De UDLD-protocolfunctie begrijpen en configureren

Inhoud

Inleiding

Dit document legt uit hoe het protocol Unidirectional Link Detection (UDLD) kan helpen bij het voorkomen van lusvorming en het blokkeren van verkeer in switched netwerken.

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.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Probleemdefinitie

Spanning-Tree Protocol (STP) lost redundante fysieke topologie in een lus-vrije, boom-achtige verzendende topologie op.

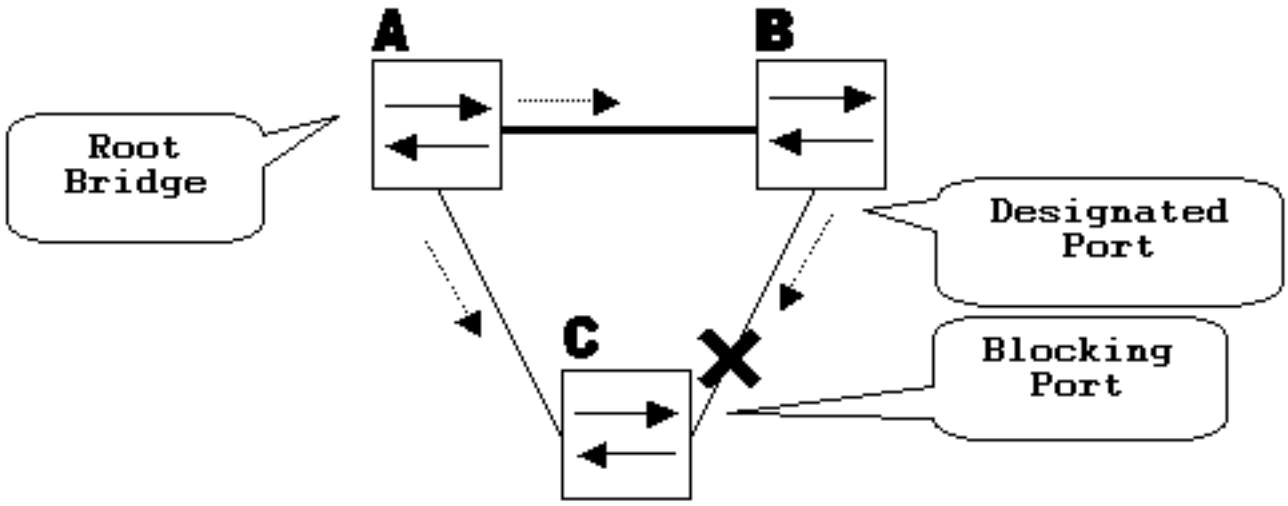
Dit gebeurt door een of meer havens te blokkeren. Door één of meer havens te blokkeren, zijn er geen loops in de het verzenden topologie. STP steunt in zijn werking op ontvangst en transmissie van de Bridge Protocol Data Units (BPDU's). Als het STP-proces dat op de switch loopt met een blokkerende poort niet meer BPDU's ontvangt vanaf de upstream (aangewezen) switch in de poort, zal STP uiteindelijk de STP-informatie voor de poort achterhalen en naar de `verzendende` staat verhuizen. Dit creëert een verstuurde lus of een STP lus.

Packets beginnen oneindig te programmeren langs het pad met een maas en nemen steeds meer bandbreedte in beslag. Dit leidt tot een mogelijke netwerkstoring.

Hoe is het mogelijk dat de switch stopt met het ontvangen van BPDU's terwijl de haven `omhoog` is? De reden is eenrichtingsverkeer. Een link wordt als eenrichtingsverkeer beschouwd wanneer dit gebeurt:

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

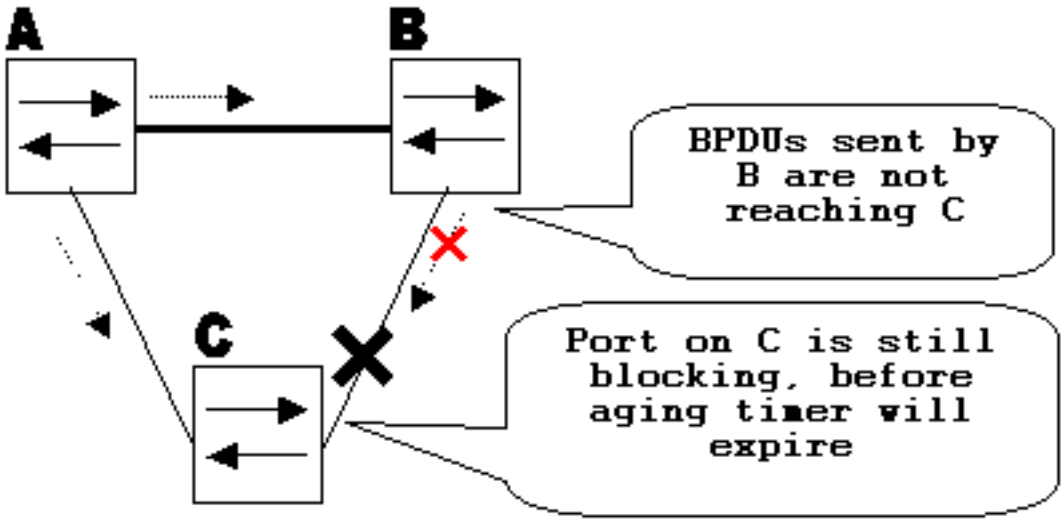
Neem dit scenario in overweging. De pijlen geven de stroom van STP BPDU's aan.



Tijdens normaal gebruik wordt bridge B aangewezen op de link B-C. Bridge B verstuurt BPDU's naar C, dat de haven blokkeert. De poort is geblokkeerd terwijl C BPDU's van B ziet op die link.

Bedenk nu wat er gebeurt als de link B-C in de richting C faalt en het verkeer van B stopt, maar B krijgt nog steeds verkeer van C.

C stopt met het ontvangen van BPDU's op de link B-C en leest de informatie die bij de laatste BPDU is ontvangen. Dit duurt tot 20 seconden, afhankelijk van de maxAge STP-timer. Zodra de STP informatie op de haven uitgerold is, die haven overschakelt van de `blokkerende` staat naar het `luisteren`, `het leren`, en uiteindelijk naar de `expanderen` STP staat. Dit creëert een doorvoerlus, aangezien er geen blokkerende poort in de driehoek A-B-C is. Het programma van pakketten langs het pad (B ontvangt nog pakketten van C) die extra bandbreedte tot de links volledig ingevuld zijn. Dit brengt het netwerk naar beneden.



Een ander mogelijk probleem dat kan worden veroorzaakt door een unidirectionele link is het blokkeren van verkeer.

Hoe een unidirectioneel koppelingsprotocol werkt

Om de unidirectionele koppelingen te detecteren voordat de verzendlus wordt aangemaakt, is Cisco ontworpen en uitgevoerd in het UDLD-protocol.

UDLD is een Layer 2 (L2) protocol dat met de mechanismen van Layer 1 (L1) werkt om de fysieke status van een link te bepalen. Bij Layer 1 zorgt de automatische onderhandeling voor fysieke signalering en foutdetectie. UDLD voert taken uit die de automatische onderhandeling niet kan uitvoeren, zoals het detecteren van de identiteit van buren en het afsluiten van niet-verbonden poorten. Wanneer u zowel automatische onderhandeling als UDLD toelaat, 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 protocolpakketten tussen de aangrenzende apparaten uit te wisselen. Om UDLD te kunnen werken, moeten beide apparaten op de link UDLD ondersteunen en deze op respectievelijke poorten hebben ingeschakeld.

Elke switch poort die voor UDLD is geconfigureerd stuurt IP-protocolpakketten naar het UDLD-protocol die de eigen voorziening/poort-ID van de poort bevatten, en de client-id's van de buurman/poort die door UDLD op die poort zijn gezien. De omliggende havens moeten hun eigen hulp/poort-ID (echo) zien in de pakketten die van de andere kant worden ontvangen.

Als de poort geen eigen id van een apparaat/poort in de inkomende UDLD-pakketten ziet voor een bepaalde tijd, wordt de link als eenrichtings beschouwd.

Dit echo-algoritme maakt het mogelijk deze problemen te detecteren:

- De link is aan beide zijden `open`, maar pakketten worden slechts aan één kant ontvangen.
- bedradingsfouten bij het ontvangen en verzenden van vezels zijn niet verbonden met dezelfde poort aan de afgelegen zijde.

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

`UDLD-3-UITGESCHAKELD: Unidirectionele link gedetecteerd op poort 1/2.0 Poorten uitgeschakeld`

Poortsluiting door UDLD blijft uitgeschakeld totdat deze handmatig wordt ingeschakeld of totdat de tijdelijke versie `automatisch` verloopt (indien geconfigureerd).

UDLD-werkingsmodi

UDLD kan op twee manieren werken: `Normaal` en `agressief`.

In de `normale` modus wordt, indien de verbindingsstaat van de haven geacht werd tweerichtings te zijn en de UDLD-informatietijden buiten, geen actie ondernomen door UDLD. De poortstatus voor UDLD is gemarkeerd als `onbepaald`. De haven gedraagt zich volgens zijn STP staat.

In `agressieve` modus, als de verbindingsstaat van de haven wordt bepaald in twee richtingen en de UDLD informatietijden uit terwijl de verbinding op de haven nog `omhoog` is, probeert UDLD de staat van de haven te herstellen. Als dit niet lukt, wordt de poort in de `foutmelding` gezet.

Veroudering van UDLD-informatie gebeurt wanneer de poort die UDLD draait geen UDLD-pakketten van de buurpoort ontvangt voor de duur van de houdtijd. De opslagtijd voor de poort wordt bepaald door de externe poort en is afhankelijk van het berichtinterval aan de afstandszijde. Hoe korter het bericht interval, hoe korter de houtetijd en hoe sneller de detectie. Recente implementaties van UDLD maken configuratie van berichtinterval mogelijk.

De informatie van UDLD kan uit door het hoge foutenpercentage op de haven veroorzaakt door een of ander fysiek probleem of duplex mismatch verouderen. Deze pakketdaling betekent niet dat de link in `normale` modus eenrichtings is en UDLD kan een dergelijke link niet uitschakelen.

Het is belangrijk om het juiste berichtinterval te kunnen kiezen om een goede detectietijd te waarborgen. Het berichtinterval moet snel genoeg zijn om de unidirectionele link te detecteren voordat de verzendloop wordt aangemaakt. De switch CPU mag echter niet overladen. Het standaardberichtinterval is 15 seconden, en is snel genoeg om de unidirectionele verbinding te detecteren voordat de verstuurde loop met standaard STP timers gecreëerd wordt. De detectietijd is ongeveer gelijk aan drie keer het berichtinterval.

Bijvoorbeeld: $_{\text{Tdetectie}}$ ~ bericht_interval x3

Dit is 45 seconden voor het standaardberichtinterval van 15 seconden.

Het duurt $_{\text{Treconvergence}}$=max_age + 2x forward_default voor de STP om opnieuw te converteren in het geval van een unidirectionele link defect. Met de standaard timers duurt het 20+2x15=50 seconden.

Aanbevolen wordt om de $_{\text{detectie}}$ < $_{\text{Tregence}}$ te houden door een geschikt berichtinterval te kiezen.

In de `agressieve` modus, zodra de informatie is verouderd, zal UDLD proberen de verbindingsstaat opnieuw te creëren door elke seconde gedurende acht seconden pakketten te verzenden. Als de verbindingsstatus nog steeds niet is bepaald, wordt de link uitgeschakeld.

`Aggressive` Mode voegt extra detectie van deze situaties toe:

- De haven zit vast (aan de ene kant geeft de haven geen opdrachten, maar de verbinding is

`aan` beide kanten niet toegestaan).
- De link is `omhoog` aan de ene kant en `omlaag` aan de andere kant. Dit probleem kan worden gezien in de vezelhavens. Wanneer de stekker van de transportvezel op de lokale poort is verwijderd, blijft de link `omhoog` aan de lokale zijde. Maar hij staat `omlaag` aan de afgelegen kant.

Onlangs hebben de hardware-implementaties van glasvezel Fast Ethernet de functies Far End Fout Indication (FEFI) om de link in deze situaties aan beide kanten naar `beneden` te brengen. Op Gigabit Ethernet wordt een soortgelijke functie geleverd door link onderhandeling. Koperpoorten zijn normaal niet gevoelig voor dit type probleem, omdat ze Ethernet link pulsen gebruiken om de link te controleren. Het is belangrijk om te vermelden dat in beide gevallen geen doorvoerlus plaatsvindt omdat er geen verbinding tussen de havens is. Als de link `aan` de ene kant `open` is en aan de andere kant `omlaag`, kan er echter een blokkering van het verkeer optreden. Aggressieve UDLD is ontworpen om dit te voorkomen.

Beschikbaarheid

UDLD is in de normale modus beschikbaar voor:

- Catalyst OS, versie 5.1.1 en hoger voor Catalyst 4500/4000, 5500/5000 en 6500/6000 Series switches
- Cisco IOS® softwarerelease 12.0(5)XU en hoger voor Catalyst 2900XL en 3500XL switches
- Cisco IOS-softwarerelease 12.1(13)AY en hoger voor Catalyst 2940 switches
- Cisco IOS-softwarerelease 12.0(5)WC(1) of hoger voor Catalyst 2950 switches
- Cisco IOS-softwarerelease 12.1(12c)EA1 of hoger voor Catalyst 2955 switches
- Cisco IOS-softwarerelease 12.1(11)AX of hoger voor Catalyst 2970-switches
- Cisco IOS-softwarerelease 12.1(4)EA1 of hoger voor Catalyst 3550 switches
- Cisco IOS-softwarerelease 12.1(19)EA1 of hoger voor Catalyst 3560 switches
- Cisco IOS-softwarerelease 12.1(11)AX of hoger voor Catalyst 3750 switches
- Cisco IOS-softwarerelease 12.1(2)E en hoger voor Catalyst 6500/6000 switches die Cisco IOS-systeemsoftware gebruiken
- Cisco IOS-softwarerelease 12.1(8a)EW en hoger voor Catalyst 4500/4000 switches die Cisco IOS-softwarerelease uitvoeren

`Aggressive` Mode wordt uitgevoerd om te beginnen met deze softwareversies:

- Catalyst OS, versie 5.4.3 en hoger voor Catalyst 4500/4000, 5500/5000 en 6500/6000 Series switches
- Cisco IOS-softwarerelease 12.1(3a)E3 en hoger voor Catalyst 6500/6000 switches die Cisco IOS-systeemsoftware gebruiken
- Cisco IOS-softwarerelease 12.1(6)EA2 of hoger voor Catalyst 2950 switches
- Cisco IOS-softwarerelease 12.1(12c)EA1 of hoger voor Catalyst 2955 switches
- Cisco IOS-softwarerelease 12.1(11)AX of hoger voor Catalyst 2970-switches
- Cisco IOS-softwarerelease 12.1(4)EA1 of hoger voor Catalyst 3550 switches
- Cisco IOS-softwarerelease 12.1(11)AX of hoger voor Catalyst 3750 switches

Configuratie- en bewaking

Deze opdrachten gedetailleerd de UDLD-configuratie op Catalyst-switches die CatOS uitvoeren. UDLD moet mondiaal eerst worden ingeschakeld (standaard is uitgeschakeld) met deze opdracht:

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

Deze opdracht geven: om te controleren of de UDLD is ingeschakeld

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

UDLD moet ook worden ingeschakeld op de benodigde poorten met deze opdracht:

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

Geef de **show udld port** opdracht uit om te controleren of UDLD ingeschakeld of uitgeschakeld is in de poort en wat de link status is:

```
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
```

Aggressive UDLD is ingeschakeld per poort met de **ingestelde** agressieve **modus maakt** *<module/poort>*opdracht **mogelijk**:

```
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
```

Geef deze opdracht uit om het berichtinterval te wijzigen:

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

Het interval kan variëren van 7 tot 90 seconden, met standaard 15 seconden.

Raadpleeg deze documenten voor meer informatie over de IOS UDLD-configuratie:

- Raadpleeg voor Catalyst 6500/6000 switches die Cisco IOS-systeemsoftware gebruiken, UDLD configureren.
- Raadpleeg voor Catalyst 2900XL/3500XL switches het gedeelte *UniDirectional Link Detectie* configureren van de Switch poorten.
- Raadpleeg voor Catalyst 2940-switches het configureren van UDLD.
- Raadpleeg voor Catalyst 2950/2955 switches het configureren van UDLD.

- Raadpleeg voor Catalyst 2970-switches het configureren van UDLD.
- Raadpleeg voor Catalyst 3550-switches het configureren van UDLD.
- Raadpleeg voor Catalyst 3560-switches het configureren van UDLD.
- Raadpleeg voor Catalyst 4500/4000 actieve Cisco IOS voor het configureren van UDLD.

Gerelateerde informatie

- Ondersteuning voor LAN-switching technologie
- Productondersteuning voor Catalyst LAN- en ATM-Switches
- Technische ondersteuning en documentatie – Cisco Systems