el comportamiento esperado del cliente.

¿Por qué utilizar los desencadenadores?

Esta sección explica cuándo debe utilizar los **disparadores de retraso pos [line | path]** y cuando no debe utilizarlo.

Estos son los escenarios en los que no debe utilizar **disparadores de retraso pos**. Hay varios escenarios:

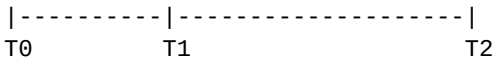
- No puede utilizar desencadenadores de línea con interfaces configuradas por APS. Las versiones anteriores a la versión 12.0(28)S del software del IOS de Cisco no permitían ni siquiera el uso de disparadores de trayecto.
- Cuando explícitamente no desea que los defectos del nivel de PATH desactiven la interfaz, no puede utilizar estos desencadenadores.
- Cuando desea que los disparadores de nivel de línea desactiven la interfaz sin demora, no puede utilizar este comando.

Estos son los escenarios en los que puede utilizar el comando **pos delay triggers**:

- Cuando desea mantener desactivado temporalmente el efecto de un defecto de nivel de línea.
- Para habilitar la capacidad para que los defectos del nivel PATH desactiven la interfaz inmediatamente.
- Para habilitar los defectos de nivel PATH para que derriben la interfaz, pero con algunos vaciados incluidos.

Disparadores de SLA y POS

Examine esta línea de tiempo:



- Tiempo t=0 (t0): cuando se detecta el defecto.
- Tiempo t2: el tiempo de restauración de SLA necesario.
- Tiempo t1: cualquier retención del comando **pos delay triggers** configurado (el valor predeterminado para LINE es 0 y el valor predeterminado para PATH no está habilitado).
- X es el valor de retención (por lo que X = el valor de t1).
- Y es el tiempo que tardará la capa 3 en restaurar el servicio.

Teorema

A veces, puede utilizar el comando **pos delay triggers**, mientras que en otras ocasiones, no puede hacerlo, especialmente cuando intenta cumplir los Acuerdos de nivel de servicio (SLA) estrictos.

Postulados

- Si Y > (t2-t1) para cualquier valor de t1, un vaciado no es una buena idea porque, no puede cumplir con su SLA si configura algún vaciado.
- Si Y <= (t2-t1), puede considerar la implementación de un holdoff. Si la duración de la falla es menor que (t1-t0), puede retenerla porque, no tiene que utilizar los recursos del router y puede cumplir con el SLA deseado. Si el defecto persiste después de la hora t1, aún puede cumplir con el SLA, aunque pierda algún tiempo antes de iniciar la restauración en el nivel IP.

Debe tener algún conocimiento sobre la red de transporte subyacente y los tiempos de convergencia de la red de Capa 3, para conocer los valores que puede utilizar en estas fórmulas. También debe realizar algunas pruebas.

Así es como funcionan los desencadenadores:

- El **retardo POS desencadena la línea *n*** el comando apaga LOS/LOF/AIS para *n* ms antes de que el comando active la línea hacia abajo. El valor predeterminado es 100 ms. Puede utilizar este comando en cualquier interfaz POS que no sea APS. El comando **pos delay dispara la línea *n*** no permite que la línea caiga en el breve LOS que proviene del equipo DWDM protegido internamente, desde el momento en que se produce un switch de protección

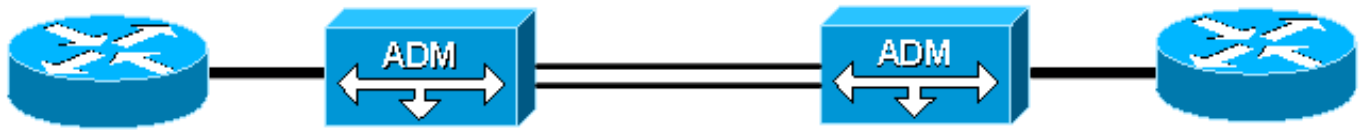
DWDM interno. Si el defecto se elimina durante el período de retención, es como si nunca hubiera ocurrido.
- El comando **pos delay triggers line** suspenderá cualquier acción basada en el defecto (excepto para incrementar el contador de defectos), hasta que termine el período de retención especificado.Si no habilita este comando, APS y link inactivo se activan inmediatamente en el RP.

Implementación de disparadores SONET

Esta sección describe la implementación de los desencadenadores SONET.

Red SONET protegida: No hay APS en los routers

Figura 1: Red SONET Internamente Protegida



La red SONET tiene protección interna, lo que significa que una falla dentro de la red SONET hace que algún switch de protección restaure el servicio muy rápido. Por lo tanto, debe considerar si desea desactivar la interfaz y notificar la Capa 3. En la mayoría de los casos, cuando se produce un switch de protección dentro de la red SONET, los routers ven una línea breve o un AIS de trayectoria mientras la red realiza una acción reparadora. Sin embargo, esto ocurre solamente si la falla está a un salto de cualquiera de los routers. La red SONET puede ser posiblemente de varios NE de diámetro, cualquiera de los routers ve las fallas de LINE solamente como fallas de PATH. En este caso, considere los desencadenadores de ruta y nivel de línea si desea un vaciado.

Para tomar esta decisión, debe comprender el coste asociado con ambos enfoques. Como operador de red, debe tener en cuenta estas preguntas:

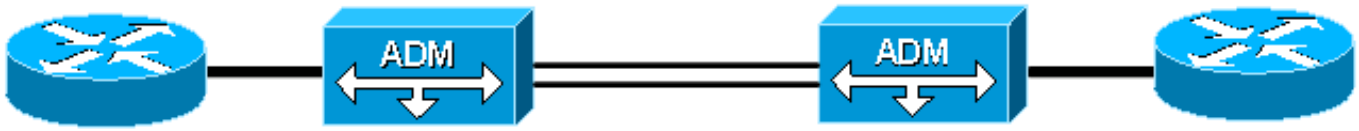
- ¿La red converge lo suficientemente rápido? De lo contrario, este enfoque no es adecuado.
- ¿Cuál es el impacto del ruteo en torno a tal falla? ¿El impacto en el router es tan grande que el rendimiento cae por debajo de un nivel aceptable?

En última instancia, debe decidir si puede ignorar un posible resultado de ~60 mseg o si prefiere enrutar alrededor de tal evento. Si puede ignorar el resultado, debe identificar cuánto de un "factor de elusión" agregar porque, no desea retener este defecto sólo para esperar varios milisegundos a unos pocos y, por lo tanto, retrasar la acción correctiva.

En este escenario, **pos delay triggers line** and **path** probablemente sean suficientes. Además, considere valores de al menos 60 ms si se justifica una retención. Si la red es lo suficientemente amplia y desea tomar medidas inmediatas tanto en los defectos de línea como de ruta, no necesita configurar los desencadenadores de nivel de línea. Sin embargo, debe configurar **pos delay triggers path** con un valor de 0 para habilitar el procesamiento inmediato de los defectos del nivel PATH.

Red SONET interna no protegida

Figura 2: Red SONET interna desprotegida

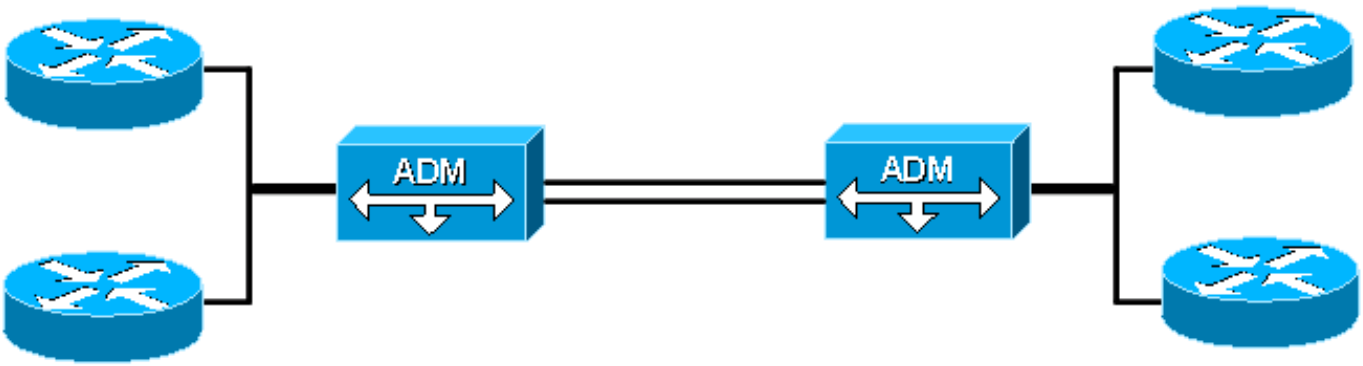


En una red SONET desprotegida, corre los mismos riesgos que en el primer escenario, además de algunos más. Si la red es lo suficientemente grande, los routers posiblemente nunca puedan ver un defecto de nivel de LÍNEA en caso de una falla, porque todos los defectos se filtran. Los routers pueden ver que el nivel PATH viola el flujo ascendente y descendente. Por lo tanto, en algunas situaciones, donde ocurre una falla dentro de la red, el router sólo ve eventos de nivel PATH y no hay continuidad de extremo a extremo entre los routers. Peor aún, no se produce ninguna restauración a nivel de SONET para remediar esta situación.

En este escenario, debe configurar los desencadenadores de trayecto simplemente para permitir que los routers en cualquiera de los extremos tomen acción cuando los routers encuentren un defecto PATH, incluso si los routers no desean ningún efecto de vaciado. Cuando haya configurado los disparadores de trayecto, como operador de red, debe verificar si es mejor detener o activar una restauración de Capa 3.

Red SONET protegida o desprotegida

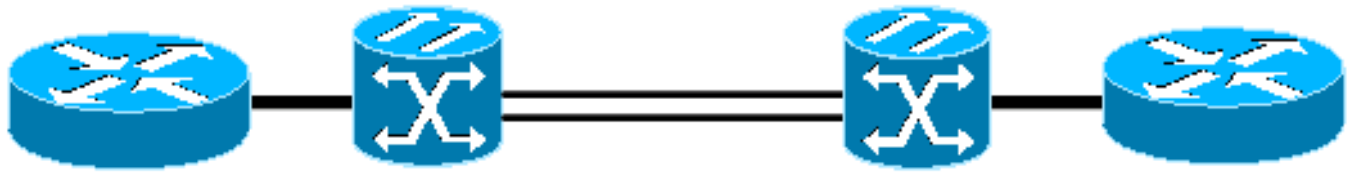
Figura 3: Red SONET Internamente Desprotegida



En Cisco IOS Software Release 12.0(28)S, puede habilitar los desencadenadores PATH en los circuitos APS. Cuando se implementa APS en los routers locales o remotos, un switch APS hace que los routers remotos Working and Protect vean un breve defecto de nivel PATH. Con un pequeño valor de disparador, las interfaces se desactivan y esta situación no es deseable. Una interfaz que se desactiva retrasa la restauración del servicio que ya está en curso. Una falla momentánea que ocurre dentro de la nube también puede retrasar la restauración del servicio. Sin embargo, la aparición de un error de nivel PATH persistente indica que la protección del circuito (ya sea dentro de la red o en el otro extremo) no ha podido restaurar la conectividad. En este caso, los routers APS deben tomar medidas e iniciar la reconvergencia de ruteo. Puede configurar valores de retardo del disparador de trayecto de >= 100 ms. Con esta configuración, cuando se produce un error persistente dentro de la red SONET o en el extremo remoto, los routers envían ambas interfaces APS a un estado de link inactivo. Por lo tanto, los routers inician un re-ruteo más rápido y la restauración del servicio.

Red DWDM protegida

Figura 4: Red DWDM protegida



En este escenario, no necesitamos utilizar los desencadenadores de rutas, porque la red DWDM no participa en el nivel de protocolo SONET. El router detecta cualquier falla en el nivel SECTION o LINE.

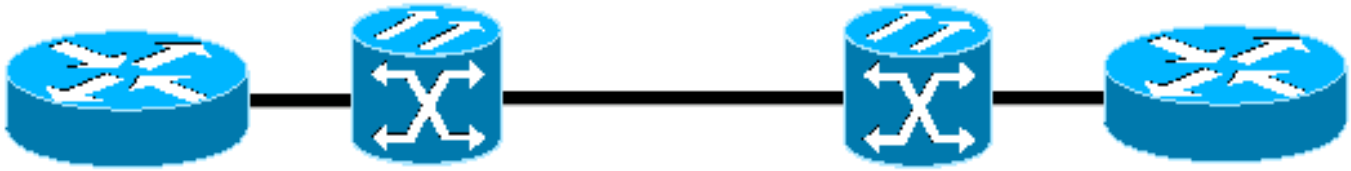
Una vez más, debido a que la red DWDM está protegida internamente, una falla interna en la red provoca que pronto se produzca la restauración. El router suele ver una ráfaga de errores BIP, LOF o LOS muy breves.

Por lo tanto, sólo tiene que decidir si una retención es deseable en esta red.

El comando **pos delay triggers line** es suficiente en esta situación, si elige una demora.

Red DWDM no protegida

Figura 5: Red DWDM desprotegida



Con una red DWDM desprotegida en el transporte, debe abordar cualquier falla dentro de los routers. En esta situación, la configuración predeterminada permitiría una respuesta inmediata a cualquier falla observada en cualquiera de los routers porque el DWDM no participa en el protocolo SONET. Si desea este efecto, la configuración predeterminada de ningún disparador POS configurado es apropiada.

Si necesita algún tipo de retención, el comando **pos delay triggers line** es suficiente para proporcionar esta funcionalidad.

Routers conectados adosados

Figura 6: Routers conectados adosados

Dos routers conectados adosados entre dos interfaces POS deben funcionar exactamente como el último escenario. Puede ver fallas inmediatamente en cualquier router, porque no hay ningún equipo intermediario que funcione en la sobrecarga SONET o que termine cualquier parte de la señal de nivel SONET.

Una situación interesante es cuando R1 ve S-LOS y R2 ve tanto L-RDI como P-RDI, ya que R1 es tanto equipo de terminación de línea (LTE) como equipo de terminación de trayecto (PTE). Dado que L-RDI rechaza explícitamente cualquier acción resultante que se tome al recibirla, R2 no descarta la interfaz como resultado. Este problema puede conducir potencialmente a una situación donde una interfaz de R1 está inactiva, pero la interfaz de R2 sigue activa y reenvía tráfico. Por supuesto, cualquier señal de mantenimiento de capa 2 (como el High-Level Data Link Control (HDLC) proporciona) se agota el tiempo de espera y declara el enlace inactivo, normalmente en 30 segundos, en función de los temporizadores configurados. Sin embargo, varios operadores desactivan estas señales de mantenimiento de Capa 2 y no pueden evitar esta situación. Para abordar este problema, puede adoptar varios enfoques, y cada enfoque aborda esto desde una perspectiva diferente, como se explica aquí:

- Activar desencadenadores de trayecto: a medida que P-RDI hace caer una interfaz con activadores de trayecto, puede utilizar este método para causar una respuesta rápida y descartar la interfaz. Lo interesante es que L-RDI enmascara el P-RDI bajo funcionamiento normal según GR-253. A medida que los disparadores POS se manejan en el nivel de defecto, los disparadores se procesan antes del enmascaramiento de la alarma, y la interfaz sigue descartándose según el tiempo de demora configurado.
- Activar Keepalives de Capa 2: esta opción hace que la interfaz en R2 se agote el tiempo de espera después de que se pierdan 3 keepalives. Esto suele ser un total de 30 segundos (3x10), y Cisco no recomienda generalmente esta opción como herramienta para ajustar la convergencia rápida de enlaces.
- Enable a Link-State Routing Protocol (Activar un Link-State Routing Protocol): cuando la interfaz en R1 se desactiva debido al S-LOS, se envía inmediatamente un mensaje de estado de link. Aunque la interfaz en R2 todavía puede estar activa, cuando se recibe el mensaje de estado del link en todo el área, se ejecuta SPF y el link se quita de la topología porque el link falla la verificación de conectividad bidireccional. Esto evita que la red intente rutear a través de ese escenario simple.

Notificación remota basada en la calidad de la señal

Cuando se conectan dos routers, adosados o a través de una red SONET, la arquitectura OAM proporcionada cubre la detección de la mayoría de escenarios de fallas.

Normalmente, hay notificaciones locales y notificaciones remotas. Sin embargo, cuando un número elevado de errores BIP atraviesan un umbral (SD o SF, o B3-TCA), no se envía ninguna notificación remota para indicar que se ha producido esta condición. Por lo tanto, cuando utiliza la protección de Fast Re-Route de Multi Protocol Label Switching (MPLS), ningún disparador activa un switch de protección inmediato. El tráfico continúa en la lista negra hasta que se pierde tráfico suficiente para provocar una falla en las señales de mantenimiento de capa 2 en el enlace o en las relaciones de vecinos entre los pares de protocolo de gateway interior (IGP). A veces esto nunca ocurre y continúa chantajeando el tráfico.

Para abordar este escenario, CSCec85117 introduce el comando **pos action b3-ber prdi** en la estructura de comandos POS y SONET.

Este comando permite al operador configurar la interfaz para enviar un P-RDI cuando se ha cruzado el umbral B3. Esta opción le permite monitorear el link de extremo a extremo de manera óptima, independientemente de la topología. Si **pos delay triggers path** está habilitado en los routers, el comando **pos action b3-ber prdi** activa el link que se desactiva (y la correspondiente Fast ReRoute (FRR) o actualización de routing). Esto evita el efecto de agujero negro en los links degradados.

Para cambiar la sensibilidad de esta acción, ajuste el b3-tca como se muestra aquí:

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

El valor proporcionado es el componente exponencial para el cálculo de BER (por ejemplo, **pos threshold b3-tca 3** establece el B3-TCA como equivalente a una velocidad de 1x10^-3).

Información Relacionada

- Telcordia Information SuperStore
- Soporte Técnico y Documentación - Cisco Systems