Solución de problemas de STP y consideraciones de diseño relacionadas

Contenido

Introducción

Este documento describe las recomendaciones para implementar una red segura sobre la conexión en puente de switches Cisco Catalyst que ejecutan Catalyst OS/Cisco IOS® Software.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y 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.

Antecedentes

Este documento explica algunas de las razones comunes por las que puede fallar Spanning Tree Protocol (STP) y la información que debe examinar para identificar el origen del problema. También muestra el tipo de diseño que minimiza los problemas relacionados con el spanning tree y es fácil de resolver.

Este documento no hace referencia al funcionamiento básico de STP. Para obtener información acerca de cómo funciona STP, consulte este documento:

- Introducción y Configuración del Spanning Tree Protocol (STP) en los Switches Catalyst

Este documento no analiza el STP rápido (RSTP) definido en la norma IEEE 802.1w. Además, este documento no analiza el protocolo de árbol de expansión múltiple (MST), definido en la norma IEEE 802.1s. Para obtener más información sobre RSTP y MST, consulte estos documentos:

- Introducción al Protocolo Rapid Spanning Tree Protocol [protocolo de árbol de expansión rápida] (802.1s)
- Introducción al Rapid Spanning Tree Protocol [protocolo de árbol de expansión rápida] (802.1w)

Para obtener un documento de solución de problemas de STP más específico para los switches

Catalyst que ejecutan software Cisco IOS, consulte el documento Solución de problemas de STP en el switch Catalyst que ejecuta Cisco IOS integrado (modo nativo).

Falla del protocolo de árbol de expansión

La función primaria del algoritmo del árbol de expansión (STA) es cortar los bucles creados por enlaces redundantes en redes con conexión en puente. El STP opera en la capa 2 del modelo de Interconexión de sistemas abiertos (OSI). Por medio de unidades de datos de protocolo puente (BPDU) que intercambian entre puentes, el STP elige los puertos que finalmente reenvían o bloquean el tráfico. Este protocolo puede fallar en algunos casos específicos, y para resolver la situación que los resultados pueden ser muy difíciles, que depende del diseño de la red. En esta área concreta, debe realizar la parte más importante del proceso de solución de problemas antes de que se produzca el problema.

Un error en el STA lleva, por lo general, a un bucle de conexión en puente. La mayoría de los clientes que llama a Cisco Technical Support por problemas de árbol de expansión sospecha que se ha producido un error, pero rara vez la causa es un error. Incluso si el problema es el software, un loop de conexión en puente en un entorno STP aún proviene de un puerto que puede bloquear, pero en cambio reenvía el tráfico.

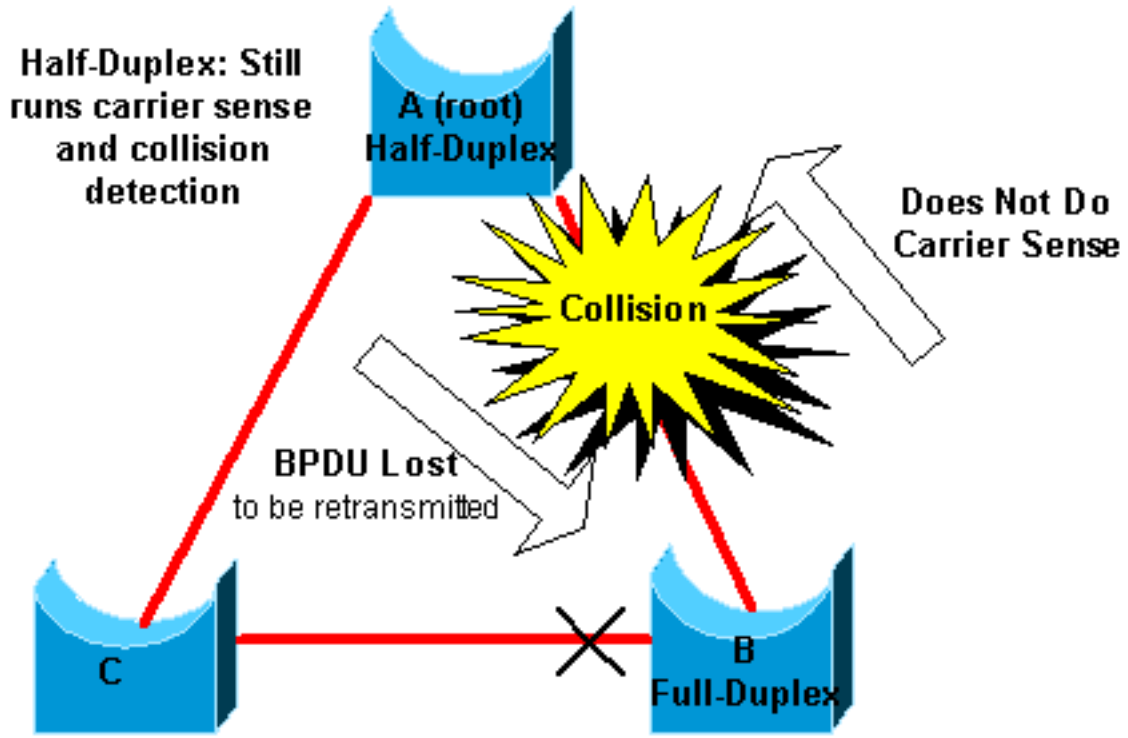
Convergencia del árbol de expansión

Consulte el video del árbol de expansión para ver un ejemplo que explica cómo el árbol de expansión converge inicialmente. En el ejemplo también se explica por qué un puerto bloqueado entra en el modo de reenvío a puerto asignado debido a una pérdida excesiva de BPDU, lo que genera una falla en el STA.

El resto de este documento enumera las diferentes situaciones que pueden causar un error en el STA. La mayoría de estos errores está relacionada con una pérdida masiva de BPDU. La pérdida ocasiona el bloqueo de puertos para la transición al modo de reenvío.

discordancia dúplex

La discordancia dúplex en un enlace punto a punto es un error de configuración muy habitual Si establece manualmente el modo dúplex en Completo en un lado del enlace y deja el otro lado en el modo de autonegociación, el enlace termina en semidúplex. (Un puerto configurado con modo dúplex completo ya no negocia.)



El peor de los casos se produce cuando un puente que envía BPDU tiene el modo dúplex configurado en semidúplex en un puerto, pero el puerto par en otro extremo del enlace tiene el modo dúplex configurado en dúplex completo. En el ejemplo anterior, la discordancia dúplex en el link entre el puente A y B puede conducir fácilmente a un loop de conexión en puente. Dado que el puente B tiene una configuración de dúplex completo, no lleva a cabo la detección de la portadora antes de acceder al enlace. El puente B comienza a enviar tramas incluso si el puente A ya utiliza el link. Esta situación es un problema para A; el bridge A detecta una colisión y ejecuta el algoritmo de backoff antes de que el bridge intente otra transmisión de la trama. Si hay suficiente tráfico de B a A, cada paquete que envía A, que incluye las BPDU, se somete a un aplazamiento o colisión y, finalmente, se elimina. Desde el punto de vista de un STP, dado que el puente B no recibe más BPDU desde A, el puente B perdió el puente de ruta. Esto hace que B desbloquee el puerto conectado al puente C, y crea el bucle.

Siempre que haya una discrepancia de dúplex, se ven estos mensajes de error en las consolas de los switches Catalyst que ejecutan el software Cisco IOS y CatOS:

CatOS

```
CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on port [mod]/[port]
```

Cisco IOS Software

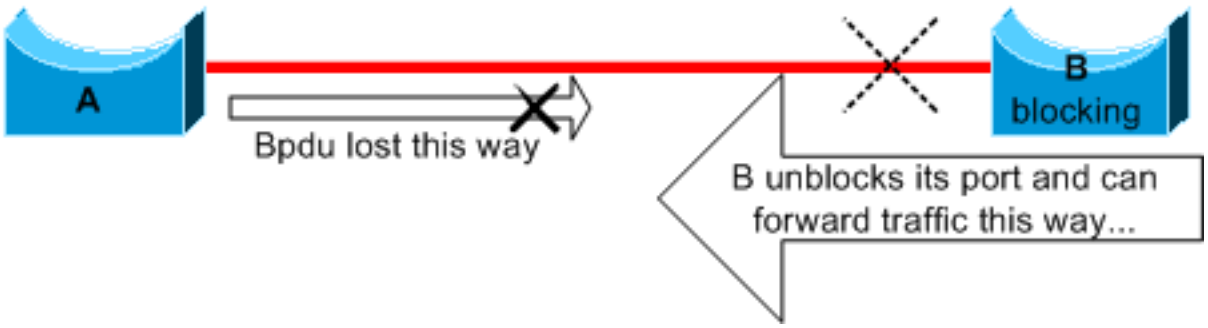
```
%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet5/1 (not half
duplex), with TBA05071417(Cat6K-B) 4/1 (half duplex).
```

Verifique la configuración de dúplex y, si no coincide, configúrela correctamente.

Para obtener más información sobre cómo solucionar los problemas de discrepancia de dúplex, consulte el documento Configuración y solución de problemas de autonegociación de dúplex completo/semidúplex de Ethernet 10/100/1000 MB.

link unidireccional

Los links unidireccionales son una causa común del loop de conexión en puente. En los enlace de fibra, un error no detectado suele ocasionar enlaces unidireccionales. También puede provocar un problema con un transceptor. Todo lo que haga que un enlace se mantenga activo mientras suministra comunicación unidireccional es muy peligroso en lo que concierne a STP. El siguiente ejemplo puede aclararlo:



En este caso, suponga que el enlace entre A y B es unidireccional. El enlace elimina el tráfico de A a B, mientras transmite el tráfico de B a A. Supongamos que el puente B se bloqueó antes de que el enlace se vuelva unidireccional. Sin embargo, un puerto solo puede bloquear si recibe BPDU desde un puente con una prioridad superior. Dado que, en este caso, se pierden todas las BPDU que provienen de A, el puente B finalmente realiza la transición de su puerto hacia A al estado de reenvío y reenvía el tráfico. De esta forma, se crea un bucle. Si la falla se produce en el inicio, el STP no converge correctamente. En el caso de una discordancia dúplex, un reinicio ayuda temporalmente; pero en este caso, un reinicio de los puentes no tiene absolutamente ningún efecto.

Cisco diseñó e implementó el protocolo de detección de enlace unidirección (UDLD) para detectar los enlaces unidireccionales antes de crear el bucle de reenvío. Esta función puede detectar cableado incorrecto o enlaces unidireccionales en la capa 2 e interrumpir automáticamente los bucles resultantes al deshabilitar algunos puertos. Ejecute UDLD siempre que sea posible en un entorno de puente.

Para obtener más información sobre el uso de UDLD, consulte el documento Comprensión y configuración de la función del protocolo de detección de enlaces unidireccionales.

Corrupción de paquetes

La corrupción del paquete también puede conducir a la misma clase de falla. Si un enlace tiene una gran cantidad de errores físicos, puede perder una determinada cantidad de BPDU consecutivas. Esta pérdida puede hacer que un puerto de bloqueo cambie al estado de reenvío. Este caso no se ve con mucha frecuencia porque los parámetros STP predeterminados son muy conservadores. El puerto de bloqueo debe perder BPDU por 50 segundos antes de la transición al reenvío. La transmisión exitosa de una sola BPDU interrumpe el bucle. Este caso ocurre habitualmente cuando los parámetros de STP se han ajustado de forma descuidada. Un ejemplo de ajuste es la reducción de la duración máxima.

La discordancia de dúplex, los cables defectuosos o la longitud incorrecta de los cables pueden provocar el daño de los paquetes. Consulte el documento Solución de problemas del puerto para switch y la interfaz para obtener una explicación de la salida del contador de errores del software CatOS y Cisco IOS.

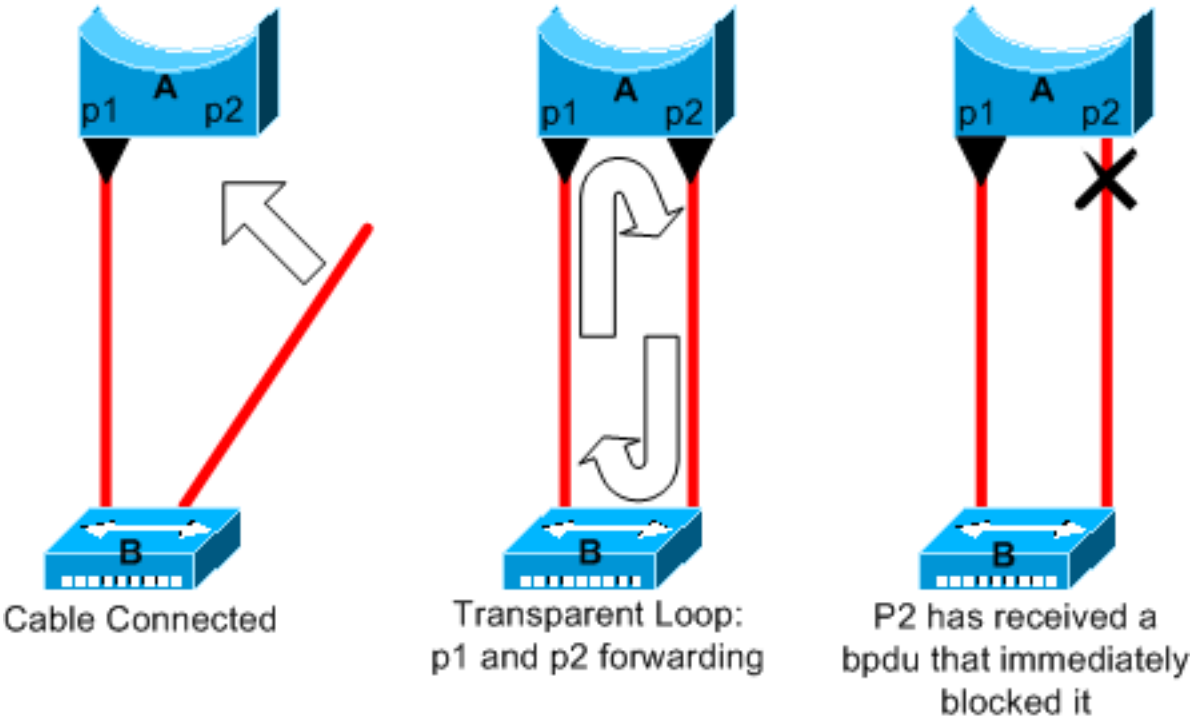
Errores de recurso

El STP se implementa en el software, aun en los switches de alta gama que realizan la mayoría de las funciones de switch en el hardware mediante circuitos integrados de aplicación específica (ASIC). Si por cualquier motivo, hay un uso excesivo de la CPU del puente, es posible que los recursos sean inadecuados para la transmisión de BPDU. El STA generalmente no hace un uso intensivo del procesador y tiene prioridad sobre otros procesos. En la sección Búsqueda de errores de recursos de este documento, se proporcionan algunas pautas sobre la cantidad de instancias de STP que una plataforma específica puede gestionar.

Error de configuración de PortFast

PortFast es una función que típicamente desea habilitar únicamente para un puerto o interfaz que se conecta a un host. Cuando el enlace se presenta en este puerto, el puente omite las primeras etapas del STA, y pasa directamente al modo de reenvío.

> **Precaución**: no utilice la función PortFast en puertos de switch o interfaces que se conectan a otros switches, hubs o routers. De lo contrario, puede crear un bucle de red.



En este ejemplo, el dispositivo A es un puente con un puerto p1 que ya reenvía. El puerto p2 tiene una configuración para PortFast. El dispositivo B es un concentrador. Tan pronto como enchufe el segundo cable en A, el puerto p2 pasa al modo de reenvío y crea un bucle entre p1 y p2. Este bucle se detiene apenas p1 o p2 reciben una BPDU que coloca uno de estos dos puertos en modo de bloqueo. Pero hay un problema con este tipo de bucle transitorio. Si el tráfico de bucle es muy intenso, es probable que el puente pueda tener problemas para transmitir exitosamente la BPDU que detiene el bucle. Este problema puede retrasar la convergencia de manera considerable o, en casos extremos, hacer que la red se caiga.

Para obtener más información sobre el uso correcto de PortFast en los switches que ejecutan el software CatOS y Cisco IOS, consulte el documento Uso de PortFast y otros comandos para resolver retrasos en la conectividad de inicio de la estación de trabajo.

Incluso con la configuración de PortFast, el puerto o la interfaz aún participan en STP. Si un switch con una prioridad de puente inferior a la del puente de ruta activo actual se conecta a un puerto o una interfaz configurados para PortFast, se puede seleccionar como puente de ruta. Este cambio de puente de ruta puede afectar negativamente la topología STP activa y hacer que la red esté por debajo de los valores óptimos. Para evitar que se produzca esta situación, la mayoría de switches Catalyst que ejecutan el software CatOS y Cisco IOS disponen de una función denominada Protección BPDU. La protección de BPDU deshabilita un puerto o una interfaz configurados para PortFast si el puerto o la interfaz reciben una BPDU.

Para obtener más información sobre el uso de la función de protección de BPDU en los switches que ejecutan el software CatOS y Cisco IOS, consulte el documento Mejora de la protección de BPDU de Portfast del árbol de expansión.

Ajuste complicado de parámetros STP y problemas de diámetro

Un valor radical para el parámetro de duración máxima y el retraso de reenvío puede generar una topología de STP muy inestable. En estos casos, la pérdida de algunas BPDU puede causar la aparición de un bucle. Otro problema, no muy conocido, está relacionado con el diámetro de la red puente. Los valores predeterminados conservadores para los temporizadores de STP imponen un diámetro de red máximo de siete. El máximo diámetro de red limita la distancia posible entre los puentes de la red. En este caso, dos puentes distintos no deben estar a más de siete saltos de distancia. Parte de esta restricción proviene del campo de edad que tiene BPDU.

Cuando una BPDU se propaga del puente de ruta hacia las hojas del árbol, el campo de duración aumenta cada vez que la BPDU atraviesa un puente. Finalmente, el puente descarta la BPDU cuando el campo de duración supera la duración máxima. Si la raíz está demasiado lejos de algunos puentes de la red, puede haber problemas. Este problema afecta a la convergencia del árbol de expansión.

Por lo tanto, preste especial atención si va a cambiar los valores predeterminados de los temporizadores STP. No hay peligro si intenta obtener una reconvergencia más rápida de esta manera. Un cambio en el temporizador STP afecta al diámetro de la red y a la estabilidad del STP. Puede cambiar la prioridad del puente para seleccionar el puente de ruta y cambiar el parámetro de prioridad o costo de puerto para controlar la redundancia y el balance de carga.

El software Cisco Catalyst le brinda macros que ajustan los parámetros de STP más importantes para usted:

- **set spantree root [secondary]** el comando macro disminuye la prioridad de bridge para que se convierta en root (o root alternativo). Una opción opcional para este comando consiste en el ajuste de los temporizadores STP mediante la especificación del diámetro de red. Incluso cuando se realiza correctamente, el ajuste del temporizador no mejora significativamente el tiempo de convergencia e introduce algunos riesgos de inestabilidad en la red. Además, este tipo de ajuste debe actualizarse cada vez que se agrega un dispositivo a la red. Mantenga los valores predeterminados conservadores, que son conocidos por los ingenieros en redes.
- **set spantree uplinkfast** para CatOS o el **spanning-tree uplinkfast** para el software Cisco IOS aumenta la prioridad del switch de modo que el switch no pueda ser root. El comando aumenta el tiempo de convergencia de STP en el caso de error del enlace ascendente. Use este comando en un switch de distribución con conexión dual con switches de núcleo. Consulte el documento Comprensión y configuración de la función UplinkFast de Cisco.
- **set spantree backbonefast enable** para CatOS o el **spanning-tree backbonefast** para el software Cisco

IOS puede aumentar el tiempo de convergencia STP del switch en caso de una falla de link indirecto. BackboneFast es una función patentada de Cisco. Consulte el documento Comprensión y configuración de Backbone Fast en switches Catalyst.

Para obtener más información sobre los temporizadores de STP y las reglas para ajustarlos cuando sea absolutamente necesario, consulte el documento Comprensión y ajuste de los temporizadores de protocolo de árbol de expansión.

Errores de software

Como se mencionó en la Introducción, el STP es una de las primeras funciones que se implementaron en los productos de Cisco. Por lo general, esta característica es muy estable. Sólo la interacción con funciones más recientes, como EtherChannel, ha provocado que el STP falle en algunos casos muy específicos que ya se trataron. Diversos factores pueden causar un error de software y esto pueden tener diferentes efectos. No hay un modo de describir adecuadamente los problemas que puede causar un error. La situación más peligrosa que surge de los errores de software es si ignora algunas BPDU o si tiene una transición de puerto de bloqueo a reenvío.

Resolución de problemas de falla

Desafortunadamente, no hay ningún procedimiento sistemático para solucionar un problema de STP. Sin embargo, en esta sección se resumen algunas de las acciones que están a su disposición. La mayoría de los pasos descritos en esta sección se aplican a la resolución de problemas de bucles de conexión en puente en general. Puede utilizar un método más convencional para identificar otros errores del STP que llevan a la pérdida de conectividad. Por ejemplo, puede explorar el trayecto que toma el tráfico cuando se encuentra con un problema.

> **Nota**: La mayoría de estos pasos para resolver problemas asumen conectividad con los diferentes dispositivos de la red puente. Esta conectividad significa que tiene acceso a la consola. Por ejemplo, durante un loop de conexión en puente probablemente no pueda realizar una conexión Telnet.

Si tiene el resultado de un **show-tech support** desde su dispositivo Cisco, puede utilizar Cisco CLI Analyzer (sólo para clientes registrados) para mostrar posibles problemas y soluciones.

Utilice el diagrama de la red

Antes de solucionar un bucle de conexión en puente, como mínimo debe conocer estos elementos:

- La topología de la red conectada en puente
- La ubicación del puente de ruta
- La ubicación de los puertos bloqueados y los enlaces redundantes

Estos conocimientos son esenciales por lo menos por estas dos razones:

- Para saber qué se debe reparar en la red, debe saber cómo se ve la red cuando funciona correctamente.
- La mayoría de los pasos para solucionar problemas se limitan a **show** comandos para intentar identificar condiciones de error. Tener conocimientos sobre la red lo ayuda a concentrarse en

los puertos críticos de los principales dispositivos.

Identificación de una conexión en puente

Antes, solía ocurrir que una tormenta de difusión podía tener un efecto desastroso en la red. En la actualidad, con los dispositivos y los enlaces de alta velocidad, que permiten la conmutación en el nivel de hardware, no es probable que un solo host, por ejemplo, un servidor, desactive una red a través de difusiones. La mejor manera de identificar un bucle de conexión en puente es capturar el tráfico en un enlace saturado y verificar que se vean paquetes similares varias veces. Sin embargo, para ser realista, si todos los usuarios en un dominio de puente determinado tienen problemas de conectividad al mismo tiempo, ya puede sospechar que hay un bucle de conexión en puente.

Verifique la utilización de los puertos de sus dispositivos y busque valores anormales. Consulte la sección Verificar uso de puertos de este documento.

En los switches Catalyst que ejecutan CatOS, puede verificar fácilmente el uso general de la placa de interconexiones con el **show system** comando. El comando proporciona el uso actual de la placa de circuito del switch y también especifica los picos de uso y la fecha de estos. Un pico de uso inusual le indica si ha habido alguna vez un bucle de conexión en puente en ese dispositivo.

Restaurar rápidamente la conectividad y prepararse para otro momento

Desactive los puertos para interrumpir el bucle

Los bucles de conexión en puente acarrean consecuencias extremadamente graves en una red en puente. En general, los administradores no tienen tiempo para buscar la causa del bucle y prefieren restaurar la conectividad lo antes posible. La salida fácil en este caso es deshabilitar manualmente todos los puertos que proporcionan redundancia en la red. Si puede identificar una parte de la red que se vea más afectada, empiece a deshabilitar puertos en esta área. O, si es posible, inhabilite inicialmente los puertos que pueden estar bloqueando. Cada vez que deshabilite un puerto, verifique si ha restaurado la conectividad en la red. Al identificar el puerto deshabilitado que detiene el bucle, también se identifica la ruta redundante en la que está ubicado el puerto. Si este puerto ha estado bloqueando, probablemente haya encontrado el link en el que apareció la falla.

Registro de eventos STP en dispositivos que alojan puertos bloqueados

Si no puede identificar con precisión el origen del problema, o si el problema es transitorio, habilite el registro de eventos de STP en los puentes y switches de la red que experimenta la falla. Si desea limitar el número de dispositivos a configurar, al menos habilite este registro en los dispositivos que alojan puertos bloqueados; la transición de un puerto bloqueado es lo que crea un loop.

- Cisco IOS Software-Ejecute el comando exec **debug spanning-tree events** para habilitar la información de depuración STP. Ejecute el comando general config mode **logging buffered** para capturar esta información de depuración en los búferes de dispositivos.
- CatOS-The **set logging level spantree 7 default** aumenta el nivel predeterminado de eventos relacionados con STP al nivel de depuración. Asegúrese de registrar un número máximo de mensajes en las memorias intermedias del switch con el uso de la **set logging buffer 500**

comando.

También puede intentar enviar el resultado de la depuración a un dispositivo syslog. Desafortunadamente, cuando se produce un bucle de conexión en puente, pocas veces se mantiene la conectividad con un servidor syslog.

Verificar puertos

Los puertos críticos que deben analizarse primero son los puertos de bloqueo. Aquí se presenta una lista de lo que puede buscar en los distintos puertos, con una descripción rápida de los comandos a ejecutar para switches que ejecutan el software CatOS y Cisco IOS.

Verificación de los puertos bloqueados que reciben BPDU

Especialmente en los puertos bloqueados y en los puertos de ruta, verifique que reciba BPDU de forma periódica. Varios problemas pueden derivar en que un puerto no reciba paquetes o BPDU.

- Cisco IOS Software-In Cisco IOS Software Release 12.0 o posterior, salida del **show spanning-tree bridge-group #** tiene un campo `BPDU`. El campo muestra la cantidad de BPDU recibida para cada interfaz. Ejecute el comando una o dos veces más para determinar si el dispositivo recibe BPDU.Si no tiene el campo `BPDU` en la salida de **show spanning-tree** , puede habilitar la depuración STP con el comando **debug spanning-tree** para verificar la recepción de BPDU.
- CatOS-The **show mac module/port** indica el número de paquetes de multidifusión que recibe un puerto específico. Pero el comando más simple de usar es el **show spantree statistics module#/port# vlan#** comando. Este comando muestra la cantidad exacta de BDPU de configuración recibida por un puerto específico, en una VLAN específica. Un puerto puede pertenecer a varias VLAN, si es troncal. Consulte la sección Un comando de CatOS adicional de este documento.

Comprobación de discordancias dúplex

Para buscar una discordancia de dúplex, debe comprobar cada lado del enlace punto a punto.

- Cisco IOS Software-Ejecute el comando **show interfaces [interface interface-number] status** para verificar la velocidad y el estado dúplex del puerto específico.
- CatOS: las primeras líneas de la salida del **show port module#/port#** le dará la velocidad y el dúplex de acuerdo con la configuración del puerto.

Verificar utilización de puertos

Es posible que una interfaz con una sobrecarga de tráfico no logre transmitir BPDU importantes. Un enlace sobrecargado también es un indicador de un posible bucle de conexión en bridge.

- Software Cisco IOS: utilice el comando **show interfaces** para determinar la utilización en una interfaz. Existen varios campos que lo ayudan en esta determinación, como `carga y entrada/salida de paquetes`. Consulte el documento Resolución de Problemas de Puerto e Interfaz del Switch para obtener una explicación del **show interfaces** resultado del comando.
- CatOS-The **show mac module#/port#** muestra estadísticas sobre los paquetes que un puerto recibe y envía. **show top** evalúa automáticamente la utilización del puerto durante un período de 30 segundos y muestra el resultado. El comando clasifica los resultados según el

porcentaje de uso del ancho de banda, si bien hay otras opciones disponibles para la clasificación de los resultados. Además, el **show system** da una indicación de la utilización de la placa de interconexiones, aunque el comando no apunte a un puerto específico.

Verificar el daño de paquetes

- Cisco IOS Software-Look para incrementos de error en el contador de `errores de entrada` del **show interfaces** comando. Los contadores de errores incluyen fragmentos minúsculos, fragmentos gigantes, sin búfer, CRC, tramas, desbordamiento y recuentos ignorados.Consulte el documento Resolución de Problemas de Puerto e Interfaz del Switch para obtener una explicación del **show interfaces** command output.
- CatOS-El comando **show port module#/port#** proporciona información detallada sobre los campos `Align-Err, FCS-Err, Xmit-Err, Rcv-Err` y `Undersize`. **show counters module#/port#** proporciona estadísticas con aún más detalle.

Comando de CatOS adicional

El comando **show spantree statistics module#/port# vlan#** proporciona información muy precisa acerca de un puerto específico. Ejecute este comando en los puertos que crea oportunos y preste especial atención a estos campos:

- `Forward trans count: Este contador registra cuántas veces el puerto pasa de aprendizaje a reenvío.` En una topología estable, este contador siempre muestra 1. Este contador se restablece en 0 a medida que se desactiva y activa el puerto. Por lo tanto, un valor mayor que 1 indica que la transición experimentada por el puerto es el resultado de un nuevo cálculo de STP. La transición no es el resultado de un error de enlace directo.
- `Max age expiry count: Este contador registra el número de veces que caduca la duración máxima en este enlace.` Básicamente, un puerto que espera BPDU espera la duración máxima antes de considerar que se perdió el puente designado. La edad máxima predeterminada son 20 segundos. Cada vez que ocurre este evento, el contador se incrementa. Cuando el valor no es 0, indica que el puente designado para esta LAN es inestable o tiene un problema con la transmisión de BPDU.

Búsqueda de errores de recursos

Una alta utilización de la CPU puede resultar peligrosa para un sistema que ejecuta STA. Utilice el método siguiente para comprobar que los recursos de la CPU son adecuados para un dispositivo:

- Software Cisco IOS: Ejecute el **comando show processes cpu.** Verifique que la utilización de la CPU no sea demasiado elevada. Para los switches de la serie 4500/4000 de Catalyst que ejecutan CatOS o el software Cisco IOS, consulte el documento Uso de la CPU en los switches Catalyst 4500/4000, 2948G, 2980G y 4912G.
- CatOS-Emita el **show proc cpu** command to display CPU utilization information. Check that the CPU utilization is not too high.

Hay una limitación en la cantidad de instancias diferentes de STP que pude gestionar un motor supervisor. Asegúrese de que el número total de puertos lógicos a través de todas las instancias de STP para las diferentes VLAN no excedan la cantidad máxima soportada por cada tipo y de Supervisor Engine y configuración de memoria.

Ejecute el comando **show spantree summary** para los switches que ejecutan CatOS o el **show spanning-tree summary totals** para los switches que ejecutan Cisco IOS Software. Estos comandos muestran la cantidad de puertos lógicos o interfaces por VLAN en la `columna activa de STP`. El total aparece en la parte inferior de esta columna. El total representa la suma de todos los puertos lógicos a través de todas las instancias de STP para las diferentes VLAN. Asegúrese de que este número no exceda la cantidad máxima admitida por cada tipo de motor supervisor.

Nota: La fórmula para calcular la suma de los puertos lógicos en el switch es:

```
(number of non-ATM trunks * number of active Vlans on that trunk)
+ 2*(number of ATM trunks * number of active Vlans on that trunk)
+ number of non-trunking ports
```

Para obtener un resumen de las restricciones para STP que se aplican a los switches Catalyst, consulte estos documentos:

Platform	Restricciones de STP para CatOS	Restricciones de STP para el softwa Cisco IOS
Motor de supervisión I y II Catalyst 6500/6000	Solución de problemas de STP	
Motor supervisor 720 Catalyst 6500/6000	Solución de problemas de STP	Solución de problemas de árbol de expansión
Catalyst 4500/4000	Spanning Tree	Solución de problemas de árbol de expansión
Catalyst 3750		Configuración de STP

Inhabilitación de funciones innecesarias

Al resolver problemas, intenta identificar qué hay actualmente mal en la red. Deberá inhabilitar tantas funciones como sea posible. La dehabilitación permite simplificar la estructura de la red y facilita la identificación del problema. Por ejemplo, EtherChanneling es una función que requiere que STP agrupe lógicamente varios links diferentes en un solo link; la inhabilitación de esta función durante el proceso de solución de problemas tiene sentido. Como regla general, para hacer la configuración lo más simple posible hace que el proceso de solución de problemas del problema sea mucho más fácil.

Comandos útiles

Comandos del Cisco IOS Software

- **show interfaces**
- **show spanning-tree**
- **show bridge**
- **show processes cpu**
- **debug spanning-tree**
- **logging buffered**

Comandos CatOS

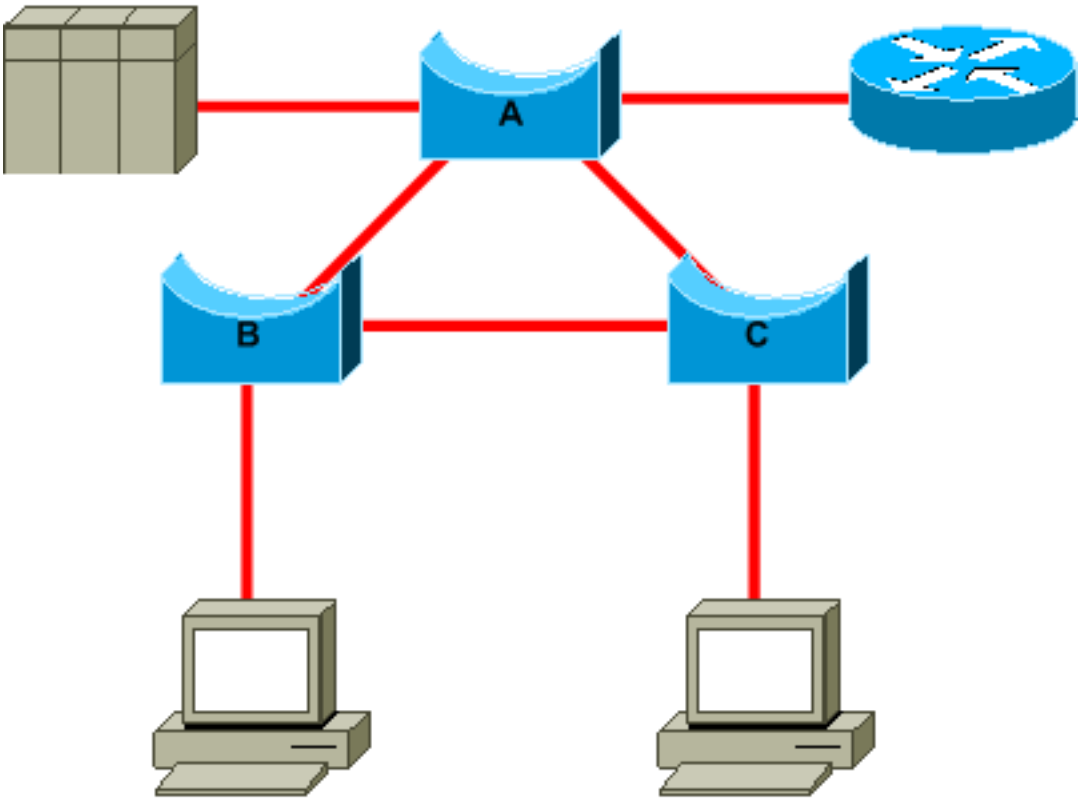
- **show port**
- **show mac**
- **show spantree**

- **show spantree statistics**
- **show spantree blockedports**
- **show spantree summary**
- **show top**
- **show proc cpu**
- **show system**
- **show counters**
- **set spantree root [secondary]**
- **set spantree uplinkfast**
- **set logging level**
- **set logging buffered**

Diseñe STP para evitar inconvenientes

Conocer la ubicación de la raíz

A menudo, la información sobre la ubicación de la raíz no está disponible al momento de solucionar los problemas. No deje que sea el STP el que decida qué puente es el puente de ruta. Para cada VLAN, normalmente se puede identificar qué switch puede servir mejor como raíz. Esto depende del diseño de la red. En general, se recomienda elegir un puente potente en el medio de la red. Si coloca el puente de ruta en el centro de la red, con conexión directa a los servidores y routers, reduce generalmente la distancia promedio desde los clientes a los servidores y routers.



Este diagrama indica:

- Si el puente B es de ruta, el enlace de A a C se bloquea en el puente A o en el puente C. En este caso, los hosts que se conectan al switch B pueden acceder al servidor y al router en dos saltos. Los hosts que se conectan al puente C pueden acceder al servidor y al router en tres saltos. La distancia promedio es de dos saltos y medio.
- Si el puente A es raíz, el router y el servidor son alcanzables en dos saltos para ambos hosts que se conectan en B y C. La distancia promedio ahora es de dos saltos.

La lógica que hay detrás de este ejemplo se puede trasladar a topologías más complejas.

> **Nota**: Para cada VLAN, incluya en el código duro el puente raíz y el puente raíz de respaldo una reducción en el valor del parámetro de prioridad STP. O bien, puede usar la macro set spantree root.

Conozca dónde existe redundancia

Proyecte la manera en que se organizan sus enlaces redundantes. Olvídese de la función plug-and-play del STP. Ajuste el parámetro de costo de STP para decidir qué puertos bloquear. Por lo general, este ajuste no es necesario si dispone de un diseño jerárquico y un puente de ruta en una buena ubicación.

> **Nota**: Para cada VLAN, sepa qué puertos pueden estar bloqueando en la red estable. Tenga un diagrama de red que muestre claramente cada loop físico en la red en el que los puertos bloqueados rompen los loops.

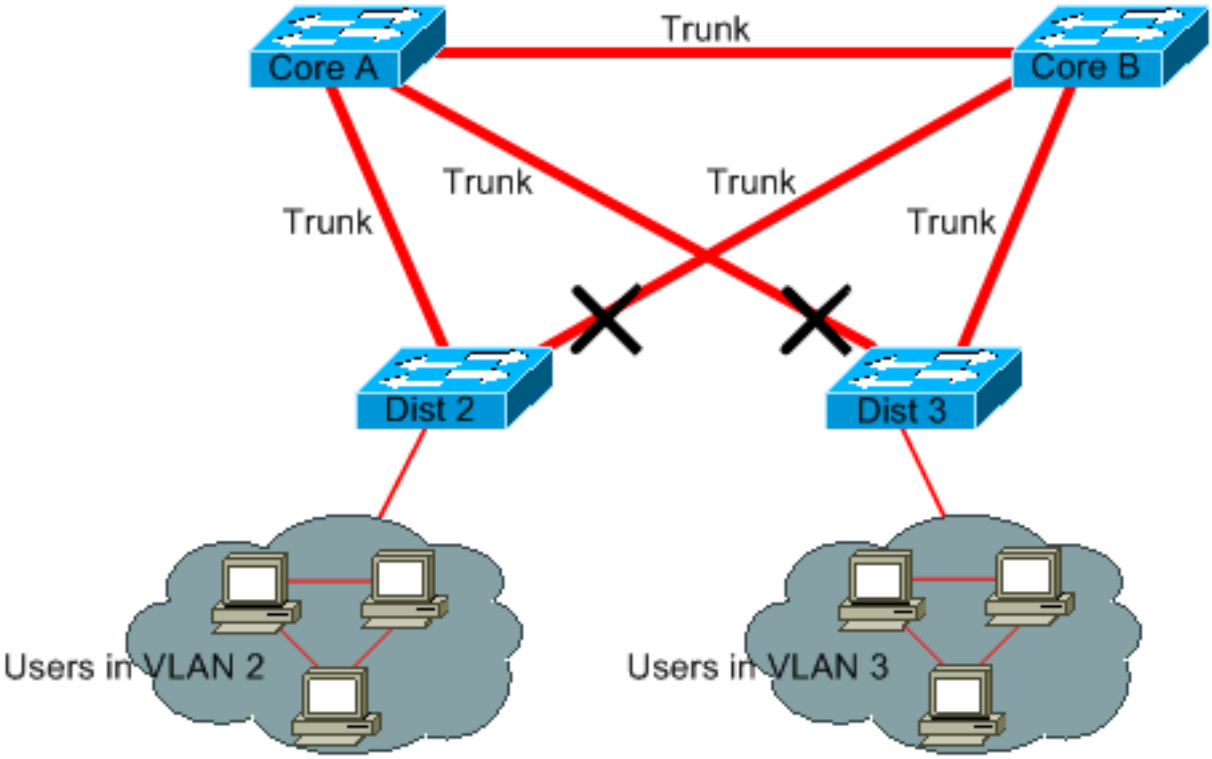
Conocer la ubicación de los enlaces redundantes permite identificar un bucle de conexión en puente accidental y la causa. Además, conocer la ubicación los puertos bloqueados le permitirá determinar la ubicación del error.

Minimizar la cantidad de puertos bloqueados

La única acción crítica que realiza el STP es el bloqueo de los puertos. Un sólo puerto de bloqueo que cambie a reenvío por equivocación puede fundir una gran parte de la red. Una buena manera de limitar el riesgo inherente al uso de STP es reducir el número de puertos bloqueados en la medida que sea posible.

Separar las VLAN que no se utilizan

No necesita más de dos enlaces redundantes entre dos nodos en una red conectada en puente. De todas formas, este tipo de configuración es común:

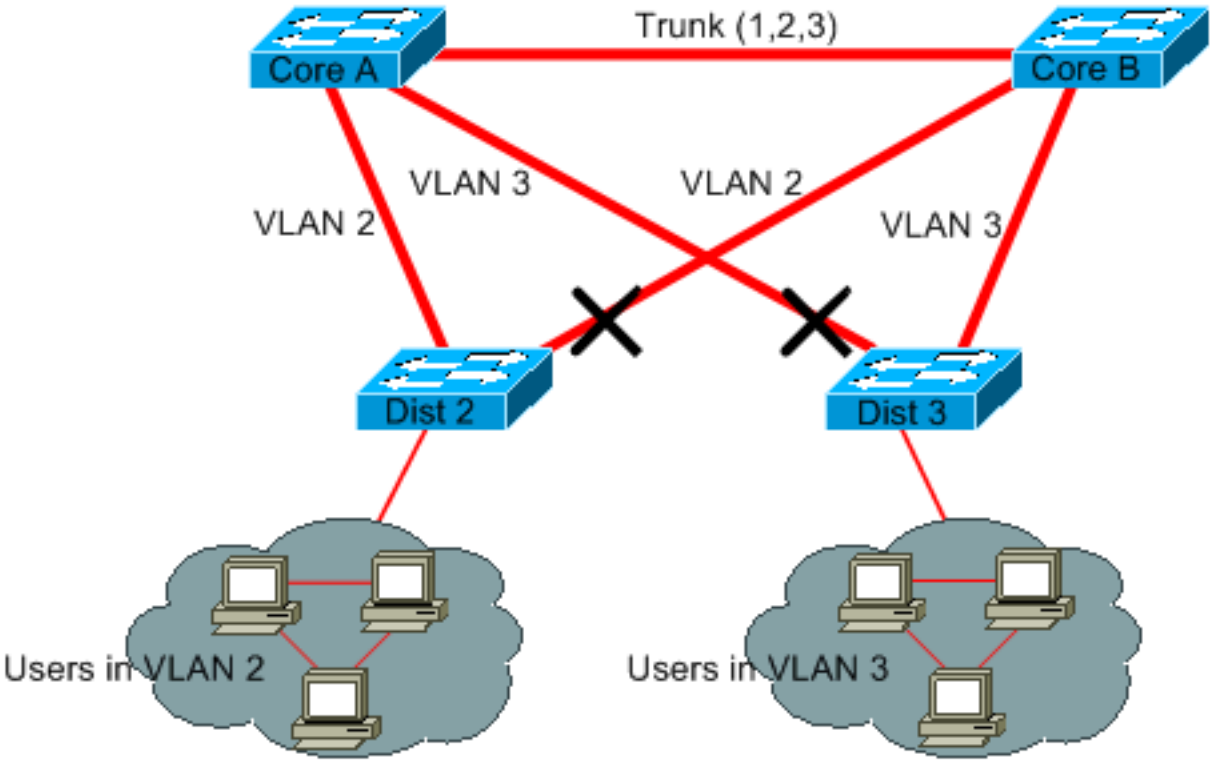


Los switches de distribución están vinculados en forma dual a dos switches de núcleo. Los usuarios que se conectan en switches de distribución sólo se encuentran en un subconjunto de VLAN disponibles en la red. En este ejemplo, los usuarios que se conectan en el Dist 2 están todos en la VLAN 2; el Dist 3 sólo conecta a los usuarios en la VLAN 3. De forma predeterminada, los trunks transportan todas las VLAN definidas en el dominio VLAN Trunk Protocol (VTP). Solo Dist 2 recibe tráfico de difusión y de multidifusión innecesario para VLAN 3, pero también bloquea uno de sus puertos para VLAN 3. El resultado es tres rutas redundantes entre el núcleo A y el núcleo B. Esta redundancia tiene como consecuencia más puertos bloqueados y una mayor probabilidad de bucle.

Nota: Elimine cualquier VLAN que no necesite de sus troncos.

El recorte VTP puede facilitar esto, pero en realidad ese tipo de función plug and play no se necesita en el núcleo de la red.

En este ejemplo, sólo se usa una VLAN de acceso para conectar los switches de distribución al núcleo:



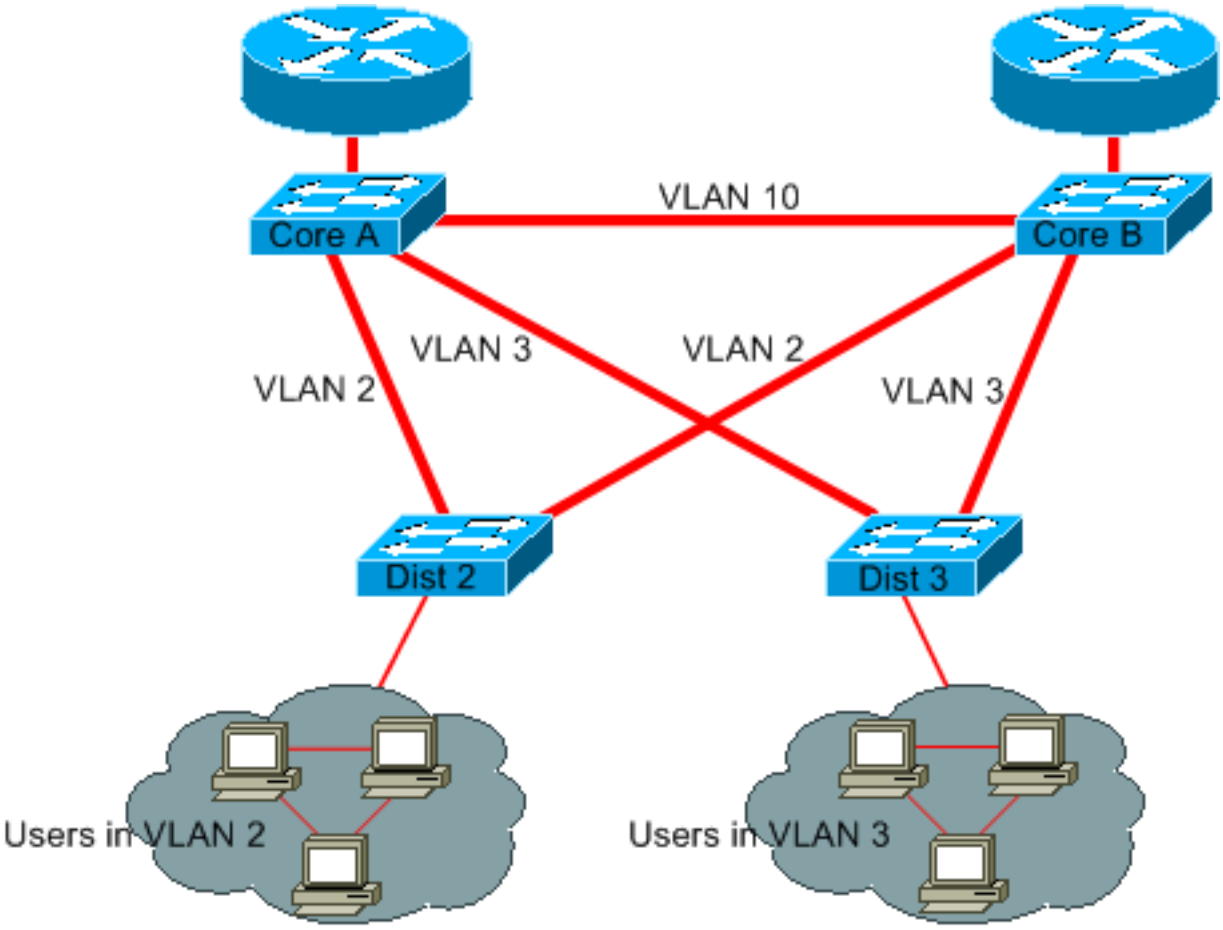
En este diseño, sólo un puerto está bloqueado por cada VLAN. Además, con este diseño, es posible remover enlaces redundantes en sólo un paso si se cierra el núcleo A o el núcleo B.

Use la conmutación de Capa 3

Switching de Capa 3 significa un routing aproximadamente a la velocidad de switching. Un router realiza dos funciones principales:

- Un router crea una tabla de reenvíos. En general, el router intercambia información con los pares mediante protocolos de routing.
- Un router recibe paquetes y los reenvía a la interfaz correcta según la dirección de destino.

Ahora, los switches de Capa 3 de última generación de Cisco son capaces de realizar esta segunda función a la misma velocidad que la función de conmutación de Capa 2. Si introduce un salto de routing y crea una segmentación adicional de la red, no hay penalidad en la velocidad. En este diagrama, se utiliza el ejemplo de la sección Recortar VLAN que no usa como base:



El núcleo A y el B son ahora algunos switches de la Capa 3. La VLAN 2 y VLAN 3 ya no están conectadas en puente entre el núcleo A y el B, por lo que no existe la posibilidad de crear un bucle de STP.

- La redundancia aún está presente, con una dependencia en los protocolos de routing de la Capa 3. El diseño asegura una nueva convergencia que incluso es más rápida que la nueva convergencia con STP.
- Ya no hay ningún puerto que bloquee STP. Por lo tanto, no es posible la creación de un bucle de conexión en puente.
- No hay penalización de velocidad, ya que dejar la VLAN por switching de Capa 3 es tan rápido como hacer bridging dentro de la VLAN.

Hay un único inconveniente con este diseño. La migración de este tipo de diseño implica generalmente un reprocesamiento del esquema de direccionamiento.

Mantener STP incluso si no es necesario

Aun si pudo quitar todos los puertos bloqueados de su red y no tiene ninguna redundancia física, no deshabilite el STP. El STP generalmente no hace un uso intensivo del procesador; el switching de paquetes no involucra a la CPU en la mayoría de los switches de Cisco. Además, las pocas BPDU que se envían en cada enlace no reducen de forma significativa el ancho de banda disponible. Sin embargo, una red conectada en puente sin STP puede desaparecer en una fracción de segundos si un operador comete un error en un panel de conexiones, por ejemplo. Por lo general, no es aconsejable desactivar el STP en una red conectada en puente.

Mantener la VLAN administrativa sin tráfico y evitar que una única VLAN se expanda por toda la red

Por lo general, un switch de Cisco tiene una sola dirección IP que se vincula con una VLAN, conocida como la VLAN administrativa. En esta VLAN, el switch se comporta como un host IP genérico. En particular, cada paquete de difusión o multidifusión se envía a la CPU. Un índice alto de paquetes de difusión o multidifusión en la VLAN administrativa, puede afectar negativamente la CPU y su capacidad de procesar las BPDU vitales. Por lo tanto, mantenga el tráfico de usuario fuera de la VLAN administrativa.

Hasta hace poco, no se podía eliminar la VLAN 1 desde un enlace troncal en una implementación de Cisco. En general, la VLAN 1 suele servir como VLAN administrativa, en la que se puede acceder a todos los switches en la misma subred IP. Aunque sea útil, esta configuración podría ser riesgosa porque un bucle de conexión en puente en la VLAN 1 afecta todos los enlaces troncales y puede hacer caer la red completa. Sin duda, el mismo problema existe independientemente de la VLAN que se use. Intente segmentar los dominios de conexión en puente que usen switches de alta velocidad de capa 3.

A partir de la versión 5.4 de CatOS y la versión 12.1(11b)E del software del IOS de Cisco, puede quitar la VLAN 1 de los troncos. La VLAN 1 aún existe, pero bloquea el tráfico, lo que evita cualquier posibilidad de bucle.

Información Relacionada

- Herramientas y recursos: Soporte técnico y Documentación
- Soporte Técnico y Documentación - Cisco Systems

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).