

Acionadores SONET

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Eventos que desativam uma interface POS](#)

[Disparadores de nível de linha e seção](#)

[Acionadores de caminho](#)

[Resumo do comportamento da CLI dos disparadores de POS](#)

[Debate sobre alarmes SONET](#)

[Tratamento de Defeitos](#)

[Acionadores em ação](#)

[Por que usar disparadores?](#)

[Disparadores de SLAs e POS](#)

[Theorem](#)

[Postulados](#)

[Implantação de disparadores SONET](#)

[Rede SONET protegida: Nenhum APS nos roteadores](#)

[Rede SONET desprotegida internamente](#)

[Rede SONET protegida ou desprotegida](#)

[Rede DWDM protegida](#)

[Rede DWDM desprotegida](#)

[Roteadores conectados back-to-back](#)

[Notificação remota baseada na qualidade do sinal](#)

[Informações Relacionadas](#)

[Introduction](#)

Um gatilho é qualquer evento que cumpra a função de *causa* na relação causa-e-efeito em uma interface de SONET (Synchronous Optical Network, Rede Óptica Síncrona) no IOS. Às vezes, você pode usar o comando **pos delay triggers**. Em outras ocasiões, a Cisco recomenda que você não use o comando **pos delay triggers**, especialmente quando você tenta cumprir contratos de nível de serviço (SLAs) rígidos. Os provedores de serviços vendem níveis de serviço diferenciados com base em certos contratos. Os contratos tratam de como a rede roteia, protege ou prioriza o tráfego do cliente internamente. Esses comandos ajudam os provedores a sintonizar redes para atender a contratos de serviço.

Este documento examina os disparadores relacionados aos eventos de interface ativo e inativo. Este documento também explica como implantar o Packet Over SONET (POS) e considera os

SLAs e os tempos de convergência na Camada 3.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

Eventos que desativam uma interface POS

Esta seção descreve os eventos que desativam uma interface POS e lista os comandos relacionados.

Disparadores de nível de linha e seção

A lista de disparadores nesta seção refere-se aos *sistemas de transporte* GR-253-CORE *Synchronous Optical Network (SONET)*: Especificação de critérios genéricos comuns:

- Perda de Sinal da Seção (SLOS - Section Loss of Signal)—A especificação indica que você deve detectar não menos que 2,5us e não mais que 100us (6.2.1.1.1).
- Perda de quadro (SLOF) da seção—A especificação indica que você deve detectar isso em no mínimo 3 ms (ou 24 padrões de enquadramento com erros consecutivos) (6.2.1.1.2).
- Alarm Indication Signal - Line (AIS-L)—AIS-L deve ser enviado, quando apropriado, no prazo de 125 horas após a detecção. Um dispositivo deve detectar a recepção de AIS-L se o dispositivo vir 5 quadros consecutivos em que os bits 6,7 e 8 de K2 estão definidos como 111 (6.2.1.2.1).
- Signal Degrade Bit Error Rate (SD-BER)—SD-BER é um gatilho somente em interfaces com Automatic Protection Switching (APS) (vinculada ao cálculo B2 BER).
- Signal Failure Bit Error Rate (SF-BER)—SF-BER é um disparador para interfaces APS e não APS (ligadas ao cálculo de B2 BER).
- Remote Defect Indication - Line (RDI-L)—RDI-L não é um disparador para POS ou APS. (No entanto, RDI-L é um gatilho para MPLS FRR) (seção 5.3.3.1).

Para obter mais informações sobre as seções mencionadas nesta lista, consulte o site [Telcordia Information SuperStore](#) .

[Comandos relacionados](#)

O comando **pos delay triggers line *n*** mantém o LOS/LOF/AIS para *n* ms antes que o comando dispare a linha para baixo:

Se você configurar o comando sem nenhum valor numérico, o tempo de atraso será de 100 ms por padrão. Você pode usar disparadores de linha em qualquer interface POS que não seja APS. Não é possível usar disparadores de linha em interfaces que participam do APS, porque os disparadores de linha interferem na operação do APS. O comando **pos delay triggers line *n*** não permite que a linha caia no breve LOS que vem da engrenagem DWDM (Dense Wavelength Division Multiplexing) protegida internamente, desde o momento em que ocorre um switch de proteção DWDM interno. Se o defeito desaparecer durante o período de holdoff, é como se o defeito nunca tivesse ocorrido.

O comando **pos delay triggers line** mantém qualquer ação baseada no defeito (exceto para incrementar o contador do defeito) até que o período de holdoff especificado termine.

Se você não habilitar esse comando, o APS e o link para baixo dos defeitos SONET acima serão disparados imediatamente no Route Processor (RP).

[Acionadores de caminho](#)

Esses defeitos específicos de nível de PATH iniciam uma alteração de estado somente se você ativou o **caminho de disparos de atraso** na interface:

- AIS-P—Este defeito deve ser levantado dentro de 125 usec a partir da detecção do defeito que resulta no AIS-P. O PTE (Path Terminating Equipment, Equipamento de Terminação de Caminho) deve detectar esse defeito quando os bytes H1 e H2 para um caminho STS contêm todos 1s para 3 quadros consecutivos. Os caminhos concatenados precisam observar apenas os primeiros bytes H1 e H2. Para mais informações, ver seção 6.2.1.2.2 de R6-175 e R6-176.
- RDI-P—Se RDI-P estiver presente, o defeito deve ser detectado em 10 quadros. Ver 6.2.1.3.2 de R6-221.
- B3-TCA (Threshold Crossing Alarm, Alarmes de Cruzamento de Limites) para B3—Este alarme está ligado ao cálculo de IP (BIP) de Comunicações Síncronas Binárias (Bisync) B3.
- LOP-P (Perda de caminho do ponteiro) (se a versão do IOS incluir [CSCdx58021](#))—Consulte a seção 6.2.1.1.3 do GR-253.

Para obter mais informações sobre as seções mencionadas nesta lista, consulte o site [Telcordia Information SuperStore](#).

[Comando relacionado](#)

O comando **pos delay triggers path <msec>** *permite o disparo de link down em erros AIS-P, RDI-P e B3 excessivos*. Por padrão, o disparo de link-down para erros de caminho está desabilitado.

O comando também especifica um tempo de holdoff no intervalo de 0 a 511 ms (o padrão é 100ms). Os defeitos de disparo de caminho (AIS-P, RDI-P) que forem eliminados antes do fim do período de holdoff não causam disparo. Quando você não configurou explicitamente esse comando em uma interface POS, nenhuma ação resultará se os defeitos no nível PATH forem processados. Diferentemente dos disparadores de linha, as interfaces APS permitem

disparadores de caminho, porque os disparadores de caminho não interferem na atividade de nível de linha do APS. Os disparadores de caminho não podiam ser configurados com APS em versões anteriores ao Cisco IOS® Software Release 12.0(28)S. Os disparadores de caminho foram adicionados para acelerar o comportamento de link ativo/inativo das interfaces POS quando conectados a redes SONET. Isso permitiu uma convergência de Camada 3 mais rápida na presença de erros remotos.

Resumo do comportamento da CLI dos disparadores de POS

Esta tabela lista as condições dos disparadores de POS e os resultados associados:

Condição	Resultado
Se você não configurou nada explicitamente relacionado a disparadores POS.	Os disparadores de nível de linha são processados imediatamente.
Se você configurou o comando pos delay triggers line .	Os disparadores de nível de linha são processados após um atraso de 100 ms.
Se você configurou o comando pos delay triggers line x .	Os disparadores de nível de linha são processados após x msec, onde x está entre 0 e 511.
Se você não tiver configurado nada explicitamente relacionado aos disparadores de caminho.	Os acionadores de caminho não são processados e não farão com que nenhuma ação seja tomada.
Se você configurou o comando pos delay triggers path .	Os disparadores de nível de caminho são processados após um atraso de 100 ms.
Se você configurou o comando pos delay triggers path x .	Os disparadores de nível de caminho são processados após x msec, onde x está entre 0 e 511.

Debate sobre alarmes SONET

Os alarmes SONET que resultam de defeitos são mantidos por 10 segundos (10,5 +/-,5) depois que o defeito se apaga.

Tratamento de Defeitos

No IOS, as placas POS mudam seu estado de LINHA devido a disparadores diferentes, através de dois meios gerais para o processamento de defeitos. Embora isso dependa da configuração específica da interface (APS ou não APS), em geral há dois tipos de falhas:

- Gerenciado
- Não gerenciado

Você deve entender os termos específicos de tratamento de alarme que este documento usa:

- Defeito—A condição de falha que o hardware reconhece.
- Falha — Um defeito que foi encharcado para os ~2,5 segundos necessários e, em seguida, é relatado através das mensagens SONET-4-ALARM. Qualquer defeito que seja um gatilho não fica encharcado.
- Falhas não gerenciadas — Eventos como LOS, LOF, etc. São detectados pelo framer SONET por um conjunto definido de parâmetros e não exigem cálculo. Há um defeito presente e confirmado pelo hardware ou não há defeito. Falhas graves como essas, em geral, são tratadas por meio de interrupções. LOS, LOF, AIS-L e, em casos especiais, AIS-P e RDI-P são afirmados imediatamente. Eles dependem do framer e das regras definidas para detectar cada um desses defeitos. O efeito desses defeitos é imediato. No entanto, você pode instruir o roteador a adiar a asserção desse defeito como uma falha. Há dois temporizadores que determinam o valor de atraso, **pos delay triggers [caminho] | linha** e atraso da portadora. Estes são abordados posteriormente no documento.
- Alarmes gerenciados—Eventos como TCAs e cálculos SD/SF-BER. Eles exigem algum cálculo para determinar se estão presentes, se estão aumentando ou diminuindo, etc. Por exemplo, você não pode ter um LOS que aumente sua "LOS-ness" da perspectiva do roteador. No entanto, você pode ter um BER que esteja aumentando ou diminuindo; a ação tomada pode ser diferente. Falhas de software, como BER e TCA, precisam de algum cálculo, pois dependem de vários fatores, por exemplo, limiares que um usuário pode configurar, taxa de bits e número máximo de CVs de BIP (porque são diferentes para B1, B2 e B3). Essas falhas também demoram mais para ser detectadas, porque o hardware é pesquisado para os contadores BIP e também porque esses tipos de defeitos são graduais e acumulados ao longo do tempo. Também é verdade que, em geral, você não passa de 0 BIP direto para um sinal degradado (SD) ou uma falha de sinal (SF) sem algum outro tipo de falha física presente na rede. Esses defeitos são mais lentos quando comparados a falhas de hardware.

Aqui está uma abordagem generalizada dos cálculos básicos que descreve como calcular o BER:

Depois de cada reinício dos cálculos e até que BER_Period atinja Required_BER_Period (a janela de integração não está totalmente implantada), o algoritmo funciona estritamente como um integrando ou fazendo uma média:

- $BER_Period = BER_Period + 1 \text{ segundo.}$
- $Current_BIP = Current_BIP + BIP_new.$
- $Current_BER = Current_BIP/BER_Period.$

Depois que BER_Period alcançar Required_BER_Period (a janela de integração foi completamente implantada e começa a deslizar), o algoritmo funciona como um bucket vazado:

- $BER_Period = Required_BER_Period.$
- $Current_BIP = Current_BIP + BIP_new - Current_BER * 1 \text{ segundo.}$
- $Current_BER = Current_BIP/BER_Period.$

O Required_BER_Period é determinado somente com base na taxa de linha e no limite de BER configurado, seguindo os padrões (veja a figura 5-5, Critérios de tempo de início do switch, GR-253). No entanto, ela é menor que 1 segundo, nossa taxa de amostragem.

Assim, o BER_Period (janela de integração) se move com cada pesquisa e um novo BER é calculado com cada pesquisa. Se Current_BER alguma vez ultrapassar um limite definido,

levantamos o defeito apropriado imediatamente durante a mesma pesquisa ou intervalo de cálculo e mantemos a resposta mínima. Repetimos esses cálculos a cada segundo e verificamos se um dos três eventos ocorreu:

- BER ainda está dentro desse mesmo intervalo. Não há nova ação.
- O BER aumentou novamente e ultrapassou um limite SD ou SF (para B2). Sobe um novo alarme.
- O BER diminuiu abaixo de um limite de BER. Limpe o alarme.

Para a asserção de um TCA ou SD/SF, você precisa esperar apenas até que tenha ultrapassado um limite nesse intervalo de pesquisa respectivo. No momento do cálculo, verifique se Current_BER ultrapassou um limite e, se tiver, você pode fazer a asserção do alarme imediatamente através do software.

Isso é válido porque, se Current_BER é grande o suficiente para disparar o alarme inicialmente, a condição ainda é verdadeira no final do BER_Period. Isso se baseia na forma como os valores são definidos e comparados em relação à janela de cálculo.

Ao limpar um alarme, você precisa esperar até o final da janela de cálculo BER_Period. Isso serve para garantir que nenhum BIP novo seja acumulado durante a última parte da janela que possa mantê-lo acima de um limite.

Observação: de acordo com o GR-253, SD-BER e SF-BER estão vinculados estritamente à contagem de BIP B2. Os limiares padrão atuais são:

- Limites de BER—SF = $10e-3$ SD = $10e-6$
- Limiares de TCA—B1 = $10e-6$ B2 = $10e-6$ B3 = $10e-6$

Observação: as placas OC-48 Engine2 têm estes limiares padrão:

- Limites de BER—SF = $10e-4$ SD = $10e-6$
- Limiares de TCA—B1 = $10e-6$ B2 = $10e-6$ B3 = $10e-6$

Se você quiser que o acionador de caminho B3 TCA seja semelhante ao SF, o limite B3 deve ser definido para o mesmo limite, $10e-3$. Você pode fazer isso por meio do comando **pos threshold b3-tca 3** no prompt `router(config-if)#`.

Observação: como o intervalo de sondagem é de um segundo, esse é o tempo mínimo em que veremos e elevaremos o defeito TCA ou SD/SF. Além disso, devido à natureza acumulada do TCA/SD/SF, esses tipos de falhas são acompanhados por alguma outra falha quando ocorrem rapidamente em falhas típicas. Isso mantém um equilíbrio entre a utilização e o desempenho do processador do roteador. O intervalo de sondagem não pode ser configurado.

[Acionadores em ação](#)

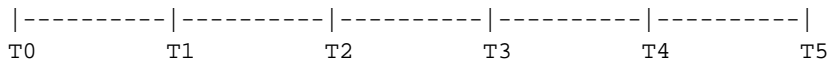
Esta seção fornece algumas informações de fundo para examinar a interação de alguns dos vários botões ajustáveis do usuário no IOS:

Os **disparadores de retardo pos [line comando | path]** atrasa brevemente a geração de relatórios e a ação de um defeito.

A linha disparadora de retardo POS é o tempo de espera antes de reagir a um alarme de linha. O padrão é reação imediata, o que significa **pós delay trigger line 0**. Se você configurar diretamente

pos delay trigger line sem nenhum valor, o valor padrão de 100ms será considerado. Isso permite uma resposta imediata ou atrasada, com base no efeito desejado. Com qualquer um desses configurados, o defeito não aparece como um alarme ativo até que o período de holdoff tenha terminado.

Cronograma:



Aqui:

- t0 — hora em que o defeito ocorre.
- t1—Hora em que o hardware detecta o defeito.
- t2 — Hora em que o defeito é relatado como uma falha.
- t2-t3—Tempo que é suspenso para qualquer acionador configurado.
- t3-t4 — Tempo pelo qual você espera devido ao atraso da portadora.
- t4—Hora em que a interface realmente fica inativa no IOS.
- t5—Hora em que qualquer adjacência para um protocolo de roteamento é desativada.

Examine a linha do tempo para observar como ajustar os diferentes botões para obter vários resultados.

O comando **post delay triggers** afeta a duração entre t2 e t3, e, na verdade, oculta o defeito do IOS, até que o período de holdoff termine. Claro, se o defeito for eliminado antes de você alcançar t3, nada ocorrerá, e é como se nada tivesse acontecido. O valor padrão para disparadores de linha e de caminho é 100 ms e o intervalo é de 0 a 511 ms. Os disparadores de caminho não estão ativados (em outras palavras, eles não tomam nenhuma ação) a menos que o **caminho de disparadores de atraso pós** seja configurado primeiro. **pos delay trigger path** é o tempo de espera antes de reagir a um alarme de caminho. O padrão é nenhuma reação. Se você configurar diretamente o **caminho do disparador de atraso pos** sem qualquer valor, o valor padrão 100ms será atribuído automaticamente. Isso inclui AIS-P, RDI-P e B3-TCA. Essa funcionalidade foi adicionada por meio do [CSCds82814](#) (cerca de 12.0(15.5)S/ST).

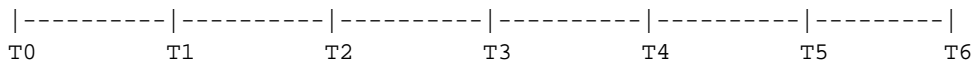
O retardo da portadora é o tempo de espera entre o final do tempo de espera do retardo do POS e desativará a interface do IOS. O padrão é 2000 ms. O atraso da portadora é o tempo entre t3 (quando o IOS se torna consciente de uma falha) e t4 (quando a interface fica inativa). Por padrão, ela é definida como 2 segundos e pode ser configurada para valores msec. Como a linha do tempo indica, é uma função aditiva sobre os temporizadores holdoff de nível SONET. Ele se comporta da mesma forma que os disparadores de POS - se o alarme desaparecer antes do fim do período de holdoff, a interface não é desativada. No entanto, há aqui um problema. O temporizador de devolução SONET não elimina o defeito antes que o atraso da portadora seja ativado, a menos que o atraso da portadora seja grande (bem mais de 10 segundos). Isso resulta em uma situação em que o atraso da portadora é quase sempre ativado e, portanto, deve ser considerado um pouco pequeno quando implantado com interfaces POS. O atraso da portadora também é adicionado depois que o alarme é cancelado, antes que a interface seja declarada ativa também. Portanto, você pode contar o valor do atraso da portadora duas vezes antes que a interface volte a funcionar.

Com algumas interfaces e mídia física, isso é útil. No entanto, com interfaces POS, há vários disparadores e temporizadores que você pode usar e combinados para criar o efeito desejado, sem retardo de portadora assumindo uma função tão importante. Um valor de atraso da portadora

de 0 a 8 ms é um bom ponto de partida para os clientes considerarem quando testarem esses botões sozinhos. Em geral, uma boa estratégia é usar o comando **pos delay triggers** para absorver qualquer problema e fornecer o efeito holdoff desejado. O atraso da portadora pode ser mantido pequeno para minimizar seu impacto.

O temporizador de devolução SONET mencionado acima é definido em 10 segundos (+/- .5sec) e é exigido pelo GR-253 para garantir que não ocorra um período de sincronização inferior a 10 segundos. O temporizador começa depois que o defeito é eliminado. O temporizador será redefinido se outro evento de defeito ocorrer antes que a janela do temporizador expire.

Cronograma:



Aqui:

- t0—O defeito é limpo.
- t0 — O temporizador de débito é iniciado.
- t4—t0 + 10sec (portanto, a falha deve ser eliminada se não ocorrerem novos defeitos entre t0 e t4).

Se um evento ocorrer antes de t4, (digamos) em t2 (pode ser outro defeito ou uma nova ocorrência do mesmo tipo de defeito), o temporizador será interrompido até que esse novo defeito seja eliminado. Em t3, o temporizador começa novamente, quando não há defeitos ativos e conta por aproximadamente 10 segundos. Se nenhum evento novo for encontrado, limpe o alarme em t5 e inicie o temporizador de atraso da portadora. Quando o atraso da portadora tiver sido cancelado em t6, ative a interface novamente.

Essas informações devem permitir que o cliente entenda mais claramente como as interfaces POS reagem a várias condições SONET/SDH. Isso permite que o equipamento seja configurado com mais precisão de acordo com o comportamento pretendido pelo cliente.

[Por que usar disparadores?](#)

Esta seção explica quando você deve usar os **disparadores de retardo pos [line | path]** e quando você não deve usá-lo.

Aqui estão os cenários em que você não deve usar os **disparadores de retardo pos**. Há vários cenários:

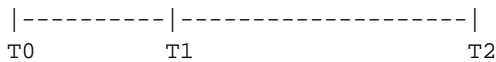
- Não é possível usar disparadores de linha com interfaces configuradas para APS. Versões anteriores ao Cisco IOS Software Release 12.0(28)S não permitiam nem mesmo o uso de disparadores de caminho.
- Quando você explicitamente não deseja que os defeitos de nível de caminho desativem a interface, não poderá usar esses disparadores.
- Quando você deseja que os disparadores de nível de linha desativem a interface sem atraso, não é possível usar esse comando.

Aqui estão os cenários em que você pode usar o comando **pos delay triggers**:

- Quando quiser interromper temporariamente o efeito de um defeito no nível da linha.
- Para habilitar a capacidade dos defeitos de nível de PATH de desativar a interface imediatamente.
- Para habilitar defeitos de nível de caminho para desativar a interface, mas com alguma separação incluída.

Disparadores de SLAs e POS

Examine esta linha do tempo:



- Tempo $t=0$ (t_0)—Quando o defeito é detectado.
- Tempo t_2 — O tempo de restauração do SLA necessário.
- Tempo t_1 —Qualquer holdoff do comando **pos delay triggers** configurado (o padrão para LINE é 0 e o padrão para PATH não está ativado).
- X é o valor holdoff (então $X =$ o valor de t_1).
- Y é o tempo que a Camada 3 leva para restaurar o serviço.

Theorem

Às vezes, você pode usar o comando **pos delay triggers**, enquanto outras vezes, você não pode, especialmente quando tenta cumprir SLAs (Service Level Agreements, contratos de nível de serviço) rigorosos.

Postulados

- Se $Y > (t_2 - t_1)$ para qualquer valor de t_1 , um holdoff não é uma boa ideia porque, se você configurar qualquer holdoff, você não poderá atender ao SLA.
- Se $Y \leq (t_2 - t_1)$, você pode considerar a implementação de um holdoff. Se a duração da falha for menor do que $(t_1 - t_0)$, você pode adiar porque não precisa utilizar os recursos do roteador e pode atender ao SLA desejado. Se o defeito persistir no tempo t_1 passado, você ainda poderá atender ao SLA, mesmo que perca algum tempo antes de iniciar a restauração no nível IP.

Você deve ter algum conhecimento sobre a rede de transporte subjacente e os tempos de convergência da rede de Camada 3, para conhecer os valores que você pode usar nessas fórmulas. Você também precisa executar alguns testes.

Veja como os acionadores funcionam:

- O comando **pos delay triggers line n** mantém o LOS/LOF/AIS para n ms antes que o comando dispare a linha para baixo. O valor padrão é 100ms. Você pode usar esse comando em qualquer interface POS que não seja APS. O comando **pos delay triggers line n** não permite que a linha caia no breve LOS que vem do equipamento DWDM protegido internamente, do momento em que ocorre um switch de proteção DWDM interno. Se o defeito desaparecer durante o período de holdoff, é como se o defeito nunca tivesse ocorrido.

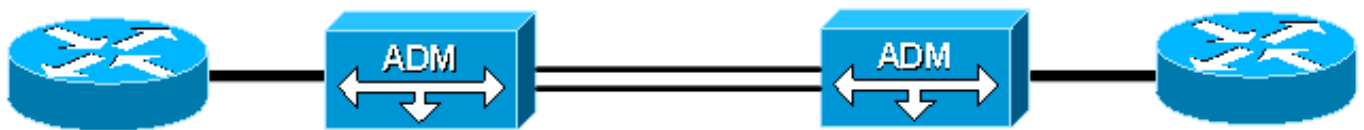
- O comando **pos delay triggers line** suspenderá qualquer ação baseada no defeito (exceto para incrementar o contador de defeito), até que o período de holdoff especificado termine. Se você não habilitar esse comando, APS e link inativo serão disparados imediatamente no RP.

Implantação de disparadores SONET

Esta seção descreve a implantação de disparadores SONET.

Rede SONET protegida: Nenhum APS nos roteadores

Figura 1: Rede SONET protegida internamente



A rede SONET tem proteção interna, o que significa que uma falha dentro da rede SONET aciona algum switch de proteção para restaurar o serviço muito rapidamente. Portanto, você precisa considerar se deseja desativar a interface e notificar a Camada 3. Na maioria dos casos, quando um switch de proteção ocorre dentro da rede SONET, os roteadores veem uma breve linha ou AIS de caminho enquanto a rede executa a ação restauradora. No entanto, isso ocorrerá somente se a falha estiver a um salto de cada roteador. A rede SONET pode possivelmente ser composta por vários NEs de diâmetro, ou o roteador vê falhas de LINE apenas como falhas de PATH. Nesse caso, considere os disparadores de nível de linha e caminho se quiser uma separação.

Para tomar essa decisão, você precisa entender o custo associado com ambas as abordagens. Como operador de rede, você deve considerar estas perguntas:

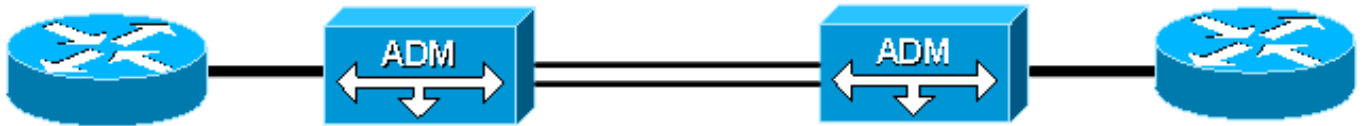
- A rede converge com rapidez suficiente? Caso contrário, esta abordagem não é adequada.
- Qual é o impacto do roteamento em torno de tal falha? O impacto é tão grande no roteador que o desempenho cai abaixo de um nível aceitável?

Em última análise, você precisa decidir se pode ignorar um possível acerto de ~60 ms ou se prefere rotear em torno de um evento desse tipo. Se você puder ignorar o acerto, será necessário identificar o tamanho de um "fator de enganação" a ser adicionado, pois, você não deseja manter esse defeito apenas para esperar alguns milissegundos a mais e, portanto, atrasar a ação corretiva.

Nesse cenário, **os disparadores de atraso de pos e caminho** provavelmente são suficientes. Além disso, considere valores de pelo menos 60 ms se uma separação for justificada. Se a rede for ampla o suficiente e você quiser tomar medidas imediatas em defeitos de linha e de nível de caminho, não será necessário configurar disparadores de nível de linha. No entanto, você precisa configurar o **caminho de disparadores de retardo pos** com um valor 0 para permitir o processamento imediato de defeitos de nível de PATH.

Rede SONET desprotegida internamente

Figura 2: Rede SONET interna desprotegida

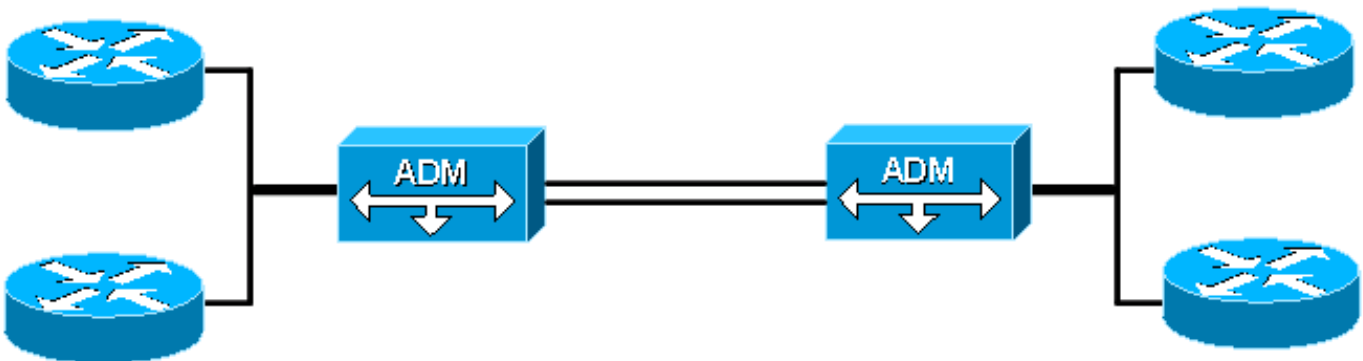


Em uma rede SONET desprotegida, você executa os mesmos riscos que no primeiro cenário, além de mais alguns. Se a rede for grande o suficiente, os roteadores potencialmente nunca poderão ver um defeito de nível de LINHA em caso de falha, pois os defeitos são todos filtrados. Os roteadores podem ver defeitos no nível de PATH no fluxo para cima e para baixo. Dessa forma, em algumas situações, em que ocorre uma falha na rede, o roteador vê apenas eventos de nível de PATH e não há continuidade fim-a-fim entre os roteadores. Pior ainda, nenhuma restauração ocorre no nível SONET para corrigir essa situação.

Nesse cenário, você deve configurar os disparadores de caminho simplesmente para permitir que os roteadores em cada extremidade tomem medidas quando os roteadores encontrarem um defeito de caminho, mesmo que os roteadores não queiram nenhum efeito de holdoff. Quando você configurou os disparadores de caminho, como um operador de rede, você deve verificar se é melhor interromper ou disparar uma restauração de Camada 3.

Rede SONET protegida ou desprotegida

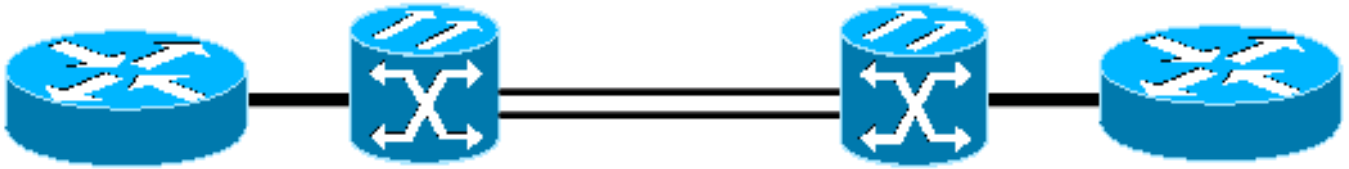
Figura 3: Rede SONET interna desprotegida



No Cisco IOS Software Release 12.0(28)S, você pode ativar disparadores PATH em circuitos APS. Quando você implanta APS nos roteadores locais ou remotos, um switch APS faz com que os roteadores remotos de Trabalho e Proteção vejam um breve defeito de nível de caminho. Com um pequeno valor de disparo, as interfaces ficam inativas e essa situação não é desejável. Uma interface que fica inativa atrasa a restauração do serviço que já está em andamento. Uma falha momentânea que ocorre na nuvem também pode atrasar a restauração do serviço. No entanto, a ocorrência de um erro de nível de PATH persistente indica que a proteção do circuito (na rede ou na extremidade distante) não conseguiu restaurar a conectividade. Nesse caso, os roteadores APS devem agir e iniciar a reconvergência de roteamento. Você pode configurar valores de atraso do disparador de caminho de ≥ 100 ms. Com essa configuração, quando ocorre um erro persistente na rede SONET ou na extremidade remota, os roteadores levam as duas interfaces APS para um estado de link inativo. Portanto, os roteadores iniciam um reroteamento e restauração mais rápidos do serviço.

Rede DWDM protegida

Figura 4: Rede DWDM protegida



Neste cenário, não precisamos usar disparadores de caminho, pois a rede DWDM não participa no nível de protocolo SONET. O roteador detecta qualquer falha no nível SEÇÃO ou LINHA.

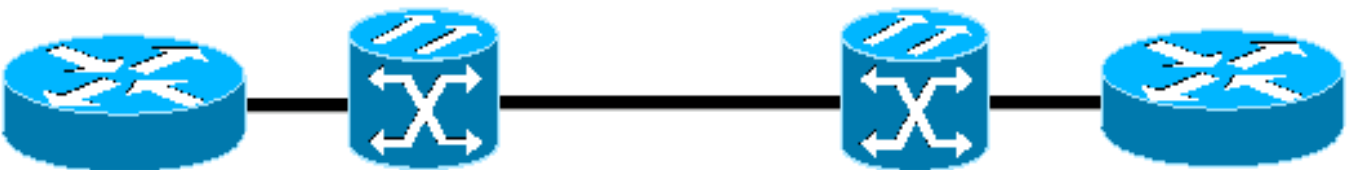
Novamente, como a rede DWDM está protegida internamente, uma falha interna da rede faz com que a restauração ocorra em breve. O roteador normalmente vê um LOS, LOF ou uma intermitência de erros de BIP muito breve.

Portanto, você só precisa decidir se uma separação é desejável nesta rede.

O comando **pos delay triggers line** é suficiente nessa situação, se você escolher um atraso.

Rede DWDM desprotegida

Figura 5: Rede DWDM desprotegida

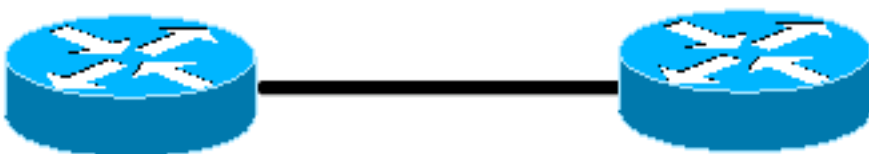


Com uma rede DWDM desprotegida no transporte, você precisa resolver qualquer falha dentro dos roteadores. Nessa situação, a configuração padrão permitiria uma resposta imediata a quaisquer falhas vistas em qualquer roteador porque o DWDM não participa do protocolo SONET. Se desejar esse efeito, a configuração padrão de sem disparadores POS configurados é apropriada.

Se você precisar de alguma suspensão, o comando **pos delay triggers line** é suficiente para fornecer essa funcionalidade.

Roteadores conectados back-to-back

Figura 6 - Roteadores conectados back-to-back



Dois roteadores conectados back-to-back entre duas interfaces POS devem operar como no último cenário. Você pode ver falhas imediatamente em qualquer roteador, pois não há nenhum

equipamento intermediário que opere na sobrecarga SONET ou termine qualquer parte do sinal de nível SONET.

Uma situação interessante é quando R1 vê S-LOS e R2 vê L-RDI e P-RDI, já que R1 é LTE (Line-Terminating Equipment, Equipamento de terminação de linha) e PTE (Path-Terminating Equipment, Equipamento de terminação de caminho). Como o L-RDI despermite explicitamente qualquer ação resultante a ser tomada após o recebimento, o R2 não descarta a interface como resultado. Esse problema pode potencialmente levar a uma situação em que uma interface de R1 está inativa, mas a interface de R2 ainda está ativa e encaminha o tráfego. É claro que qualquer manutenção de atividade da camada 2 (como o High-Level Data Link Control (HDLC) fornece) expira e declara o link inativo, normalmente em 30 segundos, com base nos temporizadores configurados. No entanto, vários operadores desabilitam essas manutenções de atividade da Camada 2 e não podem impedir essa situação. Para resolver esse problema, você pode adotar várias abordagens, e cada abordagem trata disso de uma perspectiva diferente, como explicado aqui:

- Ativar os disparadores de caminho—Como o P-RDI ativa uma interface com os disparadores de caminho ativados, você pode usar esse método para causar uma resposta rápida e descartar a interface. O ponto interessante a observar é que L-RDI mascara o P-RDI em operação normal de acordo com o GR-253. À medida que os disparadores POS são tratados no nível de defeito, os disparadores são processados antes da máscara de alarme e a interface ainda cai de acordo com o tempo de atraso configurado.
- Ativar keepalives da camada 2—Esta opção faz com que a interface em R2 exceda o tempo limite após 3 keepalives terem sido perdidos. Geralmente, esse é um total de 30 segundos (3x10) e a Cisco geralmente não recomenda essa opção como uma ferramenta para ajustar a convergência de link rápido.
- Ativar um protocolo de roteamento link-state—Quando a interface em R1 é desativada devido ao S-LOS, uma mensagem de link state é enviada imediatamente. Mesmo que a interface em R2 ainda possa estar ativa, quando a mensagem de estado do link é recebida em toda a área, o SPF é executado e o link é removido da topologia porque o link falha na verificação de conectividade bidirecional. Isso evita que a rede tente rotear através desse cenário simplex.

[Notificação remota baseada na qualidade do sinal](#)

Quando você conecta dois roteadores, back-to-back ou através de uma rede SONET, a arquitetura OAM fornecida cobre a detecção da maioria dos cenários de falha.

Geralmente, há notificações locais e notificações remotas. No entanto, quando um número elevado de erros de BIP atravessa um limite (SD ou SF, ou B3-TCA), nenhuma notificação remota é enviada para indicar que essa condição ocorreu. Assim, quando você emprega a proteção de Rota Rápida MPLS (Multi Protocol Label Switching), nenhum disparador ativa um switch de proteção imediata. O tráfego continua a ser bloqueado até que o tráfego suficiente seja perdido para causar uma falha dos keepalives da Camada 2 no link ou nas relações de vizinhos entre os peers do Interior Gateway Protocol (IGP). Às vezes isso nunca ocorre e continua a fazer buracos no tráfego.

Para lidar com esse cenário, o [CSCec85117](#) apresenta o comando **pos action b3-ber prdi** à estrutura de comandos POS e SONET.

Esse comando permite que o operador configure a interface para enviar um P-RDI quando o

limite B3 tiver sido ultrapassado. Essa opção permite que você monitore o link de ponta a ponta da maneira ideal, independentemente da topologia. Se o **caminho de disparo de retardo pos** estiver ativado nos roteadores, o comando **pos action b3-ber prdi** ativará o link que fica inativo (e a **Rota Rápida (FRR - Fast ReRoute)** ou **atualização de roteamento correspondente**). Isso evita o efeito do buraco negro em links degradados.

Para alterar a sensibilidade desta ação, ajuste o b3-tca conforme mostrado aqui:

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

O valor fornecido é o componente exponencial para o cálculo do BER (por exemplo, **pos threshold b3-tca 3** define o B3-TCA como equivalente a uma taxa de 1×10^{-3}).

[Informações Relacionadas](#)

- [Telcordia Information SuperStore](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)