Comprensión de las Funciones de STP Loop Guard y UDLD

Contenido

Introducción

Este documento describe las funciones del Spanning Tree Protocol que están diseñadas para mejorar la estabilidad de la red de Capa 2.

Prerequisites

Requirements

Este documento asume que el lector está familiarizado con el funcionamiento básico de STP. Consulte Comprensión y Configuración del Spanning Tree Protocol (STP) en Switches Catalyst para obtener más información.

Componentes Utilizados

Este documento se basa en switches Catalyst, sin embargo la disponibilidad de las funciones descritas puede depender de la versión de software utilizada.

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.

Antecedentes

Spanning-Tree Protocol (STP) resuelve físicamente las topologías redundantes en topologías de árbol sin loop. El mayor problema con el STP es que algunos errores de hardware pueden hacerlo fallar. Este error crea forwarding loops (o STP loops). Los loops STP causan importantes interrupciones de red.

Este documento describe la función STP de protección contra loops diseñada para mejorar la estabilidad de las redes de Capa 2. Este documento también describe la detección de desviación de la Unidad de datos de protocolo de puente (BPDU). La detección de desviación de BPDU es una función de diagnóstico que genera mensajes syslog cuando las BPDU no se reciben a tiempo.

Disponibilidad de funciones

IOS de Cisco

- La función de protección contra loops STP se introdujo en Cisco IOS® Software Release 12.1(12c)EW para los switches Catalyst 4500 y Cisco IOS Software Release 12.1(11b)EX para Catalyst 6500.

Funciones de puerto STP

Internamente, STP asigna a cada puerto de puente (o switch) un rol basado en la configuración, la topología, la posición relativa del puerto en la topología y otras consideraciones. El rol del puerto define el comportamiento del puerto desde el punto de vista STP. Según la función de puerto, el puerto envía o recibe BPDU STP y reenvía o bloquea el tráfico de datos. Esta lista proporciona un breve resumen de cada función de puerto STP:

- Designado: se selecciona un puerto designado por enlace (segmento). El puerto designado es el puerto más cercano al puente raíz. Este puerto envía BPDU en el link (segmento) y reenvía el tráfico hacia el puente raíz. En una red convergente STP, cada puerto designado se encuentra en el estado de reenvío STP.

- Raíz: el puente sólo puede tener un puerto raíz. El puerto raíz es el puerto que conduce al puente raíz. En una red convergente STP, el puerto raíz se encuentra en el estado de reenvío STP.

- Alternar: los puertos alternativos conducen al puente raíz, pero no son puertos raíz. Los puertos alternativos mantienen el estado bloqueado del STP.

- Copia de seguridad: se trata de un caso especial en el que dos o más puertos entre los mismos switches están conectados entre sí, directamente o a través de medios compartidos. En este caso, se designa un puerto y el resto de los puertos se bloquean. La función para este puerto es copia de seguridad.

Loop Guard STP

Descripción de la Función

La función de protección de loop del STP brinda protección adicional contra los loops de reenvío de Capa 2 (loops STP). Un loop de STP se crea cuando un puerto de bloqueo STP en las transiciones erróneas de una topología redundante al estado de reenvío. Esto sucede generalmente porque uno de los puertos de una topología redundante (no no necesariamente el puerto de bloqueo STP) recibe físicamente no más de BPDU de STP. En su operación, el STP está basado en la transmisión o en la recepción continua de las BPDU, según el rol del puerto. El puerto designado transmite los BPDU, y el puerto no designado recibe los BPDU.

Cuando uno de los puertos en una topología físicamente redundante deja de recibir BPDU, el STP considera a la topología como un loop libre. Finalmente, se designa el puerto de bloqueo del puerto de respaldo o alternativo y pasa al estado de reenvío. Esta situación crea un loop.

La función de protección de loop hace verificaciones adicionales. Si ya no se reciben las BPDU en un puerto no designado y el protector de loop está habilitado, ese puerto será desplazado a un estado de bloqueo incoherente con el loop en lugar de desplazarse a un estado de escuchar/aprender/reenviar. Sin la función de protección de loop, el puerto asumiría el rol de puerto designado. El puerto se desplaza al estado de reenvío de STP y crea un loop.

Cuando la protección contra loops bloquea un puerto inconsistente, se registra este mensaje:

- IOS de Cisco

```
%SPANTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port FastEthernet0/24 on VLAN0050.
```

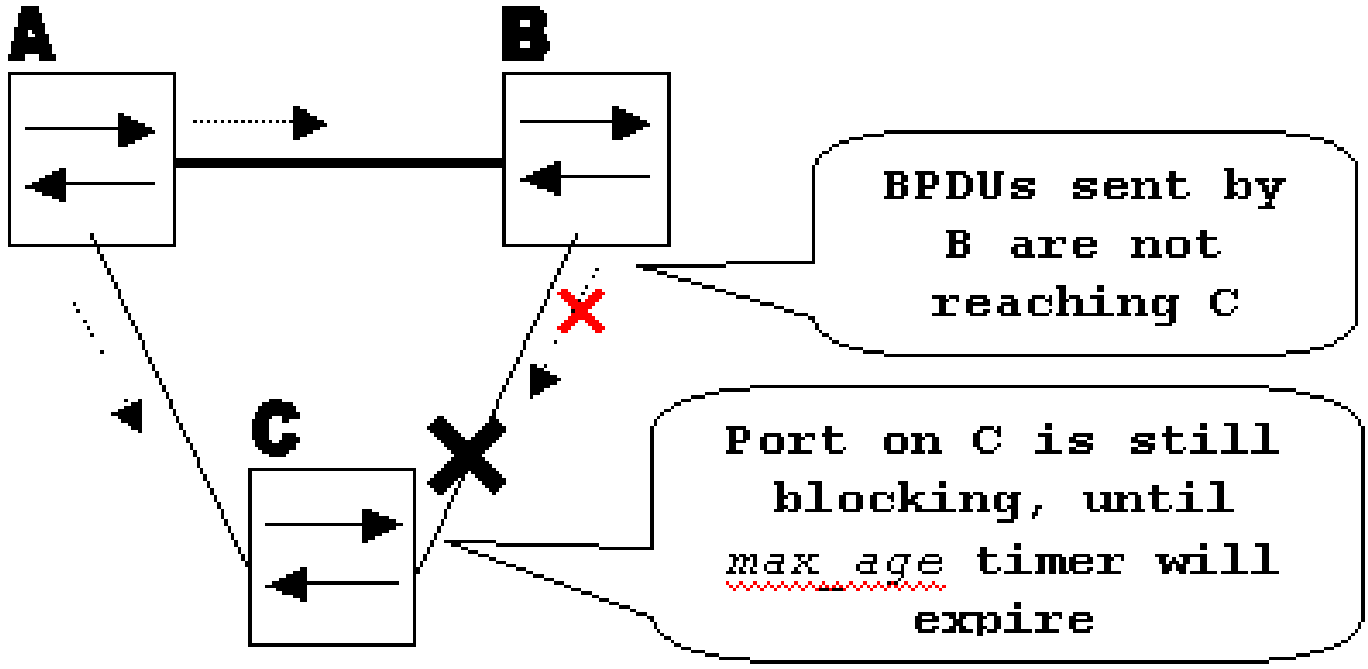
Una vez que se recibe la BPDU en un puerto en un estado STP incoherente con el loop, el puerto pasa a otro estado STP. Para la BPDU recibida, esto significa que la recuperación es automática y que la intervención no es necesaria. Después de la recuperación, se registra este mensaje:

- IOS de Cisco

```
%SPANTREE-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port FastEthernet0/24 on VLAN0050.
```

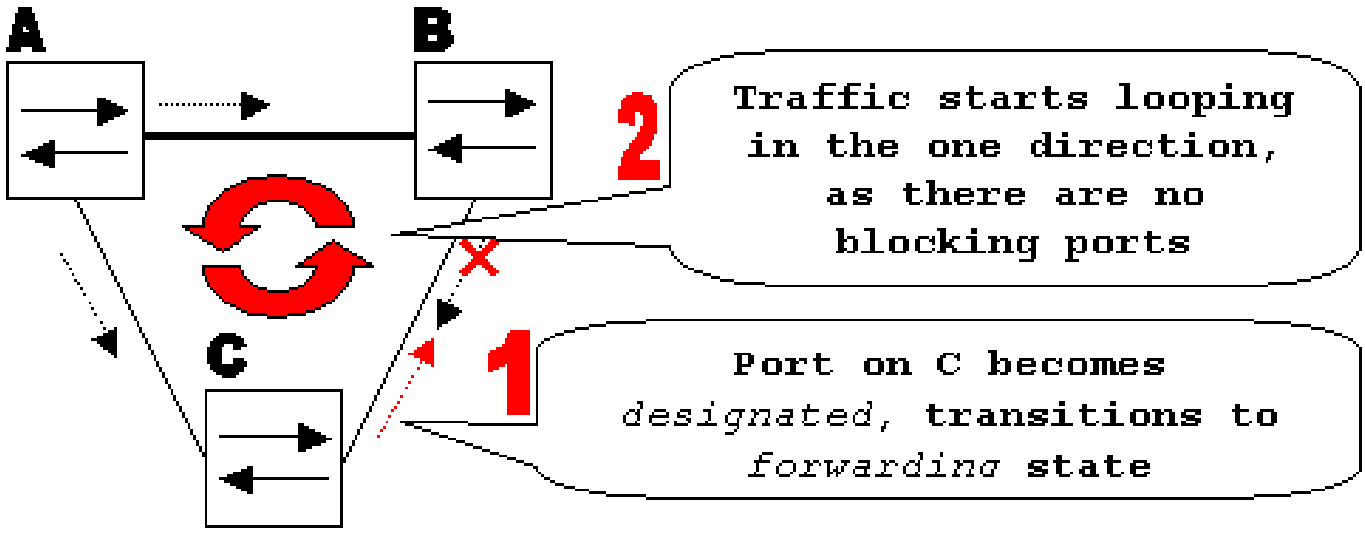
Considere este ejemplo para ilustrar este comportamiento:

El switch A es el switch raíz. El switch C no recibe BPDU del switch B debido a una falla de link unidireccional en el link entre el switch B y el switch C.



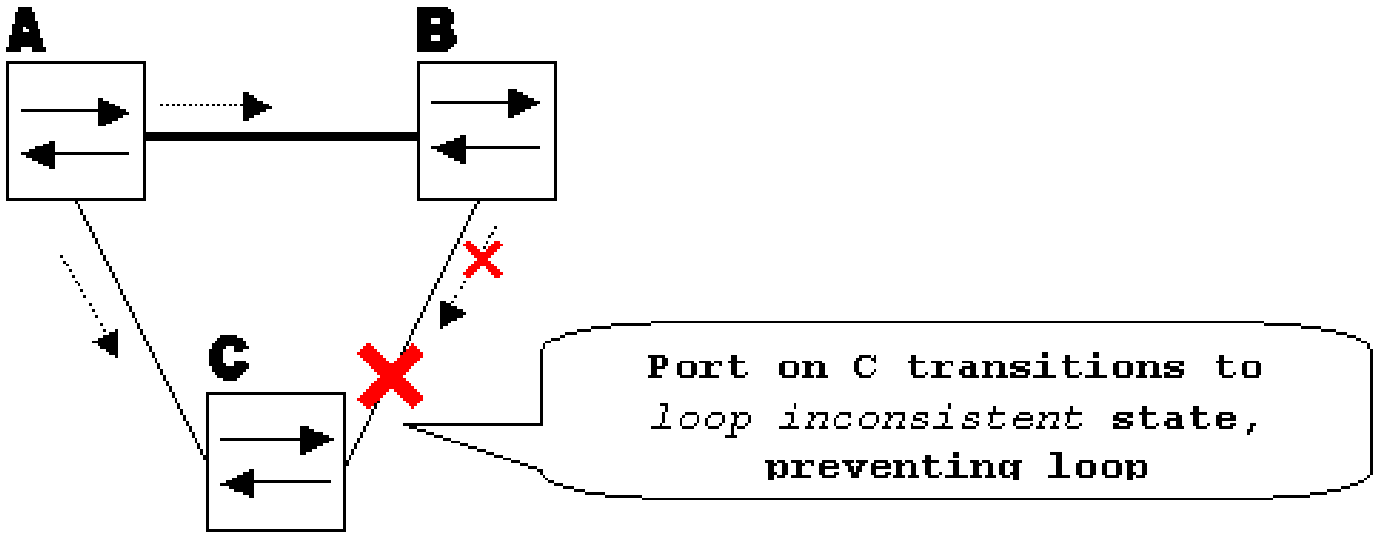
Falla de link unidireccional

Sin protección contra loops, el puerto de bloqueo STP en el switch C pasa al estado de escucha STP cuando el temporizador max_age caduca, y luego pasa al estado de reenvío en dos veces el tiempo forward_delay. Esta situación crea un loop.



Se crea un bucle

Con la protección contra loops habilitada, el puerto de bloqueo en el switch C pasa al estado STP loop-inconsistent cuando caduca el temporizador max_age. Un puerto en estado STP loop-inconsistent no pasa el tráfico de usuario, por lo que no se crea un loop. (El estado loop-inconsistent es efectivamente igual al estado de bloqueo.)



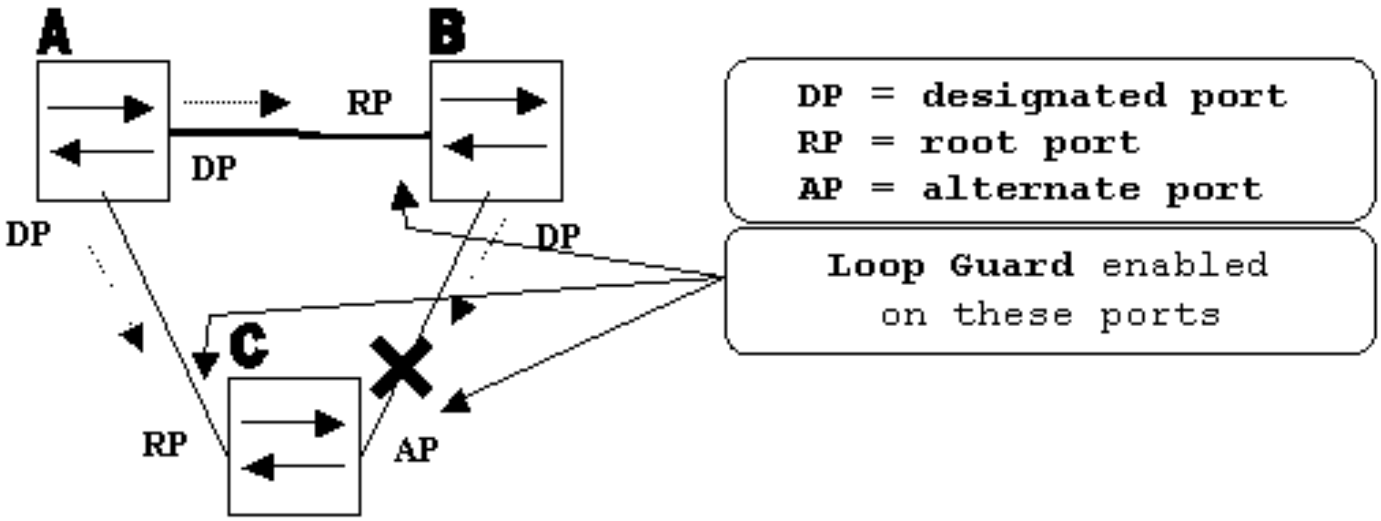
La protección de bucle activada evita el bucle

Consideraciones de Configuración

La función de protección contra loops se habilita por puerto. Sin embargo, mientras bloquee el puerto en el nivel STP, la protección contra loops bloquea los puertos inconsistentes por VLAN (debido al STP por VLAN). Es decir, si las BPDU no se reciben en el puerto trunk para solamente una VLAN determinada, solamente esa VLAN se bloquea (se mueve al estado STP loop-inconsistent). Por la misma razón, si se habilita en una interfaz EtherChannel, el canal completo se bloquea para una VLAN determinada, no sólo para un link (porque EtherChannel se considera como un puerto lógico desde el punto de vista STP).

¿En qué puertos se debe habilitar la protección contra loops? La respuesta más obvia se encuentra en los puertos de bloqueo. Sin embargo, esto no es totalmente correcto. La protección contra loops debe estar habilitada en los puertos no designados (más precisamente, en los puertos raíz y alternativos) para todas las combinaciones posibles de topologías activas. Mientras la protección contra loops no sea una función por VLAN, el mismo puerto (trunk) puede ser designado para una VLAN y no designado para la otra. También se deben considerar los posibles escenarios de failover.

Ejemplo:



Puertos con Protección de Bucle Activada

De forma predeterminada, la protección contra loops está inhabilitada. Este comando se utiliza para habilitar la protección contra loops:

- IOS de Cisco

```
<#root>

spanning-tree guard loop


Router(config)#

interface gigabitEthernet 1/1

Router(config-if)#

spanning-tree guard loop
```

Efectivamente, la protección contra loops se puede habilitar en todos los links punto a punto. El estado dúplex del link detecta el link punto a punto. Si el modo es dúplex completo, el link se considera de punto a punto. Todavía es posible configurar, o invalidar, las configuraciones globales por puerto.

Ejecute este comando para habilitar la protección contra loops globalmente:

- IOS de Cisco

```
<#root>

Router(config)#

spanning-tree loopguard default
```

Ejecute este comando para inhabilitar la protección contra loops:

- IOS de Cisco

```
<#root>

Router(config-if)#

no spanning-tree guard loop
```

Ejecute este comando para inhabilitar globalmente la protección contra loops:

- IOS de Cisco

```
<#root>

Router(config)#

no spanning-tree loopguard default
```

Ejecute este comando para verificar el estado de la protección contra loops:

- IOS de Cisco

```
<#root>

show spanning-tree


Router#

show spanning-tree summary

Switch is in pvst mode
Root bridge for: none
EtherChannel misconfig guard is enabled
Extended system ID           is disabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Pathcost method used         is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
Total                         0         0        0          0          0
```

Protección de Loop frente a UDLD

La funcionalidad de protección contra loops y de detección de link unidireccional (UDLD) se superponen, en parte en el sentido de que ambas protegen contra fallas de STP causadas por links unidireccionales. Sin embargo, estas dos características difieren en funcionalidad y en cómo abordan el problema. Esta tabla describe la funcionalidad de protección contra loops y UDLD:

Funcionalidad	Protección de loop	UDLD
Configuración	Por puerto	Por puerto
Granularidad de acciones	Por VLAN	Por puerto
Recuperación automática	Yes	Sí, con la función err-disable timeout
Protección contra fallas de STP causadas por links unidireccionales	Sí, cuando está habilitado en todos los puertos raíz y alternativos en la topología redundante	Sí, cuando está habilitado en todos los links en la topología redundante
Protección contra fallas de STP causadas por problemas en el software (el switch designado no envía BPDU)	Yes	No
Protección contra cableado incorrecto.	No	Yes

Según las diversas consideraciones de diseño, puede elegir el UDLD o la función de protección contra loops. Con respecto al STP, la diferencia más notable entre las dos funciones es la ausencia de protección en el UDLD contra las fallas del STP causadas por problemas en el software. Como resultado, el switch designado no envía BPDU. Sin embargo, este tipo de falla es (por un orden de magnitud) menos frecuente que las fallas causadas por links unidireccionales. A cambio, el UDLD puede ser más flexible en el caso de links unidireccionales en EtherChannel. En este caso, el UDLD inhabilita solamente los links fallidos, y el canal puede permanecer funcional con los links que permanecen. En tal falla, el protector de loop lo pone en estado loop-inconsistent para bloquear todo el canal.

Además, la protección contra loop no funciona en links compartidos o en aquellas situaciones en las que el link ha sido unidireccional desde la activación del link. En el último caso, el puerto nunca recibe BPDU y se designa. Debido a que este comportamiento podría ser normal, este caso en particular no está cubierto por la protección contra loops. UDLD proporciona protección contra este tipo de escenario.

Como se ha descrito, el nivel más alto de protección se proporciona cuando se habilita el UDLD y la protección contra loops.

Interoperabilidad de Loop Guard con otras características de STP

Protección de raíz

El protector de raíz es mutuamente excluyente con el protector de loop. La protección de raíz se utiliza en los puertos designados y no permite que el puerto se convierta en no designado. La

protección contra loops funciona en los puertos no designados y no permite que el puerto sea designado a través del vencimiento de max_age. El protector de raíz no puede estar habilitado en el mismo puerto que el protector de loop. Cuando la protección contra loops está configurada en el puerto, inhabilita la protección contra loops configurada en el mismo puerto.

link ascendente rápido y Estructura básica rápida

Tanto el link ascendente rápido como la estructura básica rápida son transparentes para el protector de loop. Cuando max_age es omitido por backbone fast en el momento de la reconvergencia, no activa la protección contra loops. Para obtener más información sobre uplink fast y backbone fast, consulte estos documentos:

- Comprensión y Configuración de la Función UplinkFast de Cisco
- Comprensión y configuración de Backbone Fast en switches Catalyst

PortFast y Protección BPDU y VLAN dinámica

La protección contra loops no se puede habilitar para los puertos en los que portfast está habilitado. Dado que la protección BPDU funciona en los puertos habilitados para portfast, se aplican algunas restricciones a la protección BPDU. La protección contra loops no se puede habilitar en los puertos VLAN dinámicos ya que estos puertos tienen portfast habilitado.

links compartidos

La protección contra loops no debe estar habilitada en links compartidos. Si habilita la protección contra loops en los links compartidos, el tráfico de los hosts conectados a los segmentos compartidos se puede bloquear.

Árbol de expansión múltiple (MST)

La protección contra loops funciona correctamente en el entorno MST.

Información Relacionada

- Mejore el protocolo de árbol de extensión (STP) con protección de raíz
- Configuración de la función de protocolo UDLD
- Uso de Portfast y otros comandos para solucionar retrasos al iniciar la conectividad de la estación de trabajo
- 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).