

# Identificar e Solucionar Problemas de STP em Switches Catalyst

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Conventions](#)

[Informações de Apoio](#)

[Causas de falhas de STP](#)

[Solucionar problemas de loops de encaminhamento](#)

[1. Identificar o Loop](#)

[2. Descobrir a Topologia \(Escopo\) do Loop](#)

[3. Quebre o Loop](#)

[4. Localizar e Corrigir a Causa do Loop](#)

[5. Restaurar a Redundância](#)

[Investigar Alterações de Topologia](#)

[Encontre a causa da inundação](#)

[Localize a origem dos TCs](#)

[Etapas para prevenir o excesso de TCs](#)

[Solucionar problemas relacionados ao tempo de convergência](#)

[Usar Comandos de Depuração do STP](#)

[Proteger a rede contra loops de encaminhamento](#)

[1. Habilitar Unidirectional Link Detection \(UDLD\) em todos os Links Switch a Switch](#)

[2. Ativar o protetor de loop em todos os Switches](#)

[3. Habilitar Portfast em todas as Portas de Estação Final](#)

[4. Defina EtherChannels como DesirableMode nos Dois Lados \(onde suportado\) e Non-SilentOption](#)

[5. Não Desative a Autonegociação \(se suportada\) em Links Switch a Switch](#)

[6. Tenha cuidado ao ajustar os temporizadores do STP](#)

[7. Se houver a possibilidade de ataques de negação de serviço, proteja o perímetro de STP da rede com protetor de raiz](#)

[8. Ative o BPDU Guard em portas com portfast habilitado para impedir que o STP afete dispositivos de rede não autorizados \(como hubs, switches e roteadores de bridging\) conectados às portas](#)

[9. Evite tráfego de usuário na VLAN de gerenciamento](#)

[10. Um Posicionamento Previsível \(codificado\) da Raiz STP e da Raiz STP de Backup](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve como usar o software Cisco IOS® para solucionar problemas com o Spanning Tree Protocol (STP).

# Pré-requisitos

## Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Vários tipos de Spanning Tree e como configurá-los. Consulte [Configuração do STP e do MST IEEE 802.1s](#) para obter mais informações.
- Vários recursos de Spanning Tree e como configurá-los. Consulte [Configurando recursos do STP](#) para obter mais informações.

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Catalyst 6500 com mecanismo Supervisor 2
- Cisco IOS Software Release 12.1(13)E

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Conventions

Consulte as Convenções de dicas técnicas da Cisco para obter mais informações sobre as convenções do documento.

## Informações de Apoio

Há comandos específicos que se aplicam apenas ao Catalyst 6500/6000; no entanto, você pode aplicar a maioria dos princípios a qualquer switch Cisco Catalyst que execute o software Cisco IOS.

Problemas com a maioria dos STPs têm estes três problemas:

- Loops de encaminhamento.
- Inundação excessiva devido a uma alta taxa de Alterações de Topologia (TC) de STP.
- Questões relacionadas com o tempo de convergência.

Porque uma bridge não tem nenhum mecanismo para rastrear se um determinado pacote é encaminhado várias vezes (por exemplo, um IP Time to Live [TTL]) ou é usado para descartar o tráfego que circula por muito tempo na rede. Apenas um caminho pode existir entre dois dispositivos no mesmo domínio de Camada 2 (L2).

A finalidade do STP é bloquear portas redundantes com base em um algoritmo STP e resolver a topologia física redundante em uma topologia em árvore. Um loop de encaminhamento (como um loop de STP) ocorre quando nenhuma porta em uma topologia redundante é bloqueada e o tráfego é encaminhado em círculos indefinidamente.

Quando o loop de encaminhamento começa, ele congela os links de menor largura de banda ao longo do caminho. Se todos os links tiverem a mesma largura de banda, todos os links estarão congestionados. Esse congestionamento causa perda de pacotes e leva a uma situação de inatividade da rede no domínio L2 afetado.

Com inundações excessivas, os sintomas não são tão aparentes. Links lentos podem se tornar congestionados pelo tráfego inundado, e os dispositivos ou usuários por trás desses links congestionados podem sofrer lentidão ou perda total de conectividade.

## Causas de falhas de STP

O STP faz algumas suposições sobre seu ambiente operacional. Estas são as suposições mais relevantes para este documento:

- Cada link entre as duas bridges é bidirecional. Isso significa que, se A se conecta diretamente a B, então A recebe o que B enviou e B recebe o que A enviou, desde que o link esteja ativo entre eles.
- Cada bridge que executa o STP é capaz de receber, processar e transmitir regularmente BPDUs (Bridge Protocol Data Units, unidades de dados de protocolo de ponte) do STP, também conhecidos como pacotes STP.

Embora essas suposições pareçam lógicas e óbvias, há situações em que elas não são atendidas. A maioria dessas situações envolve um tipo de problema de hardware; no entanto, defeitos de software também podem levar a falhas de STP. Várias falhas de hardware, configurações incorretas e problemas de conexão causam a maioria das falhas de STP, enquanto as falhas de software são responsáveis pela minoria. As falhas de STP também podem ocorrer devido a conexões adicionais desnecessárias que existem entre os switches. As VLANs entram em um estado inoperante devido a essas conexões adicionais. Para resolver esse problema, remova todas as conexões indesejadas entre os switches.

Quando uma dessas suposições não é atendida, uma ou mais bridges não podem receber ou processar as BPDUs. Isso significa que a bridge (ou bridges) não está descobrindo a topologia de rede. Sem o conhecimento da topologia correta, o switch não pode bloquear os loops. Portanto, o tráfego inundado circula pela topologia em loop, consome toda a largura de banda e derruba a rede.

Exemplos de por que os switches não podem receber BPDUs incluem transceptores defeituosos ou Conversores de Interface Gigabit (GBICs), problemas de cabo ou falhas de hardware na porta, na placa de linha ou no mecanismo Supervisor. Um motivo frequente para falhas de STP é um link unidirecional entre as bridges. Em tal condição, uma ponte envia BPDUs, mas a ponte downstream nunca os recebe. O processamento STP também pode ser interrompido por uma

CPU sobrecarregada (99 por cento ou mais) porque o switch não consegue processar BPDUs recebidos. As BPDUs podem ser corrompidas ao longo do caminho de uma ponte para a outra, o que também impede o comportamento adequado do STP.

Além dos loops de encaminhamento, quando nenhuma porta é bloqueada, há situações em que somente determinados pacotes são encaminhados incorretamente através das portas que bloqueiam o tráfego. Na maioria dos casos, isso é causado por problemas de software. Tal comportamento pode causar loops lentos. Isso significa que alguns pacotes estão em loop, mas a maior parte do tráfego ainda flui pela rede, porque os links não estão congestionados.

## Solucionar problemas de loops de encaminhamento

Os loops de encaminhamento variam muito em sua origem (causa) e efeito. Devido à grande variedade de problemas que podem afetar o STP, este documento só pode fornecer diretrizes gerais sobre como solucionar problemas de loops de encaminhamento.

Antes de começar a solucionar problemas, você precisa destas informações:

- Um diagrama de topologia real que detalha todos os switches e bridges.
- Seus números de porta correspondentes (interconectados).
- Detalhes de configuração do STP, como qual switch é a raiz e raiz de backup, quais links têm um custo ou prioridade não padrão e o local das portas que bloqueiam o tráfego.

### 1. Identificar o Loop

Quando um loop de encaminhamento é desenvolvido na rede, os sintomas comuns são:

- Perda de conectividade para, de e através das regiões afetadas.
- Utilização alta de CPU em roteadores conectados a segmentos afetados ou VLANs que podem levar a vários sintomas, como o Routing Protocol Neighbor Flapping ou o Hot Standby Router Protocol (HSRP) Active Router Flapping.
- Alta utilização do link (geralmente 100%).
- Alta utilização do painel traseiro do switch (em comparação com a utilização da linha de base).
- Mensagens de syslog que indicam looping de pacotes na rede (por exemplo, mensagens de endereço IP duplicadas do HSRP).
- Mensagens de syslog que indicam reaprendizado constante de endereço ou mensagens oscilantes de endereço MAC.
- O número de descartes de saída em muitas interfaces aumenta.

Qualquer um desses motivos pode indicar problemas diferentes (ou nenhum problema). No

entanto, quando muitos desses motivos são observados ao mesmo tempo, é muito provável que um loop de encaminhamento tenha se desenvolvido na rede. A maneira mais rápida de verificar isso é verificar a utilização do tráfego do painel traseiro do switch:

```
<#root>
```

```
cat#
```

```
show catalystr6000 traffic-meter
```

```
traffic meter = 13%
```

```
Never cleared
```

```
peak = 14%
```

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



Observação: o Catalyst 4000 com Cisco IOS Software atualmente não suporta esse comando.

---

Se o nível de tráfego atual for excessivo ou se o nível de linha de base não for conhecido, verifique se o nível de pico foi atingido recentemente e se está próximo do nível de tráfego atual. Por exemplo, se o nível de tráfego de pico for de 15% e tiver sido atingido há apenas dois minutos e o nível de tráfego atual for de 14%, isso significa que o switch tem uma carga excepcionalmente alta. Se a carga de tráfego estiver em um nível normal, isso provavelmente significa que não há loop ou que esse dispositivo não está envolvido no loop. No entanto, ele ainda pode estar envolvido em um loop lento.

## 2. Descobrir a Topologia (Escopo) do Loop

Uma vez estabelecido que o motivo da interrupção da rede é um loop de encaminhamento, a prioridade mais alta é parar o loop e restaurar a operação da rede.

Para interromper o loop, você deve saber quais portas participam do loop: observe as portas com a utilização de link mais alta (pacotes por segundo). O comando `show interface` Cisco IOS Software exibe a utilização para cada interface.

Para exibir apenas as informações de utilização e o nome da interface (para uma análise rápida), filtre a saída da expressão regular com o software Cisco IOS. Emita o comando `show interface | include line|Vseccommand` para exibir somente as estatísticas de pacote por segundo e o nome da interface:

```
<#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 atenção às interfaces com a utilização de link mais alta. Neste exemplo, essas são as interfaces g2/3, g2/4 e g2/8; elas são as portas que participam do loop.

### 3. Quebre o Loop

Para interromper o loop, você deve encerrar ou desconectar as portas envolvidas. É particularmente importante não apenas parar o loop, mas também encontrar e corrigir a causa raiz do loop. É relativamente mais fácil quebrar o ciclo

---

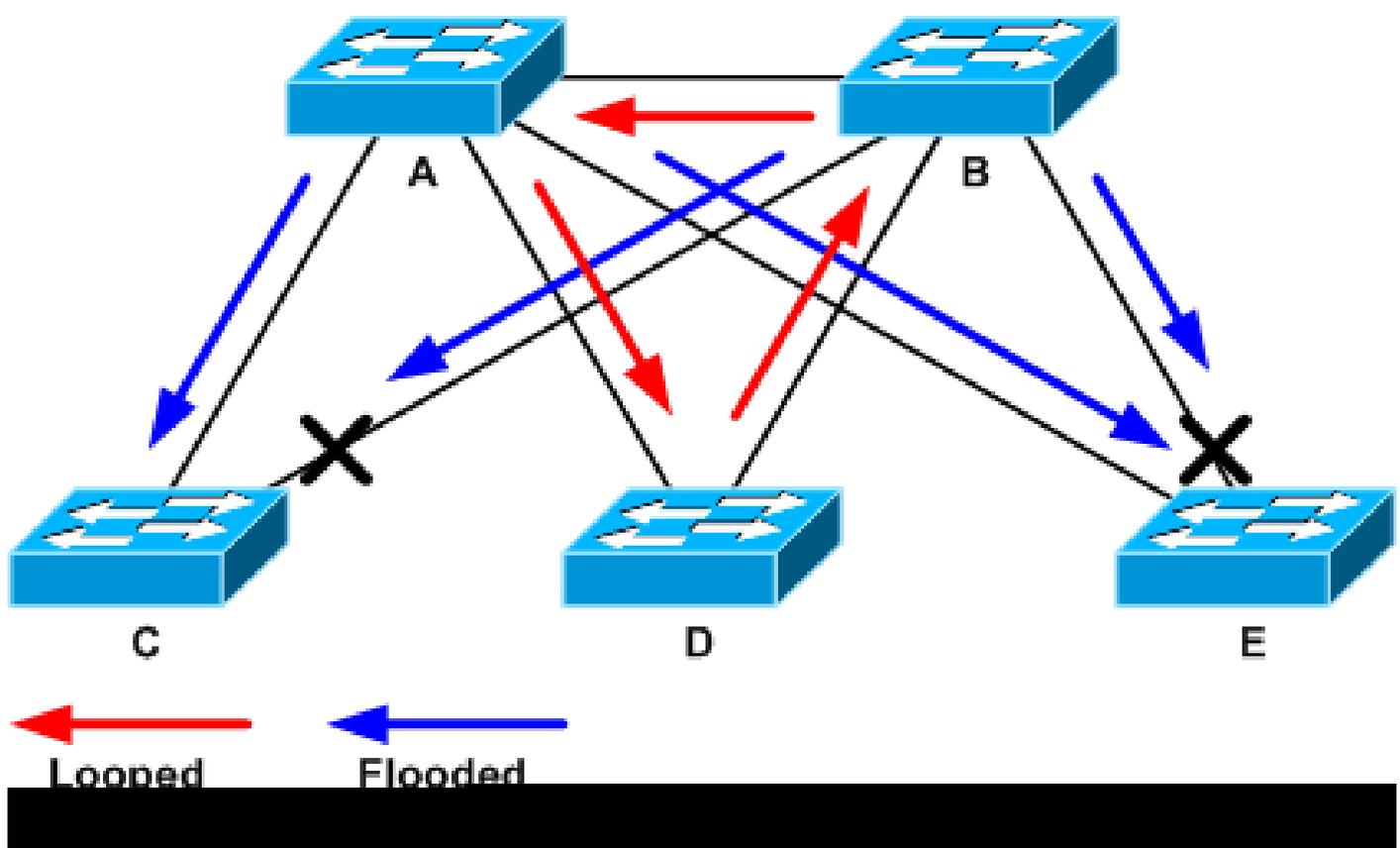
 **Observação:** você não precisa encerrar ou desconectar todas as portas ao mesmo tempo. Você pode desligá-las uma de cada vez. É melhor desativar as portas no ponto de agregação afetado pelo loop, como um switch de distribuição ou de núcleo. Se você encerrar todas as portas de uma vez e ativá-las ou reconectá-las uma a uma, isso não funcionará; o loop será interrompido e não poderá ser iniciado imediatamente após a porta defeituosa ser reconectada. Portanto, é difícil correlacionar a falha a qualquer porta específica.

---

✎ Observação: para interromper o loop, é recomendável coletar informações antes de reinicializar os switches. Caso contrário, a análise subsequente da causa raiz será difícil. Depois de desabilitar ou desconectar cada porta, você deve verificar se a utilização do painel traseiro do switch está de volta ao nível normal.

✎ Observação: lembre-se de que as portas não sustentam o loop, mas estão inundando o tráfego que chega com o loop. Ao desativar essas portas de inundação, você reduz apenas um pouco a utilização do painel traseiro, mas não interrompe o loop.

No próximo exemplo de topologia, o loop é entre os switches A, B e D. Portanto, os links AB, AD e BD são mantidos. Se você desligar qualquer um desses links, você interromperá o loop. Os links AC, AE, BC e BE estão apenas inundando o tráfego que chega com o loop.



Tráfego em loop e inundado

Depois que a porta de suporte é desligada, a utilização do painel traseiro cai para um valor normal. Você precisa saber qual porta de desligamento trouxe a utilização do painel traseiro (e a utilização de outras portas) para um nível normal. Nesse ponto, o loop é interrompido e a operação da rede melhora; no entanto, como a causa original do loop não foi corrigida, ainda há outros problemas.

#### 4. Localizar e Corrigir a Causa do Loop

Quando o loop for interrompido, você precisará determinar a razão do início do loop. Essa é a parte difícil do processo, pois os motivos podem variar. Também é difícil formalizar um

procedimento exato que funcione em todos os casos.

Diretrizes:

- Investigue o diagrama de topologia para encontrar um caminho redundante. Isso inclui a porta de suporte encontrada na etapa anterior que volta para o mesmo switch (os pacotes de caminho conversados durante o loop). Na topologia do exemplo anterior, esse caminho é AD-DB-BA.
- Para cada switch no caminho redundante, verifique se o switch conhece a raiz STP correta.

Todos os switches em uma rede L2 devem concordar em uma raiz STP comum. É um sintoma claro de problemas quando as bridges exibem consistentemente um ID diferente para a raiz do STP em uma determinada VLAN ou instância do STP. Emita o comando `show spanning-tree vlan vlan-id` para exibir o ID da bridge raiz de uma determinada 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
```

O número da VLAN pode ser encontrado na porta, pois as portas envolvidas no loop foram estabelecidas em etapas anteriores. Se as portas em questão forem troncos, todas as VLANs do tronco estarão frequentemente envolvidas. Se esse não for o caso (por exemplo, se parecer que o loop aconteceu em uma única VLAN), você poderá tentar emitir o comando `show interfaces | include L2|line|broadcasts` (somente no Supervisor 2 e em mecanismos posteriores nos Catalyst 6500/6000 Series Switches, porque o Supervisor 1 não fornece estatísticas de switching por VLAN). Observe apenas as interfaces VLAN. A VLAN com o maior número de pacotes comutados é frequentemente aquela em que o loop ocorreu:

```
<#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
```

Neste exemplo, a VLAN 1 é responsável pelo maior número de broadcasts e pelo tráfego comutado de L2. Verifique se a porta raiz está identificada corretamente.

A porta raiz deve ter o menor custo para a bridge raiz (às vezes, um caminho é menor em termos de saltos, mas maior em termos de custo, pois as portas de baixa velocidade têm custos mais altos). Para determinar qual porta é considerada a raiz de uma determinada VLAN, emita o 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

Certifique-se de que os BPDUs sejam recebidos regularmente na porta raiz e nas portas que supostamente devem ser bloqueadas.

Os BPDUs são enviados pela bridge raiz em cada intervalo de saudação (dois segundos por padrão). As bridges não raiz recebem, processam, modificam e propagam as BPDUs que são recebidas da raiz. Emita o comando `show spanning-tree interface interface detail` para ver se as BPDUs são recebidas:

```
<#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
```

 Observação: um BPDU foi recebido entre as duas saídas do comando (o contador foi de 53 para 54).

Os contadores mostrados, na verdade, são contadores mantidos pelo próprio processo STP. Isso significa que, se os contadores de recebimento fossem incrementados, não apenas o BPDU era recebido por uma porta física, mas também era recebido pelo processo STP. Se o contador de recebido BPDU não incrementar na porta que deve ser a raiz alternativa ou a porta de backup, verifique se a porta recebe multicasts (BPDUs são enviados como multicast). Emita o comando `show interface counters` comando:

```
<#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

Uma breve descrição das funções de porta do STP pode ser encontrada na seção [Melhorar o STP com Proteção de Loop e Detecção de Desvio de BPDU](#) de Aprimoramentos do Protocolo Spanning-Tree usando Recursos de Proteção de Loop e Detecção de Desvio de BPDU. Se nenhuma BPDU for recebida, verifique se a porta conta os erros. Emita o comando `show interface interface counters errors`:

```
<#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
```

É possível que os BPDUs sejam recebidos pela porta física, mas ainda não alcancem o processo STP. Se os comandos usados nos dois exemplos anteriores mostrarem que alguns multicasts são recebidos e que os erros não são contados, verifique se os BPDUs são descartados no nível do processo STP. Emita o comando `remote command switch test spanning-tree process-stats` no 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
```

O comando usado neste exemplo exibe as estatísticas do processo STP. É importante verificar se

os contadores de queda não aumentam e se os pacotes recebidos aumentam. Se os pacotes recebidos não forem aumentados, mas a porta física não receber multicasts, verifique se os pacotes são recebidos pela interface in-band do switch (a interface da CPU). Emita comando remoto switch show ibc | i rx\_input no 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 exemplo mostra que, entre as saídas, a porta in-band recebeu 23 pacotes.

---

 Observação: esses 23 pacotes não são apenas pacotes BPDU; esse é um contador global para todos os pacotes recebidos pela porta in-band.

---

Se não houver indicação de que os BPDUs são descartados no switch ou na porta local, você deve mover para o switch no outro lado do link e verificar se esse switch envia os BPDUs. Verifique se as BPDUs são enviadas regularmente em portas designadas não raiz. Se a função de porta concorrer, a porta enviará BPDUs, mas o vizinho não os receberá. Verifique se as BPDUs são enviadas. Emita o 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
```

```
BPDUs: 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
```

```
BPDUs: sent 1776
```

```
, received 1
```

Neste exemplo, dois BPDUs são enviados entre as saídas.

---

 Observação: o processo de STP mantém o contador de sentenças BPDUs: Isso significa que o contador indica que a BDU foi enviada para a porta física e é enviada. Verifique se os contadores de porta aumentam para pacotes multicast transmitidos. Emita o comando `show interface interface counters`. Isso pode ajudar a determinar o fluxo de tráfego de BPDUs.

---

```
<#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
--------------

OutBcastPkts		
Gi3/1	131826447	3442

872346

386

Com todas essas etapas, a ideia é encontrar o switch ou link onde as BPDUs não são recebidas, enviadas ou processadas. É possível que o STP tenha calculado o estado correto para a porta, mas devido a um problema no plano de controle, ele não pode definir esse estado no hardware de encaminhamento. Um loop pode ser criado se a porta não estiver bloqueada no nível do hardware. Se você acha que isso é um problema na sua rede, entre em [contato com o Suporte Técnico da Cisco](#) para obter assistência adicional.

## 5. Restaurar a Redundância

Quando o dispositivo ou link que causa o loop for encontrado, esse dispositivo deverá ser isolado da rede ou o problema deverá ser resolvido (como substituir a fibra ou o GBIC). Os links redundantes, desconectados na Etapa 3, devem ser restaurados.

É importante não manipular o dispositivo ou link que causa o loop, pois muitas condições que levam a um loop são transitórias, intermitentes e instáveis. Isso significa que, se a condição for eliminada durante ou após a investigação, a condição não ocorrerá por um tempo ou não ocorrerá. A condição deve ser registrada para que o [Suporte Técnico da Cisco](#) possa investigá-la melhor. É importante que você colete informações sobre a condição antes de redefinir os switches. Se uma condição desaparecer, é impossível determinar a causa raiz do loop. Se você coletar as informações, certifique-se de que esse problema não cause o loop novamente. Para obter mais informações, consulte [Protegendo a rede contra loops de encaminhamento](#).

## Investigar Alterações de Topologia

A função do mecanismo Topology Change (TC) é corrigir as tabelas de encaminhamento de L2 depois que a topologia é alterada. Isso é necessário para evitar uma interrupção de conectividade, pois os endereços MAC anteriormente acessíveis por meio de portas específicas podem mudar e se tornar acessíveis por meio de portas diferentes. O TC encurta o tempo de existência da tabela de encaminhamento em todos os switches na VLAN onde o TC ocorre.

Portanto, se o endereço não for reaprendido, ele envelhecerá e ocorrerá uma inundação para garantir que os pacotes cheguem ao endereço MAC destino.

O TC é acionado pela alteração do estado STP de uma porta para ou do estado de encaminhamento de STP. Após o TC, mesmo se o endereço MAC destino específico tiver expirado, a inundação não continuará por muito tempo. O endereço é reaprendido pelo primeiro pacote que vem do host cujo endereço MAC foi desatualizado. O problema pode surgir quando o TC ocorre repetidamente, com intervalos curtos. Os switches estão constantemente envelhecendo rapidamente suas tabelas de encaminhamento, portanto a inundação pode ser quase constante.

---

 Observação: com o Rapid STP ou o Multiple STP (IEEE 802.1w e IEEE 802.1s), o TC é disparado por uma alteração do estado da porta para encaminhamento, bem como a alteração de função de `designatedroot`. Com o Rapid STP, a tabela de encaminhamento L2 é imediatamente liberada, ao contrário do 802.1d, que diminui o tempo de envelhecimento. A liberação imediata da tabela de encaminhamento restaura a conectividade mais rapidamente, mas pode causar mais inundação

---

O TC é um evento raro em uma rede bem configurada. Quando um link em uma porta de switch é ativado ou desativado, ocorre eventualmente um TC, uma vez que o estado STP da porta é alterado para ou de encaminhamento. Quando uma porta não está sincronizada, o resultado pode ser inundação e TCs repetitivos.

As portas com o recurso `portfast` STP habilitado não podem causar TCs quando entram ou saem do estado `forwarding`. A configuração de `portfast` em todas as portas de dispositivos finais (como impressoras, PCs e servidores) pode limitar os TCs a uma quantidade baixa e é altamente recomendável.

Se houver TCs repetitivos na rede, você deverá identificar a origem desses TCs e tomar medidas para reduzi-los, para reduzir ao mínimo a inundação.

Com 802.1d, as informações de STP sobre um evento de TC são propagadas entre as ligações através de uma notificação de TC (TCN), que é um tipo especial de BPDU. Se você seguir as portas que recebem TCN BPDUs, poderá encontrar o dispositivo que originou os TCs.

## Encontre a causa da inundação

Você pode determinar que há inundação de desempenho lento, quedas de pacotes em links que não deveriam estar congestionados e o analisador de pacotes mostra vários pacotes unicast para o mesmo destino que não está no segmento local. Para obter mais informações sobre inundação de unicast, consulte [Inundação de unicast em redes de campus comutadas](#).

Em um Catalyst 6500/6000 que executa o software Cisco IOS, você pode verificar o contador do mecanismo de encaminhamento (somente no mecanismo Supervisor 2) para estimar a quantidade de inundação. Emita o comando remoto `switch show earl statistics | i MISS_DA|ST_FR`command:

```
<#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
```

Neste exemplo, a primeira coluna mostra a alteração desde a última vez que este comando foi executado e a segunda coluna mostra o valor cumulativo desde a última reinicialização. A primeira linha mostra a quantidade de quadros inundados e a segunda linha mostra a quantidade de quadros processados. Se os dois valores estiverem próximos, ou se o primeiro valor aumentar em uma taxa alta, pode ser que o switch esteja inundando o tráfego. No entanto, isso só pode ser usado em conjunto com outras maneiras de verificar a inundação, já que os contadores não são granulares. Há um contador por switch, não por porta ou VLAN. É normal ver alguns pacotes de inundação, pois o switch sempre pode inundar se o endereço MAC destino não estiver na tabela de encaminhamento. Esse pode ser o caso quando o switch recebe um pacote com um endereço de destino que ainda não foi aprendido.

## Localize a origem dos TCs

Se o número da VLAN for conhecido para a VLAN em que ocorre inundação excessiva, verifique os contadores STP para ver se o número de TCs é alto ou incrementa regularmente. Emita o comando `show spanning-tree vlan vlan-id detail` (neste exemplo, a VLAN 1 é usada):

```
<#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 o número da VLAN não for conhecido, use o analisador de pacotes ou verifique os contadores TC para todas as VLANs.

## Etapas para prevenir o excesso de TCs

Você pode monitorar o contador de alterações de topologia para ver se ele aumenta regularmente. Em seguida, vá até a ponte que está conectada à porta mostrada, para receber o último TC (no exemplo anterior, a porta GigabitEthernet1/1) e veja de onde veio o TC para essa ponte. Esse processo deve ser repetido até que a porta da estação final sem o portfast de STP habilitado seja encontrada ou até que o link não sincronizado seja encontrado e precise ser corrigido. Todo o procedimento precisa ser repetido se os TCs vêm de outras fontes. Se o link pertencer a um host final, você poderá configurar o recurso portfast para impedir a geração de TCs.

---

 Observação: na implementação STP do software Cisco IOS, o contador para TCs só pode ser incrementado se um TCN BPDU for recebido por uma porta em uma VLAN. Se um BPDU de configuração normal com um flag definido de TC for recebido, o contador de TC não será incrementado. Isso significa que, se você suspeitar que um TC seja o motivo da inundação, comece a rastrear as origens do TC a partir da bridge raiz do STP nessa VLAN. Ele pode ter as informações mais precisas sobre o número e a origem dos TCs.

---

## Solucionar problemas relacionados ao tempo de convergência

Existem situações em que a operação real do STP não coincide com o comportamento esperado. Estas são as duas questões mais frequentes:

- A convergência ou reconvergência do STP leva mais tempo do que o esperado.
- O resultado da topologia é diferente do esperado.

Na maioria das vezes, estas são as razões para este comportamento:

- Uma incompatibilidade entre as topologias real e documentada.
- Configuração incorreta, como uma configuração inconsistente de temporizadores STP, um diâmetro de STP que aumenta ou configuração incorreta de portfast.
- CPU do switch sobrecarregada durante a convergência ou reconvergência.
- Defeito de software.

Como mencionado anteriormente, este documento só pode fornecer diretrizes gerais para Troubleshooting, devido à grande variedade de problemas que podem afetar o STP. Para entender por que a convergência demora mais do que o esperado, observe a sequência de eventos de STP para descobrir o que acontece e em que ordem. Como a implementação do STP no software Cisco IOS não registra resultados (exceto para eventos específicos, como

inconsistências de porta), você pode usar o software Cisco IOS para depurar o STP para obter uma visão mais clara. Para o STP, com um Catalyst 6500/6000 que executa o software Cisco IOS, o processamento é feito no Switch Processor (SP) (ou Supervisor), portanto, as depurações precisam ser ativadas no SP. Para grupos de bridge do software Cisco IOS, o processamento é feito no RP (Route Processor), portanto, as depurações precisam ser ativadas no RP (MSFC).

## Usar Comandos de Depuração do STP

Muitos comandos STPdebugsão destinados ao uso da engenharia de desenvolvimento. Eles não fornecem nenhuma saída significativa para alguém sem conhecimento detalhado da implementação do STP no software Cisco IOS. Algumas depurações podem fornecer saída que é imediatamente legível, como alterações de estado de porta, alterações de função, eventos como TCs e um dump de BPDUs recebidos e transmitidos. Esta seção não fornece uma descrição completa de todas as depurações, mas apresenta brevemente as mais usadas.

---

 **Observação:** quando você usa debugcommands, habilite as depurações mínimas necessárias. Se as depurações em tempo real não forem necessárias, registre a saída no registro em vez de imprimi-la no console. Depurações excessivas podem sobrecarregar a CPU e interromper a operação do switch.

---

Para direcionar a saída de depuração para o registro em vez de para o console ou para sessões Telnet, emita os comandos logging console informationalandno logging monitor no modo de configuração global. Para ver o registro de eventos gerais, emita o comando debug spanning-tree eventpara Per VLAN Spanning-Tree (PVST) e Rapid-PVST. Esta é a primeira depuração que fornece informações sobre o que aconteceu com o STP. No modo MST (Multiple Spanning-Tree), não funciona executar o comando debug spanning-tree eventcommand. Portanto, emita o comando debug spanning-tree mstp rolespara ver as alterações de função de porta. Para ver as alterações de estado de STP da porta, emita o comando debug spanning-tree switch statejunto com o 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
```

Para entender por que o STP se comporta de uma determinada maneira, é geralmente útil ver as BPDUs que são recebidas e enviadas pelo switch:

```
<#root>
```

```
cat-sp#
```

```
debug spanning-tree bpdud receive
```

```
Spanning Tree BPDUD Received debugging is on
```

```
Nov 6 11:44:27: SP: STP: VLAN1 rx BPDUD: 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 00000000000000000074F1CE8470000001380480006525F0E4
080100100140002000F00
```

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

Essa depuração funciona para os modos PVST, Rapid-PVST e MST, mas não decodifica o conteúdo das BPDUs. No entanto, você pode usá-lo para garantir que as BPDUs sejam recebidas. Para ver o conteúdo da BPDUD, emita o comando `debug spanning-tree switch rx decode` para PVST e Rapid-PVST. Emita o comando `debug spanning-tree mstp bpdud-rx` para ver o conteúdo da BPDUD para o 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 bpdud 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 o modo MST, você pode habilitar a decodificação BPDU detalhada com este comando debug:

```
<#root>
```

```
cat-sp#
```

```
debug spanning-tree mstp bpdump
```

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

```

---

 Observação: para o Cisco IOS Software Release 12.1.13E e posterior, depurações condicionais para STP são suportadas. Isso significa que você pode depurar BPDUs que são recebidos ou transmitidos por porta ou por VLAN.

---

Emita os comandos `debug condition vlan vlan_num` ou `debug condition interface interface`, para limitar o escopo da saída de depuração para por interface ou por VLAN.

## Proteger a rede contra loops de encaminhamento

A Cisco desenvolveu vários recursos e aprimoramentos para proteger as redes contra loops de encaminhamento quando um STP não pode gerenciar determinadas falhas.

Ao solucionar problemas do STP, ele ajuda a isolar e possivelmente encontrar a causa de uma falha específica, enquanto a implementação desses aprimoramentos é a única maneira de proteger a rede contra loops de encaminhamento.

Estes são os métodos para proteger sua rede contra loops de encaminhamento:

### 1. Habilitar Unidirectional Link Detection (UDLD) em todos os Links Switch a Switch

Para obter mais informações sobre o UDLD, consulte [Entendendo e Configurando o Recurso de Protocolo de Detecção de Link Unidirecional](#).

### 2. Ativar o protetor de loop em todos os Switches

Para obter mais informações sobre Proteção de Loop, consulte [Aprimoramentos do Spanning-Tree Protocol usando Proteção de Loop e Recursos de Detecção de Desvio de BPDU](#).

Quando ativados, o UDLD e o protetor de loop eliminam a maioria das causas dos loops de encaminhamento. Em vez de criar um loop de encaminhamento, o link defeituoso (ou todos os links dependentes do hardware defeituoso) é desligado ou é bloqueado.

---

 Observação: embora esses dois recursos pareçam redundantes, cada um tem suas capacidades exclusivas. Portanto, use ambos os recursos ao mesmo tempo para fornecer o mais alto nível de proteção. Para obter uma comparação detalhada do UDLD e do protetor de loop, consulte [Proteção de loop vs. Detecção de enlace unidirecional](#).

---

Há opiniões diferentes em relação ao uso de UDLD agressivo ou normal. O UDLD assertivo não pode fornecer mais proteção contra loops em comparação ao UDLD de modo normal. O UDLD agressivo detecta cenários de travamento de porta (quando o link está ativo, mas não há buracos negros de tráfego associados). A desvantagem dessa funcionalidade adicional é que a UDLD agressiva pode potencialmente desativar enlaces quando nenhuma falha consistente estiver presente. Frequentemente, as pessoas confundem a modificação do `UDLDhellointerval` com o recurso UDLD agressivo. Isso está incorreto. Os cronômetros podem ser modificados nos dois modos UDLD.

---

 Observação: em raros casos, o UDLD agressivo pode desativar todas as portas de uplink, o que basicamente isola o switch do resto da rede. Por exemplo, isso pode acontecer quando ambos os switches upstream experimentam uma utilização de CPU extremamente alta e o modo assertivo UDLD é usado. Portanto, é recomendável que você configure tempos limite que não possam ser erodidos, se o switch não tiver um gerenciamento fora de banda em vigor.

---

### 3. Habilitar Portfast em todas as Portas de Estação Final

Você deve habilitar o portfast para limitar a quantidade de TCs e inundações subsequentes, que podem afetar o desempenho da rede. Use esse comando apenas com portas que se conectam a estações finais. Caso contrário, um loop acidental de topologia pode causar um loop de pacote de dados e interromper o switch e a operação da rede.

---

 Cuidado: Tenha cuidado ao usar o comando no spanning-tree portfast. Esse comando remove apenas os comandos portfast específicos da porta. Esse comando habilita implicitamente o portfast se você definir o comando spanning-tree portfast default no modo de configuração global e se a porta não for uma porta de tronco. Se você não configurar o portfast globalmente, o comando no spanning-tree portfast será equivalente ao comando spanning-tree portfast disable.

---

### 4. Defina EtherChannels no modo `desirable` em ambos os lados (onde suportado) e na opção `Non-silent`

Desirablemode pode habilitar o Port Aggregation Protocol (PAgP) para garantir a consistência do tempo de execução entre os peers de canalização. Isso fornece um grau adicional de proteção contra loops, especialmente durante reconfigurações de canal (como quando os links entram ou saem do canal e detecção de falha de link). Há um protetor interno de configuração incorreta do canal, que é ativado por padrão e que evita loops de encaminhamento devido à configuração incorreta do canal ou a outras condições. Para obter mais informações sobre esse recurso, consulte [Entendendo a detecção de inconsistência do EtherChannel](#).

### 5. Não Desative a Autonegociação (se suportada) em Links Switch a Switch

Os mecanismos de autonegociação podem transmitir informações de falha remota, que é a maneira mais rápida de detectar falha no lado remoto. Se for detectada uma falha no lado remoto, o lado local desativará o link mesmo que ele receba pulsos. Comparada aos mecanismos de detecção de alto nível, como o UDLD, a autonegociação é extremamente rápida (em microssegundos), mas não tem a cobertura de ponta a ponta do UDLD (como todo o caminho de dados: CPU—lógica de encaminhamento—porta1—porta2—lógica de encaminhamento—CPU versus porta1—porta2). O modo UDLD agressivo fornece funcionalidade semelhante à da autonegociação com relação à detecção de falha. Quando a negociação é suportada nos dois lados do enlace, não há necessidade de habilitar o UDLD do modo agressivo.

## 6. Tenha cuidado ao ajustar os temporizadores do STP

Os temporizadores STP dependem um do outro e da topologia de rede. O STP não funciona corretamente com modificações arbitrárias feitas nos temporizadores. Para obter mais informações sobre temporizadores STP, consulte [Entendendo e Ajustando Temporizadores do Spanning Tree Protocol](#).

7. Se houver a possibilidade de ataques de negação de serviço, proteja o perímetro de STP da rede com protetor de raiz

O Protetor de Raiz e o Protetor de BPDU permitem que você proteja o STP contra influências externas. Se tal ataque for possível, o protetor de raiz e o protetor de BPDU devem ser usados para proteger a rede. Para obter mais informações sobre Protetor de Raiz e Protetor de BPDU, consulte estes documentos:

- [Melhoria de protetor de raiz do protocolo de árvore de abrangência](#)
- [Aprimoramento do Protetor de BPDU do PortFast de Spanning Tree](#)

8. Ative o BPDU Guard em portas com portfast habilitado para impedir que o STP afete dispositivos de rede não autorizados (como hubs, switches e roteadores de bridging) conectados às portas

Se você configurar o Protetor de Raiz corretamente, ele evitará que o STP tenha influência externa. Se o BPDU Guard estiver habilitado, ele desligará as portas que recebem BPDUs. Isso é útil para investigar incidentes, pois o BPDU Guard produz a mensagem de syslog e desliga a porta. Se os protetores de raiz ou BPDU não impedirem loops de ciclo curto, duas portas ativadas rapidamente se conectarão diretamente ou através do hub.

9. Evite tráfego de usuário na VLAN de gerenciamento

O gerenciamento da VLAN está incluído em um bloco de construção, e não na rede inteira.

A interface de gerenciamento do switch recebe pacotes de broadcast na VLAN de gerenciamento. Se ocorrerem broadcasts excessivos (como uma tempestade de broadcasts ou um aplicativo defeituoso), a CPU do switch poderá ficar sobrecarregada, o que poderia distorcer a operação do STP.

10. Um Posicionamento Previsível (codificado) da Raiz STP e da Raiz STP de Backup

A raiz STP e a raiz STP de backup devem ser configuradas de modo que a convergência, no caso de falhas, ocorra de forma previsível e crie a topologia ideal em cada cenário. Não deixe a prioridade de STP com o valor padrão, para evitar uma seleção imprevisível do switch-raiz.

## Informações Relacionadas

- [Suporte a Produtos de LAN](#)
- [Suporte de tecnologia de switching de LAN](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.