Fehlerbehebung bei STP-Problemen mit Catalyst Switches

Inhalt

Einleitung

In diesem Dokument wird die Verwendung der Cisco IOS®-Software zur Behebung von STP-Problemen (Spanning Tree Protocol) beschrieben.

Hintergrundinformationen

Es gibt spezifische Befehle, die nur für Catalyst 6500/6000 gelten. Die meisten Prinzipien können jedoch

auf alle Cisco Catalyst Switches angewendet werden, auf denen Cisco IOS-Software ausgeführt wird.

Bei den meisten STPs treten die folgenden drei Probleme auf:

- Weiterleitungsschleifen.
- Überschwemmungen aufgrund einer hohen Rate von STP Topology Changes (TC)
- Probleme im Zusammenhang mit Konvergenzzeiten.

Da eine Bridge nicht über einen Mechanismus verfügt, mit dem nachverfolgt werden kann, ob ein bestimmtes Paket mehrmals weitergeleitet wird (z. B. eine IP Time to Live [TTL]), um Datenverkehr zu verwerfen, der zu lange im Netzwerk zirkuliert. Es kann nur ein Pfad zwischen zwei Geräten in derselben Layer-2-Domäne (L2) vorhanden sein.

Der Zweck von STP besteht darin, redundante Ports auf der Grundlage eines STP-Algorithmus zu blockieren und die redundante physische Topologie in eine baumartige Topologie aufzulösen. Eine Weiterleitungs-Schleife (z. B. eine STP-Schleife) tritt auf, wenn kein Port in einer redundanten Topologie blockiert wird und der Datenverkehr unbegrenzt in Kreisen weitergeleitet wird.

Sobald der Weiterleitungs-Loop startet, verstopft er die Links mit der niedrigsten Bandbreite entlang des Pfades. Wenn alle Verbindungen die gleiche Bandbreite haben, sind alle Verbindungen überlastet. Diese Überlastung verursacht einen Paketverlust und führt zu einem Netzwerkausfall in der betroffenen L2-Domäne.

Bei Überschwemmungen sind die Symptome weniger offensichtlich. Langsame Verbindungen können durch überschwemmten Datenverkehr überlastet werden, und Geräte oder Benutzer hinter diesen überlasteten Verbindungen können Langsamkeit oder einen totalen Verbindungsverlust erleben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Verschiedene Spanning Tree-Typen und deren Konfiguration Weitere Informationen finden Sie unter Configuring STP and IEEE 802.1s MST.
- Verschiedene Spanning Tree-Funktionen und deren Konfiguration Weitere Informationen finden Sie unter Konfigurieren der STP-Funktionen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Catalyst 6500 mit Supervisor 2-Engine
- Cisco IOS Software-Version 12.1(13)E

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 kennen.

Konventionen

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

Ursachen von STP-Ausfällen

STP stellt bestimmte Annahmen hinsichtlich der Betriebsumgebung her. Dies sind die für dieses Dokument wichtigsten Annahmen:

- Jede Verbindung zwischen den beiden Brücken ist bidirektional. Das bedeutet, dass, wenn A direkt mit B verbunden ist, A empfängt, was B gesendet hat, und B empfängt, was A gesendet hat, solange die Verbindung zwischen ihnen besteht.
- Jede Bridge, die STP ausführt, kann STP Bridge Protocol Data Units (BPDUs), auch als STP-Pakete bezeichnet, regelmäßig empfangen, verarbeiten und übertragen.

Obwohl diese Annahmen logisch und offensichtlich erscheinen, gibt es Situationen, in denen sie nicht erfüllt werden. In den meisten Fällen handelt es sich dabei um eine Art Hardwareproblem. Softwarefehler können jedoch auch zu STP-Ausfällen führen. Verschiedene Hardwareausfälle, Fehlkonfigurationen und Verbindungsprobleme verursachen die Mehrzahl der STP-Ausfälle, während Softwareausfälle die Minderheit ausmachen. STP-Fehler können auch aufgrund unnötiger zusätzlicher Verbindungen zwischen den Switches auftreten. Aufgrund dieser zusätzlichen Verbindungen gehen die VLANs in den Ruhezustand. Um dieses Problem zu beheben, entfernen Sie alle unerwünschten Verbindungen zwischen den Switches.

Wenn eine dieser Annahmen nicht erfüllt wird, können ein oder mehrere Bridges die BPDUs nicht empfangen oder verarbeiten. Das bedeutet, dass die Bridge (oder Bridges) die Netzwerktopologie nicht erkennt. Ohne Kenntnis der richtigen Topologie kann der Switch die Schleifen nicht blockieren. Daher fließt der Datenverkehr in der Looped-Topologie, beansprucht die gesamte Bandbreite und führt zu Netzwerkausfällen.

Beispiele dafür, warum die Switches keine BPDUs empfangen können, sind defekte Transceiver oder Gigabit Interface Converter (GBICs), Kabelprobleme oder Hardwarefehler am Port, der Linecard oder der Supervisor Engine. Ein häufiger Grund für STP-Ausfälle ist eine unidirektionale Verbindung zwischen den Bridges. In einem solchen Zustand sendet eine Bridge BPDUs, die Downstream-Bridge empfängt sie jedoch nie. Die STP-Verarbeitung kann auch durch eine überlastete CPU (99 Prozent oder mehr) unterbrochen werden, da der Switch empfangene BPDUs nicht verarbeiten kann. BPDUs können entlang des Pfads von einer Bridge zur anderen beschädigt werden, wodurch auch das ordnungsgemäße STP-Verhalten verhindert wird.

Wenn keine Ports blockiert werden, kann es vorkommen, dass neben den Weiterleitungsschleifen nur bestimmte Pakete fehlerhaft über die Ports weitergeleitet werden, die den Datenverkehr blockieren. In den meisten Fällen wird dies durch Softwareprobleme verursacht. Ein solches Verhalten kann "langsame Schleifen" verursachen. Das bedeutet, dass einige Pakete in Loops zusammengefasst sind, der Großteil des Datenverkehrs jedoch weiterhin durch das Netzwerk fließt, da die Verbindungen nicht überlastet sind.

Fehlerbehebung bei Weiterleitungsschleifen

Die Weiterleitungsschleifen unterscheiden sich sowohl hinsichtlich ihrer Ursache als auch ihrer Wirkung erheblich. Aufgrund der Vielzahl von Problemen, die sich auf das STP auswirken können, kann dieses Dokument nur allgemeine Richtlinien zur Fehlerbehebung bei Weiterleitungsschleifen bereitstellen.

Bevor Sie mit der Fehlerbehebung beginnen können, benötigen Sie folgende Informationen:

- Ein tatsächliches Topologiediagramm, das alle Switches und Bridges beschreibt.
- Die entsprechenden Portnummern (verbunden).
- STP-Konfigurationsdetails, z. B. welcher Switch der Root und Backup-Root ist, welche Verbindungen eine nicht standardmäßige Kosten- oder Prioritätsstufe haben und wo sich die Ports befinden, die den Datenverkehr blockieren.

1. Identifizieren der Schleife

Wenn sich im Netzwerk eine Weiterleitungsschleife entwickelt hat, treten die üblichen Symptome auf:

- Verlust der Verbindung zu, von und durch die betroffenen Netzwerkregionen
- Die hohe CPU-Auslastung auf Routern, die mit betroffenen Segmenten oder VLANs verbunden sind, kann zu verschiedenen Symptomen führen, wie Flapping beim Routing-Protokoll-Nachbarn oder aktives HSRP-Router-Flapping (Hot Standby Router Protocol).
- Hohe Verbindungsauslastung (oft 100 Prozent).
- Hohe Nutzung der Switch-Backplane (im Vergleich zur Baseline-Nutzung).
- Syslog-Meldungen, die auf Paketschleifen im Netzwerk hinweisen (z. B. HSRP-Meldungen über doppelte IP-Adressen).
- Syslog-Meldungen, die auf ein ständiges erneutes Lernen der Adresse oder Flapping-Meldungen bei MAC-Adressen hinweisen.
- Die Anzahl der Ausgaben nimmt an vielen Schnittstellen zu.

Jeder dieser Gründe allein kann auf verschiedene Probleme hinweisen (oder überhaupt kein Problem). Wenn jedoch viele dieser Ereignisse gleichzeitig beobachtet werden, ist es sehr wahrscheinlich, dass sich im Netzwerk eine Weiterleitungsschleife entwickelt hat. Die schnellste Möglichkeit, dies zu überprüfen, besteht in der Überprüfung der Nutzung des Switch-Backplane-Datenverkehrs:

```
<#root>

cat#

show catalyst6000 traffic-meter



traffic meter =   13%

  Never cleared

peak =   14%

  reached at 12:08:57 CET Fri Oct 4 2002
```

Hinweis: Der Catalyst 4000 mit Cisco IOS-Software unterstützt diesen Befehl derzeit nicht.

Wenn der aktuelle Datenverkehr zu hoch ist oder der Basiswert nicht bekannt ist, überprüfen Sie, ob der Spitzenwert in letzter Zeit erreicht wurde und ob er in der Nähe des aktuellen Datenverkehrs liegt. Wenn der Peak-Traffic-Level beispielsweise 15 Prozent beträgt und erst vor zwei Minuten erreicht wurde und der aktuelle Traffic-Level bei 14 Prozent liegt, bedeutet dies, dass der Switch eine ungewöhnlich hohe Last hat. Liegt die Datenverkehrslast auf einem normalen Niveau, bedeutet dies wahrscheinlich, dass entweder keine Schleife vorhanden ist oder dass dieses Gerät nicht in die Schleife involviert ist. Allerdings könnte es noch in einer langsamen Schleife beteiligt sein.

2. Ermitteln der Topologie (des Umfangs) der Schleife

Nachdem festgestellt wurde, dass der Grund für den Netzwerkausfall ein Weiterleitungs-Loop ist, besteht die höchste Priorität darin, den Loop zu stoppen und den Netzwerkbetrieb wiederherzustellen.

Um den Loop zu stoppen, müssen Sie wissen, welche Ports am Loop beteiligt sind: Schauen Sie sich die Ports mit der höchsten Verbindungsauslastung an (Pakete pro Sekunde). **Theshow**-SchnittstelleDer Cisco IOS-Softwarebefehl zeigt die Auslastung für jede Schnittstelle an.

Um nur die Nutzungsdaten und den Schnittstellennamen anzuzeigen (für eine schnelle Analyse), filtern Sie die Ausgabe des regulären Ausdrucks mit der Cisco IOS-Software. Stellen Sie **die** Show-**Schnittstelle aus. | include line**|\/seccommand to display only the packet per second statistics and the interface name:

```
<#root>

cat#

show interface | include line|\/sec


GigabitEthernet2/1 is up, line protocol is down
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
GigabitEthernet2/2 is up, line protocol is down
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec

GigabitEthernet2/3 is up, line protocol is up
  5 minute input rate 99765230 bits/sec, 24912 packets/sec

  5 minute output rate 0 bits/sec, 0 packets/sec

GigabitEthernet2/4 is up, line protocol is up

  5 minute input rate 1000 bits/sec, 27 packets/sec


 5 minute output rate 101002134 bits/sec, 25043 packets/sec

GigabitEthernet2/5 is administratively down, line protocol is down
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
GigabitEthernet2/6 is administratively down, line protocol is down
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
GigabitEthernet2/7 is up, line protocol is down
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec

GigabitEthernet2/8 is up, line protocol is up

  5 minute input rate 2000 bits/sec, 41 packets/sec
```

```
5 minute output rate 99552940 bits/sec, 24892 packets/sec
```

Achten Sie auf die Schnittstellen mit der höchsten Verbindungsauslastung. In diesem Beispiel sind dies die Schnittstellen g2/3, g2/4 und g2/8. Dies sind die Ports, die zum Loop gehören.

3. Den Kreislauf durchbrechen

Um den Loop zu unterbrechen, müssen Sie die beteiligten Ports herunterfahren oder trennen. Es ist besonders wichtig, nicht nur die Schleife zu stoppen, sondern auch die Ursache der Schleife zu finden und zu beheben. Relativ einfacher ist es, die Schleife zu brechen

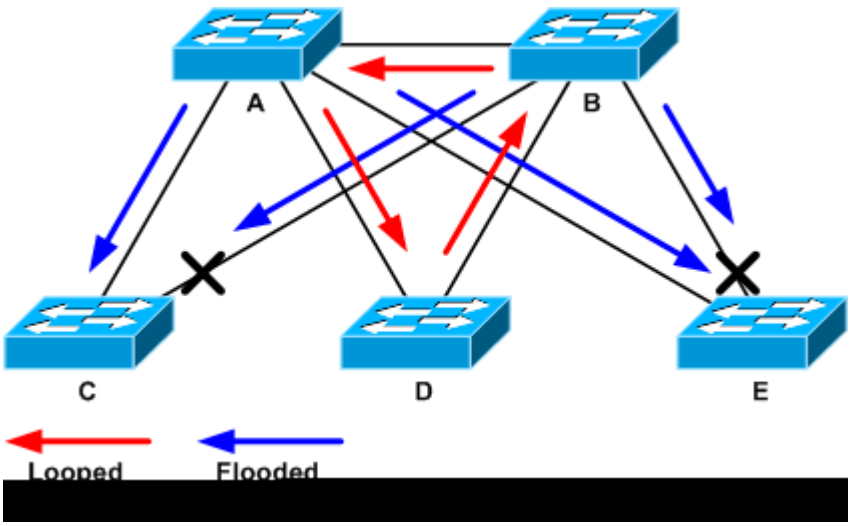
---

> **Hinweis**: Sie müssen nicht alle Ports gleichzeitig herunterfahren oder trennen. Man kann sie einzeln abschalten. Es ist besser, die Ports am Aggregationspunkt, der vom Loop betroffen ist, wie z. B. ein Distribution- oder Core-Switch, abzuschalten. Wenn Sie alle Ports gleichzeitig abschalten und einzeln aktivieren oder wieder anschließen, funktioniert das nicht. Der Loop wird gestoppt und kann nicht sofort nach dem Wiederanschließen des fehlerhaften Ports gestartet werden. Daher ist es schwierig, Ausfälle mit einem bestimmten Port zu korrelieren.

> **Hinweis**: Um den Loop zu unterbrechen, sollten Sie Informationen sammeln, bevor Sie die Switches neu starten. Andernfalls ist eine anschließende Ursachenanalyse schwierig. Nachdem Sie jeden Port deaktiviert oder getrennt haben, müssen Sie überprüfen, ob die Rückwandplatinenauslastung des Switches wieder auf dem normalen Niveau ist.

> **Hinweis**: Beachten Sie, dass Ports den Loop nicht unterstützen, aber den Datenverkehr überfluten, der mit dem Loop ankommt. Wenn Sie solche Überflutungsanschlüsse ausschalten, reduzieren Sie die Backplane-Auslastung nur geringfügig, ohne den Loop zu stoppen.

In der Topologie des nächsten Beispiels verläuft die Schleife zwischen den Switches A, B und D. Daher werden die Verbindungen AB, AD und BD aufrechterhalten. Wenn Sie einen dieser Links ausschalten, stoppen Sie die Schleife. Die Verbindungen AC, AE, BC und BE fluten den Datenverkehr, der über die Schleife eingeht.



Looped- und Flooded-Datenverkehr

Wenn der Support-Port ausgeschaltet wurde, sinkt die Backplane-Auslastung auf einen Normalwert. Sie müssen wissen, durch welches Abschalten des Ports die Backplane-Auslastung (und die Auslastung anderer Ports) auf ein normales Niveau gebracht wurde.

An diesem Punkt wird die Schleife angehalten, und der Netzwerkbetrieb wird verbessert. Da die ursprüngliche Ursache der Schleife jedoch nicht behoben wurde, gibt es noch andere Probleme.

4. Die Ursache der Schleife finden und beheben

Sobald die Schleife angehalten wurde, müssen Sie den Grund für den Beginn der Schleife ermitteln. Dies ist der schwierige Teil des Prozesses, da die Gründe variieren können. Es ist auch schwierig, ein exaktes Verfahren zu formalisieren, das in jedem Fall funktioniert.

Leitlinien:

- Suchen Sie im Topologiediagramm nach einem redundanten Pfad. Dazu gehört auch der im vorherigen Schritt gefundene Support-Port, der zu demselben Switch zurückkehrt (die Pfadpakete, die während des Loops übertragen wurden). In der Topologie des vorherigen Beispiels lautet dieser Pfad AD-DB-BA.

- Überprüfen Sie für jeden Switch auf dem redundanten Pfad, ob der Switch den richtigen STP-Root kennt.

Alle Switches in einem L2-Netzwerk müssen sich auf einen gemeinsamen STP-Root einigen. Es ist ein deutliches Symptom für Probleme, wenn Bridges konsistent eine andere ID für den STP-Root in einer bestimmten VLAN- oder STP-Instanz anzeigen. Führen Sie **den Befehl spanning-tree vlan vlan-**idaus aus, um die Root-Bridge-ID für ein bestimmtes VLAN anzuzeigen:

```
<#root>

cat#

show spanning-tree vlan 333


MST03
  Spanning tree enabled protocol mstp


Root ID    Priority    32771
             Address     0050.14bb.6000

             Cost        20000
             Port        136 (GigabitEthernet3/8)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32771  (priority 32768 sys-id-ext 3)
             Address     00d0.003f.8800
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- ------------------------
Gi3/8            Root FWD 20000     128.136  P2p
Po1              Desg FWD 20000     128.833  P2p
```

Die VLAN-Nummer kann vom Port abgerufen werden, da die am Loop beteiligten Ports in den vorherigen

Schritten eingerichtet wurden. Handelt es sich bei den betreffenden Ports um Trunks, sind in der Regel alle VLANs am Trunk beteiligt. Wenn dies nicht der Fall ist (wenn sich beispielsweise herausstellt, dass die Schleife auf einem einzelnen VLAN stattgefunden hat), können Sie versuchen, die **Show-Schnittstellen** auszugeben. **| umfassen den Befehl L2|line|**broadcast (nur für Supervisor 2 und höhere Engines auf Catalyst Switches der Serien 6500/6000, da Supervisor 1 keine Statistiken für VLAN-basiertes Switching bereitstellt). Beachten Sie nur VLAN-Schnittstellen. Das VLAN mit der höchsten Anzahl an Switch-Paketen ist häufig das VLAN, in dem der Loop stattfand:

<#root>

cat#

show interface | include L2|line|broadcast

Vlan1 is up, line protocol is up
** L2 Switched: ucast: 653704527 pkt, 124614363025 bytes - mcast:**
**   23036247 pkt, 1748707536 bytes**
**   Received 23201637 broadcasts, 0 runts, 0 giants, 0 throttles**

```
Vlan10 is up, line protocol is up
  L2 Switched: ucast: 2510912 pkt, 137067402 bytes - mcast:
         41608705 pkt, 1931758378 bytes
     Received 1321246 broadcasts, 0 runts, 0 giants, 0 throttles
Vlan11 is up, line protocol is up
  L2 Switched: ucast: 73125 pkt, 2242976 bytes - mcast:
         3191097 pkt, 173652249 bytes
     Received 1440503 broadcasts, 0 runts, 0 giants, 0 throttles
Vlan100 is up, line protocol is up
  L2 Switched: ucast: 458110 pkt, 21858256 bytes - mcast:
         64534391 pkt, 2977052824 bytes
     Received 1176671 broadcasts, 0 runts, 0 giants, 0 throttles
Vlan101 is up, line protocol is up
  L2 Switched: ucast: 70649 pkt, 2124024 bytes - mcast:
         2175964 pkt, 108413700 bytes
     Received 1104890 broadcasts, 0 runts, 0 giants, 0 throttles
```

In diesem Beispiel berücksichtigt VLAN 1 die höchste Anzahl an Broadcasts und L2-Switched-Datenverkehr. Stellen Sie sicher, dass der Root-Port richtig identifiziert wurde.

Der Root-Port muss die niedrigsten Kosten für die Root-Bridge aufweisen (manchmal ist ein Pfad im Hinblick auf Hops kürzer, aber im Hinblick auf Kosten länger, da Ports mit niedriger Geschwindigkeit höhere Kosten verursachen). Um zu bestimmen, welcher Port als Root für ein bestimmtes VLAN gilt, führen Sie den Befehl **show spanning-tree vlan** aus:

<#root>

cat#

show spanning-tree vlan 333

```
MST03
  Spanning tree enabled protocol mstp
  Root ID    Priority    32771
             Address     0050.14bb.6000
```

```
             Cost        20000

Port        136 (GigabitEthernet3/8)

             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32771  (priority 32768 sys-id-ext 3)
             Address     00d0.003f.8800
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- ------------------------
Gi3/8            Root FWD 20000     128.136  P2p
Po1              Desg FWD 20000     128.833  P2p
```

Stellen Sie sicher, dass die BPDUs regelmäßig am Root-Port und an Ports empfangen werden, die blockiert werden sollen.

BPDUs werden von der Root-Bridge in jedem Hellointervall gesendet (standardmäßig zwei Sekunden). Nicht-Root-Bridges empfangen, verarbeiten, ändern und propagieren die BPDUs, die vom Root empfangen werden. Führen Sie **den Schnittstellendetailbefehl Spanning-Tree aus**, um zu überprüfen, ob die BPDUs empfangen werden:

<#root>

```
cat#
show spanning-tree interface g3/2 detail


Port 130 (GigabitEthernet3/2) of MST00 is backup blocking
   Port path cost 20000, Port priority 128, Port Identifier 128.130.
   Designated root has priority 0, address 0007.4f1c.e847
   Designated bridge has priority 32768, address 00d0.003f.8800
   Designated port id is 128.129, designated path cost 2000019
   Timers: message age 4, forward delay 0, hold 0


Number of transitions to forwarding state: 0

   Link type is point-to-point by default, Internal
   Loop guard is enabled by default on the port
   BPDU: sent 3,

received 53


cat#
show spanning-tree interface g3/2 detail


Port 130 (GigabitEthernet3/2) of MST00 is backup blocking
   Port path cost 20000, Port priority 128, Port Identifier 128.130.
   Designated root has priority 0, address 0007.4f1c.e847
   Designated bridge has priority 32768, address 00d0.003f.8800
   Designated port id is 128.129, designated path cost 2000019
   Timers: message age 5, forward delay 0, hold 0
   Number of transitions to forwarding state: 0
```

```
   Link type is point-to-point by default, Internal
   Loop guard is enabled by default on the port
   BPDU: sent 3,
```

received 54

> **Hinweis**: Zwischen den beiden Ausgaben des Befehls wurde eine BPDU empfangen (der Zähler wechselte von 53 zu 54).

Bei den dargestellten Zählern handelt es sich um Zähler, die vom STP-Prozess selbst verwaltet werden. Das bedeutet, dass bei einer Erhöhung der Empfangszähler nicht nur BPDU von einem physischen Port, sondern auch vom STP-Prozess empfangen wurde. Wenn die received Der BPDU-Zähler wird nicht auf dem Port inkrementiert, der der alternative Root- oder Backup-Port sein soll. Überprüfen Sie dann, ob der Port überhaupt Multicasts empfängt (BPDUs werden als Multicast gesendet). Stellen Sie **die** Zähler **für die Schnittstellenanzeige ausBefehl**:

<#root>

```
cat#
```

show interface g3/2 counters

```
Port            InOctets    InUcastPkts
```

InMcastPkts

```
   InBcastPkts
Gi3/2           14873036             2
```

89387

```
             0

Port           OutOctets  OutUcastPkts  OutMcastPkts  OutBcastPkts
Gi3/2          114365997         83776        732086            19

cat#
```

show interface g3/2 counters

```
Port            InOctets    InUcastPkts
```

InMcastPkts

```
   InBcastPkts
Gi3/2           14873677             2
```

89391

```
             0

Port           OutOctets  OutUcastPkts  OutMcastPkts  OutBcastPkts
Gi3/2          114366106         83776        732087            19
```

Eine kurze Beschreibung der STP-Portrollen finden Sie im Abschnitt Enhance STP with Loop Guard and BPDU Skew Detection (STP mit Loop Guard und BPDU-Skew-Erkennung) von Spanning-Tree Protocol-

Erweiterungen mit Loop Guard- und BPDU Skew-Erkennungsfunktionen. Wenn keine BPDUs empfangen werden, überprüfen Sie, ob der Port die Fehler zählt. Ausgabe **der Schnittstellenzähler** errorsBefehl:

<#root>

cat#

show interface g4/3 counters errors

```
Port      Align-Err    FCS-Err   Xmit-Err    Rcv-Err UnderSize OutDiscards
Gi4/3         0          0          0          0         0           0

Port  Single-Col Multi-Col  Late-Col Excess-Col Carri-Sen   Runs    Giants
Gi4/3       0         0         0          0         0        0         0
```

Es ist möglich, dass die BPDUs vom physischen Port empfangen werden, aber dennoch nicht den STP-Prozess erreichen. Wenn die in den beiden vorherigen Beispielen verwendeten Befehle zeigen, dass einige Multicasts empfangen werden und Fehler nicht gezählt werden, überprüfen Sie, ob die BPDUs auf STP-Prozessebene verworfen werden. Führen Sie **den Befehl theremote command switch test spanning-tree process-**statsauf dem Catalyst 6500 aus:

<#root>

cat#

remote command switch test spanning-tree process-stats

```
------------------TX STATS------------------
 transmission rate/sec     = 2
 paks transmitted          = 5011226
 paks transmitted (opt)    = 0
 opt chunk alloc failures  = 0
 max opt chunk allocated   = 0
------------------RX STATS------------------

receive rate/sec          = 1

 paks received at stp isr  = 3947627
 paks queued at stp isr    = 3947627

paks dropped at stp isr   = 0
 drop rate/sec             = 0

 paks dequeued at stp proc = 3947627
 paks waiting in queue     = 0
 queue depth               = 7(max) 12288(total)
--------------PROCESSING STATS---------------
 queue wait time (in ms)   = 0(avg) 540(max)
 processing time (in ms)   = 0(avg) 4(max)
 proc switch count         = 100
 add vlan ports            = 20
 time since last clearing  = 2087269 sec
```

Der in diesem Beispiel verwendete Befehl zeigt die STP-Prozessstatistiken an. Es ist wichtig zu überprüfen, ob die Zähler für das Verwerfen von Paketen und für das Empfangen von Paketen erhöht werden. Wenn die empfangenen Pakete nicht erhöht werden, der physische Port jedoch Multicasts empfängt, stellen Sie sicher, dass die Pakete von der In-Band-Schnittstelle des Switches (der Schnittstelle der CPU) empfangen werden. Ausgabe **des Fernbefehls show ibc | i rx_**inputcommand auf dem Catalyst 6500/6000:

```
<#root>

cat#

remote command switch show ibc | i rx_input


rx_inputs=

5626468

, rx_cumbytes=859971138

cat#

remote command switch show ibc | i rx_input


rx_inputs=

5626471

, rx_cumbytes=859971539
```

Dieses Beispiel zeigt, dass der In-Band-Port zwischen den Ausgängen 23 Pakete empfangen hat.

> **Hinweis**: Diese 23 Pakete sind nicht nur BPDU-Pakete. Dies ist ein globaler Zähler für alle Pakete, die vom In-Band-Port empfangen werden.

Wenn es keinen Hinweis darauf gibt, dass BPDUs auf dem lokalen Switch oder Port verloren gehen, müssen Sie zum Switch auf der anderen Seite der Verbindung wechseln und überprüfen, ob dieser Switch die BPDUs sendet. Überprüfen Sie, ob die BPDUs regelmäßig an designierte Nicht-Root-Ports gesendet werden. Wenn die Portrolle übereinstimmt, sendet der Port BPDUs, der Nachbar empfängt sie jedoch nicht. Überprüft, ob BPDUs gesendet werden. Stellen Sie **die** folgende **Spanning-Tree-Schnittstellenbeschreibung ausBefehl**:

```
<#root>

cat#

show spanning-tree interface g3/1 detail


Port 129 (GigabitEthernet3/1) of MST00 is

designated

 forwarding
   Port path cost 20000, Port priority 128, Port Identifier 128.129.
   Designated root has priority 0, address 0007.4f1c.e847
   Designated bridge has priority 32768, address 00d0.003f.8800
```

```
   Designated port id is 128.129, designated path cost 2000019
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 0
   Link type is point-to-point by default, Internal
   Loop guard is enabled by default on the port


BPDU: sent 1774

, received 1

cat#

show spanning-tree interface g3/1 detail


Port 129 (GigabitEthernet3/1) of MST00 is

designated

 forwarding
   Port path cost 20000, Port priority 128, Port Identifier 128.129.
   Designated root has priority 0, address 0007.4f1c.e847
   Designated bridge has priority 32768, address 00d0.003f.8800
   Designated port id is 128.129, designated path cost 2000019
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 0
   Link type is point-to-point by default, Internal
   Loop guard is enabled by default on the port


BPDU: sent 1776

, received 1
```

In diesem Beispiel werden zwei BPDUs zwischen den Ausgängen gesendet.

> **Hinweis**: Der STP-Prozess erhält den Sentcounter `BPDU`: aufrecht. Dies bedeutet, dass der Zähler anzeigt, dass die BPDU an den physischen Port gesendet wurde und gesendet wird. Überprüfen Sie, ob die Port-Zähler für übertragene Multicast-Pakete ansteigen. Geben Sie den Befehl **show interface counters**ein. Dies kann bei der Bestimmung des Datenverkehrsflusses der BPDUs helfen.

<#root>

```
cat#

show interface g3/1 counters


Port            InOctets   InUcastPkts   InMcastPkts   InBcastPkts
Gi3/1          127985312         83776        812319            19

Port           OutOctets  OutUcastPkts

OutMcastPkts

  OutBcastPkts
Gi3/1          131825915          3442

872342
```

```
           386

cat#

show interface g3/1 counters


Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Gi3/1          127985312          83776         812319             19

Port           OutOctets   OutUcastPkts

OutMcastPkts

  OutBcastPkts
Gi3/1          131826447           3442

872346

           386
```

Bei all diesen Schritten soll nach dem Switch oder Link gesucht werden, über den keine BPDUs empfangen, gesendet oder verarbeitet werden. Möglicherweise hat das STP den richtigen Status für den Port berechnet, kann diesen Status jedoch aufgrund eines Problems auf der Kontrollebene nicht auf der Weiterleitungshardware festlegen. Eine Schleife kann erstellt werden, wenn der Port nicht auf Hardwareebene blockiert wird. Wenn Sie der Meinung sind, dass dieses Problem in Ihrem Netzwerk auftritt, wenden Sie sich an den technischen Support von Cisco, um weitere Unterstützung zu erhalten.

5. Stellen Sie die Redundanz wieder her

Sobald das Gerät oder die Verbindung gefunden wurde, das bzw. die den Loop verursacht, muss dieses Gerät vom Netzwerk isoliert werden, oder das Problem muss behoben werden (z. B. Glasfaser oder GBIC ersetzen). Die redundanten Verbindungen, die in Schritt 3 getrennt wurden, müssen wiederhergestellt werden.

Es ist wichtig, das Gerät oder die Verbindung, die die Schleife verursacht, nicht zu manipulieren, da viele Bedingungen, die zu einer Schleife führen, vorübergehend, intermittierend und instabil sind. Dies bedeutet, dass, wenn die Bedingung in oder nach der Untersuchung gelöscht wird, die Bedingung nicht für eine Weile oder überhaupt nicht auftreten. Diese Bedingung muss aufgezeichnet werden, damit der technische Support von Cisco sie weiter untersuchen kann. Es ist wichtig, dass Sie Informationen über den Zustand sammeln, bevor Sie die Switches zurücksetzen. Wenn eine Bedingung nicht mehr vorliegt, ist es unmöglich, die Ursache der Schleife zu bestimmen. Wenn Sie die Informationen sammeln, stellen Sie sicher, dass dieses Problem nicht die Schleife erneut verursacht. Weitere Informationen finden Sie unter Absichern des Netzwerks gegen Weiterleitungsschleifen.

Untersuchung von Topologieänderungen

Die Rolle des Topologieänderungsmechanismus (TC) besteht darin, die L2-Weiterleitungstabellen zu korrigieren, nachdem die Topologie geändert wurde. Dies ist erforderlich, um einen Verbindungsausfall zu vermeiden, da MAC-Adressen, auf die zuvor über bestimmte Ports zugegriffen wurde, sich ändern und über verschiedene Ports zugänglich werden können. TC verkürzt das Alter der Weiterleitungstabelle auf allen Switches im VLAN, auf denen das TC auftritt. Wenn die Adresse also nicht neu gelernt wird, altert sie und es tritt ein Flooding auf, um sicherzustellen, dass die Pakete die MAC-Zieladresse erreichen.

TC wird durch die Änderung des STP-Status eines Ports in den oder aus dem STPforwardingstate ausgelöst. Auch wenn die bestimmte MAC-Zieladresse nach TC veraltet ist, wird das Flooding nicht lange fortgesetzt.

Die Adresse wird erneut vom ersten Paket des Hosts abgerufen, dessen MAC-Adresse veraltet ist. Das Problem kann auftreten, wenn TC wiederholt auftreten, mit kurzen Intervallen. Da die Switches ihre Weiterleitungstabellen ständig veralten, können Überflutungen nahezu konstant sein.

> **Hinweis:** Bei Rapid STP oder Multiple STP (IEEE 802.1w und IEEE 802.1s) wird TC durch eine Änderung des Port-Status `in Richtung Weiterleitung` sowie durch die Rollenänderung `von designiertem Torot` ausgelöst. Mit Rapid STP wird die L2-Weiterleitungstabelle sofort geleert, im Gegensatz zu 802.1d, wodurch die Alterungszeit verkürzt wird. Die sofortige Leerung der Weiterleitungstabelle stellt die Verbindung schneller wieder her, kann jedoch zu mehr Überflutung führen.

TC ist ein seltenes Ereignis in einem gut konfigurierten Netzwerk. Wenn ein Link an einem Switch-Port aktiv oder inaktiv wird, kommt es schließlich zu einem TK, sobald der STP-Status des Ports in oder von `Forwarding` geändert wird. Wenn der Port flattert, führt dies zu sich wiederholenden TCPs und Flooding.

Ports mit aktivierter STP-Portfast-Funktion können keine TKs verursachen, wenn sie in den oder aus dem `Weiterleitungsstatus` wechseln. Die Konfiguration von PortFast auf allen Endgeräte-Ports (z. B. Drucker, PCs und Server) kann die Anzahl der TCs auf ein Minimum beschränken. Dies wird dringend empfohlen.

Wenn sich wiederholende TCs im Netzwerk vorhanden sind, müssen Sie die Quelle dieser TCs identifizieren und Maßnahmen zu deren Reduzierung ergreifen, um die Überflutung auf ein Minimum zu reduzieren.

Bei 802.1d werden STP-Informationen über ein TC-Ereignis über eine TC Notification (TCN), eine spezielle Art von BPDU, an die Bridges propagiert. Wenn Sie den Ports folgen, die TCN-BPDUs empfangen, können Sie das Gerät finden, das die TCs erstellt hat.

Die Ursache der Überschwemmungen ermitteln

Sie können feststellen, dass aufgrund der langsamen Leistung eine Überlastung auftritt, Pakete auf Verbindungen verworfen werden, die nicht überlastet werden sollten, und der Paketanalysator zeigt mehrere Unicast-Pakete an dasselbe Ziel an, das sich nicht im lokalen Segment befindet. Weitere Informationen zu Unicast Flooding finden Sie unter Unicast Flooding in Switched Campus Networks.

Auf einem Catalyst 6500/6000 mit Cisco IOS-Software können Sie den Zähler der Weiterleitungs-Engine (nur auf der Supervisor 2-Engine) überprüfen, um das Ausmaß der Überflutung zu schätzen. Ausgabe **des Remote-Befehlsschalters zur Anzeige früherer Statistiken | i MISS_DA|ST_**FRBefehl:

<#root>

```
cat#
remote command switch show earl statistics | i MISS_DA|ST_FR

         ST_MISS_DA     =       18                      530308834
         ST_FRMS        =       97                      969084354

cat#
remote command switch show earl statistics | i MISS_DA|ST_FR

         ST_MISS_DA     =       4                       530308838
         ST_FRMS        =       23                      969084377
```

In diesem Beispiel zeigt die erste Spalte die Änderung seit der letzten Ausführung dieses Befehls und die zweite Spalte den kumulierten Wert seit dem letzten Neustart an. Die erste Zeile zeigt die Anzahl überfluteter Frames an, die zweite Zeile die Anzahl verarbeiteter Frames. Wenn die beiden Werte nahe beieinander liegen oder der erste Wert mit hoher Geschwindigkeit zunimmt, kann es sein, dass der Switch den Datenverkehr überflutet. Dies kann jedoch nur in Verbindung mit anderen Methoden zur Überprüfung von Überschwemmungen verwendet werden, da die Zähler nicht granular sind. Es gibt einen Zähler pro Switch, nicht pro Port oder VLAN. Es ist normal, dass einige Flooding-Pakete angezeigt werden, da der Switch immer Flooding ausführen kann, wenn die MAC-Zieladresse nicht in der Weiterleitungstabelle enthalten ist. Dies kann der Fall sein, wenn der Switch ein Paket mit einer Zieladresse empfängt, die noch nicht abgefragt wurde.

Die Quelle der TCs finden

Wenn die VLAN-Nummer für das VLAN bekannt ist, in dem eine Überlastung auftritt, überprüfen Sie die STP-Zähler, um festzustellen, ob die Anzahl der TCs hoch ist oder sich regelmäßig erhöht. Geben Sie **den Befehl show spanning-tree vlan vlan-id** detail ein (in diesem Beispiel wird VLAN 1 verwendet):

```
<#root>

cat#

show spanning-tree vlan 1 detail


VLAN0001 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, sysid 1, address 0007.0e8f.04c0
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 0, address 0007.4f1c.e847
  Root port is 65 (GigabitEthernet2/1), cost of root path is 119
  Topology change flag not set, detected flag not set


Number of topology changes 1 last change occurred 00:00:35 ago
          from GigabitEthernet1/1

  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300
```

Wenn die VLAN-Nummer nicht bekannt ist, können Sie den Paketanalysator verwenden oder die TC-Zähler für alle VLANs überprüfen.

Ergreifung von Maßnahmen zur Vermeidung übermäßiger Risikofaktoren

Sie können die `Anzahl der Topologieänderungen` überwachen, um festzustellen, ob sie regelmäßig zunimmt. Wechseln Sie dann zur Bridge, die mit dem gezeigten Port verbunden ist, um den letzten TC (im vorherigen Beispiel Port GigabitEthernet1/1) zu empfangen und zu sehen, von wo der TC für diese Bridge kam. Dieser Vorgang muss wiederholt werden, bis der Endstations-Port ohne aktiviertes STP-Portfast gefunden wird oder bis die zu reparierende Flapping-Verbindung gefunden wird. Das gesamte Verfahren muss wiederholt werden, wenn TCs aus anderen Quellen stammen. Wenn der Link zu einem End-Host gehört, können Sie die PortFast-Funktion konfigurieren, um die Generierung von TCs zu verhindern.

> **Hinweis**: In der Cisco IOS Software-STP-Implementierung kann der Zähler für TCs nur inkrementiert werden, wenn ein TCN-BPDU von einem Port in einem VLAN empfangen wird. Wird eine normale

---

Konfigurations-BPDU mit einem gesetzten TC-Flag empfangen, so wird der TC-Zähler nicht inkrementiert. Das bedeutet, dass Sie, wenn Sie vermuten, dass ein TC der Grund für das Flooding ist, beginnen, die Quellen für das TC von der STP-Root-Bridge in diesem VLAN aufzuspüren. Er kann über die genauesten Informationen über die Anzahl und die Quelle der TCs verfügen.

Fehlerbehebung bei Konvergenzzeitproblemen

In bestimmten Situationen entspricht der tatsächliche STP-Betrieb nicht dem erwarteten Verhalten. Dies sind die zwei häufigsten Probleme:

- Die STP-Konvergenz oder -Rekonvergenz dauert länger als erwartet.
- Das Ergebnis der Topologie ist anders als erwartet.

Am häufigsten sind dies die Gründe für dieses Verhalten:

- Eine Diskrepanz zwischen der tatsächlichen und der dokumentierten Topologie.
- Konfigurationsfehler, z. B. eine inkonsistente Konfiguration der STP-Timer, ein zunehmender STP-Durchmesser oder eine portfast-fehlerhafte Konfiguration.
- Überlastete Switch-CPU während der Konvergenz oder Rekonvergenz
- Softwarefehler.

Wie bereits erwähnt, kann dieses Dokument aufgrund der Vielzahl von Problemen, die STP betreffen können, nur allgemeine Richtlinien für die Fehlerbehebung bereitstellen. Um zu verstehen, warum die Konvergenz länger dauert als erwartet, sehen Sie sich die Abfolge der STP-Ereignisse an, um herauszufinden, was passiert und in welcher Reihenfolge. Da bei der STP-Implementierung in der Cisco IOS-Software keine Ergebnisse protokolliert werden (mit Ausnahme bestimmter Ereignisse, z. B. Port-Inkonsistenzen), können Sie die Cisco IOS-Software verwenden, um STP zu debuggen und so eine klarere Übersicht zu erhalten. Bei STP erfolgt die Verarbeitung mit einem Catalyst 6500/6000, der Cisco IOS-Software ausführt, auf dem Switch Processor (SP) (oder Supervisor), sodass die Fehlerbehebungen auf dem SP aktiviert werden müssen. Für Cisco IOS Software-Bridge-Gruppen erfolgt die Verarbeitung auf dem Route Processor (RP), daher müssen die Debug-Meldungen auf dem RP (MSFC) aktiviert werden.

STP-Debug-Befehle verwenden

Viele STPdebugbefehle sind für die Entwicklungstechnik bestimmt. Ohne detaillierte Kenntnisse der STP-Implementierung in Cisco IOS-Software liefern sie keine sinnvollen Ergebnisse. Einige Debugging-Programme können sofort lesbare Ausgaben bereitstellen, z. B. Port-Statusänderungen, Rollenänderungen, Ereignisse wie TCs und ein Dump von empfangenen und übertragenen BPDUs. Dieser Abschnitt enthält keine vollständige Beschreibung aller Debugs, sondern stellt die am häufigsten verwendeten kurz vor.

Hinweis: Wenn Sie debugcommands verwenden, aktivieren Sie die minimal erforderlichen debugs. Wenn keine Echtzeit-Fehlerbehebung erforderlich ist, zeichnen Sie die Ausgabe im Protokoll auf, anstatt sie in der Konsole auszugeben. Übermäßige Fehlerbehebungen können die CPU überlasten und den Switch-Betrieb unterbrechen.

Um die Debug-Ausgabe an das Protokoll statt an die Konsole oder an Telnet-Sitzungen weiterzuleiten, geben Sie im globalen Konfigurationsmodus **die Protokollinformationen** und keine Protokollüberwachungsbefehle ein. Um das allgemeine Ereignisprotokoll anzuzeigen, geben Sie den Befehl

debug spanning-tree event für Per VLAN Spanning-Tree (PVST) und Rapid-PVST ein. Dies ist das erste Debugging, das Informationen über den STP-Vorgang liefert. Im MST-Modus (Multiple Spanning-Tree) funktioniert die Ausgabe des Befehls **debug spanning-tree** event nicht. Geben Sie daher den Befehl **debug spanning-tree mstp** roles ein, um die Änderungen der Portrolle anzuzeigen. Um die Port-STP-Statusänderungen anzuzeigen, geben Sie **den Befehl debug spanning-tree switch** state zusammen mit dem Befehl **debug pm** vpcommand ein:

<#root>

```
cat-sp#
debug spanning-tree switch state

Spanning Tree Port state changes debugging is on
cat-sp#
debug pm vp

Virtual port events debugging is on
Nov 19 14:03:37: SP:     pm_vp 3/1(333): during state forwarding, got event 4(remove)
Nov 19 14:03:37: SP:
 @@@
pm_vp 3/1(333):
  forwarding -> notforwarding

port 3/1 (was forwarding) goes down in vlan 333

Nov 19 14:03:37: SP: *** vp_fwdchange: single: notfwd: 3/1(333)
Nov 19 14:03:37: SP: @@@ pm_vp 3/1(333): notforwarding -> present
Nov 19 14:03:37: SP: *** vp_linkchange: single: down: 3/1(333)
Nov 19 14:03:37: SP: @@@ pm_vp 3/1(333): present -> not_present
Nov 19 14:03:37: SP: *** vp_statechange: single: remove: 3/1(333)
Nov 19 14:03:37: SP:     pm_vp 3/2(333): during state notforwarding,
  got event 4(remove)
Nov 19 14:03:37: SP:
 @@@
pm_vp 3/2(333): notforwarding -> present
Nov 19 14:03:37: SP: *** vp_linkchange: single: down: 3/2(333)

Port 3/2 (was not forwarding) in vlan 333 goes down

Nov 19 14:03:37: SP: @@@ pm_vp 3/2(333): present -> not_present
Nov 19 14:03:37: SP: *** vp_statechange: single: remove: 3/2(333)

Nov 19 14:03:53: SP:     pm_vp 3/1(333): during state not_present,
  got event 0(add)
Nov 19 14:03:53: SP: @@@ pm_vp 3/1(333): not_present -> present
Nov 19 14:03:53: SP: *** vp_statechange: single: added: 3/1(333)
Nov 19 14:03:53: SP:     pm_vp 3/1(333): during state present,
  got event 8(linkup)
```

```
Nov 19 14:03:53: SP:

 @@@

pm_vp 3/1(333): present ->
  notforwarding
Nov 19 14:03:53: SP: STP SW: Gi3/1 new blocking req for 0 vlans
Nov 19 14:03:53: SP: *** vp_linkchange: single: up: 3/1(333)

Port 3/1 link goes up and blocking in vlan 333


Nov 19 14:03:53: SP:     pm_vp 3/2(333): during state not_present,
  got event 0(add)
Nov 19 14:03:53: SP: @@@ pm_vp 3/2(333): not_present -> present
Nov 19 14:03:53: SP: *** vp_statechange: single: added: 3/2(333)

Nov 19 14:03:53: SP:     pm_vp 3/2(333): during state present,
  got event 8(linkup)
Nov 19 14:03:53: SP:

 @@@

pm_vp 3/2(333): present ->
  notforwarding
Nov 19 14:03:53: SP: STP SW: Gi3/2 new blocking req for 0 vlans
Nov 19 14:03:53: SP: *** vp_linkchange: single: up: 3/2(333)

Port 3/2 goes up and blocking in vlan 333

Nov 19 14:04:08: SP: STP SW: Gi3/1 new learning req for 1 vlans
Nov 19 14:04:23: SP: STP SW: Gi3/1 new forwarding req for 0 vlans
Nov 19 14:04:23: SP: STP SW: Gi3/1 new forwarding req for 1 vlans
Nov 19 14:04:23: SP:     pm_vp 3/1(333): during state notforwarding,
  got event 14(forward_notnotify)
Nov 19 14:04:23: SP:



@@@ pm_vp 3/1(333): notforwarding ->
  forwarding
Nov 19 14:04:23: SP: *** vp_list_fwdchange: forward: 3/1(333)

Port 3/1 goes via learning to forwarding in vlan 333
```

Um zu verstehen, warum sich STP auf eine bestimmte Weise verhält, ist es häufig hilfreich, die BPDUs anzuzeigen, die vom Switch empfangen und gesendet werden:

<#root>

```
cat-sp#

debug spanning-tree bpdu receive


Spanning Tree BPDU Received debugging is on
Nov  6 11:44:27: SP: STP: VLAN1 rx BPDU: config protocol = ieee,
  packet from GigabitEthernet2/1  , linktype IEEE_SPANNING ,
  enctype 2, encsize 17
Nov  6 11:44:27: SP: STP: enc 01 80 C2 00 00 00 00 06 52 5F 0E 50 00 26 42 42 03
Nov  6 11:44:27: SP: STP: Data 0000000000000000074F1CE847000000138048000652 5F0E4
```

```
  080100100140002000F00
Nov  6 11:44:27: SP: STP: VLAN1 Gi2/1:0000 00 00 00 000000074F1CE847 00000013
  80480006525F0E40 8010 0100 1400 0200 0F00
```

Dieses Debugging funktioniert für den PVST-, Rapid-PVST- und MST-Modus, jedoch nicht für den Inhalt der BPDUs. Sie können es jedoch verwenden, um sicherzustellen, dass BPDUs empfangen werden. Um den Inhalt der BPDU anzuzeigen, geben Sie den Befehl **debug spanning-tree switch rx** decodecommand zusammen mit dem Befehl **debug spanning-tree switch rx** process für PVST und Rapid-PVST ein. Geben Sie **den Befehl debug spanning-tree mstp bpdu-**rxein, um den Inhalt der BPDU für MST anzuzeigen:

```
<#root>

cat-sp#

debug spanning-tree switch rx decode


Spanning Tree Switch Shim decode received packets debugging is on

cat-sp#

debug spanning-tree switch rx process


Spanning Tree Switch Shim process receive bpdu debugging is on

Nov  6 12:23:20: SP: STP SW: PROC RX: 0180.c200.0000<-0006.525f.0e50 type/len 0026
Nov  6 12:23:20: SP:     encap SAP linktype ieee-st vlan 1 len 52 on v1 Gi2/1
Nov  6 12:23:20: SP:     42 42 03 SPAN
Nov  6 12:23:20: SP:     CFG P:0000 V:00 T:00 F:00 R:0000 0007.4f1c.e847 00000013
Nov  6 12:23:20: SP:     B:8048 0006.525f.0e40 80.10 A:0100 M:1400 H:0200 F:0F00

Nov  6 12:23:22: SP: STP SW: PROC RX: 0180.c200.0000<-0006.525f.0e50 type/len 0026
Nov  6 12:23:22: SP:     encap SAP linktype ieee-st vlan 1 len 52 on v1 Gi2/1
Nov  6 12:23:22: SP:     42 42 03 SPAN
Nov  6 12:23:22: SP:     CFG P:0000 V:00 T:00 F:00 R:0000 0007.4f1c.e847 00000013
Nov  6 12:23:22: SP:     B:8048 0006.525f.0e40 80.10 A:0100 M:1400 H:0200 F:0F00
```

Im MST-Modus können Sie mit dem folgenden Befehl debugeine detaillierte BPDU-Dekodierung durchführen:

```
<#root>

cat-sp#

debug spanning-tree mstp bpdu-rx


Multiple Spanning Tree Received BPDUs debugging is on
Nov 19 14:37:43: SP: MST:BPDU DUMP [

rcvd_bpdu Gi3/2

 Repeated]
Nov 19 14:37:43: SP: MST:   Proto:0 Version:3 Type:2 Role: DesgFlags[   F    ]
Nov 19 14:37:43: SP: MST:   Port_id:32897 cost:2000019
Nov 19 14:37:43: SP: MST:   root_id  :0007.4f1c.e847 Prio:0
```

```
Nov 19 14:37:43: SP: MST:   br_id    :00d0.003f.8800 Prio:32768
Nov 19 14:37:43: SP: MST:   age:2 max_age:20 hello:2 fwdelay:15
Nov 19 14:37:43: SP: MST:   V3_len:90 PathCost:30000 region:STATIC rev:1
Nov 19 14:37:43: SP: MST:   ist_m_id :0005.74
Nov 19 14:37:43: SP: MST:BPDU DUMP [
```

rcvd_bpdu Gi3/2

```
 Repeated]
Nov 19 14:37:43: SP: MST:   Proto:0 Version:3 Type:2 Role: DesgFlags[   F    ]
Nov 19 14:37:43: SP: MST:   Port_id:32897 cost:2000019
Nov 19 14:37:43: SP: MST:   root_id  :0007.4f1c.e847 Prio:0
Nov 19 14:37:43: SP: MST:   br_id    :00d0.003f.8800 Prio:32768
Nov 19 14:37:43: SP: MST:   age:2 max_age:20 hello:2 fwdelay:15
Nov 19 14:37:43: SP: MST:   V3_len:90 PathCost:30000 region:STATIC rev:1
Nov 19 14:37:43: SP: MST:   ist_m_id :0005.7428.1440 Prio:32768  Hops:18
  Num Mrec: 1
Nov 19 14:37:43: SP: MST: stci=3  Flags[ F    ] Hop:19 Role:Desg [Repeated]
Nov 19 14:37:43: SP: MST:         br_id:00d0.003f.8800 Prio:32771 Port_id:32897
  Cost:2000028.1440 Prio:32768  Hops:18  Num Mrec: 1
Nov 19 14:37:43: SP: MST: stci=3  Flags[ F    ] Hop:19 Role:Desg [Repeated]
Nov 19 14:37:43: SP: MST:         br_id:00d0.003f.8800 Prio:32771 Port_id:32897
  Cost:20000
```

> **Hinweis**: Für Cisco IOS Software, Version 12.1.13E und höher, werden bedingte Fehlerbehebungen für STP unterstützt. Das bedeutet, dass Sie BPDUs debuggen können, die auf Port- oder VLAN-Basis empfangen oder übertragen werden.

Geben Sie die **debug condition vlan vlan_num oder debug condition interface interface** commands ein, um den Bereich der debug-Ausgabe auf "per-interface" oder "per-VLAN" zu beschränken.

Schutz des Netzwerks vor Weiterleitungsschleifen

Cisco hat eine Reihe von Funktionen und Erweiterungen entwickelt, um Netzwerke vor Weiterleitungsschleifen zu schützen, wenn ein STP bestimmte Ausfälle nicht bewältigen kann.

Bei der Fehlerbehebung hilft es, einen bestimmten Fehler zu isolieren und möglicherweise zu finden, während die Implementierung dieser Verbesserungen die einzige Möglichkeit ist, das Netzwerk gegen Weiterleitungsschleifen zu schützen.

Diese Methoden schützen Ihr Netzwerk vor Weiterleitungsschleifen:

1. Aktivieren Sie Unidirectional Link Detection (UDLD) auf allen Switch-to-Switch-Verbindungen.

Weitere Informationen zu UDLD finden Sie unter Verstehen und Konfigurieren der Unidirectional Link Detection Protocol-Funktion.

2. Loop Guard auf allen Switches aktivieren

Weitere Informationen zu Loop Guard finden Sie unter Spanning-Tree Protocol Enhancements using Loop Guard and BPDU Skew Detection Features.

Wenn diese Funktion aktiviert ist, eliminieren UDLD und Loop Guard die meisten Ursachen von Weiterleitungsschleifen. Anstatt eine Weiterleitungsschleife zu erstellen, wird die defekte Verbindung (oder

alle Verbindungen, die von der defekten Hardware abhängen) heruntergefahren oder blockiert.

> **Hinweis**: Obwohl diese beiden Funktionen etwas redundant erscheinen, bietet jede ihre eigenen Funktionen. Verwenden Sie daher beide Funktionen gleichzeitig, um ein Höchstmaß an Schutz zu bieten. Einen detaillierten Vergleich von UDLD und Loop Guard finden Sie unter Loop Guard vs. Unidirectional Link Detection.

Es gibt verschiedene Meinungen darüber, ob Sie aggressives oder normales UDLD verwenden müssen. Das aggressive UDLD bietet im Vergleich zum normalen UDLD-Modus keinen besseren Schutz vor Schleifen. Aggressive UDLD erkennt Port-Engpässe (wenn die Verbindung aktiv ist, aber keine damit verbundenen Blackholes für den Datenverkehr vorhanden sind). Die Kehrseite dieser neuen Funktion ist, dass aggressives UDLD potenziell Links deaktivieren kann, wenn kein konsistenter Fehler auftritt. Häufig wird die Änderung des UDLDhellointerval mit der aggressiven UDLD-Funktion verwechselt. Das ist falsch. Timer können in beiden UDLD-Modi geändert werden.

> **Hinweis**: In seltenen Fällen kann aggressives UDLD alle Uplink-Ports abschalten, wodurch der Switch vom Rest des Netzwerks isoliert wird. Dies kann z. B. der Fall sein, wenn beide Upstream-Switches eine extrem hohe CPU-Auslastung aufweisen und UDLD im aggressiven Modus verwendet wird. Es wird daher empfohlen, Zeitüberschreitungen zu konfigurieren, die nicht erodieren können, wenn der Switch kein Out-of-Band-Management verwendet.

---

3. Aktivieren Sie PortFast auf allen Endgeräte-Ports.

Sie müssen portfast aktivieren, um die Anzahl der TCs und die anschließenden Überflutungen zu begrenzen, die sich auf die Leistung des Netzwerks auswirken können. Verwenden Sie diesen Befehl nur für Ports, die mit Endgeräten verbunden sind. Andernfalls kann eine versehentliche Topologieschleife eine Datenpaket-Schleife verursachen und den Switch- und Netzwerkbetrieb unterbrechen.

> **Achtung**: Gehen Sie vorsichtig vor, wenn Sie den Befehl **no spanning-tree portfast** verwenden. Dieser Befehl entfernt nur Port-spezifische PortFast-Befehle. Mit diesem Befehl wird "portfast" implizit aktiviert, wenn Sie den **Standardbefehl "spanning-tree portfast"** im globalen Konfigurationsmodus definieren und wenn der Port kein Trunk-Port ist. Wenn Sie portfast nicht global konfigurieren, entspricht der Befehl **no spanning-tree portfast** dem Befehl **spanning-tree portfast disable**.

---

4. Stellen Sie EtherChannels auf beiden Seiten auf den `erwünschten` Modus (sofern unterstützt) und die Option für `nicht-leise Verbindungen ein.`

Der Desirablemode kann das Port Aggregation Protocol (PAgP) aktivieren, um die Laufzeitkonsistenz zwischen den Channeling-Peers sicherzustellen. Dies bietet einen zusätzlichen Schutz vor Schleifen, insbesondere bei Kanalneukonfigurationen (z. B. wenn Verbindungen dem Kanal beitreten oder ihn verlassen, und Erkennung von Verbindungsausfällen). Es gibt einen integrierten Channel Misconfiguration Guard, der standardmäßig aktiviert ist und Weiterleitungsschleifen aufgrund von Channel-Fehlkonfigurationen oder anderen Bedingungen verhindert. Weitere Informationen zu dieser Funktion finden Sie unter Understanding EtherChannel Inconsistency Detection.

5. Deaktivieren Sie die automatische Aushandlung (falls unterstützt) auf Switch-to-Switch-Verbindungen nicht.

Mechanismen zur automatischen Aushandlung können Remote-Fehlerinformationen übermitteln, was die

schnellste Möglichkeit zur Fehlererkennung an der Remote-Seite darstellt. Wird auf der Fernseite ein Fehler erkannt, so fährt die lokale Seite die Verbindung herunter, auch wenn die Verbindung Impulse erhält. Im Vergleich zu High-Level-Erkennungsmechanismen wie UDLD ist die automatische Aushandlung extrem schnell (innerhalb von Mikrosekunden), bietet jedoch keine End-to-End-Abdeckung wie bei UDLD (z. B. der gesamte Datenpfad: CPU - Weiterleitungslogik - Port1 - Port2 - Weiterleitungslogik - CPU im Vergleich zu Port1 - Port2). Der aggressive UDLD-Modus bietet hinsichtlich der Fehlererkennung eine ähnliche Funktionalität wie die automatische Aushandlung. Wenn die Aushandlung auf beiden Seiten des Links unterstützt wird, muss UDLD nicht im aggressiven Modus aktiviert werden.

6. Vorsicht beim Einstellen der STP-Timer

STP-Timer sind voneinander und von der Netzwerktopologie abhängig. STP funktioniert nicht ordnungsgemäß, wenn an den Timern willkürliche Änderungen vorgenommen wurden. Weitere Informationen zu STP-Timern finden Sie unter Verstehen und Anpassen von Spanning Tree Protocol-Timern.

7. Wenn Denial of Service-Angriffe möglich sind, sichern Sie den Netzwerk-STP-Perimeter mit Root Guard

Root Guard und BPDU Guard ermöglichen Ihnen, STP gegen äußere Einflüsse zu schützen. Wenn ein solcher Angriff möglich ist, müssen Root Guard und BPDU Guard eingesetzt werden, um das Netzwerk zu schützen. Weitere Informationen zu Root Guard und BPDU Guard finden Sie in den folgenden Dokumenten:

- Spanning Tree Protocol Root Guard-Erweiterung
- Spanning-Tree-Verbesserung des Portfast BPDU Guard

8. Aktivieren Sie BPDU Guard an Port-Fast-fähigen Ports, um zu verhindern, dass STP die Auswirkungen von nicht autorisierten Netzwerkgeräten (z. B. Hubs, Switches und Bridging-Router) verursacht, die mit den Ports verbunden sind.

Wenn Sie Root Guard korrekt konfigurieren, verhindert dies, dass STP von außen beeinflusst wird. Wenn BPDU Guard aktiviert ist, werden die Ports, die BPDUs empfangen, geschlossen. Dies ist nützlich, um Vorfälle zu untersuchen, da BPDU Guard die Syslog-Meldung generiert und den Port herunterfährt. Wenn Root- oder BPDU-Guards Kurzzyklusschleifen nicht verhindern, werden zwei schnell aktivierte Ports direkt oder über den Hub verbunden.

9. Vermeiden Sie Benutzerdatenverkehr auf dem Management-VLAN

Das Management-VLAN ist in einem Baustein enthalten, nicht im gesamten Netzwerk.

Die Switch-Management-Schnittstelle empfängt Broadcast-Pakete über das Management-VLAN. Wenn übermäßige Broadcasts auftreten (z. B. ein Broadcast-Sturm oder eine fehlerhafte Anwendung), kann die Switch-CPU überlastet werden, was den STP-Betrieb verzerren kann.

10. Eine vorhersagbare (hardcodierte) STP-Root- und Backup-STP-Root-Platzierung

Der STP-Root und der Backup-STP-Root müssen so konfiguriert werden, dass die Konvergenz bei Ausfällen auf vorhersehbare Weise erfolgt und in jedem Szenario eine optimale Topologie erstellt wird. Belassen Sie die STP-Priorität nicht beim Standardwert, um eine unvorhersehbare Root-Switch-Auswahl zu vermeiden.

Zugehörige Informationen

- **LAN-Produkt-Support**
- **Support für LAN-Switching-Technologie**

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.