Konfigurieren der UDLD-Protokollfunktion

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie das Unidirectional Link Detection (UDLD)-Protokoll dazu beitragen kann, Schleifen und Datenverkehrsanomalien in Switched-Netzwerken zu verhindern.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Convention.

Problemdefinition

Das Spanning Tree Protocol (STP) löst redundante physische Topologie in eine schleifenfreie,

baumartige Vorwärtstopologie auf.

Zu diesem Zweck werden ein oder mehrere Ports blockiert. Wenn ein oder mehrere Ports blockiert sind, gibt es keine Schleifen in der Vorwärtstopologie. STP ist auf den Empfang und die Übertragung von Bridge Protocol Data Units (BPDUs) angewiesen. Wenn der STP-Prozess, der auf dem Switch mit `blockierendem` Port ausgeführt wird, keine BPDUs von seinem Upstream-Switch (designierten Switch) empfängt, altert STP die STP-Informationen für den Port schließlich und verschiebt sie in den `Weiterleitungsstatus`.

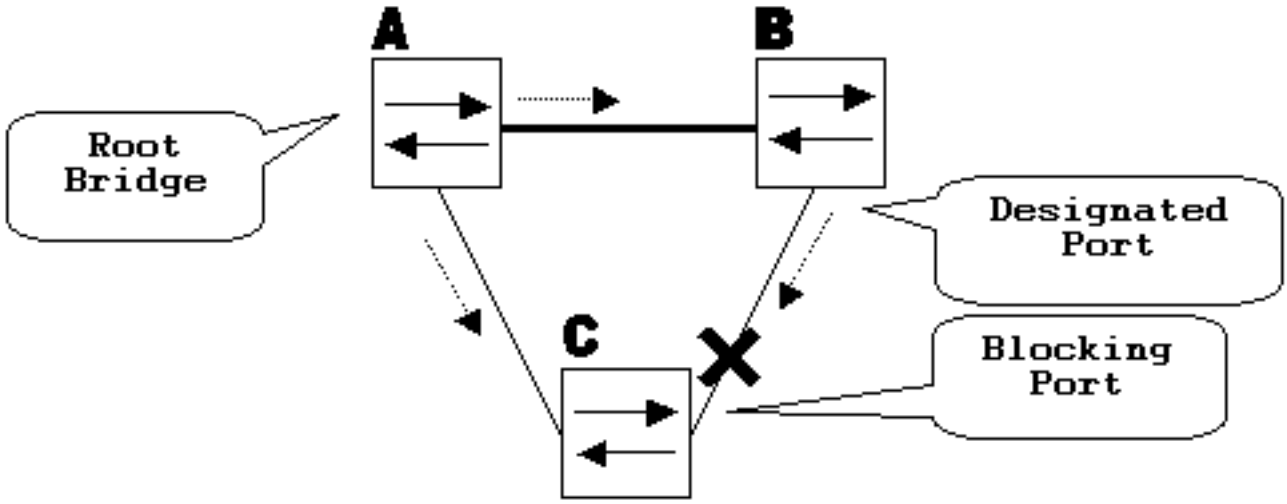
Dadurch kann eine STP-Schleife entstehen, in der Pakete unbegrenzt entlang des Schleifenpfads zyklisch verarbeitet werden und mehr Bandbreite und Ressourcen verbrauchen. Dies führt zu einem möglichen Netzwerkausfall.

Wie ist es möglich, dass der Switch keine BPDUs empfängt, während der Port `aktiv ist`? Der Grund dafür ist eine unidirektionale Verbindung.

Eine Verbindung gilt als unidirektional, wenn Folgendes auftritt:

- Die Verbindung befindet sich auf beiden Seiten der Verbindung.
- Die lokale Seite empfängt die von der Remote-Seite gesendeten Pakete nicht, während die Remote-Seite die von der lokalen Seite gesendeten Pakete empfängt.

Betrachten wir dieses Szenario. Die Pfeile zeigen den Fluss von STP-BPDUs an.

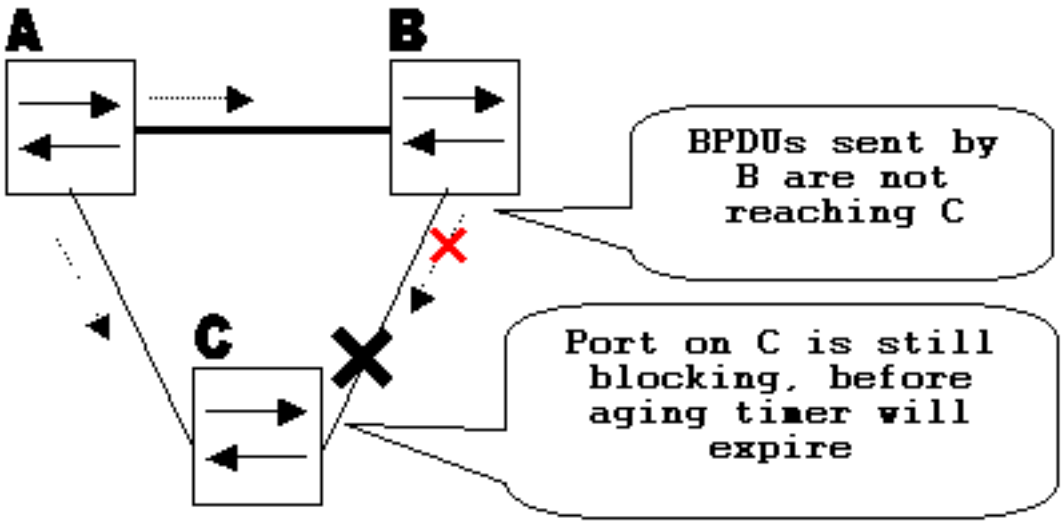


Im Normalbetrieb ist Bridge B ein designierter Port an der Verbindung B-C. Bridge B sendet BPDUs nach unten an C, wodurch der Port blockiert wird. Der Port wird blockiert, während C BPDUs von B für diese Verbindung erkennt.

Nun überlegen Sie, was passiert, wenn die Verbindung B-C in Richtung C ausfällt. C hört auf, Datenverkehr von B zu empfangen, aber B empfängt weiterhin Datenverkehr von C.

C empfängt keine BPDUs für die Verbindung B-C und altert die mit der letzten BPDU empfangenen Informationen. Dies dauert bis zu 20 Sekunden, abhängig vom maxAge STP-Timer. Sobald die STP-Informationen auf dem Port veraltet sind, wechselt dieser Port vom gesperrten Zustand in den `überwachenden, lernenden` und schließlich in den weiterleitenden STP-Zustand. Dadurch wird eine Schleife erzeugt, da es im Dreieck A-B-C keinen gesperrten Port gibt. Pakete laufen entlang des Pfads (B empfängt noch Pakete von C), was zusätzliche Bandbreite verbraucht, bis die Verbindungen vollständig gefüllt sind.

In diesem Szenario kann es zu einem Netzwerkausfall kommen. Ein weiteres mögliches Problem, das durch eine unidirektionale Verbindung verursacht werden kann, ist ein schwarzes Loch im Datenverkehr.



Funktionsweise des Unidirectional Link Detection Protocol

Um die unidirektionale Verbindung zu erkennen, bevor eine Schleife im Netzwerk erstellt wird, hat Cisco das UDLD-Protokoll entwickelt und implementiert.

UDLD ist ein Layer-2-Protokoll (L2), das mit den Layer-1-Mechanismen (L1) zusammenarbeitet, um den physischen Status einer Verbindung zu bestimmen. Auf Layer 1 übernimmt die automatische Aushandlung die physische Signalisierung und Fehlererkennung. UDLD führt Aufgaben aus, die die automatische Aushandlung nicht ausführen kann, wie die Erkennung der Identitäten von Nachbarn und das Herunterfahren falsch angeschlossener Ports. Wenn Sie sowohl Auto-Negotiation als auch UDLD aktivieren, werden Erkennungen auf Layer 1 und Layer 2 eingesetzt, um physische und logische unidirektionale Verbindungen und andere Protokollfehler zu verhindern.

UDLD ermöglicht den Austausch von Protokollpaketen zwischen benachbarten Geräten. Damit UDLD funktioniert, müssen beide Geräte an der Verbindung UDLD unterstützen und es an den jeweiligen Ports aktiviert haben.

Jeder für UDLD konfigurierte Switch-Port sendet UDLD-Protokollpakete, die die Port-Geräte-/Port-ID und die von UDLD auf diesem Port erkannten Geräte-/Port-IDs der Nachbarn enthalten. Benachbarte Ports sehen ihre eigene Geräte-/Port-ID (Echo) in den von der anderen Seite empfangenen Paketen. Wenn der Port seine eigene Geräte-/Port-ID in den eingehenden UDLD-Paketen für einen bestimmten Zeitraum nicht sieht, wird die Verbindung als unidirektional angesehen.

Dieser Echo-Algorithmus ermöglicht die Erkennung folgender Probleme:

- Die Verbindung erfolgt auf beiden Seiten, Pakete werden jedoch nur von einer Seite empfangen.
- Fehler bei der Verbindung (Verdrahtung), wenn Empfangs- und Übertragungskabel nicht am gleichen Port der Gegenstelle angeschlossen sind.

Sobald die unidirektionale Verbindung von UDLD erkannt wurde, wird der entsprechende Port

deaktiviert und die folgende Meldung auf der Konsole ausgegeben:

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

Das Port-Shutdown durch UDLD bleibt deaktiviert, bis es manuell aktiviert wird oder bis "untilerrdisabletimeout" abläuft (falls konfiguriert).

UDLD-Betriebsmodi

UDLD kann in zwei Modi betrieben werden: `normal und aggressiv`.

antwort: Wenn festgestellt wurde, dass der Verbindungsstatus des Ports bidirektional ist und die UDLD-Informationen eine Zeitüberschreitung verursachen, führt UDLD im normalen Modus keine Aktion aus. Der Port-Status für UDLD ist als `unbestimmt` markiert. Der Port verhält sich entsprechend seinem STP-Status.

b. Wenn im inaggressiven Modus der Verbindungsstatus des Ports als bidirektional festgelegt wird und die UDLD-Informationen eine Zeitüberschreitung verursachen, während die Verbindung am Port `stillgelegt` ist, versucht UDLD, den Status des Ports wiederherzustellen. Wenn dies nicht erfolgreich ist, wird der Port in den Status "errdisable" versetzt.

Eine "Age out" (Alter) der UDLD-Informationen tritt auf, wenn der Port, auf dem UDLD ausgeführt wird, während der Haltezeit keine UDLD-Pakete vom benachbarten Port empfängt. Die Haltezeit für den Port wird vom Remote-Port vorgegeben und hängt vom Nachrichtenintervall auf der Remote-Seite ab. Je kürzer das Nachrichtenintervall, desto kürzer die Haltezeit und desto schneller wird die Erkennung. Kürzlich durchgeführte UDLD-Implementierungen ermöglichen die Konfiguration des Nachrichtenintervalls. UDLD-Informationen können aufgrund der hohen Fehlerrate am Port, die durch ein physisches Problem oder Duplexungleichheit verursacht wird, veraltet sein. Ein solcher Paketverlust bedeutet nicht, dass die Verbindung unidirektional ist, und der UDLD-Normalmodus deaktiviert diese Verbindung nicht.

Es ist wichtig, das richtige Nachrichtenintervall auswählen zu können, um eine korrekte Erkennungszeit zu gewährleisten. Das Nachrichtenintervall muss schnell genug sein, um die unidirektionale Verbindung zu erkennen, bevor die Vorwärtsschleife erstellt wird. Die Switch-CPU darf dabei jedoch nicht überlastet werden. Das Standard-Nachrichtenintervall beträgt 15 Sekunden und ist schnell genug, um die unidirektionale Verbindung zu erkennen, bevor die Vorwärtsschleife mit STP-Standard-Timern erstellt wird. Die Erkennungszeit entspricht ungefähr dem Dreifachen des Nachrichtenintervalls.

Beispiel: $_{Tdetection}$~ message_interval x3

Dies sind 45 Sekunden für das Standard-Nachrichtenintervall von 15 Sekunden.

$_{Treconvergence=}$max_age + 2x forward_delay erfordert die Wiederherstellung der STP-Konvergenz bei Ausfall einer unidirektionalen Verbindung. Bei den Standard-Timern dauert es 20+2x15=50 Sekunden.

Es wird empfohlen, $_{Tdetection}$< $_{Treconvergence}$ beizubehalten und ein geeignetes Nachrichtenintervall auszuwählen.

Sobald die Informationen veraltet sind, versucht UDLD im inaggressiven Modus, den Verbindungsstatus wiederherzustellen und Pakete jede Sekunde für acht Sekunden zu senden.

Wenn der Verbindungsstatus immer noch nicht ermittelt wurde, wird die Verbindung deaktiviert.

Aggressivemode fügt zusätzliche Erkennung dieser Situationen hinzu:

- Der Port ist blockiert (auf einer Seite sendet und empfängt der Port nicht, die Verbindung befindet sich jedoch auf beiden Seiten).
- Der Link befindet sich auf der einen Seite und auf der anderen Seite. Dieses Problem tritt an Glasfaser-Ports auf, wenn die Glasfaserübertragung am lokalen Port getrennt wird und die Verbindung auf der lokalen Seite verbleibt. Es befindet sich jedoch auf der abgelegenen Seite.

In letzter Zeit verfügen Fiber FastEthernet-Hardware-Implementierungen über Far End Fault Indication (FEFI)-Funktionen, um die Verknüpfung in diesen Situationen auf beiden Seiten zu deaktivieren. Bei GigabitEthernet wird eine ähnliche Funktion durch die Link-Aushandlung bereitgestellt. Kupferports sind normalerweise nicht anfällig für diese Art von Problem, da sie Ethernet-Verbindungspulse verwenden, um die Verbindung zu überwachen. Es ist wichtig zu erwähnen, dass in beiden Fällen kein Forward-Loop auftritt, da keine Verbindung zwischen den Ports besteht. Steht die Verbindung jedoch auf der einen Seite nach oben und auf der anderen Seite nach unten, kann es zu einem Blackhole-Problem kommen. Aggressive UDLD wurde entwickelt, um dies zu verhindern.

Verfügbarkeit

UDLD ist im normalen und aggressiven Modus ab Version 12 der Cisco IOS® Software verfügbar.

Konfiguration und Überwachung

Führen Sie den Befehl **show udld** aus, um zu überprüfen, ob UDLD auf den Schnittstellen aktiviert ist:

```
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
```

Aggressive UDLD kann an der Schnittstelle mit dem **udld port aggressive**command:

```
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#
```

Stellen Sie die**show udld** und **show udld neighbors** -Befehl, um zu überprüfen, ob UDLD auf dem Port aktiviert oder deaktiviert ist, und um festzustellen, welcher Link- und Nachbarstatus vorliegt:

```
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
```

Verwenden Sie **udld message time** Befehl, um das Nachrichtenintervall zu ändern:

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

Das Intervall kann zwischen 1 und 90 Sekunden liegen, wobei der Standardwert 15 Sekunden beträgt.

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme

- Informationen zu Catalyst 3560-Switches finden Sie unter Configuring UDLD.
- Informationen zu Catalyst 4500/4000, auf denen Cisco IOS ausgeführt wird, finden Sie unter Configuring UDLD (Konfigurieren von UDLD).
- Informationen zu Catalyst 9300-Switches finden Sie unter How to Configure UDLD
- Informationen zu Catalyst 9500-Switches finden Sie unter How to Configure UDLD

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.