

Configurare la funzione di protocollo UDLD

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Descrizione del problema](#)

[Come funziona il protocollo ULDP](#)

[Modalità di funzionamento del protocollo ULDP](#)

[Disponibilità](#)

[Configurazione e monitoraggio](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come il protocollo UDLD (Unidirectional Link Detection) possa aiutare a prevenire loop e anomalie del traffico nelle reti commutate.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Descrizione del problema

Il protocollo STP (Spanning-Tree Protocol) risolve la topologia fisica ridondante in una topologia ad albero senza loop.

A tale scopo, blocca una o più porte. Se una o più porte sono bloccate, non vi sono loop nella topologia di inoltro. A tal fine, il protocollo STP trasmette e riceve unità BPDU (Bridge Protocol Data Unit). Se il processo STP che viene eseguito sullo switch con una porta in stato di blocco non riceve BPDU dallo

switch a monte (designato), STP alla fine esaurisce le informazioni STP per la porta e le sposta nello stato di inoltro.

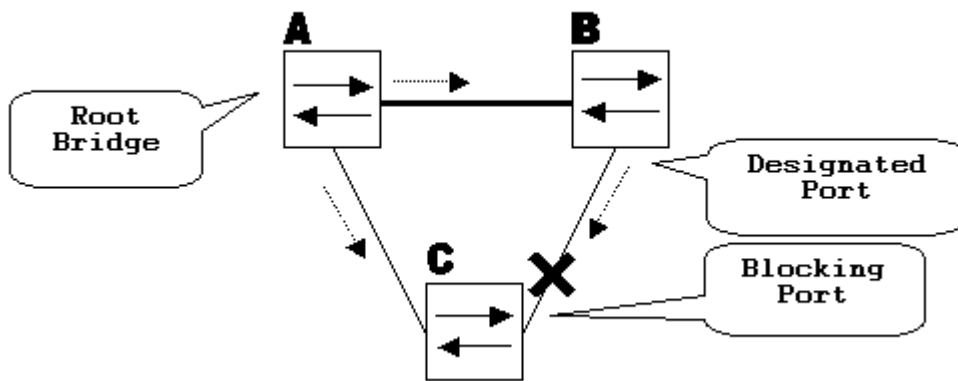
Questo può creare un loop STP in cui i pacchetti iniziano a circolare a tempo indefinito lungo il percorso con loop e consumano sempre più larghezza di banda e risorse. Ciò può causare l'interruzione della rete.

Come è possibile che lo switch non riceva i BPDU quando la porta è attiva? Il motivo è un collegamento unidirezionale.

Un collegamento è considerato unidirezionale quando si verifica quanto segue:

- Il collegamento è attivo su entrambi i lati del collegamento.
- Il dispositivo locale non riceve i pacchetti inviati dal dispositivo remoto, mentre il dispositivo remoto riceve i pacchetti inviati dal dispositivo locale.

Considerare questo scenario. Le frecce indicano il flusso di BPDU del protocollo STP.



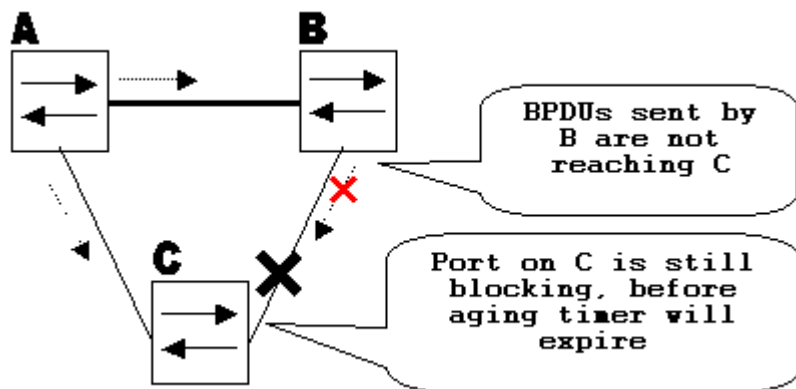
Durante il normale funzionamento, il ponte B è una porta designata sul collegamento B-C. Il ponte B invia le BPDU alla porta C, che blocca la porta. La porta è bloccata mentre C vede le BPDU provenienti da B su quel collegamento.

Ora, considera cosa succede se il collegamento B-C fallisce in direzione C. C cessa di ricevere traffico da B, tuttavia, B riceve ancora traffico da C.

verso l'alto

C non riceve le BPDU sul collegamento B-C e analizza le informazioni ricevute con l'ultima BPDU. Questa operazione può richiedere fino a 20 secondi, a seconda del timer STP maxAge. Quando le informazioni STP scadono, le transizioni sulla porta passano dallo stato blocco allo stato ascolto e apprendimento, quindi infine allo STP inoltro. Questo crea un loop, poiché non ci sono porte bloccate nel triangolo A-B-C. I pacchetti scorrono lungo il percorso (B riceve ancora i pacchetti da C) che consumano ulteriore larghezza di banda finché i collegamenti non sono completamente riempiti.

Questo scenario può compromettere la rete. Un altro possibile problema che può essere causato da un collegamento unidirezionale è un blackhole del traffico.



Come funziona il protocollo UDLD

UDLD è un protocollo di Layer 2 (L2) che funziona con i meccanismi di Layer 1 (L1) per determinare lo stato fisico di un collegamento. Sul Layer 1, la negoziazione automatica si occupa della segnalazione fisica e del rilevamento degli errori. UDLD esegue attività che la negoziazione automatica non è in grado di eseguire, ad esempio il rilevamento dell'identità delle porte adiacenti e la chiusura di porte con connessione errata. Quando si abilita la negoziazione automatica e il protocollo UDLD, i rilevamenti di Layer 1 e di Layer 2 interagiscono per impedire connessioni unidirezionali fisiche e logiche e il malfunzionamento di altri protocolli.

il protocollo UDLD si basa sullo scambio di pacchetti tra dispositivi adiacenti. per il corretto funzionamento del protocollo UDLD, i dispositivi collegati devono supportare entrambi il protocollo UDLD e averlo abilitato sulle rispettive porte.

Ogni porta dello switch configurata con il protocollo UDLD invia pacchetti UDLD contenenti l'ID della porta/dispositivo e gli ID delle porte/dispositivi adiacenti rilevati da UDLD su questa porta. Le porte adiacenti vedono il proprio ID porta/dispositivo (eco) nei pacchetti provenienti dall'altro lato del collegamento. Se la porta non legge il proprio ID porta/dispositivo nei pacchetti UDLD in arrivo per un determinato periodo di tempo, il collegamento viene considerato unidirezionale.

Questo algoritmo echo consente di rilevare i seguenti problemi:

- Il collegamento è attivo su entrambi i lati; tuttavia, i pacchetti vengono ricevuti solo da un lato.
- Errori di connessione (cavo) quando le fibre di ricezione e trasmissione non sono collegate alla stessa porta sul lato remoto.

Dopo che il collegamento unidirezionale è stato rilevato dal protocollo UDLD, la rispettiva porta viene disabilitata e sulla console viene visualizzato questo messaggio:

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

La porta disabilitata dal protocollo UDLD rimane disabilitata finché non viene abilitata manualmente o finché non scade (se configurato).

Modalità di funzionamento del protocollo UDLD

Il protocollo UDLD può funzionare in due modalità, normale e aggressiva.

- In modalità normale, se lo stato del collegamento della porta era impostato su bidirezionale e le informazioni UDLD scadono, il protocollo UDLD non prende alcuna iniziativa. Lo stato della porta del protocollo UDLD è contrassegnato come undetermined (non determinato). Il comportamento della porta è conforme allo stato STP.
- In modalità aggressiva, se lo stato del collegamento della porta è impostato su bidirezionale e le informazioni UDLD scadono mentre il collegamento sulla porta è ancora attivo, il protocollo UDLD cerca di ristabilire lo stato della porta. In caso contrario, la porta viene messa nello stato errdisable.

Le informazioni UDLD scadute si verificano quando la porta con protocollo UDLD non riceve pacchetti UDLD dalla porta adiacente per l'intera durata del tempo di attesa. Il tempo di attesa della porta è determinato dalla porta remota e dipende dall'intervallo tra i messaggi sul lato remoto. Più breve è l'intervallo tra i messaggi, più breve sarà il tempo di attesa e più veloce sarà il rilevamento. Nelle implementazioni più recenti del protocollo UDLD, è possibile configurare l'intervallo tra i messaggi. Le informazioni UDLD possono scadere a causa dell'elevato tasso di errori sulla porta causato da un problema fisico o da una mancata corrispondenza duplex. Il packet drop non significa che il collegamento sia unidirezionale e il protocollo UDLD in modalità normale non disabilita tale collegamento.

Per garantire un tempo di rilevamento adeguato, è importante essere in grado di scegliere l'intervallo tra i messaggi corretto. L'intervallo dei messaggi deve essere sufficientemente veloce da rilevare il collegamento unidirezionale prima della creazione del loop di inoltro. Tuttavia, non deve sovraccaricare la CPU dello switch. L'intervallo predefinito per i messaggi è di 15 secondi ed è abbastanza veloce da rilevare il collegamento unidirezionale prima che il loop di inoltro venga creato con timer STP predefiniti. Il tempo di rilevamento è approssimativamente uguale a tre volte l'intervallo tra i messaggi.

Ad esempio: $T_{\text{detection}} \sim \text{intervallo_messaggi} \times 3$

Se l'intervallo tra i messaggi è 15 secondi, il tempo di rilevamento è quindi 45 secondi.

Per riconvergere in caso di collegamento unidirezionale, il protocollo STP impiega un tempo calcolabile con la seguente formula: $T_{\text{riconvergenza}} = \text{durata_max} + 2 \times \text{ritardo_inoltro}$. Con i timer predefiniti, sono necessari $20 + 2 \times 15 = 50$ secondi.

Si consiglia di mantenere $T_{\text{detection}} < T_{\text{reconvergence}}$ e scegliere un intervallo di messaggi appropriato.

In modalità aggressiva, una volta che le informazioni sono scadute, UDLD cerca di ristabilire lo stato del collegamento e invia i pacchetti ogni secondo per otto secondi. Se lo stato del collegamento non è stato ancora determinato, il collegamento è disabilitato.

La modalità aggressiva aggiunge il rilevamento di queste situazioni:

- La porta è bloccata (su un lato della porta i dati non vengono né trasmessi né ricevuti, anche se il collegamento è attivo sui due lati).
- Il collegamento è attivo su un lato e inattivo sull'altro. Il problema è visibile sulle porte in fibra quando la fibra di trasmissione è scollegata sulla porta locale, il collegamento rimane attivo sul lato locale. Tuttavia, è inattivo sul lato remoto.

Recentemente, le implementazioni di dispositivi con fibra FastEthernet hanno funzionalità FEFI (Far End Fault Indication) per rendere il collegamento inattivo su entrambi i lati in situazioni simili. Su Gigabit Ethernet, una funzione simile viene fornita dalla negoziazione dei collegamenti. In genere, le porte in rame non sono soggette a questo tipo di problema, in quanto utilizzano impulsi di collegamento Ethernet per monitorare il collegamento. È importante notare che in entrambi i casi non si verifica alcun loop in avanti perché non è presente alcuna connettività tra le porte. Tuttavia, se il collegamento è su un lato e giù

sull'altro, può verificarsi un blackhole del traffico. La modalità aggressiva del protocollo UDLD è progettata proprio per evitarlo.

Disponibilità

Il protocollo UDLD è disponibile in modalità normale e aggressiva dal software Cisco IOS® versione 12 e successive.

Configurazione e monitoraggio

Eeguire il comando **show udld** per verificare se il protocollo UDLD è abilitato sulle interfacce:

```
<#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
```

Il protocollo UDLD aggressivo può essere configurato sull'interfaccia con il **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#
```

Utilizzare il comando `show udd`

e `show udd neighbors` per verificare se il protocollo UDLD è abilitato o disabilitato sulla porta e lo stato del collegamento e del router adiacente:

```
<#root>
```

```
Switch#
```

```
show udd 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 uddl 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

Utilizzare il `uddl message time` per modificare l'intervallo dei messaggi:

<#root>

Switch(config)#

uddl message time 10

UDLD message interval set to 10 seconds

L'intervallo può variare da 1 a 90 secondi, con l'impostazione predefinita di 15 secondi.

Informazioni correlate

- [Supporto tecnico e download Cisco](#)
- Per gli switch Catalyst 3560, fare riferimento [alla configurazione del protocollo UDLD](#).
- Per gli switch Catalyst 4500/4000 con Cisco IOS, fare riferimento [alla configurazione del protocollo UDLD](#).
- Per gli switch Catalyst 9300, fare riferimento alla sezione [Configurazione del protocollo UDLD](#)
- Per gli switch Catalyst 9500, fare riferimento alla sezione [Configurazione del protocollo UDLD](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).