

Solución de problemas de STP en switches Catalyst

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Causas de las fallas de STP](#)

[Troubleshooting de Loops de Reenvío](#)

- [1. Identificar el bucle](#)
- [2. Descubra la topología \(alcance\) del bucle](#)
- [3. Romper el bucle](#)
- [4. Encuentre y corrija la causa del loop](#)
- [5. Restauración de la redundancia](#)

[Investigar cambios de topología](#)

[Encuentre la causa de la inundación](#)

[Buscar el origen de los TC](#)

[Tome medidas para evitar TCs excesivas](#)

[Solucionar problemas relacionados con el tiempo de convergencia](#)

[Usar comandos de depuración STP](#)

[Proteja la red contra los bucles de reenvío](#)

- [1. Activar la detección de enlaces unidireccionales \(UDLD\) en todos los enlaces de switch a switch](#)
- [2. Activar la protección de bucle en todos los switches](#)
- [3. Activar Portfast en todos los puertos de la estación final](#)
- [4. Establezca EtherChannels en DesirableMode en Ambos Lados \(donde se soporta\) y Non-SilentOption](#)
- [5. No desactivar la negociación automática \(si se admite\) en los enlaces entre switches](#)
- [6. Tenga cuidado al ajustar los temporizadores STP](#)
- [7. Si los ataques de denegación de servicio son posibles, proteja el perímetro STP de la red con protección de raíz](#)
- [8. Habilite la protección BPDU en los puertos habilitados para Portfast para evitar el STP del efecto de los dispositivos de red no autorizados \(como hubs, switches y routers de puente\) que están conectados a los puertos](#)
- [9. Evite el tráfico de usuarios en la VLAN de administración](#)
- [10. Una ubicación de raíz STP predecible \(codificada\) y raíz STP de respaldo](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo utilizar el software Cisco IOS® para resolver problemas con el protocolo de árbol de extensión (STP).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Varios tipos de árbol de extensión y cómo configurarlos. Consulte [Configuración de STP y IEEE 802.1s MST](#) para obtener más información.
- Varias funciones del árbol de extensión y cómo configurarlas. Consulte [Configuración de las Funciones STP](#) para obtener más información.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

Consulte el documento Cisco Technical Tips Conventions (Convenciones sobre consejos técnicos de Cisco) para obtener más información sobre las convenciones de los documentos.

Antecedentes

Existen comandos específicos que se aplican solamente a Catalyst 6500/6000; sin embargo, puede aplicar la mayoría de los principios a cualquier switch Cisco Catalyst que ejecute el software Cisco IOS.

Los problemas con la mayoría de los STP tienen estos tres problemas:

- Loops de reenvío.
- Inundación excesiva debido a una alta tasa de cambios de topología (TC) STP.
- Cuestiones relacionadas con el tiempo de convergencia.

Debido a que un puente no tiene ningún mecanismo para rastrear si un paquete determinado se reenvía varias veces (por ejemplo, un tiempo de vida de IP [TTL]) o se utiliza para descartar el tráfico que circula durante demasiado tiempo en la red. Solo puede existir una ruta entre dos

dispositivos en el mismo dominio de capa 2 (L2).

El propósito de STP es bloquear los puertos redundantes basados en un algoritmo STP, y resolver la topología física redundante en una topología tipo árbol. Un loop de reenvío (como un loop STP) ocurre cuando ningún puerto en una topología redundante se encuentra bloqueado y el tráfico se reenvía en círculos en forma indefinida.

Una vez que se inicia el loop de reenvío, congestionará los links de ancho de banda más bajo a lo largo de su trayectoria. Si todos los links son del mismo ancho de banda, todos los links están congestionados. Esta congestión provoca la pérdida de paquetes y conduce a una situación de caída de la red en el dominio L2 afectado.

Con inundaciones excesivas, los síntomas no son tan evidentes. Los enlaces lentos pueden congestionarse debido al tráfico saturado, y los dispositivos o usuarios detrás de estos enlaces congestionados pueden experimentar lentitud o pérdida total de conectividad.

Causas de las fallas de STP

STP hace ciertas suposiciones sobre su entorno operativo. Estas son las suposiciones más relevantes para este documento:

- Cada enlace entre los dos puentes es bidireccional. Esto significa que, si A se conecta directamente con B, A recibe lo que B ha enviado y B recibe lo que A ha enviado, siempre y cuando el link esté activo entre ellos.
- Cada puente que ejecuta STP puede recibir, procesar y transmitir regularmente Unidades de datos de protocolo de puente STP (BPDU), también conocidas como paquetes STP.

Aunque estas suposiciones parecen lógicas y obvias, hay situaciones en las que no se cumplen. La mayoría de estas situaciones implican un tipo de problema de hardware; sin embargo, los defectos de software también pueden conducir a fallas de STP. Diversos fallos de hardware, configuraciones erróneas y problemas de conexión causan la mayoría de los fallos de STP, mientras que los fallos de software son la minoría. Los fallos de STP también pueden ocurrir debido a conexiones adicionales innecesarias que existen entre los switches. Las VLAN entran en un estado de inactividad debido a estas conexiones adicionales. Para resolver este problema, elimine todas las conexiones no deseadas entre los switches.

Cuando una de estas suposiciones no se cumple, uno o más puentes no pueden recibir o procesar las BPDU. Esto significa que el puente (o puentes) no detecta la topología de red. Sin conocimiento de la topología correcta, el switch no puede bloquear los loops. Por lo tanto, el tráfico inundado circula sobre la topología en loop, consume todo el ancho de banda y desactiva la red.

Entre los ejemplos de por qué los switches no pueden recibir BPDU se incluyen los transceptores defectuosos o los convertidores de interfaz Gigabit (GBIC), los problemas de cable o las fallas de hardware en el puerto, la tarjeta de línea o el motor supervisor. Una razón frecuente de las fallas de STP es un link unidireccional entre los puentes. En tal condición, un puente envía BPDU, pero el puente de flujo descendente nunca las recibe. El procesamiento STP también puede ser

interrumpido por una CPU sobrecargada (99 por ciento o más) porque el switch no puede procesar las BPDU recibidas. Las BPDU pueden dañarse a lo largo de la trayectoria de un puente a otro, lo que también impide un comportamiento STP adecuado.

Aparte de los loops de reenvío, cuando no se bloquean puertos, hay situaciones en las que sólo ciertos paquetes se reenvían incorrectamente a través de los puertos que bloquean el tráfico. En la mayoría de los casos, esto se debe a problemas de software. Tal comportamiento puede causar loops lentos. Esto significa que algunos paquetes están en loop, pero la mayor parte del tráfico sigue fluyendo a través de la red, porque los links no están congestionados.

Troubleshooting de Loops de Reenvío

Los bucles de reenvío varían mucho tanto en su origen (causa) como en su efecto. Debido a la amplia variedad de problemas que pueden afectar el STP, este documento sólo puede proporcionar pautas generales sobre cómo resolver problemas de loops de reenvío.

Antes de iniciar la solución de problemas, necesita esta información:

- Un diagrama de topología real que detalla todos los switches y puentes.
- Sus números de puerto correspondientes (interconectados).
- Detalles de configuración de STP, como qué switch es la raíz y la raíz de respaldo, qué links tienen un costo o prioridad no predeterminada y la ubicación de los puertos que bloquean el tráfico.

1. Identificar el bucle

Cuando se ha desarrollado un loop de reenvío en la red, los síntomas usuales son:

- Pérdida de conectividad con, desde y a través de regiones de red afectadas.
- Uso excesivo de CPU en routers conectados a los segmentos afectados o VLAN que puede generar diversos síntomas, como inestabilidad en el vecino de protocolo de ruteo o inestabilidad en el router activo de Protocolo de ruteo de reserva directa (HSRP).
- Alta utilización de enlaces (a menudo al 100%).
- Alta utilización de la placa base del switch (en comparación con la utilización de referencia).
- Mensajes de registro del sistema que indican bucles de paquetes en la red (por ejemplo, mensajes de dirección IP duplicada HSRP).
- Mensajes de registro del sistema que indican el reaprendizaje constante de direcciones o mensajes de inestabilidad de direcciones MAC.
- El número de caídas de salida en muchas interfaces aumenta.

Cualquiera de estas razones por sí sola puede indicar diferentes problemas (o ningún problema

en absoluto). Sin embargo, cuando se observan muchos de estos al mismo tiempo, es muy probable que un loop de reenvío se haya desarrollado en la red. La manera más rápida de verificar esto es verificar la utilización del tráfico de la placa de interconexiones del 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: El Catalyst 4000 con el software del IOS de Cisco no soporta actualmente este comando.

Si el nivel de tráfico actual es excesivo o si se desconoce el nivel de línea de base, compruebe si el nivel de pico se ha alcanzado recientemente y si está próximo al nivel de tráfico actual. Por ejemplo, si el nivel de tráfico máximo es del 15% y se alcanzó hace solo dos minutos y el nivel de tráfico actual es del 14%, esto significa que el switch tiene una carga inusualmente alta. Si la carga de tráfico está en un nivel normal, entonces probablemente eso significa que no hay loop o que este dispositivo no está involucrado en el loop. Sin embargo, todavía podría estar involucrado en un loop lento.

2. Descubra la topología (alcance) del bucle

Una vez que se ha establecido que el motivo de la interrupción de la red es un loop de reenvío, la prioridad más alta es detener el loop y restaurar el funcionamiento de la red.

Para detener el loop, debe saber qué puertos participan en el loop: observe los puertos con la mayor utilización de link (paquetes por segundo). El comando `show interface` Cisco IOS software muestra la utilización de cada interfaz.

Para mostrar solamente la información de utilización y el nombre de la interfaz (para un análisis rápido), filtre la salida de la expresión regular con el software del IOS de Cisco. Ejecute la interfaz `show | include line|Vseccommand` para mostrar solamente las estadísticas de paquetes por segundo y el nombre de la interfaz:

```
<#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
```


Preste atención a las interfaces con la mayor utilización de enlaces. En este ejemplo, estas son las interfaces g2/3, g2/4 y g2/8; son los puertos que participan en el loop.

3. Romper el bucle

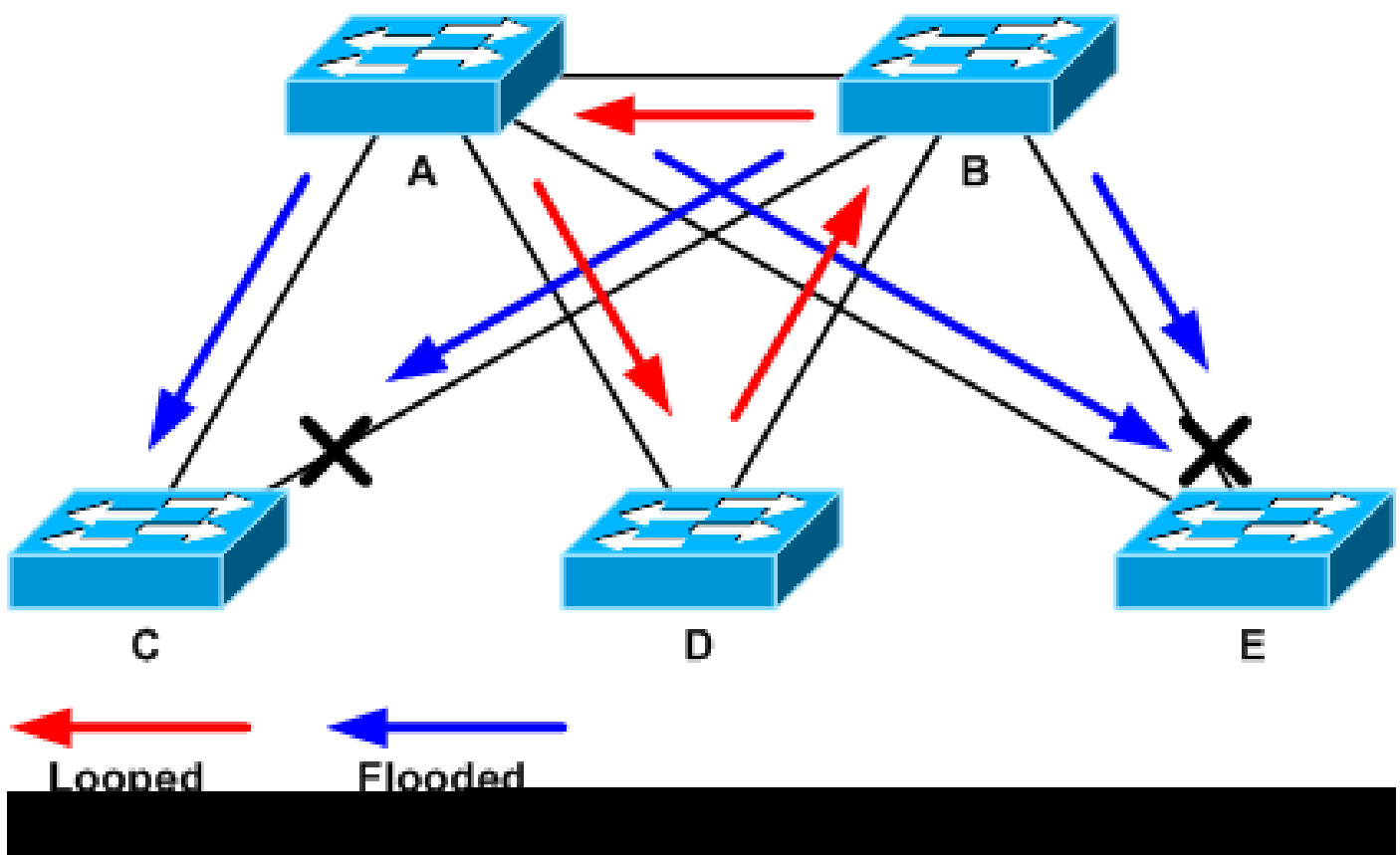
Para romper el loop, debe apagar o desconectar los puertos involucrados. Es particularmente importante no sólo detener el loop sino también encontrar y reparar la causa raíz del loop. Es relativamente más fácil romper el bucle

 Nota: No tiene que apagar o desconectar todos los puertos al mismo tiempo. Puedes apagarlos de uno en uno. Es mejor apagar los puertos en el punto de agregación afectado por el loop, como una distribución o un switch de núcleo. Si apaga todos los puertos a la vez y los habilita o vuelve a conectar uno por uno, no funciona; el loop se detiene y no puede iniciarse inmediatamente después de que el puerto defectuoso se vuelva a conectar. Por lo tanto, es difícil correlacionar la falla con cualquier puerto en particular.

 Nota: Para interrumpir el loop, se recomienda que recopile información antes de reiniciar los switches. De lo contrario, el análisis posterior de la causa raíz es difícil. Después de inhabilitar o desconectar cada puerto, debe verificar si la utilización de la placa de interconexiones del switch ha vuelto a un nivel normal.

 Nota: Tenga en cuenta que los puertos no mantienen el loop pero están inundando el tráfico que llega con el loop. Cuando apaga estos puertos de inundación, sólo reduce la utilización de la placa de interconexiones en una pequeña cantidad, pero no detiene el loop.

En la siguiente topología de ejemplo, el loop está entre los switches A, B y D. Por lo tanto, los links AB, AD y BD se mantienen. Si apaga cualquiera de estos links, detendrá el loop. Los links AC, AE, BC y BE están inundando el tráfico que llega con el loop.



Tráfico en bucle e inundado

Después de que se apague el puerto de soporte, la utilización de la placa de interconexiones baja a un valor normal. Debe saber qué apagado del puerto llevó la utilización de la placa de interconexiones (y la utilización de otros puertos) a un nivel normal. En este punto, el loop se detiene y el funcionamiento de la red mejora; sin embargo, debido a que la causa original del loop no fue arreglada, todavía hay otros problemas.

4. Encuentre y corrija la causa del loop

Una vez que se detiene el loop, debe determinar la razón por la que comenzó el loop. Esta es la parte difícil del proceso porque las razones pueden variar. También es difícil formalizar un

procedimiento exacto que funcione en todos los casos.

Pautas:

- Investigue el diagrama de topología para encontrar una ruta redundante. Esto incluye el puerto de soporte que se encuentra en el paso anterior y que vuelve al mismo switch (los paquetes de trayectoria que se mencionan durante el loop). En la topología de ejemplo anterior, esta ruta es AD-DB-BA.
- Para cada switch en la trayectoria redundante, verifique si el switch conoce la raíz STP correcta.

Todos los switches en una red L2 deben acordar una raíz STP común. Es un síntoma claro de problemas cuando los puentes muestran consistentemente un ID diferente para la raíz STP en una VLAN o instancia STP determinada. Ejecute el comando `show spanning-tree vlan vlan-id` para mostrar el ID del puente raíz para una VLAN determinada:

```
<#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

El número de VLAN se puede encontrar en el puerto, porque los puertos involucrados en el loop se establecieron en pasos anteriores. Si los puertos en cuestión son troncos, a menudo están comprendidas todas las VLAN en el tronco. Si este no es el caso (por ejemplo, si parece que el loop ha ocurrido en una sola VLAN), puede intentar emitir las interfaces `show | include` el comando `L2|line|broadcast` (sólo en motores Supervisor 2 y posteriores en switches Catalyst 6500/6000 Series, porque el Supervisor 1 no proporciona estadísticas de conmutación por VLAN). Observe solamente las interfaces VLAN. La VLAN con el mayor número de paquetes conmutados suele ser la que produjo el 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
```

En este ejemplo, la VLAN 1 representa el mayor número de difusiones y tráfico conmutado por L2. Asegúrese de que el puerto raíz esté identificado correctamente.

El puerto raíz debe tener el costo más bajo para el puente raíz (a veces una trayectoria es más corta en términos de saltos pero más larga en términos de costo, ya que los puertos de baja velocidad tienen costos más altos). Para determinar qué puerto se considera la raíz para una VLAN determinada, ejecute el 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

Asegúrese de que las BPDUs se reciban regularmente en el puerto raíz y en los puertos que se supone que deben bloquearse.

Las BPDUs son enviadas por el bridge root en cada intervalo (dos segundos de forma predeterminada). Los puentes no raíz reciben, procesan, modifican y propagan las BPDUs que se reciben de la raíz. Ejecute el comando `show spanning-tree interface detail` para ver si se reciben las BPDUs:

```
<#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: Se ha recibido una BPDU entre las dos salidas del comando (el contador pasó de 53 a 54).

Los contadores que aparecen son, en realidad, contadores mantenidos por el proceso STP en sí mismo. Esto significa que, si los contadores de recepción incrementaron, no sólo se recibió BPDU por un puerto físico, sino que también fue recibida por el proceso STP. Si el contador de `received BPDU` no aumenta en el puerto que se supone que es el puerto raíz alternativo o de respaldo, verifique si el puerto recibe multicast en absoluto (las BPDU se envían como multicast). Ejecute el comando `show interface interface counters`:

```
<#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

Puede encontrar una breve descripción de los roles de puerto STP en [la sección Mejora de STP con protección de loop y detección de desviación de BPDU de Mejoras del protocolo de árbol de expansión mediante las funciones de protección de loop y detección de desviación de BPDU](#). Si no se reciben BPDU, verifique si el puerto cuenta los errores. Ejecute el comando `show interface 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  Runts   Giants
Gi4/3      0           0         0         0         0         0       0
```

Es posible que el puerto físico reciba las BPDU pero aún no alcance el proceso STP. Si los comandos utilizados en los dos ejemplos anteriores muestran que se reciben algunas multidifusiones y que no se cuentan los errores, verifique si las BPDU se descartan en el nivel de proceso STP. Ejecute el comando `remote command switch test spanning-tree process-statscommand` en el 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
```

El comando utilizado en este ejemplo muestra las estadísticas de proceso STP. Es importante

verificar que los contadores de caídas no aumenten y que los paquetes recibidos aumenten. Si los paquetes recibidos no aumentan pero el puerto físico sí recibe multidifusión, verifique que los paquetes son recibidos por la interfaz en banda del switch (la interfaz de la CPU). Ejecute el comando `remote switch show ibc | i rx_inputcommand` en el 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
```

Este ejemplo muestra que, entre las salidas, el puerto en banda ha recibido 23 paquetes.

 Nota: Estos 23 paquetes no son sólo paquetes BPDU; es un contador global para todos los paquetes recibidos por el puerto en banda.

Si no hay ninguna indicación de que las BPDU se descarten en el switch o puerto local, debe desplazarse al switch del otro lado del link y verificar si ese switch envía las BPDU. Verifique si las BPDU se envían regularmente en los puertos designados no raíz. Si el rol de puerto está de acuerdo, el puerto envía BPDU, pero el vecino no las recibe. Verifique si se envían las BPDU. Ejecute el comando `show spanning-tree interface 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
```

En este ejemplo, se envían dos BPDU entre las salidas.

 Nota: El proceso STP mantiene el contador `BPDU:sentcounter`. Esto significa que el contador indica que la BPDU se envió hacia el puerto físico y se envía. Verifique si los contadores de puertos aumentan para los paquetes de multidifusión transmitidos. Ejecute el comando `show interface interface counters`. Esto puede ayudar a determinar el flujo de tráfico de las BPDU.

```
<#root>
```

```
cat#
```

```
show interface g3/1 counters
```

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

Port	OutOctets	OutUcastPkts
------	-----------	--------------

```
OutMcastPkts
```

Port	OutBcastPkts	OutMcastPkts
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

Port	OutOctets	OutUcastPkts
Gi3/1	131826447	3442

872346

386

Con todos estos pasos, la idea es encontrar el switch o link donde las BPDU no se reciben, envían o procesan. Es posible que el STP haya calculado el estado correcto para el puerto, pero debido a un problema del plano de control, no puede establecer este estado en el hardware de reenvío. Se puede crear un loop si el puerto no está bloqueado en el nivel de hardware. Si cree que se trata de un problema en su red, póngase en [contacto con el servicio de asistencia técnica de Cisco](#) para obtener más ayuda.

5. Restauración de la redundancia

Una vez que se encuentra el dispositivo o link que causa el loop, este dispositivo debe aislarse de la red o el problema debe resolverse (como reemplazar la fibra o GBIC). Los links redundantes, desconectados en el Paso 3, deben ser restaurados.


Es importante no manipular el dispositivo o link que causa el loop, porque muchas condiciones que conducen a un loop son transitorias, intermitentes e inestables. Esto significa que, si la condición se aclara en o después de la investigación, la condición no ocurre por un tiempo o no ocurre en absoluto. Se debe registrar la condición para que el [Soporte Técnico de Cisco](#) pueda investigarla más a fondo. Es importante que recopile información sobre la condición antes de reiniciar los switches. Si una condición desaparece, es imposible determinar la causa raíz del loop. Si recopila la información, se asegura de que este problema no cause el loop nuevamente. Para obtener más información, consulte [Protección de la Red contra Loops de Reenvío](#).

Investigar cambios de topología

La función del mecanismo de cambio de topología (TC) es corregir las tablas de reenvío L2 después de que la topología haya cambiado. Esto es necesario para evitar una interrupción de la conectividad porque las direcciones MAC previamente accesibles a través de determinados puertos pueden cambiar y volverse accesibles a través de diferentes puertos. TC acorta la antigüedad de la tabla de reenvío en todos los switches de la VLAN donde se produce el TC. Por

lo tanto, si la dirección no se vuelve a aprender, se desactualiza y se produce la inundación para garantizar que los paquetes lleguen a la dirección MAC de destino.

TC se activa por el cambio del estado STP de un puerto hacia o desde el estado de reenvío STP. Después de TC, incluso si la dirección MAC de destino en particular ha caducado, la inundación no continuará por mucho tiempo. La dirección es reaprendida por el primer paquete que proviene del host cuya dirección MAC ha caducado. El problema puede surgir cuando el TC ocurre repetidamente, con intervalos cortos. Los switches están envejeciendo constantemente rápidamente sus tablas de reenvío, por lo que la inundación puede ser casi constante.

 Nota: Con STP rápido o STP múltiple (IEEE 802.1w e IEEE 802.1s), el TC se activa por un cambio del estado del puerto a `reenvío`, así como el cambio de rol desde `designatedtoroot`. Con el STP rápido, la tabla de reenvío L2 se vacía inmediatamente, a diferencia de 802.1d, que acorta el tiempo de envejecimiento. El vaciado inmediato de la tabla de reenvío restaura la conectividad más rápido, pero puede causar más inundación

TC es un evento poco común en una red bien configurada. Cuando un link en un puerto de switch sube o baja, eventualmente hay un TC, una vez que el estado STP del puerto se cambia a `reenvío`. Cuando el puerto está inestable, se podrían ocasionar TC e inundaciones reiteradamente.

Los puertos con la función STP portfast habilitada no pueden causar TC cuando entran o salen del estado de `reenvío`. La configuración de portfast en todos los puertos de los dispositivos finales (como impresoras, PC y servidores) puede limitar los TC a una cantidad baja y se recomienda encarecidamente.

Si hay TC repetitivos en la red, debe identificar el origen de estos TC y tomar medidas para reducirlos, para reducir la inundación al mínimo.

Con 802.1d, la información de STP sobre un evento TC se distribuye entre los puentes a través de una Notificación TC (TCN), que es un tipo especial de BPDU. Si sigue los puertos que reciben TCN BPDU, puede encontrar el dispositivo que originó los TC.

Encuentre la causa de la inundación

Puede determinar que hay una inundación de rendimiento lento, caídas de paquetes en links que se supone no están congestionados y el analizador de paquetes muestra varios paquetes unicast al mismo destino que no está en el segmento local. Para obtener más información sobre la inundación de unidifusión, consulte [Inundación de unidifusión en redes de campus conmutadas](#).

En un Catalyst 6500/6000 que ejecuta Cisco IOS Software, puede verificar el contador del motor de reenvío (sólo en el motor Supervisor 2) para estimar la cantidad de inundación. Ejecute el comando `remote switch show earl statistics | 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

```

En este ejemplo, la primera columna muestra el cambio desde la última vez que se ejecutó este comando, y la segunda columna muestra el valor acumulado desde el último reinicio. La primera línea muestra la cantidad de tramas inundadas y la segunda la cantidad de tramas procesadas. Si los dos valores están cerca, o el primer valor aumenta a una velocidad alta, puede que el switch esté inundando el tráfico. Sin embargo, esto solo se puede utilizar junto con otras formas de verificar la inundación, ya que los contadores no son granulares. Hay un contador por switch, no por puerto o VLAN. Es normal ver algunos paquetes de inundación, ya que el switch siempre puede inundarse si la dirección MAC de destino no está en la tabla de reenvío. Este puede ser el caso cuando el switch recibe un paquete con una dirección de destino que aún no se ha aprendido.

Buscar el origen de los TC

Si el número de VLAN es conocido para la VLAN donde se produce una inundación excesiva, verifique los contadores de STP para ver si el número de TC es alto o aumenta regularmente. Ejecute el comando `show spanning-tree vlan vlan-id detail` (en este ejemplo, se utiliza 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

```

Si el número de VLAN no se conoce, puede usar el analizador de paquetes o revisar los contadores de TC para todas las VLAN.

Tome medidas para evitar TCs excesivas

Puede monitorear el número de contadores de cambios de topología para ver si aumenta regularmente. Luego, vaya al puente que está conectado al puerto que se muestra, para recibir el último TC (en el ejemplo anterior, el puerto GigabitEthernet1/1) y ver de dónde vino el TC para ese puente. Este proceso debe repetirse hasta que se encuentre el puerto de la estación final sin STP portfast habilitado, o hasta que se encuentre el link inestable que necesita ser corregido. Es necesario repetir todo el procedimiento si los TC proceden de otras fuentes. Si el link pertenece a un host final, puede configurar la función portfast para evitar la generación de TC.

 Nota: En la implementación STP del software Cisco IOS, el contador para TCs sólo puede incrementarse si un puerto en una VLAN recibe una TCN BPDU. Si se recibe una BPDU de configuración normal con un indicador TC establecido, el contador TC no se incrementa. Esto significa que, si sospecha que un TC es la razón de la inundación, comience a rastrear las fuentes para el TC desde el puente raíz STP en esa VLAN. Puede tener la información más precisa sobre el número y la fuente de los TC.

Solucionar problemas relacionados con el tiempo de convergencia

Hay situaciones en las cuales el funcionamiento efectivo de un STP no coincide con el comportamiento esperado. Estos son los dos problemas más frecuentes:

- La convergencia o reconvergencia de STP tarda más de lo esperado.
- El resultado de la topología es diferente del esperado.

A menudo, estas son las razones de este comportamiento:


- Una falta de coincidencia entre la topología documentada y la real.
- Configuración incorrecta, como una configuración incoherente de los temporizadores STP, un diámetro STP que aumenta o una configuración incorrecta de Portfast.
- CPU del switch sobrecargada durante la convergencia o reconvergencia.
- Defecto de software.

Como se mencionó anteriormente, este documento sólo puede proporcionar pautas generales para la resolución de problemas, debido a la amplia variedad de problemas que podrían afectar el STP. Para comprender por qué la convergencia tarda más de lo esperado, observe la secuencia de eventos STP para averiguar qué sucede y en qué orden. Debido a que la implementación STP en el software Cisco IOS no registra los resultados (excepto para eventos específicos, tales como

inconsistencias de puerto), puede utilizar el software Cisco IOS para depurar el STP para obtener una vista más clara. Para STP, con un Catalyst 6500/6000 que ejecuta Cisco IOS Software, el procesamiento se realiza en el Switch Processor (SP) (o Supervisor), por lo que los debugs deben habilitarse en el SP. Para los grupos de puentes del software Cisco IOS, el procesamiento se realiza en el procesador de ruta (RP), por lo que los debugs deben habilitarse en el RP (MSFC).

Usar comandos de depuración STP

Muchos comandos STPdebug están pensados para el uso en ingeniería de desarrollo. No proporcionan ningún resultado que sea significativo para alguien sin conocimiento detallado de la implementación STP en el software Cisco IOS. Algunas depuraciones pueden proporcionar resultados que se pueden leer instantáneamente, como cambios de estado de puerto, cambios de rol, eventos como TC y un volcado de BPDU recibidas y transmitidas. Esta sección no proporciona una descripción completa de todas las depuraciones, sino que presenta brevemente las que se utilizan con más frecuencia.

 Nota: Cuando utilice los comandos debug, habilite las depuraciones mínimas necesarias. Si no se necesitan depuraciones en tiempo real, registre el resultado en el registro en lugar de imprimirlo en la consola. Los debugs excesivos pueden sobrecargar la CPU e interrumpir el funcionamiento del switch.

Para dirigir el resultado de la depuración al registro en lugar de a la consola o a las sesiones Telnet, ejecute los comandos `logging console informational` and `no logging monitor` en el modo de configuración global. Para ver el registro de eventos generales, ejecute el comando `debug spanning-tree eventcommand` para Per VLAN Spanning-Tree (PVST) y Rapid-PVST. Esta es la primera depuración que brinda información sobre lo que sucedió con el STP. En el modo de árbol de expansión múltiple (MST), no funciona el comando `debug spanning-tree eventcommand`. Por lo tanto, ejecute el comando `debug spanning-tree mstp rolespara` para ver los cambios del rol de puerto. Para ver los cambios de estado del puerto STP, ejecute el comando `debug spanning-tree switch statecommand` junto con el comando `debug pm vpccommand`:

```
<#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
```

Para comprender por qué el STP se comporta de cierta manera, a menudo es útil ver las BPDU que recibe y envía el switch:

```
<#root>
```

```
cat-sp#
```

```
debug spanning-tree bpdv 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 0000000000000000074F1CE8470000001380480006525F0E4
      080100100140002000F00
```

```
Nov 6 11:44:27: SP: STP: VLAN1 Gi2/1:0000 00 00 00 000000074F1CE847 00000013
      80480006525F0E40 8010 0100 1400 0200 0F00
```

Esta depuración funciona para los modos PVST, Rapid-PVST y MST, pero no descodifica el contenido de las BPDU. Sin embargo, puede utilizarlo para asegurarse de que se reciben las BPDU. Para ver el contenido de la BPDU, ejecute el comando `debug spanning-tree switch rx decode` junto con el comando `debug spanning-tree switch rx processcommand` para PVST y Rapid-PVST. Ejecute el comando `debug spanning-tree mstp bpdv-rx` para ver el contenido de la BPDU para 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
```

Para el modo MST, puede habilitar la decodificación detallada de BPDU con este comando debug:

```
<#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: Para Cisco IOS Software Release 12.1.13E y posteriores, se soportan los debugs condicionales para STP. Esto significa que puede depurar las BPDU que se reciben o transmiten por puerto o por VLAN.

Ejecute los comandos `debug condition vlan vlan_num` o `debug condition interface interface` para limitar el alcance de la salida de depuración a per-interface o per-VLAN.

Proteja la red contra los bucles de reenvío

Cisco ha desarrollado una serie de funciones y mejoras para proteger las redes contra loops de reenvío cuando un STP no puede gestionar ciertos fallos.

Cuando se resuelve el problema del STP, ayuda a aislar y posiblemente encontrar la causa de una falla particular, mientras que la implementación de estas mejoras es la única manera de proteger la red contra loops de reenvío.

Estos son métodos para proteger su red contra loops de reenvío:

1. Activar la detección de enlaces unidireccionales (UDLD) en todos los enlaces de switch a switch

Para obtener más información sobre el UDLD, consulte [Comprensión y Configuración de la Función Unidirectional Link Detection Protocol](#).

2. Activar la protección de bucle en todos los switches

Para obtener más información sobre la protección de loop, consulte [Mejoras del Spanning-Tree Protocol con las Funciones de Protección de Loop y Detección de Desviación de BPDU](#).


Cuando está habilitado, UDLD y la protección de loop eliminan la mayoría de las causas de los loops de reenvío. En lugar de crear un bucle de reenvío, el enlace defectuoso (o todos los enlaces dependientes del hardware defectuoso) se apagan o se bloquean.



Nota: Aunque estas dos funciones parecen algo redundantes, cada una tiene sus propias funciones. Por lo tanto, utilice ambas funciones al mismo tiempo para proporcionar el máximo nivel de protección. Para obtener una comparación detallada de UDLD y la protección de loop, consulte [Protección de Loop vs. Detección de Link Unidireccional](#).


Existen diferentes opiniones respecto de si debe usar UDLD agresivo o normal. El UDLD agresivo no puede proporcionar más protección contra loops en comparación con el UDLD de modo normal. El UDLD agresivo detecta escenarios de atascamiento de puertos (cuando el link está activo, pero no hay agujeros negros de tráfico asociados). La desventaja de esta funcionalidad agregada es que el UDLD agresivo puede potencialmente inhabilitar links en los que no hay falla consistente alguna. A menudo, la gente confunde la modificación del `UDLDhellointerval` con la función UDLD agresiva. Esto es incorrecto. Los temporizadores pueden modificarse en ambos

modos de UDLD.

 Nota: En casos excepcionales, el UDLD agresivo puede apagar todos los puertos de enlace ascendente, lo que básicamente aísla el switch del resto de la red. Por ejemplo, esto podría suceder cuando ambos switches ascendentes experimentan una utilización de CPU extremadamente alta y se utiliza el modo agresivo UDLD. Por lo tanto, se recomienda que configure tiempos de espera que no se puedan erosionar, si el switch no tiene una administración fuera de banda en funcionamiento.

3. Activar Portfast en todos los puertos de la estación final

Debe habilitar portfast para limitar la cantidad de TC y la subsiguiente inundación, que puede afectar el rendimiento de la red. Utilice solamente este comando con los puertos que conectan con las estaciones finales. De lo contrario, un loop de topología accidental puede causar un loop de paquete de datos e interrumpir el funcionamiento del switch y la red.

 Precaución: Tenga cuidado cuando utilice el comando `no spanning-tree portfast`. Este comando solamente quita cualquier comando portfast específico del puerto. Este comando habilita implícitamente portfast si define el comando `spanning-tree portfast default` en el modo de configuración global y si el puerto no es un puerto trunk. Si no configura portfast globalmente, el comando `no spanning-tree portfast` es equivalente al comando `spanning-tree portfast disable`.

4. Establezca EtherChannels en el modo `Disable` en ambos lados (donde se soporta) y la opción `no silenciosa`

Desirablemode puede habilitar el protocolo de agregación de puertos (PAgP) para garantizar la coherencia en tiempo de ejecución entre los pares de canalización. Esto proporciona un grado adicional de protección contra bucles, especialmente durante las reconfiguraciones de canal (como cuando los enlaces se unen o salen del canal y la detección de fallos de enlace). Existe un Channel Misconfiguration Guard incorporado, que está habilitado de forma predeterminada y que evita los loops de reenvío debido a una configuración incorrecta del canal u otras condiciones. Para obtener más información sobre esta función, consulte [Cómo Comprender la Detección de Inconsistencias EtherChannel](#).

5. No desactivar la negociación automática (si se admite) en los enlaces entre switches

Los mecanismos de negociación automática pueden transmitir información de fallas remotas, que es la manera más rápida de detectar fallas en el lado remoto. Si se detecta una falla en el lado remoto, el lado local hace caer el link incluso si el link recibe pulsos. En comparación con los mecanismos de detección de alto nivel como el UDLD, la negociación automática es extremadamente rápida (en microsegundos) pero carece de la cobertura de extremo a extremo del UDLD (como la ruta de datos completa: CPU—lógica de reenvío—puerto1—puerto2—lógica de reenvío—CPU versus puerto1—puerto2). El modo UDLD agresivo proporciona una

funcionalidad similar a la de la negociación automática con respecto a la detección de fallas. Si se admite una negociación en ambos extremos del link, no hay necesidad de permitir un UDLD de modo agresivo.

6. Tenga cuidado al ajustar los temporizadores STP

Los temporizadores STP dependen unos de otros y de la topología de red. STP no funciona correctamente con las modificaciones arbitrarias realizadas en los temporizadores. Para obtener más información sobre los temporizadores STP, consulte [Comprensión y ajuste de los temporizadores del protocolo de árbol de expansión](#).

7. Si los ataques de denegación de servicio son posibles, proteja el perímetro STP de la red con protección de raíz

El protector de raíz y el protector BPDU le permiten asegurar el STP contra la influencia del exterior. Si tal ataque es una posibilidad, la protección de raíz y la protección de BPDU se deben utilizar para proteger la red. Para obtener más información sobre la protección de raíz y la protección BPDU, consulte estos documentos:

- [Mejora del protector de raíz del protocolo de árbol de expansión](#)
- [Mejoras de la Protección de Spanning Tree PortFast BPDU](#)

8. Habilite la protección BPDU en los puertos habilitados para Portfast para evitar el STP del efecto de los dispositivos de red no autorizados (como hubs, switches y routers de puente) que están conectados a los puertos

Si configura la protección de raíz correctamente, evita que el STP influya desde el exterior. Si la protección BPDU está habilitada, apaga los puertos que reciben cualquier BPDU. Esto es útil para investigar incidentes, porque la protección BPDU produce el mensaje syslog y apaga el puerto. Si las protecciones de raíz o BPDU no evitan los loops de ciclo corto, entonces dos puertos activados rápidamente se conectan directamente o a través del hub.

9. Evite el tráfico de usuarios en la VLAN de administración

La VLAN de administración está contenida en un bloque de construcción, y no en toda la red.

La interfaz de administración del switch recibe los paquetes de broadcast en la VLAN de administración. Si se producen difusiones excesivas (como una tormenta de difusión o una aplicación que no funciona correctamente), la CPU del switch puede sobrecargarse, lo que posiblemente podría distorsionar el funcionamiento del STP.

10. Una ubicación de raíz STP predecible (codificada) y raíz STP de respaldo

La raíz STP y la raíz STP de respaldo deben configurarse de modo que la convergencia, en caso de fallas, ocurra de manera predecible y genere una topología óptima en cada escenario. No deje la prioridad STP en el valor predeterminado, para evitar la selección impredecible del switch raíz.

Información Relacionada

- [Soporte de Producto de LAN](#)
- [Soporte de Tecnología de LAN Switching](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).