Configurare STP con Loop Guard e BPDU Skew Detection

Sommario

Introduzione

Questo documento descrive le funzionalità dello Spanning Tree Protocol che hanno lo scopo di migliorare la stabilità della rete di layer 2.

Prerequisiti

Requisiti

In questo documento si presume che il lettore abbia familiarità con le operazioni di base di STP. per ulteriori informazioni, fare riferimento a Comprensione e configurazione dello Spanning Tree Protocol (STP) sugli switch Catalyst.

Componenti usati

Questo documento è basato sugli switch Catalyst, ma la disponibilità delle funzionalità descritte può dipendere dalla versione software in uso.

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.

Premesse

Il protocollo STP (Spanning Tree Protocol) risolve le topologie fisicamente ridondanti in topologie senza loop e di tipo albero. Il problema più grande con STP è che alcuni guasti hardware possono causarne il malfunzionamento. Questo errore crea loop di inoltro (o loop STP). Le principali interruzioni di rete sono causate da loop STP.

Questo documento descrive la funzione LOOP GUARD STP che ha lo scopo di migliorare la stabilità delle reti di layer 2. Questo documento descrive anche il rilevamento di inclinazioni BDPU (Bridge Protocol Data Unit). Il rilevamento dello skew della BPDU è una funzione diagnostica che genera messaggi syslog quando i BPDU non vengono ricevuti in tempo.

Disponibilità delle funzionalità

CatOS

- La funzione STP loop guard è stata introdotta nella versione 6.2.1 del software Catalyst per le piattaforme Catalyst 4000 e Catalyst 5000 e nella versione 6.2.2 per la piattaforma Catalyst 6000.
- La funzione di rilevamento dell'inclinazione della BPDU è stata introdotta nella versione 6.2.1 del software Catalyst per le piattaforme Catalyst 4000 e Catalyst 5000 e nella versione 6.2.2 per la piattaforma Catalyst 6000.

Cisco IOS

- La funzione STP loop guard è stata introdotta nel software Cisco IOS® versione 12.1(12c)EW per gli switch Catalyst 4500 e nel software Cisco IOS versione 12.1(11b)EX per Catalyst 6500.
- La funzione di rilevamento dell'inclinazione della BPDU non è supportata sugli switch Catalyst con software di sistema Cisco IOS.

Ruoli porta STP

Internamente, STP assegna a ciascuna porta bridge (o switch) un ruolo basato su configurazione, topologia, posizione relativa della porta nella topologia e altre considerazioni. Il ruolo porta

definisce il comportamento della porta dal punto di vista STP. In base al ruolo della porta, la porta invia o riceve BPDU STP e inoltra o blocca il traffico di dati. Di seguito viene riportato un breve riepilogo di ciascun ruolo della porta STP:

- Designato (Designated) - Viene selezionata una porta designata per ciascun collegamento (segmento). La porta designata è la porta più vicina al bridge radice. Questa porta invia pacchetti BPDU sul collegamento (segmento) e inoltra il traffico verso il bridge radice. In una rete convergente STP, ciascuna porta designata si trova nello stato di inoltro STP.
- Radice (Root) - Il bridge può avere una sola porta radice. La porta radice è la porta che conduce al bridge radice. In una rete convergente STP, la porta radice si trova nello stato di inoltro STP.
- Alternativo (Alternate) - Le porte alternative conducono al bridge radice ma non sono porte radice. Le porte alternative mantengono lo stato di blocco STP.
- Backup: questo è un caso speciale quando due o più porte tra gli stessi switch sono collegate tra loro, direttamente o tramite supporti condivisi. In questo caso, viene designata una porta e le altre porte vengono bloccate. Il ruolo per questa porta è backup.

Protezione loop STP

Descrizione delle funzionalità

La funzionalità STP Loop Guard fornisce una protezione aggiuntiva dai loop di inoltro di layer 2 (loop STP). Un loop STP si crea quando una porta di blocco STP in una topologia ridondante passa erroneamente allo stato di inoltro. Ciò si verifica in genere perché una delle porte di una topologia con ridondanza fisica (non necessariamente la porta di blocco STP) non riceve più le BPDU del protocollo. STP basa il suo funzionamento sulla ricezione o la trasmissione continua di BPDU in base al ruolo della porta. Le BPDU vengono trasmesse sulla porta designata e ricevute dalla porta non designata.

Quando una delle porte in una topologia con ridondanza fisica non riceve più BPDU, il protocollo STP ritiene che la topologia sia priva di loop. Alla fine, la porta alternativa o di backup bloccata diventa la porta designata e passa allo stato di inoltro. Questa situazione si ripete ciclicamente.

La funzionalità Loop Guard effettua controlli aggiuntivi. Se le BPDU non vengono ricevute su una porta non designata e Loop Guard è abilitata, tale porta passa allo stato di blocco STP loop-inconsistent, anziché allo stato di ascolto / apprendimento / inoltro. Senza la funzionalità Loop Guard, la porta assume il ruolo di porta designata. La porta passa allo stato di inoltro STP e crea un loop.

Quando il controllo loop blocca una porta incoerente, viene registrato questo messaggio:

- CatOS

```
%SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 3/2 in vlan 3. Moved to
```

```
loop-inconsistent state.
```

- Cisco IOS

```
%SPANTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port FastEthernet0/24 on
VLAN0050.
```

Dopo aver ricevuto la BPDU su una porta in uno stato STP con loop incoerente, la porta passa a un altro stato STP. Per la BPDU ricevuta, ciò significa che il ripristino è automatico e che non è necessario alcun intervento. Dopo il ripristino, viene registrato questo messaggio:

- CatOS

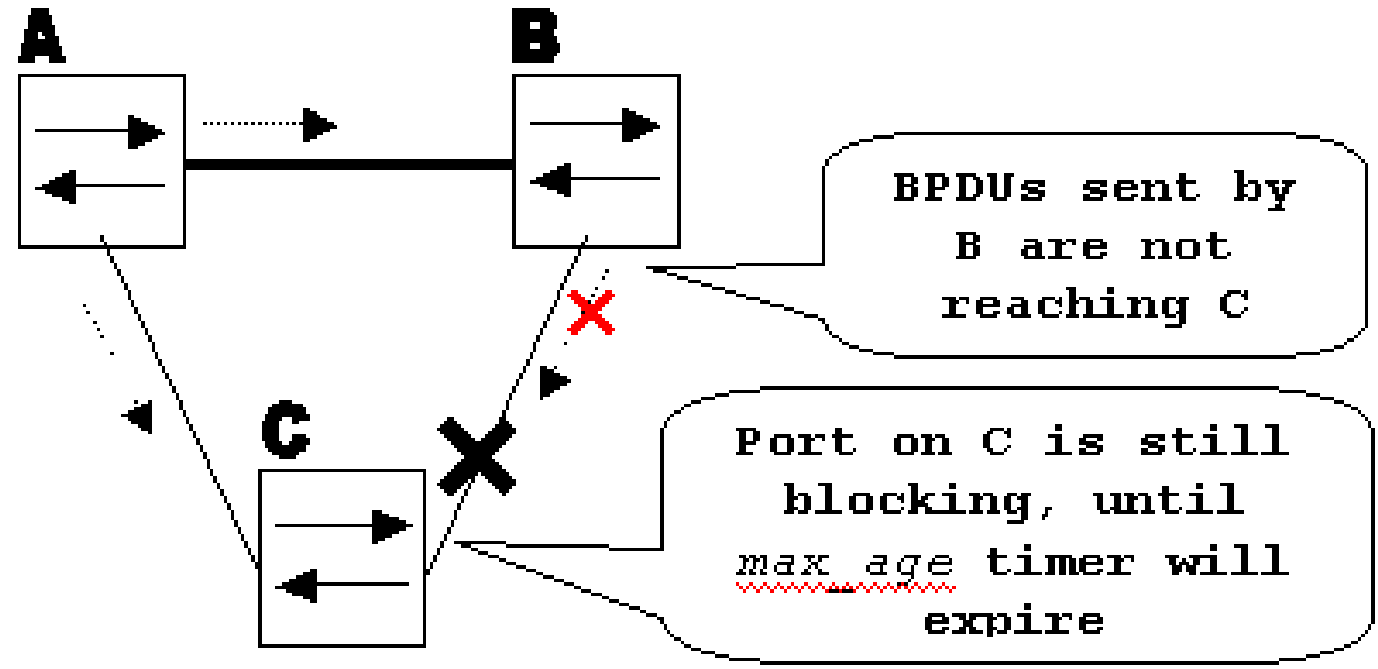
```
%SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.
```

- Cisco IOS

```
%SPANTREE-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port FastEthernet0/24 on
VLAN0050.
```

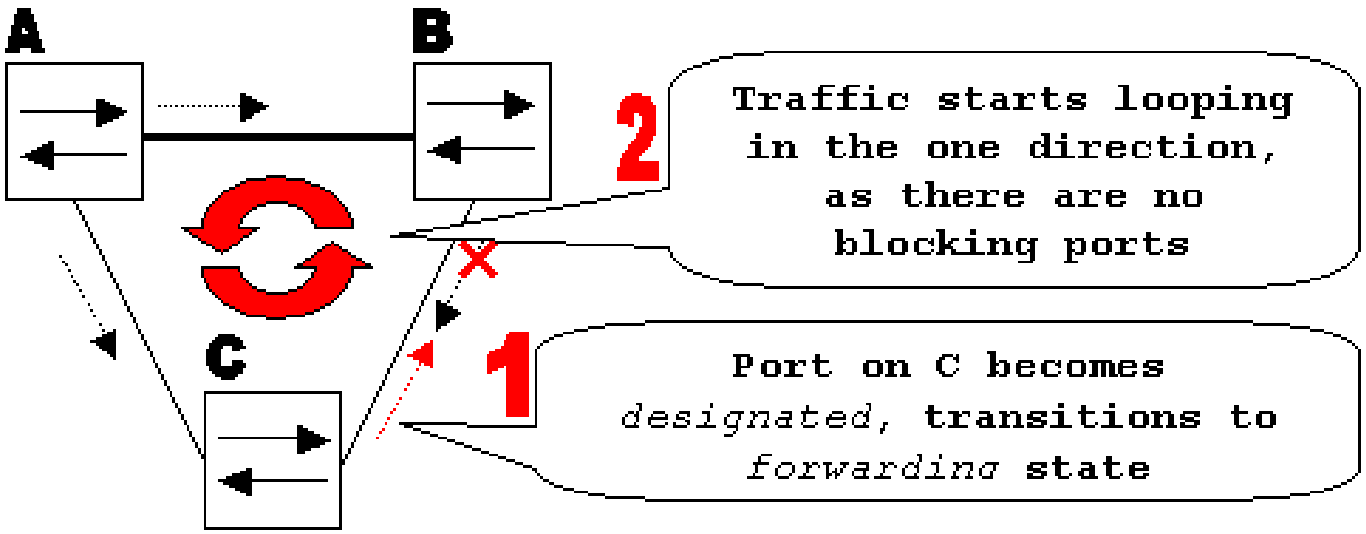
Considerare questo esempio per illustrare questo comportamento:

Lo switch A è lo switch radice. Lo switch C non riceve le BPDU dallo switch B a causa di un errore di collegamento unidirezionale sul collegamento tra lo switch B e lo switch C.



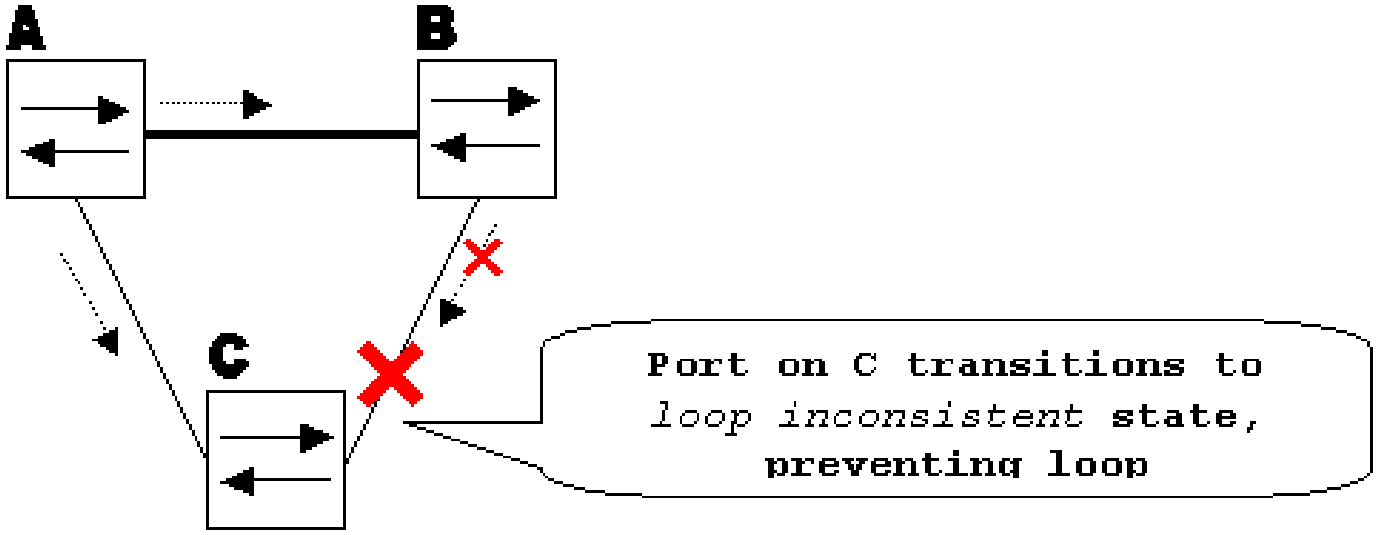
Errore di collegamento unidirezionale

Senza protezione in loop, la porta di blocco STP sullo switch C passa allo stato di ascolto STP quando il timer max_age scade, quindi passa allo stato di inoltro in due volte il tempo forward_delay. Questa situazione si ripete ciclicamente.



Ciclo creato

Con la protezione loop abilitata, la porta di blocco sullo switch C passa in stato di loop incoerente con il protocollo STP quando il timer max_age scade. Una porta in stato di loop incoerente STP non passa il traffico dell'utente, quindi non viene creato un loop. Lo stato di incoerenza del ciclo è in effetti uguale allo stato di blocco.



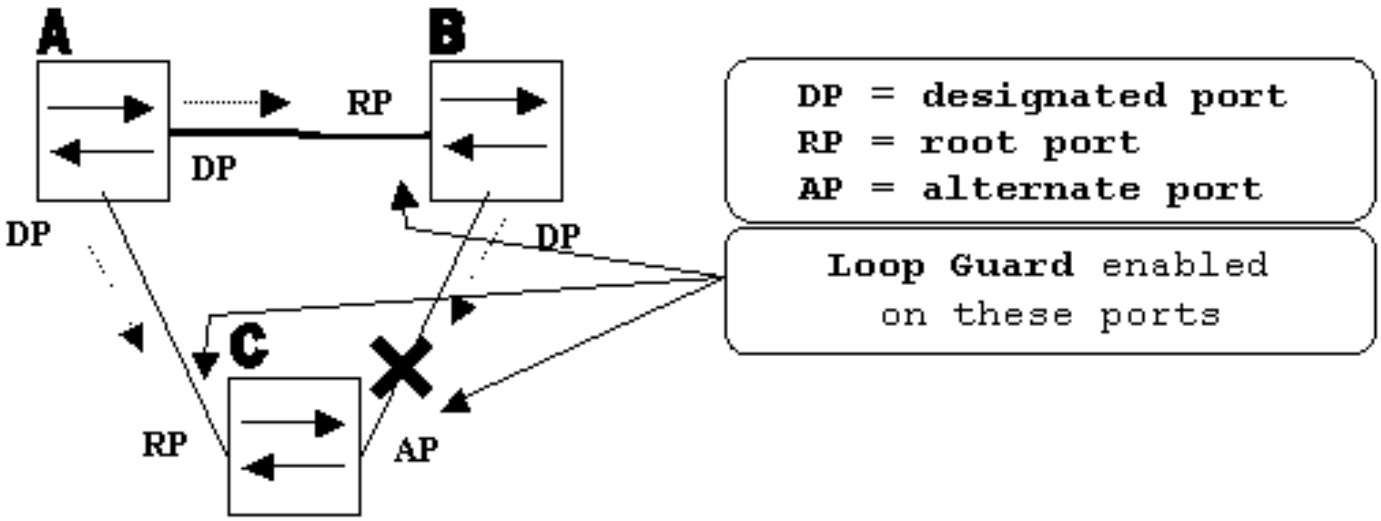
Protezione loop abilitata impedisce il loop

Considerazioni sulla configurazione

La funzione di protezione del loop è abilitata per ciascuna porta. Tuttavia, finché blocca la porta a livello STP, il controllo loop blocca le porte incoerenti per singola VLAN (a causa del protocollo STP per VLAN). In altri termini, se i BPDU non vengono ricevuti sulla porta trunk per una sola VLAN specifica, solo la VLAN viene bloccata (spostata in stato STP non coerente nel loop). Per lo stesso motivo, se abilitato su un'interfaccia EtherChannel, l'intero canale viene bloccato per una VLAN specifica, non solo per un collegamento (perché EtherChannel è considerato come una porta logica dal punto di vista STP).

Su quali porte deve essere abilitato il controllo loop? La risposta più ovvia è data dal blocco delle porte. Tuttavia, non è del tutto corretto. È necessario abilitare la protezione loop sulle porte non designate (più precisamente, sulle porte radice e alternative) per tutte le possibili combinazioni di topologie attive. Finché il controllo del loop non è una funzione per VLAN, la stessa porta (trunk) può essere designata per una VLAN e non per l'altra. Devono essere presi in considerazione anche i possibili scenari di failover.

Esempio



Porte con Loop Guard abilitato

Per impostazione predefinita, la protezione loop è disattivata. Questo comando viene utilizzato per abilitare la protezione loop:

- CatOS

  <#root>

  set spantree guard loop

  Console> (enable)

  set spantree guard loop 3/13

  Enable loopguard will disable rootguard if it's currently enabled on the port(s).
  Do you want to continue (y/n) [n]?

  y

  Loopguard on port 3/13 is enabled.

- Cisco IOS

  <#root>

  spanning-tree guard loop

  Router(config)#

  interface gigabitEthernet 1/1

```
Router(config-if)#
spanning-tree guard loop
```

Con la versione 7.1(1) del software Catalyst (CatOS), la protezione loop può essere abilitata a livello globale su tutte le porte. In effetti, la protezione loop è attivata su tutti i collegamenti point-to-point. Il collegamento point-to-point viene rilevato dallo stato duplex del collegamento. Se il duplex è pieno, il collegamento viene considerato point-to-point. È ancora possibile configurare o ignorare le impostazioni globali per ciascuna porta.

Per abilitare la protezione loop a livello globale, eseguire questo comando:

- CatOS

  <#root>

  ```
  Console> (enable)
  set spantree global-default loopguard enable
  ```

- Cisco IOS

  <#root>

  ```
  Router(config)#
  spanning-tree loopguard default
  ```

Per disabilitare la protezione loop, usare questo comando:

- CatOS

  <#root>

  ```
  Console> (enable)
  set spantree guard none
  ```

- Cisco IOS

```
<#root>

Router(config-if)#

no spanning-tree guard loop
```

Per disabilitare globalmente la protezione loop, usare questo comando:

- CatOS

```
<#root>

Console> (enable)

set spantree global-default loopguard disable
```

- Cisco IOS

```
<#root>

Router(config)#

no spanning-tree loopguard default
```

Per verificare lo stato di protezione del loop, usare questo comando:

- CatOS

```
<#root>

show spantree guard
```

```
Console> (enable)

show spantree guard 3/13

Port                     VLAN Port-State    Guard Type
------------------------ ---- ------------- ----------
3/13                     2    forwarding          loop
Console> (enable)
```

- Cisco IOS

```
<#root>

show spanning-tree


Router#

show spanning-tree summary

Switch is in pvst mode
Root bridge for: none
EtherChannel misconfig guard is enabled
Extended system ID           is disabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Pathcost method used         is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
Total                         0         0        0          0          0
```

Protezione loop e UDLD

La funzionalità Loop Guard e UDLD (Unidirectional Link Detection) si sovrappongono, in parte nel senso che entrambe proteggono dagli errori STP causati dai collegamenti unidirezionali. Tuttavia, queste due caratteristiche differiscono per funzionalità e per il modo in cui affrontano il problema. Nella tabella seguente vengono descritte le funzionalità di protezione loop e UDLD:

Funzionalità	Loop Guard	UDLD
Configurazione	Per porta	Per porta
Granularità azione	Per VLAN	Per porta
Ripristino automatico	Sì	Sì, con la funzione di timeout di errr-disable
Protezione da errori STP causati da collegamenti unidirezionali	Sì, se abilitata su tutte le porte principali e alternative nella topologia ridondante	Sì, se abilitato su tutti i collegamenti nella topologia ridondante
Protezione da errori STP causati da problemi software (lo switch designato non invia BPDU)	Sì	No
Protezione contro cavi non corretti.	No	Sì

In base alle diverse considerazioni di progettazione, è possibile scegliere il protocollo UDLD o la funzione di protezione del loop. Per quanto riguarda l'STP, la differenza più evidente tra le due funzionalità è l'assenza di protezione in UDLD dagli errori STP causati da problemi nel software. Di conseguenza, lo switch designato non invia pacchetti BPDU. Tuttavia, questo tipo di errore è (in ordine di grandezza) più raro rispetto a quello causato dai collegamenti unidirezionali. In cambio, il

protocollo UDLD può essere più flessibile in caso di collegamenti unidirezionali su EtherChannel. In questo caso, UDLD disabilita solo i collegamenti non riusciti e il canale può continuare a funzionare con i collegamenti rimanenti. In questo caso, la protezione del loop lo mette in stato di loop incoerente per bloccare l'intero canale.

Inoltre, la protezione loop non funziona sui collegamenti condivisi o nelle situazioni in cui il collegamento è stato unidirezionale dopo l'attivazione del collegamento. Nell'ultimo caso, la porta non riceve mai BPDU e viene designata. Poiché questo comportamento potrebbe essere normale, questo caso particolare non è coperto da protezione in loop. Il protocollo UDLD offre protezione contro questo scenario.

Come descritto, il livello di protezione più alto viene fornito quando si abilita il protocollo UDLD e la protezione loop.

Interoperabilità di Loop Guard con altre funzionalità STP

Root Guard

La protezione root si esclude a vicenda con la protezione loop. La protezione root viene utilizzata sulle porte designate e non consente alla porta di diventare non designata. Il controllo loop funziona su porte non designate e non consente che la porta venga designata fino alla scadenza di max_age. Impossibile abilitare la protezione radice sulla stessa porta della protezione del loop. Quando il controllo loop è configurato sulla porta, disabilita il controllo radice configurato sulla stessa porta.

Uplink Fast e Backbone Fast

Sia uplink fast che backbone fast sono trasparenti alla protezione del loop. Quando max_age viene saltato dalla backbone rapidamente al momento della riconvergenza, non attiva la protezione del loop. Per ulteriori informazioni su uplink fast e backbone fast, fare riferimento a questi documenti:

- Descrizione e configurazione della funzione Cisco Uplink Fast
- Comprensione e configurazione di Backbone Fast sugli switch Catalyst

PortFast e BPDU Guard e VLAN dinamica

Non è possibile abilitare la protezione del loop per le porte su cui è abilitata portfast. Poiché BPDU Guard funziona sulle porte abilitate portfast, alcune restrizioni si applicano a BPDU Guard. Non è possibile abilitare la funzione di protezione in loop sulle porte VLAN dinamiche perché per queste porte è abilitata la funzione portfast.

Collegamenti condivisi

La protezione del ciclo non deve essere abilitata nei collegamenti condivisi. Se si abilita la protezione loop sui collegamenti condivisi, il traffico proveniente dagli host connessi ai segmenti condivisi può essere bloccato.

MST (Multiple Spanning Tree)

La protezione in loop funziona correttamente nell'ambiente MST.

Rilevamento inclinazione BPDU

La protezione in loop può funzionare correttamente con il rilevamento di distorsione della BPDU.

Rilevamento inclinazione BPDU

Descrizione delle funzionalità

Il funzionamento dell'STP dipende in larga misura dalla ricezione tempestiva delle BPDU. Ad ogni messaggio hello_time (2 secondi per impostazione predefinita), il bridge radice invia pacchetti BPDU. I bridge non radice non rigenerano BPDU per ogni messaggio hello_time, ma ricevono BPDU inoltrati dal bridge radice. Pertanto, ciascun bridge non radice deve ricevere i BPDU su ciascuna VLAN per ciascun messaggio hello_time. In alcuni casi, le BPDU vengono perse o la CPU del bridge è troppo occupata per inoltrare le BPDU tempestivamente. Questi problemi, così come altri, possono causare ritardi nell'arrivo delle BPDU (se raggiunti). Questo problema compromette potenzialmente la stabilità della topologia Spanning Tree.

Il rilevamento dell'inclinazione della BPDU consente allo switch di tenere traccia delle BPDU che arrivano in ritardo e di informare l'amministratore con i messaggi syslog. Per ogni porta sulla quale una BPDU è arrivata in ritardo (o ha inclinato), il rilevamento dell'inclinazione segnala l'inclinazione più recente e la durata dell'inclinazione (latenza). Segnala anche il ritardo BPDU più lungo su questa particolare porta.

Per proteggere la CPU del bridge dall'overload, non viene generato un messaggio syslog ogni volta che si verifica uno skewing BPDU. La velocità dei messaggi è limitata a un messaggio ogni 60 secondi. Tuttavia, se il ritardo della BPDU supera il valore di max_age diviso per 2 (che per impostazione predefinita è pari a 10 secondi), il messaggio viene stampato immediatamente.

Nota: il rilevamento dell'inclinazione della BPDU è una funzione diagnostica. Quando viene rilevato un distorsione della BPDU, il sistema invia un messaggio syslog. Il rilevamento dell'inclinazione della BPDU non intraprende ulteriori azioni correttive.

Nota: la funzione di rilevamento dell'inclinazione della BPDU non è supportata sugli switch Catalyst con software di sistema Cisco IOS.

Questo è un esempio di messaggio syslog generato dal rilevamento di distorsioni BPDU:

```
%SPANTREE-2-BPDU_SKEWING: BPDU skewed with a delay of 10 secs (max_age/2)
```

Considerazioni sulla configurazione

Il rilevamento dello skew della BPDU è configurato per ciascuno switch. L'impostazione predefinita è disattivata. Per abilitare il rilevamento dell'inclinazione della BPDU, usare questo comando:

<#root>

```
Cat6k> (enable)

set spantree bpdu-skewing enable


   Spantree bpdu-skewing enabled on this switch.
```

Per visualizzare le informazioni sull'inclinazione della BPDU, usare il comando show spantree bpdu-skewing <vlan>|<mod/porta>, come mostrato nell'esempio:

<#root>

```
Cat6k> (enable)

show spantree bpdu-skewing 1

Bpdu skewing statistics for vlan 1
Port Last Skew (ms) Worst Skew (ms) Worst Skew Time
-------------- --------------- --------------- -------------------------
3/12 4000 4100 Mon Nov 19 2001, 16:36:04
```

Informazioni correlate

- Migliorare il protocollo STP (Spanning Tree Protocol) con Root Guard
- Configurare la funzione di protocollo UDLD
- Utilizzo di PortFast e di altri comandi per correggere i ritardi di connettività all'avvio della postazione di lavoro
- Supporto tecnico Cisco e download

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).