

Présentation et configuration du protocole UDLD (Unidirectional Link Detection)

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Définition du problème](#)

[Comment fonctionne le protocole UDLD \(Unidirectional Link Detection\)](#)

[Modes de fonctionnement d'UDLD](#)

[Disponibilité](#)

[Configuration et surveillance](#)

[Informations connexes](#)

[Introduction](#)

Ce document explique comment le protocole UDLD peut aider à empêcher le transfert de boucles et le blackholing du trafic dans des réseaux commutés.

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

[Conventions](#)

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

[Définition du problème](#)

Le protocole STP (Spanning Tree Protocol) résout la topologie physique redondante dans une topologie de transfert sans boucles, de type arbre.

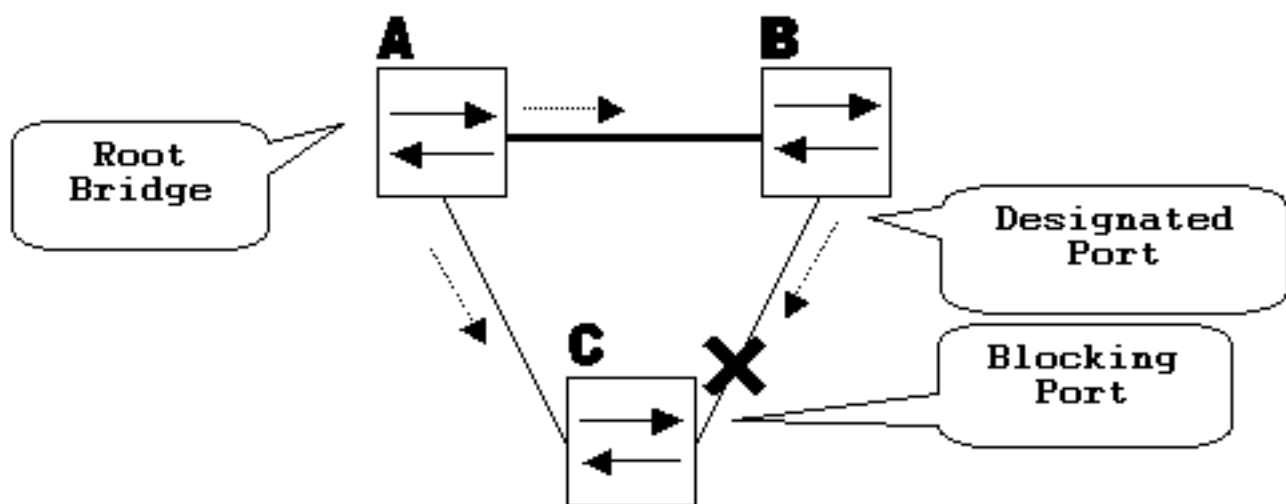
Ceci est fait en bloquant un ou plusieurs ports. En bloquant un ou plusieurs ports, il n'y a aucune boucle dans la topologie de transfert. Dans son fonctionnement, le protocole STP compte sur la réception et la transmission des unités BPDU (Bridge Protocol Data Unit). Si le processus STP qui fonctionne sur le commutateur avec un port de blocage arrête de recevoir des BPDU de son commutateur ascendant (désigné) sur le port, le protocole STP finit par expirer les informations STP pour le port et les place à l'état de transfert (forwarding state). Ceci crée une boucle de transfert ou boucle STP.

Les paquets commencent à faire un cycle indéfiniment le long du chemin en boucle, et consomme de plus en plus de bande passante. Ceci mène à une éventuelle panne de réseau.

Comment est-il possible pour le commutateur d'arrêter de recevoir des unités BPDU tandis que le port est up? La raison est la liaison unidirectionnelle. Une liaison est considérée unidirectionnelle quand ceci se produit :

- La liaison est up des deux côtés de la connexion. Le côté local ne reçoit pas les paquets envoyés par le côté distant tandis que le côté distant reçoit les paquets envoyés par le côté local.

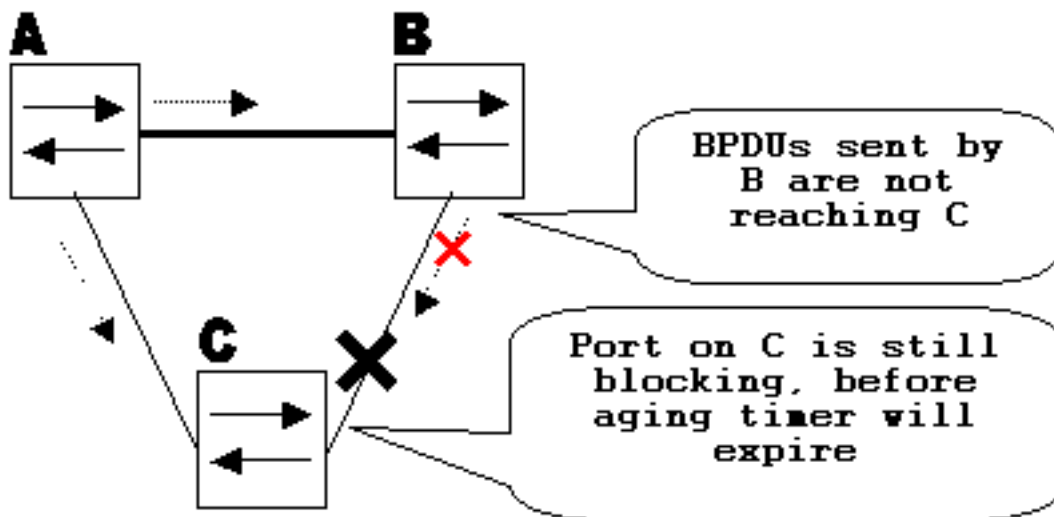
Considérez ce scénario. Les flèches indiquent le flux des BPDU STP.



Pendant le fonctionnement normal, le pont B est désigné sur la liaison B-C. Le pont B envoie des BPDU au C, qui bloque le port. Le port est bloqué tandis que C voit des BPDU de B sur cette liaison.

Maintenant, considérez ce qui se produit si le lien échoue BC en direction des arrêts de C. C recevant le trafic de B, cependant, B reçoit toujours le trafic du C.

C cesse de recevoir des BPDU sur la liaison B-C, et expire les informations reçues avec les dernières BPDU. Ceci prend jusqu'à 20 secondes, selon le temporisateur de maxAge STP. Une fois que les informations STP ont expiré sur le port, ce dernier passe de l'état de blocking à l'état STP de listening, learning et par la suite forwarding . Ceci crée une boucle de transfert, car il n'y a aucun port de blocage dans le triangle ABC. Le cycle de paquets le long du chemin (B reçoit toujours des paquets de C) prend de la bande passante supplémentaire jusqu'à ce que les liaisons soient complètement remplies. Ceci crée une défaillance du réseau.



Un autre problème possible qui peut être provoqué par une liaison unidirectionnelle est le blackholing de trafic.

[Comment fonctionne le protocole UDLD \(Unidirectional Link Detection\)](#)

Afin de détecter les liaisons unidirectionnelles avant que la boucle de transfert ne soit créée, Cisco a conçu et mis en application le protocole UDLD.

UDLD est un protocole de couche 2 (L2) qui fonctionne avec les mécanismes de la couche 1 (L1) pour déterminer l'état physique d'une liaison. À la couche 1, la négociation automatique prend soin de la signalisation physique et de la détection des pannes. UDLD effectue les tâches que la négociation automatique ne peut pas effectuer, comme détecter les identités des voisins et arrêter les ports mal-connectés. Quand vous activez la négociation automatique et UDLD, la détection de la couche 1 et celle de la couche 2 fonctionnent ensemble pour empêcher les connexions unidirectionnelles physiques et logiques et le défaut de fonctionnement d'autres protocoles.

UDLD fonctionne en permutant des paquets de protocole entre des périphériques voisins. Pour que UDLD fonctionne, les deux périphériques sur la liaison doivent prendre en charge UDLD qui doit être activé sur les ports respectifs.

Chaque port de commutation configuré pour UDLD envoie les paquets du protocole UDLD qui contiennent l'ID du propre périphérique/port du port, et les ID du périphérique/port du voisin vus par UDLD sur ce port. Les ports voisins devraient voir leur propre ID de périphérique/port (écho) dans les paquets reçus de l'autre côté.

Si le port ne voit pas son propre ID de périphérique/port dans les paquets UDLD entrant pendant une durée spécifique, la liaison est considérée unidirectionnelle.

Cet écho-algorithme permet la détection des problèmes suivants :

- La liaison est up des deux côtés, mais les paquets ne sont reçus que par un côté.
- Erreurs de câblage quand les fibres de réception et transmission ne sont pas connectées au même port du côté distant.

Une fois la liaison unidirectionnelle détectée par UDLD, le port respectif est désactivé et ce

message est imprimé sur la console :

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

Le port arrêté par UDLD reste désactivé jusqu'à ce qu'il soit manuellement réactivé, ou jusqu'à ce que le délai d'atteinte errdisable expire (si configuré).

Modes de fonctionnement d'UDLD

UDLD peut fonctionner en deux modes : normal et agressive.

Dans le mode normal, si l'état de la liaison du port a été déterminé pour être bidirectionnel et que les informations UDLD expirent, aucune mesure n'est prise par UDLD. L'état du port pour UDLD est marqué en tant que undetermined. Le port se comporte selon son état STP.

Dans le mode agressive, si l'état de la liaison du port est déterminé pour être bidirectionnel et que les informations UDLD expirent tandis que la liaison sur le port est toujours up, UDLD essaye de rétablir l'état du port. En cas d'échec, le port est placé en l'état errdisable.

L'expiration des informations UDLD se produit quand le port qui exécute UDLD ne reçoit pas les paquets UDLD du port voisin pendant la durée du temps d'attente. Le temps d'attente pour le port est dicté par le port distant et dépend de l'intervalle des messages sur le côté distant. Plus l'intervalle des messages est court, plus le temps d'attente est court et plus la détection est rapide. Les réalisations récentes d'UDLD autorisent la configuration de l'intervalle des messages.

Les informations UDLD peuvent expirer en raison du taux d'erreur élevé sur le port provoqué par un problème physique ou une erreur de correspondance de duplex. Une telle perte de paquets ne signifie pas que la liaison est unidirectionnelle et UDLD en mode normal ne désactivera pas de telles liaisons.

Il est important de pouvoir choisir le bon intervalle de messages afin d'assurer un temps de détection approprié. L'intervalle des messages devrait être assez rapide pour détecter la liaison unidirectionnelle avant que la boucle de transfert soit créée, mais elle ne devrait pas surcharger le CPU du commutateur. L'intervalle des messages par défaut est de 15 secondes, et est assez rapide pour détecter la liaison unidirectionnelle avant que la boucle de transfert ne soit créée avec des temporisateurs STP par défaut. Le temps de détection est approximativement égal à trois fois l'intervalle des messages.

Exemple : $T_{\text{Détection}} | \times 3 \text{ message_interval}$

C'est 45 secondes pour l'intervalle de messages par défaut de 15 secondes.

Il prend le $T_{\text{reconvergence}=\text{max_age}}$ + le $2 \times \text{forward_delay}$ pour que le STP reconverge en cas de panne unidirectionnelle de lien. Avec les temporisateurs par défaut, cela prend $20 + 2 \times 15 = 50$ secondes.

Il est recommandé pour garder la $T_{\text{détection}} < T_{\text{reconvergence}}$ en choisissant un intervalle de messages approprié.

Dans le mode agressive, une fois que les informations ont expiré, UDLD essayera de rétablir l'état de la liaison en envoyant des paquets chaque seconde pendant huit secondes. Si l'état de la liaison n'est toujours pas déterminé, la liaison est désactivée.

Le mode aggressive ajoute une détection supplémentaire de ces situations :

- Le port est coincé (d'un côté le port ne transmet ni ne reçoit, mais la liaison est up des deux côtés).
- La liaison est up d'un côté et down de l'autre côté. Ce problème peut être vu sur des ports fibre. Quand la fibre de transmission est débranchée au port local, la liaison reste up du côté local. Cependant, elle est down du côté distant.

Récemment, les réalisations de matériel FastEthernet par fibre ont des fonctions d'indication de panne d'extrémité lointaine (FEFI) afin que la liaison soit down des deux côtés dans ces situations. Sur un Gigabit Ethernet, une fonction semblable est fournie par négociation de liaison. Les ports cuivre ne sont normalement pas sujets à ce type de problème, car ils utilisent des impulsions de liaison Ethernet pour surveiller la liaison. Il est important de mentionner que dans les deux cas, aucune boucle de transfert ne se produit parce qu'il n'y a aucune connectivité entre les ports. Néanmoins, si la liaison est up d'un côté et down de l'autre, un blackholing de trafic peut se produire. La détection UDLD agressive est conçue pour empêcher ceci.

Disponibilité

UDLD est disponible dans le mode normal pour :

- Logiciel Catalyst OS Version 5.1.1 et ultérieure pour les commutateurs de la famille Catalyst 4500/4000, 5500/5000 et 6500/6000
- Logiciel Cisco IOS® Version 12.0(5)XU et ultérieure pour les commutateurs Catalyst 2900XL et 3500XL
- Logiciel Cisco IOS® Version 12.1(13)AY et ultérieure pour les commutateurs Catalyst 2940
- Logiciel Cisco IOS® Version 12.0(5)WC(1) ou ultérieure pour les commutateurs Catalyst 2950
- Logiciel Cisco IOS® Version 12.1(12c)EA1 ou ultérieure pour les commutateurs Catalyst 2955
- Logiciel Cisco IOS® Version 12.1(11)AX ou ultérieure pour les commutateurs Catalyst 2970
- Logiciel Cisco IOS® Version 12.1(4)EA1 ou ultérieure pour les commutateurs Catalyst 3550
- Logiciel Cisco IOS® Version 12.1(19)EA1 ou ultérieure pour les commutateurs Catalyst 3560
- Logiciel Cisco IOS® Version 12.1(11)AX ou ultérieure pour les commutateurs Catalyst 3750
- Logiciel Cisco IOS Version 12.1(2)E et ultérieure pour les commutateurs Catalyst 6500/6000 qui exécutent la plate-forme Cisco IOS
- Logiciel Cisco IOS Version 12.1(8a)EW et ultérieure pour les commutateurs Catalyst 4500/4000 qui exécute Cisco IOS

Le mode agressive est mis en œuvre à partir de ces versions de logiciel :

- Catalyst OS Version 5.4.3 et ultérieure pour les commutateurs de la famille Catalyst 4500/4000, 5500/5000 et 6500/6000
- Logiciel Cisco IOS Version 12.1(3a)E3 et ultérieure pour les commutateurs Catalyst 6500/6000 qui exécutent la plate-forme Cisco IOS
- Logiciel Cisco IOS® version 12.1(6)EA2 ou ultérieure pour les commutateurs Catalyst 2950
- Logiciel Cisco IOS® Version 12.1(12c)EA1 ou ultérieure pour les commutateurs Catalyst 2955
- Logiciel Cisco IOS® Version 12.1(11)AX ou ultérieure pour les commutateurs Catalyst 2970
- Logiciel Cisco IOS® Version 12.1(4)EA1 ou ultérieure pour les commutateurs Catalyst 3550
- Logiciel Cisco IOS® Version 12.1(11)AX ou ultérieure pour les commutateurs Catalyst 3750

Configuration et surveillance

Ces commandes détaillent la configuration du protocole UDLD sur les commutateurs Catalyst qui exécutent CatOS. UDLD doit d'abord être activé globalement (il est désactivé par défaut) avec cette commande :

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

Émettez la commande suivante : pour vérifier si UDLD est activé

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

UDLD doit également être activé sur les ports nécessaires avec cette commande :

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

Émettez la commande **show udld port** pour vérifier si UDLD est activé ou désactivé sur le port et connaître l'état de la liaison :

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

L'activation du protocole UDLD en mode agressif se fait par port avec la commande **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 -----
enabled undetermined
```

Émettez cette commande pour changer l'intervalle des messages :

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

L'intervalle peut aller de 7 à 90 secondes, la valeur par défaut étant de 15 secondes.

Référez-vous à ces documents pour plus d'informations sur la configuration d'UDLD sur le logiciel :

- Pour les commutateurs Catalyst 6500/6000 qui exécutent la plate-forme logicielle Cisco IOS, référez-vous à [Configuration d'UDLD](#).
- Pour les commutateurs Catalyst 2900XL/3500SL, référez-vous à la section *Configuration de la détection unidirectionnelle* de [Configuration des ports de commutation](#).
- Pour les commutateurs Catalyst 2940, référez-vous à [Configuration du protocole UDLD](#).
- Pour les commutateurs Catalyst 2950/2955, référez-vous à [Configuration du protocole UDLD](#).
- Pour les commutateurs Catalyst 2970, référez-vous à [Configuration du protocole UDLD](#).
- Pour les commutateurs Catalyst 3550, référez-vous à [Configuration du protocole UDLD](#).
- Pour les commutateurs Catalyst 3560, référez-vous à [Configuration du protocole UDLD](#).
- Pour Catalyst 4500/4000 exécutant Cisco IOS, référez-vous à [Configuration du protocole UDLD](#).

[Informations connexes](#)

- [Prise en charge de la technologie de commutation LAN](#)
- [Support produit pour commutateurs ATM et LAN Catalyst](#)
- [Support et documentation techniques - Cisco Systems](#)