Verständnis und Konfiguration der Unidirectional Link Detection Protocol-Funktion

Inhalt

Einführung

In diesem Dokument wird erläutert, wie das Unidirectional Link Detection (UDLD)-Protokoll dazu beitragen kann, Weiterleitungsschleifen und Blackholing des Datenverkehrs 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.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Problemdefinition

Das Spanning Tree Protocol (STP) löst redundante physische Topologien in einer schleifenfreien,

baumähnlichen Weiterleitungstopologie auf.

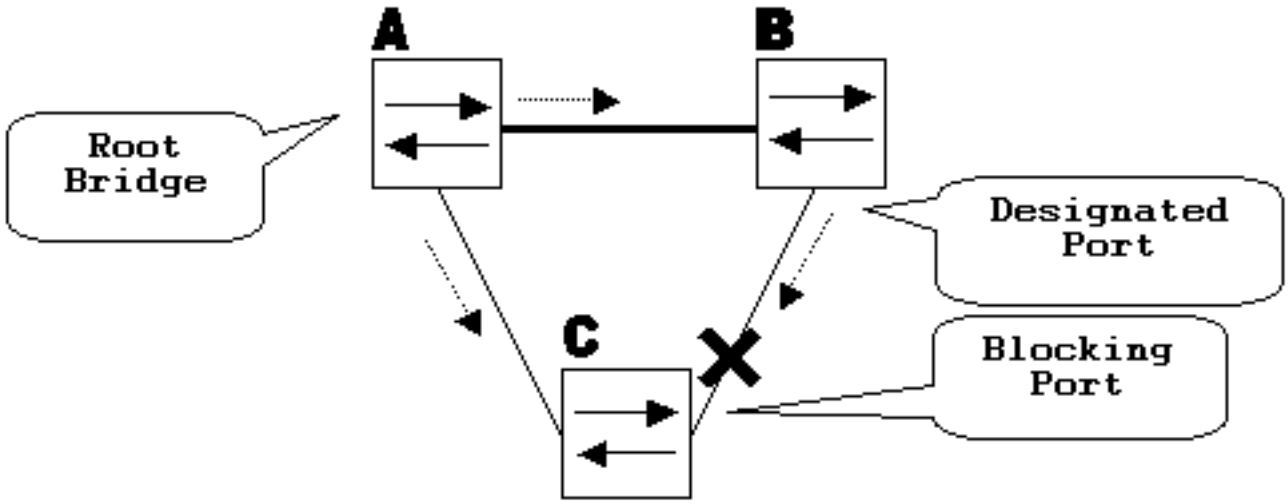
Dies geschieht durch Blockieren eines oder mehrerer Ports. Durch die Blockierung eines oder mehrerer Ports gibt es in der Weiterleitungstopologie keine Schleifen. STP ist auf den Empfang und die Übertragung der Bridge Protocol Data Units (BPDUs) angewiesen. Wenn der STP-Prozess, der auf dem Switch mit einem blockierenden Port ausgeführt wird, den Empfang von BPDUs von seinem (designierten) Upstream-Switch am Port unterbricht, werden die STP-Informationen für den Port letztendlich vom STP-System gelöscht und in den `Weiterleitungsstatus` verschoben. Dadurch wird eine Weiterleitungsschleife oder eine STP-Schleife erstellt.

Pakete beginnen auf unbestimmte Zeit über den Looped-Pfad zu laufen und verbrauchen immer mehr Bandbreite. Dies führt zu einem möglichen Netzwerkausfall.

Wie kann der Switch die BPDUs nicht mehr empfangen, während der Port `aktiv` ist? Der Grund hierfür ist eine unidirektionale Verbindung. Eine Verbindung gilt als unidirektional, wenn dies auftritt:

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

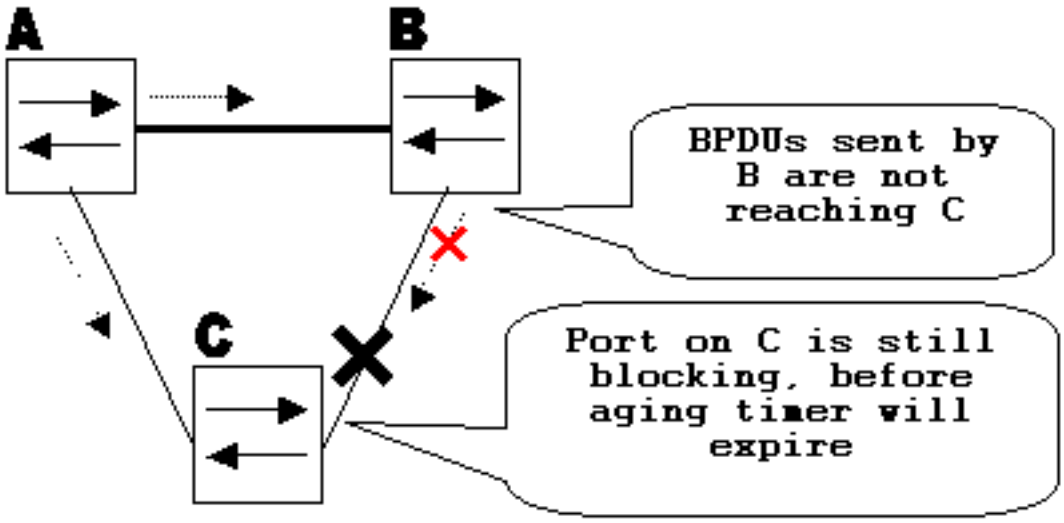
Betrachten Sie dieses Szenario. Die Pfeile zeigen den Fluss von STP-BPDUs an.



Während des normalen Betriebs ist Bridge B auf der Verbindung B-C festgelegt. Bridge B sendet BPDUs an C, der den Port blockiert. Der Port wird blockiert, während C BPDUs von B für diese Verbindung sieht.

Nun überlegen Sie, was geschieht, wenn die Verbindung B-C in Richtung C ausfällt. C stoppt den Empfang von Datenverkehr von B, aber B empfängt weiterhin Datenverkehr von C.

C beendet den Empfang von BPDUs auf der Verbindung B-C und gibt die mit der letzten BPDU erhaltenen Informationen wieder. Dies dauert je nach maxAge STP-Timer bis zu 20 Sekunden. Sobald die STP-Informationen auf dem Port ausgereift sind, wechselt dieser Port vom `Blockierungsstatus` zum `Zuhören`, `Lernen` und schließlich zum `weiterleitenden` STP-Status. Dadurch wird eine Weiterleitungs-Schleife erstellt, da im Dreieck A-B-C kein blockierender Port vorhanden ist. Pakete laufen entlang des Pfads ab (B empfängt weiterhin Pakete von C) und nehmen zusätzliche Bandbreite in Anspruch, bis die Verbindungen vollständig gefüllt sind. Dadurch wird das Netzwerk ausgeschaltet.



Ein weiteres mögliches Problem, das durch eine unidirektionale Verbindung verursacht werden kann, ist Blackholing von Datenverkehr.

Funktionsweise des Unidirectional Link Detection Protocol

Um unidirektionale Verbindungen vor der Erstellung der Weiterleitungsschleife zu erkennen, hat Cisco das UDLD-Protokoll entwickelt und implementiert.

UDLD ist ein Layer 2 (L2)-Protokoll, das mit den Layer 1 (L1)-Mechanismen arbeitet, um den physischen Status einer Verbindung zu bestimmen. Auf Layer 1 übernimmt die automatische Aushandlung die physische Signalisierung und die Fehlererkennung. UDLD führt Aufgaben aus, die die automatische Aushandlung nicht ausführen kann, z. B. die Erkennung von Nachbarn und das Herunterfahren falsch verbundener Ports. Wenn Sie die automatische Aushandlung und UDLD aktivieren, werden die Erkennungsfunktionen auf Layer 1 und Layer 2 zusammenarbeiten, um physische und logische unidirektionale Verbindungen und die Fehlfunktion anderer Protokolle zu verhindern.

UDLD tauscht Protokollpakete zwischen den benachbarten Geräten aus. Damit UDLD funktioniert, müssen beide Geräte der Verbindung UDLD unterstützen und auf den entsprechenden Ports aktiviert sein.

Jeder für UDLD konfigurierte Switch-Port sendet UDLD-Protokollpakete, die die Geräte-/Port-ID des Ports und die Geräte-/Port-IDs des Nachbarn enthalten, die UDLD an diesem Port erkennt. Benachbarte Ports sollten ihre eigene Geräte-/Port-ID (Echo) in den von der anderen Seite empfangenen Paketen sehen.

Wenn der Port seine eigene Geräte-/Port-ID für einen bestimmten Zeitraum nicht in den eingehenden UDLD-Paketen sieht, wird die Verbindung als unidirektional betrachtet.

Dieser Echo-Algorithmus ermöglicht die Erkennung folgender Probleme:

- Die Verbindung ist `auf` beiden Seiten `aktiv`, Pakete werden jedoch nur auf einer Seite empfangen.
- Verkabelungsfehler, wenn Empfangs- und Übertragungsfasern nicht mit demselben Port auf der Remote-Seite verbunden sind.

Sobald die unidirektionale Verbindung von UDLD erkannt wurde, ist der entsprechende Port deaktiviert und diese Nachricht wird auf der Konsole ausgegeben:

```
UDLD-3-DISABLE: Unidirektionale Verbindung wird an Port 1/2 erkannt. Port deaktiviert
```

Port-Shutdown durch UDLD bleibt deaktiviert, bis der Port manuell erneut aktiviert wird oder bis `errdisable` timeout abläuft (falls konfiguriert).

UDLD-Betriebsmodi

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

Im `normalen` Modus wird UDLD keine Aktion ausgeführt, wenn der Verbindungsstatus des Ports als bidirektional festgelegt wurde und die UDLD-Informationen das Zeitlimit überschreiten. Der Port-Status für UDLD ist als `nicht bestimmt` markiert. Der Port verhält sich entsprechend seinem STP-Status.

Wenn im `aggressiven` Modus der Linkstatus des Ports als bidirektional festgelegt wird und die UDLD-Informationen das Zeitlimit überschreiten, während die Verbindung am Port noch `aktiv` ist, versucht UDLD, den Status des Ports wiederherzustellen. Wenn der Port nicht erfolgreich ist, wird er in den Status `errdisable` gesetzt.

Das Veralten von UDLD-Informationen erfolgt, wenn der Port, der UDLD ausführt, während der Haltezeit keine UDLD-Pakete vom Nachbarport empfängt. Die Haltezeit für den Port wird vom Remote-Port bestimmt und hängt vom Nachrichtenintervall auf der Remote-Seite ab. Je kürzer das Nachrichtenintervall, desto kürzer ist die Haltezeit und desto schneller wird die Erkennung durchgeführt. Aktuelle UDLD-Implementierungen ermöglichen die Konfiguration des Nachrichtenintervalls.

UDLD-Informationen können aufgrund der hohen Fehlerrate am Port aufgrund eines physischen Problems oder einer Duplexungleichheit veraltet sein. Ein solcher Paketverlust bedeutet nicht, dass die Verbindung unidirektional ist, und UDLD im `normalen` Modus deaktiviert diese Verbindung nicht.

Es ist wichtig, dass Sie das richtige Nachrichtenintervall auswählen können, um eine angemessene Erkennungszeit zu gewährleisten. Das Nachrichtenintervall sollte schnell genug sein, um die unidirektionale Verbindung zu erkennen, bevor die Weiterleitungsschleife erstellt wird. Es sollte jedoch die Switch-CPU nicht überlasten. Das Standard-Nachrichtenintervall beträgt 15 Sekunden und ist schnell genug, um die unidirektionale Verbindung zu erkennen, bevor die Weiterleitungsschleife mit Standard-STP-Timern erstellt wird. Die Erkennungszeit entspricht etwa dem Dreifachen des Nachrichtenintervalls.

Beispiele: $_{TDetection}$ ~ message_interval x3

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

Bei Ausfall einer unidirektionalen Verbindung wird $_{Trekonvergenz}$=max_age + 2x forward_delay für das STP benötigt. Bei den Standard-Timern dauert es 20+2x15=50 Sekunden.

Es wird empfohlen, die $_{Erkennung}$ < $_{Trekonvergenz}$ beizubehalten, indem Sie ein geeignetes Nachrichtenintervall auswählen.

Im aggressiven Modus versucht UDLD nach dem Altern der Informationen, den Verbindungsstatus wiederherzustellen, indem es alle acht Sekunden Pakete sendet. Wenn der Linkstatus immer noch nicht bestimmt ist, ist der Link deaktiviert.

Der aggressive Modus fügt eine zusätzliche Erkennung dieser Situationen hinzu:

- Der Port ist festgeklemmt (auf einer Seite überträgt oder empfängt der Port nicht, aber die Verbindung ist auf beiden Seiten aktiv).
- Die Verbindung ist auf der einen Seite oben und unten auf der anderen Seite. Dieses Problem tritt möglicherweise an den Glasfaser-Ports auf. Wenn die Übertragungsfaser vom lokalen Port getrennt wird, bleibt die Verbindung auf der lokalen Seite aktiv. Allerdings ist es nicht auf der Fernseite.

Kürzlich wurden bei Fibre FastEthernet-Hardware-Implementierungen Far End Fault Indication (FEFI)-Funktionen implementiert, um die Verbindung in diesen Situationen auf beiden Seiten herabzusetzen. Auf Gigabit Ethernet wird eine ähnliche Funktion durch Link-Negotiation bereitgestellt. Kupferports sind normalerweise nicht für diese Art von Problemen anfällig, da sie zur Überwachung der Verbindung über Ethernet-Link-Pulse verfügen. Es ist zu erwähnen, dass in beiden Fällen keine Weiterleitungsschleife erfolgt, da keine Verbindung zwischen den Ports besteht. Wenn die Verbindung auf der einen und auf der anderen Seite aktiv ist, kann es jedoch zu Blackholing des Datenverkehrs kommen. Aggressive UDLD wurde entwickelt, um dies zu verhindern.

Verfügbarkeit

UDLD ist im normalen Modus verfügbar für:

- Catalyst OS Version 5.1.1 und höher für Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000
- Cisco IOS® Softwareversion 12.0(5)XU und höher für Catalyst Switches der Serien 2900XL und 3500XL
- Cisco IOS Software Release 12.1(13)AY und höher für Catalyst 2940 Switches
- Cisco IOS Software Release 12.0(5)WC(1) oder höher für Catalyst 2950 Switches
- Cisco IOS Softwareversion 12.1(12c)EA1 oder höher für Catalyst 2955-Switches
- Cisco IOS Software Release 12.1(11)AX oder höher für Catalyst 2970 Switches
- Cisco IOS Software Release 12.1(4)EA1 oder höher für Catalyst 3550 Switches
- Cisco IOS Software Release 12.1(19)EA1 oder höher für Catalyst 3560 Switches
- Cisco IOS Software Release 12.1(11)AX oder höher für Catalyst 3750 Switches
- Cisco IOS Software Release 12.1(2)E und höher für Catalyst 6500/6000-Switches mit Cisco IOS-Systemsoftware
- Cisco IOS Software Release 12.1(8a)EW und höher für Catalyst 4500/4000-Switches mit Cisco IOS

Der aggressive Modus wird ab den folgenden Softwareversionen implementiert:

- Catalyst OS Version 5.4.3 und höher für Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000
- Cisco IOS Software Release 12.1(3a)E3 und höher für Catalyst 6500/6000-Switches mit Cisco IOS-Systemsoftware
- Cisco IOS Software Release 12.1(6)EA2 oder höher für Catalyst 2950 Switches
- Cisco IOS Softwareversion 12.1(12c)EA1 oder höher für Catalyst 2955-Switches

- Cisco IOS Software Release 12.1(11)AX oder höher für Catalyst 2970 Switches
- Cisco IOS Software Release 12.1(4)EA1 oder höher für Catalyst 3550 Switches
- Cisco IOS Software Release 12.1(11)AX oder höher für Catalyst 3750 Switches

Konfiguration und Überwachung

Diese Befehle geben die UDLD-Konfiguration auf Catalyst-Switches an, auf denen CatOS ausgeführt wird. UDLD muss zuerst global aktiviert werden (Standard ist deaktiviert) mit dem folgenden Befehl:

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

Geben Sie den folgenden Befehl ein: um zu überprüfen, ob UDLD aktiviert ist.

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

UDLD muss auch an den erforderlichen Ports mit dem folgenden Befehl aktiviert werden:

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

Geben Sie den Befehl **show udld port** ein, um zu überprüfen, ob UDLD am Port aktiviert oder deaktiviert ist und welcher Verbindungsstatus vorliegt:

```
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 wird auf Port-Basis mit dem **festgelegten udld Aggressive-Mode enable**-Befehl ***<module/port>*** aktiviert:

```
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
```

Geben Sie diesen Befehl ein, um das Nachrichtenintervall zu ändern:

```
Vega> (enable) set udld interval 10
```

```
UDLD message interval set to 10 seconds
```
Das Intervall kann zwischen 7 und 90 Sekunden liegen, die Standardeinstellung ist 15 Sekunden.

Weitere Informationen zur IOS UDLD-Konfiguration finden Sie in diesen Dokumenten:

- Informationen zu Catalyst 6500/6000-Switches, auf denen Cisco IOS-Systemsoftware ausgeführt wird, finden Sie unter Konfigurieren von UDLD.
- Informationen zu Catalyst Switches der Serien 2900XL/3500XL finden Sie im Abschnitt *Configuring UniDirectional Link Detection (UniDirectional Link Detection* konfigurieren) zur Konfiguration der Switch-Ports.
- Informationen zu Catalyst 2940-Switches finden Sie unter Konfigurieren von UDLD.
- Informationen zu Catalyst 2950/2955-Switches finden Sie unter Konfigurieren von UDLD.
- Informationen zu Catalyst 2970-Switches finden Sie unter Konfigurieren von UDLD.
- Informationen zu Catalyst Switches der Serie 3550 finden Sie unter Konfigurieren von UDLD.
- Informationen zu Catalyst 3560-Switches finden Sie unter Konfigurieren von UDLD.
- Informationen zu Catalyst 4500/4000 mit Cisco IOS finden Sie unter Konfigurieren von UDLD.

Zugehörige Informationen

- Support für LAN-Switching-Technologie
- Produkt-Support für Catalyst LAN- und ATM-Switches
- Technischer Support und Dokumentation für Cisco Systeme