# Compreendendo e configurando o recurso do protocolo de detecção de enlace unidirecional

## Índice



## Introdução

Este documento explica como o protocolo UDLD pode ajudar a evitar loops de encaminhamento e blackholing de tráfego em redes comutadas.

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

### Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

### Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

## Definição do problema

O Protocolo STP resolve a topologia física redundante em uma topologia de encaminhamento semelhante a árvore sem circuitos.

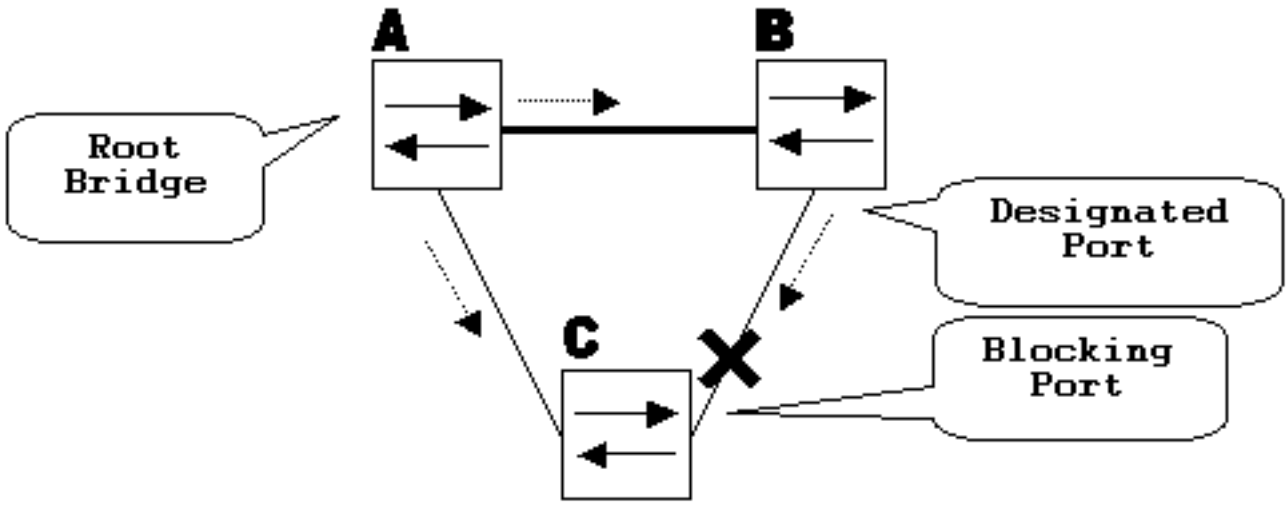
Isso é feito com o bloqueio de uma ou mais portas. Com o bloqueio de uma ou mais portas, não há nenhum loop na topologia da transmissão. A operação do STP depende de recepção e transmissão de BPDUs (Unidades de Dados de Protocolo de Ponte). Se o processo STP que é executado no switch com uma porta bloqueada parar de receber BPDUs de seu switch de upstream (designado) na porta, o STP eventualmente envelhecerá as informações de STP para a porta e irá movê-la para o estado de encaminhamento. Isso cria um loop de encaminhamento ou loop de STP.

Os pacotes entram em um ciclo indefinidamente ao longo caminho em loop, consumindo cada vez mais largura de banda. Isso leva a uma possível interrupção da rede.

Como é possível para o switch parar de receber BPDUs quando a porta está ativada? O motivo é o enlace unidirecional. Um link é considerado unidirecional quando:

- O enlace está ativado em ambos os lados da conexão. O lado local não está recebendo os pacotes enviados pelo lado remoto, ao passo que o lado remoto recebe os pacotes enviados pelo lado local.

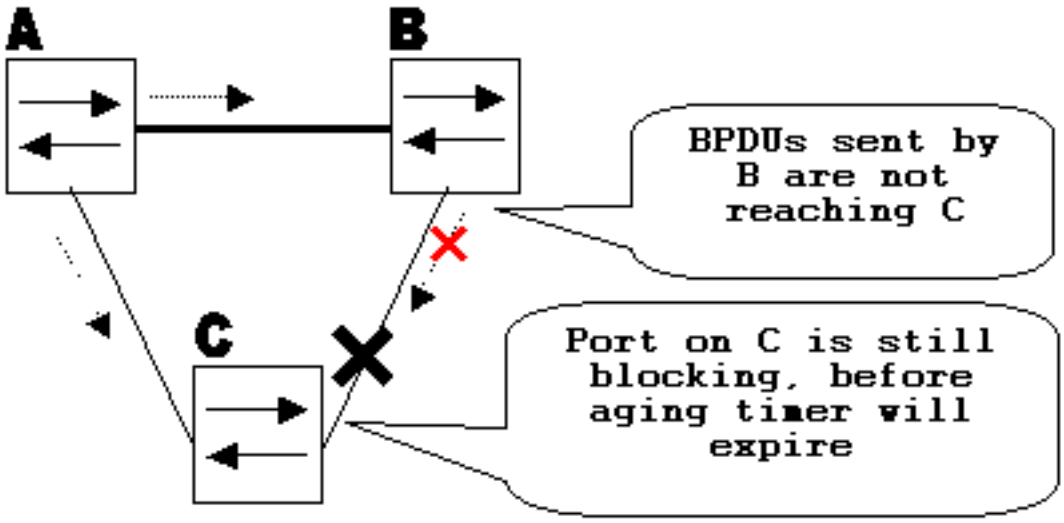
Considere este cenário. As setas indicam o fluxo de STP BPDUs.




Durante a operação normal, a bridge B é designada no link B-C. A bridge B envia BPDUs para C, o qual está bloqueando a porta. A porta é bloqueada enquanto C vê BPDUs de B naquele lnk.

Agora, considere o que acontece se o link B-C falhar na direção de C.C para de receber tráfego de B. No entanto, B ainda recebe o tráfego de C.

C para de receber BPDUs no link B-C e expira a informação recebida com os últimos BPDUs. Isso pode levar até 20 segundos, dependendo do temporizador de STP maxAge. Uma vez que as informações de STP são expiradas na porta, essa porta transiciona do estado de bloqueio para o estado listening, learning e, eventualmente, para estado forwarding do STP. Isso cria um loop de encaminhamento, já que não há nenhuma porta de bloqueio no triângulo A-B-C. Os pacotes circulam pelo caminho (B ainda recebe pacotes de C) consumindo largura de banda adicional até os links se tornarem completamente preenchidos. Isso derruba a rede.




Outro problema que pode ser causado por um link unidirecional é o blackholing de tráfego.

## Como funciona o protocolo de deteção de enlace unidirecional

Para detectar os links unidirecionais antes de criar o loop de encaminhamento, a Cisco projetou e implementou o protocolo UDLD.

O UDLD é um protocolo Camada 2 (L2) que funciona com os mecanismos de Camada 1 (L1) para determinar o status físico de um link. Na Camada 1, a autonegociação toma conta da sinalização física e da detecção de falhas. O UDLD executa as tarefas que a autonegociação não pode executar, como a detecção das identidades de vizinhos e o encerramento de portas conectadas de forma incorreta. Quando você habilita a autonegociação e o UDLD, as detecções da Camada 1 e da Camada 2 trabalham junto para impedir conexões unidirecionais físicas e lógicas e o funcionamento incorreto de outros protocolos.

O UDLD funciona através da troca de pacotes de protocolo entre os dispositivos vizinhos. Para que o UDLD funcione, ambos os dispositivos no link devem oferecer suporte ao UDLD e tê-lo habilitado nas respectivas portas.

Cada porta de switch configurada para o UDLD envia os pacotes do protocolo UDLD que contêm a ID de dispositivo/porta da própria porta , e as IDs de dispositivo/porta dos vizinhos vistas pelo UDLD nessa porta. As portas vizinhas devem ver sua própria ID de dispositivo/porta (eco) nos pacotes recebidos do outro lado.

Se a porta não vê sua própria ID de dispositivo/porta nos pacotes UDLD recebidos por um período de tempo específico, o link é considerado unidirecional.

Este algoritmo de eco permite a detecção destes problemas:

- O link está ativo nos dois lados, mas os pacotes são recebidos apenas por um lado.
- Erros de fiação quando as fibras de recepção e transmissão não estão conectadas à mesma porta no lado remoto.

Uma vez que o link unidirecional é detectado pelo UDLD, a respectiva porta é desabilitada e esta mensagem é mostrada no console:

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

O fechamento de porta pelo UDLD permanece desabilitado até que ele seja reabilitado manualmente ou até que o intervalo errdisable expire (se configurado).

## Modos de operação de UDLD

O UDLD pode operar em dois modos: normal e agressivo.

No modo normal, se o estado do link da porta foi identificado como bidirecional e houver timeout das informações de UDKD, nenhuma ação é tomada pelo UDLD. O estado da porta para o UDLD é marcado como indeterminado. A porta comporta-se de acordo com seu estado STP.

No modo agressivo, se o estado do link da porta for identificado como bidirecional e houver timeout das informação de UDLD enquanto o link na porta ainda estiver ativo, o UDLD tentará restabelecer o estado da porta. Se não houver êxito, a porta é colocada no estado errdisable.

O envelhecimento das informações de UDLD acontece quando a porta que executa o UDLD não recebe pacotes UDLD da porta vizinha durante o tempo de espera. O tempo de espera da porta é determinado pela porta remota e depende do intervalo de mensagem no lado remoto. O menor intervalo de mensagem, o menor tempo de espera e a detecção mais rápida. As implementações recentes de UDLD permitem a configuração de intervalo de mensagem.

Informações sobre UDLD podem expirar devido à alta taxa de erros na porta, causada por algum problema físico ou incompatibilidade de duplex. Tal queda de pacote não significa que o enlace seja unidirecional e que UDLD em modo normal não desativará tal enlace.

Éimportante poder selecionar o intervalo da mensagem correta para garantir o tempo de detecção adequado. O intervalo de mensagens deve ser rápido o bastante para detectar o link unidirecional antes que o loop de encaminhamento seja criado. No entanto, ele não deve sobrecarregar a CPU do switch. O intervalo padrão de mensagens é de 15 segundos e é rápido o suficiente para detectar o link unidirecional antes do loop de encaminhamento ser criado com temporizadores STP padrão. O tempo de detecção é aproximadamente igual a três vezes o intervalo das mensagens.

Por exemplo: $_{\text{Detecção}}$ T ~ message_interval x3

Este é 45 segundos para o intervalo de mensagens padrão de 15 segundos.

Toma o$_{\text{reconvergence=max_age}}$ T + o forward_delay 2x para o STP ao reconvergir em caso da falha de link unidirecional. Com os temporizadores padrão, o tempo necessário é 20+2x15=50 segundos.

Érecomendado manter a$_{\text{detecção}}$ T < a$_{\text{reconvergência}}$ T escolhendo um intervalo de mensagem apropriado.

No modo agressivo, assim que as informações expiram, o UDLD fará uma tentativa de restabelecer o estado do enlace, enviando pacotes a cada segundo durante oito segundos. Se o estado do link anda não for determinado, ele é desabilitado.

O modo agressivo adiciona a detecção adicional destas situações:

- A porta está presa (em um lado a porta não transmite nem recebe. No entanto, o link está

ativo em ambos os lados).
- O link está ativo em um dos lados e inativo, no outro lado. Esse problema pode ser visto em portas de fibra. Quando a fibra de transmissão está desconectada na porta local, o link permanece ativo no lado local. No entanto, permanece desativado no lado remoto.

Mais recentemente, as implementações de hardware dos FastEthernet de fibra possuem funções do Far End Fault Indication (FEFI) para desativar o link ambos os lados nessas situações. No Gigabit Ethernet, uma função similar é fornecida pela negociação de enlaces. Em geral, portas de cobre não são suscetíveis a esse tipo de problema, pois usam pulsos de links de Ethernet para monitorar o link. É importante mencionar que, em ambos os casos, nenhum loop de encaminhamento ocorre porque não há nenhuma conectividade entre as portas. Se o link estiver ativo em um dos lados e inativo no outro, poderá haver blacholing de tráfego. UDLD agressivo for designado para impedir isso.

## Disponibilidade

O UDLD está disponível no modo normal para:

- Catalyst OS Versão 5.1.1 ou posterior para switches da família Catalyst 4500/4000, 5500/5000 e 6500/6000
- Cisco IOS® Software Release 12.0(5)XU ou posterior para Catalyst 2900XL e 3500XL Switches
- Cisco IOS Software Release 12.1(13)AY ou posterior para Catalyst 2940 Switches
- Cisco IOS Software Release 12.0(5)WC(1) ou posterior para Catalyst 2950 Switches
- Cisco IOS Software Release 12.1(12c)EA1 ou posterior para Catalyst 2955 Switches
- Cisco IOS Software Release 12.1(11)AX ou posterior para Catalyst 2970 Switches
- Cisco IOS Software Release 12.1(4)EA1 ou posterior para Catalyst 3550 Switches
- Cisco IOS Software Release 12.1(19)EA1 ou posterior para Catalyst 3560 Switches
- Cisco IOS Software Release 12.1(11)AX ou posterior para Catalyst 3750 Switches
- Cisco IOS Software Release 12.1(2)E ou posterior para Catalyst 6500/6000 Switches com Cisco IOS System Software
- Cisco IOS Software Release 12.1(8a)EW ou posterior para Catalyst 4500/4000 Switches com Cisco IOS

O modo agressivo foi implementado a partir destas versões de software:

- Catalyst OS Versão 5.4.3 ou posterior para switches da família Catalyst 4500/4000, 5500/5000 e 6500/6000
- Cisco IOS Software Release 12.1(3a)E3 ou posterior para Catalyst 6500/6000 Switches com Cisco IOS System Software
- Cisco IOS Software Release 12.1(6)EA2 ou posterior para Catalyst 2950 Switches
- Cisco IOS Software Release 12.1(12c)EA1 ou posterior para Catalyst 2955 Switches
- Cisco IOS Software Release 12.1(11)AX ou posterior para Catalyst 2970 Switches
- Cisco IOS Software Release 12.1(4)EA1 ou posterior para Catalyst 3550 Switches
- Cisco IOS Software Release 12.1(11)AX ou posterior para Catalyst 3750 Switches

## Configuração e monitoramento

Estes comandos detalham a configuração do UDLD em Catalyst Switches com CatOS. O UDLD

precisa ser habilitado globalmente primeiro (o padrão é desabilitado) com este comando:

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

Emita este comando: para verificar se o UDLD está habilitado

```
Vega> (enable) show udld UDLD: enabled Message Interval: 15 seconds
```

O UDLD também precisa ser habilitado nas portas necessárias com este comando:

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

Execute o **comando show udld port** para verificar se o UDLD está habilitado ou desabilitado na porta e qual é o estado da interface:

```
Vega> (enable) show udld port UDLD : enabled Message Interval : 15 seconds Port Admin Status
Aggressive Mode Link State -------- ------------ -------------- --------------- 1/1 enabled
disabled undetermined 1/2 enabled disabled bidirectional
```

O UDLD agressivo é habilitado porta a porta com o **comando set udld aggressive-mode enable <module/port>**:

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

Execute este comando para mudar o intervalo de mensagens:

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

O intervalo pode variar de 7 a 90 segundos, sendo que o padrão é de 15 segundos.

Consulte estes documentos para obter mais informações sobre a configuração do UDLD no IOS:

- Para Catalyst 6500/6000 Switches com Cisco IOS System Software, consulte Configuração do UDLD.
- Para Catalyst 2900XL/3500XL Switches, consulte a seção *Configuração da Detecção de Links Unidirecionais* de Configuração de Portas de Switch.
- Para Catalyst 2940 Switches, consulte Configuração do UDLD.
- Para Catalyst 2950/2955 Switches, consulte Configuração do UDLD.
- Para Catalyst 2970 Switches, consulte Configuração do UDLD.
- Para Catalyst 3550 Switches, consulte Configuração do UDLD.
- Para Catalyst 3560 Switches, consulte Configuração do UDLD.
- Para Catalyst 4500/4000 com Cisco IOS, consulte Configuração do UDLD.

# Informações Relacionadas

- Suporte de tecnologia de switching de LAN
- Suporte dos Produtos Catalyst LAN e ATM Switches
- Suporte Técnico e Documentação - Cisco Systems