Pesquisando defeitos o STP nos Catalyst Switches que executam o software do sistema do Cisco IOS

Índice

Introdução

Este documento fornece as diretrizes para usar o software Cisco IOS® para resolver problemas com o Spanning-Tree Protocol (STP). Há comandos específicos que se aplicam somente ao Catalyst 6500/6000; contudo, é possível aplicar a maioria dos princípios a qualquer switch Cisco Catalyst que executa o software Cisco IOS.

A maioria de Troubleshooting de STP revolve ao redor três edições:

- loops de encaminhamento
- inundação excessiva causada por alta taxa de Alterações na Topologia STP (TC)
- edições relativas ao tempo de convergência

Porque construir uma ponte sobre não tem nenhum mecanismo a seguir se um determinado pacote está sendo enviado épocas múltiplas (por exemplo, um [TTL] do Time to Live IP está usada para rejeitar o tráfego que está circulando demasiado por muito tempo na rede), simplesmente um trajeto pode existir entre dois dispositivos no mesmo domínio da camada 2 (L2).

A finalidade do STP é obstruir as portas redundantes baseadas em um algoritmo STP, para resolver a topologia física redundante em uma topologia da árvore (como). 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.

Uma vez que o loop de encaminhamento começa, congestionará provavelmente os links da

baixo-largura de banda ao longo de seu trajeto — se todos os links são da mesma largura de banda, todos os links estarão congestionados provavelmente. Esta congestão causará a perda de pacotes e conduzi-la-á a uma situação da rede para baixo no domínio L2 afetado.

Com inundação excessiva, os sintomas não puderam ser como aparentes. Alguns enlaces lentos puderam tornar-se congestionados pelo tráfego inundado, e os dispositivos ou os usuários atrás destes links congestionados puderam experimentar a lentidão ou a perda total de Conectividade.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Vária medida - tipos da árvore e como configurar-los. Consulte Configuração de STP e MST IEEE 802.1s para obter mais informações.
- Vários recursos de Spanning Tree e como configurar-los. Refira configurar características STP para mais informação.

Componentes Utilizados

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

- Catalyst 6500 com o motor do 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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Por que o STP falha?

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

- Cada link entre as duas pontes é bidirecional. Isto significa que, se A conecta diretamente a B, a seguir A receberá o que B enviou e B receberá o que A enviou, enquanto o link está acima entre ele.
- Cada ponte que está executando o STP pode receber, processar, e transmitir regularmente o bridge protocol data units STP (BPDU), igualmente conhecido como pacotes de STP.

Quando estas suposições parecerem lógicas e óbvias, há umas situações quando não são encontradas. A maioria destas situações envolvem algum meio problema de hardware; contudo, os defeitos do software podem igualmente conduzir às falhas de STP. Vária falhas do hardware,

configurações incorretas, ou causa do cabeamento inadequado a maioria de falhas de STP, quando as falhas de software esclarecerem a minoria. As falhas de STP podem igualmente ocorrer devido às conexões adicionais desnecessárias que existem entre o Switches. Os VLAN entram em um estado inativo devido a estas conexões adicionais. Para resolver este problema, remova todas as conexões indesejadas entre o Switches.

Quando uma destas suposições não é encontrado, umas ou várias pontes puderam já não receber ou processar os BPDU. Isto significa que a ponte (ou as pontes) não poderão descobrir a topologia de rede. Sem conhecimento da topologia correta, o interruptor não pode obstruir os laços. Consequentemente, o tráfego inundado circulará sobre a topologia dada laços, consumirá toda a largura de banda, e derrubará a rede.

Os exemplos de porque o Switches não pode receber BPDU incluem transceptores ou os conversores de interface Gigabit (GBIC), questões de cabeamento, ou falhas do hardware ruins na porta, na placa de linha, ou no Supervisor Engine. Uma razão frequente para falhas de STP é um enlace unidirecional entre as pontes. Em tal circunstância, uma ponte envia BPDU, mas a ponte a jusante nunca recebe-os. O processamento STP pode igualmente ser interrompido por um CPU sobrecarregado (99 por cento ou mais), porque o interruptor é incapaz de processar BPDU recebidos. Os BPDU podem ser corrompidos ao longo do trajeto de uma ponte à outro, que igualmente impede o comportamento apropriado de STP.

Além dos loops de encaminhamento, em que as portas não são bloqueadas, em certas situações, apenas alguns pacotes são encaminhados incorretamente pelas portas de bloqueio. Na maioria dos casos, isto é causado por questões de software. Tal comportamento pode causar "circuitos lentos". Isto significa que alguns pacotes estão dados laços, mas a maioria do tráfego ainda está correndo através da rede, porque os links não são congestionados provavelmente.

As seções remanescente neste documento fornecem diretrizes para pesquisar defeitos as edições STP-relacionadas as mais comuns.

Troubleshooting de Circuitos de Encaminhamento

Os loop de encaminhamento variam extremamente ambos em sua origem (causa) e efetuam-nos. Devido à ampla variedade de edições que podem afetar o STP, este documento pode somente fornecer diretrizes gerais sobre como pesquisar defeitos loop de encaminhamento.

Antes que você comece pesquisar defeitos, você deve obter esta informação:

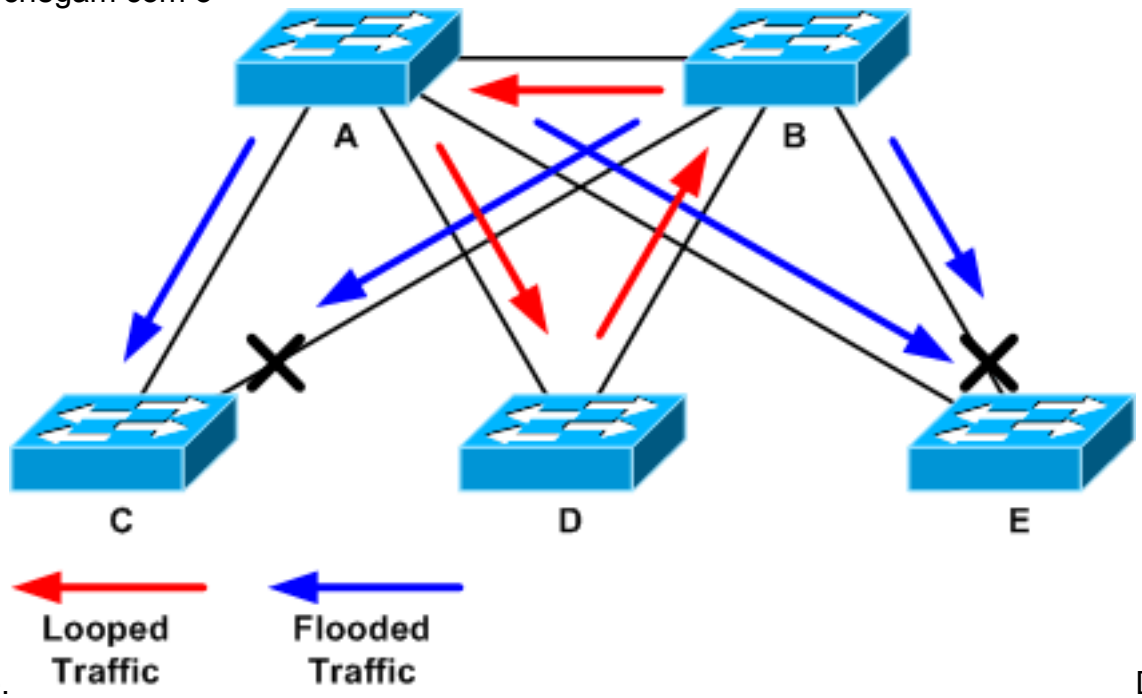
- Um diagrama da topologia real que detalhe todo o Switches e pontes
- Seus números de porta (de interconexão) correspondentes
- Detalhes da configuração STP, tais como que o interruptor é a raiz e a raiz do backup, que os links têm um custo ou uma prioridade não-padrão, e o lugar das portas de bloqueio

Geralmente, pesquisar defeitos envolve estas etapas (segundo a situação, algumas etapas não podem ser necessárias):

1. Identifique o laço.Quando um loop de encaminhamento se tornou na rede, estes são os sintomas comuns:Perda de conectividade, e através das regiões de rede afetadasA utilização elevada da CPU no Roteadores conectou aos segmentos afetados ou aos VLAN que podem conduzir aos vários sintomas, tais como o flapping do flapping do vizinho de protocolo de roteamento ou do roteador ativo do Hot Standby Router Protocol (HSRP)Grande utilização de link (com freqüência, 100%)Alta utilização da placa-mãe de

switch (comparada à utilização de linha de base)Mensagens do syslog que indicam o pacote que dá laços na rede (por exemplo as mensagens de Endereço IP Duplicado HSRP)Mensagens do syslog que indicam relearning do endereço ou mensagens não sincronizada constantes do MAC addressUm número de aumento de quedas de emissor em muitas relações**Nota:** Qualqueras um razões apenas podem não indicar edições diferentes (ou nenhuma edição de todo). No entanto, quando muitos desses motivos são observados ao mesmo tempo, é muito provável que um loop de encaminhamento tenha se desenvolvido na rede.**Nota:** A maneira a mais rápida de verificar isto é verificar a utilização do tráfego do backplane do interruptor:`cat# **show catalyst6000 traffic-meter traffic meter = 13%** Never cleared **peak = 14%** reached at 12:08:57 CET Fri Oct 4 2002` **Nota:** O catalizador 4000 com Cisco IOS Software não apoia atualmente este comando.Se o nível de tráfego atual está bem acima do normal ou se o nível de linha de base não está sabido, verifique se o nível máximo esteja conseguido recentemente e se é próximo ao nível de tráfego atual. Por exemplo, se o nível do tráfego de pico é 15 por cento e esteve alcançado apenas dois minutos há e o nível de tráfego atual é 14 por cento, a seguir que significaria que o interruptor está funcionando sob raramente uma carga elevada.Se a carga de tráfego está a nível normal, a seguir esse significa provavelmente que não há ou nenhum laço ou que este dispositivo não está envolvido no laço. Contudo, ainda poderia ser envolvido em um laço lento.
2. Descubra a topologia (espaço) do laço.Uma vez que se estabeleceu que a razão para a parada de rede é um loop de encaminhamento, a prioridade mais alta é parar o laço e restaurar a operação de rede. A fim parar o laço, você deve saber que portas são envolvidas no laço: olhe as portas com a utilização do enlace a mais alta (pacotes por segundo). O comando do Cisco IOS Software da **relação da mostra** indica a utilização para cada relação.A fim indicar somente a informação de utilização e o nome da relação (para uma rápida análise), você pôde usar o filtragem de saída da expressão regular do Cisco IOS Software. Emita a **relação da mostra | incluir linha|\ /sec** comando indicar por segundo somente as estatísticas do pacote e o nome da relação:`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**` Pague a atenção particular às relações com a utilização do enlace a mais alta. Neste exemplo, estas são as relações g2/3, g2/4, e g2/8; são provavelmente as portas que são envolvidas no laço.
3. Quebre o laço.Para quebrar o laço, você deve fechar ou desligar as portas involvidas. É muito importante para não somente a parada o laço mas para encontrar e fixar igualmente a causa de raiz do laço. É relativamente mais fácil quebrar o laço.**Nota:** A fim ajudar a análise de causa subsequente, você não precisa fechado nem desliga todas as portas imediatamente; em lugar de, feche-os para baixo um de cada vez. É geralmente melhor fechar portas no ponto de agregação afetado pelo laço, tal como uma distribuição ou um switch central. Se você fecha todas as portas imediatamente e as permite ou reconecta um a

um, não pôde trabalhar; o laço estará parado e não pôde começar imediatamente depois que a porta de ofensa é reconectada. Consequentemente, seria difícil correlacionar a falha a toda a porta particular.**Nota:** Recomenda-se que você recolhe a informação antes que você recarregue o Switches para quebrar o laço. Se não, a análise da causa raiz subsequente será muito difícil.Depois que você desabilita ou desliga cada porta, você deve verificar se a utilização de backplane do interruptor seja de volta a um nível normal.**Nota:** Mantenha na mente que, geralmente, algumas portas não estão sustentando o laço mas, um pouco, estão inundando o tráfego que chega com o laço. Quando você fecha tais portas de inundação, você reduzirá somente a utilização de backplane um a quantidade pequena, mas você não parará o laço.Na topologia do exemplo seguinte, o laço está entre comuta A, B, e D. Consequentemente, os links AB, AD, e BD estão sustentando. Se você fecha qualquens um links, você parará o laço. Os enlaces AC, AE, BC e BE são apenas tráfego de inundação que chegam com o



loop. Depois que a porta de sustentação é fechada, a utilização de backplane irá para baixo a um valor normal. É muito importante notar a parada programada de que porta trouxe à utilização de backplane (e à utilização de outras portas) a um nível normal.Neste momento, o laço será parado e a operação de rede deve melhorar; contudo, porque a causa original do laço não era provavelmente fixa, pôde ainda haver algumas edições proeminentes.

4. Encontre e fixe a causa do laço.Uma vez que o laço foi parado, você precisa de determinar a razão pela qual o laço começou. Esta é frequentemente a maioria de parte difícil do processo, porque as razões podem variar. É igualmente difícil formalizar um procedimento exato que trabalhe em todos os casos. Contudo, estas são algumas diretrizes gerais:Investigue o diagrama de topologia, para encontrar um caminho redundante. Isto inclui a porta de sustentação encontrada na etapa precedente que vem para trás ao mesmo interruptor (os pacotes de caminho estavam tomando durante o laço). Na topologia do exemplo anterior, este trajeto é AD-DB-BA.Para cada interruptor no caminho redundante, verifique para ver se há estas edições:O interruptor conhece a raiz correta STP?Todo o Switches em uma rede L2 deve concordar com uma raiz comum STP. É um sintoma claro dos problemas quando as pontes indicam consistentemente um ID diferente para a raiz STP em um VLAN particular ou no exemplo STP. Emita o **comando show spanning-tree vlan vlan-id** indicar o ID de bridge raiz para um VLAN dado:`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 de VLAN pode ser encontrado da porta, porque as portas envolvidas no laço foram estabelecidas em etapas precedentes. Se as portas em questão forem troncos, todas as VLANs do tronco estarão freqüentemente envolvidas. Se tal não for o caso (por exemplo, se parece que o laço aconteceu em um único VLAN) então você pode tentar emitir as **relações da mostra | inclua o** comando **L2|line|broadcast** (somente no supervisor 2 e nos motores mais atrasados no Catalyst 6500/6000 series switch, porque o Supervisor 1 não fornece a estatística de switching do VLAN per.). Olhe interfaces de VLAN somente. O VLAN com a quantidade a mais alta de pacotes comutados será o mais frequentemente esse onde o laço ocorreu:cat# **show int | 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, o VLAN1 esclarece o número o mais alto de transmissões e de tráfego L2-switched.A porta de raiz foi identificada corretamente?A porta de raiz deverá ter o custo mais baixo do bridge raiz (algumas vezes um caminho é menor em termos de saltos, porém maior em termos de custo, porque as portas de baixa velocidade têm custos mais elevados).Para determinar que porta é considerada a raiz para um VLAN dado, emita o **comando show spanning-tree vlan vlan**: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 P2pOs BPDU recebidos regularmente na porta de raiz e nas portas que são supostas para ser estão obstruindo?Os BPDU são enviados pelo bridge-raiz em cada intervalo de hello (dois segundos à revelia). Os bridges sem raiz recebem, processam, alteram, e propagam os BPDU que são recebidos da raiz.Emita o **comando show spanning-tree interface interface detail** ver se os BPDU estão sendo recebidos: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:** Um BPDU foi recebido entre as duas saídas do comando (o contador foi 53 a 54).Os contadores mostrados, na verdade, são contadores mantidos pelo próprio processo STP. Isto significa que, se os contadores da recepção incrementados, eram não

somente BPDU recebido por uma porta física mas foi recebida igualmente pelo processo STP.Se o contador `recebido` BPDU não está incrementando na porta que é suposta para ser a substituição ou o porto de backup da raiz, a seguir a verificação se a porta está recebendo quaisquer Multicast de todo (BPDU é enviada como o Multicast). Emita o **comando show interface interface counters**:`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` (A breve descrição A para funções da porta STP pode ser encontrada no sumário breve de funções da porta da seção STP da medida - realces do protocolo de árvore usando o protetor de loop e os recursos de detecção de desvio BPDU.)Se nenhum BPDU é recebido, verifique se a porta não esteja contando erros. Emita o **comando show interface interface counters errors**:`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` Épossível que os BPDUs sejam recebidos pela porta física, mas ainda não alcancem o processo STP. Se os comandos usados nos dois exemplos precedentes mostram que alguns Multicast estão recebidos, e os erros não estão incrementando, a seguir verifique se os BPDU estejam sendo deixados cair a nível do processo STP. Emita o **comando remote command switch test spanning-tree process-stats no** Catalyst 6500:`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 indica estatísticas do processo STP. É importante verificar que os contadores de queda não estão aumentando e que os pacotes recebidos estão aumentando.Se os pacotes recebidos não estão aumentando mas a porta física está recebendo Multicast, verifique que os pacotes estão sendo recebidos pela relação da em-faixa do interruptor (a relação do CPU). Emita o **ibc da mostra do remote command switch | mim** comando do **rx_input no** Catalyst 6500/6000:`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 da em-faixa recebeu 23 pacotes.**Nota:** Estes 23 pacotes são não somente pacotes de BPDU; este é um contador global para todos os pacotes recebidos pela porta da em-faixa.Se não há nenhuma indicação que os BPDU estão sendo deixados cair no switch local ou movem, você deve transportar-se ao interruptor no outro lado do link e verificar se esse interruptor está enviando BPDU.BPDUs são enviadas regularmente em portas não raiz designadas?Se, de acordo com a função da porta, a porta está enviando BPDU — mas o vizinho não os está recebendo — verifica se os BPDU estejam sendo enviados realmente. Emita o **comando show spanning-tree interface interface detail**:`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
```

Neste exemplo, dois BPDU foram mandados entre as saídas.**Nota:** O processo STP mantém o `BPDU: enviado` contra. Isto significa que o contador indica que o BPDU esteve enviado para a porta física, para ser mandado eventualmente. Verifique se os contadores de porta estejam aumentando para pacotes de transmissão múltipla transmitidos. Emita o **comando show interface interface counters**. Isso pode ajudar a determinar se os BPDUs estão saindo ou não:

```
cat# show interface g3/1 counters Port InOctets InUcastPkts InMcastPkts InBcastPkts Gi3/1
127985312 83776 812319 19 Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts Gi3/1
131825915 3442 872342 386 cat# show interface g3/1 counters Port InOctets InUcastPkts
InMcastPkts InBcastPkts Gi3/1 127985312 83776 812319 19 Port OutOctets OutUcastPkts
OutMcastPkts OutBcastPkts Gi3/1 131826447 3442 872346 386
```

Com as todas estas etapas, a ideia é encontrar o interruptor ou ligar onde os BPDU não são recebidos, são enviados, ou processados.Épossível, de qualquer modo improvável, que o STP calculou o estado correto para a porta, mas devido a uma edição do plano do controle, era incapaz de ajustar este estado no hardware de encaminhamento. Um laço pode ser criado, se a porta de bloqueio suposta não é obstruída a nível de hardware. Se você suspeita tal edição em sua rede, contacte o Suporte técnico de Cisco para a assistência adicional.

5. Restaure a Redundância.Uma vez que o dispositivo ou liga que está causando o laço foi encontrado, este dispositivo deve ser isolado da rede, ou as ações devem ser tomadas para resolver a edição (como substitua a fibra ou o GBIC). Os enlaces redundantes, desligados em etapa 3, devem ser restaurados.Éimportante fazer como pouca manipulação como possível ao dispositivo ou ligar que está causando o laço, porque muitas circunstâncias que conduzem a um laço podem ser muito transientes, intermitentes, e instáveis. Isto significa que, se a circunstância é cancelada durante ou depois do Troubleshooting, pode tomar um quando antes que tal circunstância ocorra outra vez. É possível que a condição nunca mais ocorra. O todo esforço deve ser feito para preservar a circunstância, de modo que possa mais ser investigado pelo Suporte técnico de Cisco. É importante que você recolhe a informação sobre a circunstância antes que você restaure o Switches. Se uma circunstância é ida, é frequentemente impossível determinar a causa de raiz do laço. Para encontrar o dispositivo ou ligá-lo que provoca o laço são uma realização principal, mas você precisam de assegurar-se de que uma outra falha do mesmo tipo não cause o laço outra vez. Para mais informação, refira a fixação da rede contra a seção dos loop de encaminhamento deste documento.

Troubleshooting de Alterações Excessivas de Topologia Causando Inundações

A função do mecanismo TC é corrigir as tabelas de encaminhamento L2 após a alteração da topologia de encaminhamento. Isto é necessário para evitar uma interrupção de conectividade porque, após um TC, algumas portas particular diretas previamente acessíveis dos endereços MAC puderam se tornar acessíveis através das portas diferentes. O TC encurta o tempo de envelhecimento da tabela do forwarding em todo o Switches no VLAN onde o TC ocorre; assim, se o endereço não relearned, idade-para fora e a inundação ocorrerá para assegurar a alcance dos pacotes o endereço MAC de destino.

O TC é provocado pela mudança do estado STP de uma porta a ou do estado do

encaminhamento STP. Depois que o TC, mesmo se o MAC address do destino particular tem antigo, inundando não deve continuar para por muito tempo. O endereço relearned pelo primeiro pacote que vem do host cujo o MAC address foi antigo. A edição pôde elevarar quando os TC estão ocorrendo repetidamente, com intervalos curtos. O Switches será constantemente fast aging suas tabelas do forwarding, assim que a inundação será quase constante.

Nota: Com STP rápido ou o STP múltiplo (IEEE 802.1W e IEEE 802.1S), o TC é provocado por uma mudança do estado de porta à `transmissão`, assim como pela mudança do papel do `designado para enraizar`. Com STP rápido, a tabela do forwarding L2 é nivelada imediatamente, ao contrário de 802.1d, que encurta o tempo de envelhecimento. A descarga imediata da tabela de encaminhamento restaura a conectividade mais rapidamente, mas provoca mais inundação.

O TC deve ser um evento raro em uma rede bem configurada. Quando um link em uma porta de switch vai para cima ou para baixo, há eventualmente um TC, uma vez o estado STP da porta está mudando a ou da `transmissão`. Quando uma porta não está sincronizada, o resultado pode ser inundação e TCs repetitivos.

As portas com a característica do STP portfast permitida não causarão TC ao ir a ou do `estado de encaminhamento`. A configuração de portfast em todas as portas de dispositivos finais (como impressoras, computadores e servidores) deve limitar os TCs para um valor inferior e isso é altamente recomendado. Para obter mais informações sobre dos TC, refira compreendendo alterações de topologia do Spanning Tree Protocol.

Se há TC repetitivos na rede, você deve identificar a fonte destes TC e tomar a ação para reduzi-los, para trazer a inundação a um mínimo.

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 segue as portas que estão recebendo TCN BPDU, você pode encontrar o dispositivo que está originando TC.

Estabelecer se a Inundação é Causada pelos TCs do STP.

Normalmente, você pode determinar que está inundando do desempenho lento, quedas de pacote de informação nos links que não são supostos ser congestionados, e o analisador de pacote que mostra pacotes do unicast múltiplos ao mesmo destino que não está no segmento local.

Para obter mais informações sobre da inundação unicast, refira a inundação unicast nas redes de campus comutadas.

Em um Catalyst 6500/6000 que executa o Cisco IOS Software, você pode verificar o Forwarding Engine contrário (somente no motor do supervisor 2) para calcular a quantidade de inundação. Emita as **estatísticas do conde da mostra do remote command switch | mim MISS_DA|**Comando **ST_FR**:

```
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 mudança desde que a última vez onde este comando foi executado, e a segunda coluna mostra o valor cumulativo desde a última repartição. A primeira linha mostra a quantidade de quadros inundados, e a segunda linha mostra a quantidade de quadros processados. Se os dois valores são próximos junto, ou o primeiro valor está

aumentando em uma taxa alta, pôde-se ser que o interruptor está inundando o tráfego. Contudo, isto pode somente ser usado conjuntamente com outras maneiras de verificar a inundação, porque os contadores não são granulados. Há um contador pelo interruptor, não pela porta ou o VLAN. É normal ver alguns pacotes da inundação, porque o interruptor inundará sempre se o endereço MAC de destino não está na tabela do forwarding. Este será o caso quando o interruptor recebe um pacote com um endereço de destino que não esteja aprendido ainda.

Siga para baixo a fonte dos TC

Se o número de VLAN é sabido para o VLAN onde a inundação excessiva está ocorrendo, verifique os contadores STP para ver se o número de TC é alto ou incrementando regularmente. Emita o **comando show spanning-tree vlan vlan-id detail** (neste exemplo, o VLAN1 é usado):

```
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 `número de alterações de topologia` ao contrário de vê se está aumentando regularmente. Então, movimento à ponte que é conectada à porta que é mostrada, receber o último TC (no exemplo anterior, na porta GigabitEthernet1/1) e vê-lo de onde o TC veio para essa ponte. Este processo deve ser repetido até que a porta de estação final sem STP portfast permitido esteja encontrada, ou até o link não sincronizado estiver encontrado que precisa de ser fixado. O procedimento inteiro precisará ser repetido se os TCs ainda estiverem vindo de outras origens. Se o link pertence a um host final, você deve configurar os recursos de portfast para impedir a geração de TC.

Nota: Na implementação de STP do Cisco IOS Software, o contador para TC incrementará somente se um TCN BPDU é recebido por uma porta em um VLAN. Se uma configuração normal BPDU com uma bandeira do grupo TC é recebida então o contador TC não está incrementado. Isto significa que, se você suspeita um TC para ser a razão para inundar, é o melhor começar seguir para baixo as fontes para o TC do bridge-raiz STP nesse VLAN. Terá a maioria de informação precisa em relação à quantidade e à fonte dos TC.

Troubleshooting de 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 edições as mais frequentes:

- A convergência de STP ou a reconvergência tomam mais por muito tempo esperado do que.
- A topologia resultante é diferente do que esperada.

O mais frequentemente, estas são as razões para este comportamento:

- Uma incompatibilidade entre a topologia real e a documentada.
- Misconfiguration, tal como uma configuração inconsistente de temporizadores STP, excedendo o diâmetro de STP, ou o misconfiguration do portfast
- Interruptor sobrecarregado CPU durante a convergência ou a reconvergência
- Defeito de software

Como mencionado mais cedo, este documento pode somente fornecer as diretrizes gerais para pesquisar defeitos, devido à ampla variedade de edições que poderiam afetar o STP.

Para compreender porque a convergência toma mais por muito tempo esperado do que, olhe a sequência de eventos STP para encontrar o que estavam acontecendo e nos que ordem. Porque a implementação de STP no Cisco IOS Software não tem o special que registra (à exceção dos eventos específicos, tais como inconsistências da porta), você pode usar capacidades de debugging do Cisco IOS Software STP para compreender o que está acontecendo.

Para o STP, com um Catalyst 6500/6000 que executa o Cisco IOS Software, processar é feito no switch processor (SP) (ou no supervisor), assim que debuga a necessidade de ser permitido no SP. Para grupos de bridge do Cisco IOS Software, processar é feito no route processor (RP), assim que debuga necessidades de ser permitido no RP (MSFC).

Comandos de depuração de STP

Muitos comandos de depuração STP são destinados ao uso da engenharia de desenvolvimento. Não fornecem nenhuma saída que for significativa a alguém sem conhecimento detalhado da implementação de STP no Cisco IOS Software. Algum debuga pode fornecer a saída que é imediatamente legível, como mudanças de estado de porta, mudanças do papel, evento tais como TC, e uma descarga de BPDU recebidos e transmitidos. Esta seção não fornece uma descrição completa do todo o debuga, mas introduz um pouco momentaneamente mais frequentemente usados.

Nota: Quando você usa **comandos debug**, permita o necessário mínimo debuga. Se o tempo real debuga não é precisado, grava a saída ao log um pouco do que imprime ao console. Excessivo debuga pode sobrecarregar o CPU e interromper a operação do interruptor. Para dirigir o resultado do debug ao log em vez ao console ou às sessões de Telnet, emita os **comandos logging console informational e no logging monitor no** modo de configuração global.

Para ver o registro de eventos geral, emita o comando debug spanning-tree event para Per VLAN Spanning-Tree (PVST) e Rapid-PVST. Este é o primeiro debuga que dá uma ideia geral do que está acontecendo com STP.

No modo do Spanning Tree Múltipla (MST), não trabalha para emitir o **comando debug spanning-tree event**. , Emita consequentemente o **comando debug spanning-tree mstp roles** ver a função da porta das mudanças.

Para ver as mudanças de estado da porta STP, emita o **comando debug spanning-tree switch state** junto com o **comando debug pm vp**:

```
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 compreender porque o STP se comporta em uma determinada maneira, é frequentemente útil ver os BPDU que são recebidos e enviados pelo interruptor:

cat-sp# **debug spanning-tree bpdu receive** Spanning Tree BPDU Received debugging is on Nov 6 11:44:27: SP: STP: VLAN1 rx BPDU: config protocol = ieee, packet from GigabitEthernet2/1 , linktype IEEE_SPANNING , enctype 2, encsize 17 Nov 6 11:44:27: SP: STP: enc 01 80 C2 00 00 00 00 06 52 5F 0E 50 00 26 42 42 03 Nov 6 11:44:27: SP: STP: Data 0000000000000000074F1CE847000000138048000 6525F0E4 0801001001400020 00F00 Nov 6 11:44:27: SP: STP: VLAN1 Gi2/1:0000 00 00 00 000000074F1CE847 00000013 80480006525F0E40 8010 0100 1400 0200 0F00

Isto debuga trabalhos para o PVST, o Rápido-PVST, e os modos de MST; mas não descodifica os índices dos BPDU. Contudo, você pode usá-lo para assegurar-se de que os BPDU estejam recebidos.

Para observar o conteúdo da BPDU, emita o comando debug spanning-tree switch rx decode junto com o debug spanning-tree switch rx process para PVST e Rapid-PVST. Emita o comando debug spanning-tree mstp bpdu-rx para visualizar o conteúdo do BPDU para MST:

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 o modo de MST, você pode permitir BPDU detalhado descodifica com este comando debug:

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 o Cisco IOS Software Release 12.1.13E e Mais Recente, condicional debuga para o STP são apoiados. Isto significa que você pode debugar os BPDU que são recebidos ou transmitidos em uma base da porta per. ou do VLAN per.

Emita os **comandos debug condition vlan vlan_num ou debug condition interface interface**, limitar o espaço do resultado do debug à interface per. ou ao VLAN per.

Protegendo a rede contra loops de encaminhamento

Para segurar a incapacidade do STP tratar corretamente determinadas falhas, Cisco desenvolveu um número características e de realces para proteger as redes contra loop de encaminhamento.

Pesquisando defeitos as ajudas STP para isolar e encontrar possivelmente a causa para uma falha particular, quando a aplicação destes realces for a única maneira de fixar a rede contra loop de encaminhamento.

Estes são métodos para proteger sua rede contra loop de encaminhamento:

1. Permita o UniDirectional Link Detection (UDLD) em todos os enlaces de switch a switch. Para obter mais informações sobre do UDLD, refira a compreensão e configurar dos Recursos de Protocolo de Detecção de Link Unidirecional.
2. Permita o protetor de loop em todo o Switches. Para obter mais informações sobre do protetor de loop, refira a medida - realces do protocolo de árvore usando o protetor de loop e os recursos de detecção de desvio BPDU.Quando permitido, o UDLD e o protetor de loop eliminam a maioria das causas possíveis para loop de encaminhamento. Um pouco do que cria um loop de encaminhamento, o link de ofensa (ou tudo liga o dependente no hardware falhando) é fechado ou obstruído.**Nota:** Enquanto esses dois recursos aparecem redundantes de alguma forma, cada um tem capacidades exclusivas. , Use consequentemente ambas as características ao mesmo tempo para fornecer o mais de nível elevado da proteção. Para uma comparação detalhada do UDLD e do protetor de loop, refira o protetor de loop contra a detecção de enlace unidirecional.Há opiniões diferentes em relação ao uso de UDLD agressivo ou normal. Observe que uma UDLD agressiva não proporcionará uma proteção maior contra os loops quando comparada ao modo de UDLD normal. O UDLD assertivo detecta encenações porta-coladas (quando o link está acima, mas lá são nenhum blackholes associado do tráfego). A desvantagem dessa funcionalidade adicional é que a UDLD agressiva pode potencialmente desativar enlaces quando nenhuma falha consistente estiver presente. Frequentemente os povos confundem a alteração do `intervalo de hello` UDLD com a característica do UDLD assertivo. Isto está incorreto. Os cronômetros podem ser modificados nos dois modos UDLD.**Nota:** Em casos raros, o UDLD assertivo pode fechar todas as portas de uplink, que isola essencialmente o interruptor do resto da rede. Por exemplo, isto poderia acontecer quando ambos Switches ascendente estão experimentando muito a utilização elevada da CPU e o modo assertivo UDLD é usado. Consequentemente, recomenda-se que você configura errordisable-intervalos, se o interruptor não tem o gerenciamento fora de banda no lugar.
3. Permita o portfast em todas as portas de estação final.Você deve permitir o portfast de

limitar a quantidade de TC e de inundação subsequente, que podem afetar o desempenho da rede. Use somente este comando com portas que conectam às estações final. Se não, um laço acidental da topologia pode causar um laço do pacote de dados e interromper o interruptor e a operação de rede.**Cuidado:** Exercite o cuidado quando você não usa **nenhum comando spanning-tree portfast**. Este comando remove somente todos os comandos portfast do específico da porta. Este comando permite implicitamente o portfast se você define o **comando default do portfast de Spanning Tree no** modo de configuração global e se a porta não é uma porta de tronco. Se você não configura o portfast globalmente, **nenhum comando spanning-tree portfast** é equivalente ao **comando disable do portfast de Spanning Tree**.

4. Ajuste EtherChannéis ao `modo desirable em` ambos os lados (onde apoiado) e na opção `não silencioso`.O modo desejável ativará o protocolo de agregação de porta (PAgP) para assegurar a consistência do tempo de corrida entre peers de canais. Isto dá um grau adicional de proteção contra laços, especialmente durante reconfigurações do canal (como quando os links se juntam ou se saem do canal, e detecção de falha do link). Há um protetor incorporado do Misconfiguration do canal, que sejam permitidos à revelia e que impeça os loop de encaminhamento devendo canalizar o misconfiguration ou as outras circunstâncias. Para obter mais informações sobre desta característica, refira compreendendo a detecção de inconsistência de EtherChannel.
5. Não desabilite a autonegociação (se apoiado) nos enlaces de switch a switch.Os mecanismos da autonegociação podem transportar a informação de falha remota, que é a maneira mais rápida detectar a falha no lado remoto. O Deve falhar seja detectado no lado remoto, o lado local derruba o link mesmo se o link ainda está recebendo pulsos. Comparado aos mecanismos de detecção de nível elevado tais como o UDLD, a autonegociação é muito rápida (dentro dos microssegundos) mas falta a cobertura fim-a-fim do UDLD (tal como o datapath inteiro: CPU — lógica da transmissão — port1 — port2 — lógica da transmissão — CPU contra port1 — port2). O modo do UDLD assertivo fornece a funcionalidade similar àquela da autonegociação a propósito da detecção de falha. Quando a negociação é suportada nos dois lados do enlace, não há necessidade de habilitar o UDLD do modo agressivo.
6. Use o cuidado quando você ajusta os temporizadores de STP.Os temporizadores de STP são dependentes de se e da topologia de rede. O STP pode não funcionar corretamente com modificações arbitrárias feitas nos cronômetros. Para obter mais informações sobre dos temporizadores de STP, refira temporizadores compreensivos e de ajustamentos do Spanning Tree Protocol.
7. Se houver a possibilidade de ocorrerem ataques de recusa de serviço, proteja o perímetro de STP da rede com o Protetor de Raiz.O Protetor de Raiz e o Protetor de BPDU permitem que você proteja o STP contra influências externas. Se tal ataque é uma possibilidade, o protetor de raiz e o protetor de BPDU devem ser usados para proteger a rede. Para obter mais informações sobre do protetor de raiz e do protetor de BPDU, refira estes documentos:Melhoria de protetor de raiz do protocolo de árvore de abrangênciaRealce do protetor de BPDU do portfast de Spanning Tree
8. Permita o protetor de BPDU em portas habilitadas de portfast, de impedir que o STP esteja afetado pelos dispositivos de rede desautorizados (tais como o Hubs, o Switches, e os roteadores de Bridging) que são conectados às portas.Se o protetor de raiz é configurado corretamente, já impedirá que o STP esteja influenciado da parte externa. Se o protetor de BPDU é permitido, fechará as portas que estão recebendo todos os BPDU (não somente bpdus superior). Isto pode ser útil se tais incidentes precisam de ser investigados, porque o

protetor de BPDU produz o mensagem do syslog e fecha a porta. Deve-se notar que os laços devida não estão impedidos pela raiz ou pelos protetores de BPDU, se duas portas habilitadas de portfast são conectadas diretamente ou através do hub.

9. Evite o tráfego de usuário no VLAN de gerenciamento. O gerenciamento da VLAN está incluído em um bloco de construção, e não na rede inteira.A relação do gerenciamento de switch recebe pacotes de transmissão no VLAN de gerenciamento. Se os broadcasts excessivos ocorrerem (como uma tempestade de transmissão ou um aplicativo funcionando mal), o interruptor CPU pôde tornar-se sobrecarregado, que poderia possivelmente distorcer a operação de STP.
10. Uma raiz (codificada) predizível e localização de raiz de STP de backup STP.A raiz STP e a raiz alternativa STP devem ser configuradas de modo que a convergência, no caso das falhas, ocorra em uma maneira previsível e construa a topologia ótima em cada encenação. Não deixe a prioridade do STP no valor padrão, para impedir a seleção imprevisível do switch-raiz.

Informações Relacionadas

- Suporte a Produtos de LAN
- Suporte de tecnologia de switching de LAN
- Suporte Técnico e Documentação - Cisco Systems