Trigger SONET

Sommario

Introduzione

Un trigger è un evento che svolge il ruolo di *causa* nella relazione causa-effetto in un'interfaccia SONET (Synchronous Optical Network) in IOS. A volte è possibile utilizzare il comando **pos delay triggers**. In altri casi, Cisco consiglia di non utilizzare il comando **pos delay triggers**, in particolare quando si tenta di soddisfare i severi accordi sui livelli di servizio (SLA). I fornitori di servizi vendono livelli di servizio differenziati in base a determinati accordi. Gli accordi riguardano il modo in cui la rete instrada internamente, protegge o assegna priorità al traffico del cliente. Questi comandi consentono ai provider di ottimizzare le reti per soddisfare i contratti di assistenza.

In questo documento vengono esaminati i trigger relativi agli eventi di interfaccia su e giù. Questo documento spiega anche come distribuire il POS (Packet Over SONET) e prende in considerazione gli SLA e i tempi di convergenza sul layer 3.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Eventi che interrompono un'interfaccia POS

In questa sezione vengono descritti gli eventi che bloccano un'interfaccia POS e vengono elencati i comandi correlati.

Trigger a livello di sezione e di linea

L'elenco dei trigger in questa sezione fa riferimento ai *sistemi di trasporto* GR-253-CORE *Synchronous Optical Network (SONET):* Specifica *Common Generic Criteria*:

- Perdita di segnale di sezione (SLOS, Section Loss of Signal) - La specifica indica che è necessario rilevare un valore non inferiore a 2,5 us e non superiore a 100 us (6.2.1.1.1).
- Perdita di fotogramma (SLOF) nella sezione - La specifica indica che è necessario rilevare questa condizione entro un minimo di 3 ms (o 24 pattern di frame errati consecutivi) (6.2.1.1.2).
- Segnale di indicazione di allarme - Linea (AIS-L): l'AIS-L deve essere inviato quando appropriato, entro 125 usc dal rilevamento. Un dispositivo deve rilevare la ricezione di AIS-L se vede 5 fotogrammi consecutivi in cui i bit 6,7 e 8 di K2 sono impostati su 111 (6.2.1.2.1).
- Signal Degrade Bit Error Rate (SD-BER): SD-BER è un trigger solo sulle interfacce con Automatic Protection Switching (APS) (collegato al calcolo BER B2).
- Frequenza errori bit segnale (SF-BER): SF-BER è un trigger per entrambe le interfacce APS e non APS (collegato al calcolo BER B2).
- RDI-L (Remote Defect Indication - Line) - RDI-L non è un trigger per POS o APS. (Tuttavia, RDI-L è un trigger per MPLS FRR) (sezione 5.3.3.1).

Per ulteriori informazioni sulle sezioni menzionate in questo elenco, visitare il sito Web Telcordia Information SuperStore .

Comandi correlati

Il comando **pos delay triggers line *n*** disattiva LOS/LOF/AIS per n ms prima che il comando attivi la riga verso il basso:

Se si configura il comando senza alcun valore numerico, il tempo di ritardo predefinito è 100 ms. È possibile utilizzare i trigger di linea su qualsiasi interfaccia non APS POS. Non è possibile utilizzare i trigger di linea sulle interfacce che partecipano ad APS, poiché i trigger di linea interferiscono con l'operazione APS. Il comando **pos delay triggers line *n*** non consente alla riga di scendere sulla breve perdita generata dall'ingranaggio DWDM (Dense Wavelength-Division Multiplexing) protetto internamente, dal momento in cui si verifica uno switch di protezione DWDM interno. Se il difetto viene eliminato durante il periodo di sospensione, è come se il difetto non si fosse mai verificato.

Il comando **pos delay triggers line** blocca qualsiasi azione basata sul difetto (tranne per incrementare il contatore difetti) fino al termine del periodo di sospensione specificato.

Se non si abilita questo comando, l'APS e il collegamento verso il basso a partire dai suddetti difetti del SONET vengono attivati immediatamente nel Route Processor (RP).

Trigger percorso

Questi difetti specifici del livello PATH avviano una modifica dello stato solo se è stato abilitato **pos delay triggers path** sull'interfaccia:

- AIS-P: questo difetto deve essere rilevato entro 125usec dal rilevamento del difetto che determina l'AIS-P. Il PTE (Path Terminating Equipment) deve rilevare questo difetto quando i byte H1 e H2 di un percorso STS contengono tutti gli 1 per 3 frame consecutivi. I percorsi concatenati devono rispettare solo i primi byte H1 e H2. Per ulteriori informazioni, vedere il paragrafo 6.2.1.2.2 di R6-175 e R6-176.
- RDI-P - Se RDI-P è presente, il difetto deve essere rilevato entro 10 fotogrammi. Cfr. il punto 6.2.1.3.2 di R6-221.
- B3-TCA (Threshold Crossing Alarms) per B3: questo allarme è legato al calcolo B3 Binary Synchronous Communications (Bisync) IP (BIP).
- LOP-P (Path Loss of Pointer) (se la versione IOS include CSCdx58021)—Vedere la sezione 6.2.1.1.3 di GR-253.

Per ulteriori informazioni sulle sezioni menzionate in questo elenco, visitare il sito Web Telcordia Information SuperStore .

Comando correlato

Il comando **pos delay triggers *<msec>*** abilita l'attivazione del collegamento in caso di errori AIS-P, RDI-P e B3 eccessivi. Per impostazione predefinita, l'attivazione link-down per gli errori di percorso è disabilitata.

Il comando specifica anche un tempo di interruzione tra 0 e 511 ms (il valore predefinito è 100 ms). I difetti di attivazione del percorso (AIS-P, RDI-P) che vengono eliminati prima della fine del periodo di sospensione non causano l'attivazione. Se questo comando non è stato configurato in modo esplicito su un'interfaccia POS, non verrà eseguita alcuna azione se vengono elaborati i difetti del livello PATH. A differenza dei trigger di linea, le interfacce APS consentono i trigger di

percorso, in quanto i trigger di percorso non interferiscono con l'attività di livello di linea di APS. La configurazione dei trigger di percorso con APS non è consentita nelle versioni precedenti al software Cisco IOS® versione 12.0(28)S. Sono stati aggiunti trigger di percorso per velocizzare il comportamento di collegamento verso l'alto e verso il basso delle interfacce POS quando collegate a reti SONET. Questo ha consentito una convergenza più rapida sul layer 3 in presenza di errori remoti.

Riepilogo del comportamento CLI dei trigger POS

In questa tabella vengono elencate le condizioni dei trigger POS e i risultati associati:

Condizione	Risultato
Se non è stato configurato alcun elemento correlato in modo esplicito ai trigger POS.	I trigger a livello di linea vengono elaborati immediatamente.
Se è stato configurato il comando **pos delay triggers line**.	I trigger a livello di linea vengono elaborati dopo un ritardo di 100 ms.
Se è stato configurato il comando **pos delay triggers riga *x***.	I trigger a livello di linea vengono elaborati dopo *x* msec, dove *x* è compreso tra 0 e 511.
Se non è stato configurato alcun elemento correlato in modo esplicito ai trigger Path.	I trigger di percorso non vengono elaborati e non determineranno l'esecuzione di alcuna azione.
Se è stato configurato il comando **pos delay triggers path**.	I trigger a livello di percorso vengono elaborati dopo un ritardo di 100 ms.
Se è stato configurato il comando **pos delay triggers path *x***.	I trigger a livello di percorso vengono elaborati dopo *x* msec, dove *x* è compreso tra 0 e 511.

Annullamento degli allarmi SONET

Gli allarmi SONET risultanti da difetti vengono mantenuti attivi per 10 secondi (10,5 +-.5) dopo la cancellazione del difetto.

Gestione dei difetti

In IOS, le schede POS cambiano il loro stato LINE a causa di diversi trigger, attraverso due mezzi generali per l'elaborazione dei difetti. Sebbene ciò dipenda dalla configurazione specifica dell'interfaccia (APS o non APS), in generale vi sono due tipi di errori:

- Gestito
- Non gestito

Ènecessario comprendere i termini specifici della gestione degli allarmi utilizzati nel presente

documento:

- Difetto (Defect) - Condizione di errore riconosciuta dall'hardware.
- Guasto: un difetto che è stato assorbito per circa 2,5 secondi e viene quindi segnalato tramite i messaggi SONET-4-ALARM. Qualunque difetto che sia un grilletto non si impregna.
- Guasti non gestiti: eventi quali perdita, LOF, ecc. Vengono rilevati dal framer SONET da un insieme definito di parametri e non richiedono alcun calcolo. È presente un difetto dichiarato dall'hardware oppure non esiste alcun difetto. I guasti gravi come questi, in generale, vengono gestiti tramite interrupt. LOS, LOF, AIS-L e, in casi speciali, AIS-P e RDI-P vengono attivati immediatamente. Questi difetti dipendono dal framer e dalle regole definite per rilevarli. L'effetto di questi difetti è immediato. Tuttavia, è possibile indicare al router di ritardare l'asserzione di questo difetto come se fosse un errore. Il valore del ritardo è determinato da due timer, **pos delay triggers [percorso | linea]** e ritardo vettore. Tali aspetti sono trattati più avanti nel documento.
- Allarmi gestiti: eventi quali TCA e calcoli SD/SF-BER. Questi richiedono alcuni calcoli per determinare se sono presenti, sono in aumento o in diminuzione, ecc. Ad esempio, non è possibile avere un errore di perdita che ne aumenti la "gravità" dal punto di vista del router. Tuttavia, è possibile che il valore di BER sia in aumento o in diminuzione; l'azione intrapresa può essere diversa. Gli errori soft, come BER e TCA, richiedono alcuni calcoli, perché dipendono da una serie di fattori, ad esempio soglie che un utente può configurare, velocità bit e numero massimo di CV BIP (in quanto sono diversi per B1, B2 e B3). Questi guasti richiedono anche più tempo per essere rilevati, perché l'hardware viene sottoposto a polling per i contatori BIP, e anche perché questi tipi di difetti sono di natura graduale e accumulati nel tempo. È anche vero che in generale non si va da 0 BIP direttamente a un degrado del segnale (SD) o errore del segnale (SF) senza qualche altro tipo di errore grave presente nella rete. Questi difetti sono più lenti rispetto ai guasti gravi.

Di seguito è riportato un approccio generalizzato ai calcoli di base che descrive come calcolare il tasso di errore relativo al produttore:

Dopo ogni riavvio dei calcoli e finché BER_Period non raggiunge Required_BER_Period (la finestra di integrazione non è completamente distribuita), l'algoritmo funziona strettamente come un algoritmo di integrazione o di calcolo della media:

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

Quando BER_Period raggiunge Required_BER_Period (la finestra di integrazione è stata completamente distribuita e inizia a slittare), l'algoritmo funziona come un bucket di perdita 1:

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

Required_BER_Period viene determinato solo in base alla velocità della linea e alla soglia BER configurata, seguendo gli standard (vedere la figura 5-5, Switch Initiation Time Criteria, GR-253). Tuttavia, è inferiore a 1 secondo, la nostra frequenza di campionamento.

Pertanto, BER_Period (finestra di integrazione) si sposta con ogni polling e viene calcolato un nuovo BER con ogni polling. Se il valore di Current_BER supera un limite definito, viene generato immediatamente il difetto appropriato durante lo stesso intervallo di polling o calcolo e la risposta

viene mantenuta al minimo. Questi calcoli vengono ripetuti ogni secondo e viene verificato se si è verificato uno dei tre eventi seguenti:

- La tecnologia BER rientra ancora nello stesso intervallo. Nessuna nuova azione.
- Il BER è aumentato ancora e ha superato la soglia SD o SF (per B2). Alza un nuovo allarme.
- Il valore di BER è sceso al di sotto della soglia di BER. Cancella l'allarme.

Per l'asserzione di un TCA o di un SD/SF, è necessario attendere solo fino al superamento di un limite al rispettivo intervallo di polling. Al momento del calcolo, controllare se Current_BER ha superato una soglia e, in caso affermativo, è possibile procedere e attivare immediatamente l'allarme tramite il software.

Ciò è valido perché, se Current_BER è abbastanza grande da attivare inizialmente l'allarme, la condizione è ancora vera alla fine di BER_Period. Questo si basa sul modo in cui i valori vengono definiti e confrontati in relazione alla finestra di calcolo.

Quando si cancella un avviso, è necessario attendere la fine della finestra di calcolo BER_Period. In questo modo, durante l'ultima parte della finestra non verranno accumulati nuovi PIF che potrebbero mantenere la soglia.

Nota: secondo il GR-253, SD-BER e SF-BER sono entrambi strettamente legati al conteggio BIP B2. Le soglie predefinite correnti sono:

- Soglie BER: SF = 10e-3 SD = 10e-6
- Soglie TCA—B1 = 10e-6 B2 = 10e-6 B3 = 10e-6

Nota: le schede OC-48 del motore 2 hanno le seguenti soglie predefinite:

- Soglie BER: SF = 10e-4 SD = 10e-6
- Soglie TCA—B1 = 10e-6 B2 = 10e-6 B3 = 10e-6

Se si desidera che il trigger del percorso TCA B3 agisca in modo simile a SF, la soglia B3 deve essere impostata sulla stessa soglia, 10e-3. A tale scopo, è possibile utilizzare il comando **pos threshold b3-tca 3** al prompt `router(config-if)#`.

Nota: poiché l'intervallo di polling è di un secondo, questo è il tempo minimo in cui noteremo e solleveremo il difetto TCA o SD/SF. Inoltre, a causa della natura accumulata di TCA/SD/SF, questi tipi di guasti sono accompagnati da altri guasti quando si verificano rapidamente nei guasti tipici. In questo modo si mantiene un equilibrio tra l'utilizzo del processore del router e le prestazioni. Impossibile configurare l'intervallo di polling.

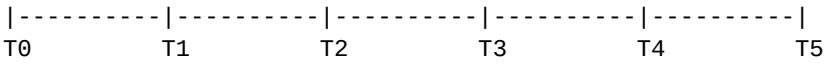
Trigger in azione

In questa sezione vengono fornite alcune informazioni di base per esaminare l'interazione di alcuni dei vari cursori regolabili dall'utente in IOS:

I **trigger di ritardo POS [riga | percorso]** ritarda brevemente la segnalazione e l'azione di un difetto.

La linea di attivazione del ritardo POS è il tempo di attesa prima di reagire a un allarme di linea. Per impostazione predefinita, la reazione è immediata, ovvero la **linea di attivazione del ritardo pos *0*** . Se si configura direttamente la **riga trigger ritardo pos** senza alcun valore, viene preso in considerazione il valore predefinito di 100 ms. Ciò consente una risposta immediata o ritardata, in base all'effetto desiderato. Con una di queste configurazioni, il difetto non viene visualizzato come allarme attivo fino al termine del periodo di sospensione.

Sequenza temporale:



Qui:

- t0 - Ora in cui si verifica il difetto.
- t1 - Ora in cui l'hardware rileva il difetto.
- t2 - Ora in cui il difetto viene segnalato come errore.
- t2-t3 - Tempo che viene sospeso per qualsiasi trigger configurato.
- t3-t4 - Tempo di attesa dovuto al ritardo della portante.
- t4 - Ora in cui l'interfaccia viene abbassata in IOS.
- t5 - Tempo in cui qualsiasi adiacenza di un protocollo di routing viene interrotta.

Esaminate la linea temporale per osservare come modificare le diverse manopole per ottenere diversi risultati.

Il comando **post delay triggers** influisce sulla durata tra t2 e t3 e in effetti nasconde il difetto in IOS fino al termine del periodo di sospensione. Naturalmente, se il difetto viene eliminato prima di raggiungere t3, non accade nulla, ed è come se nulla fosse accaduto. Il valore predefinito per i trigger line e Path è 100 ms e l'intervallo è compreso tra 0 e 511 ms. I trigger di percorso non sono abilitati (in altre parole, non eseguono alcuna azione) a meno che il **percorso dei trigger di ritardo pos** non sia stato prima configurato. **percorso di attivazione ritardo pos** è il tempo di attesa prima della reazione a un allarme percorso. Il valore di default è nessuna reazione. Se si configura direttamente il **percorso di attivazione del ritardo pos** senza alcun valore, il valore predefinito 100ms verrà assegnato automaticamente. Sono inclusi AIS-P, RDI-P e B3-TCA. Questa funzionalità è stata aggiunta tramite CSCds82814 (circa 12.0(15.5)S/ST).

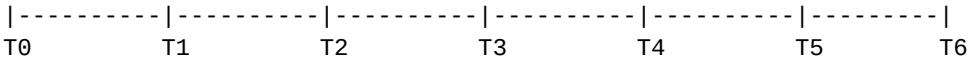
Il ritardo vettore è il tempo di attesa tra la fine del tempo di attesa del ritardo POS e l'interruzione dell'interfaccia IOS. Il valore predefinito è 2000 msec. Il ritardo vettore è il tempo tra t3 (quando IOS rileva un errore) e t4 (quando l'interfaccia perde valore). Per impostazione predefinita, questo valore è impostato su 2 secondi e può essere configurato per valori msec. Come indica la timeline, si tratta di una funzione aggiuntiva che si trova sopra i timer di spegnimento a livello SONET. Il suo comportamento è analogo a quello dei trigger POS: se l'allarme scade prima della fine del periodo di arresto, l'interfaccia non viene interrotta. Tuttavia, c'è un enigma qui. Il timer di debounce SONET non cancella il difetto prima dell'attivazione del ritardo della portante, a meno che il ritardo della portante non sia elevato (ben oltre 10 secondi). Il risultato è una situazione in cui il ritardo della portante è quasi sempre attivato, e quindi deve essere considerato piuttosto basso quando installato con interfacce POS. Il ritardo vettore viene aggiunto anche dopo che l'allarme è stato cancellato, prima che venga dichiarata anche l'interfaccia. Pertanto, è possibile contare il valore del ritardo della portante due volte prima che l'interfaccia venga ripristinata.

Con alcune interfacce e supporti fisici questo è utile. Tuttavia, con le interfacce POS è possibile utilizzare una serie di trigger e timer combinati per creare l'effetto desiderato, senza che il ritardo vettore assuma un ruolo così importante. Un valore di ritardo portante di 0-8 msec è un buon punto di partenza da considerare quando i clienti testano queste manopole da soli. In generale, una buona strategia è usare il comando **pos delay triggers** per assorbire eventuali problemi e fornire l'effetto di arresto desiderato. Il ritardo del vettore può essere ridotto per ridurre al minimo l'impatto.

Il timer di debug SONET di cui sopra è impostato su 10 secondi (+/- 0,5 sec) ed è richiesto da GR-

253 per garantire che non si verifichi un periodo di flap inferiore a 10 secondi. Il timer viene avviato dopo la cancellazione del difetto. Il timer viene reimpostato se si verifica un altro evento anomalo prima della scadenza della finestra del timer.

Sequenza temporale:



Qui:

- t0 - Il difetto viene cancellato.
- t0 - Il timer di rimbalzo inizia.
- t4 - t0 + 10 sec (di conseguenza, il fallimento deve essere cancellato se non si verificano nuovi difetti tra t0 e t4).

Se un evento si verifica prima di t4, (ad esempio) in corrispondenza di t2 (potrebbe trattarsi di un altro difetto o di una ripetizione dello stesso tipo di difetto), il timer viene interrotto fino a quando il nuovo difetto non viene cancellato. A t3, il timer ricomincia quando non ci sono difetti attivi e conta per circa 10 secondi. Se non vengono rilevati nuovi eventi, cancellare l'allarme in corrispondenza di t5, quindi avviare il timer del ritardo vettore. Quando il ritardo vettore è stato cancellato a t6, riattivare l'interfaccia.

Queste informazioni devono consentire al cliente di comprendere più chiaramente come le interfacce POS reagiscono alle varie condizioni SONET/SDH. Ciò consente di configurare l'apparecchiatura in modo più preciso a seconda del comportamento desiderato dal cliente.

Perché utilizzare i trigger?

Questa sezione spiega quando è necessario utilizzare i **trigger di ritardo pos [line | percorso]** e quando non è necessario utilizzarlo.

Di seguito sono riportati gli scenari in cui non è necessario utilizzare i **trigger di ritardo POS**. Esistono diversi scenari:

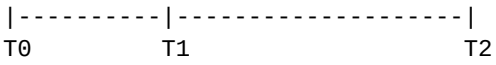
- Non è possibile utilizzare i trigger di linea con interfacce configurate con APS. Le versioni precedenti al software Cisco IOS versione 12.0(28)S non consentivano nemmeno l'uso di trigger di percorso.
- Se in modo esplicito non desiderate che i difetti del livello PATH rallentino l'interfaccia, non potete utilizzare questi trigger.
- Se si desidera che i trigger a livello di riga interrompano l'interfaccia senza alcun ritardo, non è possibile utilizzare questo comando.

Di seguito sono riportati gli scenari in cui è possibile utilizzare il comando **pos delay triggers**:

- Quando si desidera bloccare temporaneamente l'effetto di un difetto a livello di linea.
- Possibilità per i difetti di livello PATH di disattivare immediatamente l'interfaccia.
- Abilitare i difetti di livello PATH per ridurre l'interfaccia, ma con qualche interruzione inclusa.

SLA e trigger POS

Esaminare la sequenza temporale:



- Tempo t=0 (t0) - Quando viene rilevato il difetto.
- Tempo t2: il tempo di ripristino SLA richiesto.
- Tempo t1 - Qualsiasi interruzione dal comando **pos delay triggers** configurato (il valore di default per LINE è 0 e il valore di default per PATH non è abilitato).
- X è il valore di disconnessione (quindi X = il valore di t1).
- Y è il tempo necessario al layer 3 per ripristinare il servizio.

Teorema

Talvolta è possibile utilizzare il comando **pos delay triggers**, mentre in altri casi non è possibile farlo, in particolare se si tenta di rispettare i contratti di servizio (SLA, Service Level Agreement).

Postulati

- Se Y > (t2-t1) per un valore qualsiasi di t1, non è una buona idea effettuare una sospensione perché non è possibile rispettare il contratto di servizio se si configura una sospensione.
- Se Y <= (t2-t1), è possibile prendere in considerazione l'implementazione di un'interruzione. Se la durata dell'errore è inferiore a (t1-t0), è possibile attendere perché non è necessario utilizzare le risorse del router ed è possibile soddisfare lo SLA desiderato. Se il difetto persiste oltre il tempo t1, è comunque possibile soddisfare lo SLA, anche se si perde tempo prima di avviare il ripristino a livello IP.

Per conoscere i valori che è possibile utilizzare in queste formule, è necessario conoscere la rete di trasporto sottostante e i tempi di convergenza della rete di layer 3. È inoltre necessario eseguire alcuni test.

Ecco come funzionano i trigger:

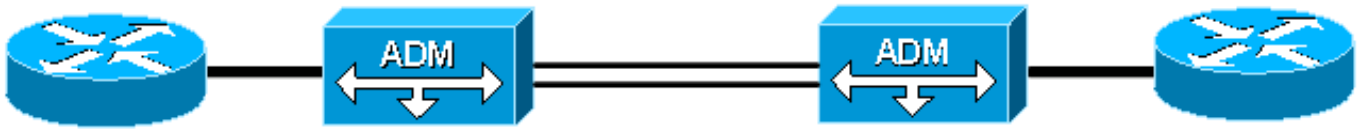
- Il comando **pos delay triggers line *n*** rimane disattivato per *n* ms prima che venga disattivata la riga. Il valore predefinito è 100 ms. È possibile utilizzare questo comando su qualsiasi interfaccia non APS POS. Il comando **pos delay triggers line *n*** non consente alla riga di scendere sulla breve perdita generata dall'unità DWDM protetta internamente, dal momento in cui si verifica uno switch di protezione DWDM interno. Se il difetto viene eliminato durante il periodo di sospensione, è come se il difetto non si fosse mai verificato.
- Il comando **pos delay triggers line** blocca qualsiasi azione basata sul difetto (tranne per incrementare il contatore difetti), fino al termine del periodo di sospensione specificato.Se non si abilita questo comando, APS e link down vengono attivati immediatamente nell'RP.

Implementazione dei trigger SONET

In questa sezione viene descritta la distribuzione dei trigger SONET.

Rete SONET protetta: Nessun APS sui router

Figura 1 - Rete SONET protetta internamente



La rete SONET è dotata di protezione interna, il che significa che un guasto all'interno della rete SONET attiva uno switch di protezione per ripristinare il servizio molto rapidamente. Pertanto, è necessario considerare se si desidera disattivare l'interfaccia e inviare una notifica al layer 3. Nella maggior parte dei casi, quando si verifica uno switch di protezione all'interno della rete SONET, i router visualizzano una breve linea o un percorso AIS mentre la rete esegue un'azione di ripristino. Tuttavia, questo si verifica solo se l'errore si verifica a un hop di distanza da uno dei router. È possibile che la rete SONET abbia un diametro diverso, in entrambi i router gli errori LINE vengono rilevati solo come errori PATH. In questo caso, prendere in considerazione i trigger a livello di percorso e di linea se si desidera una sospensione.

Per prendere questa decisione, è necessario comprendere il costo associato ad entrambi gli approcci. In qualità di operatore di rete, è necessario porsi le seguenti domande:

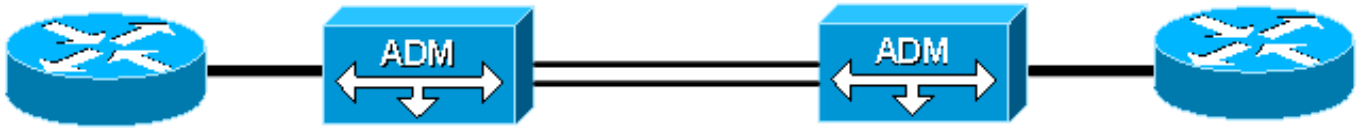
- La rete converge abbastanza rapidamente? In caso contrario, questo approccio non è adatto.
- Qual è l'impatto del routing su un errore di questo tipo? L'impatto sul router è tale che le prestazioni scendono al di sotto di un livello accettabile?

In ultima analisi, è necessario decidere se è possibile ignorare un potenziale colpo di circa 60 msec o se si preferisce instradare un evento di questo tipo. Se si può ignorare la corrispondenza, è necessario identificare la quantità di un "fattore di truffa" da aggiungere in quanto, non si desidera tenere il difetto solo per attendere alcuni millisecondi troppo pochi, e quindi ritardare l'azione correttiva.

In questo scenario, **i trigger di ritardo pos** e **percorso** sono probabilmente sufficienti. Inoltre, considerare valori di almeno 60msec se è garantito un blocco. Se la rete è sufficientemente ampia e si desidera intervenire immediatamente sui difetti a livello di linea e di percorso, non è necessario configurare i trigger a livello di linea. Tuttavia, è necessario configurare i **trigger di ritardo pos** con un valore di 0 per consentire l'elaborazione immediata dei difetti di livello PATH.

Rete SONET non protetta internamente

Figura 2 - Rete SONET non protetta internamente

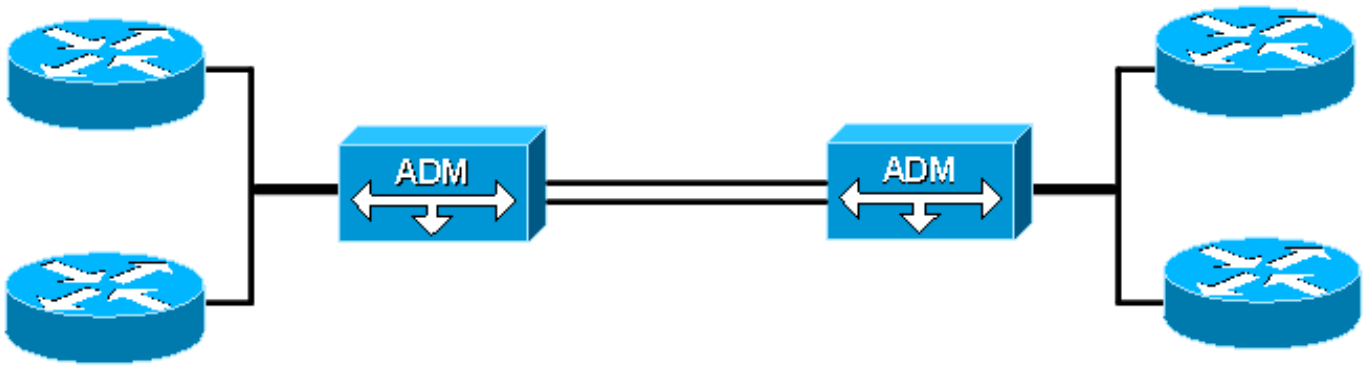


In una rete SONET non protetta, i rischi sono gli stessi del primo scenario, più altri. Se la rete è sufficientemente grande, i router potrebbero non vedere mai un difetto di livello LINE in caso di guasto, perché tutti i difetti sono filtrati. I router possono rilevare i difetti del livello PATH nel flusso verso l'alto e verso il basso. Pertanto, in alcune situazioni in cui si verifica un errore all'interno della rete, il router vede solo gli eventi di livello PATH e non c'è continuità end-to-end tra i router. Ancora peggio, non viene eseguito alcun ripristino a livello SONET per risolvere questa situazione.

In questo scenario, è necessario configurare i trigger di percorso solo per consentire ai router di entrambe le estremità di intraprendere un'azione quando rilevano un problema relativo al percorso, anche se i router non desiderano alcun effetto di arresto. Una volta configurati i trigger Path, come operatore di rete, è necessario verificare se è preferibile bloccare o attivare un ripristino di layer 3.

Rete SONET protetta o non protetta

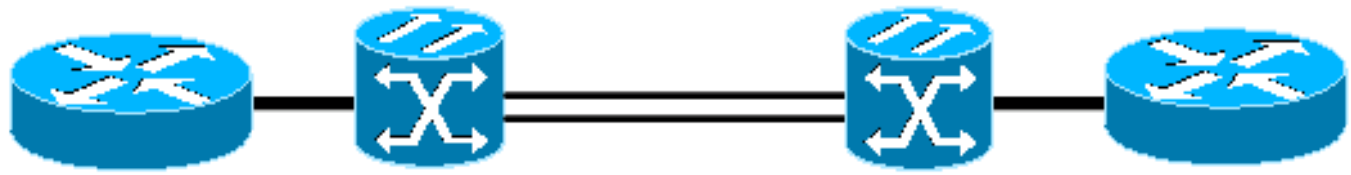
Figura 3 - Rete SONET non protetta internamente



Nel software Cisco IOS versione 12.0(28)S, è possibile abilitare i trigger PATH sui circuiti APS. Quando si distribuisce l'APS sui router locali o remoti, uno switch APS causa ai router remoti che funzionano e proteggono la visualizzazione di un breve difetto di livello PATH. Se il valore di trigger è basso, le interfacce si interrompono e questa situazione non è desiderabile. Un'interfaccia che non funziona ritarda il ripristino del servizio già in corso. Un errore temporaneo che si verifica nel cloud può inoltre ritardare il ripristino del servizio. Tuttavia, il verificarsi di un errore di livello PATH persistente indica che la protezione del circuito (sia all'interno della rete che all'estremità remota) non è stata in grado di ripristinare la connettività. In questo caso, i router APS devono eseguire un'azione e avviare la riconvergenza del routing. È possibile configurare valori di ritardo dell'innesco del percorso >= 100 ms. Con questa configurazione, quando si verifica un errore persistente nella rete SONET o sull'estremità remota, i router imposta entrambe le interfacce APS su uno stato di collegamento non attivo. Pertanto, i router avviano un reindirizzamento e un ripristino del servizio più rapidi.

Rete DWDM protetta

Figura 4 - Rete DWDM protetta



In questo scenario, non è necessario utilizzare i trigger Path, in quanto la rete DWDM non partecipa al livello del protocollo SONET. Il router rileva eventuali errori a livello di SEZIONE o LINEA.

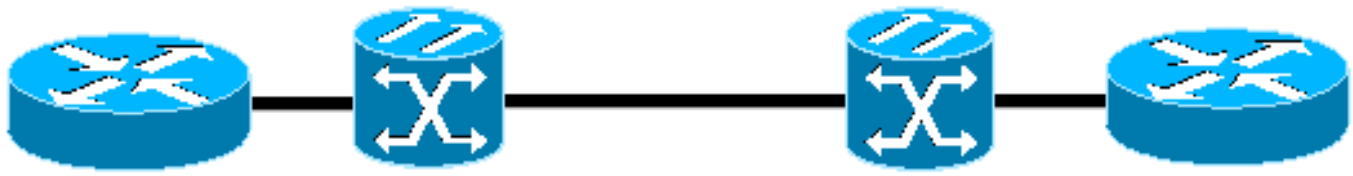
Anche in questo caso, poiché la rete DWDM è protetta internamente, un guasto interno alla rete causa un ripristino immediato. Il router in genere rileva una breve perdita, un ritardo o una frammentazione di errori BIP.

Pertanto, è sufficiente decidere se in questa rete è consigliabile un'interruzione.

Se si sceglie un ritardo, è sufficiente il comando **pos delay triggers line**.

Rete DWDM non protetta

Figura 5 - Rete DWDM non protetta



Se nel trasporto è presente una rete DWDM non protetta, è necessario risolvere tutti i problemi dei router. In questa situazione, la configurazione predefinita consente una risposta immediata a qualsiasi errore rilevato su uno dei router perché il DWDM non partecipa al protocollo SONET. Se si desidera ottenere questo effetto, è appropriata la configurazione predefinita di nessun trigger POS configurato.

Se è necessaria una qualche interruzione, il comando **pos delay triggers line** è sufficiente per fornire questa funzionalità.

Router collegati back-to-back

Figura 6 - Router collegati back-to-back

Due router collegati back-to-back tra due interfacce POS devono funzionare proprio come l'ultimo scenario. I guasti possono essere rilevati immediatamente su entrambi i router, poiché non vi sono apparecchiature intermedie che funzionano sul sovraccarico SONET o che terminano qualsiasi parte del segnale SONET.

Una situazione interessante si verifica quando R1 vede S-LOS e R2 vede sia L-RDI che P-RDI, in quanto R1 è sia un'apparecchiatura di terminazione di linea (LTE) che un'apparecchiatura di terminazione di percorso (PTE). Poiché L-RDI non consente esplicitamente di eseguire alcuna azione al momento della ricezione, R2 non elimina l'interfaccia. Questo problema può potenzialmente portare a una situazione in cui un'interfaccia di R1 è inattiva, ma l'interfaccia di R2 è ancora attiva e inoltra il traffico. Naturalmente, qualsiasi dispositivo keepalive di layer 2 (come HDLC (High-Level Data Link Control)) si interrompe e dichiara il collegamento non attivo, in genere in 30 secondi, in base ai timer configurati. Tuttavia, alcuni operatori disabilitano questi pacchetti keepalive di layer 2 e non possono prevenire questa situazione. Per risolvere questo problema, è possibile adottare diversi approcci, ognuno dei quali affronta il problema da una prospettiva diversa, come illustrato di seguito:

- Attiva trigger percorso: quando P-RDI interrompe un'interfaccia con i trigger percorso abilitati, è possibile utilizzare questo metodo per ottenere una risposta rapida ed eliminare l'interfaccia. L'aspetto interessante da notare è che L-RDI nasconde la P-RDI in condizioni operative normali, come per GR-253. Poiché i trigger POS vengono gestiti a livello di difetto, i trigger vengono elaborati prima del mascheramento dell'allarme e l'interfaccia continua a scendere a seconda del tempo di ritardo configurato.
- Enable Layer 2 Keepalives - Questa opzione determina il timeout dell'interfaccia su R2 dopo la mancata esecuzione di 3 keepalive. Questo valore è in genere pari a 30 secondi (3x10) e Cisco generalmente non consiglia questa opzione come strumento per regolare la convergenza del collegamento rapido.
- Enable a Link-State Routing Protocol: quando l'interfaccia su R1 viene interrotta a causa di S-LOS, viene inviato immediatamente un messaggio di stato del collegamento. Anche se l'interfaccia su R2 può essere ancora attiva, quando il messaggio di stato del collegamento viene ricevuto in tutta l'area, SPF viene eseguito e il collegamento viene rimosso dalla topologia perché il collegamento non supera il controllo della connettività bidirezionale. In questo modo si evita che la rete tenti di eseguire il routing attraverso lo scenario simplex.

Notifica remota basata sulla qualità del segnale

Quando si collegano due router, uno dietro l'altro o attraverso una rete SONET, l'architettura OAM fornita copre il rilevamento della maggior parte degli scenari di errore.

In genere sono presenti notifiche locali e notifiche remote. Tuttavia, quando un numero elevato di errori BIP supera una soglia (SD, SF o B3-TCA), non viene inviata alcuna notifica remota per indicare che si è verificata questa condizione. Pertanto, quando si utilizza la protezione Fast Re-Route MPLS (Multi Protocol Label Switching), nessun trigger attiva uno switch di protezione immediata. Il traffico continua a rimanere bloccato finché non viene perso un volume di traffico sufficiente per causare il guasto dei pacchetti keepalive di layer 2 sul collegamento o delle relazioni dei nodi adiacenti tra peer IGP (Interior Gateway Protocol). A volte questo non accade mai e continua a oscurare il traffico.

Per risolvere questo scenario, CSCec85117 introduce il comando **pos action b3-ber prdi** nella struttura dei comandi POS e SONET.

Questo comando consente all'operatore di configurare l'interfaccia per l'invio di un messaggio P-RDI quando la soglia B3 è stata superata. Questa opzione consente di monitorare il collegamento in modo ottimale end-to-end, indipendentemente dalla topologia. Se sui router è abilitato il **percorso dei trigger di ritardo pos**, il comando **pos action b3-ber prdi** attiva il collegamento che si disattiva (e il corrispondente Fast ReRoute (FRR) o aggiornamento del routing). In questo modo si evita l'effetto buco nero sui collegamenti danneggiati.

Per modificare la sensibilità di questa azione, sintonizzare b3-tca come mostrato di seguito:

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

Il valore fornito è il componente esponenziale per il calcolo BER (ad esempio, **pos threshold b3-tca 3** imposta B3-TCA in modo che equivalga a una velocità 1x10^-3).

Informazioni correlate

- Telcordia Informazioni SuperStore
- Documentazione e supporto tecnico – Cisco Systems