Identificar e Solucionar Problemas de Inconsistências de PVID e Tipo de Spanning Tree

Contents

Introdução

Este documento descreve como solucionar problemas de duas inconsistências do Spanning Tree Protocol (STP), Port VLAN ID (PVID) e Type.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento dos conceitos do STP.

Componentes Utilizados

Este documento não é restrito a versões de software ou hardware específicas.

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

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Informações de Apoio

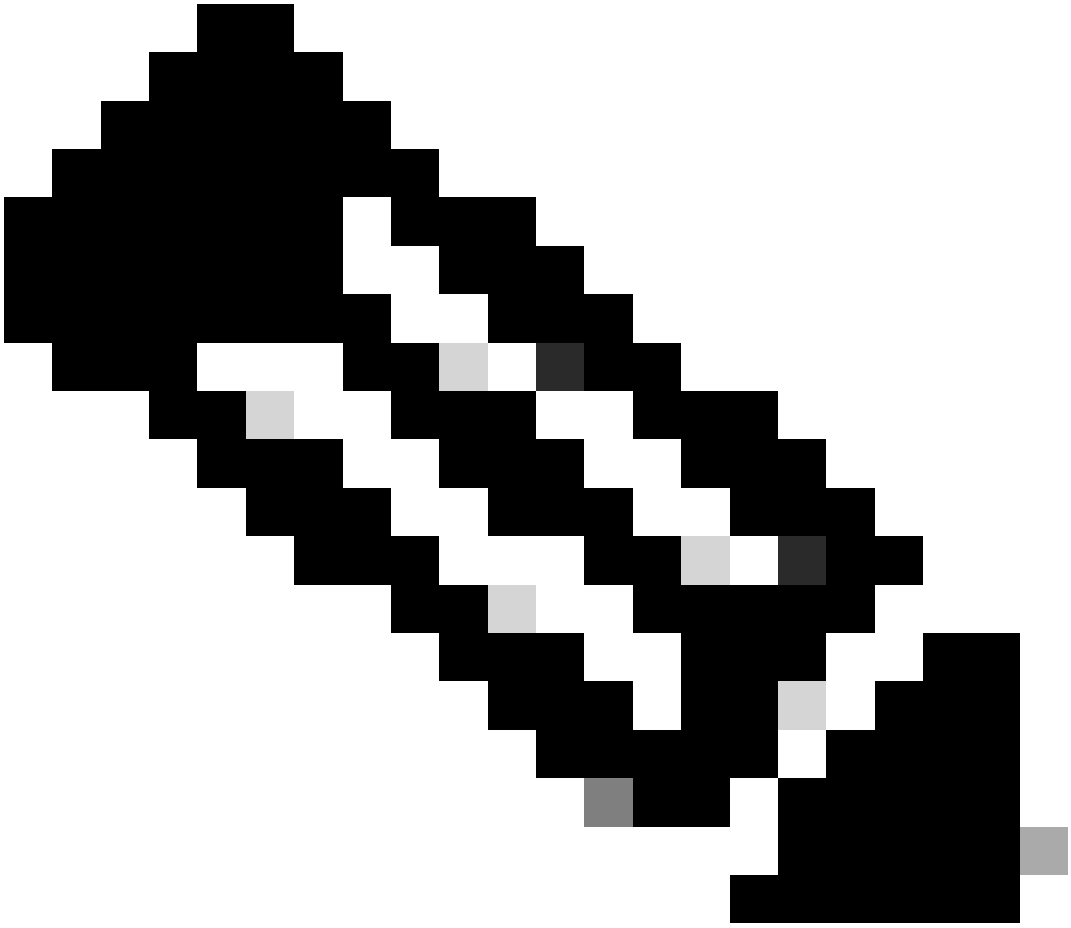
Em redes da Camada 2 (L2), pode haver somente um caminho entre quaisquer dois dispositivos. A redundância é suportada pelo Spanning-Tree Protocol (STP), que detecta e bloqueia caminhos redundantes e, assim, evitando loops de encaminhamento. Determinadas configurações incorretas podem conduzir a uma falha de STP e causar uma queda da rede. Para evitar o tempo de inatividade, algumas melhorias foram implementadas para que o STP detecte determinados casos de configuração incorreta e a porta relevante seja colocada em um estado "inconsistente".

Pode haver diferentes tipos de inconsistências de STP:

- Inconsistência de loop — Detectada pelo recurso Protetor de loop. Para obter mais informações, consulte Configurar STP com Proteção de Loop e Detecção de Desvio de BPDU.
- Inconsistência de raiz — detectada pelo recurso Protetor de raiz. Para obter mais informações, consulte Enhance Spanning Tree Protocol with Root Guard.
- Inconsistência do EtherChannel — detectada pelo recurso de detecção de consistência do EtherChannel. Para obter mais informações, consulte Noções Básicas sobre a Detecção de Inconsistência do EtherChannel.
- Inconsistência de PVID (Port VLAN ID) — Uma BPDU (Bridge Protocol Data Unit) por VLAN spanning tree (PVST+) é recebida em uma VLAN diferente da que foi originada: (`Incompatibilidade de ID de VLAN de porta` ou `*PVID_Inc`).
- Inconsistência de tipo — Um PVST+ BPDU é recebido em um tronco não 802.1Q.

Teoria por trás das inconsistências de PVID e de tipo

Os switches Cisco Catalyst implementam PVST que usam troncos Inter-Switch Link (ISL). Com o suporte do entroncamento IEEE 802.1Q e ISL, foi necessária uma forma de interoperação entre o PVST e o conceito IEEE 802.1Q de uma única árvore de abrangência para todas as VLANs. O recurso PVST+ foi introduzido para tratar desse requisito.



> Observação: do ponto de vista do STP, o IEEE 802.1D não reconhece VLAN e o IEEE 802.1Q reconhece VLAN, mas usa uma única instância do STP para todas as VLANs. Ou seja, se a porta estiver bloqueando, ela estará bloqueando para todas as VLANs nessa porta.

O mesmo se aplica ao encaminhamento.

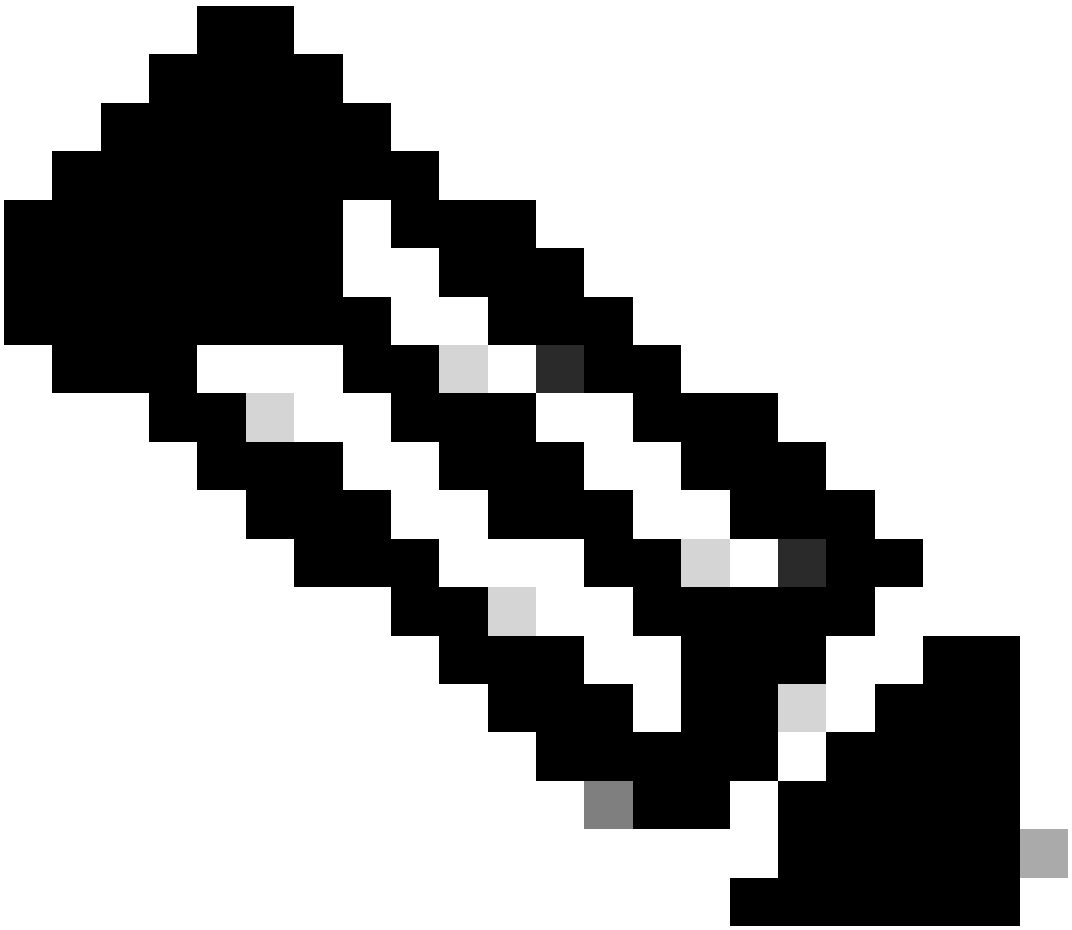
Esta lista mostra como o PVST+ interopera com IEEE 802.1Q ou IEEE 802.1D, se a VLAN Nativa em um tronco IEEE 802.1Q for a VLAN 1:

- As BPDUs de STP da VLAN 1 são enviadas para o endereço MAC de STP IEEE (0180.c200.0000), sem marcação.
- As BPDUs de STP da VLAN 1 também são enviadas para o endereço MAC do PVST+, sem marcação.
- As BPDUs STP não VLAN 1 são enviadas para o endereço MAC do PVST+ (também chamado de endereço MAC do Protocolo de Árvore Geradora Compartilhada (SSTP -

Shared Spanning Tree Protocol), 0100.0ccc.ccd), marcado com uma marca de VLAN IEEE 802.1Q correspondente.

Se a VLAN Nativa em um tronco IEEE 802.1Q não for a VLAN 1:

- As BPDUs de STP da VLAN 1 são enviadas para o endereço MAC do PVST+, marcado com uma marca de VLAN IEEE 802.1Q correspondente.
- As BPDUs de STP da VLAN 1 também são enviadas para o endereço MAC de STP IEEE na VLAN Nativa do tronco IEEE 802.1Q, sem marcação.
- As BPDUs STP não VLAN 1 são enviadas para o endereço MAC PVST+, marcado com uma marca de VLAN IEEE 802.1Q correspondente.



Observação: as BPDUs STP de VLAN nativa são enviadas sem marcação.

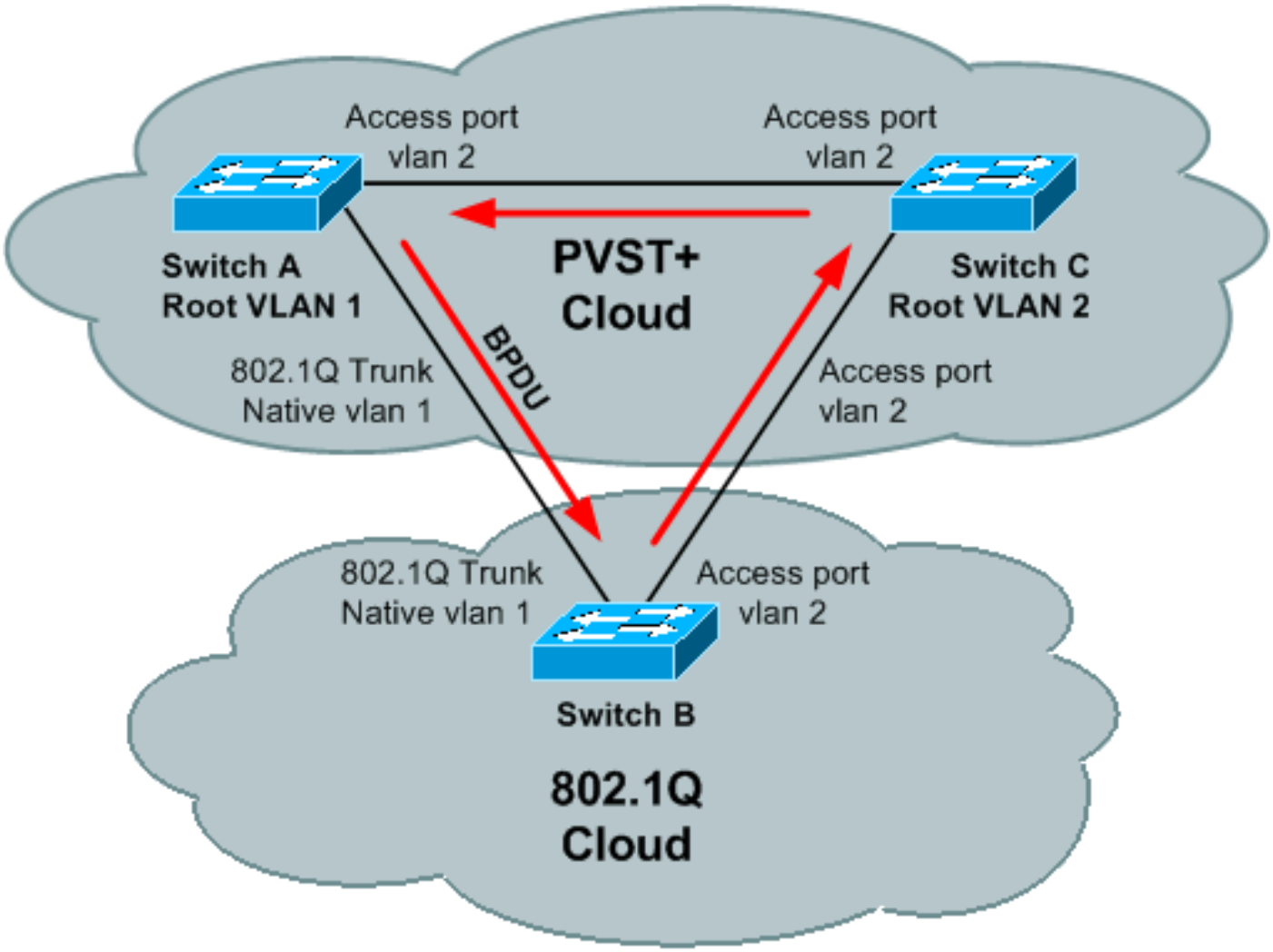
Dessa forma, o STP da VLAN 1 do PVST+ é mesclado com o STP do IEEE 802.1D ou 802.1Q, enquanto outras VLANs são encapsuladas através da nuvem de pontes IEEE 802.1D ou 802.1Q.

Por exemplo, a nuvem IEEE 802.1D ou 802.1Q é semelhante a um "fio" para as VLANs do PVST+ diferentes de 1.

Para que o STP opere corretamente, observe certas regras ao conectar pontes PVST+ a pontes IEEE 802.1D ou 802.1Q. A regra principal é que as pontes PVST+ devem se conectar a pontes IEEE 802.1D ou 802.1Q através de um tronco IEEE 802.1Q com uma VLAN Nativa consistente em todas as pontes que se conectam à nuvem de pontes IEEE 802.1Q ou 802.1D.

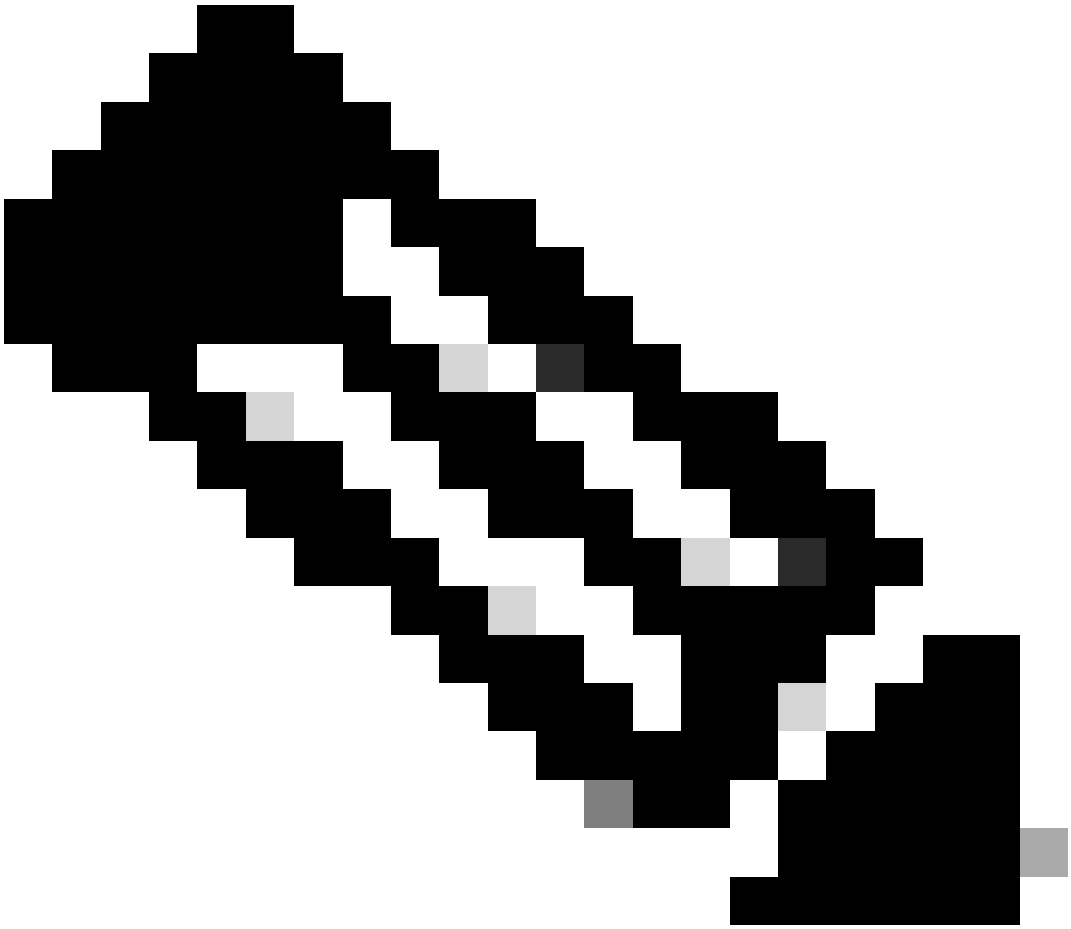
O BPDU do PVST+ contém um número de VLAN que permite que as pontes do PVST+ detectem se a regra anterior não é respeitada. Quando um switch Catalyst detecta um erro de configuração, as portas correspondentes são colocadas em um estado "PVID-inconsistency" ou "type-inconsistency", que bloqueia efetivamente o tráfego na VLAN correspondente em uma porta correspondente. Esses estados evitam loops de encaminhamento que são causados por configuração incorreta ou por conexões com fio incorretas.

Para ilustrar a necessidade de detecção de inconsistência, considere esta topologia, onde os switches A e C executam o STP PVST+ e o switch B executa o STP 802.1Q:



Se a BPDU da raiz na VLAN 1 for melhor que a BPDU da raiz na VLAN 2, não haverá porta de bloqueio na topologia da VLAN 2. A BPDU da VLAN 2 nunca faz um "círculo completo" em torno da topologia; ela é substituída pela BPDU da VLAN 1 no link B-C, porque B executa somente um

STP mesclado com VLAN 1 STP de PVST+. Assim, há um loop de encaminhamento. Felizmente, o switch A envia PVST+ BPDUs da VLAN 2 (para o endereço SSTP que é inundado pelo switch B) em direção ao switch C. O switch C pode colocar a porta C-B em um estado de tipo inconsistente, o que impede o loop.

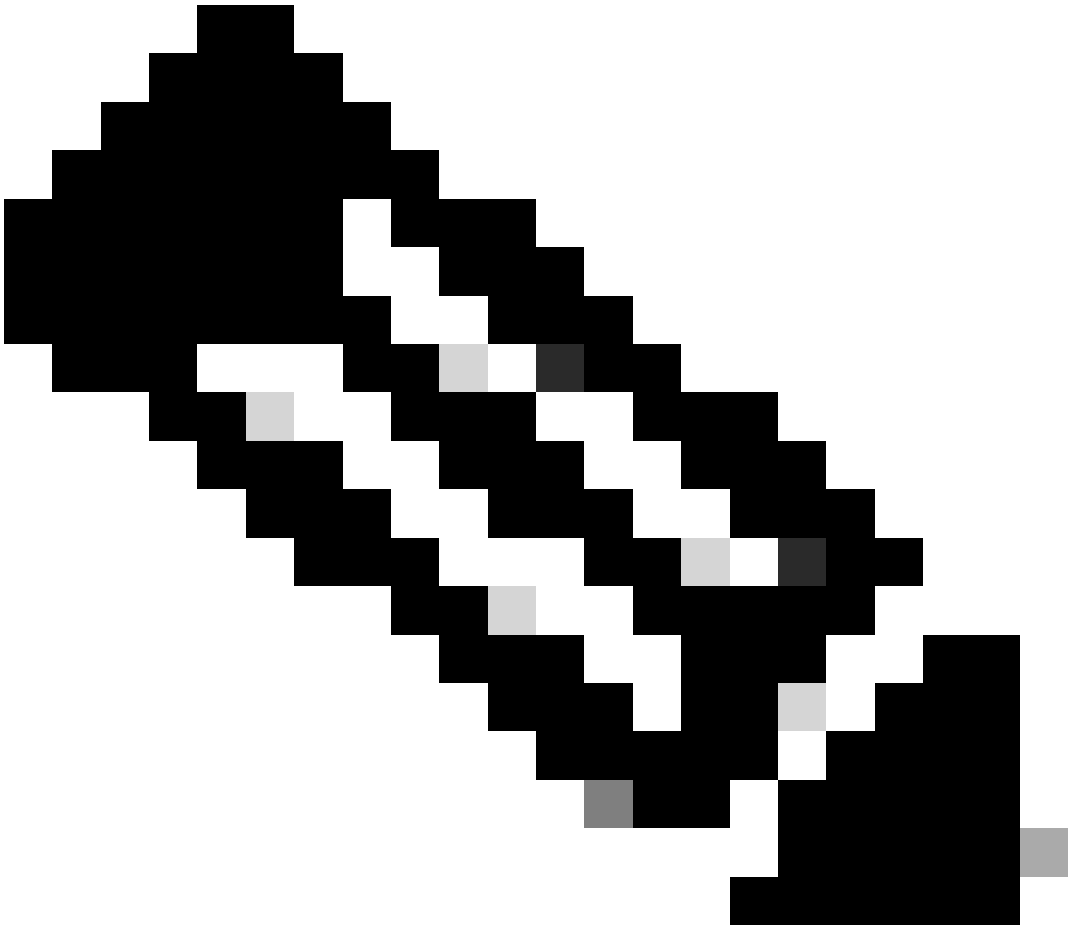


> Observação: em algumas saídas de comando, o estado *-inconsistente do STP é chamado de "interrompido".

Quando a inconsistência de STP é detectada, os switches enviam estas mensagens de syslog:

```
%SPANTREE-2-RECV_1Q_NON_TRUNK: Received IEEE 802.1Q BPDU on non trunk
FastEthernet0/1 on vlan 1.
%SPANTREE-2-BLOCK_PORT_TYPE: Blocking FastEthernet0/1 on vlan 1.
Inconsistent port type.

%SPANTREE-2-RX_1QPVIDERR: Rcved pvid_inc BPDU on 1Q port 3/25 vlan 1
%SPANTREE-2-RX_BLKPORTPVID: Block 3/25 on rcving vlan 1 for inc peer vlan 10
%SPANTREE-2-TX_BLKPORTPVID: Block 3/25 on xmtting vlan 10 for inc peer vlan
```

Nesse exemplo, a VLAN 1 é onde a BPDU foi recebida e a VLAN 10 é onde a BPDU foi originada. Quando a inconsistência é detectada, ambas as VLANs são bloqueadas na porta em que essa BPDU é recebida.



> Observação: as mensagens podem variar com base no tipo e na versão do Cisco IOS® Software Release que está em uso.

Observe que, se a porta não receber mais BPDUs inconsistentes, o estado *-inconsistente será limpo e o STP alterará o estado da porta com base na operação normal do STP. Uma mensagem do syslog é enviada para indicar a alteração:

```
%SPANTREE-SP-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on vlan 1.
Port consistency restored.
```

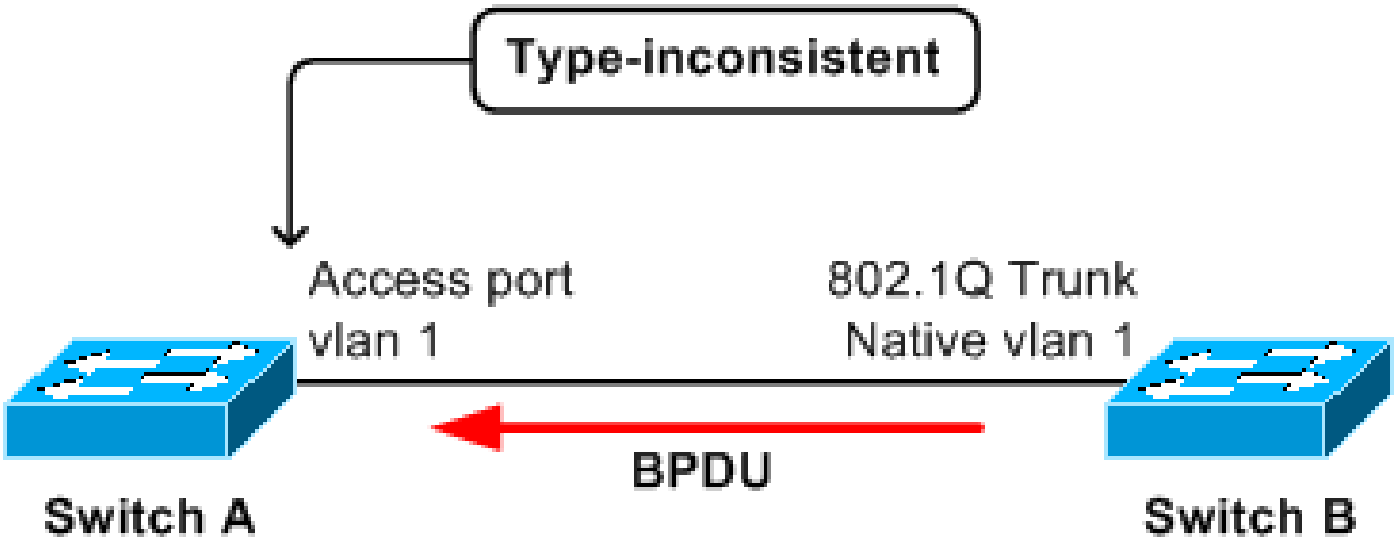
Para obter mais detalhes sobre a operação do PVST+, consulte Exemplo de Configuração de Spanning Tree de PVST+ para Migração do Rapid-PVST.

Troubleshooting

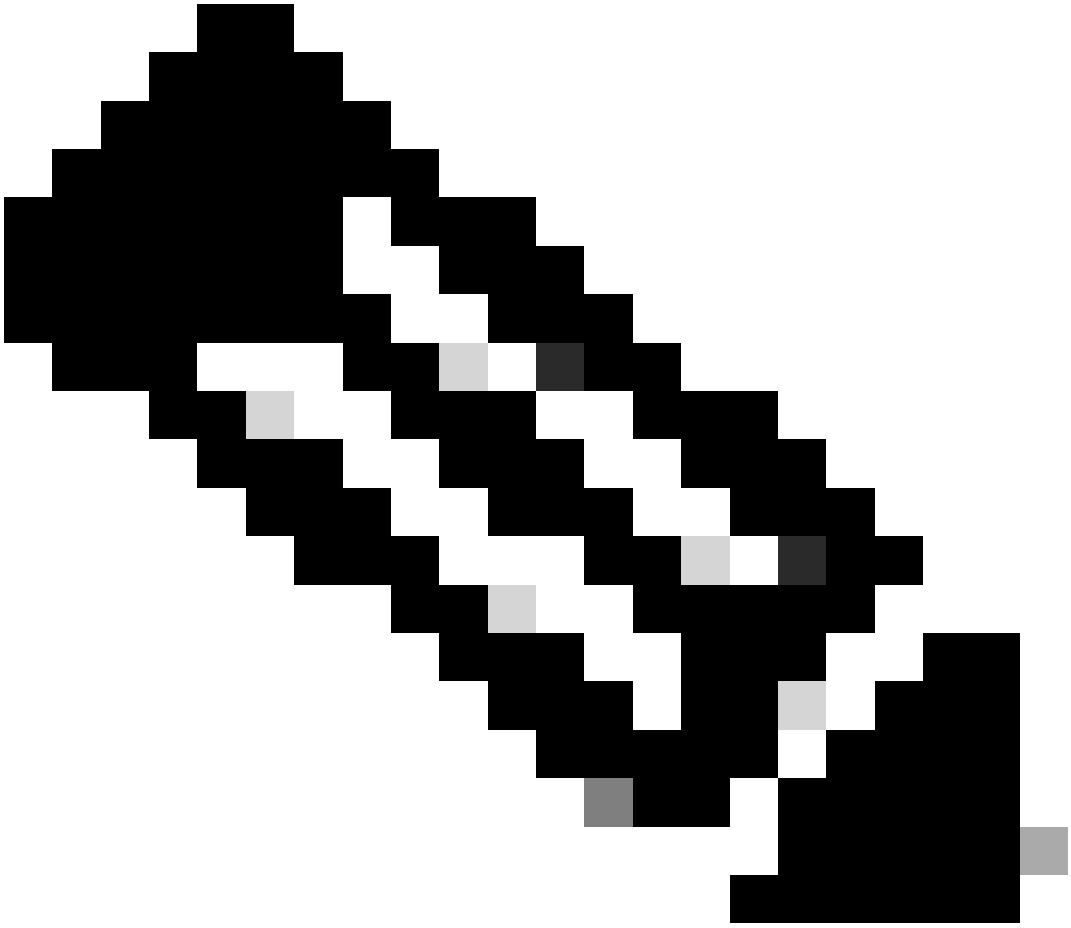
Para ver a lista de portas inconsistentes, a implementação recente do STP com base no Cisco IOS suporta o comando show spanning-tree inconsistentports.

Na maioria dos casos, o motivo para a detecção de inconsistência de STP na porta é aparente:

- A porta de acesso recebe um BPDU SSTP marcado com IEEE 802.1Q.

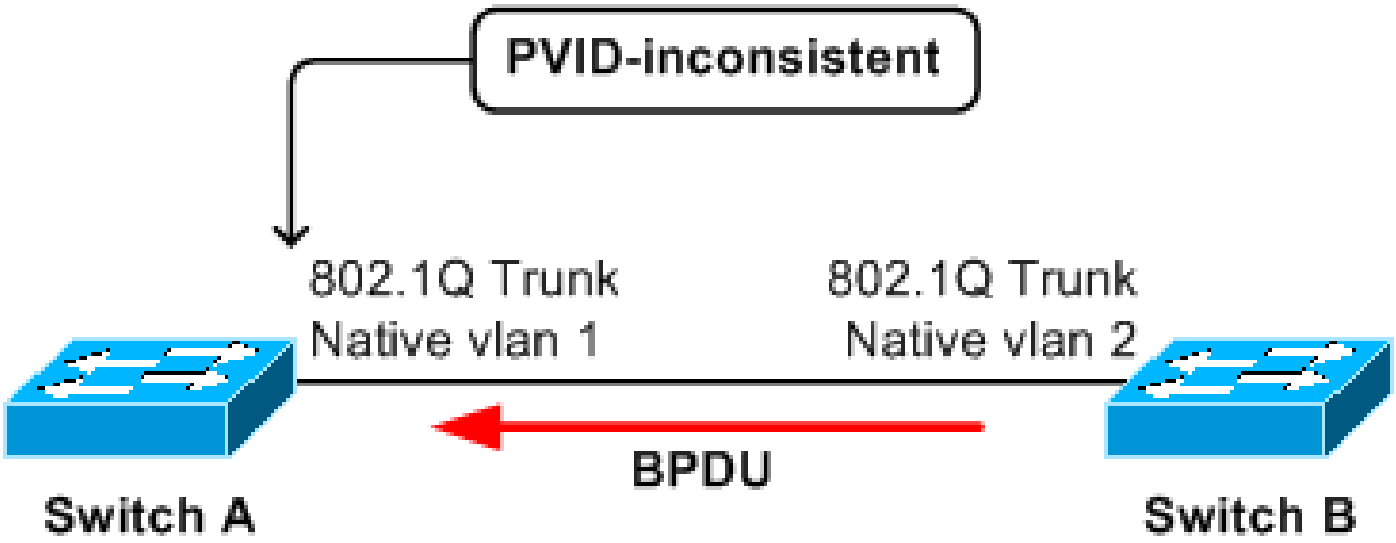


Neste cenário, a porta de acesso na ponte A recebe, da ponte B, um PVST+ BPDU marcado do STP de uma VLAN diferente de 1. A porta em A pode ser colocada em um estado de tipo inconsistente.



Observação: os switches não precisam ser conectados diretamente; se forem conectados por um ou mais switches IEEE 802.1D ou IEEE 802.1Q, ou até mesmo hubs, o efeito será o mesmo.

- A porta de entroncamento IEEE 802.1Q recebe uma BPDU SSTP não marcada com um tipo, comprimento e valor (TLV) de VLAN que não corresponde à VLAN onde a BPDU foi recebida.



Neste cenário, a porta de tronco em A recebe um PVST+ BPDU do STP de VLAN 2 com uma marca de VLAN 2. Isso dispara a porta em A para ser bloqueada na VLAN 1 e na VLAN 2.

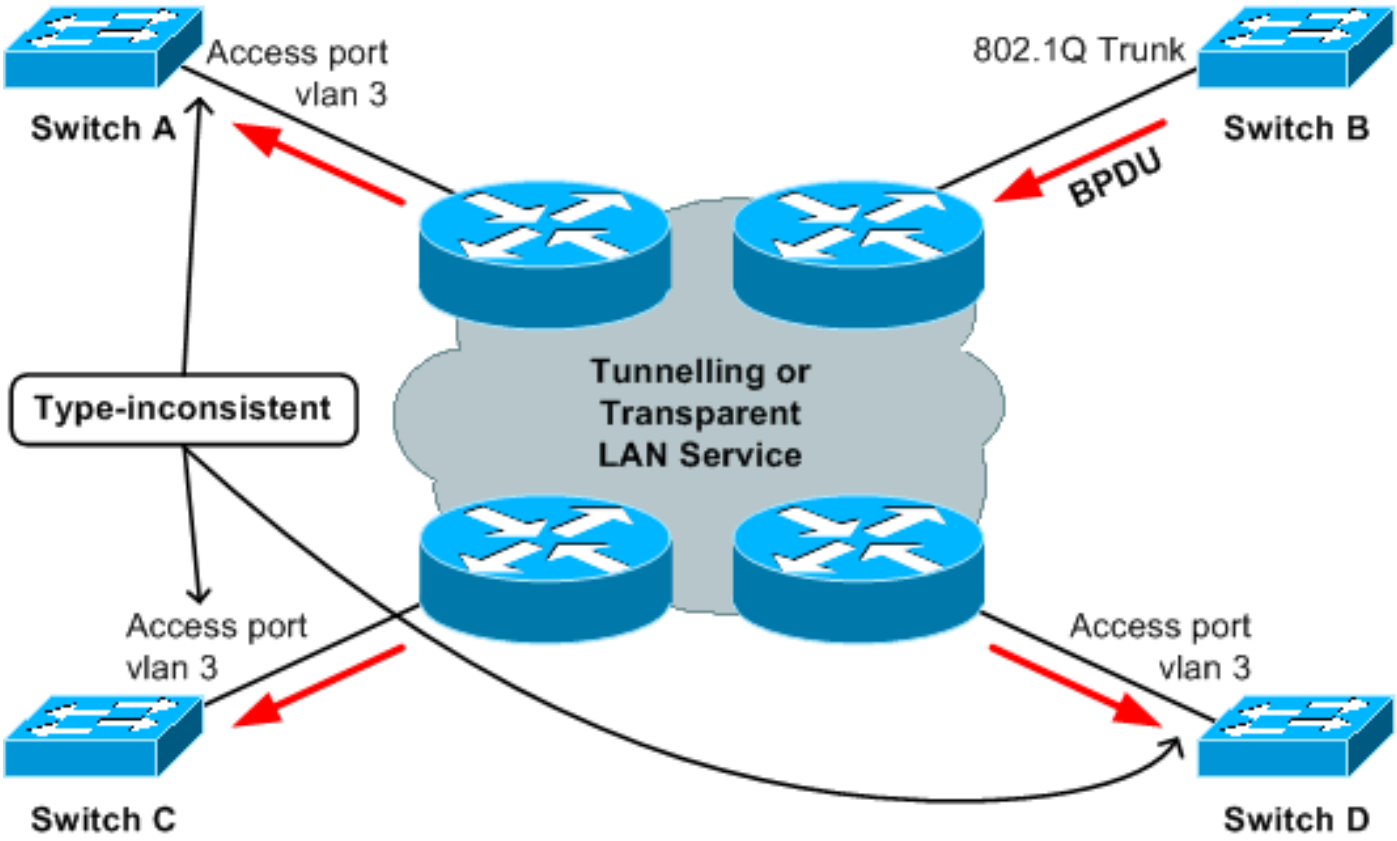
Se os dispositivos em ambas as extremidades de um link ponto-a-ponto forem switches Cisco Catalyst, um exame da configuração de porta local e remota normalmente revela a incompatibilidade de configuração:

- A porta está configurada para entroncamento IEEE 802.1Q em um lado, mas o outro lado é a porta de acesso.
- Os troncos IEEE 802.1Q estão nos dois lados, mas as VLANs nativas são diferentes.

Nesses casos, corrija a incompatibilidade de configuração para resolver a inconsistência do STP.

Em alguns casos, é mais difícil identificar o motivo:

- Um BPDU é recebido de uma mídia compartilhada com vários dispositivos.
- Um BPDU é recebido, da nuvem do switch, que implementa um modelo IEEE 802.1D ou 802.1Q STP enquanto os switches PVST+ estão conectados à nuvem.
- Um BPDU vem por trás de algum túnel (por exemplo, nuvem Data Link Switch Plus [DLSw+], tunelamento de protocolo L2, EoMPLS, Virtual Path Links [VPLs], LAN Emulation [LANE] e outros).



Neste exemplo, o switch B está configurado incorretamente e injeta um BPDU SSTP na nuvem. Isso faz com que as portas nos switches A, C e D se tornem de tipo inconsistente. O problema é que o dispositivo que origina a BPDU "ofensiva" não está diretamente conectado aos switches afetados. Assim, com muitos dispositivos no tronco, pode consumir tempo para solucionar todos eles.

Felizmente, há uma abordagem sistemática para solucionar esse problema:

1. Estabeleça o endereço MAC de origem e o ID da bridge de envio da BPDU. Isso deve ser feito enquanto o problema ocorre

2. Localize a bridge que origina a BPDU "ofensiva". Isso pode ser feito posteriormente, não necessariamente quando o problema ocorrer.

Para a Etapa 1, normalmente há duas opções: usar um analisador de pacotes ou ativar a depuração para ver o dump de BPDUs recebidas.

Para obter mais detalhes sobre o uso de uma depuração para despejar BPDUs de STP, consulte a seção Usar Comandos de Depuração de STP de Identificar e Solucionar Problemas de STP em Switches Catalyst.

Este é um exemplo de saída de depuração que mostra o BPDU recebido:

```
*Mar 14 19:33:27: STP SW: PROC RX: 0100.0ccc.cccd<-0030.9617.4f08 type/len 0032
*Mar 14 19:33:27:     encap SNAP linktype sstp vlan 10 len 64 on v10 Fa0/14
*Mar 14 19:33:27:     AA AA 03 00000C 010B SSTP
*Mar 14 19:33:27:     CFG P:0000 V:00 T:00 F:00 R:8000 0050.0f2d.4000 00000000
```

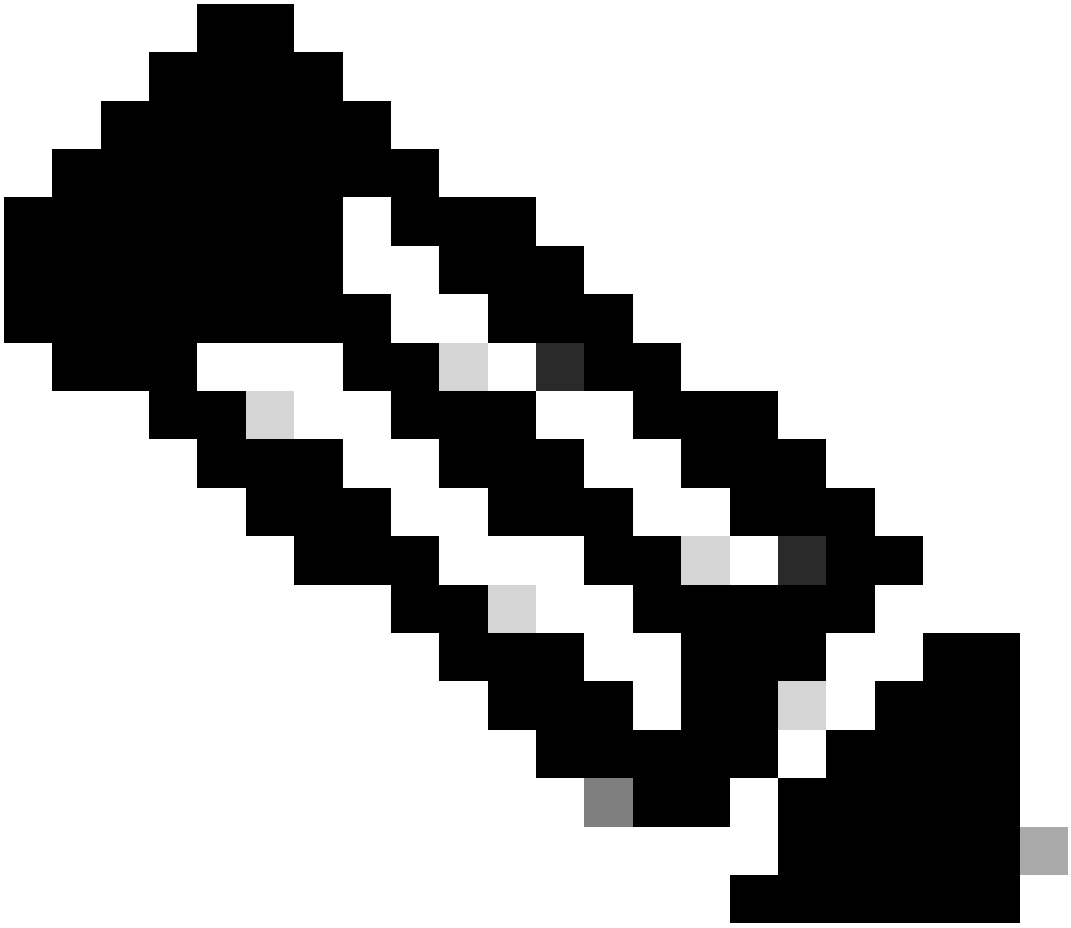
```
*Mar 14 19:33:27:      B:8000 0050.0f2d.4000 80.99 A:0000 M:1400 H:0200 F:0F00
*Mar 14 19:33:27:      T:0000 L:0002 D:0001
```

Quando souber o endereço MAC origem e o ID da bridge de envio, você precisará localizar o dispositivo ao qual esse endereço MAC pertence. Isso pode ser complicado pelo fato de que os switches normalmente não aprendem os endereços MAC de uma origem dos quadros de BPDU. Se você executar o comando show mac-address-table addressBPDU_mac_address (para switches baseados no Cisco IOS), normalmente nenhuma entrada será encontrada.

Uma maneira de encontrar o endereço MAC "ofensivo" é coletar, de todos os switches que estão conectados à nuvem, a saída do comando show spanning-tree. Essas saídas de comando incluem informações sobre o ID de cada ponte.

<#root>

```
Boris#

show spanning-tree


!--- Use with Cisco IOS.

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    0
             Address     0007.4f1c.e847
             Cost        131
             Port        136 (GigabitEthernet3/8)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00d0.003f.8800

!--- Output suppressed.
```



> Observação: com base no modelo, na versão do software e na configuração, um switch pode ter vários endereços MAC de ID de bridge. Felizmente, todos os endereços podem estar em um determinado intervalo (por exemplo, de 0001.1234.5600 a 0001.1234.5640). Se você souber um endereço MAC de ID de bridge, poderá verificar se o endereço MAC de ID de bridge enviado (encontrado na Etapa 1) está dentro do intervalo de endereços MAC de ID de bridge fornecidos. Você também pode usar ferramentas de gerenciamento de rede para coletar as IDs de todas as bridges.

Depois de encontrar a ponte que enviou a BPDU ofensiva, você precisa verificar a configuração da porta conectada à nuvem: certifique-se de que ela seja consistente (entroncamento em oposição a não entroncamento e VLAN nativa) com outros switches que também estejam conectados à mesma nuvem.

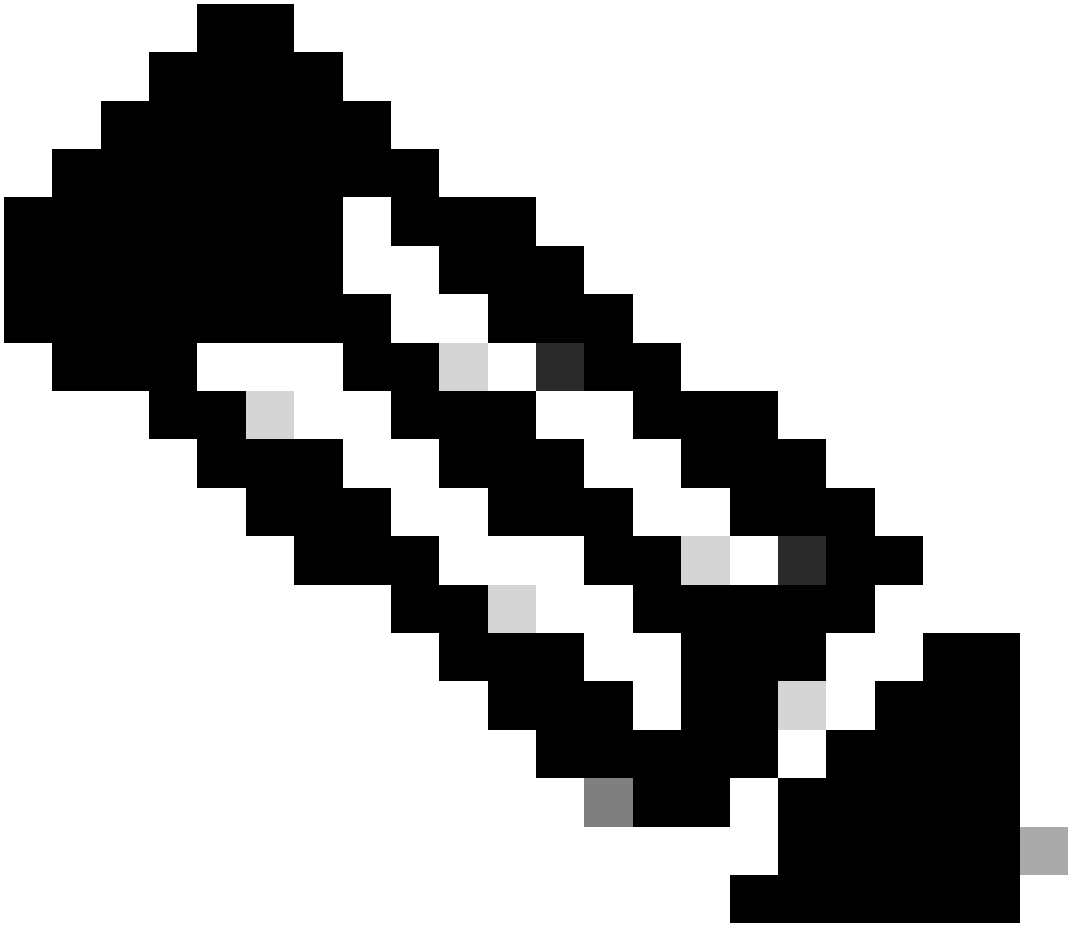
Pode acontecer que a bridge envie BPDUs apropriados, mas eles são modificados incorretamente dentro da nuvem de tunelamento. Nesse caso, você pode ver que a BPDU ofensiva que entra na nuvem é consistente com a configuração das outras pontes, mas a mesma BPDU se torna inconsistente quando sai da nuvem (por exemplo, a BPDU sai da nuvem em uma

VLAN diferente, ou se torna rotulada ou não). Nesse caso, pode ajudar a verificar se o endereço MAC origem do BPDU ofensivo pertence à mesma bridge que o ID da bridge emissora. Se esse não for o caso, você pode tentar localizar a ponte que possui o endereço MAC de origem da BPDU e verificar sua configuração.

Para localizar o switch que possui o endereço MAC de origem da BPDU, você pode usar a mesma abordagem (para encontrar o ID da bridge), exceto que agora a saída do comando show module é inspecionada (para Catalyst 4000 e 6000). Para outros switches Catalyst, você pode examinar a saída do comando show interface para ver os endereços MAC que pertencem às portas.

<#root>

```
Cat4000-#
show module


!--- Use for Catalyst 4000,5000,6000

Mod  Ports Card Type                              Model             Serial No.
----+-----+-------------------------------------+-----------------+-----------
 1      2  1000BaseX (GBIC) Supervisor(active)    WS-X4515          ZZZ00000001
 5     14  1000BaseT (RJ45), 1000BaseX (GBIC)     WS-X4412-2GB-T    ZZZ00000002

 M MAC addresses                    Hw  Fw           Sw               Status
--+--------------------------------+---+------------+----------------+---------
 1 000a.4172.ea40 to 000a.4172.ea41 1.2 12.1(12r)EW  12.1(14)E1, EARL Ok
 5 0001.4230.d800 to 0001.4230.d80d 1.0                               Ok

!--- Output suppressed.

cat3550#
show interface | i bia


  Hardware is Gigabit Ethernet, address is 0002.4b28.da80 (bia 0002.4b28.da80)
  Hardware is Gigabit Ethernet, address is 0002.4b28.da83 (bia 0002.4b28.da83)
  Hardware is Gigabit Ethernet, address is 0002.4b28.da86 (bia 0002.4b28.da86)
  Hardware is Gigabit Ethernet, address is 0002.4b28.da88 (bia 0002.4b28.da88)
  Hardware is Gigabit Ethernet, address is 0002.4b28.da89 (bia 0002.4b28.da89)

!--- Output suppressed.
```



Observação: se a nuvem for DLSw+, consulte Entendendo e configurando DLSw e 802.1Q

Informações Relacionadas

- Suporte de produto de protocolo LAN/Spanning Tree
- Suporte de tecnologia
- Suporte técnico e downloads da Cisco

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.