Comprender la mejora de la protección PortFast BPDU del árbol de expansión

Contenido

Introducción

Este documento describe la función de mejora de la protección de la Unidad de Datos del Protocolo PortFast Bridge Protocol (BPDU) del Protocolo de árbol de expansión (STP).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Estas versiones de software presentaron a la protección STP PortFast BPDU:

- Versión 5.4.1 del software Catalyst OS (CatOS) para las plataformas Catalyst 4500/4000 (Supervisor Engine II), 5500/5000, 6500/6000, 2926, 2926G, 2948G y 2980G

- Cisco IOS® Software Release 12.0(7)XE para las plataformas Catalyst 6500/6000
- Cisco IOS Software Release 12.1(8a)EW para Catalyst 4500/4000 Supervisor Engine III
- Cisco IOS Software Release 12.1(12c)EW para Catalyst 4500/4000 Supervisor Engine IV
- Cisco IOS Software Release 12.0(5)WC5 para Catalyst series 2900XL y 3500XL
- Cisco IOS Software Release 12.1(11)AX para los switches Catalyst serie 3750
- Cisco IOS Software Release 12.1(14)AX para los switches Catalyst 3750 Metro
- Cisco IOS Software Release 12.1(19)EA1 para switches Catalyst serie 3560
- Cisco IOS Software Release 12.1(4)EA1 para los switches Catalyst serie 3550
- Cisco IOS Software Release 12.1(11)AX para los switches Catalyst serie 2970
- Cisco IOS Software Release 12.1(12c)EA1 para los switches Catalyst serie 2955
- Cisco IOS Software Release 12.1(6)EA2 para los switches Catalyst serie 2950
- Cisco IOS Software Release 12.1(11)EA1 para los switches Catalyst 2950 Long-Reach Ethernet (LRE)
- Cisco IOS Software Release 12.1(13)AY para los switches serie Catalyst 2940

Nota: La protección PortFast BPDU STP no está disponible para los switches Catalyst serie 8500, 2948G-L3 o 4908G-L3.

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 el documento Cisco Technical Tips Conventions (Convenciones sobre consejos técnicos de Cisco) para obtener más información sobre las convenciones de los documentos.

Antecedentes

Este documento explica la función de protección de la Unidad de Datos del PortFast Bridge Protocol (BPDU). Esta función es una de las mejoras del Spanning-Tree Protocol (STP) que Cisco creó. Esta función aumenta la confiabilidad, la capacidad de gestión, y la seguridad de la red de switch.

Descripción de la Función

ESTP configura una topología de interconexión en una topología similar a un árbol sin loop. Cuando se activa el link en un puerto de bridge, se realiza un cálculo STP en ese puerto. El resultado del cálculo es la transición del puerto en el estado de reenvío o bloqueo. El resultado depende de la posición del puerto en la red y los parámetros STP. Este cálculo y periodo de transición suele durar de 30 a 50 segundos. En ese momento, los datos del usuario no pasan a través del puerto. Algunas aplicaciones de usuario pueden agotar el tiempo de espera durante este período.

Para permitir la transición inmediata del puerto al estado de reenvío, habilite la función Portfast STP. PortFast cambia el puerto al modo de reenvío STP inmediatamente al establecer un link. El puerto todavía participa en el STP. Por consiguiente, si el puerto forma parte de un loop, este cambia finalmente al modo de bloqueo STP.

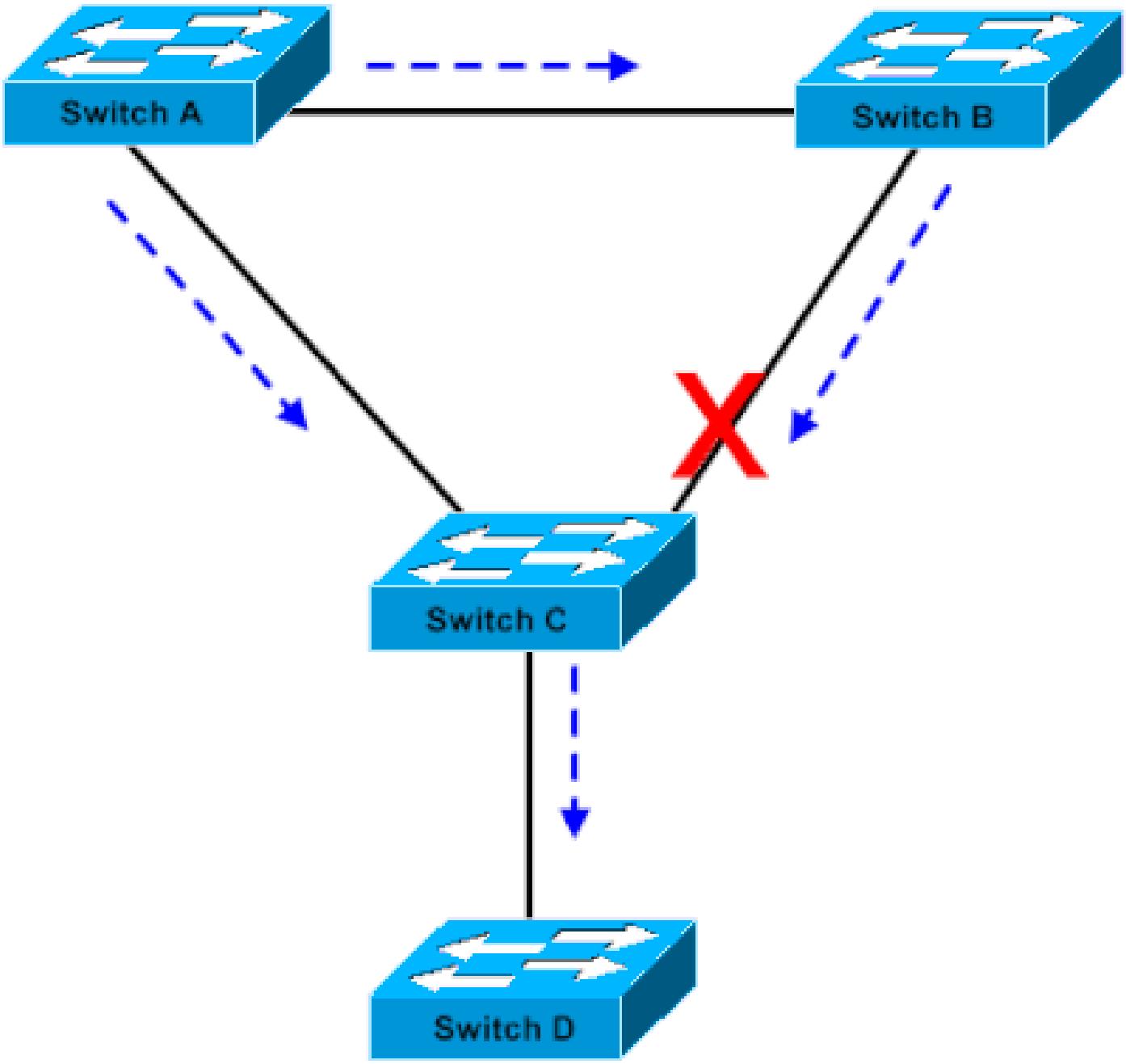
Mientras el puerto participa en STP, es posible que algunos dispositivos asuman la función de root bridge y afecten a la topología STP activa. Para asumir la función de bridge raíz, el dispositivo debería estar conectado al puerto y ejecutar STP con una prioridad de bridge menor que la del bridge root bridge. Si otro dispositivo asume la función de root bridge de esta manera, convierte la red en subóptima. Se trata de una forma simple de ataque de negación de servicio (DoS) en la red. La introducción temporal y la retirada posterior de dispositivos STP con una prioridad de bridge baja (0) provocan un cálculo nuevo de STP permanente.

La ampliación de la seguridad en BPDU Portfast STP está creada para permitirles a los diseñadores de red imponer los límites de dominio STP y mantener predecible la topología activa. Los dispositivos situados detrás de los puertos que tienen PortFast SPT habilitado no tienen capacidad para influir en la topología STP. En el momento de la recepción de BPDU, la función de protección de BPDU inhabilita el puerto que tiene configurado PortFast. La protección de BPDU cambia el puerto al estado errdisable y aparece un mensaje en la consola. Este mensaje es un ejemplo:

```
2000 May 12 15:13:32 %SPANTREE-2-RX_PORTFAST:Received BPDU on PortFast enable port.
Disabling 2/1
2000 May 12 15:13:32 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
```

Tenga en cuenta este ejemplo:

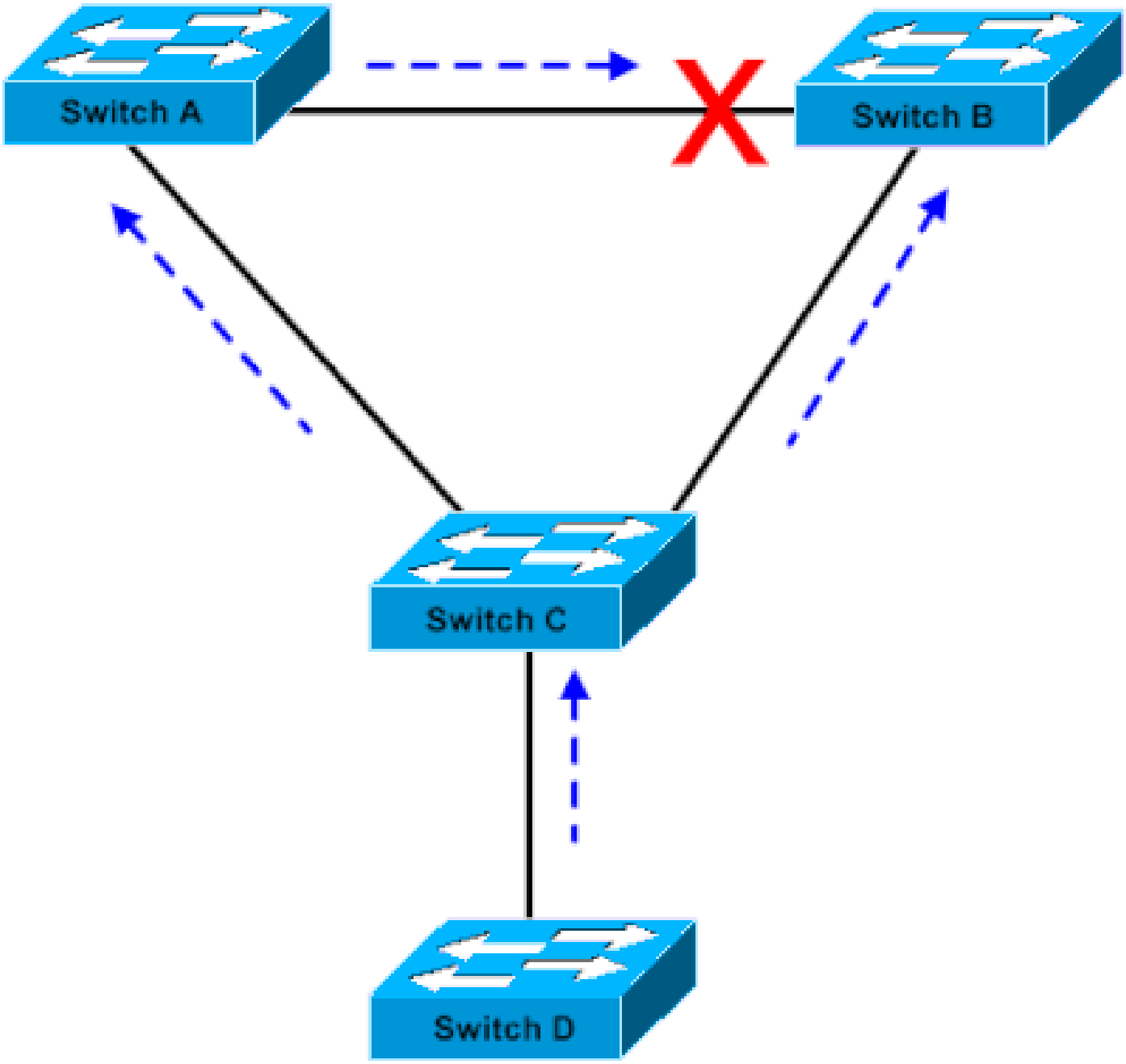
Figure 1



Conexión de puente

El bridge A tiene la prioridad 8192 y es el root bridge para la VLAN. El bridge B tiene prioridad 16384 y es el root bridge de respaldo para la misma VLAN. Los bridges A y B, conectados por un link Gigabit Ethernet, constituyen un núcleo de la red. El bridge C es un switch de acceso y tiene configurado PortFast en el puerto conectado al dispositivo D. Si los demás parámetros STP son los predeterminados, el puerto del bridge C conectado al bridge B está en el estado de bloqueo STP. El dispositivo D (PC) no participa en STP. Las flechas con guiones indican el flujo de los BPDU de STP.

Figure 2



La aplicación de puente basada en Linux se inicia en un PC

En la Figura 2, el dispositivo D ha empezado a participar en STP. Por ejemplo, se inicia una aplicación de bridge basada en Linux en un PC. Si la prioridad del puente de software es 0 o cualquier valor menor que la prioridad del puente raíz, el puente de software asume la función del puente raíz. El link Gigabit Ethernet, que conecta a los dos switches principales, cambia al modo de bloqueo. La transición hace que todos los datos en esa VLAN fluyan a través del link de 100 Mbps. Si hay más datos que fluyen a través del núcleo en la VLAN que los que el link puede almacenar, se descartan algunas tramas. Como consecuencia, tiene lugar una interrupción de la conectividad.

La función de protección PortFast BPDU STP evita que ocurra esta situación. Esta función inhabilita el puerto en cuanto el bridge C recibe las BPDU STP del dispositivo D.

Configuración

La protección Portfast BPDU STP puede habilitarse o inhabilitarse globalmente, lo que afecta a todos los puertos que tienen PortFast configurado. De forma predeterminada, la protección BPDU STP está inhabilitada. Ejecute el siguiente comando para habilitar la protección PortFast BPDU STP en el switch:

Comando de CatOS

<#root>

```
Console> (enable)
set spantree portfast bpdu-guard enable

Spantree portfast bpdu-guard enabled on this switch.
Console> (enable)
```

Comando de software de Cisco IOS®

<#root>

```
CatSwitch-IOS(config)#
spanning-tree portfast bpduguard
CatSwitch-IOS(config)
```

Cuando el puerto está deshabilitado por la protección STP BPDU, permanece en estado deshabilitado, a menos que se active manualmente. Puede configurar un puerto para que se habilite de nuevo por sí mismo de forma automática desde el estado errdisable. Ejecute estos comandos, que determinan elintervalo errdisable-timeout y habilitan la función tiempo de espera:

Comandos CatOS

<#root>

```
Console> (enable)
set errdisable-timeout interval 400

Console> (enable)
set errdisable-timeout enable bpdu-guard
```

Comandos del Cisco IOS Software

<#root>

```
CatSwitch-IOS(config)#
errdisable recovery cause bpduguard

CatSwitch-IOS(config)#
errdisable recovery interval 400
```

Nota: El intervalo de tiempo de espera predeterminado es de 300 segundos y, de forma predeterminada, la función de tiempo de espera está desactivada.

Monitor

Para verificar si la función está habilitada o inhabilitada, ejecute el siguiente comando aplicable.

Resultado del Comando

Comando de CatOS

<#root>

```
Console> (enable)
show spantree summary
Root switch for vlans: 3-4.
Portfast bpdu-guard enabled for bridge.

Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

Summary of Connected Spanning Tree Ports By VLAN:

Vlan  Blocking Listening Learning Forwarding STP Active

----- -------- --------- -------- ---------- ----------

   1         0         0        0          1          1

   3         0         0        0          1          1

   4         0         0        0          1          1

  20         0         0        0          1          1
```

```
Blocking Listening Learning Forwarding STP Active

----- -------- --------- -------- ---------- ----------

Total        0         0        0          4          4

Console> (enable)
```

Comando del Software Cisco IOS

<#root>

```
CatSwitch-IOS#

show spanning-tree summary totals

Root bridge for: none.

PortFast BPDU Guard is enabled

UplinkFast is disabled
BackboneFast is disabled
Spanning tree default pathcost method used is short


Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
  1 VLAN                  0         0         0          1          1

CatSwitch-IOS#
```

Información Relacionada

- Asistencia técnica 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).