Solución de problemas de incoherencias de tipo y PVID del árbol de extensión

Contenido

Introducción

Este documento describe cómo resolver problemas de inconsistencias de dos Spanning Tree Protocol (STP), Port VLAN ID (PVID) y Type.

Prerequisites

Requirements

Cisco recomienda que conozca los conceptos de STP.

Componentes Utilizados

Este documento no se limita a una versión específica de software o de hardware.

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

Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Antecedentes

En las redes de Capa 2 (L2), sólo puede haber una trayectoria entre dos dispositivos

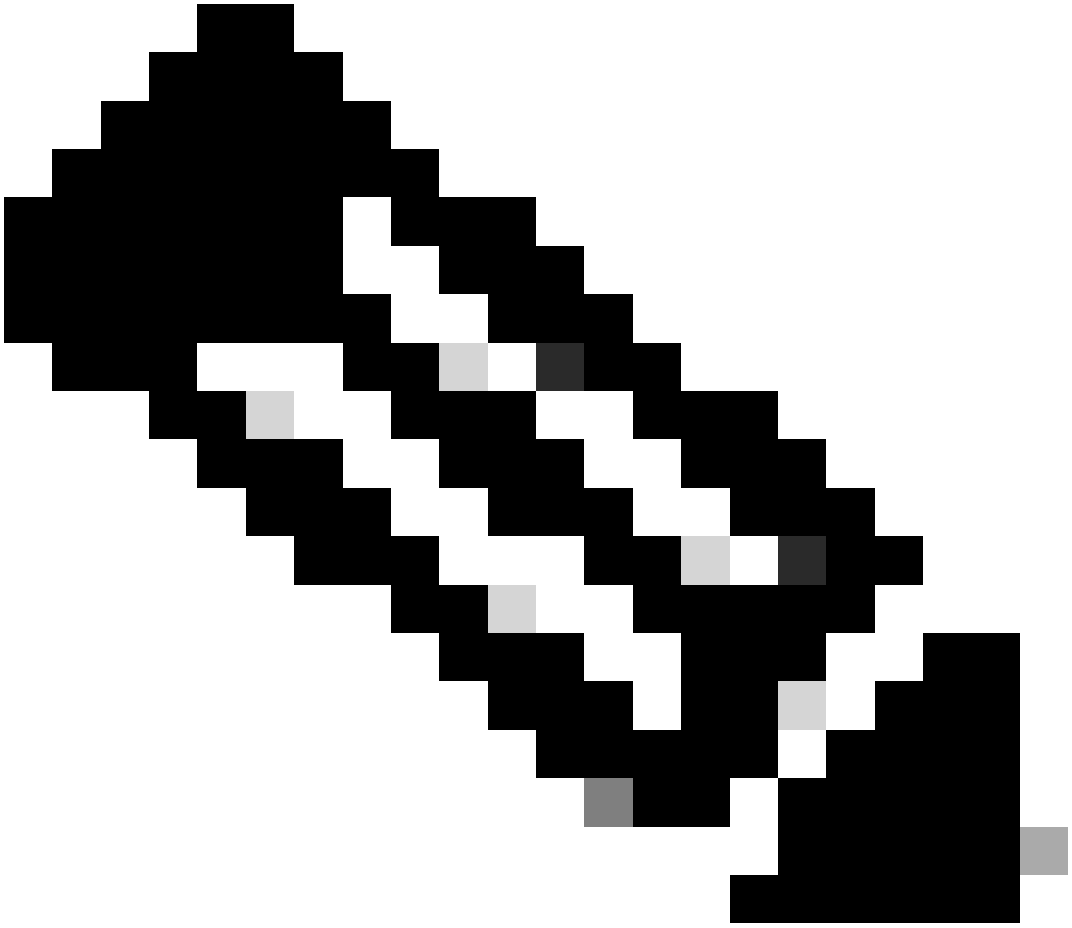
cualesquiera. La redundancia es soportada por el Spanning-Tree Protocol (STP), que detecta y bloquea las trayectorias redundantes y, por lo tanto, evita el reenvío de los loops. Ciertas configuraciones incorrectas pueden resultar en una falla del STP y provocar la interrupción de la red. Para evitar el tiempo de inactividad, se implementaron algunas mejoras para que el STP detecte ciertos casos de configuración incorrecta, y el puerto relevante se ponga en un estado "incoherente".

Pueden existir diversos tipos de inconsistencias del STP:

- Incoherencia del loop: esta incoherencia es detectada por la función Protección de Loop. Para obtener más información, consulte Configuración de STP con protección de loop y detección de desviación de BPDU.
- Incoherencia de la Raíz: esta incoherencia es detectada por la función Protección de Raíz. Para obtener más información, consulte Mejora del protocolo de árbol de expansión con protección de raíz.
- Incoherencia de EtherChannel: la función de detección de coherencia de EtherChannel detecta esta incoherencia. Para más información, consulte Cómo Comprender la Detección de Incoherencias en EtherChannel.
- Incoherencia de ID de VLAN de puerto (PVID): se recibe una unidad de datos de protocolo de puente (BPDU) de árbol de extensión por VLAN (PVST+) en una VLAN diferente de la que se originó: (`Port VLAN ID` Mismatchor`*PVID_Inc`).
- Incoherencia de tipo: se recibe una PVST+ BPDU en un trunk que no es 802.1Q.

Teoría de incoherencias de PVID y de tipo

Los switches Cisco Catalyst implementan PVST que utilizan troncales Inter-Switch Link (ISL). Con el soporte de IEEE 802.1Q y de trunking ISL, se necesitaba una forma para ejecutar el interfuncionamiento entre el PVST y el concepto de IEEE 802.1Q de un solo spanning tree para todas las VLANs. La función PVST+ fue creada para cumplir este requisito.



Nota: desde el punto de vista de STP, IEEE 802.1D no reconoce VLAN e IEEE 802.1Q sí VLAN, pero utiliza una única instancia STP para todas las VLAN. Es decir, si el puerto ejerce un bloqueo, lo hace para todas las VLANs de ese puerto.

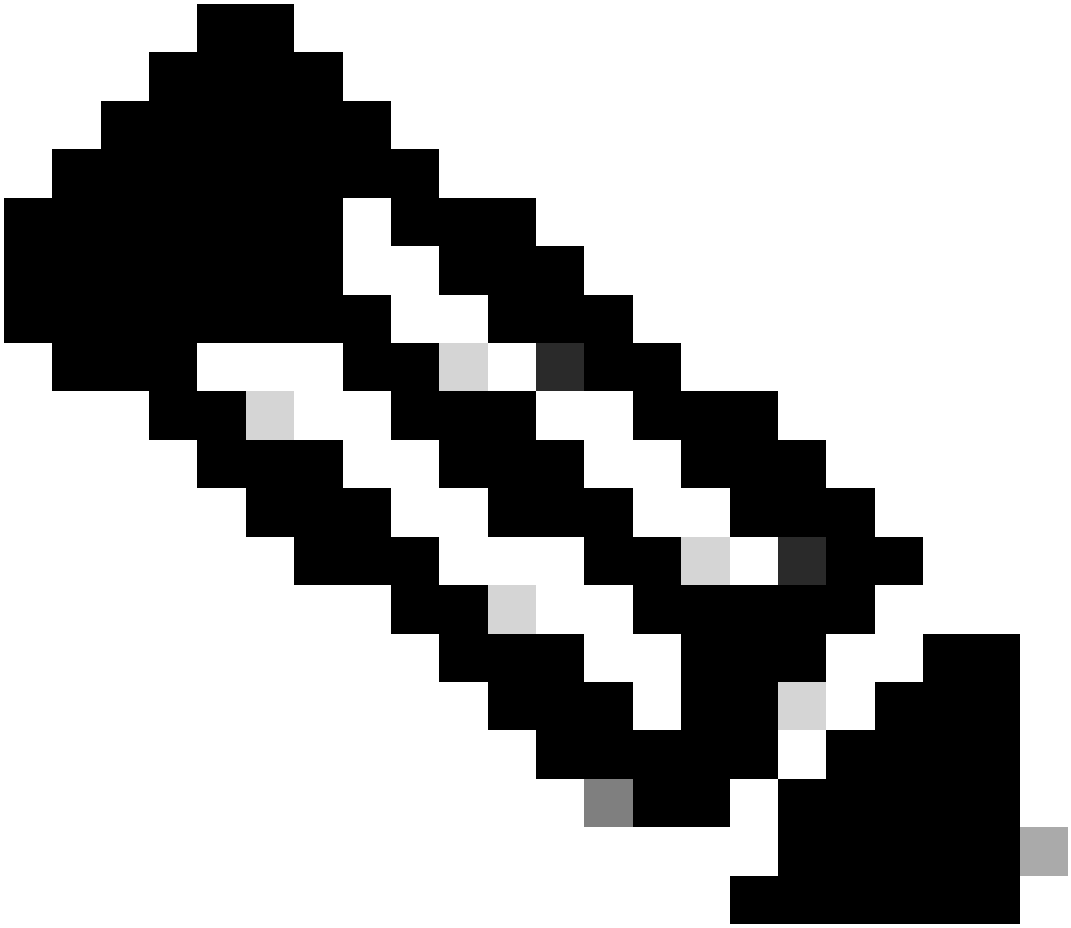
Lo mismo sucede con el reenvío.

Esta lista muestra cómo el PVST+ interactúa con el IEEE 802.1Q o el IEEE 802.1D, si la VLAN nativa en un trunk de IEEE 802.1Q es VLAN1:

- Las VLAN1 STP BPDUs se envían a la dirección MAC de IEEE STP (0180.c200.0000), sin etiqueta.
- Las VLAN1 STP BPDUs también se envían a la dirección MAC PVST+, sin etiqueta.
- Las BPDU STP que no son VLAN 1 se envían a la dirección MAC PVST+ (también denominada dirección MAC de protocolo de árbol de extensión compartido (SSTP), 0100.0ccc.cccd), etiquetada con una etiqueta IEEE 802.1Q VLAN correspondiente.

Si la VLAN nativa en un trunk IEEE 802.1Q no es VLAN1:

- Las VLAN1 STP BPDUs se envían a la dirección MAC PVST+, marcada con la etiqueta con una etiqueta IEEE 802.1Q VLAN correspondiente.
- Las VLAN1 STP BPDUs también se envían a la dirección MAC IEEE STP en la VLAN nativa del trunk IEEE 802.1Q, sin etiqueta.
- Las STP BPDUs que no son VLAN 1 se envían a la dirección MAC PVST+, marcada con una etiqueta IEEE 802.1Q VLAN correspondiente.



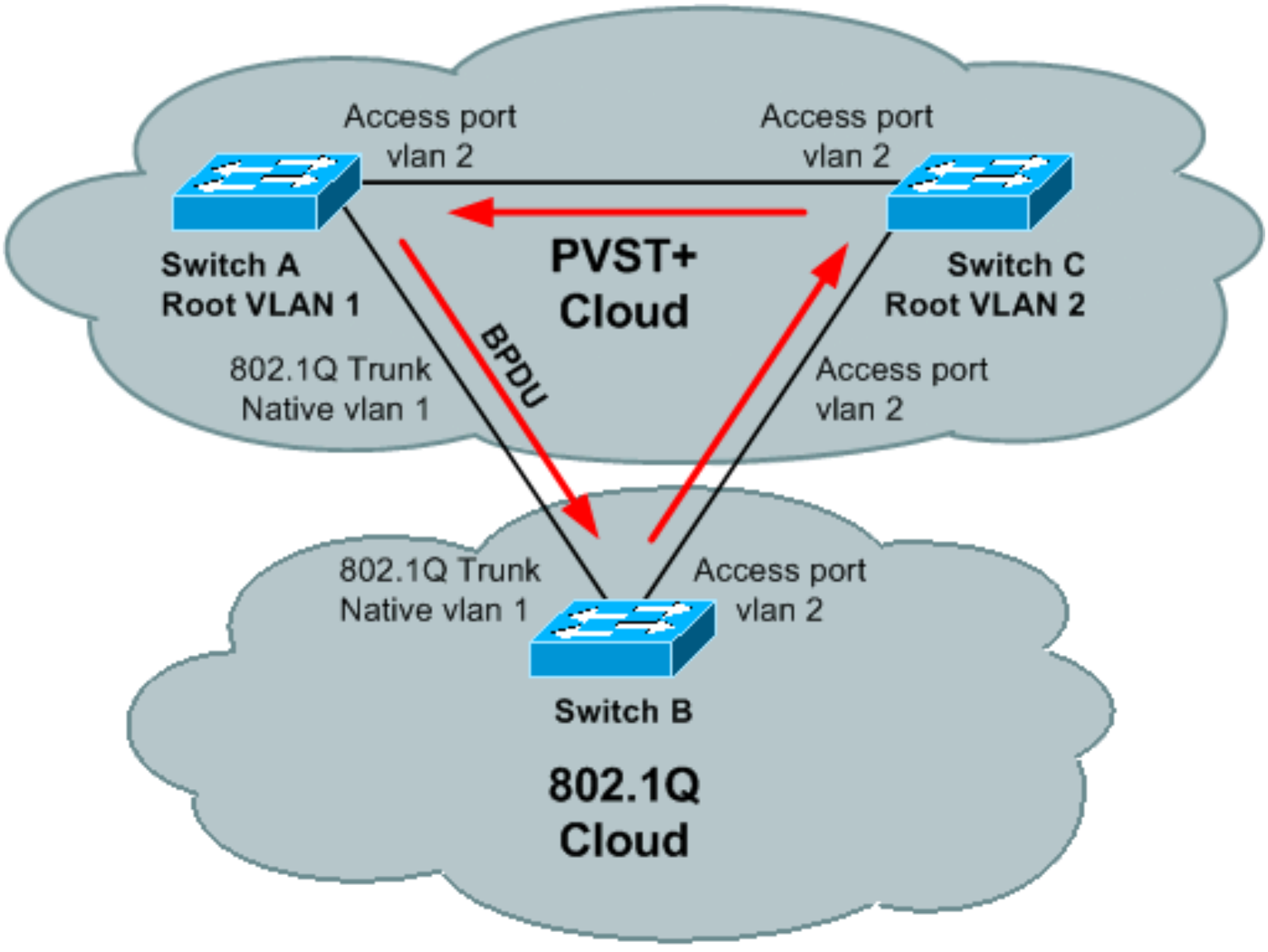
Nota: Las BPDU STP de VLAN nativa se envían sin etiqueta.

Así, la VLAN1 STP del PVST+ se combina con el STP de IEEE 802.1D o 802.1Q, mientras que otras VLANs son tuneladas a través de la nube IEEE 802.1D o los bridges 802.1Q. Por ejemplo, la nube IEEE 802.1D o 802.1Q parece similar a un “cable” conectado a PVST+ VLANs diferentes de 1.

Para que el STP funcione correctamente, observe ciertas reglas cuando conecta los bridges PVST+ con el IEEE 802.1D o los bridges 802.1Q. La regla principal es que los bridges PVST+ deben conectarse con los bridges IEEE 802.1D o 802.1Q a través de un trunk del IEEE 802.1Q con una VLAN nativa constante en todos los bridges que se conectan con la nube de los bridges IEEE 802.1Q o 802.1D.

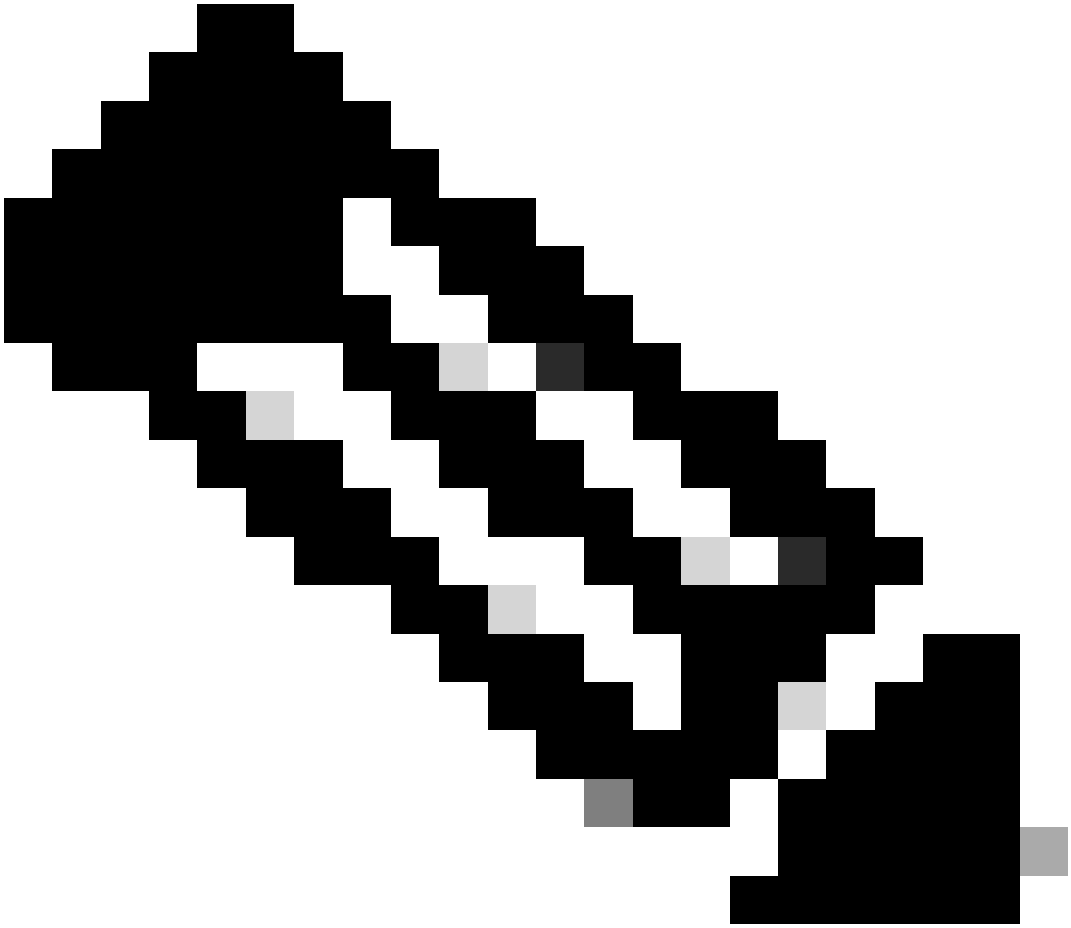
La PVST+ BPDU contiene un número VLAN que permite que los bridges PVST+ detecten si la regla anterior no se respetó. Cuando un switch Catalyst detecta una configuración incorrecta, los puertos correspondientes se colocan en estado “ incoherencia PVID” o “incoherencia de tipo”, que bloquea con eficacia el tráfico en la VLAN correspondiente en un puerto adecuado. Estos estados evitan los loops de reenvío causados por una configuración incorrecta o por un mal cableado.

Para ilustrar la necesidad de la detección de inconsistencias, considere esta topología, donde los switches A y C ejecutan PVST+ STP y el switch B ejecuta 802.1Q STP:



Si la BPDU de la raíz en la VLAN1 es mejor que la BPDU de la raíz en la VLAN2, no hay ningún puerto de bloqueo en la topología VLAN2. La BPDU de VLAN 2 nunca hace un "círculo completo" alrededor de la topología; es reemplazada por la BPDU de VLAN 1 en el link B-C, porque B ejecuta solamente un STP fusionado con el STP VLAN 1 de PVST+. Por lo tanto, hay un loop de reenvío. Afortunadamente, el switch A envía PVST+ BPDU de VLAN 2 (a la dirección SSTP que se inunda por el switch B) hacia el switch C. El switch C puede poner el puerto C-B en un estado

inconsistente con el tipo, lo que evita el loop.

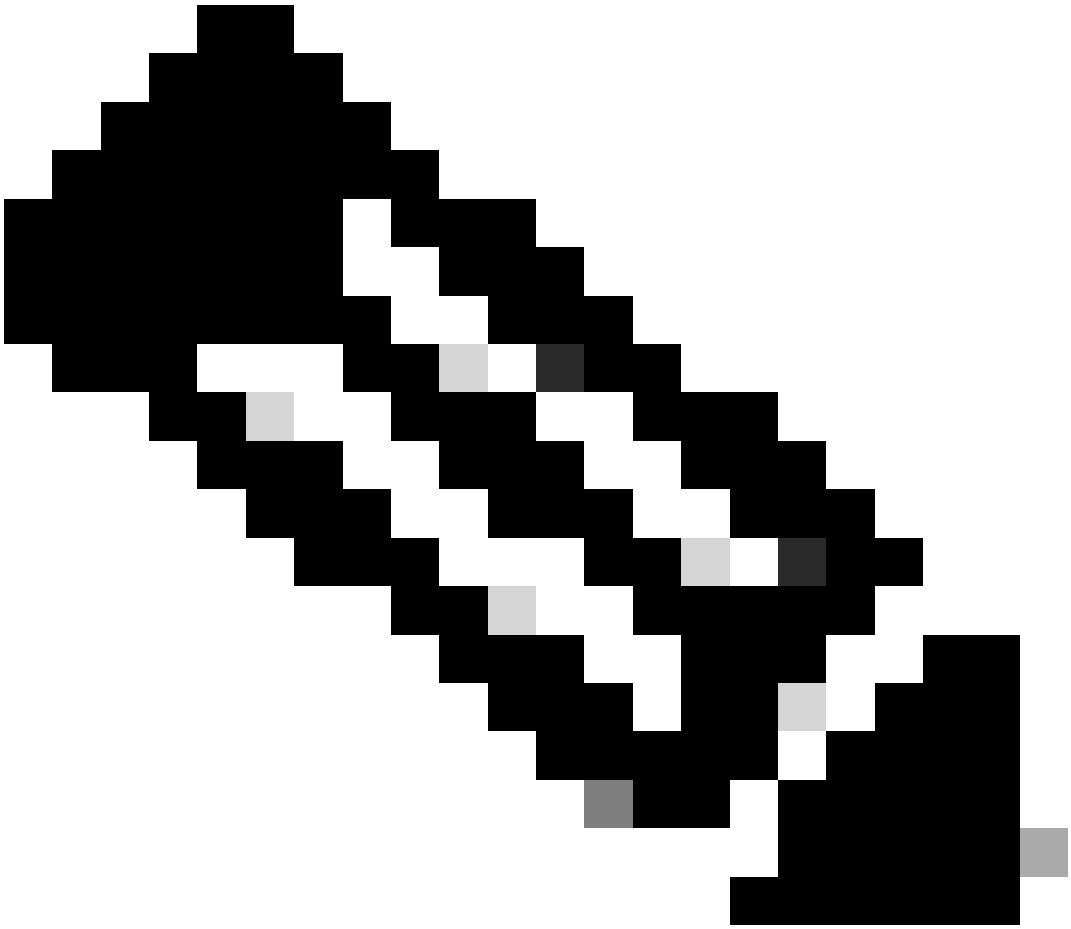


Nota: En algunos resultados de comandos, el estado STP *-inconsistent se denomina "roto".

Cuando se detecta la incoherencia de STP, los switches envían estos mensajes 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
```

En ese ejemplo, la VLAN1 es el sitio en el que la BPDU fue recibida, y la VLAN10 es el sitio en el que la BPDU fue originada. Cuando se detecta la incoherencia, ambas VLANs se bloquean en el puerto en donde se recibe esta BPDU.



Nota: Los mensajes pueden variar según el tipo y la versión de la versión del software Cisco IOS® que se esté utilizando.

Observe que si el puerto ya no recibe BPDU inconsistentes, el estado *-inconsistent se borra y el STP cambia el estado del puerto en función del funcionamiento normal del STP. Se envía un mensaje de syslog para indicar el cambio:

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

Para obtener más detalles sobre el funcionamiento de PVST+, consulte Ejemplo de Configuración

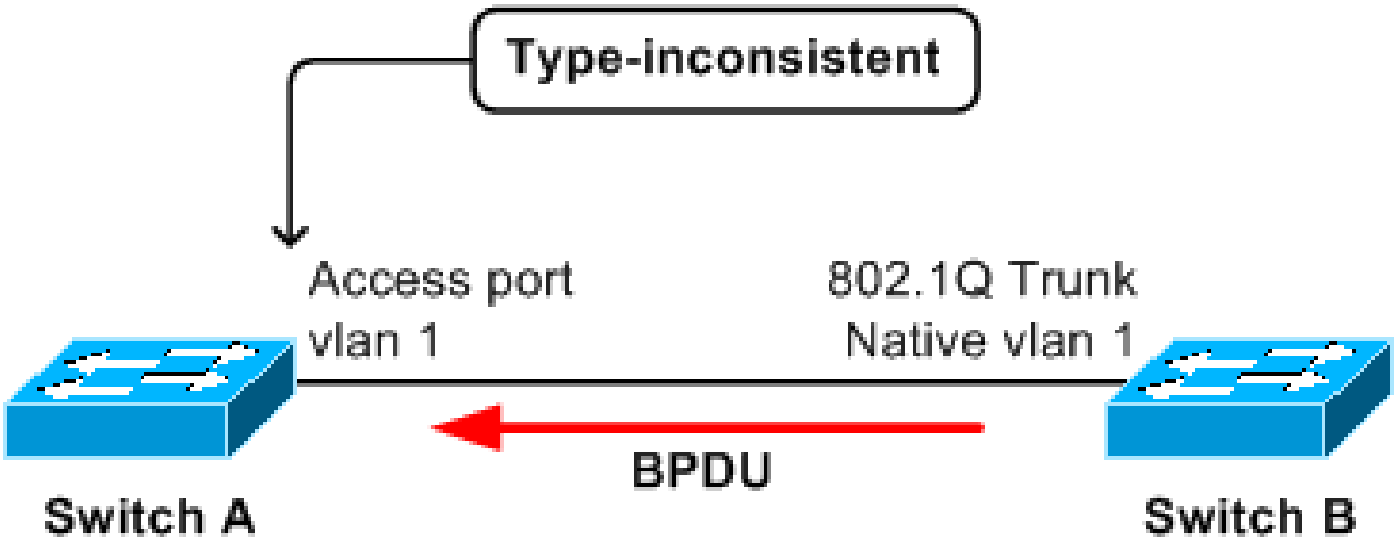
de Spanning Tree desde PVST+ a Rapid-PVST Migration.

Troubleshoot

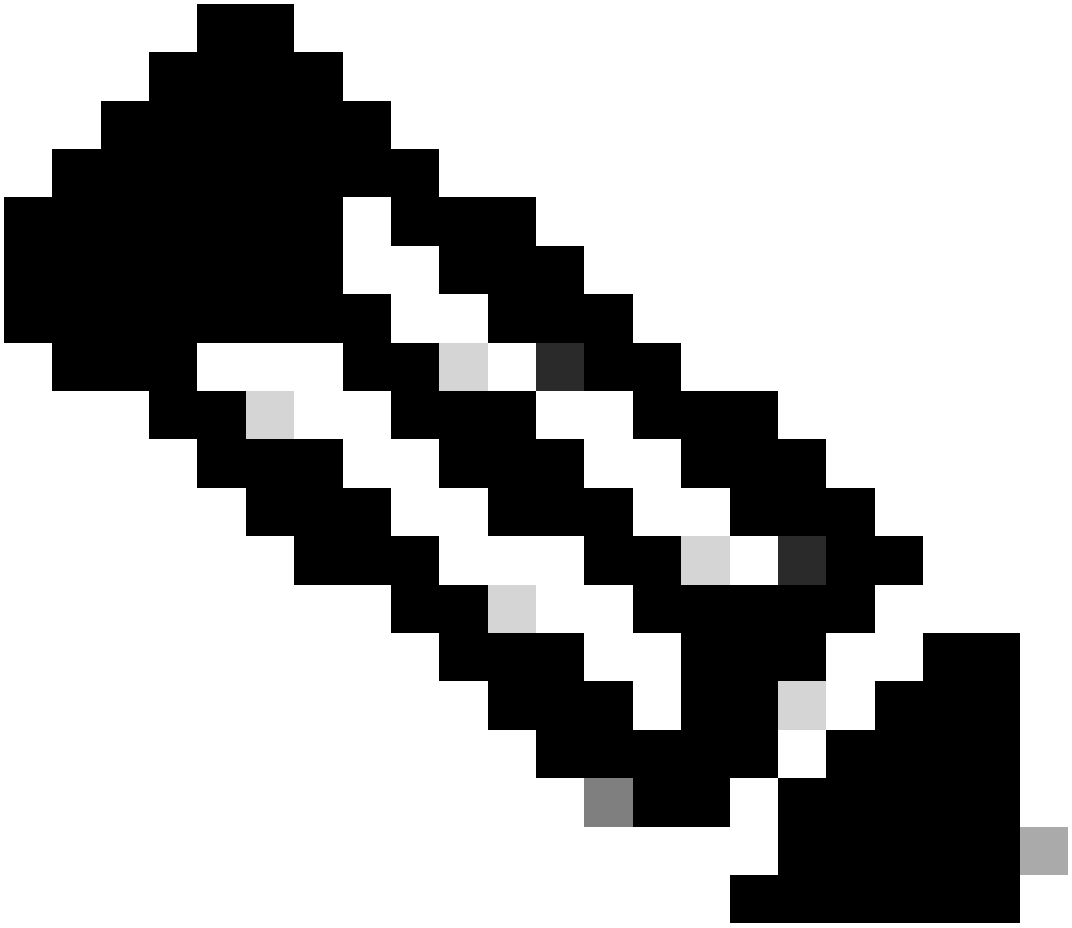
Para ver la lista de puertos incoherentes, la implementación de STP basada en IOS reciente de Cisco soporta el comando show spanning-tree inconsistentports.

En la mayoría de los casos, la razón de la detección de la incoherencia de STP en el puerto es evidente:

- El puerto de acceso recibe una SSTP BPDU etiquetada con IEEE 802.1Q.

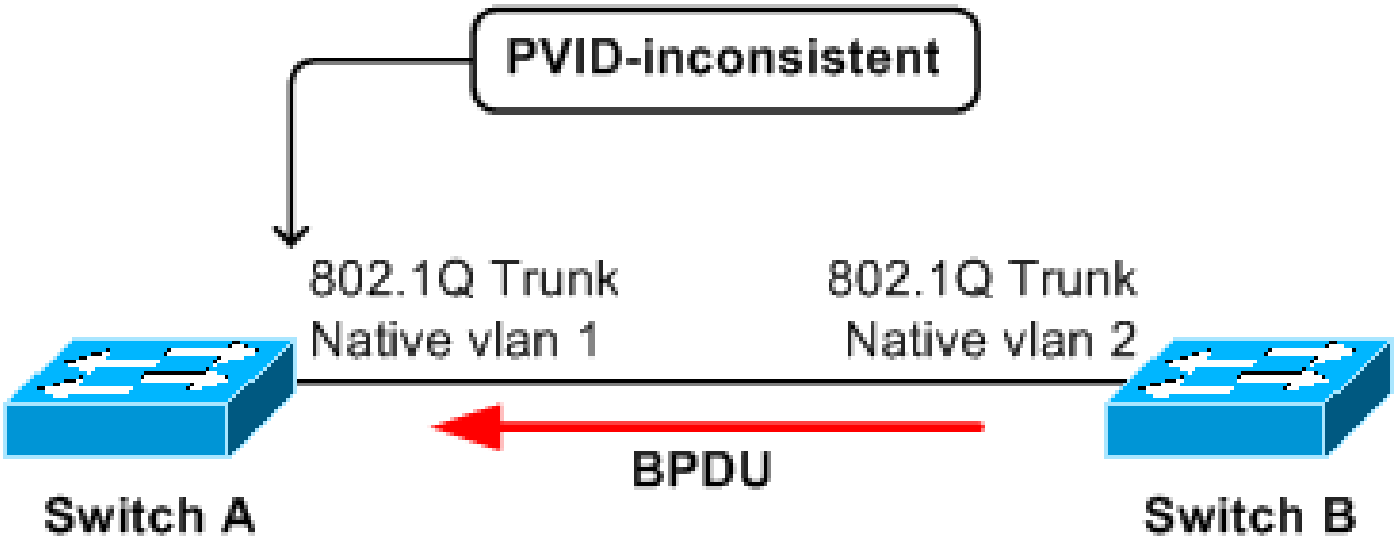


En este escenario, el puerto de acceso en el bridge A recibe, del bridge B, una PVST+ BPDU etiquetada desde el STP de una VLAN diferente de 1. El puerto en A se puede poner en estado de incoherencia de tipo.



Nota: No es necesario conectar los switches directamente; si están conectados a través de uno o más switches IEEE 802.1D o IEEE 802.1Q (o incluso hubs), el efecto es el mismo.

- El puerto de trunking IEEE 802.1Q recibe una SSTP BPDU sin etiqueta con una VLAN de tipo, longitud, valor (TLV) que no corresponde con la VLAN donde la BPDU fue recibida.



En este escenario, el puerto trunk en A recibe una PVST+ BPDU desde el STP de la VLAN2 con una etiqueta de VLAN2. Esto acciona el puerto en A que se bloqueará en la VLAN1 y la VLAN2.

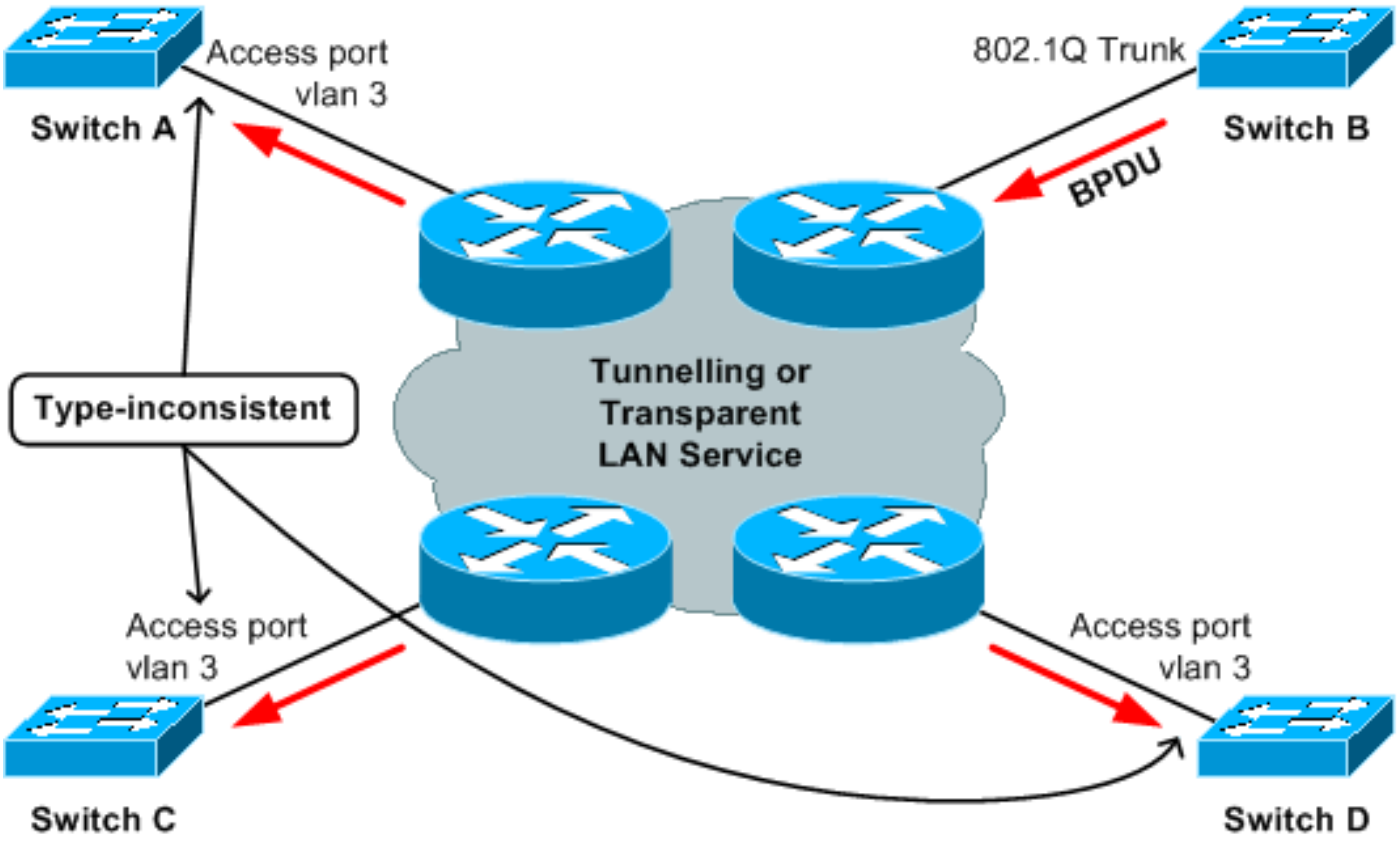
Si los dispositivos en ambos extremos de un link punto a punto son switches de Cisco Catalyst, un examen de la configuración del puerto local y remoto revela habitualmente la discrepancia de configuración:

- El puerto se configura para el trunking IEEE 802.1Q en un lado pero el otro lado es puerto de acceso.
- Los troncos IEEE 802.1Q están en ambos lados, pero las VLAN nativas son diferentes.

En estos casos, repare la discrepancia de configuración para resolver la incoherencia de STP.

En algunos casos, es más difícil identificar la razón:

- Una BPDU se recibe de un medio compartido con dispositivos múltiples.
- Se recibe una BPDU, de la nube del switch, que implementa un IEEE 802.1D o el modelo 802.1Q STP mientras que los switches PVST+ están conectados con la nube.
- Una BPDU proviene de la parte posterior de un túnel (por ejemplo, nube Data Link Switch Plus [DLSw+], tunelización de protocolo L2, EoMPLS, Links de Trayectoria Virtual [VPLs] LAN Emulation [[LANE] y otros).



En este ejemplo, el switch B se configura de forma incorrecta e inserta una SSTP BPDU en la nube. Esto hace que los puertos en los switches A, C, y D presenten una incoherencia de tipo. El problema es que el dispositivo que origina la BPDU “infractora” no está conectado directamente con los switches afectados. Por lo tanto, con muchos dispositivos en el troncal, puede consumir tiempo resolver todos ellos.

Afortunadamente, hay un enfoque sistemático para resolver problemas en estos casos:

1. Establezca la dirección MAC de origen y el ID de puente de envío de la BPDU. Esto debe hacerse mientras se produce el problema

2. Busque el bridge que origina la BPDU “infractora”. Esto se puede hacer después de un tiempo, no necesariamente cuando ocurre el problema.

Para el Paso 1, normalmente hay dos opciones: utilizar un analizador de paquetes o habilitar debug para ver el volcado de las BPDU recibidas.

Para obtener más detalles sobre el uso de una depuración para volcar STP BPDU, consulte la sección Uso de Comandos de Debug STP de Resolución de Problemas de STP en Switches Catalyst.

Éste es un ejemplo de salida de debug que muestra la BPDU recibida:

```
*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
```

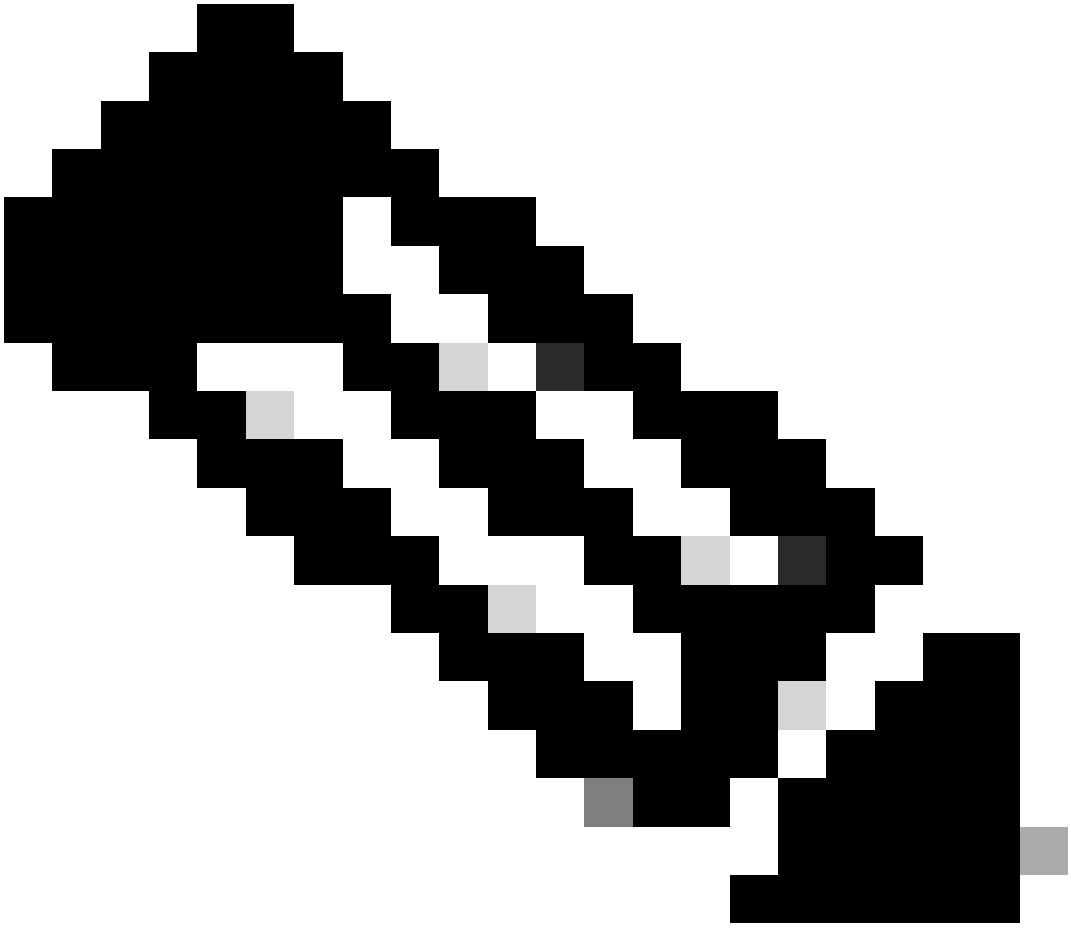
```
*Mar 14 19:33:27:     B:8000 0050.0f2d.4000 80.99 A:0000 M:1400 H:0200 F:0F00
*Mar 14 19:33:27:     T:0000 L:0002 D:0001
```

Una vez que conozca la dirección MAC de origen y la ID del bridge del envío, debe buscar el dispositivo al cual pertenece esta dirección MAC. Esto se puede complicar por el hecho de que los switches típicamente no conocen las direcciones MAC de origen de las tramas BPDU. Si ejecuta el comando show mac-address-table addressBPDU_mac_address (para los switches basados en Cisco IOS), normalmente no se encuentra ninguna entrada.

Una manera de encontrar la dirección MAC "infractora" es recopilar, de todos los switches que están conectados a la nube, la salida del comando show spanning-tree. Los resultados de estos comandos incluyen información acerca del ID de puente de cada puente.

<#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.
```



Nota: Según el modelo, la versión del software y la configuración, un switch puede tener varias direcciones MAC de ID de puente. Afortunadamente, todas las direcciones pueden estar normalmente en un rango determinado (por ejemplo, de 0001.1234.5600 a 0001.1234.5640). Si conoce una dirección MAC de ID de puente, puede verificar si la dirección MAC de ID de puente enviada (que se encuentra en el paso 1) se encuentra dentro del rango de direcciones MAC de ID de puente dadas. Puede también utilizar las herramientas de administración de red para recoger las IDs de todos los bridges.

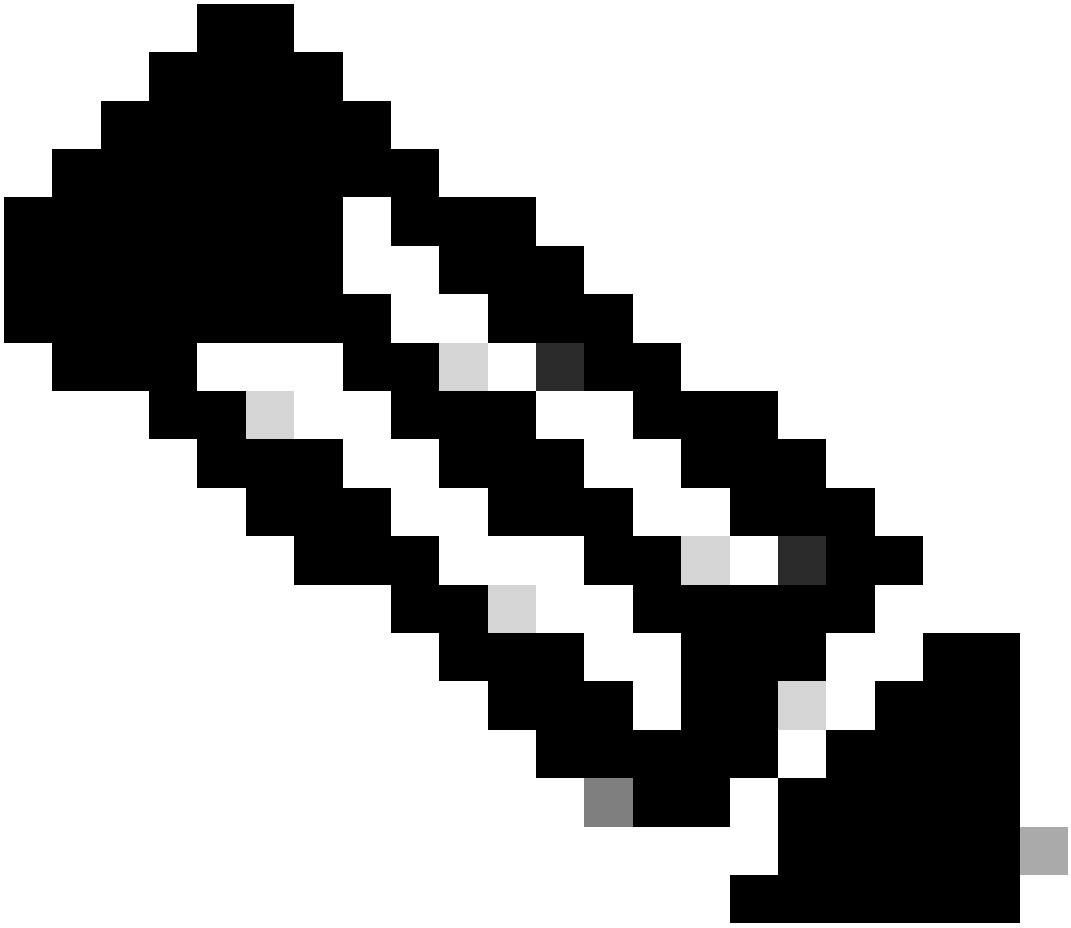
Una vez que haya encontrado el puente que ha enviado la BPDU infractora, debe verificar la configuración del puerto que está conectado a la nube: asegúrese de que sea coherente (conexión troncal en lugar de conexión troncal y VLAN nativa) con otros switches que también están conectados a la misma nube.

Podría suceder que el puente envíe las BPDU adecuadas, pero se modifican incorrectamente dentro de la nube de tunelización. En ese caso, puede ver que la BPDU infractora que ingresa a la nube es consistente con la configuración de los otros puentes, pero la misma BPDU se vuelve inconsistente cuando sale de la nube (por ejemplo, la BPDU sale de la nube en una VLAN

diferente, o se etiqueta o no se etiqueta). En tal caso, puede ayudar a verificar si la dirección MAC de origen de la BPDU infractora pertenece al mismo puente que el ID del puente de envío. Si este no es el caso, puede intentar localizar el puente que posee la dirección MAC de origen de la BPDU y verificar su configuración.

Para localizar el switch que posee la dirección MAC de origen de la BPDU, puede utilizar el mismo enfoque (para encontrar el ID de puente), excepto que ahora se inspecciona el resultado del comando show module (para Catalyst 4000 y 6000). Para otros switches Catalyst, puede examinar la salida del comando show interface para ver las direcciones MAC que pertenecen a los puertos.

```
<#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.
```



Nota: Si la nube es DLSw+, consulte Comprensión y configuración de DLSw y 802.1Q

Información Relacionada

- Soporte de productos de protocolo de árbol de extensión/LAN
- Soporte de la Tecnología
- Soporte técnico y descargas de Cisco

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

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

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