De UDLD-protocolfunctie configureren

Inhoud

Inleiding

Dit document beschrijft hoe het Unidirectional Link Detection (UDLD) protocol kan helpen om luss en verkeersanomalieën in switched netwerken te voorkomen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Conventies

Raadpleeg Cisco Technical Tips Conventies voor meer informatie over documentconventies.

Probleemdefinitie

Spanning-Tree Protocol (STP) lost redundante fysieke topologie op in een lusvrije, boomachtige voorwaartse topologie.

Om dit te doen, blokkeert het een of meerdere poorten. Met één of meerdere geblokkeerde poorten zijn er geen lussen in de voorwaartse topologie. STP vertrouwt in zijn werking op de ontvangst en transmissie van de Bridge Protocol Data Units (BPDU's). Als het STP-proces dat op de switch met een poort in een `blokkerende` staat loopt geen BPDU's ontvangt van de upstream (aangewezen) switch, verstuurt STP uiteindelijk de STP-informatie voor de poort naar de `doorstuurstatus`.

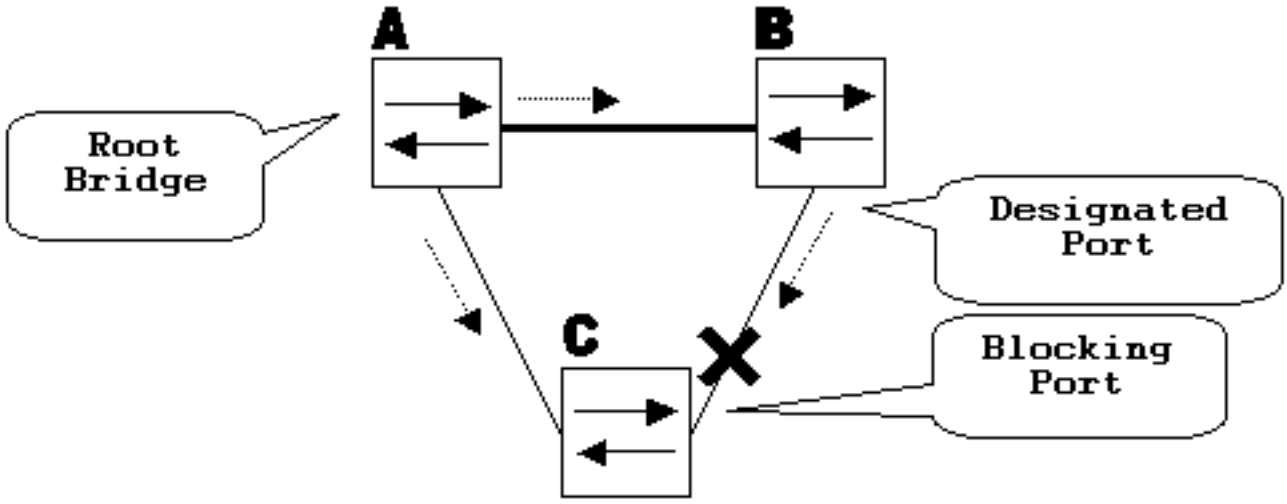
Dit kan een STP-lus creëren, waarbij pakketten oneindig langs het luspad beginnen te bladeren en steeds meer bandbreedte en bronnen verbruiken. Dit leidt tot een mogelijke netwerkonderbreking.

Hoe kan de switch BPDU's niet ontvangen terwijl de `poort is geopend`? De reden is een unidirectionele link.

Een link wordt als unidirectioneel beschouwd wanneer deze optreedt:

- De link bevindt zich aan beide zijden van de verbinding.
- De lokale kant ontvangt de pakketten niet die door de verre kant worden verzonden terwijl de verre kant pakketten ontvangt die door lokale kant worden verzonden.

Neem dit scenario. De pijlen geven de stroom van STP BPDU's aan.

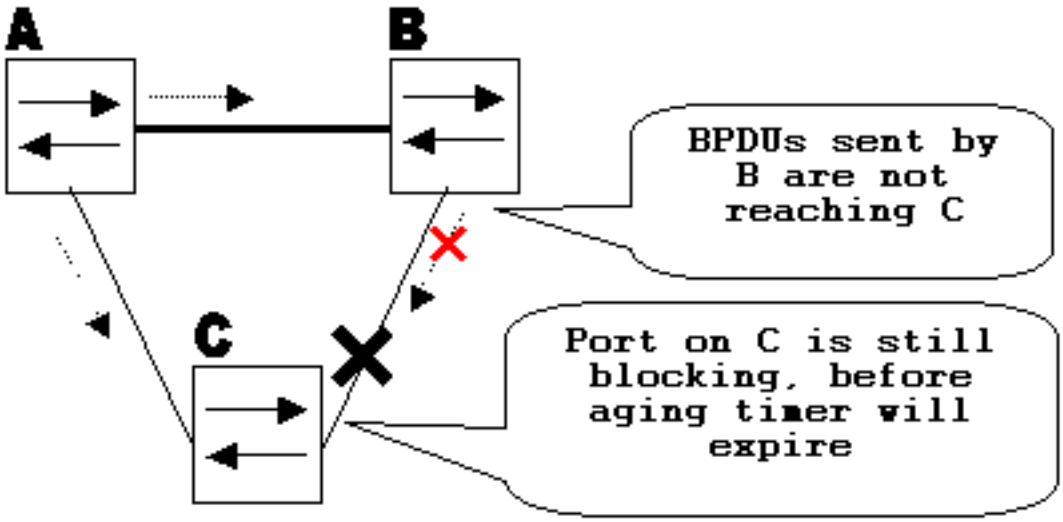


Tijdens normaal gebruik is bridge B een aangewezen poort op de koppeling B-C. Bridge B verstuurt BPDU's naar C, wat het blokkeren van de poort is. De poort wordt geblokkeerd terwijl C BPDU's van B ziet op die link.

Nu, overweeg wat gebeurt als de verbinding B-C in de richting van C. C ontbreekt om verkeer van B te ontvangen, echter, B ontvangt nog verkeer van C.

C ontvangt geen BPDU's op de koppeling B-C en veroudert de informatie die met de laatste BPDU is ontvangen. Dit duurt tot 20 seconden, wat afhankelijk is van de maxAge STP timer. Zodra de STP-informatie op de poort is verouderd, gaat die poort over van de blokkerende staat naar de `luisterstaat`, `leertoestand` en uiteindelijk naar de verzendende STP-staat. Dit leidt tot een lijn, aangezien er geen geblokkeerde haven in de driehoek A-B-C is. De pakketcyclus langs de weg (B ontvangt nog pakketten van C) die extra bandbreedte verbruikt tot de verbindingen volledig worden gevuld.

Dit scenario kan het netwerk naar beneden brengen. Een ander probleem dat door een unidirectionele verbinding kan worden veroorzaakt, is een verkeersmassa.



Hoe Unidirectionele Link Detection Protocol werkt

Om de unidirectionele link te detecteren voordat een lus in het netwerk wordt gemaakt, heeft Cisco het UDLD-protocol ontworpen en geïmplementeerd.

UDLD is een Layer 2 (L2)-protocol dat werkt met de Layer 1 (L1)-mechanismen om de fysieke status van een link te bepalen. Bij Layer 1 wordt automatisch onderhandeling uitgevoerd voor fysieke signalering en foutdetectie. UDLD voert taken uit die automatisch onderhandelen niet kan uitvoeren, zoals het detecteren van de identiteiten van buren en het afsluiten van slecht verbonden poorten. Wanneer u zowel automatische onderhandeling als UDLD inschakelt, werken Layer 1- en Layer 2-detecties samen om fysieke en logische unidirectionele verbindingen en het slecht functioneren van andere protocollen te voorkomen.

UDLD werkt door de uitwisseling van protocolpakketten tussen de aangrenzende apparaten. Om UDLD te laten werken, moeten beide apparaten op de link UDLD ondersteunen en deze ingeschakeld hebben op de betreffende poorten.

Elke switch-poort die voor UDLD is geconfigureerd, verzendt UDLD-protocolpakketten die het poortapparaat/poort-id en de buurapparaat/poort-ID's die door UDLD op die poort worden gezien, bevatten. Omliggende poorten zien hun eigen apparaat/poort-ID (echo) in de pakketten die van de andere kant worden ontvangen. Als de poort zijn eigen apparaat/poort-ID voor een bepaalde tijdsduur niet in de inkomende UDLD-pakketten ziet, wordt de koppeling als unidirectioneel beschouwd.

Dit echo-algoritme maakt de detectie van deze problemen mogelijk:

- Koppeling is aan beide kanten, maar pakketten worden slechts aan één kant ontvangen.
- Fouten in de verbinding (draad) bij het ontvangen en verzenden van glasvezel worden niet aangesloten op dezelfde poort aan de externe zijde.

Zodra de unidirectionele link door UDLD is gedetecteerd, wordt de betreffende poort uitgeschakeld en wordt dit bericht afgedrukt op de console:

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

Poortblokkering door UDLD blijft uitgeschakeld tot deze handmatig is ingeschakeld of uitschakelvertraging zonder onderbreking verloopt (indien geconfigureerd).

UDLD-werkingsmodi

UDLD kan in twee modi werken:`normalandagressief`.

a. In de normale modus, als de koppelingsstatus van de poort is bepaald als tweerichtingsverkeer en de UDLD-informatietijden zijn uitgevallen, wordt er door UDLD geen actie ondernomen. De poortstatus voor UDLD wordt aangeduid `als onbepaald`. De poort gedraagt zich in overeenstemming met zijn STP-status.

b. Inagressivemode, als de verbindingsstaat van de haven om tweerichtings wordt bepaald en de UDLD informatietijden uit terwijl de verbinding op de haven `nog` wordt `weggelaten`, UDLD probeert om de staat van de haven te herstellen. Als dit niet lukt, wordt de poort uitgeschakeld.

Leeftijd uit UDLD informatie gebeurt wanneer de haven die UDLD in werking stelt geen UDLD pakketten van de buurhaven voor de duur van greeptijd ontvangt. De wachttijd voor de poort wordt bepaald door de externe poort en is afhankelijk van het berichtinterval aan de externe kant. Hoe korter het berichtinterval, hoe korter de wachttijd en hoe sneller de detectie. Recente implementaties van UDLD maken configuratie van berichtinterval mogelijk. UDLD-informatie kan verouderen als gevolg van het hoge foutenpercentage op de poort veroorzaakt door een of ander fysiek probleem of duplex mismatch. Een dergelijke pakketdaling betekent niet dat de link unidirectioneel is en dat de UDLD innormalmode een dergelijke link niet uitschakelt.

Het is belangrijk om het juiste berichtinterval te kunnen kiezen om een juiste detectietijd te garanderen. Het berichtinterval moet snel genoeg zijn om de unidirectionele link te detecteren voordat de voorwaartse loop wordt gecreëerd, maar het mag de switch CPU niet overladen. Het standaardberichtinterval is 15 seconden, en is snel genoeg om de unidirectionele verbinding te ontdekken alvorens de voorwaartse lijn met standaardSTP timers wordt gecreëerd. De detectietijd is ongeveer gelijk aan drie keer het berichtinterval.

Bijvoorbeeld: $_{Tdetectie}$~ message_interval x3

Dit is 45 seconden voor het standaardberichtinterval van 15 seconden.

Het vereist $_{Treconvergentie}$=max_age + 2x forward_delavoor STP om in het geval van unidirectionele verbindingsmislukking terug te komen. Met de standaardtimers duurt dit 20+2x15=50 seconden.

Aanbevolen wordt om $_{Tdetectie}$< $_{Treconvergentie}$ te houden en een geschikt berichtinterval te kiezen.

Inagressivemode, zodra de informatie wordt verouderd, UDLD een poging om de verbindingsstaat opnieuw te vestigen en pakketten elke seconde voor acht seconden te verzenden. Als de verbindingsstaat nog steeds niet is bepaald, wordt de link uitgeschakeld.

Aggressivemode voegt daar een extra detectie van toe:

- De haven zit vast (aan één kant geeft noch ontvangt de haven, maar de verbinding ligt aan beide kanten).
- De link bevindt zich aan de ene kant en aan de andere kant. Dit probleem kan worden gezien op glasvezelpoorten wanneer glasvezel wordt verwijderd via de lokale poort, blijft de koppeling aan de lokale kant staan. Echter, het is aan de verre kant.

Onlangs hebben Fibre Fast Ethernet-hardwarematige implementaties Far End Fault Indication

(FEFI) functies om in deze situaties de koppeling aan beide kanten te brengen. Op Gigabit Ethernet wordt een soortgelijke functie geboden door linkonderhandeling. Koperpoorten zijn normaal gesproken niet gevoelig voor dit soort problemen, omdat ze Ethernet-linkpulsen gebruiken om de link te bewaken. Het is belangrijk om op te merken dat in beide gevallen geen voorwaartse lus optreedt omdat er geen verbinding is tussen de poorten. Echter, als de verbinding aan de ene kant is en aan de andere kant, kan zwarte gat optreden. Agressieve UDLD is ontworpen om dit te voorkomen.

Beschikbaarheid

UDLD is in de normale en agressieve modus beschikbaar bij Cisco IOS®-softwarerelease 12 en hoger.

Configuratie en bewaking

Voer de opdracht **show udld uit** om te controleren of UDLD is ingeschakeld op de interfaces:

```
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
```

Agressieve UDLD kan op de interface worden geconfigureerd met de **udld port aggressive**opdracht:

```
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#
```

Geef het**show udld** en **show udld neighbors** opdracht om te controleren of UDLD is ingeschakeld of uitgeschakeld op de poort en wat de link en de buurstaat zijn:

```
Switch#show udld 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
```

```
Switch#show udld 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
```

Gebruik de **udld message time** bevel om het berichtinterval te veranderen:

```
Switch(config)#udld message time 10
UDLD message interval set to 10 seconds
```

Het interval kan zich van 1 tot 90 seconden, met het gebrek van 15 seconden uitstrekken.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems
- Raadpleeg voor Catalyst 3560 switches de optie UDLD configureren.
- Raadpleeg voor Catalyst 4500/4000 waarop Cisco IOS wordt uitgevoerd de optie UDLD configureren.
- Raadpleeg voor Catalyst 9300 switches hoe u UDLD configureert
- Raadpleeg voor Catalyst 9500 switches hoe u UDLD configureert

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.