Risoluzione dei problemi STP sugli switch Catalyst

Sommario

Introduzione

In questo documento viene descritto come usare il software Cisco IOS® per risolvere i problemi con lo Spanning Tree Protocol (STP).

Premesse

Solo sugli switch Catalyst 6500/6000 sono disponibili comandi specifici, ma la maggior parte dei principi può essere applicata a qualsiasi switch Cisco Catalyst con software Cisco IOS.

Nella maggior parte dei casi, i problemi sono tre:

- Loop di inoltro.
- Inondazioni eccessive dovute a una frequenza elevata di modifiche della topologia STP (TC).
- Questioni relative ai tempi di convergenza.

Perché un bridge non dispone di meccanismi per tenere traccia se un determinato pacchetto viene inoltrato più volte (ad esempio, un TTL IP Time to Live) viene utilizzato per eliminare il traffico che circola troppo a lungo nella rete. Può esistere un solo percorso tra due dispositivi nello stesso dominio di layer 2 (L2).

Lo scopo di STP è bloccare le porte ridondanti basate su un algoritmo STP e risolvere la topologia fisica ridondante in una topologia ad albero. Un loop di inoltro (ad esempio un loop STP) si verifica quando nessuna porta in una topologia ridondante è bloccata e il traffico viene inoltrato in cerchio per un tempo indefinito.

Una volta avviato, il loop di inoltro congestiona i collegamenti con la larghezza di banda più bassa sul suo percorso. Se tutti i collegamenti hanno la stessa larghezza di banda, tutti i collegamenti sono congestionati. Questa congestione causa la perdita di pacchetti e porta a una situazione di inattività della rete nel dominio L2 interessato.

Con un'eccessiva inondazione, i sintomi non sono così evidenti. I collegamenti lenti possono diventare congestionati dal traffico a singhiozzo e i dispositivi o gli utenti che si trovano dietro a questi collegamenti congestionati possono sperimentare un rallentamento o una perdita totale di connettività.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Vari tipi di Spanning Tree e come configurarli. Per ulteriori informazioni, fare riferimento a Configurazione di STP e MST IEEE 802.1s.
- Varie funzionalità dello Spanning Tree e come configurarle. per ulteriori informazioni, fare riferimento a Configurazione delle funzioni STP.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Catalyst 6500 con motore Supervisor 2
- Software Cisco IOS Release 12.1(13)E

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.

Cause degli errori STP

STP fa alcune ipotesi sul proprio ambiente operativo. Di seguito sono riportati i presupposti più importanti per questo documento:

- Ogni collegamento tra i due ponti è bidirezionale. Ciò significa che, se A si connette direttamente a B, A riceve ciò che B ha inviato e B riceve ciò che A ha inviato, purché il collegamento sia attivo tra di loro.
- Ogni bridge che esegue STP è in grado di ricevere, elaborare e trasmettere regolarmente STP Bridge Protocol Data Units (BPDU), noti anche come pacchetti STP.

Anche se questi presupposti appaiono logici e ovvi, ci sono situazioni in cui non vengono rispettati. La maggior parte di queste situazioni comporta un tipo di problema hardware; tuttavia, i difetti del software possono anche portare a errori STP. Vari guasti hardware, configurazioni errate, problemi di connessione causano la maggior parte degli errori STP, mentre gli errori software rappresentano la minoranza. Gli errori STP possono anche verificarsi a causa di ulteriori connessioni non necessarie tra gli switch. Le VLAN passano a uno stato inattivo a causa di queste connessioni aggiuntive. Per risolvere il problema, rimuovere tutte le connessioni indesiderate tra gli switch.

Quando una di queste ipotesi non viene soddisfatta, uno o più bridge non possono ricevere o elaborare i BPDU. Ciò significa che il bridge (o i bridge) non è in grado di individuare la topologia di rete. Se non si conosce la topologia corretta, lo switch non può bloccare i loop. Di conseguenza, il traffico inondato circola sulla topologia a loop, utilizza tutta la larghezza di banda e blocca la rete.

Tra i motivi per cui gli switch non possono ricevere i BPDU vi sono ricetrasmettitori errati o GBIC (Gigabit Interface Converter), problemi di cavi o errori hardware sulla porta, sulla scheda di linea o sul Supervisor Engine. Un motivo frequente per gli errori STP è un collegamento unidirezionale tra

i bridge. In queste condizioni, un ponte invia pacchetti BPDU, ma il ponte a valle non li riceve mai. L'elaborazione STP può essere interrotta anche da una CPU in sovraccarico (99% o più) perché lo switch non è in grado di elaborare le BPDU ricevute. I BPDU possono essere danneggiati lungo il percorso da un bridge all'altro, il che impedisce anche il corretto comportamento dell'STP.

A parte i loop di inoltro, quando nessuna porta è bloccata, si verificano situazioni in cui solo alcuni pacchetti vengono inoltrati in modo errato attraverso le porte che bloccano il traffico. Nella maggior parte dei casi, ciò è causato da problemi software. Un comportamento di questo tipo può causare "loop lenti". Ciò significa che alcuni pacchetti sono loop, ma la maggior parte del traffico continua a passare attraverso la rete, perché i collegamenti non sono congestionati.

Risoluzione dei problemi relativi ai loop di inoltro

I loop di inoltro variano notevolmente sia nella loro origine (causa) che nell'effetto. Data l'ampia varietà di problemi che possono influire su STP, questo documento può solo fornire linee guida generali su come risolvere i problemi relativi ai loop di inoltro.

Prima di iniziare la risoluzione dei problemi, è necessario disporre delle seguenti informazioni:

- Un diagramma della topologia che mostra in dettaglio tutti gli switch e i bridge.
- I numeri di porta corrispondenti (interconnessi).
- i dettagli della configurazione STP, ad esempio lo switch che rappresenta la radice e la radice di backup, i collegamenti con un costo o una priorità non predefinita e la posizione delle porte che bloccano il traffico.

1. Identificare il loop

Quando nella rete si è sviluppato un loop di inoltro, i sintomi più comuni sono:

- Perdita di connettività verso, da e attraverso le aree di rete interessate.
- Utilizzo elevato della CPU sui router connessi ai segmenti o alle VLAN interessati che può causare vari sintomi, ad esempio il flapping dei router adiacenti al protocollo di routing o il flapping dei router attivi del protocollo HSRP (Hot Standby Router Protocol).
- Utilizzo elevato dei collegamenti (spesso del 100%).
- Utilizzo elevato del backplane dello switch (rispetto all'utilizzo di base).
- Messaggi syslog che indicano il loop dei pacchetti nella rete (ad esempio, messaggi di indirizzi IP duplicati HSRP).
- Messaggi syslog che indicano la riprogrammazione degli indirizzi costanti o messaggi di flapping degli indirizzi MAC.
- Aumenta il numero di output ridotti su molte interfacce.

Una di queste ragioni può indicare da sola problemi diversi (o nessun problema). Tuttavia, quando si osservano molti di questi elementi contemporaneamente, è molto probabile che nella rete si sia sviluppato un loop di inoltro. Il modo più rapido per verificare questa condizione è controllare l'utilizzo del traffico del backplane dello switch:

```
<#root>

cat#

show catalyst6000 traffic-meter



traffic meter =   13%

  Never cleared

peak =   14%

  reached at 12:08:57 CET Fri Oct 4 2002
```

Nota: Catalyst 4000 con software Cisco IOS non supporta attualmente questo comando.

Se il livello di traffico corrente è eccessivo o se il livello di base non è noto, verificare se il livello di picco è stato raggiunto di recente e se è vicino al livello di traffico corrente. Ad esempio, se il livello di traffico massimo è pari al 15% e viene raggiunto solo due minuti fa e il livello di traffico corrente è pari al 14%, lo switch ha un carico insolitamente elevato. Se il carico del traffico è a un livello normale, probabilmente ciò significa che non vi è alcun loop o che questo dispositivo non è coinvolto nel loop. Tuttavia, potrebbe essere ancora coinvolto in un ciclo lento.

2. Individuare la topologia (ambito) del loop

Dopo aver stabilito che la causa dell'interruzione della rete è un loop di inoltro, la priorità più alta è arrestare il loop e ripristinare il funzionamento della rete.

Per arrestare il loop, è necessario conoscere le porte che vi partecipano: osservare le porte con il più alto utilizzo dei collegamenti (pacchetti al secondo). Il comando show interfaceCisco IOS software visualizza l'utilizzo di ciascuna interfaccia.

Per visualizzare solo le informazioni sull'utilizzo e il nome dell'interfaccia (per un'analisi rapida), filtrare l'output delle espressioni regolari con il software Cisco IOS. Eseguire l'interfaccia show | includi riga|\/sec per visualizzare solo le statistiche relative al pacchetto al secondo e il nome dell'interfaccia:

```
<#root>

cat#
```

```
show interface | include line|\/sec


GigabitEthernet2/1 is up, line protocol is down
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
GigabitEthernet2/2 is up, line protocol is down
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec

GigabitEthernet2/3 is up, line protocol is up
  5 minute input rate 99765230 bits/sec, 24912 packets/sec

  5 minute output rate 0 bits/sec, 0 packets/sec

GigabitEthernet2/4 is up, line protocol is up

  5 minute input rate 1000 bits/sec, 27 packets/sec


 5 minute output rate 101002134 bits/sec, 25043 packets/sec

GigabitEthernet2/5 is administratively down, line protocol is down
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
GigabitEthernet2/6 is administratively down, line protocol is down
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
GigabitEthernet2/7 is up, line protocol is down
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec

GigabitEthernet2/8 is up, line protocol is up

  5 minute input rate 2000 bits/sec, 41 packets/sec


5 minute output rate 99552940 bits/sec, 24892 packets/sec
```

Prestare attenzione alle interfacce con il massimo utilizzo dei collegamenti. Nell'esempio, queste sono le interfacce g2/3, g2/4 e g2/8; sono le porte che partecipano al loop.

3. Interrompere il ciclo

Per interrompere il loop, è necessario arrestare o disconnettere le porte interessate. È particolarmente importante non solo arrestare il loop ma anche trovare e correggere la causa principale del loop. È relativamente più facile interrompere il ciclo

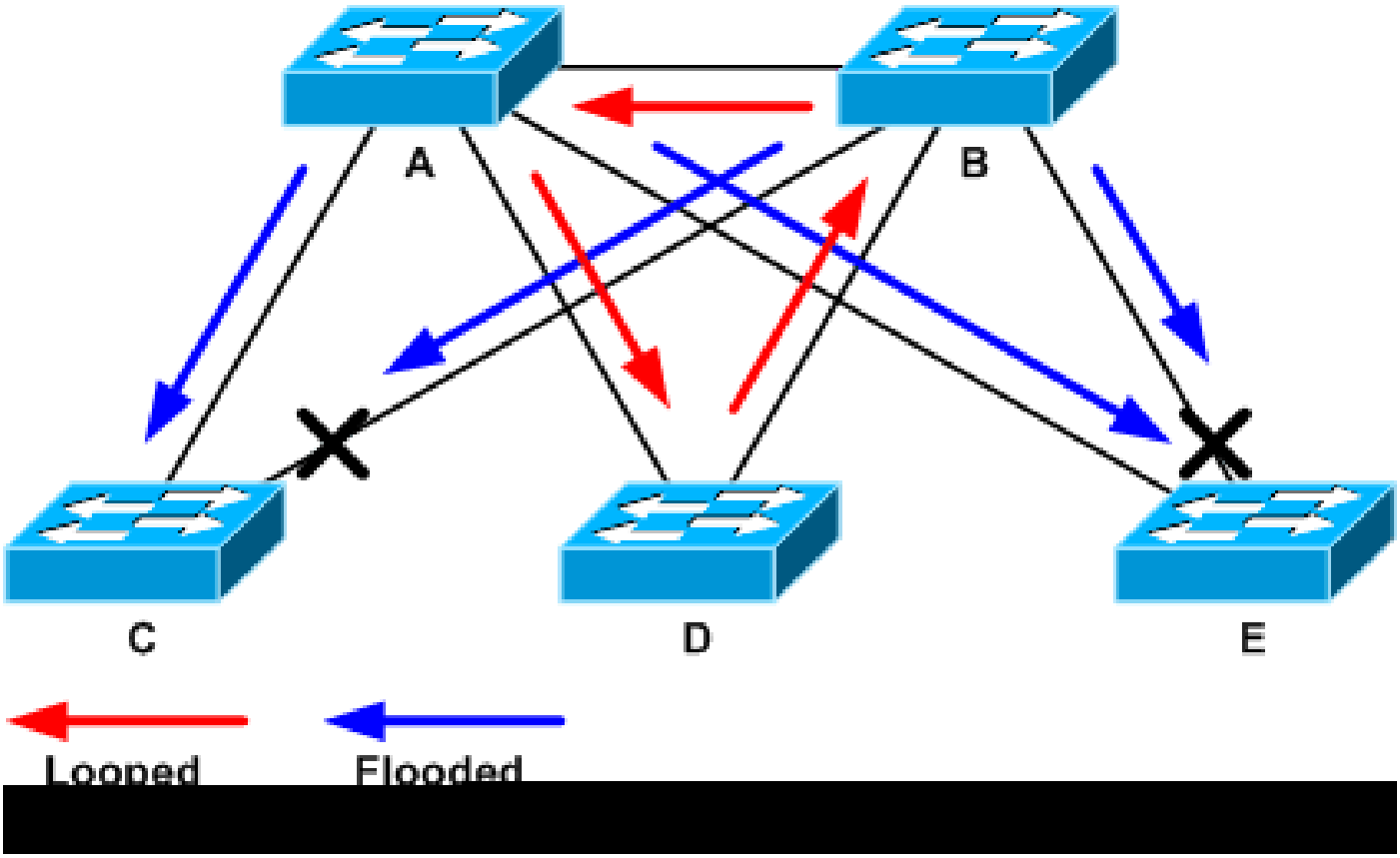
---

Nota: non è necessario arrestare o disconnettere tutte le porte contemporaneamente. È possibile arrestarli uno alla volta. È preferibile arrestare le porte nel punto di aggregazione interessato dal loop, ad esempio uno switch di distribuzione o uno switch core. Se si chiudono tutte le porte contemporaneamente e le si abilita o si riconnette una alla volta, il sistema non funziona; il loop viene arrestato e non può iniziare immediatamente dopo che la porta difettosa è stata riconnessa. Pertanto, è difficile correlare l'errore a una porta specifica.

Nota: per interrompere il ciclo, si consiglia di raccogliere le informazioni prima di riavviare gli switch. In caso contrario, l'analisi della causa principale successiva è difficile. Dopo aver disattivato o disconnesso ciascuna porta, è necessario controllare se l'utilizzo del backplane dello switch è tornato a un livello normale.

Nota: tenere presente che le porte non supportano il loop ma inondano il traffico che arriva con il loop. Quando si chiudono queste porte allagate, si riduce solo di poco l'utilizzo del backplane, ma non si arresta il loop.

Nell'esempio seguente, la topologia si trova tra gli switch A, B e D. Pertanto, i collegamenti AB, AD e BD vengono mantenuti. Se si chiude uno di questi collegamenti, il ciclo viene interrotto. I collegamenti AC, AE, BC e BE stanno semplicemente inondando il traffico che arriva con il loop.



Traffico con loop e inondazioni

Dopo la chiusura della porta di supporto, l'utilizzo del backplane scende a un valore normale. È necessario sapere quale porta ha portato l'utilizzo del backplane (e l'utilizzo di altre porte) a un livello normale.

A questo punto, il loop viene arrestato e il funzionamento della rete migliora; tuttavia, poiché la causa originale del loop non è stata risolta, ci sono ancora altri problemi.

4. Individuazione e correzione della causa del ciclo

Una volta interrotto il loop, è necessario determinare il motivo per cui è iniziato. Questa è la parte

difficile del processo perché le ragioni possono variare. E 'anche difficile formalizzare una procedura esatta che funziona in ogni caso.

Linee guida:

- Esaminare il diagramma della topologia per individuare un percorso ridondante. inclusa la porta di supporto rilevata nel passaggio precedente e che ritorna allo stesso switch (i pacchetti di percorso parlati durante il loop). Nella topologia di esempio precedente, questo percorso è AD-DB-BA.
- Per ogni switch sul percorso ridondante, verificare se lo switch conosce la radice STP corretta.

Tutti gli switch in una rete L2 devono concordare una radice STP comune. I problemi sono chiaramente sintomatici quando i bridge visualizzano in modo coerente un ID diverso per la radice STP in una particolare VLAN o istanza STP. Utilizzare il comando show spanning-tree vlan vlan-id per visualizzare l'ID del bridge radice per una determinata VLAN:

<#root>

```
cat#
show spanning-tree vlan 333


MST03
  Spanning tree enabled protocol mstp


Root ID    Priority    32771
             Address     0050.14bb.6000

             Cost        20000
             Port        136 (GigabitEthernet3/8)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32771  (priority 32768 sys-id-ext 3)
             Address     00d0.003f.8800
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- ------------------------
Gi3/8            Root FWD 20000     128.136  P2p
Po1              Desg FWD 20000     128.833  P2p
```

Il numero VLAN è reperibile dalla porta, in quanto le porte coinvolte nel loop sono state stabilite nei passaggi precedenti. Se le porte in questione sono trunk, spesso sono coinvolte tutte le VLAN sul trunk. In caso contrario (ad esempio, se il loop sembra essersi verificato su una singola VLAN), è possibile provare a utilizzare le interfacce show | includere L2|line|broadcast command (solo sui motori Supervisor 2 e versioni successive sugli switch Catalyst serie 6500/6000, in quanto Supervisor 1 non fornisce statistiche di switching per VLAN). Esaminare solo le interfacce VLAN. La VLAN con il numero più alto di pacchetti commutati è spesso quella in cui si è verificato il loop:

<#root>

cat#

show interface | include L2|line|broadcast

Vlan1 is up, line protocol is up
** L2 Switched: ucast: 653704527 pkt, 124614363025 bytes - mcast:**
**   23036247 pkt, 1748707536 bytes**
**   Received 23201637 broadcasts, 0 runts, 0 giants, 0 throttles**

Vlan10 is up, line protocol is up
  L2 Switched: ucast: 2510912 pkt, 137067402 bytes - mcast:
         41608705 pkt, 1931758378 bytes
     Received 1321246 broadcasts, 0 runts, 0 giants, 0 throttles
Vlan11 is up, line protocol is up
  L2 Switched: ucast: 73125 pkt, 2242976 bytes - mcast:
         3191097 pkt, 173652249 bytes
     Received 1440503 broadcasts, 0 runts, 0 giants, 0 throttles
Vlan100 is up, line protocol is up
  L2 Switched: ucast: 458110 pkt, 21858256 bytes - mcast:
         64534391 pkt, 2977052824 bytes
     Received 1176671 broadcasts, 0 runts, 0 giants, 0 throttles
Vlan101 is up, line protocol is up
  L2 Switched: ucast: 70649 pkt, 2124024 bytes - mcast:
         2175964 pkt, 108413700 bytes
     Received 1104890 broadcasts, 0 runts, 0 giants, 0 throttles

Nell'esempio, la VLAN 1 registra il numero più alto di broadcast e di traffico a commutazione L2. Verificare che la porta radice sia identificata correttamente.

La porta radice deve avere il costo più basso per il bridge radice (a volte un percorso è più breve in termini di hop ma più lungo in termini di costo, in quanto le porte a bassa velocità hanno costi più alti). Per determinare la porta da considerare come radice di una determinata VLAN, usare il comando show spanning-tree vlan:

<#root>

cat#

show spanning-tree vlan 333

MST03
  Spanning tree enabled protocol mstp
  Root ID   Priority   32771
             Address   0050.14bb.6000
             Cost   20000

Port   136 (GigabitEthernet3/8)

             Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID Priority   32771 (priority 32768 sys-id-ext 3)
             Address   00d0.003f.8800

```
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------
Gi3/8            Root FWD 20000     128.136  P2p
Po1              Desg FWD 20000     128.833  P2p
```

Verificare che le BPDU vengano ricevute regolarmente sulla porta radice e sulle porte che dovrebbero essere bloccate.

I BPDU vengono inviati dal bridge radice a ogni intervallo di ellisse (due secondi per impostazione predefinita). I bridge non root ricevono, elaborano, modificano e propagano le BPDU ricevute dalla root. Per verificare se le BPDU sono state ricevute, eseguire il comando show spanning-tree interface detail:

<#root>

```
cat#
```

show spanning-tree interface g3/2 detail

```
Port 130 (GigabitEthernet3/2) of MST00 is backup blocking
   Port path cost 20000, Port priority 128, Port Identifier 128.130.
   Designated root has priority 0, address 0007.4f1c.e847
   Designated bridge has priority 32768, address 00d0.003f.8800
   Designated port id is 128.129, designated path cost 2000019
   Timers: message age 4, forward delay 0, hold 0
```

Number of transitions to forwarding state: 0

```
   Link type is point-to-point by default, Internal
   Loop guard is enabled by default on the port
   BPDU: sent 3,
```

received 53

```
cat#
```

show spanning-tree interface g3/2 detail

```
Port 130 (GigabitEthernet3/2) of MST00 is backup blocking
   Port path cost 20000, Port priority 128, Port Identifier 128.130.
   Designated root has priority 0, address 0007.4f1c.e847
   Designated bridge has priority 32768, address 00d0.003f.8800
   Designated port id is 128.129, designated path cost 2000019
   Timers: message age 5, forward delay 0, hold 0
   Number of transitions to forwarding state: 0
   Link type is point-to-point by default, Internal
   Loop guard is enabled by default on the port
   BPDU: sent 3,
```

received 54

Nota: è stato ricevuto un BPDU tra i due output del comando (il contatore è passato da 53 a 54).

I contatori mostrati sono contatori gestiti dal processo STP stesso. Ciò significa che, se i contatori di ricezione sono incrementati, non solo la BPDU è stata ricevuta da una porta fisica, ma è stata ricevuta anche dal processo STP. Se il received Il contatore BPDU non viene incrementato sulla porta che deve essere la porta radice alternativa o di backup, quindi verificare se la porta riceve i multicast (i BPDU vengono inviati come multicast). Eseguire il comando show interface counterscommand:

<#root>

```
cat#
show interface g3/2 counters

Port            InOctets    InUcastPkts
InMcastPkts
   InBcastPkts
Gi3/2           14873036              2
89387
              0

Port           OutOctets  OutUcastPkts  OutMcastPkts  OutBcastPkts
Gi3/2          114365997         83776        732086            19

cat#
show interface g3/2 counters

Port            InOctets    InUcastPkts
InMcastPkts
   InBcastPkts
Gi3/2           14873677              2
89391
              0

Port           OutOctets  OutUcastPkts  OutMcastPkts  OutBcastPkts
Gi3/2          114366106         83776        732087            19
```

Una breve descrizione dei ruoli della porta STP è disponibile nella sezione Miglioramento del protocollo STP con Loop Guard e Rilevamento inclinazione BPDU (BPDU Skew Detection) di Spanning-Tree Protocol Enhancements using Loop Guard e BPDU Skew Detection. Se non vengono ricevuti BPDU, verificare che la porta conteggi gli errori. Eseguire il comando show interface counters errorscommand:

<#root>

cat#

show interface g4/3 counters errors

```
Port      Align-Err    FCS-Err   Xmit-Err    Rcv-Err UnderSize OutDiscards
Gi4/3         0          0          0          0         0           0

Port  Single-Col Multi-Col  Late-Col Excess-Col Carri-Sen   Runs    Giants
Gi4/3       0         0         0          0         0        0         0
```

È possibile che i BPDU vengano ricevuti dalla porta fisica ma ancora non raggiungano il processo STP. Se i comandi usati nei due esempi precedenti mostrano che alcuni multicast sono ricevuti e gli errori non vengono conteggiati, controllare se i BPDU vengono scartati a livello di processo STP. Eseguire il comando remote command switch test spanning-tree process-status su Catalyst 6500:

<#root>

cat#

remote command switch test spanning-tree process-stats

```
------------------TX STATS------------------
 transmission rate/sec     = 2
 paks transmitted          = 5011226
 paks transmitted (opt)    = 0
 opt chunk alloc failures  = 0
 max opt chunk allocated   = 0
------------------RX STATS------------------

receive rate/sec          = 1

 paks received at stp isr  = 3947627
 paks queued at stp isr    = 3947627

paks dropped at stp isr   = 0
 drop rate/sec             = 0

 paks dequeued at stp proc = 3947627
 paks waiting in queue     = 0
 queue depth               = 7(max) 12288(total)
--------------PROCESSING STATS---------------
 queue wait time (in ms)   = 0(avg) 540(max)
 processing time (in ms)   = 0(avg) 4(max)
 proc switch count         = 100
 add vlan ports            = 20
 time since last clearing  = 2087269 sec
```

Il comando utilizzato in questo esempio visualizza le statistiche del processo STP. È importante

verificare che i contatori delle perdite non aumentino e che i pacchetti ricevuti aumentino. Se i pacchetti ricevuti non vengono aumentati ma la porta fisica non riceve multicast, verificare che i pacchetti vengano ricevuti dall'interfaccia in-band dello switch (l'interfaccia della CPU). Eseguire il comando switch remoto show ibc | i comando rx_inputsullo switch Catalyst 6500/6000:

```
<#root>

cat#

remote command switch show ibc | i rx_input


rx_inputs=

5626468

, rx_cumbytes=859971138

cat#

remote command switch show ibc | i rx_input


rx_inputs=

5626471

, rx_cumbytes=859971539
```

Nell'esempio viene mostrato che, tra gli output, la porta in banda ha ricevuto 23 pacchetti.

Nota: questi 23 pacchetti non sono solo pacchetti BPDU; è un contatore globale per tutti i pacchetti ricevuti dalla porta in-band.

Se non ci sono indicazioni che le BPDU vengano eliminate sullo switch o sulla porta locale, è necessario passare allo switch sull'altro lato del collegamento e verificare se lo switch invia le BPDU. Verificare che i BPDU siano inviati regolarmente su porte designate non radice. Se il ruolo della porta è lo stesso, la porta invia pacchetti BPDU, ma il router adiacente non li riceve. Controllare se i BPDU sono inviati. Eseguire il comando show spanning-tree interface detail:

```
<#root>

cat#

show spanning-tree interface g3/1 detail


Port 129 (GigabitEthernet3/1) of MST00 is

designated

 forwarding
   Port path cost 20000, Port priority 128, Port Identifier 128.129.
   Designated root has priority 0, address 0007.4f1c.e847
   Designated bridge has priority 32768, address 00d0.003f.8800
```

```
   Designated port id is 128.129, designated path cost 2000019
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 0
   Link type is point-to-point by default, Internal
   Loop guard is enabled by default on the port


BPDU: sent 1774

, received 1

cat#

show spanning-tree interface g3/1 detail


Port 129 (GigabitEthernet3/1) of MST00 is

designated

 forwarding
   Port path cost 20000, Port priority 128, Port Identifier 128.129.
   Designated root has priority 0, address 0007.4f1c.e847
   Designated bridge has priority 32768, address 00d0.003f.8800
   Designated port id is 128.129, designated path cost 2000019
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 0
   Link type is point-to-point by default, Internal
   Loop guard is enabled by default on the port


BPDU: sent 1776

, received 1
```

Nell'esempio, vengono inviati due BPDU tra le uscite.

Nota: il processo STP conserva il contatore BPDU:. Ciò significa che il contatore indica che la BPDU è stata inviata alla porta fisica e viene inviata. Controllare se i contatori delle porte aumentano per i pacchetti multicast trasmessi. Eseguire il comando show interface counterscommand. Ciò può aiutare a determinare il flusso del traffico BPDU.

<#root>

```
cat#

show interface g3/1 counters


Port            InOctets   InUcastPkts   InMcastPkts   InBcastPkts
Gi3/1          127985312         83776        812319            19

Port           OutOctets  OutUcastPkts

OutMcastPkts

  OutBcastPkts
Gi3/1          131825915          3442

872342
```

```
           386

cat#

show interface g3/1 counters


Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Gi3/1          127985312          83776         812319             19

Port           OutOctets   OutUcastPkts

OutMcastPkts

  OutBcastPkts
Gi3/1          131826447           3442

872346

           386
```

Con tutti questi passaggi, l'idea è quella di trovare lo switch o il collegamento dove le BPDU non vengono ricevute, inviate o elaborate. È possibile che l'STP abbia calcolato lo stato corretto per la porta, ma a causa di un problema del control plane, non è in grado di impostare questo stato sull'hardware di inoltro. È possibile creare un loop se la porta non è bloccata a livello di hardware. Se si ritiene che questo sia un problema della rete, contattare il supporto tecnico Cisco per ulteriore assistenza.

5. Ripristinare la ridondanza

Una volta individuato il dispositivo o il collegamento che causa il loop, è necessario isolare il dispositivo dalla rete o risolvere il problema (ad esempio sostituire la fibra o il GBIC). I collegamenti ridondanti, disconnessi nel Passaggio 3, devono essere ripristinati.

È importante non manipolare il dispositivo o il collegamento che provoca il loop, in quanto molte condizioni che portano a un loop sono transitorie, intermittenti e instabili. Ciò significa che, se la condizione viene cancellata durante o dopo l'indagine, la condizione non si verifica per un certo periodo di tempo o non si verifica affatto. La condizione deve essere registrata in modo che il supporto tecnico Cisco possa approfondirla. È importante raccogliere informazioni sulla condizione prima di ripristinare gli switch. Se una condizione non viene soddisfatta, non è possibile determinare la causa principale del loop. Se si raccolgono le informazioni, assicurarsi che il problema non provochi nuovamente il loop. Per ulteriori informazioni, consultare il documento sulla protezione della rete dai loop di inoltro.

Analizza modifiche alla topologia

Il meccanismo TC (Topology Change) ha il compito di correggere le tabelle di inoltro L2 dopo la modifica della topologia. Questa operazione è necessaria per evitare un'interruzione della connettività in quanto gli indirizzi MAC a cui era precedentemente possibile accedere tramite porte specifiche possono cambiare e diventare accessibili tramite porte diverse. Il timecode riduce la durata della tabella di inoltro su tutti gli switch della VLAN in cui si verifica il timecode. Quindi, se

l'indirizzo non viene riguadagnato, scade e si verifica un flooding per garantire che i pacchetti raggiungano l'indirizzo MAC di destinazione.

TC viene attivato dalla modifica dello stato STP di una porta in o da STPforwardingstate. Dopo il timeout di TC, anche se l'indirizzo MAC di destinazione specifico è scaduto, l'allagamento non continua per molto tempo. L'indirizzo viene recuperato dal primo pacchetto che proviene dall'host il cui indirizzo MAC è scaduto. Il problema può verificarsi quando il TC si ripete più volte, a intervalli brevi. Gli switch invecchiano costantemente i loro tavoli di inoltro, quindi l'inondazione può essere quasi costante.

Nota: con Rapid STP o Multiple STP (IEEE 802.1w e IEEE 802.1s), il TC viene attivato da una modifica dello stato della porta `a forwarding`, nonché dalla modifica del ruolo `da designatedtoroot`. Con Rapid STP, la tabella di inoltro L2 viene immediatamente scaricata, a differenza di 802.1d, che riduce il tempo di aging. Lo svuotamento immediato della tabella di inoltro ripristina la connettività più rapidamente, ma può causare un aumento del flusso

---

Il TC è un evento raro in una rete ben configurata. Quando un collegamento su una porta dello switch va su o giù, alla fine esiste un TC, una volta che lo stato STP della porta è cambiato in o `da inoltro`. Quando la porta scollega, si verificano ripetitivi allagamenti e interruzioni delle connessioni.

Le porte con la funzione portfast STP abilitata non possono causare timecode quando passano da o verso lo stato `di inoltro`. La configurazione di portfast su tutte le porte dei dispositivi finali (ad esempio stampanti, PC e server) può limitare i TC a una quantità ridotta ed è consigliata.

Se sulla rete sono presenti TC ripetitivi, è necessario identificare l'origine di tali TC e adottare le misure necessarie per ridurli al minimo, in modo da ridurre al minimo il rischio di inondazioni.

Con lo standard 802.1d, le informazioni STP su un evento TC vengono propagate tra i bridge tramite una Notifica TC (TCN), un tipo speciale di BPDU. Se si seguono le porte che ricevono i BPDU TCN, è possibile trovare il dispositivo da cui sono stati originati i TC.

Trova la causa dell'inondazione

È possibile verificare che le prestazioni siano lente, che i pacchetti scarichino sui collegamenti che non dovrebbero essere congestionati e che l'analizzatore di pacchetti visualizzi più pacchetti unicast alla stessa destinazione che non si trova sul segmento locale. Per ulteriori informazioni su unicast flooding, fare riferimento a Unicast Flooding in Switched Campus Networks.

Su uno switch Catalyst 6500/6000 con software Cisco IOS, è possibile controllare il contatore del motore di inoltro (solo sul motore Supervisor 2) per stimare la quantità di allagamento. Eseguire il comando switch remoto per visualizzare le statistiche iniziali | i Comando MISS_DA|ST_FR:

<#root>

```
cat#
remote command switch show earl statistics | i MISS_DA|ST_FR
```

```
         ST_MISS_DA     =       18                      530308834
         ST_FRMS        =       97                      969084354

cat#
remote command switch show earl statistics | i MISS_DA|ST_FR

         ST_MISS_DA     =       4                       530308838
         ST_FRMS        =       23                      969084377
```

In questo esempio, la prima colonna mostra la modifica dall'ultima esecuzione del comando e la seconda colonna mostra il valore cumulativo dall'ultimo riavvio. La prima riga mostra la quantità di frame a cui è applicato il flooded, mentre la seconda riga mostra la quantità di frame elaborati. Se i due valori sono vicini o il primo aumenta ad alta velocità, è possibile che lo switch stia inondando il traffico. Tuttavia, questo può essere usato solo in combinazione con altri modi per verificare l'inondazione, in quanto i contatori non sono granulari. È disponibile un contatore per switch, non per porta o VLAN. È normale vedere alcuni pacchetti in modalità flooding, in quanto lo switch può sempre eseguire il flood se l'indirizzo MAC di destinazione non è presente nella tabella di inoltro. Ad esempio, quando lo switch riceve un pacchetto con un indirizzo di destinazione che non è ancora stato appreso.

Trova l'origine dei TC

Se il numero VLAN è noto per la VLAN in cui si verifica un eccessivo allagamento, controllare i contatori STP per verificare se il numero di TC è alto o se si incrementano regolarmente. Eseguire il comando show spanning-tree vlan vlan-id detail (nell'esempio riportato viene usata la VLAN 1):

<#root>

```
cat#
show spanning-tree vlan 1 detail


VLAN0001 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, sysid 1, address 0007.0e8f.04c0
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 0, address 0007.4f1c.e847
  Root port is 65 (GigabitEthernet2/1), cost of root path is 119
  Topology change flag not set, detected flag not set


Number of topology changes 1 last change occurred 00:00:35 ago
          from GigabitEthernet1/1

  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300
```

Se il numero VLAN non è noto, è possibile usare l'analizzatore di pacchetti o controllare i contatori

TC per tutte le VLAN.

Adottare misure per evitare un numero eccessivo di TC

È possibile monitorare `il contatore delle` modifiche alla `topologia` per verificare se aumenta regolarmente. Quindi, spostarsi sul bridge collegato alla porta mostrata, per ricevere l'ultimo TC (nell'esempio precedente, port Gigabit Ethernet1/1) e vedere da dove proviene il TC per quel bridge. Questa procedura deve essere ripetuta finché non si trova la porta della stazione terminale senza l'opzione STP portfast abilitata o finché non si trova il collegamento che deve essere corretto. L'intera procedura deve essere ripetuta se i TC provengono da altre fonti. Se il collegamento appartiene a un host finale, è possibile configurare la funzione portfast in modo da impedire la generazione di TC.

Nota: nell'implementazione del software Cisco IOS STP, il contatore dei TC può essere incrementato solo se un BPDU TCN viene ricevuto da una porta di una VLAN. Se si riceve una BPDU di configurazione normale con un flag TC impostato, il contatore TC non viene incrementato. Ciò significa che, se si sospetta che il motivo dell'inondazione sia un TC, iniziare a rintracciare le origini del TC dal ponte principale dell'STP su tale VLAN. Può contenere informazioni estremamente precise sul numero e sull'origine dei TC.

Risoluzione dei problemi relativi al tempo di convergenza

In alcuni casi, il funzionamento effettivo di STP non corrisponde al comportamento previsto. Questi sono i due problemi più frequenti:

- La convergenza o la riconvergenza dell'STP richiede più tempo del previsto.
- Il risultato della topologia è diverso dal previsto.

Molto spesso queste sono le cause di questo comportamento:

- Mancata corrispondenza tra la topologia reale e quella documentata.
- Configurazione errata, ad esempio una configurazione incoerente dei timer STP, un diametro STP che aumenta o una configurazione errata portfast.
- Sovraccarico della CPU dello switch durante la convergenza o la riconversione.
- Errore software.

Come accennato in precedenza, questo documento può solo fornire linee guida generali per la risoluzione dei problemi, a causa dell'ampia varietà di problemi che possono influire sull'STP. Per capire perché la convergenza richiede più tempo del previsto, osservare la sequenza degli eventi STP per scoprire cosa accade e in quale ordine. Poiché l'implementazione STP nel software Cisco IOS non registra i risultati (ad eccezione di eventi specifici, come le incoerenze delle porte), è possibile utilizzare il software Cisco IOS per eseguire il debug di STP e ottenere una visualizzazione più chiara. Per STP, su uno switch Catalyst 6500/6000 con software Cisco IOS,

l'elaborazione viene eseguita sul processore dello switch (SP) (o sul Supervisor), quindi è necessario abilitare i debug sull'SP. Per i gruppi bridge di software Cisco IOS, l'elaborazione viene eseguita sul processore di routing (RP), quindi i debug devono essere abilitati sull'MSFC (Route Processor).

Usa comandi di debug STP

Molti comandi STPdebugsono destinati all'utilizzo in ambito di progettazione. Non forniscono alcun output significativo per qualcuno senza una conoscenza dettagliata dell'implementazione STP nel software Cisco IOS. Alcuni debug possono fornire output immediatamente leggibili, come modifiche dello stato della porta, modifiche ai ruoli, eventi come i TC e un dump delle BPDU ricevute e trasmesse. In questa sezione non viene fornita una descrizione completa di tutti i debug, ma vengono introdotti brevemente i debug più utilizzati.

Nota: quando si utilizzano i comandi di debug, abilitare il numero minimo di debug necessari. Se non è necessario eseguire il debug in tempo reale, registrare l'output nel registro anziché stamparlo sulla console. Debug eccessivi possono sovraccaricare la CPU e interrompere il funzionamento dello switch.

Per indirizzare l'output del comando debug al log anziché alla console o alle sessioni Telnet, usare i comandi logging console informationaland no logging monitorcommands in modalità di configurazione globale. Per visualizzare il registro degli eventi generali, usare il comando debug spanning-tree event per PVST (Per VLAN Spanning-Tree) e Rapid-PVST. Questo è il primo debug che fornisce informazioni su quello che è successo con l'STP. In modalità Multiple Spanning-Tree (MST), non è possibile usare il comando debug spanning-tree event. Pertanto, eseguire il comando debug spanning-tree mstp rolesper visualizzare le modifiche del ruolo della porta. Per visualizzare le modifiche dello stato del protocollo STP della porta, usare il comando debug spanning-tree switch status insieme al comando debug pm vp:

```
<#root>

cat-sp#

debug spanning-tree switch state


Spanning Tree Port state changes debugging is on

cat-sp#

debug pm vp


Virtual port events debugging is on
Nov 19 14:03:37: SP:     pm_vp 3/1(333): during state forwarding, got event 4(remove)

Nov 19 14:03:37: SP:

 @@@

pm_vp 3/1(333):
  forwarding -> notforwarding
```

port 3/1 (was forwarding) goes down in vlan 333

```
Nov 19 14:03:37: SP: *** vp_fwdchange: single: notfwd: 3/1(333)
Nov 19 14:03:37: SP: @@@ pm_vp 3/1(333): notforwarding -> present
Nov 19 14:03:37: SP: *** vp_linkchange: single: down: 3/1(333)
Nov 19 14:03:37: SP: @@@ pm_vp 3/1(333): present -> not_present
Nov 19 14:03:37: SP: *** vp_statechange: single: remove: 3/1(333)
```

Nov 19 14:03:37: SP: pm_vp 3/2(333): during state notforwarding, got event 4(remove)
Nov 19 14:03:37: SP:

@@@

pm_vp 3/2(333): notforwarding -> present
Nov 19 14:03:37: SP: * vp_linkchange: single: down: 3/2(333)**

Port 3/2 (was not forwarding) in vlan 333 goes down

```
Nov 19 14:03:37: SP: @@@ pm_vp 3/2(333): present -> not_present
Nov 19 14:03:37: SP: *** vp_statechange: single: remove: 3/2(333)

Nov 19 14:03:53: SP:     pm_vp 3/1(333): during state not_present,
  got event 0(add)
Nov 19 14:03:53: SP: @@@ pm_vp 3/1(333): not_present -> present
Nov 19 14:03:53: SP: *** vp_statechange: single: added: 3/1(333)
```

Nov 19 14:03:53: SP: pm_vp 3/1(333): during state present, got event 8(linkup)
Nov 19 14:03:53: SP:

@@@

pm_vp 3/1(333): present -> notforwarding
Nov 19 14:03:53: SP: STP SW: Gi3/1 new blocking req for 0 vlans
Nov 19 14:03:53: SP: * vp_linkchange: single: up: 3/1(333)**

Port 3/1 link goes up and blocking in vlan 333

```
Nov 19 14:03:53: SP:     pm_vp 3/2(333): during state not_present,
  got event 0(add)
Nov 19 14:03:53: SP: @@@ pm_vp 3/2(333): not_present -> present
Nov 19 14:03:53: SP: *** vp_statechange: single: added: 3/2(333)
```

Nov 19 14:03:53: SP: pm_vp 3/2(333): during state present, got event 8(linkup)
Nov 19 14:03:53: SP:

@@@

pm_vp 3/2(333): present -> notforwarding
Nov 19 14:03:53: SP: STP SW: Gi3/2 new blocking req for 0 vlans
Nov 19 14:03:53: SP: * vp_linkchange: single: up: 3/2(333)**

Port 3/2 goes up and blocking in vlan 333

Nov 19 14:04:08: SP: STP SW: Gi3/1 new learning req for 1 vlans
Nov 19 14:04:23: SP: STP SW: Gi3/1 new forwarding req for 0 vlans
Nov 19 14:04:23: SP: STP SW: Gi3/1 new forwarding req for 1 vlans

```
Nov 19 14:04:23: SP:     pm_vp 3/1(333): during state notforwarding,
  got event 14(forward_notnotify)
Nov 19 14:04:23: SP:


@@@ pm_vp 3/1(333): notforwarding ->
  forwarding
Nov 19 14:04:23: SP: *** vp_list_fwdchange: forward: 3/1(333)

Port 3/1 goes via learning to forwarding in vlan 333
```

Per comprendere perché il protocollo STP si comporta in un certo modo, è spesso utile visualizzare i BPDU ricevuti e inviati dallo switch:

<#root>

```
cat-sp#

debug spanning-tree bpdu receive


Spanning Tree BPDU Received debugging is on
Nov  6 11:44:27: SP: STP: VLAN1 rx BPDU: config protocol = ieee,
  packet from GigabitEthernet2/1  , linktype IEEE_SPANNING ,
  enctype 2, encsize 17
Nov  6 11:44:27: SP: STP: enc 01 80 C2 00 00 00 00 06 52 5F 0E 50 00 26 42 42 03
Nov  6 11:44:27: SP: STP: Data 0000000000000000074F1CE84700000013804800006525F0E4
  0801001001400020000F00
Nov  6 11:44:27: SP: STP: VLAN1 Gi2/1:0000 00 00 00 000000074F1CE847 00000013
  80480006525F0E40 8010 0100 1400 0200 0F00
```

Questo debug funziona nelle modalità PVST, Rapid-PVST e MST, ma non decodifica il contenuto delle BPDU. Tuttavia, è possibile utilizzarlo per assicurarsi che le BPDU vengano ricevute. Per visualizzare il contenuto della BPDU, usare il comando debug spanning-tree switch rx decodecommand insieme al comando debug spanning-tree switch rx processper PVST e Rapid-PVST. Utilizzare il comando debug spanning-tree mstp bpdu-rxper visualizzare il contenuto della BPDU per MST:

<#root>

```
cat-sp#

debug spanning-tree switch rx decode


Spanning Tree Switch Shim decode received packets debugging is on

cat-sp#

debug spanning-tree switch rx process


Spanning Tree Switch Shim process receive bpdu debugging is on
```

```
Nov  6 12:23:20: SP: STP SW: PROC RX: 0180.c200.0000<-0006.525f.0e50 type/len 0026
Nov  6 12:23:20: SP:     encap SAP linktype ieee-st vlan 1 len 52 on v1 Gi2/1
Nov  6 12:23:20: SP:     42 42 03 SPAN
Nov  6 12:23:20: SP:     CFG P:0000 V:00 T:00 F:00 R:0000 0007.4f1c.e847 00000013
Nov  6 12:23:20: SP:     B:8048 0006.525f.0e40 80.10 A:0100 M:1400 H:0200 F:0F00

Nov  6 12:23:22: SP: STP SW: PROC RX: 0180.c200.0000<-0006.525f.0e50 type/len 0026
Nov  6 12:23:22: SP:     encap SAP linktype ieee-st vlan 1 len 52 on v1 Gi2/1
Nov  6 12:23:22: SP:     42 42 03 SPAN
Nov  6 12:23:22: SP:     CFG P:0000 V:00 T:00 F:00 R:0000 0007.4f1c.e847 00000013
Nov  6 12:23:22: SP:     B:8048 0006.525f.0e40 80.10 A:0100 M:1400 H:0200 F:0F00
```

Per la modalità MST, è possibile abilitare la decodifica BPDU dettagliata con questo comando debugcommand:

<#root>

```
cat-sp#

debug spanning-tree mstp bpdu-rx


Multiple Spanning Tree Received BPDUs debugging is on
Nov 19 14:37:43: SP: MST:BPDU DUMP [

rcvd_bpdu Gi3/2

 Repeated]
Nov 19 14:37:43: SP: MST:   Proto:0 Version:3 Type:2 Role: DesgFlags[   F    ]
Nov 19 14:37:43: SP: MST:   Port_id:32897 cost:2000019
Nov 19 14:37:43: SP: MST:   root_id  :0007.4f1c.e847 Prio:0
Nov 19 14:37:43: SP: MST:   br_id    :00d0.003f.8800 Prio:32768
Nov 19 14:37:43: SP: MST:   age:2 max_age:20 hello:2 fwdelay:15
Nov 19 14:37:43: SP: MST:   V3_len:90 PathCost:30000 region:STATIC rev:1
Nov 19 14:37:43: SP: MST:   ist_m_id :0005.74
Nov 19 14:37:43: SP: MST:BPDU DUMP [

rcvd_bpdu Gi3/2

 Repeated]
Nov 19 14:37:43: SP: MST:   Proto:0 Version:3 Type:2 Role: DesgFlags[   F    ]
Nov 19 14:37:43: SP: MST:   Port_id:32897 cost:2000019
Nov 19 14:37:43: SP: MST:   root_id  :0007.4f1c.e847 Prio:0
Nov 19 14:37:43: SP: MST:   br_id    :00d0.003f.8800 Prio:32768
Nov 19 14:37:43: SP: MST:   age:2 max_age:20 hello:2 fwdelay:15
Nov 19 14:37:43: SP: MST:   V3_len:90 PathCost:30000 region:STATIC rev:1
Nov 19 14:37:43: SP: MST:   ist_m_id :0005.7428.1440 Prio:32768  Hops:18
  Num Mrec: 1
Nov 19 14:37:43: SP: MST: stci=3  Flags[ F    ] Hop:19 Role:Desg [Repeated]
Nov 19 14:37:43: SP: MST:         br_id:00d0.003f.8800 Prio:32771 Port_id:32897
  Cost:2000028.1440 Prio:32768  Hops:18  Num Mrec: 1
Nov 19 14:37:43: SP: MST: stci=3  Flags[ F    ] Hop:19 Role:Desg [Repeated]
Nov 19 14:37:43: SP: MST:         br_id:00d0.003f.8800 Prio:32771 Port_id:32897
  Cost:20000
```

Nota: per il software Cisco IOS versione 12.1.13E e successive, sono supportati i debug

condizionali per STP. È quindi possibile eseguire il debug dei BPDU ricevuti o trasmessi su base porta o VLAN.

Eseguire i comandi debug condition vlan num_vlan o debug condition interface per limitare l'ambito dell'output del debug a una singola interfaccia o a una singola VLAN.

Proteggere la rete dai loop di inoltro

Cisco ha sviluppato una serie di funzionalità e miglioramenti per proteggere le reti dai loop di inoltro quando un STP non è in grado di gestire alcuni errori.

Quando si esegue la risoluzione dei problemi dell'STP, è possibile isolare e individuare la causa di un errore specifico, mentre l'implementazione di questi miglioramenti è l'unico modo per proteggere la rete dai loop di inoltro.

Per proteggere la rete dai loop di inoltro, eseguire le operazioni seguenti:

1. Abilitare il protocollo UDLD (Unidirectional Link Detection) su tutti i collegamenti switch-switch

Per ulteriori informazioni sul protocollo UDLD, consultare il documento sulla descrizione e configurazione della funzione UDLD (Unidirectional Link Detection Protocol).

2. Abilitare Loop Guard su tutti gli switch

Per ulteriori informazioni su Loop Guard, consultare il documento sui miglioramenti del protocollo Spanning-Tree con le funzioni Loop Guard e BPDU Skew Detection.

Quando abilitato, UDLD e Loop Guard eliminano la maggior parte delle cause dei loop di inoltro. Anziché creare un loop di inoltro, il link difettoso (o tutti i link dipendenti dall'hardware difettoso) si arresta o viene bloccato.

Nota: sebbene queste due funzioni appaiano in qualche modo ridondanti, ognuna ha le sue funzionalità uniche. Pertanto, utilizzare entrambe le funzionalità contemporaneamente per fornire il massimo livello di protezione. Per un confronto dettagliato tra UDLD e Loop Guard, fare riferimento a Loop Guard e Unidirectional Link Detection.

Ci sono diverse opinioni sulla necessità o meno di usare il protocollo UDLD aggressivo o normale. Il protocollo UDLD non può fornire una protezione maggiore contro i loop rispetto al protocollo UDLD in modalità normale. Il protocollo UDLD aggressivo rileva scenari di blocco delle porte (quando il collegamento è attivo, ma non vi sono blocchi del traffico associati). Lo svantaggio di questa funzionalità aggiuntiva è che un protocollo UDLD aggressivo può disabilitare i collegamenti in assenza di errori coerenti. Spesso le persone confondono la modifica di UDLDhellointerval con la funzione UDLD aggressiva. Questo non è corretto. I timer possono essere modificati in entrambe le modalità UDLD.

Nota: in rari casi, un protocollo UDLD aggressivo può disattivare tutte le porte uplink, isolando in pratica lo switch dal resto della rete. Ad esempio, ciò può verificarsi quando entrambi gli switch a monte registrano un utilizzo della CPU estremamente elevato e viene utilizzato il protocollo UDLD in modalità aggressiva. Pertanto, si consiglia di configurare timeout che non possano essere erosi, se lo switch non dispone di una gestione fuori banda.

3. Abilitare Portfast su tutte le porte della stazione terminale

È necessario abilitare portfast per limitare la quantità di TC e il conseguente flooding, che può influire sulle prestazioni della rete. Utilizzare questo comando solo con le porte che si connettono a unità terminali. In caso contrario, un loop di topologia accidentale può causare un loop di pacchetti di dati e interrompere il funzionamento dello switch e della rete.

Attenzione: prestare attenzione quando si utilizza il comando no spanning-tree portfast. Questo comando rimuove solo i comandi portfast specifici della porta. Questo comando abilita implicitamente portfast se si definisce il comando spanning-tree portfast default in modalità di configurazione globale e se la porta non è una porta trunk. se non si configura portfast a livello globale, il comando no spanning-tree portfast equivale al comando spanning-tree portfast disable.

4. Impostare EtherChannel sulla modalità **`desiderata`** su entrambi i lati (se supportata) e sull'opzione **`non silenziosa`**

Desirablemode può abilitare il protocollo PAgP (Port Aggregation Protocol) per garantire la coerenza in fase di esecuzione tra i peer di channeling. Ciò fornisce un ulteriore grado di protezione contro i loop, specialmente durante le riconfigurazioni dei canali (ad esempio quando i collegamenti si uniscono o escono dal canale e il rilevamento degli errori dei collegamenti). È presente una funzione incorporata di protezione dalla configurazione errata del canale, abilitata per impostazione predefinita, che impedisce i loop di inoltro dovuti a una configurazione errata del canale o ad altre condizioni. Per ulteriori informazioni su questa funzione, consultare il documento sul rilevamento delle incoerenze EtherChannel.

5. Non disabilitare la negoziazione automatica (se supportata) sui collegamenti tra switch

I meccanismi di negoziazione automatica possono trasmettere informazioni sugli errori remoti, che rappresentano il modo più rapido per rilevare gli errori sul lato remoto. Se viene rilevato un guasto sul lato remoto, il lato locale riduce il collegamento anche se questo viene a impulsi. Rispetto ai meccanismi di rilevamento di alto livello, ad esempio il protocollo UDLD, la negoziazione automatica è estremamente rapida (entro microsecondi) ma non dispone della copertura end-to-end del protocollo UDLD (ad esempio, l'intero datapath: CPU—logica di inoltro—porta1—porta2—logica di inoltro—CPU vs porta1—porta2). La modalità UDLD aggressiva offre una funzionalità simile a quella della negoziazione automatica per quanto riguarda il rilevamento di errori. Quando la negoziazione è supportata su entrambi i lati del collegamento, non è necessario abilitare il protocollo UDLD in modalità aggressiva.

6. Prestare attenzione quando si sintonizzano i timer STP

I timer STP dipendono l'uno dall'altro e dalla topologia di rete. Il comando STP non funziona correttamente se i timer vengono modificati in modo arbitrario. Per ulteriori informazioni sui timer STP, fare riferimento a Comprensione e tuning dei timer del protocollo Spanning Tree.

7. Se sono possibili attacchi Denial of Service, proteggere il perimetro STP della rete con Root Guard

Root Guard e BPDU Guard consentono di proteggere STP dall'influenza esterna. Se è possibile un attacco di questo tipo, è necessario utilizzare Root Guard e BPDU Guard per proteggere la rete. Per ulteriori informazioni su Root Guard e BPDU Guard, consultare i seguenti documenti:

- Miglioramenti Della Funzionalità Spanning-Tree Protocol Root Guard
- Miglioramenti della funzionalità Spanning Tree PortFast BPDU Guard

8. Abilitare BPDU Guard sulle porte abilitate Portfast per impedire che l'STP sia causato da dispositivi di rete non autorizzati (ad esempio hub, switch e router di bridging) connessi alle porte

Se si configura correttamente Root Guard, impedisce all'STP di influenzare dall'esterno. Se BPDU Guard è abilitato, chiude le porte che ricevono eventuali BPDU. Questa opzione è utile per analizzare gli incidenti, in quanto BPDU Guard produce il messaggio syslog e chiude la porta. Se le protezioni Root o BPDU non impediscono i loop a breve ciclo, due porte abilitate in modo rapido si connettono direttamente o tramite l'hub.

9. Evitare il traffico degli utenti sulla VLAN di gestione

La VLAN di gestione è contenuta in un blocco predefinito, non nell'intera rete.

L'interfaccia di gestione dello switch riceve pacchetti broadcast sulla VLAN di gestione. Se si verificano trasmissioni eccessive (ad esempio un'intasamento di una trasmissione o un'applicazione che non funziona correttamente), la CPU dello switch può sovraccaricarsi, con possibile distorsione del funzionamento dell'STP.

10. Posizionamento della radice STP e della radice STP di backup prevedibile (hardcoded)

La radice STP e la radice STP di backup devono essere configurate in modo che, in caso di errori, la convergenza si verifichi in modo prevedibile e crei una topologia ottimale in ogni scenario. Non lasciare la priorità STP sul valore predefinito, per evitare una selezione imprevedibile del commutatore root.

Informazioni correlate

- Supporto dei prodotti LAN
- Supporto della tecnologia di switching LAN

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).