Configurer la fonctionnalité de protocole UDLD

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés
- Conventions

Définition du problème

Fonctionnement du protocole de détection de liaison unidirectionnel

Modes de fonctionnement UDLD

- Mode normal
- Mode agressif
  - Minuteurs de messages et de mise en attente UDLD

Configuration et surveillance

Informations connexes

Introduction

Ce document décrit comment le protocole UDLD (Unidirectionnel Link Detection) peut aider à prévenir les boucles et les anomalies de trafic dans les réseaux commutés.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document décrit le fonctionnement général d'UDLD. Les exemples de configuration et de vérification de ce document ont été validés sur les commutateurs de la gamme Cisco Catalyst 9300 exécutant la version Cisco IOS XE 17.X.

Remarque : La syntaxe des commandes, les valeurs par défaut, les plages de minuteurs et les résultats peuvent varier selon la plate-forme et la version du logiciel.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

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 en une topologie de transfert de type arbre sans boucle. Pour ce faire, il bloque un ou plusieurs ports. Avec un ou plusieurs ports bloqués, il n'y a pas de boucles dans la topologie de transfert. Le protocole STP repose dans son fonctionnement sur la réception et la transmission des unités BPDU (Bridge Protocol Data Unit). Si un port dans l'état de blocage ou d'abandon STP cesse de recevoir des BPDU du pont désigné, STP finit par expirer les informations associées à ce port et le déplace vers un état de transmission.

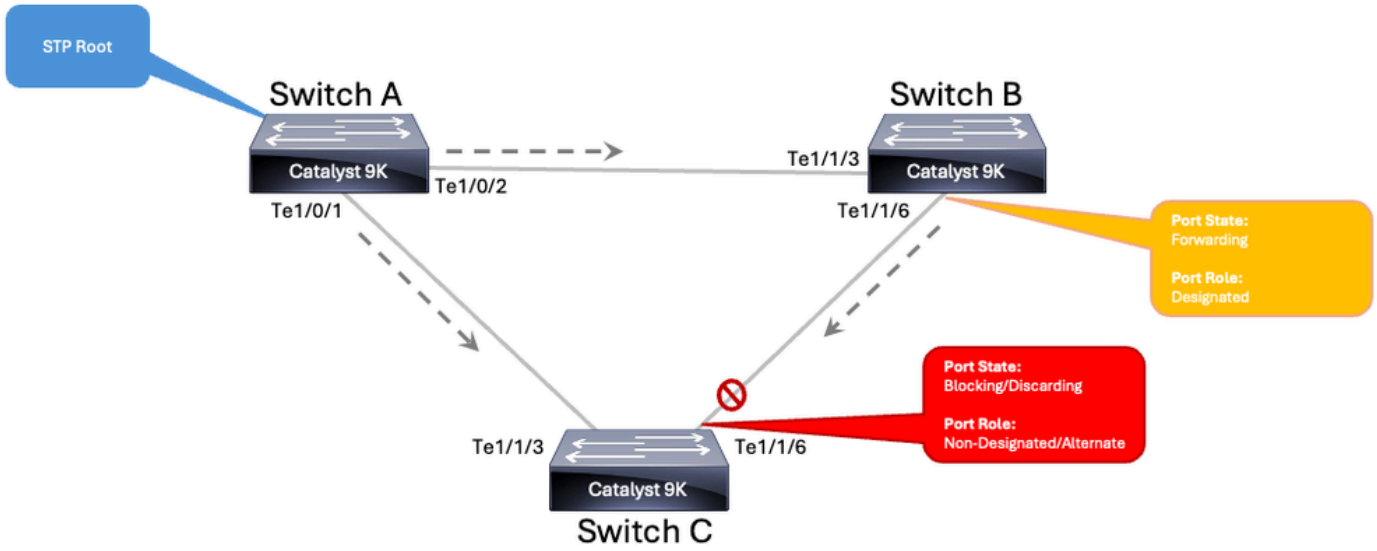
Cela peut créer une boucle STP où les paquets commencent à circuler indéfiniment le long du chemin en boucle et consomment plus de bande passante et de ressources. Cela peut entraîner une panne du réseau.

Comment est-il possible que le commutateur ne reçoive pas de BPDU lorsque le port est actif ? Cela est dû à une liaison unidirectionnelle.

Une liaison est considérée comme unidirectionnelle lorsque :

- La liaison est active 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.

Dans le scénario suivant, les flèches indiquent le flux des BPDU STP :



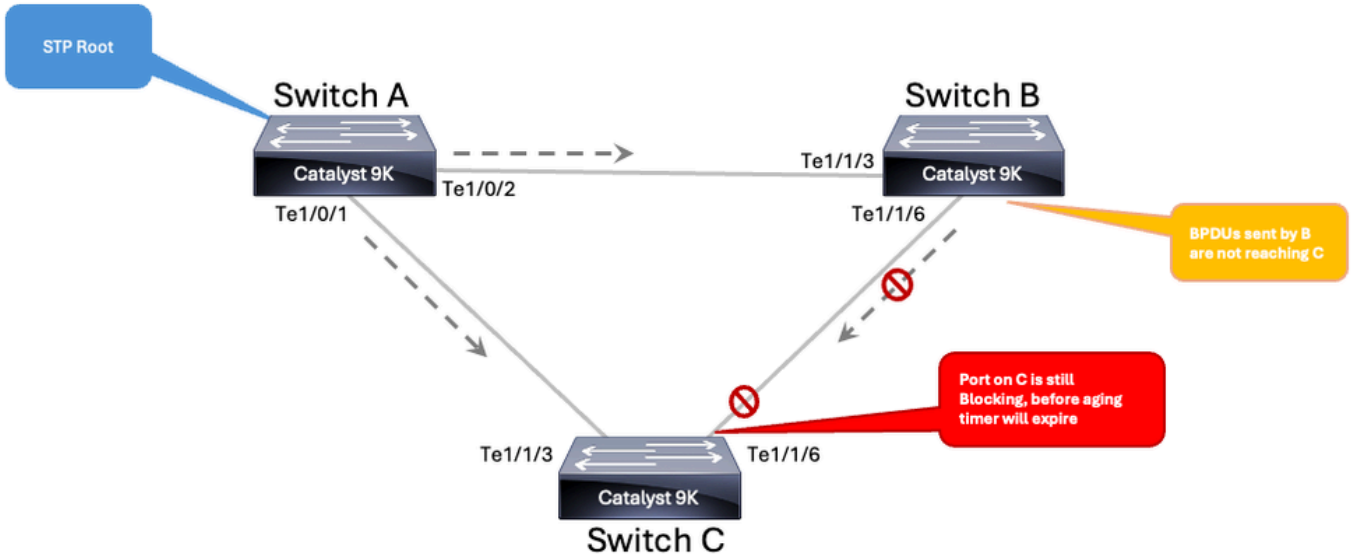
Topologie d'état des ports STP

Dans la condition illustrée dans cette topologie, l’interface du commutateur B vers le commutateur C est le port désigné pour le segment B-C et transmet les BPDU vers le commutateur C. L’interface du commutateur C vers le commutateur B est un port non désigné dans le protocole STP IEEE 802.1D classique. Ou un autre port dans RSTP et reste dans l'état de blocage/d'abandon pendant qu'il reçoit et traite des BPDU du commutateur B. Bien que l'interface sur le commutateur C soit dans l'état de blocage ou d'abandon, le port continue de recevoir et de traiter des BPDU ; ces états empêchent le port de transmettre des trames de données mais ne l'empêchent pas de recevoir des BPDU.

Imaginez ce qui se passe si la liaison B-C devient unidirectionnelle et que la direction B → C échoue. Le commutateur C ne peut plus recevoir de BPDU du commutateur B, tandis que le commutateur B peut recevoir des BPDU transmises par le commutateur C. Le commutateur C conserve les informations apprises de la dernière BPDU jusqu’à ce que ces informations expirent. Avec le protocole STP IEEE 802.1D classique et l'âge maximal par défaut de 20 secondes, cela peut prendre jusqu'à 20 secondes. Une fois que les informations STP expirent, le commutateur C ne considère plus que le commutateur B est supérieur sur ce segment, et le port peut passer du mode Blocage au mode Écoute, puis Apprentissage, et enfin Transfert.

Cela crée une boucle de transfert de couche 2 car il n'y a plus de port bloqué dans le triangle A-B-C. Les trames de diffusion, de monodiffusion inconnue et de multidiffusion peuvent circuler de manière répétée dans la boucle, consommant de la bande passante, du processeur et pouvant entraîner une tempête de diffusion.

Ce scénario peut provoquer la panne du réseau, ce qui est un autre problème possible causé par une liaison unidirectionnelle, comme un trou noir de trafic.



Flux BPDU STP

Fonctionnement du protocole de détection de liaison unidirectionnel

UDLD est un protocole de couche 2 qui complète les mécanismes de détection de liaison de couche 1 en identifiant les communications unidirectionnelles et les incohérences de câblage spécifiques entre les périphériques directement connectés.

Au niveau de la couche 1, la négociation automatique résout la signalisation physique et la détection des pannes. UDLD effectue des tâches que la négociation automatique ne peut pas effectuer, telles que la détection des identités de voisinage et l'arrêt des ports déconnectés. Lors de l'activation de la négociation automatique et de UDLD ; Les détections de couche 1 et de couche 2 fonctionnent ensemble pour empêcher les connexions unidirectionnelles physiques et logiques et le dysfonctionnement d’autres protocoles.

UDLD fonctionne par l'échange de paquets de protocole entre les périphériques voisins. Pour établir une relation de voisinage UDLD bidirectionnelle, les deux périphériques connectés directement doivent prendre en charge UDLD et l'activer sur les interfaces connectées. Vérifiez l'état bidirectionnel sur les deux périphériques.

Chaque port de commutateur configuré pour UDLD envoie des paquets de protocole UDLD qui contiennent l'ID de port/périphérique et les ID de port/périphérique voisins vus par UDLD sur ce port.

Les ports voisins voient 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 entrants pendant une durée spécifique, la liaison est considérée comme unidirectionnelle.

Cet algorithme d'écho permet de détecter les problèmes suivants :

- La liaison est active des deux côtés, mais les paquets ne sont reçus que par un côté.
- Des erreurs de connexion (fil) se produisent lorsque les fibres de réception et de transmission ne sont pas connectées au même port du côté distant.

Une fois qu'UDLD détecte une condition unidirectionnelle, il place l'interface locale de détection dans l'état err-disable. L'état de l'interface distante dépend de la détection UDLD distante et du comportement de la liaison physique. Un message similaire est imprimé sur la console :

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

Une interface désactivée par UDLD reste dans l'état err-disable jusqu'à ce qu'elle soit restaurée manuellement ou qu'un minuteur de récupération errdisable activé expire. Corrigez la défaillance de la fibre, de l'émetteur-récepteur, du câblage ou de l'interface distante avant de procéder à la récupération. Utilisez shutdown et no shutdown pour une récupération manuelle. Sur les plates-formes qui le supportent, udld reset réinitialise les interfaces désactivées/désactivées par UDLD. Après la restauration, exécutez les commandes show interfaces status err-disabled, show udld <interface-id>, et show udld neighbors pour confirmer que l'interface est opérationnelle et que la relation UDLD est bidirectionnelle. Vérifiez les journaux système pour vous assurer que l'erreur ne se reproduit pas.

Modes de fonctionnement UDLD

UDLD peut fonctionner dans deux modes : Normal et agressif :

Mode normal

Lorsque UDLD est activé sur une interface prise en charge, le mode normal est le mode de fonctionnement par défaut, sauf si le mode agressif est explicitement configuré. UDLD fonctionne avec des mécanismes de couche 1, tels que la négociation automatique, pour valider une liaison. Les mécanismes de couche 1 détectent la signalisation physique et les défaillances de liaison, tandis qu'UDLD identifie les périphériques voisins et vérifie les brins de fibre qui se connectent aux ports appropriés.

En mode normal, UDLD détecte une condition unidirectionnelle lorsque les brins de fibre sont mal connectés entre les ports et que les mécanismes de couche 1 ne détectent pas l'erreur de câblage. Si les brins de fibre se connectent aux ports corrects mais que le trafic circule dans une seule direction, le mode normal UDLD marque la liaison logique comme indéterminée et ne désactive pas le port. Ce comportement repose sur des mécanismes de couche 1 pour détecter la défaillance physique. Si un brin de fibre est déconnecté et que la négociation automatique détecte la défaillance physique, la liaison ne reste pas active. UDLD n'effectue aucune action d'arrêt car la couche 1 a déjà détecté le problème et l'état de la liaison logique UDLD est indéterminé.

Mode agressif

Le mode agressif inclut les fonctionnalités de détection du mode normal et fournit une protection supplémentaire pour les liaisons point à point à fibre optique et à paires torsadées. Il détecte les brins de fibre mal connectés et les conditions dans lesquelles un point d'extrémité ne peut pas envoyer ou recevoir de trafic, un port reste actif tandis que l'autre est en panne, ou un brin de fibre devient déconnecté.

Les paquets Hello UDLD agissent comme un battement de coeur pour la liaison point à point. Si UDLD cesse de recevoir ces paquets après que la liaison a été établie comme bidirectionnelle, le mode agressif tente de rétablir la relation bidirectionnelle. Si UDLD ne peut pas restaurer la relation, il désactive le port local affecté pour empêcher l'utilisation continue d'une liaison dont le fonctionnement bidirectionnel ne peut pas être vérifié.

Lorsque les deux brins de fibre semblent opérationnels pour la couche 1, UDLD agressif vérifie qu'ils se connectent aux ports voisins corrects et que le trafic circule de manière bidirectionnelle entre les voisins attendus. La négociation automatique ne peut pas effectuer cette validation d'identité de voisin et de port, car elle fonctionne au niveau de la couche 1.

Minuteurs de messages et de mise en attente UDLD

Les informations UDLD expirent lorsqu'un port exécutant UDLD ne reçoit pas de paquets UDLD du port voisin pendant la durée du temps d'attente. Ces minuteurs s'appliquent à la maintenance

des informations de voisinage UDLD en mode normal et agressif ; l'action après expiration dépend du mode configuré et de la condition détectée. Le temps d'attente du port est dicté par le port distant et dépend de l'intervalle des messages du côté distant. Plus l'intervalle entre les messages est court, plus le temps d'attente et la détection sont courts. Les mises en oeuvre récentes d'UDLD permettent de configurer les intervalles des messages. Les informations UDLD peuvent expirer en raison du taux d'erreur élevé sur le port causé par un problème physique ou une non-correspondance de mode duplex. Une telle perte de paquets ne signifie pas que la liaison est unidirectionnelle et UDLD en mode normal ne désactive pas la liaison.

Il est important de choisir l'intervalle de message approprié pour garantir un temps de détection approprié. L'intervalle de message doit être suffisamment rapide pour détecter la liaison unidirectionnelle avant la création de la boucle de transfert, mais il ne doit pas surcharger le processeur du commutateur. L'intervalle de message par défaut dans cet exemple est de 15 secondes. Pour le scénario de temporisateur STP IEEE 802.1D classique décrit, le temps d'expiration estimé des informations UDLD est inférieur au temps estimé pour que le port bloqué atteigne l'état de transmission.

Cette comparaison ne garantit pas que l'UDLD agressif place l'interface dans l'état err-disable avant que STP ne modifie la topologie de transfert. La durée approximative d'expiration des informations de voisinage UDLD est de trois fois l'intervalle de message. Exemple :

$$T_{expiration} \approx message_interval \times 3$$

Avec l’intervalle de message par défaut Texpiration ≈ 15 × 3 = 45 secondes. Pour le fonctionnement STP IEEE 802.1D classique, le temps approximatif pour qu’un port bloqué expire ses informations STP stockées et passe des états d’écoute et d’apprentissage à l’état de transmission est :

$$T_{forward} = max_age + (2 \times forward_delay)$$

Avec les compteurs STP par défaut : Tforward = 20 + (2 × 15) = 50 secondes -Lorsque vous comparez l'expiration des informations de voisinage UDLD à la transition du port STP, sélectionnez un intervalle de message qui conserve : Texpiration < Tforward

En mode agressif, après l'expiration des informations de voisinage UDLD, UDLD tente de rétablir la relation bidirectionnelle en envoyant un message par seconde pendant huit secondes. Si l'état bidirectionnel ne peut pas être rétabli, UDLD désactive le port local.

Remarque : Ces calculs sont approximatifs et s'appliquent au comportement UDLD et au scénario de temporisateur STP IEEE 802.1D classique décrit dans ce document. La plate-forme déployée, la version du logiciel, le mode STP, les minuteurs configurés et l'heure de la panne peuvent affecter la durée réelle.

Remarque : Le calcul STP classique Treconvergence = max_age + (2 × forward_delay) ne s'applique pas à la convergence rapide RSTP normale. Les informations de protocole RSTP peuvent expirer lorsque les BPDU ne sont pas reçues pendant trois intervalles Hello consécutifs ou lorsque la condition d'âge maximal applicable est atteinte. Un port alternatif éligible peut alors passer rapidement à l'état de transmission. Le temps de transition total dépend de la topologie, des rôles de port, du type de liaison, du processus de synchronisation et de la condition de défaillance. Par conséquent, un calcul de temporisateur fixe ne peut pas garantir qu'UDLD détecte ou désactive une liaison unidirectionnelle avant que le protocole RSTP ne modifie la topologie de transfert. Validez l'interaction entre UDLD et RSTP sur la plate-forme déployée, la version du logiciel, la topologie et la configuration du minuteur.

Voici des exemples de conditions supplémentaires détectées par le mode agressif :

- La liaison physique est active des deux côtés, mais le port d'un côté ne transmet ni ne reçoit de messages UDLD.
- La liaison est active d'un côté et inactive de l'autre. Par exemple, sur certaines interfaces à fibre optique, la déconnexion de la fibre de transmission du port local peut laisser la liaison locale active tandis que la liaison distante est désactivée. Ce comportement dépend de la plate-forme, de l'interface, de l'émetteur-récepteur et des mécanismes de la couche physique.

Certaines mises en oeuvre de PHY Ethernet fournissent des mécanismes de signalisation de panne à distance ou de négociation de liaison qui peuvent entraîner la désactivation d'un ou des deux points d'extrémité de liaison après des pannes physiques spécifiques. Le comportement varie selon la plate-forme, le type d'interface, l'émetteur-récepteur, le support et le mode de négociation. UDLD fournit une validation de couche 2 pour les conditions unidirectionnelles que la signalisation de couche physique ne détecte pas. Lorsqu'un point d'extrémité ne peut pas transmettre/recevoir, ou lorsqu'un point d'extrémité est actif tandis que l'autre est inactif, la liaison défaillante elle-même ne fournit pas un chemin de transfert complet et ne forme pas de boucle de transfert. Cependant, une interface qui reste active peut continuer à transférer le trafic vers un chemin non fonctionnel, ce qui entraîne un trou noir du trafic. Aggressive UDLD détecte la perte de communication bidirectionnelle et désactive le port local affecté s'il ne peut pas rétablir la relation UDLD.

Configuration et surveillance

Activez UDLD sur les deux interfaces connectées. Configurez le même mode UDLD sur les deux points d'extrémité pour fournir une détection de panne locale cohérente et un comportement err-disable :

<#root>

9300-1#

configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
9300-1(config)#

interface TenGigabitEthernet1/1/6

9300-1(config-if)#

udld port

9300-1(config-if)#

end

9300-2#

configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
9300-2(config)#

interface TenGigabitEthernet1/1/6

9300-2(config-if)#

udld port

9300-2(config-if)#

end

Remarque : Les commandes UDLD globales et leur portée d'interface varient selon la plate-forme ; vérifiez la référence des commandes de la plate-forme cible avant d'utiliser une commande globale.

Exécutez les commandes show udld <interface-id> et show udld neighbors sur les deux points de terminaison de liaison. Vérifiez que chaque interface est opérationnelle, que l'état actuel est bidirectionnel, et que les identifiants de port et de périphérique voisin attendus sont affichés :

<#root>

9300-1#

show udld TenGigabitEthernet1/1/6

```
Interface Te1/1/6
---
Port enable administrative configuration setting: Enabled
Port enable operational state:
```

Enabled

```
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: 37500 ms
    Cache Device index: 1
    Current neighbor state:
```

Bidirectional

```
    Device ID: F87A41A8CA00
    Port ID:
```

Te1/1/6

```
    Neighbor echo 1 device: F87A41A8C180
    Neighbor echo 1 port:
```

Te1/1/6

```
    TLV Message interval: 15 sec
    No TLV fast-hello interval
    TLV Time out interval: 5
    TLV CDP Device name: 9300-2

9300-1#
```

show udld neighbors

```
Port           Device Name     Device ID    Port ID         Neighbor State
----           -----------     ---------    -------         --------------
```

Te1/1/6 F87A41A8CA00 1 Te1/1/6 Bidirectional

```
Total number of bidirectional entries displayed: 1

9300-2#
```

show udld TenGigabitEthernet1/1/6

```
Interface Te1/1/6
---
Port enable administrative configuration setting: Enabled
Port enable operational state:
```

Enabled

```
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: 32500 ms
```

```
    Cache Device index: 1
    Current neighbor state:

Bidirectional

    Device ID: F87A41A8C180
    Port ID:

Te1/1/6



    Neighbor echo 1 device: F87A41A8CA00
    Neighbor echo 1 port:

Te1/1/6



    TLV Message interval: 15 sec
    No TLV fast-hello interval
    TLV Time out interval: 5
    TLV CDP Device name: 9300-1

9300-2#show udld neighbors
Port           Device Name     Device ID    Port ID         Neighbor State
----           -----------     ---------    -------         --------------

Te1/1/6 F87A41A8C180 1 Te1/1/6 Bidirectional

Total number of bidirectional entries displayed: 1
```

UDLD agressif peut être configuré sur l'interface avec la commande udld port agressif :

<#root>

9300-1#

configure terminal

```
Enter configuration commands, one per line.  End with CNTL/Z.
9300-1(config)#
```

interface TenGigabitEthernet1/1/6

```
9300-1(config-if)#
```

udld port aggressive

```
9300-1(config-if)#
```

```
end


9300-2#

configure terminal


Enter configuration commands, one per line.  End with CNTL/Z.
9300-2(config)#

interface TenGigabitEthernet1/1/6

9300-2(config-if)#

udld port aggressive


9300-2(config-if)#

end
```

Exécutez la commande show udld <interface-id> sur les deux terminaux pour vérifier que le mode agressif est activé de manière opérationnelle :

<#root>

```
9300-1#

show udld TenGigabitEthernet1/1/6


Interface Te1/1/6
---
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: 31200 ms
    Cache Device index: 1
    Current neighbor state: Bidirectional
    Device ID: F87A41A8CA00
    Port ID: Te1/1/6
    Neighbor echo 1 device: F87A41A8C180
    Neighbor echo 1 port: Te1/1/6

    TLV Message interval: 15 sec
    No TLV fast-hello interval
    TLV Time out interval: 5
    TLV CDP Device name: 9300-2

9300-2#
```

show udld TenGigabitEthernet1/1/6

```
Interface Te1/1/6
---
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: 38600 ms
    Cache Device index: 1
    Current neighbor state: Bidirectional
    Device ID: F87A41A8C180
    Port ID: Te1/1/6
    Neighbor echo 1 device: F87A41A8CA00
    Neighbor echo 1 port: Te1/1/6

    TLV Message interval: 15 sec
    No TLV fast-hello interval
    TLV Time out interval: 5
    TLV CDP Device name: 9300-1
```

Exécutez la commande udld message time pour modifier l'intervalle de message :

<#root>

9300-1#

configure terminal

```
Enter configuration commands, one per line.  End with CNTL/Z.
9300-1(config)#
```

udld message time ?

```
  <1-90>  Time in seconds between sending of messages in steady state
```

Sur les commutateurs des gammes Cisco Catalyst 3000 et 9000, la valeur de temps du message udld va de 1 à 90 secondes, et la valeur par défaut est 15 secondes. Reportez-vous aux guides de référence des commandes pour vérifier la plage acceptée et la valeur par défaut sur les autres systèmes.

Informations connexes

- Assistance technique de Cisco et téléchargements
- Pour les commutateurs Catalyst 3560, référez-vous à Configuration d'UDLD
- Pour les commutateurs Catalyst 9300, référez-vous à Comment configurer UDLD
- Pour les commutateurs Catalyst 9500, référez-vous à Comment configurer UDLD

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.