STP-Fehlerbehebung auf Catalyst-Switches mit Cisco IOS-Systemsoftware

Inhalt

Einführung

Dieses Dokument enthält Richtlinien zur Verwendung der Cisco IOS®-Software zur Behebung von Problemen mit dem Spanning Tree Protocol (STP). Es gibt spezielle Befehle, die nur für den Catalyst 6500/6000 gelten. Sie können die meisten Prinzipien jedoch auf alle Cisco Catalyst Switches anwenden, auf denen Cisco IOS-Software ausgeführt wird.

Die meisten STP-Fehlerbehebungen beziehen sich auf drei Punkte:

- Weiterleitungsschleifen
- Übermäßige Überflutung aufgrund einer hohen Rate von STP-Topologieänderungen (TC)
- Konvergenzzeiten

Da Bridging über keinen Mechanismus verfügt, um festzustellen, ob ein bestimmtes Paket mehrmals weitergeleitet wird (z. B. wird eine IP Time to Live [TTL] verwendet, um Datenverkehr zu lange im Netzwerk zu verwerfen), kann nur ein Pfad zwischen zwei Geräten in derselben Layer 2 (L2)-Domäne vorhanden sein.

STP soll redundante Ports auf Basis eines STP-Algorithmus blockieren, um redundante physische Topologien in eine baumähnliche Topologie aufzulösen. Eine Weiterleitungsschleife (z. B. eine STP-Schleife) tritt auf, wenn kein Port in einer redundanten Topologie blockiert und der Datenverkehr unbegrenzt weitergeleitet wird.

Sobald die Weiterleitungs-Schleife beginnt, wird sie wahrscheinlich die Verbindungen mit der niedrigsten Bandbreite entlang des Pfads überlasten. Wenn alle Verbindungen über dieselbe Bandbreite verfügen, werden wahrscheinlich alle Verbindungen überlastet. Diese Überlastung

führt zu Paketverlusten und zum Ausfall des Netzwerks in der betroffenen L2-Domäne.

Bei übermäßiger Überflutung sind die Symptome möglicherweise nicht so offensichtlich. Einige langsame Verbindungen können durch überlasteten Datenverkehr überlastet werden, und Geräte oder Benutzer hinter diesen überlasteten Verbindungen können langsamer oder gar nicht verbunden sein.

Voraussetzungen

Anforderungen

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

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

Verwendete Komponenten

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

- Catalyst 6500 mit Supervisor 2 Engine
- Cisco IOS Softwareversion 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 Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

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

Warum STP fehlschlägt

STP stellt bestimmte Annahmen über seine Betriebsumgebung an. Dies sind die Annahmen, die für dieses Dokument am wichtigsten sind:

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

Obwohl diese Annahmen logisch und offensichtlich erscheinen, gibt es Situationen, in denen sie nicht erfüllt werden. Die meisten dieser Situationen beinhalten ein Hardwareproblem. Software-Fehler können jedoch auch zu STP-Ausfällen führen. Verschiedene Hardwareausfälle,

Fehlkonfigurationen oder fehlerhafte Verkabelung verursachen die meisten STP-Ausfälle, während Softwareausfälle die Minderheit ausmachen. STP-Fehler können auch durch unnötige zusätzliche Verbindungen auftreten, die zwischen den Switches bestehen. Aufgrund dieser zusätzlichen Verbindungen gehen VLANs in einen Standby-Modus. Um dieses Problem zu beheben, entfernen Sie alle unerwünschten Verbindungen zwischen den Switches.

Wenn eine dieser Annahmen nicht erfüllt wird, werden die BPDUs möglicherweise von einer oder mehreren Bridges nicht mehr empfangen oder verarbeitet. Dies bedeutet, dass die Bridge die Netzwerktopologie nicht erkennen kann. Ohne Kenntnis der richtigen Topologie kann der Switch die Schleifen nicht blockieren. Daher wird der überflutete Datenverkehr über die Looped-Topologie übertragen, die gesamte Bandbreite beanspruchen und das Netzwerk zum Erliegen bringen.

Beispiele dafür, warum die Switches keine BPDUs empfangen, sind fehlerhafte Transceiver oder Gigabit Interface Converter (GBICs), Verkabelungsprobleme oder Hardwarefehler am Port, an der Linecard oder an der Supervisor Engine. Ein häufiger Grund für STP-Ausfälle ist eine unidirektionale Verbindung zwischen den Bridges. In diesem Fall sendet eine Bridge BPDUs, die Downstream-Bridge empfängt sie jedoch nie. Die STP-Verarbeitung kann auch durch eine überladene 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, was auch ein ordnungsgemäßes STP-Verhalten verhindert.

Abgesehen von den Weiterleitungsschleifen gibt es Situationen, in denen keine Ports blockiert werden, in denen nur bestimmte Pakete fälschlicherweise über die blockierenden Ports weitergeleitet werden. In den meisten Fällen ist dies auf Softwareprobleme zurückzuführen. Ein solches Verhalten könnte "langsame Schleifen" verursachen. Dies bedeutet, dass einige Pakete Schleifen aufweisen, der Großteil des Datenverkehrs jedoch weiterhin über das Netzwerk fließt, da die Verbindungen wahrscheinlich nicht überlastet sind.

Die übrigen Abschnitte in diesem Dokument enthalten Richtlinien zur Behebung der häufigsten STP-bezogenen Probleme.

Fehlerbehebung bei Weiterleitungsschleifen

Weiterleitungsschleifen unterscheiden sich erheblich sowohl in ihrer Herkunft (Ursache) als auch in ihrer Wirkung. Aufgrund der Vielzahl von Problemen, die sich auf STP auswirken können, kann dieses Dokument nur allgemeine Richtlinien zur Fehlerbehebung bei Weiterleitungsschleifen enthalten.

Bevor Sie mit der Fehlerbehebung beginnen, müssen Sie folgende Informationen abrufen:

- Ein tatsächliches Topologiediagramm, das alle Switches und Bridges detailliert beschreibt
- Die entsprechenden Portnummern (Verbindungen)
- STP-Konfigurationsdetails, wie z. B. welcher Switch der Root- und Backup-Root ist, welche Links nicht standardmäßige Kosten oder Priorität haben, und der Standort der blockierenden Ports

Im Allgemeinen umfasst die Fehlerbehebung die folgenden Schritte (je nach Situation sind möglicherweise einige Schritte nicht erforderlich):

1. Identifizieren der SchleifeWenn sich im Netzwerk eine Weiterleitungsschleife entwickelt hat, treten die folgenden Symptome auf:Verlust von Verbindungen zu, von und durch betroffene NetzwerkregionenHohe CPU-Auslastung bei Routern, die mit betroffenen Segmenten oder

VLANs verbunden sind und zu verschiedenen Symptomen führen können, z. B. Flapping für das Routing-Protokoll im Nachbarbereich oder Hot Standby Router Protocol (HSRP) Active Router FlappingHohe Verbindungsauslastung (häufig 100 Prozent)Hohe Nutzung der Switch-Backplane (im Vergleich zur Baseline-Nutzung)Syslog-Meldungen, die auf Paketschleifen im Netzwerk hinweisen (z. B. doppelte HSRP-IP-Adressmeldungen)Syslog-Meldungen weisen auf ein ständiges erneutes Lernen von Adressen oder Flapping-Nachrichten für MAC-Adressen hin.Zunehmend sinkende Ausgaben an vielen Schnittstellen**Hinweis:** Allein aus diesen Gründen können verschiedene Probleme (oder gar kein Problem) auftreten. Wenn jedoch viele gleichzeitig beobachtet werden, ist es sehr wahrscheinlich, dass sich im Netzwerk eine Weiterleitungs-Schleife entwickelt hat.**Hinweis:** Die schnellste Möglichkeit, dies zu überprüfen, besteht in der Überprüfung der Nutzung des Switch-Backplane-Datenverkehrs:

```
cat# show catalyst6000 traffic-meter

  traffic meter =   13%  Never cleared
           peak =   14%  reached at 12:08:57 CET Fri Oct 4 2002
```

Hinweis: Catalyst 4000 mit Cisco IOS-Software unterstützt diesen Befehl derzeit nicht.Wenn der aktuelle Datenverkehrsstand weit über dem Normalwert liegt oder der Ausgangswert nicht bekannt ist, prüfen Sie, ob der Spitzenwert in letzter Zeit erreicht wurde und ob er nahe am aktuellen Datenverkehrslevel liegt. Wenn beispielsweise der Spitzenverkehrswert 15 % beträgt und erst vor zwei Minuten erreicht wurde und der aktuelle Datenverkehrslevel 14 % beträgt, bedeutet das, dass der Switch unter einer ungewöhnlich hohen Last arbeitet.Befindet sich die Datenverkehrslast auf einem normalen Niveau, bedeutet dies wahrscheinlich, dass es entweder keine Schleife gibt oder dass dieses Gerät nicht in die Schleife eingebunden ist. Sie kann jedoch weiterhin in eine langsame Schleife eingebunden werden.

2. Entdecken Sie die Topologie (den Umfang) der Schleife.Nachdem festgestellt wurde, dass der Grund für den Netzwerkausfall eine Weiterleitungsschleife ist, besteht die höchste Priorität darin, die Schleife zu stoppen und den Netzwerkbetrieb wiederherzustellen. Um die Schleife zu stoppen, müssen Sie wissen, welche Ports an der Schleife beteiligt sind: Überprüfen Sie die Ports mit der höchsten Verbindungsauslastung (Pakete pro Sekunde). Der Befehl **show interface** Cisco IOS software zeigt die Auslastung für jede Schnittstelle an.Um nur die Nutzungsinformationen und den Schnittstellennamen anzuzeigen (für eine schnelle Analyse), können Sie die Ausgabefilterung für reguläre Ausdrücke der Cisco IOS-Software verwenden. Ausgabe der **Show-Schnittstelle | schließen den Befehl line|\/sec** ein, um nur die Paketstatistik pro Sekunde und den Schnittstellennamen anzuzeigen:

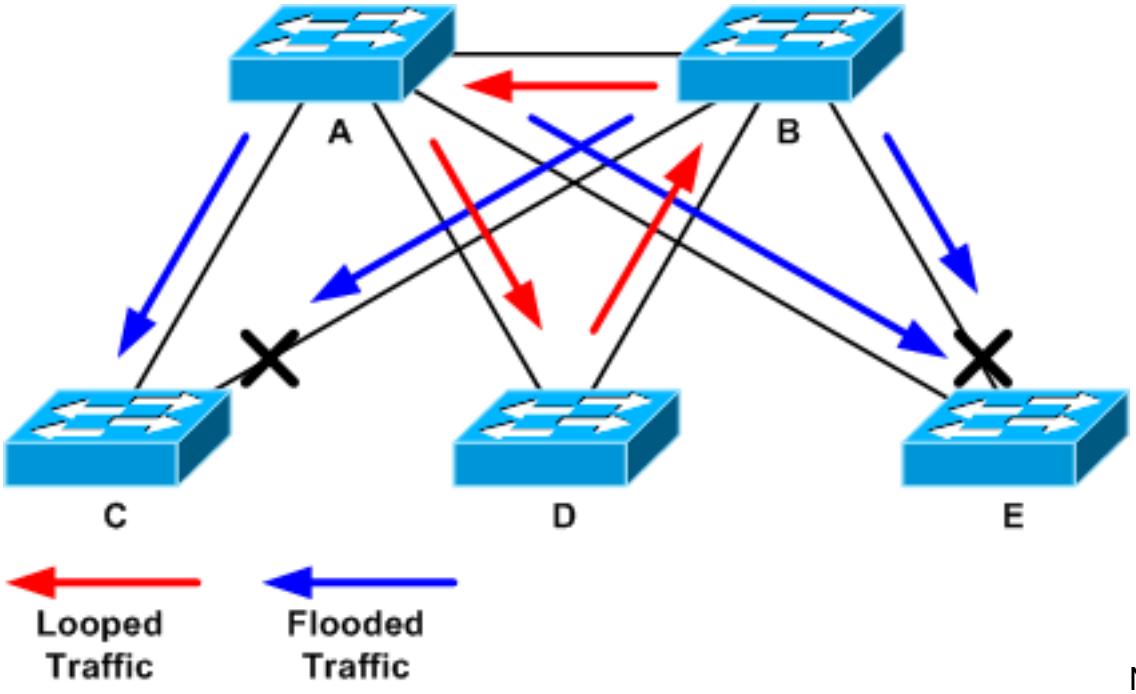
```
cat# show interface | include line|\/sec

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 besonders auf die Schnittstellen mit der höchsten Verbindungsauslastung. In diesem Beispiel sind dies die Schnittstellen g2/3, g2/4 und g2/8. wahrscheinlich sind es die Ports, die an der Schleife beteiligt sind.

3. Brechen Sie die Schleife.Um die Schleife zu unterbrechen, müssen Sie die beteiligten Ports herunterfahren oder trennen. Es ist sehr wichtig, nicht nur die Schleife zu stoppen, sondern auch die Ursache der Schleife zu finden und zu beheben. Es ist relativ einfacher, die Schleife zu durchbrechen.**Hinweis:** Um eine Analyse der Ursachen zu ermöglichen, müssen Sie nicht alle Ports gleichzeitig herunterfahren oder trennen. Stattdessen schalten Sie sie nacheinander aus. Im Allgemeinen ist es besser, Ports am Aggregationspunkt, der von der Schleife betroffen ist, abzuschalten, z. B. ein Distribution- oder Core-Switch. Wenn Sie alle Ports gleichzeitig herunterfahren und diese einzeln aktivieren oder wieder anschließen, funktioniert das möglicherweise nicht. Die Schleife wird gestoppt und wird möglicherweise nicht sofort nach dem erneuten Anschließen des Port gestartet. Daher wäre es schwierig, einen Ausfall mit einem bestimmten Port zu korrelieren.**Hinweis:** Es wird empfohlen, vor dem Neustart der Switches Informationen zu sammeln, um die Schleife zu durchbrechen. Andernfalls wird die anschließende Ursachenanalyse sehr schwierig.Wenn Sie jeden Port deaktivieren oder trennen, müssen Sie überprüfen, ob die Backplane-Nutzung des Switches wieder auf einen normalen Stand zurückgesetzt wurde.**Hinweis:** Beachten Sie, dass in der Regel einige Ports die Schleife nicht unterstützen, sondern den mit der Schleife eingehenden Datenverkehr überfluten. Wenn Sie diese Flooding-Ports ausschalten, reduzieren Sie die Nutzung der Backplane nur geringfügig, aber die Schleife wird nicht gestoppt.In der Topologie des nächsten Beispiels verläuft die Schleife zwischen den Switches A, B und D. Daher sind Links AB, AD und BD erhalten. Wenn Sie eine dieser Verbindungen ausschalten, wird die Schleife angehalten. Die Verbindungen AC, AE, BC und BE überfluten lediglich den mit der Schleife eingehenden
Datenverkehr.



Nachdem der zugeschaltete Port ausgeschaltet wurde, wird die Backplane-Auslastung auf einen Normalwert reduziert. Es ist sehr wichtig zu beachten, durch das Herunterfahren des Ports die Backplane-Auslastung (und die Auslastung anderer Ports) auf ein normales Niveau gesenkt wurde.An diesem Punkt wird die Schleife gestoppt, und der Netzwerkbetrieb sollte verbessert werden. Da die ursprüngliche Ursache der Schleife jedoch wahrscheinlich nicht behoben wurde, könnten noch einige Probleme offen sein.

4. Suchen und beheben Sie die Ursache der Schleife.Nachdem die Schleife beendet wurde, müssen Sie den Grund für den Beginn der Schleife ermitteln. Dies ist oft der schwierigste Teil des Prozesses, da die Gründe variieren können. Es ist auch schwierig, ein exaktes Verfahren zu formalisieren, das in jedem Fall funktioniert. Dies sind jedoch einige allgemeine Leitlinien:Überprüfen Sie das Topologiediagramm, um einen redundanten Pfad zu finden. Dazu gehört auch der im vorherigen Schritt gefundene SUPORT, der zum selben Switch zurückkehrt (die Pfadpakete wurden während der Schleife aufgenommen). In der Topologie des vorherigen Beispiels lautet dieser Pfad AD-DB-BA.Überprüfen Sie für jeden Switch im redundanten Pfad, ob folgende Probleme vorliegen:Weiß der Switch die richtige STP-Root?Alle Switches in einem L2-Netzwerk sollten sich auf einen gemeinsamen STP-Root einigen. Es besteht ein klares Symptom für Probleme, wenn Bridges durchgehend eine andere ID für den STP-Root in einer bestimmten VLAN- oder STP-Instanz anzeigen. Geben Sie den Befehl **show spanning-tree vlan *vlan-id* ein, um die Root-Bridge-ID für ein bestimmtes VLAN anzuzeigen:**

```
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 ist vom Port aus zu finden, da die Ports, die an der Schleife beteiligt sind, in vorherigen Schritten eingerichtet wurden. Wenn es sich bei den betreffenden Ports um Trunks handelt, sind häufig alle VLANs im Trunk beteiligt. Wenn dies nicht der Fall ist (z. B. wenn die Schleife auf einem einzelnen VLAN aufgetreten ist), können Sie versuchen, die **Schnittstellen** zum **Anzeigen** auszugeben. **| den L2|line|Broadcast-**Befehl **einschließen** (nur bei Supervisor 2- und höher-Engines auf Catalyst Switches der Serien 6500/6000, da Supervisor 1 keine VLAN-basierten Switching-Statistiken liefert). Betrachten Sie nur VLAN-Schnittstellen. Das VLAN mit der höchsten Anzahl an vermittelten Paketen ist meist das VLAN, in dem die Schleife stattfand:

```
cat# show int | 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 macht VLAN 1 die höchste Anzahl an Broadcasts und L2-Switched-Datenverkehr aus.Wurde der Root-Port richtig identifiziert?Der Root-Port sollte die niedrigsten Kosten für die Root-Bridge verursachen (manchmal ist ein Pfad kürzer in Bezug auf Hops, aber auch länger in Bezug auf die Kosten, da Low-Speed-Ports höhere Kosten verursachen).Um zu bestimmen, welcher Port als Root für ein bestimmtes VLAN gilt, führen Sie den Befehl **show spanning-tree vlan *vlan* aus:**

```
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
```

Werden regelmäßig BPDUs am Root-Port und an Ports empfangen, die blockiert werden

sollen?BPDUs werden von der Root Bridge in jedem `Hello`-Intervall (standardmäßig zwei Sekunden) gesendet. Nicht-Root-Bridges empfangen, verarbeiten, ändern und propagieren die BPDUs, die vom Root empfangen werden.Geben Sie den Befehl **show spanning-tree interface *interface* detail** ein, um festzustellen, ob die BPDUs empfangen werden:

```
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 stieg von 53 auf 54).Die gezeigten Zähler sind tatsächlich Zähler, die vom STP-Prozess selbst verwaltet werden. Das bedeutet, dass bei einer inkrementierten Empfangs-Zähler nicht nur BPDU von einem physischen Port empfangen wurde, sondern auch vom STP-Prozess empfangen wurde.Wenn der `empfangene` BPDU-Zähler auf dem Port, der als Root-Alternativport oder Backup-Port dienen soll, nicht inkrementiert, prüfen Sie, ob der Port überhaupt Multicasts empfängt (BPDUs werden als Multicast gesendet). Geben Sie den Befehl **show interface *interface* counter** ein:

```
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 Kurzübersicht der STP-Portrollen im Abschnitt Spanning-Tree Protocol Enhancements unter Verwendung von Loop Guard- und BPDU Skew Detection-Funktionen.)Wenn keine BPDUs empfangen werden, prüfen Sie, ob der Port keine Fehler zählt. Geben Sie den Befehl **show interface *interface* counters errors** ein:

```
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 den STP-Prozess immer noch nicht erreichen. Wenn die in den beiden vorherigen Beispielen verwendeten Befehle zeigen, dass einige Multicasts empfangen werden und Fehler nicht inkrementiert werden, überprüfen Sie, ob die BPDUs auf der STP-Prozessebene verworfen werden. Führen Sie den Befehl **remote command switch test spanning-tree process-stats** auf dem Catalyst 6500 aus:

```
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 STP-Prozessstatistiken an. Es ist wichtig zu überprüfen, ob die Zähler der verworfenen Pakete nicht ansteigen und ob die Anzahl der empfangenen Pakete zunimmt.Wenn die Anzahl der empfangenen Pakete nicht ansteigt, der physische Port jedoch Multicasts empfängt, stellen Sie sicher, dass die Pakete von der In-Band-Schnittstelle des Switches (der CPU-Schnittstelle) empfangen werden. Geben Sie den **Remote-Befehlsschalter show ibc ein. | i rx_input** auf dem Catalyst 6500/6000:

```
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 Ausgaben 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 keine Hinweise darauf vorliegen, dass BPDUs auf dem lokalen Switch oder Port verworfen werden, müssen Sie zum Switch auf der anderen Seite der Verbindung wechseln und überprüfen, ob dieser Switch BPDUs sendet.Werden regelmäßig BPDUs an nicht-Root-basierten, designierten Ports gesendet?Wenn der Port entsprechend der Portrolle BPDUs sendet, aber der Nachbar diese nicht empfängt, überprüfen Sie, ob BPDUs tatsächlich gesendet werden. Geben Sie

den Befehl **show spanning-tree interface *interface* detail ein**:

```
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 wurden zwischen den Ausgaben zwei BPDUs gesendet.**Hinweis:** Der STP-Prozess verwaltet die `BPDU: gesendeter` Zähler. Das bedeutet, dass der Zähler angibt, dass die BPDU an den physischen Port gesendet wurde, um schließlich ausgesendet zu werden. Überprüfen Sie, ob die Port-Zähler für übertragene Multicast-Pakete ansteigen. Geben Sie den Befehl **show interface *interface* counter** ein. So können Sie feststellen, ob BPDUs ausgehen oder nicht:

```
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 wird angestrebt, den Switch oder die Verbindung zu finden, bei dem bzw. der keine BPDUs empfangen, gesendet oder verarbeitet werden.Es ist zwar unwahrscheinlich, dass das STP den korrekten Status für den Port berechnet hat, aber aufgrund eines Problems mit der Steuerungsebene konnte es diesen Zustand nicht auf der Weiterleitungshardware festlegen. Es kann eine Schleife erstellt werden, wenn der vermeintliche blockierende Port nicht auf Hardwareebene blockiert ist. Wenn Sie einen solchen Fehler in Ihrem Netzwerk vermuten, 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 die Schleife verursacht, muss dieses Gerät vom Netzwerk isoliert werden, oder es müssen Maßnahmen ergriffen werden, um das Problem zu beheben (z. B.

Austausch der Glasfaser oder GBIC). Die redundanten Verbindungen, die in Schritt 3 getrennt wurden, müssen wiederhergestellt werden.Es ist wichtig, das Gerät oder die Verbindung, das bzw. die die Schleife verursacht, so wenig wie möglich zu manipulieren, da viele Bedingungen, die zu einer Schleife führen, sehr vorübergehend, intermittierend und instabil sein können. Dies bedeutet, dass es eine Weile dauern kann, bis eine solche Bedingung erneut auftritt, wenn die Bedingung während oder nach der Fehlerbehebung gelöscht wird. Es ist möglich, dass der Zustand überhaupt nicht mehr auftritt. Es sollte alles getan werden, um die Bedingung zu wahren, damit sie durch den technischen Support von Cisco weiter untersucht werden kann. Es ist wichtig, dass Sie vor dem Zurücksetzen der Switches Informationen über den Zustand sammeln. Wenn eine Bedingung weg ist, ist es oft unmöglich, die Ursache der Schleife zu bestimmen. Um das Gerät oder die Verbindung zu finden, die die Schleife auslöst, ist eine große Leistung, aber Sie müssen sicherstellen, dass ein anderer Ausfall der gleichen Art nicht wieder die Schleife verursacht. Weitere Informationen finden Sie im Abschnitt Sichern des Netzwerks gegen Weiterleitungsschleifen in diesem Dokument.

Fehlerbehebung bei übermäßigen Topologieänderungen, die Flooding verursachen

Der TC-Mechanismus dient der Korrektur von L2-Weiterleitungstabellen, nachdem die Weiterleitungstopologie geändert wurde. Dies ist erforderlich, um einen Verbindungsausfall zu vermeiden, da nach einem TC einige MAC-Adressen, auf die zuvor über bestimmte Ports zugegriffen wurde, über verschiedene Ports zugänglich sein können. TC verkürzt die Alterungszeit der Weiterleitungstabellen auf allen Switches im VLAN, auf denen der TK erfolgt. Wenn die Adresse also nicht erneut erfasst wird, wird sie veraltet und es kommt zu Überflutungen, um sicherzustellen, dass die Pakete die MAC-Zieladresse erreichen.

Die TC wird durch die Änderung des STP-Status eines Ports zum oder vom STP-`Weiterleitungsstatus` ausgelöst. Auch wenn die MAC-Zieladresse nach dem TC veraltet ist, sollte die Überflutung nicht länger anhalten. Die Adresse wird durch das erste Paket erneut erfasst, das vom Host stammt, dessen MAC-Adresse veraltet wurde. Das Problem kann auftreten, wenn TCs wiederholt und in kurzen Abständen auftreten. Die Weiterleitungstabellen der Switches werden immer schneller altern, sodass die Überflutung nahezu konstant bleibt.

Hinweis: Bei Rapid STP oder Multiple STP (IEEE 802.1w und IEEE 802.1s) wird TC durch eine Änderung des Portstatus in `Forwarding` ausgelöst sowie durch die Änderung der Rolle von `designiertem` zu `Root`. Bei Rapid STP wird die L2-Weiterleitungstabelle sofort geleert, im Gegensatz zu 802.1d, wodurch die Alterungszeit verkürzt wird. Durch die sofortige Leerung der Weiterleitungstabelle werden die Verbindungen schneller wiederhergestellt, es kommt jedoch zu weiteren Überflutungen.

TK sollte in einem gut konfigurierten Netzwerk selten vorkommen. Wenn eine Verbindung an einem Switch-Port aktiv oder inaktiv ist, gibt es irgendwann einen TC, sobald der STP-Status des Ports an die `Weiterleitung` oder von dieser `umgestellt` wird. Wenn der Port flattert, würde dies wiederholte TCs und Überflutungen verursachen.

Ports mit aktivierter STP-Portfast-Funktion verursachen keine TCs beim Wechsel vom oder zum `Weiterleitungsstatus`. Die Konfiguration von Portfast an allen Endgeräte-Ports (wie Drucker, PCs und Server) sollte die Anzahl der TCs auf ein Minimum beschränken und wird dringend empfohlen. Weitere Informationen zu TCs finden Sie unter Verstehen von Topologieänderungen

des Spanning-Tree-Protokolls.

Wenn sich im Netzwerk repetitive TCs befinden, müssen Sie die Quelle dieser TCs identifizieren und Maßnahmen ergreifen, um diese zu reduzieren und die Überflutung auf ein Minimum zu beschränken.

Bei 802.1d werden STP-Informationen über ein TC-Ereignis über eine TC Notification (TCN), einen speziellen BPDU-Typ, auf die Bridges verteilt. Wenn Sie die Ports befolgen, die TCN-BPDUs empfangen, können Sie das Gerät finden, von dem die TCs stammen.

Stellen Sie fest, ob Flooding durch STP-TCs verursacht wird.

Normalerweise können Sie feststellen, dass eine Überflutung durch langsame Leistung vorliegt, Paketverluste bei Verbindungen, die nicht überlastet werden sollen, und der Paketanalysator, der mehrere Unicast-Pakete an dasselbe Ziel anzeigt, 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, auf dem Cisco IOS-Software ausgeführt wird, können Sie den Zähler der Weiterleitungs-Engine (nur auf der Supervisor 2 Engine) überprüfen, um die Flutungsrate zu schätzen. Ausgabe des **Remote-Befehls-Switches** zur **Anzeige von Frühstatistiken** Befehl **| i MISS_DA|ST_FR**:

```
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. Die erste Zeile zeigt die Anzahl der überfluteten Frames und die zweite Zeile die Anzahl der verarbeiteten 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 zusammen mit anderen Methoden zur Überflutung 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 erkannt werden, da der Switch immer dann überflutet wird, wenn die MAC-Zieladresse nicht in der Weiterleitungstabelle gespeichert ist. Dies ist der Fall, wenn der Switch ein Paket mit einer Zieladresse empfängt, die noch nicht erfasst wurde.

Nachverfolgen der Quelle der TKs

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

```
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 Paketanalyzer verwenden oder die TC-Zähler für alle VLANs überprüfen.

Maßnahmen zur Verhinderung übermäßiger Regelverletzungen

Sie können die `Anzahl der Topologieänderungen` überwachen, um festzustellen, ob sie regelmäßig zunimmt. Wechseln Sie dann zu der Bridge, die mit dem angezeigten Port verbunden ist, um den letzten TC (im vorherigen Beispiel Port GigabitEthernet1/1) zu erhalten, und sehen Sie, woher der TC für diese Bridge gekommen ist. Dieser Prozess muss wiederholt werden, bis der End-Station-Port ohne aktiviertes STP-Portfast gefunden wurde oder der Flapping-Link gefunden wurde, der behoben werden muss. Das gesamte Verfahren muss wiederholt werden, wenn TKs noch aus anderen Quellen stammen. Wenn der Link zu einem End-Host gehört, sollten Sie die Portfast-Funktion konfigurieren, um die Generierung von TCs zu verhindern.

Hinweis: In der STP-Implementierung der Cisco IOS-Software erhöht sich der Zähler für TCs nur, wenn ein TCN-BPDU von einem Port in einem VLAN empfangen wird. Wenn eine normale BPDU-Konfiguration mit einem festgelegten TC-Flag empfangen wird, wird der TC-Zähler nicht erhöht. Wenn Sie vermuten, dass ein TC der Grund für die Überflutung ist, sollten Sie daher am besten damit beginnen, die Quellen für den TC von der STP-Root-Bridge in diesem VLAN zu verfolgen. Er wird über die genauesten Informationen hinsichtlich der Menge und Quelle der TKs verfügen.

Beheben von Problemen im Zusammenhang mit der Konvergenzzeit

Es gibt Situationen, in denen der tatsächliche Betrieb von STP nicht mit dem erwarteten Verhalten übereinstimmt. Dies sind die beiden häufigsten Probleme:

- STP-Konvergenz oder -Rekonvergenz dauert länger als erwartet.
- Die resultierende Topologie ist anders als erwartet.

Häufig sind dies die Gründe für dieses Verhalten:

- Eine Diskrepanz zwischen der tatsächlichen und der dokumentierten Topologie
- Fehlkonfiguration, z. B. inkonsistente Konfiguration von STP-Timern, Überschreitung des STP-Durchmessers oder portfast-fehlerhafte Konfiguration
- Überlastete Switch-CPU während Konvergenz oder Rekonvergenz
- Softwarefehler

Wie bereits erwähnt, kann dieses Dokument nur allgemeine Richtlinien für die Fehlerbehebung enthalten, da es eine Vielzahl von Problemen mit Auswirkungen auf STP gibt.

Um zu verstehen, warum die Konvergenz länger als erwartet dauert, sehen Sie sich die Abfolge von STP-Ereignissen an, um herauszufinden, was in welcher Reihenfolge vor sich ging. Da die STP-Implementierung in der Cisco IOS-Software nicht über eine spezielle Protokollierung verfügt (außer bei bestimmten Ereignissen, wie z. B. inkonsistenten Ports), können Sie die STP-Debugging-Funktionen der Cisco IOS-Software verwenden, um zu verstehen, was geschieht.

Bei STP erfolgt die Verarbeitung beim Catalyst 6500/6000 mit Cisco IOS-Software auf dem Switch-Prozessor (SP) (oder Supervisor), sodass die Fehlerbehebung auf dem SP aktiviert werden muss. Bei Cisco IOS-Software-Bridge-Gruppen erfolgt die Verarbeitung auf dem Route Processor (RP), sodass die Debug-Aufgaben auf dem RP (MSFC) aktiviert werden müssen.

STP-Debugging-Befehle

Viele STP-**Debugbefehle** sind für die Verwendung durch Entwicklungstechniken vorgesehen. Sie liefern niemandem aussagekräftige Ergebnisse, ohne detaillierte Kenntnisse der STP-Implementierung in der Cisco IOS-Software zu besitzen. Einige Debugger können Ausgaben bereitstellen, die sofort lesbar sind, z. B. Portstatusänderungen, Rollenänderungen, Ereignisse wie TCs und ein Dump von empfangenen und übertragenen BPDUs. Dieser Abschnitt enthält keine vollständige Beschreibung aller Debuggen, sondern führt die am häufigsten verwendeten ein.

Hinweis: Wenn Sie **Debugbefehle** verwenden, aktivieren Sie die erforderlichen Mindestdebugs. Wenn keine Echtzeit-Fehlersuche erforderlich ist, zeichnen Sie die Ausgabe im Protokoll auf, statt sie in die Konsole zu drucken. Übermäßige Debug-Vorgänge können die CPU überlasten und den Switch-Betrieb stören. Um die Debug-Ausgabe in das Protokoll anstatt in die Konsole oder in Telnet-Sitzungen zu leiten, geben Sie die **Protokollierungskonsole-**Befehle **mit Informationen** und **ohne Protokollierungsmonitor** im globalen Konfigurationsmodus aus.

Um das allgemeine Ereignisprotokoll anzuzeigen, führen Sie den Befehl **debug spanning-tree event** für Per VLAN Spanning-Tree (PVST) und Rapid-PVST aus. Dies ist der erste Debugger, der eine allgemeine Vorstellung davon gibt, was mit STP geschieht.

Im MST-Modus (Multiple Spanning Tree) wird der Befehl **debug spanning-tree event** nicht ausgeführt. Führen Sie daher den Befehl **debug spanning-tree mstp roles aus,** um die Änderungen der Portrolle anzuzeigen.

Führen Sie den Befehl **debug spanning-tree switch state** zusammen mit dem Befehl **debug pm vp** aus, um die Port-STP-Statusänderungen anzuzeigen:

```
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 in gewisser Weise verhält, ist es häufig hilfreich, die BPDUs anzuzeigen, die vom Switch empfangen und gesendet werden:

```
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 000000000000000074F1CE847000000138048000652 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 eignet sich für die Modi PVST, Rapid-PVST und MST. Der Inhalt der BPDUs wird jedoch nicht decodiert. Sie können es jedoch verwenden, um sicherzustellen, dass BPDUs empfangen werden.

Um den Inhalt der BPDU anzuzeigen, führen Sie den Befehl **debug spanning-tree switch rx decode** zusammen mit dem Befehl **debug spanning-tree switch rx process** für PVST und Rapid-PVST aus. Geben Sie den Befehl **debug spanning-tree mstp bpdu-rx** ein, um den Inhalt der BPDU für MST anzuzeigen:

```
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
```

Für den MST-Modus können Sie mit dem folgenden **Debug-**Befehl eine detaillierte BPDU-Dekodierung aktivieren:

```
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 Release 12.1.13E und höher werden bedingte Debug-Änderungen für STP unterstützt. Dies bedeutet, dass Sie BPDUs debuggen können, die auf Port- oder VLAN-Basis empfangen oder übertragen werden.

Geben Sie die **Befehle für die Debugbedingung "vlan *vlan_num*"** oder "**debug condition interface *interface***" ein, um den Gültigkeitsbereich der Debugausgabe auf "per interface" oder "per VLAN" zu beschränken.

Schutz des Netzwerks vor Weiterleitungsschleifen

Um die Unfähigkeit von STP, mit bestimmten Ausfällen richtig umzugehen, zu bewältigen, hat Cisco eine Reihe von Funktionen und Erweiterungen entwickelt, die das Netzwerk vor Weiterleitungsschleifen schützen.

Die Fehlerbehebung bei STP hilft, die Ursache eines bestimmten Fehlers zu isolieren und zu finden. Die Implementierung dieser Erweiterungen ist die einzige Möglichkeit, das Netzwerk gegen Weiterleitungsschleifen zu schützen.

Diese Methoden schützen Ihr Netzwerk vor Weiterleitungsschleifen:

1. Aktivieren Sie UDLD (Unidirectional Link Detection) auf allen Switch-to-Switch-Verbindungen. Weitere Informationen zu UDLD finden Sie unter Understanding and Configuring the Unidirectional Link Detection Protocol Feature.
2. Aktivieren Sie Loop Guard auf allen Switches. Weitere Informationen zu Loop Guard finden Sie unter Spanning Tree Protocol Enhancements using Loop Guard and BPDU Skew Detection Features.Wenn UDLD und Loop Guard aktiviert sind, eliminieren sie die meisten möglichen Ursachen für Weiterleitungsschleifen. Anstatt eine Weiterleitungs-Schleife zu erstellen, wird der fehlerhafte Link (oder alle Verbindungen, die von der fehlerhaften Hardware abhängig sind) geschlossen oder blockiert.**Hinweis:** Diese beiden Funktionen scheinen zwar etwas redundant zu sein, bieten jedoch jeweils eigene Funktionen. Verwenden Sie daher beide Funktionen gleichzeitig, um ein Höchstmaß an Schutz zu gewährleisten. Einen detaillierten Vergleich von UDLD und Loop Guard finden Sie unter Loop Guard und Unidirectional Link Detection.Es gibt unterschiedliche Meinungen darüber, ob Sie aggressive oder normale UDLD anwenden müssen. Es ist zu beachten, dass aggressive UDLD keinen größeren Schutz vor Schleifen bietet als normale UDLD-Modus. Aggressive UDLD erkennt Szenarien, bei denen der Port blockiert ist (wenn die Verbindung aktiv ist, jedoch keine entsprechenden Blackholes für den Datenverkehr sind). Der Nachteil dieser zusätzlichen Funktionalität besteht darin, dass aggressive UDLD möglicherweise Links deaktivieren kann, wenn kein konsistenter Ausfall auftritt. Häufig verwechseln die Leute die Änderung des UDLD `Hello`-Intervalls mit der aggressiven UDLD-Funktion. Das ist falsch. Timer können in beiden UDLD-Modi geändert werden.**Hinweis:** In seltenen Fällen kann aggressives UDLD alle Uplink-Ports schließen, wodurch der Switch im Wesentlichen vom Rest des Netzwerks isoliert wird. Dies kann beispielsweise der Fall sein, wenn beide Upstream-Switches eine sehr hohe CPU-Auslastung aufweisen und UDLD im aggressiven Modus verwendet wird. Daher wird empfohlen, dass Sie errordisable-timeouts konfigurieren, wenn der Switch über keine Out-of-Band-Verwaltung verfügt.
3. Aktivieren Sie "portfast" auf allen Endstation-Ports.Sie müssen "portfast" aktivieren, um die Anzahl der TCs und die anschließende Überflutung zu begrenzen, was die Leistung des Netzwerks beeinträchtigen kann. Verwenden Sie diesen Befehl nur für Ports, die mit

Endstationen verbunden sind. Andernfalls kann eine unbeabsichtigte Topologieschleife eine Datenpaketschleife verursachen und den Switch- und Netzwerkbetrieb unterbrechen.**Vorsicht:** Seien Sie vorsichtig, wenn Sie den Befehl **no spanning-tree portfast** verwenden. Mit diesem Befehl werden nur Port-spezifische Port-Fast-Befehle entfernt. Dieser Befehl aktiviert implizit "portfast", wenn Sie den Befehl **spanning-tree portfast default** im globalen Konfigurationsmodus definieren und 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. Legen Sie die Option EtherChannels auf beiden Seiten (sofern unterstützt) und `nicht` auf den `gewünschten` Modus fest.`Der erwünschte` Modus aktiviert PAgP (Port Aggregation Protocol), um die Laufzeitkonsistenz zwischen den Channel-Peers sicherzustellen. Dies bietet einen zusätzlichen Schutz vor Schleifen, insbesondere bei Neukonfigurationen von Kanälen (z. B. wenn Links den Kanal betreten oder verlassen und wenn Link-Fehler erkannt werden). Es gibt einen integrierten Channel Misconfiguration Guard, der standardmäßig aktiviert ist und Weiterleitungsschleifen aufgrund von Kanalfehlkonfigurationen oder anderen Bedingungen verhindert. Weitere Informationen zu dieser Funktion finden Sie unter Understanding EtherChannel Inkonsistency Detection.
5. Deaktivieren Sie die automatische Aushandlung (falls unterstützt) für Switch-to-Switch-Verbindungen nicht.Auto-Negotiation-Mechanismen können Informationen zu Remote-Fehlern übertragen. Dies ist die schnellste Methode zur Fehlererkennung auf der Remote-Seite. Sollte ein Ausfall an der Remote-Seite festgestellt werden, fährt die lokale Seite die Verbindung herunter, selbst wenn die Verbindung noch Impulse empfängt. Im Vergleich zu High-Level-Erkennungsmechanismen wie UDLD ist die automatische Aushandlung sehr schnell (innerhalb von Mikrosekunden), aber ohne End-to-End-Abdeckung für UDLD (z. B. den gesamten Datenpfad: CPU - Weiterleitungslogik - Port1 - Port2 - Weiterleitungslogik - CPU versus port1 - port2). Der aggressive UDLD-Modus bietet ähnliche Funktionen wie die automatische Aushandlung in Bezug auf die Fehlererkennung. Wenn auf beiden Seiten der Verbindung Verhandlungen unterstützt werden, muss kein aggressiver Modus für UDLD aktiviert werden.
6. Seien Sie vorsichtig, wenn Sie die STP-Timer einstellen.STP-Timer sind voneinander und von der Netzwerktopologie abhängig. STP funktioniert möglicherweise nicht korrekt, wenn an den Timern beliebige Änderungen vorgenommen wurden. Weitere Informationen zu STP-Timern finden Sie unter Understanding and Tuning Spanning Tree Protocol Timers.
7. Wenn Denial-of-Service-Angriffe möglich sind, sichern Sie den STP-Perimeter des Netzwerks mit Root Guard.Mit Root Guard und BPDU Guard können Sie STP vor Einflussnahme von außen schützen. Wenn ein solcher Angriff möglich ist, müssen Root Guard und BPDU Guard zum Schutz des Netzwerks eingesetzt werden. Weitere Informationen zu Root Guard und BPDU Guard finden Sie in den folgenden Dokumenten:Erweiterung der Spanning Tree Protocol Root GuardErweiterung des Spanning Tree Portfast BPDU Guard
8. Aktivieren Sie BPDU Guard an portfast-fähigen Ports, um zu verhindern, dass STP von nicht autorisierten Netzwerkgeräten (wie Hubs, Switches und Bridging-Routern) betroffen wird, die mit den Ports verbunden sind.Wenn Root Guard korrekt konfiguriert ist, verhindert es bereits, dass das STP von außen beeinflusst wird. Wenn BPDU Guard aktiviert ist, werden die Ports geschlossen, die BPDUs empfangen (nicht nur überlegene BPDUs). Dies kann nützlich sein, wenn solche Vorfälle untersucht werden müssen, da BPDU Guard die Syslog-Meldung erstellt und den Port herunterfährt. Es ist zu beachten, dass kurze Loops nicht durch Root- oder BPDU-Guards verhindert werden, wenn zwei portfast-fähige Ports direkt oder über den

Hub verbunden sind.

9. Vermeiden Sie Benutzerdatenverkehr im Management-VLAN. Das Management-VLAN ist in einem Baustein enthalten, nicht im gesamten Netzwerk.Die Switch-Management-Schnittstelle empfängt Broadcast-Pakete im Management-VLAN. Bei exzessiven Broadcasts (z. B. ein Broadcast-Sturm oder eine nicht funktionierende Anwendung) kann die Switch-CPU überlastet werden, was den STP-Betrieb verzerren könnte.
10. Eine vorhersehbare (hardcodierte) STP-Root- und Backup-STP-Root-Platzierung.Der STP-Root und der Backup-STP-Root müssen so konfiguriert werden, dass bei Ausfällen die Konvergenz vorhersehbar erfolgt und in jedem Szenario eine optimale Topologie erstellt wird. Lassen Sie die STP-Priorität nicht auf dem Standardwert zurück, um eine unvorhersehbare Root-Switch-Auswahl zu vermeiden.

Zugehörige Informationen

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