Problemas de Spanning Tree Protocol y Consideraciones de Diseño Relacionadas

Contenido

Introducción

Este documento presenta una lista de recomendaciones que ayuden a implementar una red segura con respecto al bridging para el Switches del Cisco Catalyst que funciona con el Catalyst OS (CatOS) y el software de Cisco IOS®. 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. El documento también muestra la clase de diseño que minimiza los problemas relacionados con el árbol de expansión y cuyo Troubleshooting resulta fácil.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

Antecedentes

Este documento no discute el funcionamiento básico de STP. Para aprender cómo el STP trabaja, refiera a este documento:

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

Este documento no discute STP rápido (RSTP), definido en el IEEE 802.1W. También, este documento no discute Múltiples Árboles de expansión (MST) el protocolo, definido en el IEEE 802.1S. Para más información sobre el RSTP y el MST, refiera a 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 un documento más específico del Troubleshooting de STP para los switches de Catalyst que funcionan con el Cisco IOS Software, refiera al documento que resuelve problemas el STP en el switch de Catalyst que ejecuta IOS integrado Cisco (modo nativo).

Falla del protocolo de árbol de expansión

La función primaria del Algoritmo del árbol de expansión (STA) es cortar los loopes que los links redundantes crean en las redes de Bridge. El STP actúa en la capa 2 del modelo del interconexión de sistema abierto (OSI). Mediante las Unidades (BPDU) ese intercambio entre los Bridges, el STP elige los puertos que remiten o bloquean eventual el tráfico. Este protocolo puede fallar en algunos casos específicos, y resolver problemas la situación resultante puede ser muy difícil, que depende del diseño de la red. En esta área determinada, usted realiza a la mayoría de la parte importante del troubleshooting antes de que ocurra el problema.

Un error en el STA lleva generalmente a un Bridging Loop. La mayoría de los clientes que llaman el Soporte técnico de Cisco para atravesar - sospechoso de los problemas del árbol un bug, solamente un bug es raramente la causa. Incluso si el software es el problema, un Bridging Loop en un entorno STP todavía viene de un puerto que deba bloquear, sino que por el contrario adelante trafica.

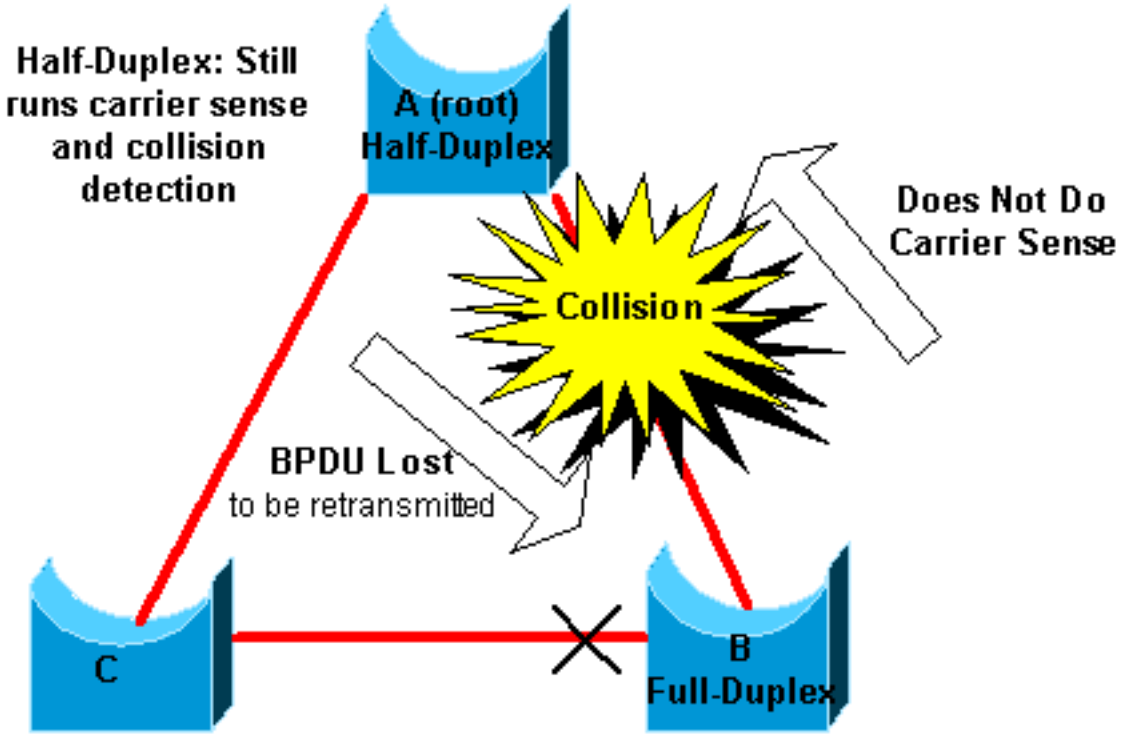
Convergencia del árbol de expansión

Refiera al vídeo del Spanning-tree para ver un ejemplo que explique cómo converge el Spanning-tree inicialmente. El ejemplo también explica porqué un puerto bloqueado entra el modo de reenvío debido a una pérdida excesiva de BPDU, dando por resultado la falla de STA.

El resto de este documento enumera las diferentes situaciones que pueden causar un error en el STA. La mayor parte de estos errores se relacionan con una pérdida masiva de BPDU. La pérdida causa los puertos bloqueados a la transición al modo de reenvío.

Discordancia dúplex

La discordancia dúplex en un enlace punto a punto es mismo un error de la configuración común. Si usted fija manualmente al modo dúplex a por completo en un lado del link y deja el otro lado en el modo de negociación automática, el link termina para arriba en semidúplex. (El puerto A con el conjunto del modo dúplex a por completo negocia no más.)



El escenario de caso peor es cuando un Bridge que envía los BPDU tiene el modo dúplex fijado a semidúplex en un puerto, pero el puerto de peer en el otro extremo del link tiene el FULL-duplex fijado modo dúplex. En el ejemplo anterior, la discordancia dúplex en el link entre el puente A y el B puede fácilmente conducir a un loop de conexión en puente. Porque el Bridge B tiene configuración para el FULL-duplex, no realiza la detección de portadora antes de que acceso del link. El Bridge B comienza a enviar las tramas incluso si el Bridge A está utilizando ya el link. Esta situación es un problema para A; interligue A detecta una colisión y funciona con el algoritmo del retroceso antes de que el Bridge intente otra transmisión del bastidor. Si hay bastante tráfico de B a A, cada paquete que A envía, que incluye los BPDU, experimenta el aplazamiento o la colisión y consigue eventual caído. Desde un punto de vista STP, porque el Bridge B no recibe los BPDU de A más, el Bridge B ha perdido el Root Bridge. Esto lleva B a desbloquear el puerto conectado para interligar el C, que crea el loop.

Siempre que haya una discordancia dúplex, estos mensajes de error están en las consolas del Switch de los switches de Catalyst que funcionan con CatOS y el Cisco IOS Software:

CatOS

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

Cisco IOS Software

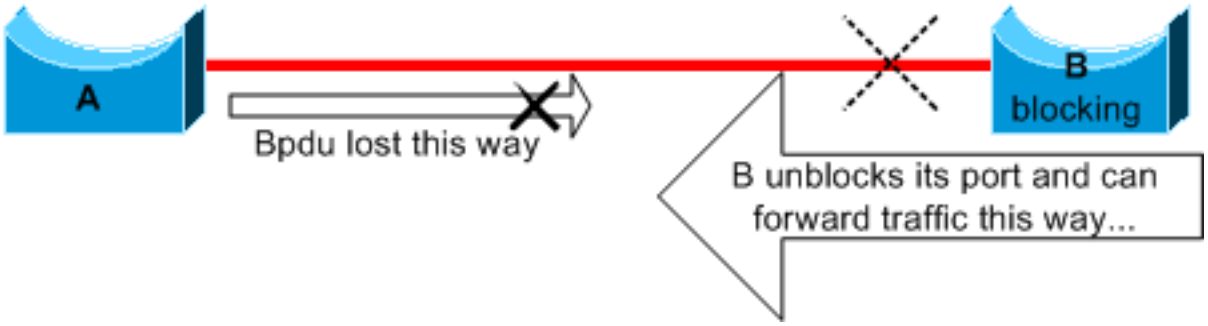
```
%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet5/1 (not half
duplex), with TBA05071417(Cat6K-B) 4/1 (half duplex).
```

Marque las configuraciones dúplex y, si la configuración dúplex no hace juego, para fijar la configuración apropiadamente.

Para más información sobre cómo resolver problemas una discordancia dúplex, refiera al documento que configura y que resuelve problemas la negociación automática del dúplex completo y del semidúplex de los Ethernetes 10/100/1000Mb.

link unidireccional

Los links unidireccionales son una causa común del loop de conexión en puente. En los links de fibra, un error que va sin la detección causa a menudo los links unidireccionales. Otra causa es un problema con un transmisor-receptor. Cualquier cosa que puede llevar un link para permanecer para arriba y para proporcionar una comunicación unidireccional es muy peligroso con respecto al STP. Este ejemplo aclara:



Aquí, suponga que el link entre A y B es unidireccional. El link cae el tráfico de A a B mientras que el link transmite el tráfico de B a A. Assume que interliga B bloqueaba antes de que el link llegó a ser unidireccional. Sin embargo, un puerto puede bloquear solamente si recibe los BPDU de un Bridge que tenga una prioridad más alta. Puesto que, en este caso, se pierden todos los BPDU que vienen de A, interligue las transiciones B eventual su puerto hacia A al estado de reenvío y adelante trafique. Esto crea un loop. Si este error existe en el lanzamiento, el STP no converge correctamente. En el caso de una discordancia dúplex, una reinicialización ayuda temporalmente; pero en este caso, una reinicialización de los Bridges no tiene absolutamente ningún efecto.

Para detectar los links unidireccionales antes de la creación del Forwarding Loop, Cisco diseñó y implementó el protocolo del UniDirectional Link Detection (UDLD). Esta característica puede detectar el cableado o los links unidireccionales incorrectos en la capa 2 y romper automáticamente los loopes resultantes inhabilitando algunos puertos. Ejecute el UDLD donde sea posible en un Bridged Environment.

Para más información sobre el uso del UDLD, refiera al documento que entiende y que configura la función del Unidirectional Link Detection Protocol.

Corrupción de paquetes

La corrupción del paquete también puede conducir a la misma clase de falla. Si un link tiene un gran número de errores físicos, usted puede perder algunos BPDU consecutivos. Esta pérdida puede llevar un puerto de bloqueo a la transición al estado de reenvío. Usted no ve este caso muy a menudo porque los parámetros predeterminados STP son muy conservadores. El puerto de bloqueo necesita faltar los BPDU por 50 segundos antes de la transición al envío. La transmisión exitosa de un solo BPDU rompe el loop. Este caso ocurre comúnmente con el ajuste descuidado de los parámetros STP. Un ejemplo de un ajuste es reducción de la edad máxima.

La discordancia dúplex, los malos cables, o la longitud de Cable incorrecto pueden causar el daño del paquete. Refiera al puerto del switch del troubleshooting del documento e interconecte los problemas para una explicación salida del contador de errores de CatOS y del Cisco IOS Software.

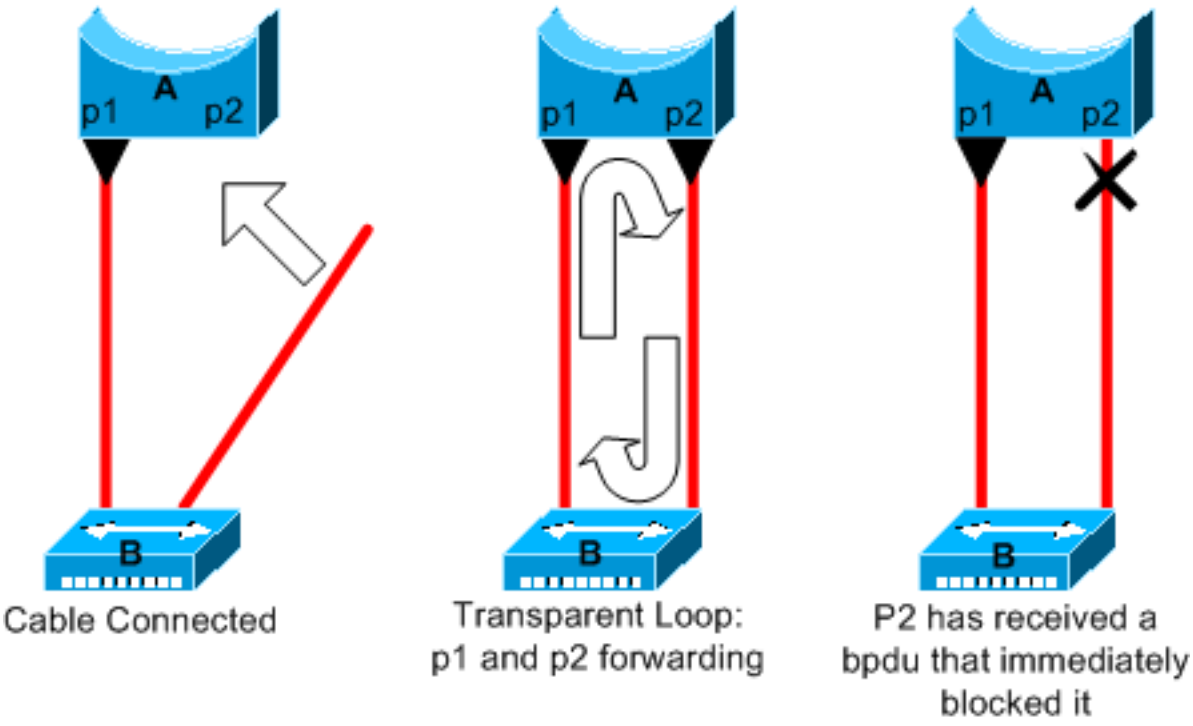
Errores de recurso

El STP se implementa en el software, incluso en los switches de mayor capacidad que realizan la mayoría de las funciones de Switching en hardware con los circuitos específicos de la aplicación especializados (ASIC). Si por cualquier motivo hay un overutilization del CPU del Bridge, los recursos pueden ser inadecuados para la transmisión de los BPDU. El STA no es generalmente uso intensivo del procesador y tiene prioridad sobre otros procesos. La sección de los errores de recurso del buscar de este documento proporciona algunas directrices sobre el número de casos del STP que una plataforma particular pueda manejar.

Error de configuración de PortFast

PortFast es una característica que usted habilita típicamente solamente para un puerto o interconecta que conecta con un host. Cuando el link sube en este puerto, el Bridge salta las primeras fases del STA y directamente de las transiciones al modo de reenvío.

Precaución: No utilice la característica portfast en los puertos del switch o las interfaces que conectan con el otro Switches, Hubs, o Routers. Si no, usted puede crear un loop de la red.



En este ejemplo, el dispositivo A es un Bridge con el p1 del puerto que remite ya. El p2 del puerto tiene una configuración de PortFast. El dispositivo B es un concentrador. Tan pronto como usted conecte el segundo cable en A, el p2 del puerto va al modo de reenvío y crea un loop entre el p1 y el p2. Paradas de este loop tan pronto como el p1 o el p2 reciba un BPDU que ponga uno de estos dos puertos en el modo de bloqueo. Pero hay un problema con esta clase de Transient Loop. Si el tráfico colocado es muy intensivo, el Bridge puede tener problema con con éxito la transmisión del BPDU que para el loop. Este problema puede retrasar la convergencia considerablemente o derribar la red en los casos extremos.

Para más información sobre el uso correcto de PortFast en el Switches que funciona con CatOS y el Cisco IOS Software, refiera al documento usando PortFast y a otros comandos de reparar los retardos de la conectividad de inicialización de la estación de trabajo.

Incluso con la configuración de PortFast, el puerto o la interfaz todavía participa en el STP. Si un Switch con una prioridad de Bridge más baja que el de los attaches activos actuales del Root Bridge a un puerto o a una interfaz del Portfast configurado, él se puede elegir como el Root Bridge. Este cambio del Root Bridge puede afectar al contrario a la topología de STP activa y puede rendir el subóptimo de la red. Para prevenir esta situación, la mayoría de los switches de Catalyst que funcionan con CatOS y el Cisco IOS Software tienen una característica con la protección BPDU del nombre. La protección BPDU inhabilita un puerto o una interfaz del Portfast configurado si el puerto o la interfaz recibe un BPDU.

Para más información sobre el uso de la característica de la protección BPDU en el Switches que funciona con CatOS y el Cisco IOS Software, refiera a la mejora de la protección BPDU del árbol de expansión Portfast del documento.

Ajuste y problemas de diámetro del parámetro awkard STP

Un valor agresivo para el parámetro de la edad máxima y el retardo de reenvío puede llevar a una topología de STP muy inestable. En estos casos, la pérdida de algunos BPDU puede hacer un loop aparecer. El Otro problema que no es bien sabido se relaciona con el diámetro de la red de Bridge. Los valores conservadores predeterminados para los temporizadores STP imponen a un diámetro de red máximo de siete. Este diámetro de red máximo restringe hasta dónde lejos de

uno a los Bridges en la red pueden estar. En este caso, dos Bridges distintos no pueden ser más de siete saltos lejos de uno a. Parte de esta restricción proviene del campo de edad que tiene BPDU.

Cuando un BPDU propaga del Root Bridge hacia las hojas del árbol, el campo de edad incrementa cada vez que va el BPDU sin embargo un Bridge. Eventual, el Bridge desecha el BPDU cuando el campo de edad va más allá de la Edad máxima. Si la raíz es demasiado lejos de algunos Bridges de la red, este problema puede ocurrir. Este problema afecta a la convergencia de atravesar - árbol.

Tome el particular cuidado si usted planea cambiar los temporizadores STP del valor predeterminado. Hay peligro si usted intenta conseguir un reconvergence más rápido de esta manera. Un cambio del temporizador STP tiene un impacto en el diámetro de la red y la estabilidad del STP. Usted puede cambiar la prioridad de Bridge para seleccionar el Root Bridge, y cambia el costo de puerto o el parámetro de prioridad para controlar la Redundancia y el Equilibrio de carga.

El software de Cisco Catalyst provee de usted las macros que ajustan finalmente los parámetros STP más importantes para usted:

- El comando macro del **set spantree root secondary** disminuye la prioridad de Bridge de modo que se convierta en raíz (o raíz alternativa). Una opción adcional está disponible para este comando ese los resultados en ajustar de los temporizadores STP especificando el diámetro de su red. Incluso cuando está hecho correctamente, el ajuste del temporizador no mejora perceptiblemente el tiempo de convergencia e introduce algunos riesgos de la inestabilidad en la red. También, esta clase de ajustar tiene que ser actualizada cada vez que un dispositivo se agrega en la red. Guarde los valores conservadores predeterminados, que son familiares a los ingenieros de red.
- **El comando set spantree uplinkfast** para CatOS o el **comando spanning-tree uplinkfast** para el Cisco IOS Software aumenta la prioridad del Switch de modo que el Switch no pueda ser raíz. El comando aumenta el tiempo de la convergencia de STP en caso de falla de link ascendente. Utilice este comando en un switch de distribución con la conexión dual a algunos switches del núcleo. Refiera al documento que entiende y que configura la Función UplikFast de Cisco.
- **El comando set spantree backbonefast enable** para CatOS o el **comando spanning-tree backbonefast** para el Cisco IOS Software puede aumentar la época de la convergencia de STP del Switch en caso de falla de link indirecto. El BackboneFast es una función propietaria de Cisco. Refiera al documento que entiende y que configura el Backbone Fast en los switches de Catalyst.

Para más información sobre los temporizadores STP y las reglas para ajustarlas cuando absolutamente es necesario, refiera al documento que entiende y que ajusta los temporizadores del Spanning Tree Protocol.

Errores de software

Como se menciona en la introducción, el STP es una de las primeras características que fue implementado en Productos Cisco. Por lo general, esta característica es muy estable. Solamente la interacción con más nuevas características, tales como EtherChannel, ha hecho el STP fallar en algunos casos muy específicos que ahora se han dirigido. Varios diversos factores pueden causar un bug de software y pueden tener varios diversos efectos. No hay manera de describir

adecuadamente los problemas que un bug puede introducir. La mayoría de la situación peligrosa que se presenta de los errores del software es si usted ignora algunos BPDU o, hablando en términos generales, usted tiene una transición del puerto de bloqueo al envío.

Resolución de problemas de falla

Desafortunadamente, no hay procedimiento sistemático para resolver problemas un problema STP. Sin embargo, esta sección resume algunas de las acciones que están disponibles para usted. La mayor parte de los pasos en esta sección se aplican al troubleshooting de los loopes del bridging en general. Usted puede utilizar un acercamiento más convencional para identificar otros errores del STP que lleven a una pérdida de conectividad. Por ejemplo, usted puede explorar la trayectoria que el tráfico que experimenta las tomas de un problema.

Nota: La mayor parte de estos pasos de Troubleshooting asumen la Conectividad a los diversos dispositivos de la red de Bridge. Esta Conectividad significa que usted tiene acceso a la consola. Por ejemplo, durante un loop de conexión en puente probablemente no pueda realizar una conexión Telnet.

Si usted tiene la salida de un **comando show-tech support de** su dispositivo de Cisco, usted puede utilizar el analizador del CLI de Cisco (clientes registrados solamente) para visualizar los problemas potenciales y los arreglos.

Utilice el diagrama de la red

Antes de que usted resuelva problemas un Bridging Loop, usted necesita conocer estos elementos, al mínimo:

- La topología de la red de Bridge
- La ubicación del Root Bridge
- La ubicación de los puertos bloqueados y de los links redundantes

Este conocimiento es esencial por lo menos estas dos razones:

- Para conocer qué reparar en la red, usted necesita saber la red mira cuando trabaja correctamente.
- La mayoría de los pasos de solución de problemas simplemente utilizan comandos show 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

Era que una tormenta de broadcast podría tener un efecto catastrófico en la red. Hoy, con los links de alta velocidad y los dispositivos que proporcionan la transferencia en el nivel del hardware, no es probable que un solo host, por ejemplo, un servidor, derribe una red con los broadcasts. La mejor manera de identificar un Bridging Loop es capturar el tráfico en un link saturado y un control que usted ve los tiempos similares del múltiplo de los paquetes. Realista, sin embargo, si todos los usuarios en cierto dominio de Bridge tienen problemas de conectividad al mismo tiempo, usted puede sospechar ya un Bridging Loop.

Verifique la utilización de los puertos de sus dispositivos y busque valores anormales. Refiera a la sección de utilización de puertos del control de este documento.

En los switches de Catalyst que ejecutan CatOS, usted puede marcar fácilmente el uso de backplane total con el **comando show system**. El comando proporciona el uso actual del backplane del Switch y también especifica el USO pico y la fecha del USO pico. Un pico máximo inusual le muestra si ha habido nunca un Bridging Loop en este dispositivo.

Restaurar rápidamente la conectividad y prepararse para otro momento

Puertos de la neutralización para romper el loop

Interligando los loopes tenga consecuencias extremadamente graves en una red de Bridge. Los administradores no tienen generalmente tiempo que buscar la causa del loop y preferirla para restablecer la Conectividad cuanto antes. La salida fácil en este caso es inhabilitar manualmente cada puerto que proporcione la Redundancia en la red. Si usted puede identificar a una parte de la red que se afecta la mayoría, comience a inhabilitar los puertos en esta área. O, si es posible, inhabilite inicialmente los puertos que deben bloquear. Cada vez que usted inhabilita un puerto, marque para ver si usted ha restablecido la Conectividad en la red. Identificando que los minusválidos viran las paradas hacia el lado de babor el loop, usted también identifica el trayecto redundante en donde se localiza este puerto. Si este puerto debería haber estado bloqueando, quizás haya encontrado el link en donde apareció la falla.

Eventos del registro STP en los dispositivos que reciben los puertos bloqueados

Si usted no puede identificar exacto la fuente del problema, o si el problema es transitorio, habilite el registro de los eventos STP en los Bridges y el Switches de la red que experimenta el error. Si usted quiere limitar el número de dispositivos para configurar, por lo menos habilite esto los dispositivos de apertura de sesión que reciben los puertos bloqueados; la transición de un puerto bloqueado es qué crea un loop.

- Problema de software del Cisco IOS el **debug spanning-tree events del** comando exec para habilitar la información del debug STP. Publique el **registro del** comando general config mode **mitigado** para capturar esta información del debug en los buffers del dispositivo.
- El del de CatOS- el **comando set logging level spantree 7 default** aumenta el nivel predeterminado de eventos que se relacionen con el STP con el nivel de debug. Esté seguro que usted registra un número máximo de mensajes en los buffers del Switch con el uso del **comando set logging buffer 500**.

También puede intentar enviar el resultado de la depuración a un dispositivo syslog. Desafortunadamente, cuando ocurre un Bridging Loop, usted mantiene raramente la Conectividad a un servidor de Syslog.

Verificar puertos

Los puertos críticos a investigar primero son los puertos de bloqueo. Esta sección proporciona una lista qué buscar en los diversos puertos, con una descripción rápida de los comandos de publicar para el Switches que funciona con CatOS y el Cisco IOS Software.

Marque que los puertos bloqueados reciben los BPDU

Especialmente en los puertos bloqueados y los puertos raíz, control que usted recibe los BPDU periódicamente. Varios problemas pueden llevar a una falla de puerto de recibir los paquetes o los

BPDU.

- El Cisco IOS Software-en el Cisco IOS Software Release 12.0 o Posterior, salida del **comando show spanning-tree bridge-group -** tiene un campo `BPDU`. El campo le muestra el número de BPDU recibidos para cada interfaz. Publique el comando las uno o dos épocas adicionales de determinar si el dispositivo recibe los BPDU.Si usted no tiene el campo `BPDU` en la salida del **comando show spanning-tree**, usted puede habilitar el debug STP con el **comando debug spanning-tree** de verificar el recibo de los BPDU.
- **El comando show mac module/port de** CatOS-The le dice el número de paquete multidifusión que un puerto específico recibe. Pero el comando más simple de utilizar es el **comando show spantree statistics module-/port- vlan-**. Este comando visualiza la cantidad exacta de BPDU de configuración que un puerto específico recibió, en un VLA N específico. Un puerto puede pertenecer a varios VLA N, si enlace. Vea una sección de comando catos adicional de este documento.

Marque para saber si hay una discordancia dúplex

Para buscar una discordancia dúplex, usted debe marcar a cada lado del enlace punto a punto.

- Problema de software del Cisco IOS el **comando show interfaces [interface interface-number] status** de marcar el estatus de la velocidad y dúplex del puerto específico.
- Las primeras líneas de CatOS-The de la salida del **comando show port module-/port-** le dan la velocidad y dúplex según la configuración del puerto.

Verificar utilización de puertos

Una interfaz con la sobrecarga del tráfico puede no poder transmitir el BPDU vital. Una sobrecarga del link también indica un Bridging Loop posible.

- Software-uso del Cisco IOS el comando show interfaces **de determinar la utilización en una interfaz.** Varios campos le ayudan con esta determinación, tal como `carga` y `entrada-salida de los paquetes`. Refiera al puerto del switch del troubleshooting del documento e interconecte los problemas para una explicación de la salida del **comando show interfaces**.
- **El comando show mac module-/port- de** CatOS-The visualiza las estadísticas sobre los paquetes que un puerto recibe y envía. **El comando show top** evalúa automáticamente la utilización de puertos durante un período 30-second y visualiza el resultado. El comando clasifica los resultados por el uso del ancho de banda del porcentaje, aunque las otras opciones para la clasificación de los resultados estén disponibles. También, el **comando show system** da una indicación de la utilización de backplane, aunque el comando no señala a un puerto específico.

Verificar el daño de paquetes

- La Software-mirada del Cisco IOS para el error incrementa en el contador de `errores de entrada del` **comando show interfaces**. Los contadores de errores incluyen los `runts, los gigantes, ningún buffer, el CRC, la trama, el overrun`, y los `conteos ignorados`.Refiera al puerto del switch del troubleshooting del documento e interconecte los problemas para una explicación de la salida del **comando show interfaces**.

- El comando show port module-/port- de CatOS-The **le da algunos detalles con** `Alinee Yerran, El FCS Yerra, Xmit Yerra, Rcv-Err,` y los campos `de tamaño insuficiente`. **El comando show counters module-/port-** proporciona las estadísticas en aún más detalle.

Comando de CatOS adicional

El comando show spantree statistics module-/port- vlan- *da mismo la información precisa sobre un puerto específico.* Publique este comando en los puertos que usted sospecha y presta la especial atención a estos campos:

- `Remita la cuenta transporte que` este contador recuerda cuántas veces las transiciones de puerto del aprendizaje al envío. En una topología estable, este contador muestra siempre 1. Este los contadores se reinicia a 0 como el puerto van abajo y suben. Así pues, un valor que es más alto de 1 indica que la transición experimentada por el puerto es el resultado de un recálculo de STP. La transición no es el resultado de una falla de link directo.
- `La cuenta del vencimiento de la edad máxima` este contador sigue la cantidad de veces que la edad máxima expiró en este link. Básicamente, un puerto que cuenta con las esperas BPDU para la edad máxima antes de que el puerto considere el Bridge designado ser perdido. El valor por defecto de la edad máxima es 20 segundos. Cada vez que ocurre este evento, el contador incrementa. Cuando el valor no es 0, indica que el Bridge designado para este LAN es inestable o tiene un problema con la transmisión de los BPDU.

Búsqueda de errores de recursos

CPU elevada una utilización puede ser peligrosa para un sistema que ejecute el STA. Utilice este método para marcar que los recursos de la CPU son adecuados para un dispositivo:

- Problema de software del Cisco IOS el **comando show processes cpu**. Verifique que la utilización de la CPU no sea demasiado elevada. Para el Switches de las 4500/4000 Series del Catalyst que funciona con CatOS o el Cisco IOS Software, refiera a la utilización de la CPU del documento en el Catalyst 4500/4000, 2948G, 2980G, y 4912G Switch.
- CatOS-problema el **comando show proc cpu** de visualizar la información de la utilización de la CPU. Verifique que la utilización de la CPU no sea demasiado elevada.

Hay una limitación en el número de diversos casos del STP que un Supervisor Engine pueda manejar. 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.

Publique el **comando show spantree summary** para el Switches que funciona con CatOS o el **comando show spanning-tree summary totals** para el Switches que funciona con el Cisco IOS Software. Estos comandos display el número de puertos lógicos o de interfaces por el VLA N 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 todos los casos del STP para los diversos VLA N. Aseegurese que este número no excede el número máximo soportado para cada tipo de motor supervisor.

Nota: La fórmula para computar la suma de 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 un resumen de las restricciones para el STP que se aplican a los switches de Catalyst, refiera a estos documentos:

Plataforma	Restricciones STP de CatOS	Restricciones STP del Cisco IOS Software
Supervisor Engine I e II del Catalyst 6500/6000	Troubleshooting de STP	
Supervisor Engine 720 del Catalyst 6500/6000	Troubleshooting de STP	Solución de problemas de árbol de expansión
Catalyst 4500/4000	Spanning-tree	Resolver problemas el Spanning-tr
Catalyst 3750		Configurar el STP

Características innecesarias de la neutralización

El troubleshooting es una cuestión de identificar cuál está actualmente mal en la red. Inhabilite tantas características como sea posible. Las ayudas de la incapacidad simplifican la estructura de red y facilitan la identificación del problema. Por ejemplo, EtherChanneling es una característica que requiere el STP liar lógicamente varios diversos links en un solo link; la incapacidad de esta característica durante el troubleshooting tiene sentido. Como regla general, la fabricación de la configuración tan simple como sea posible hace resolviendo problemas el problema más fácil.

Comandos útiles

Comandos del Cisco IOS Software

- show interfaces
- show spanning-tree
- muestre el Bridge
- show processes cpu
- haga el debug del atravesar-árbol
- logging buffered

Comandos CatOS

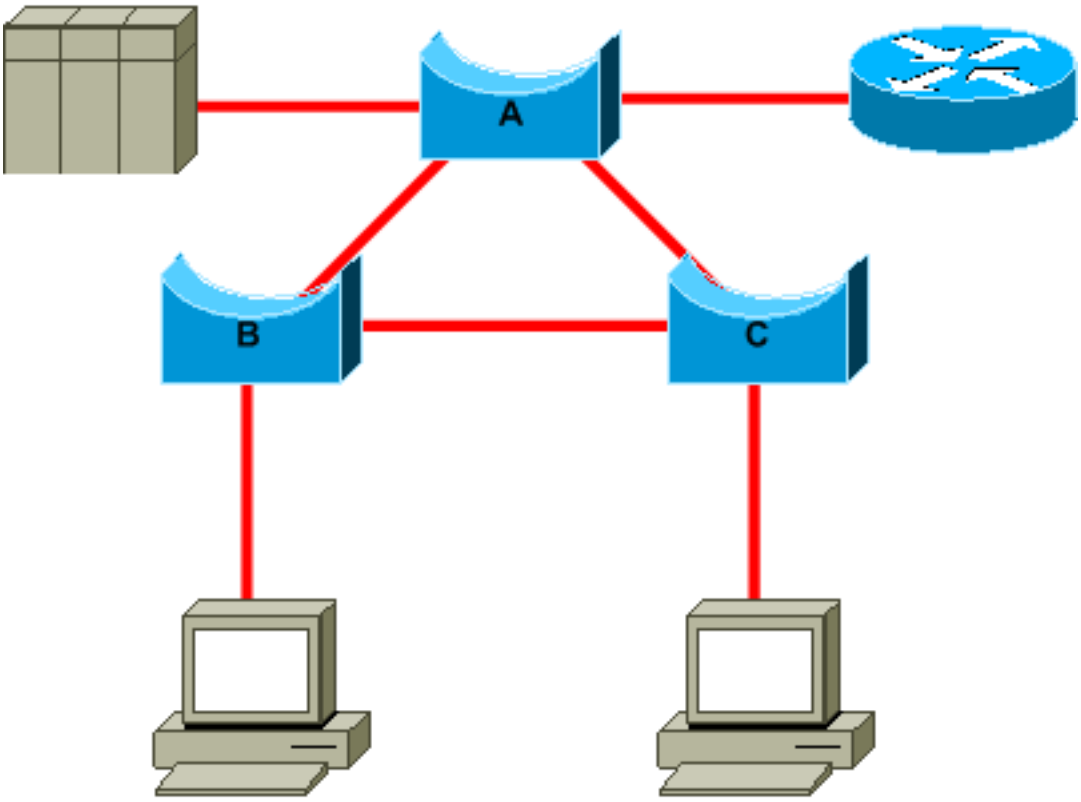
- show port
- show mac
- show spantree
- muestre las estadísticas del árbol de expansión
- muestre los blockedports del spantree
- show spantree summary
- show top
- show proc cpu
- show system
- show counters
- set spantree root secondary
- configura el link ascendente rápido del árbol de expansión
- set logging level

- fije el registro mitigado

Diseñe STP para evitar inconvenientes

Conocer la ubicación de la raíz

Muy a menudo, la información sobre la ubicación de la raíz no está disponible en el tiempo de Troubleshooting. No deje el STP para decidir qué Bridge es raíz. Para cada VLA N, usted puede identificar generalmente que el Switch puede el mejor servicio como raíz. Esto depende del diseño de la red. Generalmente, elija un Bridge potente en el medio de la red. Si usted pone el Root Bridge en el centro de la red con la conexión directa a los servidores y al Routers, usted reduce generalmente la distancia promedio de los clientes a los servidores y al Routers.



Este diagrama muestra:

- Si el Bridge B es raíz, conecte A al C se bloquea en el Bridge A o el Bridge C. en este caso, los host que conectan con el switch B pueden acceder el servidor y al router en dos saltos. Los host que conectan para interligar el C pueden acceder el servidor y al router en tres saltos. La distancia promedio es dos y una mitad de los saltos.
- Si el Bridge A es raíz, el router y el servidor son accesibles en dos saltos para ambos host que conecten en B y el C. La distancia promedio ahora es dos saltos.

La lógica detrás de las transferencias de este ejemplo simple a más topologías complejas.

Nota importante: Para cada VLA N, código duro el Root Bridge y el Root Bridge de backup con una reducción en el valor del parámetro de prioridad STP. O usted puede utilizar el set spantree root macro.

Conozca dónde existe redundancia

Planee la organización de sus links redundantes. Olvide el característica Plug and play del STP. Ajuste el parámetro de costo STP para decidir qué puertos bloquean. Esto que ajusta no es generalmente necesario si usted tiene un diseño jerárquico y un Root Bridge en una buena ubicación.

Nota importante: Para cada VLA N, sepa qué puertos deben bloquear en la red estable. Tenga un diagrama de la red que muestre claramente cada loop físico en la red y qué puertos bloqueados rompen los loopes.

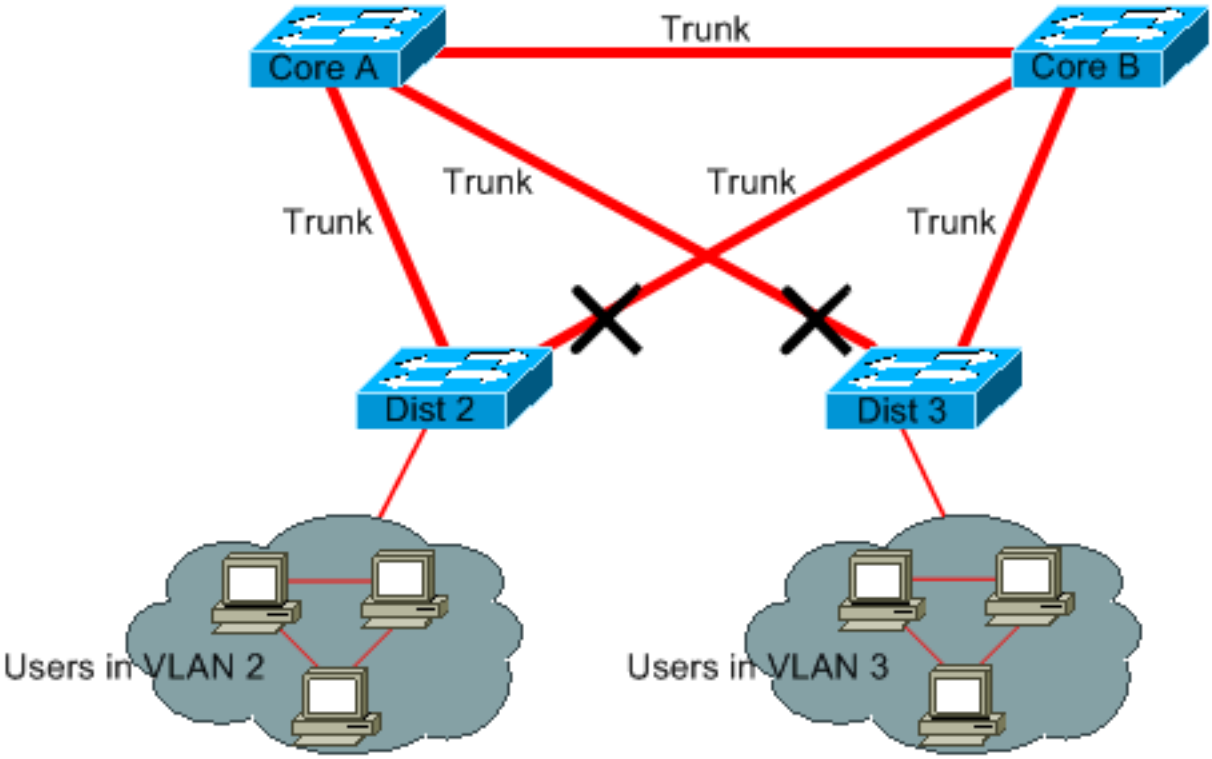
El conocimiento de la ubicación de los links redundantes le ayuda a identificar un Bridging Loop accidental y la causa. También, el conocimiento de la ubicación de los puertos bloqueados permite que usted determine la ubicación del error.

Minimizar la cantidad de puertos bloqueados

La única acción crítica que el STP toma es el bloqueo de los puertos. Un solo puerto de bloqueo que las transiciones al envío pueden derretir equivocadamente a una parte de grande la red. Una buena manera de limitar el riesgo inherente en el uso del STP es reducir el número de puertos bloqueados tanto cuanto sea posible.

VLA N de la pasa que usted no utiliza

Usted no necesita más de dos links redundantes entre dos Nodos en una red de Bridge. Sin embargo, este tipo de configuración es común:



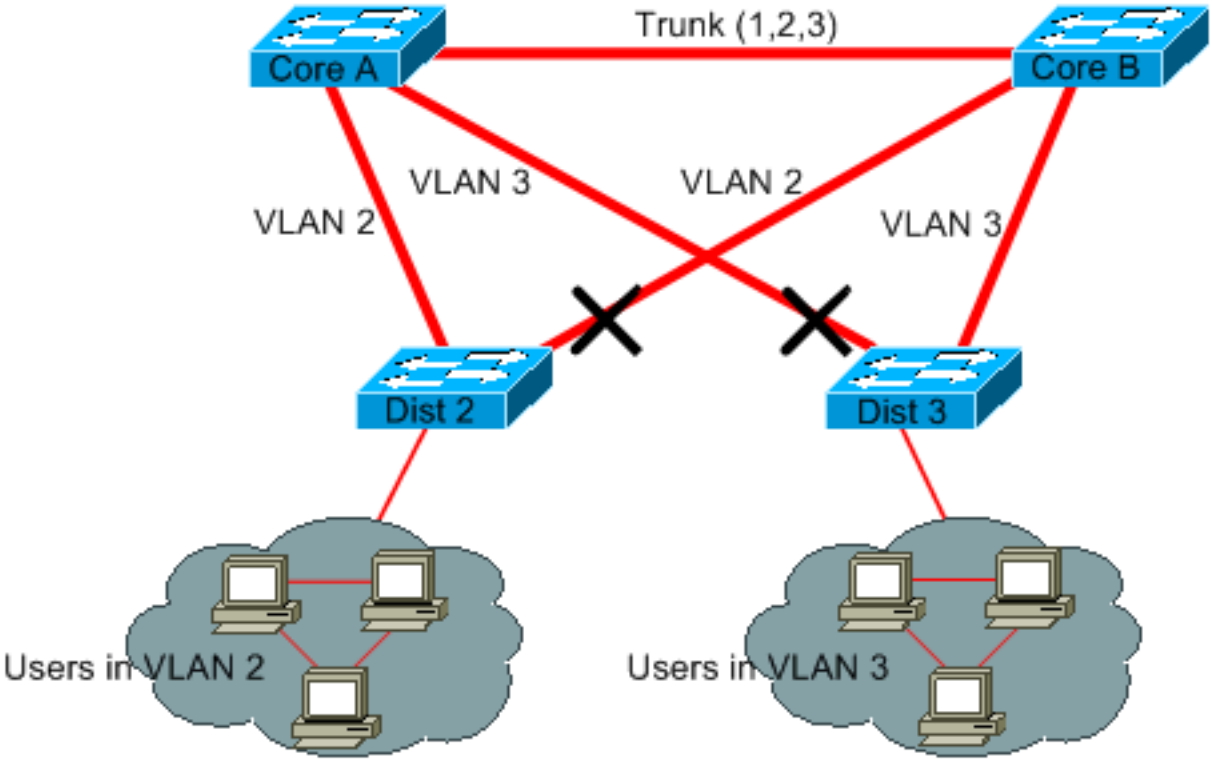
Los switches de distribución están vinculados en forma dual a dos switches de núcleo. Los usuarios que conectan en los switches de distribución están solamente en un subconjunto de los VLA N disponibles en la red. En este ejemplo, los usuarios que conectan en Dist 2 son todos en el VLAN2; Dist 3 conecta solamente a los usuarios en el VLA N 3. por abandono, los trunks lleva todos los VLA N definidos en el dominio del VLAN Trunk Protocol (VTP). Solamente Dist 2 recibe el broadcast innecesario y el tráfico Multicast para el VLAN3, pero también está bloqueando uno

de sus puertos para el VLAN3. El resultado es tres trayectos redundantes entre la base A y la base B. Esta Redundancia da lugar a más puertos bloqueados y a una mayor probabilidad de un loop.

Nota importante: Pode cualquier VLA N que usted no necesite de sus trunks.

El recorte VTP puede ayudar, pero esta clase de característica Plug and play no es necesaria en la base de la red.

En este ejemplo, solamente un VLA N del acceso se utiliza para conectar los switches de distribución con la base:



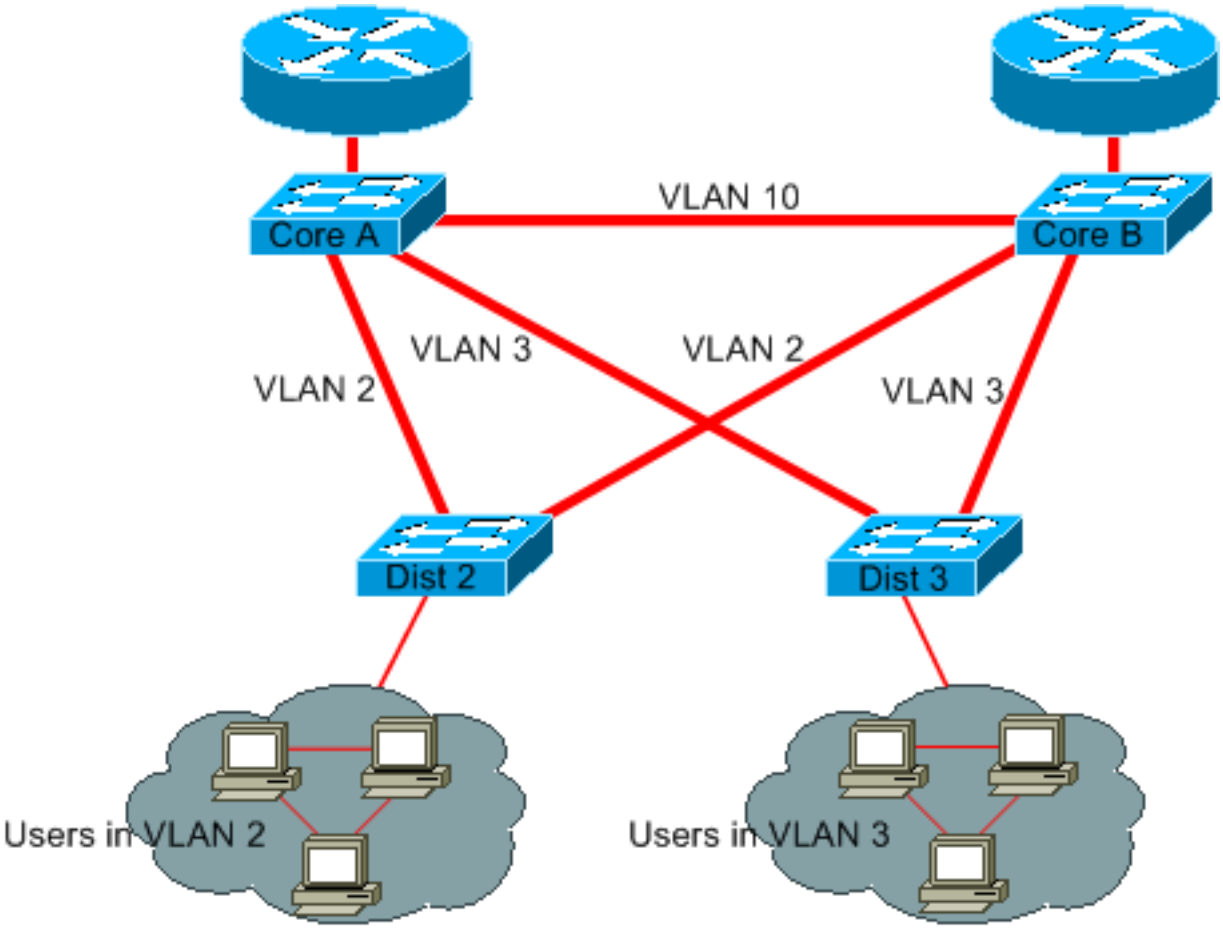
En este diseño, sólo un puerto está bloqueado por cada VLAN. También, con este diseño, usted puede quitar todos los links redundantes en apenas un paso si usted apaga la base A o la base B.

Use la conmutación de Capa 3

El Layer 3 Switching significa rutear aproximadamente a la velocidad de la transferencia. Un router realiza dos funciones principales:

- Un router construye una tabla de reenvío. El router intercambia generalmente la información por los pares por los Routing Protocol.
- Un router recibe los paquetes y adelante los a la interfaz correcta basada en la dirección 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 usted introduce un salto de la encaminamiento y crea una segmentación adicional de la red, no hay penalidad en la velocidad. Este diagrama utiliza el ejemplo en los VLA N de la pasa de la sección que usted no utiliza como base:



Quite el corazón a A y a la base B ahora son algunos switches de la capa 3. El VLAN2 y el VLAN3 se interligan no más entre la base A y la base B, tan allí no es ninguna posibilidad de un STP loop.

- La Redundancia está todavía presente, con una confianza en los Routing Protocol de la capa 3. El diseño asegura un reconvergence que es incluso más rápido que el reconvergence con el STP.
- Hay no más cualquier puerto único que el STP bloquee. Por lo tanto, no hay potencial para un Bridging Loop.
- No existe penalidad de velocidad, ya que abandonar la VLAN 3 mediante conmutación de Capa 3 es tan rápido como realizar una conexión en puente dentro de la VLAN.

Hay una sola desventaja con este diseño. La migración a esta clase de diseño implica generalmente un retrabajo del esquema de direccionamiento.

Guarde el STP incluso si es innecesario

Incluso si usted ha tenido éxito con el retiro de todos los puertos bloqueados de su red y usted no tiene ninguna redundancia física, no inhabilite el STP. El STP no es generalmente muy uso intensivo del procesador; el packet switching no implica el CPU en la mayoría de los switches Cisco. También, los pocos BPDU que se envían en cada link no reducen perceptiblemente el ancho de banda disponible. Sin embargo, una red de Bridge sin el STP puede derretirse en una parte un segundo si un operador hace un error en un panel de conexiones, por ejemplo. Generalmente, inhabilitar el STP en una red de Bridge no está digno del riesgo.

Guarde el tráfico del VLAN administrativo y no tenga un solo palmo del VLA N toda la red

Un switch Cisco tiene típicamente una sola dirección IP que ate a un VLA N, conocida como el VLAN administrativo. En este VLA N, el Switch se comporta como un host IP genérico. Particularmente, cada broadcast o paquete de multidifusión se remite al CPU. Una alta velocidad del broadcast o tráfico Multicast en el VLAN administrativo pueden afectar al contrario el CPU y la capacidad de la CPU de procesar el BPDU vital. Por lo tanto, guarde el tráfico de usuarios del VLAN administrativo.

Hasta hace poco tiempo, no había manera de quitar el VLAN1 de un trunk en la implementación de Cisco. El VLAN1 sirve generalmente como VLAN administrativo, donde está accesible todo el Switches en la misma subred IP. Aunque es útil, esta configuración puede ser peligrosa porque un Bridging Loop en el VLAN1 afecta a todos los trunks, que pueden derribar la red completa. Por supuesto, el mismo problema existe ninguna materia que el VLA N usted utilice. Intente dividir los dominios de Bridging en segmentos con el uso de los 3 Switch de la capa de alta velocidad.

A la Versión 5.4 de CatOS y la versión 12.1(11b)E del software del IOS de Cisco, puede eliminar la VLAN 1 de los troncales. El VLAN1 todavía existe, pero bloquea el tráfico, que previene cualquier posibilidad del loop.

Información Relacionada

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