Configuración de la función de protocolo UDLD

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[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 describe cómo el protocolo de Detección de Link Unidireccional (UDLD) puede ayudar a prevenir loops y anomalías de tráfico en redes conmutadas.

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.

Definición del problema

El protocolo de árbol de extensión (STP) resuelve la topología física redundante en una topología de reenvío tipo árbol sin bucles.

Para ello, bloquea uno o más puertos. Con uno o más puertos bloqueados, 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 en

estado de `bloqueo` no recibe BPDU de su switch ascendente (designado), el STP finalmente desactualiza la información STP para el puerto y la mueve al estado de `reenvío`.

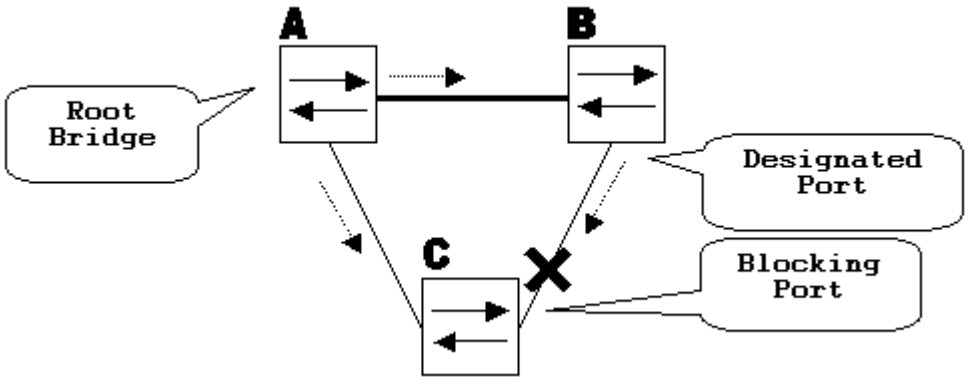
Esto puede crear un loop STP donde los paquetes comienzan a recorrer indefinidamente el trayecto en loop, y consumen más y más ancho de banda y recursos. Esto origina una posible interrupción de la red.

¿Cómo es posible que el switch no reciba BPDU mientras el puerto está `activo`? La razón es un 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 lado remoto mientras que el lado remoto recibe los paquetes enviados por el lado local.

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



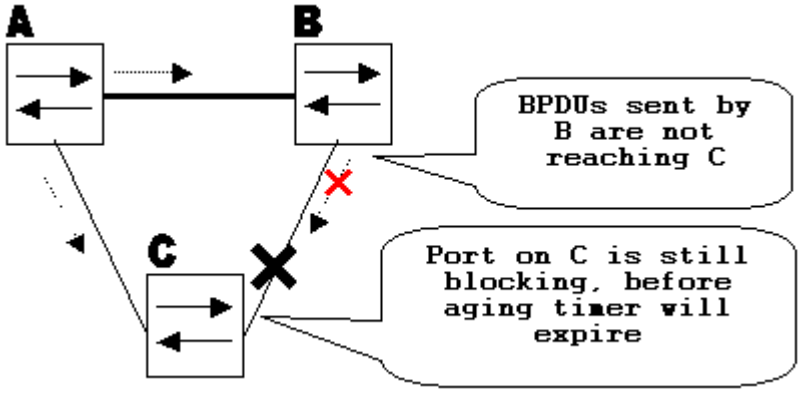
Durante el funcionamiento normal, el puente B es un puerto designado en el link B-C. El puente B envía las BPDU a C, que es el puerto de bloqueo. El puerto está bloqueado mientras que C detecta las BPDUs de B en ese link.

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

en funcionamiento

C no recibe BPDU en el link B-C y envejece la información recibida con la última BPDU. Esto tarda hasta 20 segundos, lo que depende del temporizador STP maxAge. 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, ya que no hay ningún puerto bloqueado en el triángulo A-B-C. Los paquetes recorren el trayecto (B aún recibe paquetes de C) lo que consume ancho de banda adicional hasta que los links se llenan completamente.

Esta situación puede provocar que la red se desactive. Otro posible problema que puede ser causado por un link unidireccional es un agujero negro de tráfico.



Cómo funciona el protocolo de detección de link unidireccional

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. UDLD realiza tareas que la negociación automática no puede realizar, como la detección de las identidades de los vecinos y el cierre de los puertos mal conectados. 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.

UDLD funciona a través del intercambio de paquetes de protocolo entre los dispositivos vecinos. Para que el UDLD funcione, ambos dispositivos en el link deben soportar el UDLD y tenerlo habilitado en los puertos respectivos.

Cada puerto de switch configurado para UDLD envía paquetes de protocolo UDLD que contienen el dispositivo de puerto/ID de puerto, y los ID de dispositivo vecino/puerto vistos por UDLD en ese puerto. Los puertos vecinos ven su propio dispositivo/ID de puerto (echo) 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 conexión (cable) 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 se habilita manualmente, o hasta que caduca el tiempo de espera disabletimeout (si se configura).

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 de acuerdo con 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.

La antigüedad de la información UDLD ocurre cuando el puerto que ejecuta UDLD no recibe 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 será 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 paquetes no significa que el link sea unidireccional y el UDLD en el modo `normal` no inhabilita tal link.

Es importante tener la capacidad de elegir el intervalo de mensaje correcto para asegurar un tiempo de detección apropiado. El intervalo del mensaje 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 la CPU del switch. El intervalo de mensaje predeterminado es de 15 segundos y es lo suficientemente rápido como para detectar el link unidireccional antes de que se cree el loop de reenvío con los temporizadores STP predeterminados. El tiempo de detección equivale aproximadamente a tres veces el intervalo del mensaje.

Por ejemplo: $_{Tdetection}$~ message_interval x3

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

Se necesita $_{Treconvergence}$=max_age + 2x forward_delay para que el STP vuelva a converger en caso de falla de link unidireccional. Con los temporizadores predeterminados, se requieren 20+2x15=50 segundos.

Se recomienda mantener $_{Tdetection}$< $_{Treconvergence}$ y elegir un intervalo de mensajes apropiado.

En el modo `agresivo`, una vez que la información se envejece, el UDLD intenta restablecer el estado del link y enviar paquetes cada segundo durante ocho segundos. Si el estado del link todavía no está determinado, se inhabilita el link.

Aggressivemode agrega 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 observarse en los puertos de fibra cuando la fibra de transmisión está desconectada en el puerto local, el link permanece `activo` en el lado local. Sin embargo, está `inactiva< /tt>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 GigabitEthernet, una función similar es proporcionada por la negociación de link. 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 ocurre ningún loop de reenvío porque no hay conectividad entre los puertos. Sin embargo, si el link está activo en un lado y inactivo en el otro, puede ocurrir un agujero negro de tráfico. UDLD agresivo está diseñado para evitar esto.

Disponibilidad

UDLD está disponible en modo normal y agresivo desde Cisco IOS® Software Release 12 y posteriores.

Configuración y control

Ejecute el comando **show udld** para verificar si el UDLD está habilitado en las interfaces:

<#root>

```
Switch#
```

```
show udld
```

```
Interface Gi1/0/1
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Gi1/0/2
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Gi1/0/3
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown
```

El UDLD agresivo se puede configurar en la interfaz con el **udld port aggressive** comando:

<#root>

```
Switch#
```

```
configure terminal
```

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

```
interface gigabitEthernet1/0/1
```

```
Switch(config-if)#
```

```
udld port aggressive
```

```
Switch(config-if)#
```

```
end
```

```
Switch#
```

Ejecute el comando**show udld**
y **show udld neighbors** para verificar si el UDLD está habilitado o inhabilitado en el puerto y cuál es el estado del link y del vecino:

<#root>

Switch#

show udld GigabitEthernet1/0/1

```
Interface Gi1/0/1
---
Port enable administrative configuration setting: Enabled / in aggressive mode
Port enable operational state:
```

Enabled / in aggressive mode

```
Current bidirectional state:
```

Bidirectional

```
Current operational state: Advertisement - Single neighbor detected
Message interval: 15000 ms
Time out interval: 5000 ms

Port fast-hello configuration setting: Disabled
Port fast-hello interval: 0 ms
Port fast-hello operational state: Disabled
Neighbor fast-hello configuration setting: Disabled
Neighbor fast-hello interval: Unknown


Entry 1
---
Expiration time: 31600 ms
Cache Device index: 1
Current neighbor state:
```

Bidirectional

```
Device ID: 346288238580
Port ID: Gi4/0/1
Neighbor echo 1 device: 70B4F35F080
Neighbor echo 1 port: Gi1/0/1

TLV Message interval: 15 sec
No TLV fast-hello interval
TLV Time out interval: 5
TLV CDP Device name: MXC.TAC.M.02-3850-01
```

<#root>

Switch#

show udld neighbors

```
Port      Device Name    Device ID   Port ID     Neighbor State
----      -----------    ---------   -------     --------------
Gi1/0/1   346288238580   1           Gi4/0/1     Bidirectional

Total number of bidirectional entries displayed: 1
```

Use el comando **udld message time** para cambiar el intervalo de mensajes:

<#root>

```
Switch(config)#
```

udld message time 10

```
UDLD message interval set to 10 seconds
```

El intervalo puede oscilar entre 1 y 90 segundos, con el valor predeterminado de 15 segundos.

Información Relacionada

- Asistencia técnica y descargas de Cisco
- Para los switches Catalyst 3560, consulte Configuración de UDLD.
- Para Catalyst 4500/4000 que ejecuta Cisco IOS, consulte Configuración de UDLD.
- Para los switches Catalyst 9300, consulte Cómo Configurar el UDLD
- Para los switches Catalyst 9500, consulte Cómo Configurar el UDLD

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).