Descrizione e configurazione della funzionalità del protocollo UDLD

Sommario

Introduzione

In questo documento viene spiegato come il protocollo Unidirectional Link Detection (UDLD) possa aiutare a prevenire i loop di inoltro e il blackholing 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.

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) trasforma la topologia fisica ridondante in una topologia di inoltro ad albero senza loop

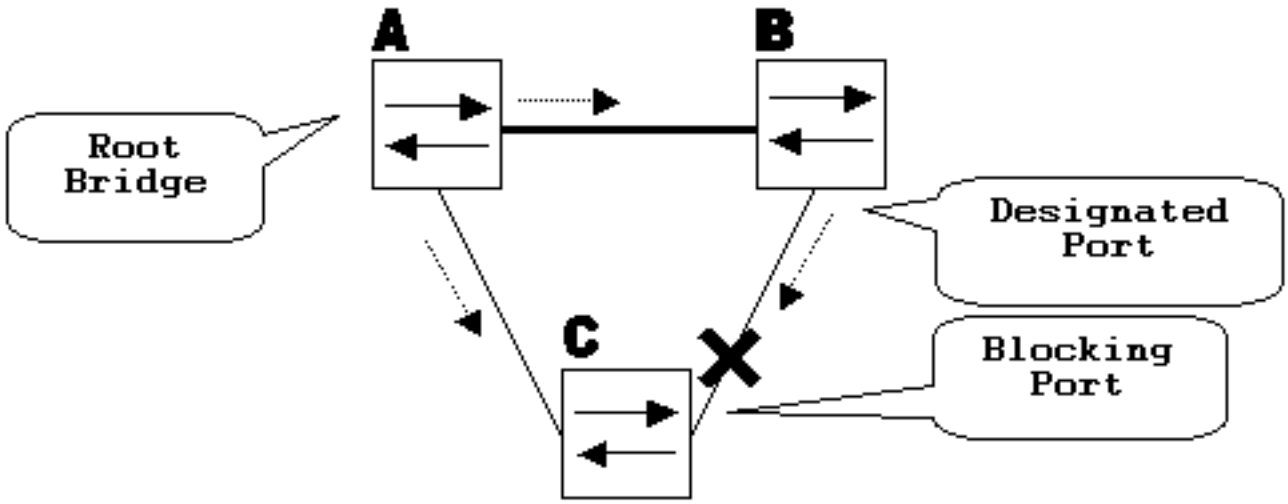
bloccando una o più porte. In questo modo, nella topologia di inoltro non si formano loop. A tal fine, il protocollo STP trasmette e riceve unità BPDU (Bridge Protocol Data Unit). Se il processo STP eseguito sullo switch con la porta di blocco arresta la ricezione delle BPDU dallo switch precedente (designato) su tale porta, il protocollo STP fa scadere le informazioni STP e passa allo stato di `inoltro`. Ciò crea un loop di inoltro o un loop STP.

I pacchetti iniziano a essere trasmessi continuamente lungo il percorso dove si è formato il loop usando sempre più larghezza di banda. Ciò può causare l'interruzione della rete.

Perché lo switch arresta la ricezione delle BPDU mentre la porta è `attiva`? Perché il collegamento è unidirezionale. Un collegamento è considerato unidirezionale quando si verifica quanto segue:

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

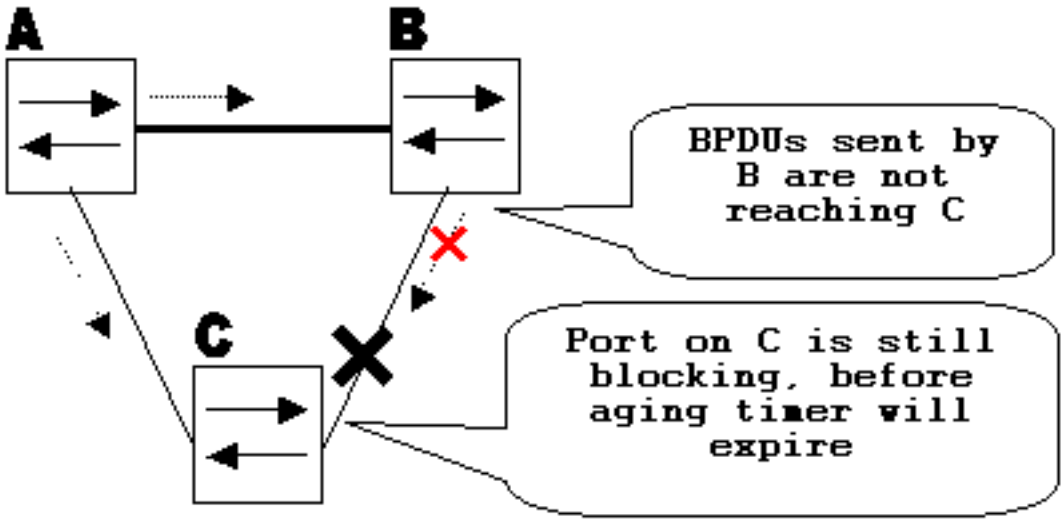
Considerare questo scenario. Le frecce indicano il flusso di BPDU del protocollo STP.



Durante il normale funzionamento, sul collegamento B-C l'unità B viene designata come bridge. Il bridge B invia le BPDU all'unità C, su cui la porta è bloccata. La porta è bloccata mentre C vede le BPDU provenienti da B su quel collegamento.

Ora, supponiamo che il collegamento B-C sia interrotto verso C. C arresta la ricezione del traffico proveniente da B, mentre B continua a ricevere il traffico da C.

C arresta la ricezione delle BPDU sul collegamento B-C e fa scadere le informazioni ricevute con l'ultima BPDU. Questa operazione richiede fino a 20 secondi, a seconda del valore impostato dal timer di durata massima del protocollo STP (maxAge STP). Quando le informazioni STP scadono, le transizioni sulla porta passano dallo stato `blocco` allo stato `ascolto` e `apprendimento`, quindi infine allo STP `inoltro`. Si crea quindi un loop di inoltro, in quanto non vi è alcuna porta di blocco nei collegamenti A-B-C. I pacchetti si spostano lungo il percorso (B riceve ancora i pacchetti da C) occupando ulteriore larghezza di banda fino a sovraccaricare del tutto i collegamenti e rendere inattiva la rete.



Il collegamento unidirezionale può causare un altro problema, noto come blackholing del traffico.

Come funziona il protocollo ULDP

Per rilevare i collegamenti unidirezionali prima che si crei un loop di inoltro, Cisco ha progettato e implementato 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. Il protocollo UDLD esegue attività che la negoziazione automatica non può eseguire, ad esempio il rilevamento delle identità dei nodi vicini e la chiusura di porte non connesse correttamente. 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 funzionare, il protocollo UDLD deve essere supportato su entrambi i dispositivi del collegamento e 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 dal protocollo UDLD sulla porta. Le porte adiacenti devono poter leggere il proprio ID porta/dispositivo (echo) 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 cablaggio dovuti a fibre di ricezione e trasmissione non 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 (UDLD-3-DISABLE:
```

`Collegamento unidirezionale rilevato sulla porta 1/2. Porta disabilitata.)`

La chiusura della porta da parte del protocollo UDLD rimane disabilitata finché non viene riabilitata manualmente o finché il timeout `errdisable`, se configurato, non scade.

Modalità di funzionamento del protocollo ULDP

Il protocollo UDLD può operare in due modalità: `normale` o `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). La porta si comporta in base 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 scadono quando la porta su cui viene eseguito il protocollo UDLD non riceve pacchetti UDLD dalla porta adiacente per tutto il 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 è il tempo di attesa e più veloce è 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 rifiuto del pacchetto non significa che il collegamento è unidirezionale e il protocollo UDLD in modalità `normale` non lo disabiliterà.

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

Ad esempio: $T_{rilevamento}$ ~ intervallo_messaggi x3

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: $T_{riconvergenza}$=durata_max + 2x ritardo_inoltro. Con i timer predefiniti, sono necessari 20+2x15 = 50 secondi.

Si consiglia di mantenere $T_{rilevamento} < T_{riconvergenza}$ scegliendo un intervallo tra i messaggi adeguato.

In modalità `aggressiva`, dopo che le informazioni sono scadute, il protocollo UDLD farà un tentativo di ristabilire lo stato del collegamento inviando i pacchetti ogni secondo per otto secondi. Se lo stato del collegamento non è stato ancora determinato, il collegamento è disabilitato.

`In modalità aggressiva`, vengono rilevate anche 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. Questo problema potrebbe verificarsi sulle porte in fibra ottica. Quando la fibra di trasmissione non è collegata sulla porta locale, il collegamento rimane `attivo` sul lato locale, anche se 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 è fornita dalla negoziazione del collegamento. 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 ricordare che in entrambi i casi non si verifica alcun loop di inoltro perché non è presente connettività tra le porte. Se il collegamento è `attivo` su un lato e `inattivo` sull'altro, potrebbe comunque verificarsi il blackholing del traffico. La modalità aggressiva del protocollo UDLD è progettata proprio per evitarlo.

Disponibilità

Il protocollo UDLD è disponibile in modalità normale in:

- Catalyst OS Version 5.1.1 e successive per la famiglia di switch Catalyst 4500/4000, 5500/5000 e 6500/6000
- Cisco IOS® Software Release 12.0(5)XU e successive per gli switch Catalyst 2900XL e 3500XL
- Cisco IOS Software Release 12.1(13)AY e successive per gli switch Catalyst 2940
- Cisco IOS Software Release 12.0(5)WC(1) o successive per gli switch Catalyst 2950
- Cisco IOS Software Release 12.1(12c)EA1 o successive per gli switch Catalyst 2955
- Cisco IOS Software Release 12.1(11)AX o successive per gli switch Catalyst 2970
- Cisco IOS Software Release 12.1(4)EA1 o successive per gli switch Catalyst 3550
- Cisco IOS Software Release 12.1(19)EA1 o successive per gli switch Catalyst 3560
- Cisco IOS Software Release 12.1(11)AX o successive per gli switch Catalyst 3750
- Cisco IOS Software Release 12.1(2)E e successive per gli switch Catalyst 6500/6000 con software di sistema Cisco IOS
- Cisco IOS Software Release 12.1(8a)EW e successive per gli switch Catalyst 4500/4000 con Cisco IOS

`La modalità aggressiva` viene implementata da queste versioni software:

- Catalyst OS Version 5.4.3 e successive per la famiglia di switch Catalyst 4500/4000, 5500/5000 e 6500/6000
- Cisco IOS Software Release 12.1(3a)E3 e successive per gli switch Catalyst 6500/6000 con software di sistema Cisco IOS
- Cisco IOS Software Release 12.1(6)EA2 o successive gli switch Catalyst 2950
- Cisco IOS Software Release 12.1(12c)EA1 o successive per gli switch Catalyst 2955
- Cisco IOS Software Release 12.1(11)AX o successive per gli switch Catalyst 2970
- Cisco IOS Software Release 12.1(4)EA1 o successive per gli switch Catalyst 3550
- Cisco IOS Software Release 12.1(11)AX o successive per gli switch Catalyst 3750

Configurazione e monitoraggio

Questi comandi descrivono in dettaglio la configurazione UDLD sugli switch Catalyst con CatOS. Il protocollo UDLD deve essere prima abilitato a livello globale (l'impostazione predefinita è disabilitato) con questo comando:

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

Immettere questo comando per verificare se il protocollo UDLD è abilitato:

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

Èinoltre necessario abilitare il protocollo UDLD sulle porte necessarie con questo comando:

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

Usare il comando **show udld port** per verificare se il protocollo UDLD è abilitato o disabilitato sulla porta e qual è lo stato del collegamento:

```
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
```

La modalità aggressiva del protocollo UDLD viene abilitata sulle singole porte con il 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
```

Immettere questo comando per modificare l'intervallo tra i messaggi:

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

L'intervallo può essere compreso tra 7 e 90 secondi; il valore predefinito è 15 secondi.

Per ulteriori informazioni sulla configurazione del protocollo UDLD in IOS, consultare questi documenti:

- Sugli switch Catalyst 6500/6000 con software di sistema Cisco IOS, fare riferimento a

Configurazione del protocollo UDLD.

- Sugli switch Catalyst 2900XL/3500XL, fare riferimento alla sezione *Configurazione del rilevamento del collegamento unidirezionale* in Configurazione delle porte dello switch.
- Sugli switch Catalyst 2940, fare riferimento a Configurazione del protocollo UDLD.
- Sugli switch Catalyst 2950/2955, fare riferimento a Configurazione del protocollo UDLD.
- Sugli switch Catalyst 2970, fare riferimento a Configurazione del protocollo UDLD.
- Sugli switch Catalyst 3550, fare riferimento a Configurazione del protocollo UDLD.
- Sugli switch Catalyst 3560, fare riferimento a Configurazione del protocollo UDLD.
- Sugli switch Catalyst 4500/4000 con Cisco IOS, fare riferimento a Configurazione del protocollo UDLD.

Informazioni correlate

- Supporto della tecnologia di switching LAN
- Supporto dei prodotti per gli switch Catalyst LAN e ATM
- Documentazione e supporto tecnico – Cisco Systems