Mejore el protocolo de árbol de extensión (STP) con protección de raíz

Contenido

Introducción

Este documento describe las funciones mejoradas de protección de raíz STP que mejoran la confiabilidad, manejabilidad y seguridad de la red conmutada.

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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Descripción de la Función

El STP estándar no proporciona ningún medio para que el administrador de la red aplique de forma segura la topología de la red conmutada de Capa 2 (L2). Un medio para aplicar la topología puede ser especialmente importante en redes con control administrativo compartido, donde diferentes entidades administrativas o empresas controlan una red conmutada.

Se calcula la topología de reenvío de la red conmutada. El cálculo se basa en la posición del puente raíz, entre otros parámetros. Cualquier switch puede ser el puente raíz de una red. Sin embargo, una topología de reenvío más óptima coloca el puente raíz en una ubicación predeterminada específica. Con el STP estándar, cualquier puente en la red con un ID de puente inferior asume la función del puente raíz. El administrador no puede imponer la posición del puente raíz.

Nota: El administrador puede establecer la prioridad del puente raíz en 0 en un esfuerzo por asegurar la posición del puente raíz. Pero no hay garantía contra un bridge con una prioridad de 0 y una dirección MAC inferior.

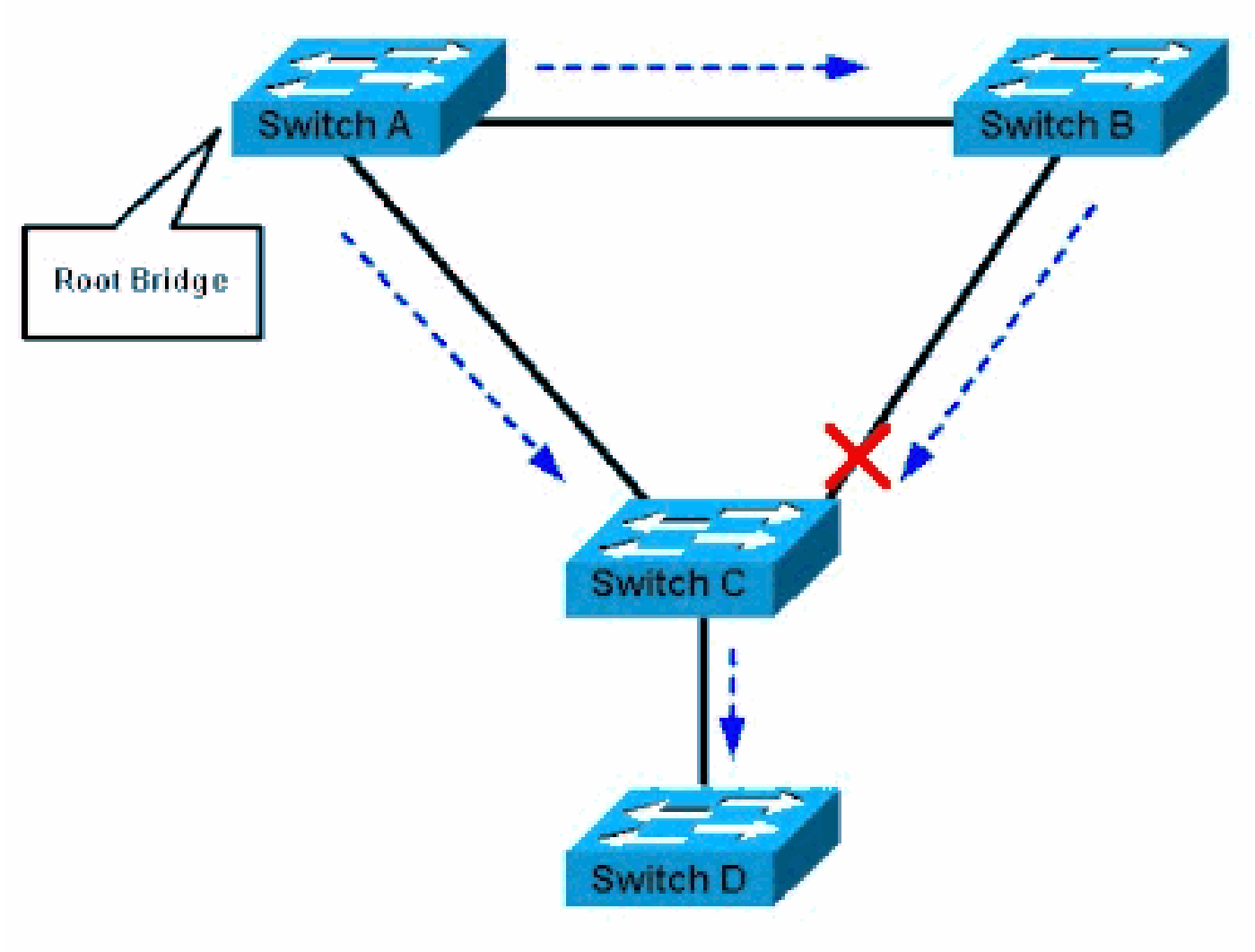
La función de protección de raíz proporciona una manera de asegurar la posición de root bridge en la red.

La protección de raíz se asegura de que el puerto en el que está habilitada la protección de raíz sea el puerto designado. Normalmente, los puertos root bridge son todos puertos designados, a menos que dos o más puertos del root bridge estén conectados. Si el puente recibe Unidades de datos de protocolo de puente STP (BPDU) superiores en un puerto habilitado para protección de raíz, la protección de raíz mueve este puerto a un estado STP incoherente con la raíz. Este estado root-inconsistent es con eficacia igual a un estado de escucha. No se reenvía tráfico a través de este puerto. De esta manera, el protector de raíz aplica la posición del puente de raíz.

El ejemplo de esta sección demuestra cómo un root bridge no autorizado puede causar problemas en la red y cómo el protector de raíz puede ayudar.

En la Imagen 1, los Switches A y B constituyen el núcleo de la red, y A es el puente raíz para una VLAN. Switch C es un layer switch de acceso. El enlace entre B y C está bloqueado en el lado C. Las flechas muestran el flujo de BPDU STP.

Imagen 1

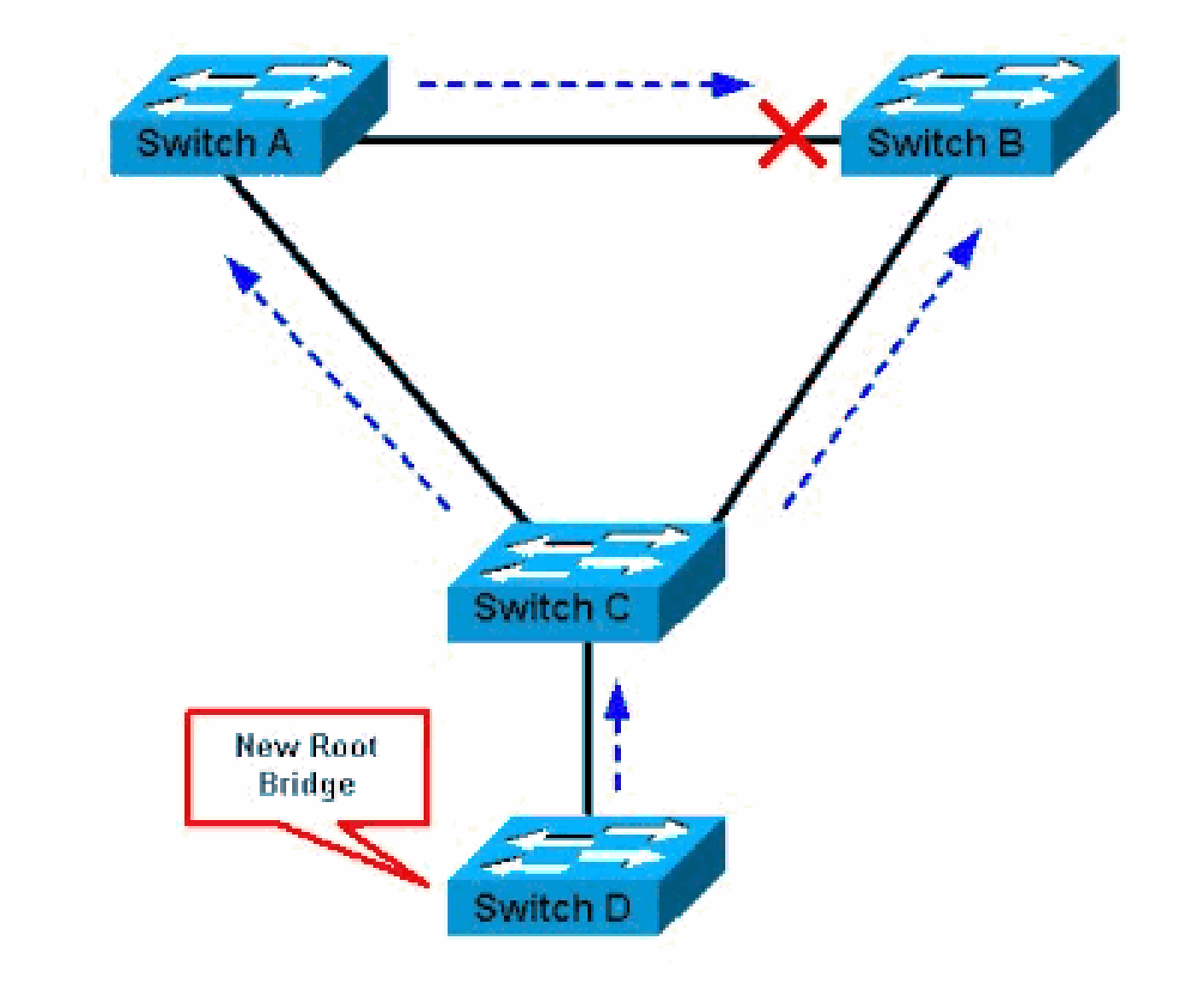


El switch A es un puente raíz

En la Imagen 2, el dispositivo D comienza a participar en STP. Por ejemplo, las aplicaciones de puente basadas en software se inician en PC u otros switches que se conectan a una red de proveedor de servicios. Si la prioridad del puente D es 0 o cualquier valor menor que la prioridad del puente raíz, el dispositivo D se elige como puente raíz para esta VLAN. Si el link entre el dispositivo A y B es de 1 gigabit y los links entre A y C así como entre B y C son de 100 Mbps, la elección de D como root hace que el link Gigabit Ethernet que conecta los dos switches principales se bloquee.

Este bloque hace que todos los datos en esa VLAN fluyan a través de un link de 100 Mbps a través de la capa de acceso. Si más datos fluyen a través del núcleo en esa VLAN de los que este link puede acomodar, se produce la caída de algunas tramas. La caída de tramas provoca una pérdida de rendimiento o una interrupción de la conectividad.

Imagen 2



El switch D es un nuevo puente raíz

La función de protección de raíz protege la red contra estos problemas.

La configuración de la protección de raíz se realiza por puerto. La protección de raíz no permite que el puerto se convierta en un puerto raíz STP, por lo que el puerto siempre está designado por STP. Si llega una mejor BPDU a este puerto, la protección de raíz no tiene en cuenta la BPDU y selecciona una nueva raíz STP. En cambio, la protección de raíz coloca el puerto en el estado STP incoherente con la raíz. Debe habilitar la protección de raíz en todos los puertos en los que no debe aparecer el puente raíz. De alguna manera, puede configurar un perímetro alrededor de la parte de la red donde se puede ubicar la raíz STP.

En la Imagen 2, habilite la protección de raíz en el puerto del Switch C que se conecta al Switch D.

El switch C inImage 2bloquea el puerto que conecta con el switch D, después de que el switch reciba una BPDU superior. La protección de raíz coloca el puerto en el estado STP incoherente con la raíz. Ningún tráfico pasa a través del puerto en este estado. Una vez que el dispositivo D deja de enviar BPDU superiores, el puerto se desbloquea nuevamente. A través de STP, el puerto

pasa del estado de escucha al estado de aprendizaje y, finalmente, pasa al estado de reenvío. La recuperación es automática; no es necesaria la intervención humana.

Este mensaje aparece después de que el protector de raíz bloquee un puerto:

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated in VLAN 77.
Moved to root-inconsistent state
```

Disponibilidad

La protección de raíz está disponible en Catalyst 6500/6000 que ejecuta el software del sistema Cisco IOS®. Esta función se introdujo por primera vez en Cisco IOS Software Release 12.0(7)XE. Para el Catalyst 4500/4000 que ejecuta el software del sistema Cisco IOS, esta función está disponible en todas las versiones.

Para los switches Catalyst 2900XL y 3500XL, la protección de raíz está disponible en Cisco IOS Software Release 12.0(5)XU y posteriores. Los switches Catalyst de la serie 2950 admiten la función de protección de raíz en Cisco IOS Software Release 12.0(5.2)WC(1) y posteriores. Los switches Catalyst de la serie 3550 soportan la función de protección de raíz en Cisco IOS Software Release 12.1(4)EA1 y posteriores.

Esta función también está disponible en los nuevos switches de la serie Catalyst de Cisco.

Configuración

Configuración del software Cisco IOS para Catalyst 6500/6000 y Catalyst 4500/4000

En los switches Catalyst 6500/6000 o Catalyst 4500/4000 que ejecutan el software del sistema Cisco IOS, ejecute este conjunto de comandos para configurar la protección de raíz STP:

```
<#root>

Switch#

configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
!
Switch#(config)#

interface fastethernet 3/1

Switch#(config-if)#

spanning-tree guard root

!
```

Nota: Cisco IOS Software Release 12.1(3a)E3 para Catalyst 6500/6000 que ejecuta Cisco IOS system software cambió este comando de spanning-tree rootguard a spanning-tree guard root. El Catalyst 4500/4000 que ejecuta el software del sistema Cisco IOS utiliza el comando spanning-tree guard root en todas las versiones.

Configuración del software Cisco IOS para Catalyst 2900XL/3500XL, 2950 y 3550

En el Catalyst 2900XL, 3500XL, 2950 y 3550, configure los switches con protección de raíz en el modo de configuración de la interfaz, como se muestra en este ejemplo:

<#root>

```
Switch#

configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#

interface fastethernet 0/8

Switch(config-if)#

spanning-tree rootguard

Switch(config-if)#

^Z

*Mar 15 20:15:16: %SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Rootguard enabled on
port FastEthernet0/8 VLAN 1.

Switch#
```

¿Cuál es la diferencia entre seguridad STP BPDU y seguridad raíz STP

La protección BPDU y la protección de raíz son similares, pero su impacto es diferente. La protección BPDU deshabilita el puerto con la recepción de BPDU si portfast se encuentra activado en el puerto. La inhabilitación niega efectivamente la participación en STP a los dispositivos detrás de tales puertos. Debe volver a habilitar manualmente el puerto que se pone en estado errdisable o configurar errdisable-timeout .

La protección de raíz permite que el dispositivo participe en STP mientras el dispositivo no intente convertirse en la raíz. Si el protector de raíz bloquea el puerto, la recuperación posterior es automática. La recuperación ocurre tan pronto como el dispositivo desviado deja de enviar BPDU superiores.

Para obtener más información sobre la protección BPDU, vea Mejora de la protección BPDU

PortFast del árbol de expansión.

¿Ayuda la protección de raíz con el problema de las dos raíces?

Puede haber una falla de link unidireccional entre dos puentes en una red. Debido a la falla, un bridge no recibe las BPDU del bridge root. Con tal falla, el switch root recibe las tramas que otros switches envían, pero los otros switches no reciben las BPDU que envía el switch root. Esto puede llevar a un loop STP. Debido a que los otros switches no reciben ninguna BPDU de la raíz, estos switches creen que son la raíz y comienzan a enviar BPDU.

Cuando el puente raíz real comienza a recibir BPDU, la raíz descarta las BPDU porque no son superiores. El puente raíz no cambia. Por lo tanto, la protección de raíz no ayuda a resolver este problema. Las funciones de detección de link unidireccional (UDLD) y de protección contra loops resuelven este problema.

Para obtener más información sobre los escenarios de falla de STP y cómo solucionarlos, vea Problemas del Spanning Tree Protocol y Consideraciones de Diseño Relacionadas.

Información Relacionada

- Comprenda y configure la función del protocolo UDLD
- Recuperar el estado de puerto errDisable en plataformas Cisco IOS
- 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).