Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Definición del problema](#)
[Cómo funciona el protocolo de detección de link unidireccional](#)
[Modos de funcionamiento del UDLD](#)
[Disponibilidad](#)
[Configuración y control](#)
[Información Relacionada](#)

Introducción

Este documento explica cómo el protocolo de detección de link unidireccional (UDLD) puede ayudar a evitar los loops de reenvío y la creación de agujeros negros en el tráfico en las redes conmutadas.

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.

Convenciones

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

Definición del problema

El Protocolo de árbol de expansión (STP) resuelve una topología física redundante en una topología de reenvío similar a un árbol y sin loop.

Para lograrlo, bloquea uno o más puertos. Al bloquear uno o más puertos, no hay loops en la topología de reenvío. STP depende para su funcionamiento de la recepción y transmisión de las Unidades de datos del protocolo de conexión en puente (BPDU). Si el proceso STP que se

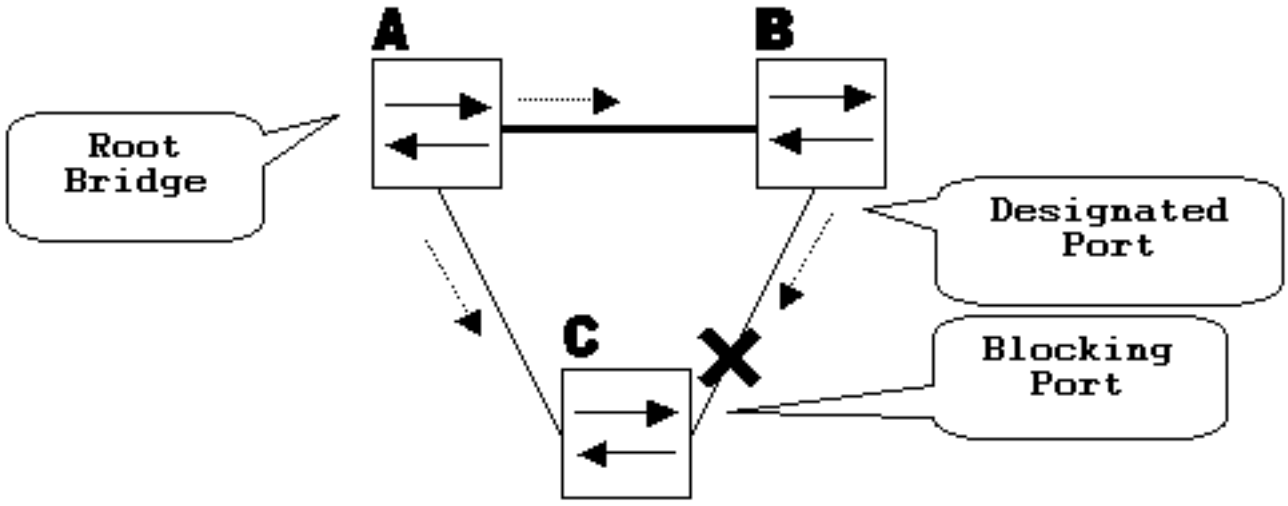
ejecuta en el switch con un puerto de bloqueo deja de recibir las BPDUs de su switch ascendente (designado) en el puerto, el STP finalmente desactualiza la información del STP para el puerto y la pasa al estado de reenvío. Esto crea un loop de reenvío o loop de STP.

Los paquetes inician un ciclo indefinido a lo largo de la trayectoria del loop, y consumen cada vez más ancho de banda. Esto origina una posible interrupción de la red.

¿Cómo es posible que el switch deje de recibir las BPDUs mientras el puerto está en funcionamiento? La razón es el link unidireccional. Un link se considera unidireccional cuando sucede lo siguiente:

- El link funciona en ambos lados de la conexión. El lado local no recibe los paquetes enviados por el sitio remoto mientras que el sitio remoto recibe los paquetes enviados por el lado local.

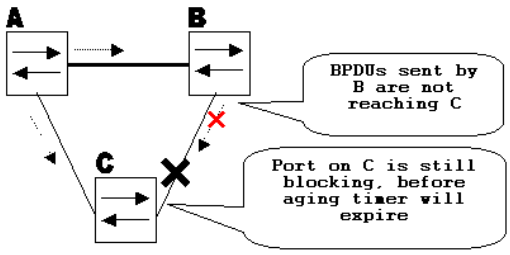
Considere este escenario. Las flechas indican el flujo de los BPDU de STP.



Durante el funcionamiento normal, el bridge B es designado en el link B-C. El bridge B envía las BPDUs al bridge inferior C, que está bloqueando el puerto. El puerto está bloqueado mientras que C detecta las BPDUs de B en ese link.

Ahora, considere qué sucede si el link B-C falla en dirección de C. C deja de recibir el tráfico de B; sin embargo, B todavía recibe el tráfico de C.

C deja de recibir BPDUs en el link B-C, y desactualiza la información recibida con la última BPDU. Este proceso tarda hasta 20 segundos, según el temporizador maxAge STP. Una vez que la información STP se desactualiza en el puerto, dicho puerto pasa del estado de bloqueo al estado de escucha, aprendizaje y, finalmente al estado de reenvío de STP. Esto crea un loop de reenvío, ya que no hay un puerto de bloqueo en el triángulo A-B-C. Los paquetes inician un ciclo a lo largo de la trayectoria (B aún recibe los paquetes de C) y consumen ancho de banda adicional hasta que los links se llenan totalmente. Esto hace que la red se caiga.



Otro problema posible que puede originar un link unidireccional es el filtrado del tráfico.

Cómo funciona el protocolo de detección de link unidireccional

Cisco diseñó e implementó el protocolo UDLD para detectar los links unidireccionales antes de crear el loop de reenvío.

UDLD es un protocolo Capa 2 (L2) que trabaja con los mecanismos de la Capa 1 (L1) para determinar el estado físico de un link. En la Capa 1, la negociación automática se ocupa de la señalización física y de la detección de fallas. El UDLD realiza las tareas que la negociación automática no puede realizar, por ejemplo, detectar las identidades de los vecinos y cerrar los puertos conectados de forma incorrecta. Cuando habilita la negociación automática y el UDLD, las detecciones de la Capa 1 y la Capa 2 trabajan juntas para prevenir las conexiones unidireccionales físicas y lógicas y el malfuncionamiento de otros protocolos.

El UDLD trabaja intercambiando los paquetes del protocolo entre los dispositivos de vecindad. Para que el UDLD funcione, ambos dispositivos en el link deben soportar el UDLD y habilitarlo en los puertos respectivos.

Cada puerto del switch configurado para el UDLD envía los paquetes del protocolo UDLD que contienen el dispositivo /la ID de puerto del puerto, y el dispositivo /IDs de puerto del vecino detectados por el UDLD en ese puerto. Los puertos vecinos deben detectar su propio dispositivo /ID de puerto (eco) en los paquetes recibidos del otro lado.

Si el puerto no detecta su propio dispositivo /ID de puerto en los paquetes UDLD entrantes durante un período específico, el link se considera unidireccional.

Este algoritmo de eco permite la detección de estos problemas:

- El link está activo en ambos lados, sin embargo los paquetes sólo son recibidos por un solo lado.
- Errores de cableado cuando las fibras de recepción y transmisión no están conectadas al mismo puerto en el lado remoto.

Una vez que el link unidireccional es detectado por el UDLD, se inhabilita el puerto respectivo y este mensaje se imprime en la consola:

```
UDLD-3-DISABLE: Unidirectional link detected on port 1/2. Port disabled
```

El cierre de puerto por UDLD permanece inhabilitado hasta que vuelva a habilitarse en forma manual o hasta que errdisable timeout caduque (si está configurado).

Modos de funcionamiento del UDLD

El UDLD puede funcionar en dos modos: normal y agresivo.

En el modo normal, si se determinó que el estado del link del puerto debía ser bidireccional y finaliza el tiempo de espera de la información UDLD, el UDLD no toma ninguna medida. El estado de puerto para el UDLD se marca como indeterminado. El puerto se comporta según su estado STP.

En el modo agresivo, si se determinó que el link del puerto era bidireccional y finaliza el tiempo de espera de la información UDLD mientras que el link en el puerto todavía está activo, el UDLD intenta restablecer el estado del puerto. Si no lo logra, el puerto se coloca en el estado de errdisable.

El envejecimiento de la información UDLD se produce cuando el puerto que ejecuta el UDLD no recibe los paquetes UDLD del puerto vecino durante el tiempo de espera. El tiempo de espera del puerto está determinado por el puerto remoto y depende del intervalo del mensaje del lado remoto. Cuanto más corto sea el intervalo del mensaje, más corto el tiempo de espera y más rápida será la detección. Las implementaciones recientes de UDLD permiten la configuración del intervalo de mensajes.

La información de UDLD puede desactualizarse debido a una tasa de errores alta en el puerto causada por el mismo problema físico o por una discordancia del dúplex. Tal caída de paquete no significa que el link sea unidireccional y que el UDLD en modo normal no inhabilite tal link.

Es importante tener la capacidad de elegir el intervalo de mensaje correcto para asegurar un tiempo de detección apropiado. El intervalo de mensajes debe ser lo suficientemente rápido como para detectar el link unidireccional antes de que se cree el loop de reenvío; sin embargo, no debe sobrecargar el switch CPU. El intervalo de mensajes predeterminado es 15 segundos, y es lo suficientemente rápido para detectar el link unidireccional antes de la creación del loop de reenvío con temporizadores STP predeterminados. El tiempo de detección equivale aproximadamente a tres veces el intervalo del mensaje.

Por ejemplo: $_{\text{Detección}}$ T ~ message_interval x3

Es decir, 45 segundos para el intervalo de mensajes predeterminado de 15 segundos.

Lleva el$_{\text{reconvergence=max_age}}$ T + el forward_delay 2x para el STP el reconverge en caso del Error de link unidireccional. Con los temporizadores predeterminados, se requieren 20+2x15=50 segundos.

Es recomendado para guardar la$_{\text{detección}}$ T < el$_{\text{reconvergence}}$ T eligiendo un intervalo entre mensajes apropiado.

En modo agresivo, una vez que la información ha caducado, UDLD intentará restablecer el estado del link enviando un paquetes a cada segundo durante ocho segundos. Si el estado del link todavía no está determinado, se inhabilita el link.

El modo agresivo agrega la detección adicional de estas situaciones:

- El puerto está atascado (en un lado el puerto no transmite ni recibe; sin embargo, el link está activo en ambos lados).
- El link está activo de un lado e inactivo del otro lado. Este problema puede aparecer en puertos de fibra óptica. Cuando se desenchufa la fibra en el puerto local, el link permanece activo en el lado local. Sin embargo, está inactivo en el lado remoto.

Recientemente, las implementaciones de hardware de la fibra FastEthernet tienen funciones de Indicación de Falla Final (FEFI) para desactivar el link en ambos lados, en estas situaciones. En Gigabit Ethernet, se brinda una función similar por medio de la negociación de links. Los puertos Copper normalmente no tienen este tipo de problemas, ya que utilizan impulsos de link Ethernet para monitorear el link. Es importante mencionar que en ambos casos, no se produce ningún loop de reenvío porque no hay conectividad entre los puertos. Si el link está activo en un lado y

desactivo en el otro, sin embargo, puede producirse el filtrado del tráfico. UDLD agresivo está diseñado para evitar esto.

Disponibilidad

El UDLD está disponible en el modo normal para:

- Catalyst OS Version 5.1.1 y posterior para los switches de las familias Catalyst 4500/4000, 5500/5000, and 6500/6000
- Cisco IOS® Software Release 12.0(5)XU y posterior para los switches Catalyst 2900XL y 3500XL
- Cisco IOS Software Release 12.1(13)AY y posterior para Catalyst 2940 switches
- Cisco IOS Software Release 12.0(5)WC(1) o posterior para Catalyst 2950 switches
- Cisco IOS Software Release 12.1(12c)EA1 o posterior para Catalyst 2955 switches
- Cisco IOS Software Release 12.1(11)AX o posterior para Catalyst 2970 switches
- Cisco IOS Software Release 12.1(4)EA1 o posterior para los Catalyst 3550 switches
- Cisco IOS Software Release 12.1(19)EA1 o posterior para los Catalyst 3560 switches
- Cisco IOS Software Release 12.1(11)AX o posterior para los Catalyst 3750 switches
- Cisco IOS Software Release 12.1(2)E y posterior para los Catalyst 6500/6000 switches que ejecutan Cisco IOS system software
- Cisco IOS Software Release 12.1(8a)EW y posterior para Catalyst 4500/4000 switches que ejecutan Cisco IOS

El modo agresivo se implementa a partir de estas versiones de software:

- Catalyst OS Version 5.4.3 y posterior para los switches de las familias Catalyst 4500/4000, 5500/5000, y 6500/6000
- Cisco IOS Software Release 12.1(3a)E3 y posterior para Catalyst 6500/6000 switches que ejecutan Cisco IOS system software
- Cisco IOS Software Release 12.1(6)EA2 o posterior para los Catalyst 2950 switches
- Cisco IOS Software Release 12.1(12c)EA1 o posterior para Catalyst 2955 switches
- Cisco IOS Software Release 12.1(11)AX o posterior para los Catalyst 2970 switches
- Cisco IOS Software Release 12.1(4)EA1 o posterior para los Catalyst 3550 switches
- Cisco IOS Software Release 12.1(11)AX o posterior para los Catalyst 3750 switches

Configuración y control

Estos comandos detallan la configuración UDLD en los switches de Catalyst que ejecutan CatOS. El UDLD primero debe ser habilitado globalmente (el valor predeterminado se inhabilita) con este comando:

```
Vega> (enable) set udld enableUDLD enabled globally
```

Ejecutar este comando: para verificar si el UDLD está habilitado

```
Vega> (enable) show udldUDLD:  enabledMessage Interval: 15 seconds
```

El UDLD también debe ser habilitado en los puertos necesarios con este comando:

```
Vega> (enable) set udld enable 1/2UDLD enabled on port 1/2
```

Publique el **comando show udld port** para verificar si el UDLD está habilitado o inhabilitado en el

puerto y cuál es el estado del link:

```
Vega> (enable) show udld portUDLD              : enabledMessage Interval   : 15 secondsPort
Admin Status  Aggressive Mode  Link State--------  ------------  ---------------  --------------
-- 1/1      enabled       disabled         undetermined 1/2      enabled       disabled
bidirectional
```

El UDLD agresivo se habilita en cada puerto con el **comando set udld aggressive-mode enable <module/port>**:

```
Vega> (enable) set udld aggressive-mode enable 1/2Aggressive UDLD enabled on port 1/2.Vega>
(enable) show udld port 1/2UDLD              : enabledMessage Interval   : 15 secondsPort
Admin Status  Aggressive Mode  Link State--------  ------------  ---------------  --------------
-- 1/2      enabled       enabled          undetermined
```

Publique este comando para cambiar el intervalo de mensajes:

```
Vega> (enable) set udld interval 10UDLD message interval set to 10 seconds
```

El intervalo puede variar de 7 a 90 segundos y el valor predeterminado es 15 segundos.

Consulte estos documentos para obtener más información sobre la configuración del IOS UDLD:

- Para los switches Catalyst 6500/6000 que ejecutan el Cisco IOS system software, consulte Configuración de UDLD.
- Para los switches Catalyst 2900XLl/3500XL, consulte la sección *Configuración de Detección de Links Unidireccionales en* Configuración de Puertos del Switch.
- Para los Catalyst 2940 switches, consulte Configuración del UDLD.
- Para los switches Catalyst 2950/2955, consulte Configuración del UDLD.
- Para los switches Catalyst 2970, consulte Configuración del UDLD.
- Para los switches Catalyst 3550, consulte la Configuración UDLD.
- Para los switches Catalyst 3560, consulte Configuración del UDLD.
- Para Catalyst 4500/4000 que ejecuta Cisco IOS, consulte Configuración del UDLD.

Información Relacionada

- Soporte de Tecnología de LAN Switching
- Soporte de Producto para Switches de ATM y Catalyst de LAN
- Soporte Técnico y Documentación - Cisco Systems