Fehlerbehebung bei STP-Problemen und Überlegungen zum zugehörigen Design

Inhalt

Einleitung

In diesem Dokument werden Empfehlungen zur Implementierung eines sicheren Netzwerks im Hinblick auf die Überbrückung von Cisco Catalyst Switches mit Catalyst OS/Cisco IOS®-Software beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

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

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

Hintergrundinformationen

In diesem Dokument werden einige der häufigsten Gründe für Fehler bei STP (Spanning Tree Protocol) erläutert, und Sie erhalten Informationen zum Ermitteln der Problemursache. Darüber hinaus wird das Design vorgestellt, das Spanning Tree-bezogene Probleme auf ein Minimum reduziert und eine problemlose Fehlerbehebung ermöglicht.

Die grundlegende Funktionsweise von STP wird in diesem Dokument nicht erläutert. Weitere Informationen zur Funktionsweise von STP finden Sie in diesem Dokument:

- Verstehen und Konfigurieren von Spanning Tree Protocol (STP) auf Catalyst Switches

RSTP (Rapid STP) gemäß IEEE 802.1w wird in diesem Dokument nicht behandelt. Auch auf das in IEEE 802.1s definierte MST-Protokoll (Multiple Spanning Tree) wird in diesem Dokument nicht eingegangen. Weitere Informationen zu RSTP und MST finden Sie in diesen Dokumenten:

- Grundlegendes zum Spanning Tree Protocol (802.1s)
- Grundlegendes zum Rapid Spanning Tree Protocol (802.1w)

Konkretere Informationen zur STP-Fehlerbehebung für Catalyst Switches mit Cisco IOS-Software finden Sie im Dokument zur Fehlerbehebung bei STP auf Catalyst Switches mit Cisco Integrated IOS (nativer Modus).

Fehler bei STP (Spanning Tree Protocol)

Die primäre Funktion des Spanning-Tree-Algorithmus (STA) ist es, Schleifen zu unterbinden, die durch redundante Verbindungen in Bridge-Netzwerken entstehen. STP arbeitet auf Schicht 2 des OSI-Modells (Open System Interconnection). Mittels BPDUs (Bridge Protocol Data Units), die zwischen Bridges ausgetauscht werden, wählt STP die Ports aus, die den Datenverkehr weiterleiten oder blockieren sollen. Dieses Protokoll kann in bestimmten Fällen fehlschlagen, und die Problembehebung kann sehr schwierig sein, je nach Netzwerkdesign. In diesem speziellen Bereich führen Sie den wichtigsten Teil des Fehlerbehebungsprozesses durch, bevor das Problem auftritt.

Ein Ausfall des STA führt in der Regel zu einer Bridging-Schleife. Die meisten Kunden, die sich wegen Spanning Tree-Problemen an den technischen Support von Cisco wenden, vermuten einen Bug, aber ein Bug ist selten die Ursache. Selbst wenn die Software das Problem darstellt, stammt ein Bridging-Loop in einer STP-Umgebung immer noch von einem Port, der blockieren kann, aber Datenverkehr weiterleitet.

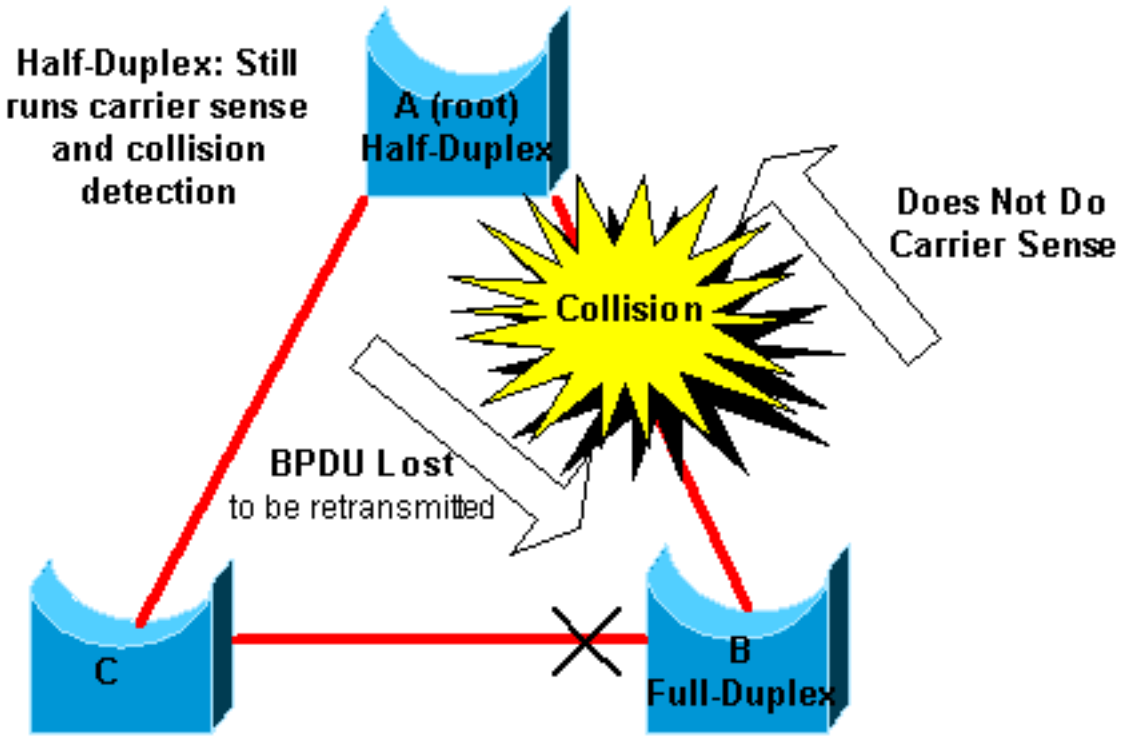
Spanning Tree-Konvergenz

Im Video zu Spanning Tree sehen Sie ein Beispiel, das zeigt, wie Spanning Tree anfänglich konvergiert. Das Beispiel erläutert auch, warum ein blockierter Port aufgrund eines übermäßigen Verlusts von BPDUs in den Weiterleitungsmodus wechselt, was zu einem STA-Fehler führt.

Im Rest dieses Dokuments werden die verschiedenen Situationen aufgeführt, die zu Fehlern beim STA führen können. Die meisten dieser Fehler hängen mit einem massiven Verlust von BPDUs zusammen. Der Verlust führt dazu, dass blockierte Ports in den Weiterleitungsmodus wechseln.

Duplexkonflikt

Ein Duplexkonflikt bei einer Punkt-zu-Punkt-Verbindung ist ein sehr häufiger Konfigurationsfehler. Wenn Sie den Duplexmodus auf einer Seite der Verbindung manuell auf Vollduplex setzen und die andere Seite im Modus für die automatische Aushandlung belassen, ist der Link letztlich im Halbduplex. (Ein Port, bei dem der Duplexmodus auf Vollduplex eingestellt ist, verhandelt nicht mehr.)



Im schlimmsten Fall wird bei einer Bridge, die BPDUs sendet, der Duplexmodus für einen Port auf Halbduplex eingestellt, für den Peer-Port am anderen Ende der Verbindung jedoch auf Vollduplex. Im vorherigen Beispiel kann die Duplexungleichheit auf der Verbindung zwischen Brücke A und B leicht zu einer Bridging-Schleife führen. Da Bridge B für Vollduplex konfiguriert ist, führt sie vor dem Link-Zugriff kein Carrier Sense durch. Bridge B beginnt, Frames zu senden, auch wenn Bridge A die Verbindung bereits verwendet. Diese Situation ist ein Problem für A; Brücke A erkennt eine Kollision und führt den Backoff-Algorithmus aus, bevor die Brücke eine weitere Übertragung des Rahmens versucht. Wenn genügend Datenverkehr von B nach A fließt, wird jedes Paket, das A sendet, einschließlich der BPDUs, aufgeschoben oder kollidiert und wird schließlich verworfen. Aus STP-Sicht hat Bridge B die Root-Bridge verloren, da Bridge B keine BPDUs mehr von A empfängt. Dies führt dazu, dass B die Blockierung des mit Bridge C verbundenen Ports aufhebt, wodurch die Schleife erzeugt wird.

Wann immer ein Duplexkonflikt vorliegt, werden folgende Fehlermeldungen auf den Switch-Konsolen von Catalyst Switches angezeigt, auf denen CatOS und Cisco IOS-Software ausgeführt werden:

CatOS

```
CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on port [mod]/[port]
```

Cisco IOS Software

```
%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet5/1 (not half
duplex), with TBA05071417(Cat6K-B) 4/1 (half duplex).
```

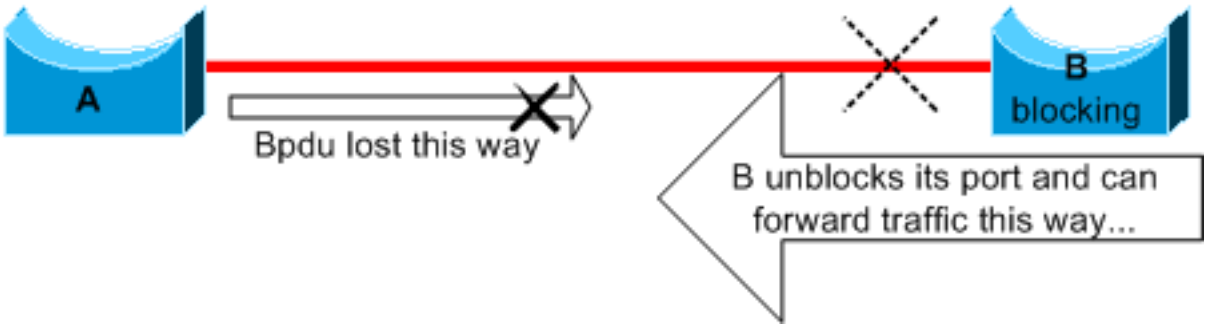
Überprüfen Sie die Duplexeinstellungen, und stellen Sie die Konfiguration entsprechend ein, wenn die Duplexkonfiguration nicht übereinstimmt.

Weitere Informationen zur Behebung eines Duplexkonflikts finden Sie im Dokument zu [Konfiguration und Fehlerbehebung bei Ethernet 10/100/1000Mb mit automatischer Halb-]

/Vollduplex-Aushandlung.

Unidirektionaler Link

Unidirektionale Links sind eine häufige Ursache für Bridging-Schleifen. Bei Glasfaser-Links führt ein unerkannter Ausfall häufig zu unidirektionalen Links. Eine weitere mögliche Ursache ist ein Problem mit einem Transceiver. Alles, was dazu führen kann, dass ein Link bestehen bleibt und eine unidirektionale Kommunikation bereitstellt, ist im Hinblick auf STP sehr riskant. Das folgende Beispiel verdeutlicht dies:



Angenommen, der Link zwischen A und B ist unidirektional. Die Verbindung verwirft Datenverkehr von A nach B, während die Verbindung Datenverkehr von B nach A überträgt. Angenommen, Bridge B wurde blockiert, bevor die Verbindung unidirektional wurde. Ein Port kann nur dann blockieren, wenn er BPDUs von einer Bridge mit höherer Priorität empfängt. Da in diesem Fall alle von A ausgehenden BPDUs verloren gehen, wechselt der Port von Bridge B zu A schließlich in den Weiterleitungsstatus und leitet den Datenverkehr weiter. So entsteht eine Schleife. Wenn dieser Fehler schon beim Start besteht, konvergiert STP nicht richtig. Im Falle einer Duplex-Diskrepanz hilft vorübergehend ein Neustart, aber in diesem Fall hat ein Neustart der Bridges absolut keine Wirkung.

Um die unidirektionalen Links zu erkennen, bevor eine Weiterleitungsschleife entsteht, hat Cisco das UDLD-Protokoll (UniDirectional Link Detection) entwickelt und implementiert. Mit dieser Funktion können falsche Kabelverbindungen oder unidirektionale Links auf Layer 2 erkannt und die daraus resultierenden Schleifen automatisch behoben werden, indem einige Ports deaktiviert werden. Führen Sie UDLD nach Möglichkeit in einer Umgebung mit Bridge aus.

Weitere Informationen zur Verwendung von UDLD finden Sie im Dokument zur Konfiguration der Unidirectional Link Detection Protocol-Funktion.

Paketbeschädigung

Auch beschädigte Pakete können zu Fehlern dieser Art führen. Wenn eine Verbindung einen hohen Anteil physischer Fehler aufweist, kann eine gewisse Anzahl aufeinanderfolgender BPDUs verloren gehen. Dieser Verlust kann dazu führen, dass ein blockierender Port in den Weiterleitungsstatus übergeht. Dieser Fall tritt nicht sehr häufig ein, da die STP-Standardparameter sehr konservativ sind. Der blockierende Port muss BPDUs 50 Sekunden lang verpassen, bevor der Übergang zur Weiterleitung erfolgt. Schon die erfolgreiche Übertragung einer einzelnen BPDU unterbricht die Schleife. Dieser Fall tritt häufig bei unvorsichtiger Anpassung von STP-Parametern auf. Ein Beispiel für eine Anpassung ist die Verringerung des maximalen Alters.

Duplexkonflikte, fehlerhafte Kabel oder falsche Kabellängen können zu Paketbeschädigungen

führen. Eine Erläuterung der Ausgabe des Fehlerzählers bei CatOS und Cisco IOS-Software finden Sie im Dokument zur Fehlerbehebung bei Switch-Port- und Schnittstellenproblemen.

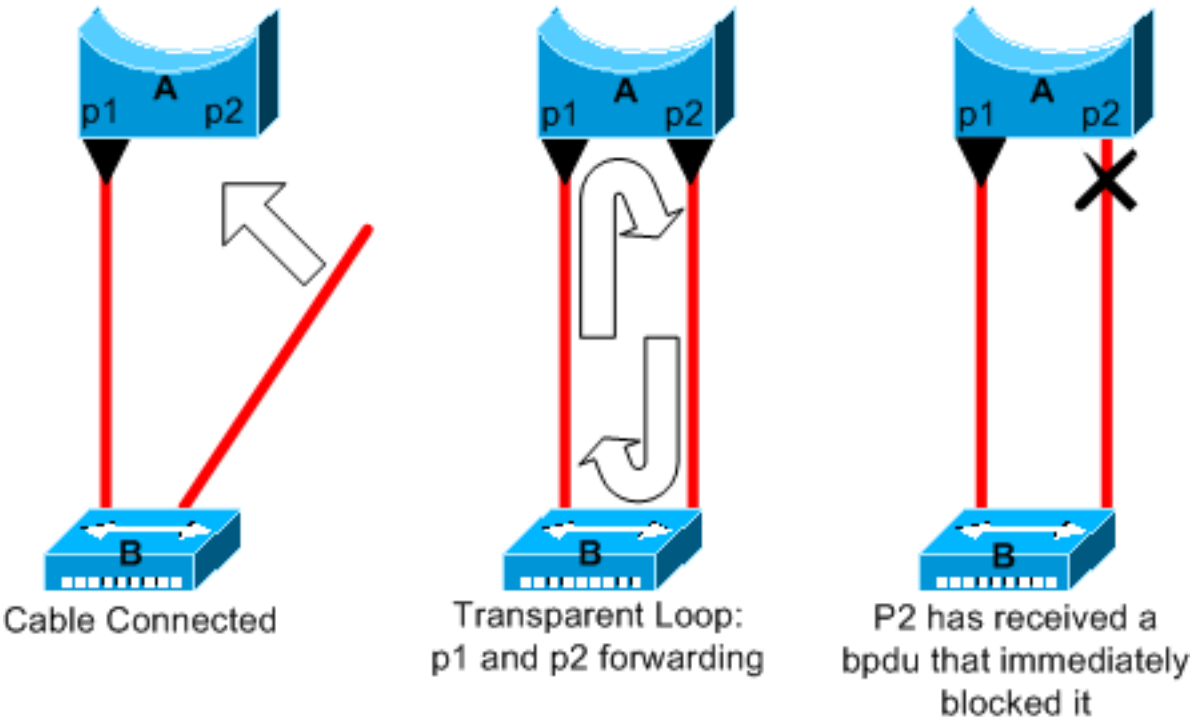
Ressourcenfehler

STP wird in Software implementiert, sogar auf High-End-Switches, die die meisten Switching-Funktionen auf Hardware mit speziellen anwendungsspezifischen integrierten Schaltungen (Application-Specific Integrated Circuits, ASICs) ausführen. Wenn die CPU der Bridge aus irgendeinem Grund überlastet wird, können die Ressourcen für die Übertragung der BPDUs unzureichend sein. Der STA ist im Allgemeinen nicht prozessorintensiv und hat Priorität gegenüber anderen Prozessen. Der Abschnitt Suchen nach Ressourcenfehlern in diesem Dokument enthält einige Richtlinien zur Anzahl der STP-Instanzen, die eine bestimmte Plattform verarbeiten kann.

PortFast-Konfigurationsfehler

PortFast ist eine Funktion, die Sie normalerweise nur für einen Port oder eine Schnittstelle aktivieren, der/die mit einem Host verbunden ist. Wenn der Link an diesem Port hergestellt wird, überspringt die Bridge die ersten Phasen des STA und wechselt direkt in den Weiterleitungsmodus.

> **Achtung:** Verwenden Sie die PortFast-Funktion nicht auf Switch-Ports oder Schnittstellen, die mit anderen Switches, Hubs oder Routern verbunden sind. Andernfalls können Sie eine Netzwerkschleife erstellen.



In diesem Beispiel ist Gerät A eine Bridge, deren Port p1 bereits weiterleitet. Port p2 weist eine PortFast-Konfiguration auf. Gerät B ist ein Hub. Sobald Sie das zweite Kabel an A anschließen, wechselt Port p2 in den Weiterleitungsmodus und erzeugt eine Schleife zwischen p1 und p2. Diese Schleife wird behoben, sobald p1 oder p2 eine BPDU empfängt, die einen dieser beiden Ports in den Blockiermodus versetzt. Es gibt jedoch ein Problem mit dieser Art von vorübergehender Schleife. Wenn der Datenverkehr in der Schleife sehr intensiv ist, kann die

Bridge Probleme mit der erfolgreichen Übertragung der BPDU haben, die die Schleife behebt. Dieses Problem kann die Konvergenz erheblich verzögern oder im Extremfall das Netzwerk zum Ausfallen bringen.

Weitere Informationen zur richtigen Verwendung von PortFast auf Switches, auf denen CatOS oder Cisco IOS-Software ausgeführt wird, finden Sie im Dokument zum Verwenden von PortFast und anderen Befehlen zur Behebung von Verzögerungen beim Start der Workstation-Verbindungen.

Selbst bei einer PortFast-Konfiguration nimmt der Port oder die Schnittstelle weiterhin an STP teil. Wenn ein Switch mit einer niedrigeren Bridge-Priorität als die aktuell aktive Root-Bridge an einen mit PortFast konfigurierten Port oder eine Schnittstelle angeschlossen wird, kann er als Root-Bridge ausgewählt werden. Diese Änderung der Root-Bridge kann die aktive STP-Topologie und damit das Netzwerk beeinträchtigen. Um dies zu verhindern, verfügen die meisten Catalyst Switches, auf denen CatOS oder Cisco IOS-Software ausgeführt wird, über eine Funktion mit dem Namen BPDU Guard. BPDU Guard deaktiviert einen mit PortFast konfigurierten Port oder eine Schnittstelle, wenn der Port oder die Schnittstelle eine BPDU empfängt.

Weitere Informationen zur Verwendung der BPDU Guard-Funktion auf Switches, auf denen CatOS oder Cisco IOS-Software ausgeführt wird, finden Sie im Dokument zur Spanning Tree PortFast BPDU Guard-Erweiterung.

Ungünstige Feinabstimmung von STP-Parametern und Probleme mit dem Durchmesser

Ein aggressiver Wert der Parameter für das maximale Alter und die Weiterleitungsverzögerung kann zu einer sehr instabilen STP-Topologie führen. In solchen Fällen kann der Verlust einiger BPDUs dazu führen, dass eine Schleife entsteht. Ein weiteres eher unbekanntes Problem betrifft den Durchmesser des Bridge-Netzwerks. Die konservativen Standardwerte für die STP-Timer legen einen maximalen Netzwerkdurchmesser von sieben fest. Dieser maximale Netzwerkdurchmesser beschränkt, wie weit voneinander entfernt Bridges im Netzwerk sein dürfen. In diesem Fall dürfen zwei unterschiedliche Bridges nicht mehr als sieben Hops voneinander entfernt sein. Ein Teil dieser Einschränkung ergibt sich aus dem Altersfeld in den BPDUs.

Wenn sich eine BPDU von der Root-Bridge nach außen ausbreitet, wird der Wert im Altersfeld jedes Mal erhöht, wenn die BPDU eine Bridge passiert. Schließlich verwirft die Bridge die BPDU, wenn das Altersfeld das maximale Alter überschreitet. Wenn die Entfernung zwischen der Root-Bridge und einigen Bridges des Netzwerks zu weit ist, kann dieses Problem auftreten. Dieses Problem betrifft die Spanning Tree-Konvergenz.

Seien Sie besonders vorsichtig, wenn Sie vorhaben, bei STP-Timern vom Standardwert abzuweichen. Es ist riskant, auf diese Weise eine schnellere Rekonvergenz erreichen zu wollen. Eine STP-Timer-Änderung hat Auswirkungen auf den Durchmesser des Netzwerks und die Stabilität von STP. Sie können die Bridge-Priorität ändern, um die Root-Bridge auszuwählen, und den Portkosten- oder Prioritätsparameter ändern, um Redundanz und Load Balancing zu steuern.

Die Cisco Catalyst-Software stellt Ihnen Makros zur Verfügung, mit denen Sie die wichtigsten STP-Parameter optimieren können:

- Die Fehlermeldung **set spantree root [secondary]** makro-Befehl verringert die Bridge-Priorität, sodass sie als Root (oder alternativer Root) fungiert. Für diesen Befehl ist eine zusätzliche

Option verfügbar, die zur Optimierung der STP-Timer führt, wenn Sie den Durchmesser Ihres Netzwerks angeben. Selbst wenn dies korrekt durchgeführt wird, verbessert die Timer-Optimierung die Konvergenzzeit nicht wesentlich und führt zu gewissen Instabilitätsrisiken im Netzwerk. Außerdem muss diese Art der Optimierung jedes Mal aktualisiert werden, wenn ein Gerät zum Netzwerk hinzugefügt wird. Behalten Sie die konservativen Standardwerte bei, die Netzwerktechnikern vertraut sind.

- Die Fehlermeldung **set spantree uplinkfast** für CatOS oder die **spanning-tree uplinkfast** für Cisco IOS Software erhöht die Switch-Priorität, sodass der Switch kein Root-Switch sein kann. Der Befehl erhöht die STP-Konvergenzzeit im Falle eines Uplink-Fehlers. Verwenden Sie diesen Befehl auf einem Distribution-Switch mit doppelter Verbindung zu einigen Core-Switches. Weitere Informationen finden Sie im Dokument zu Verständnis und Konfiguration der Cisco UplinkFast-Funktion.
- Die Fehlermeldung **set spantree backbonefast enable** für CatOS oder die **spanning-tree backbonefast** -Befehls für Cisco IOS Software die STP-Konvergenzzeit des Switches bei einem Ausfall der indirekten Verbindung erhöhen kann. BackboneFast ist eine proprietäre Funktion von Cisco. Weitere Informationen finden Sie im Dokument zu Verständnis und Konfiguration von Backbone Fast auf Catalyst Switches.

Weitere Informationen zu STP-Timern und Regeln für deren Optimierung (nur wenn unbedingt erforderlich) finden Sie im Dokument zu Verständnis und Konfiguration von Spanning Tree Protocol-Timern.

Softwarefehler

Wie eingangs erwähnt, ist STP eine der ersten Funktionen, die in Cisco Produkten implementiert wurde. Sie können davon ausgehen, dass diese Funktion sehr stabil ist. Nur die Interaktion mit neueren Funktionen wie EtherChannel hat dazu geführt, dass bei STP in einigen sehr speziellen Fällen Fehler auftraten, die jetzt behoben wurden. Eine Reihe von Faktoren kann einen Software-Bug verursachen und verschiedene Auswirkungen haben. Es gibt keine Möglichkeit, die Probleme, die ein Bug verursachen kann, angemessen zu beschreiben. Die gefährlichste Situation, die sich aus Softwarefehlern ergibt, ist, wenn Sie einige BPDUs ignorieren oder einen blockierenden Port-Übergang zur Weiterleitung haben.

Fehlerbehebung

Leider gibt es kein systematisches Verfahren zur Behebung eines STP-Problems. In diesem Abschnitt werden jedoch einige der Aktionen zusammengefasst, die Ihnen zur Verfügung stehen. Die meisten Schritte in diesem Abschnitt gelten für die Fehlerbehebung bei Bridging-Schleifen im Allgemeinen. Sie können einen konventionelleren Ansatz verwenden, um andere STP-Fehler zu identifizieren, die zu einem Verbindungsverlust führen. Sie können beispielsweise den Pfad untersuchen, den der Datenverkehr nimmt, bei dem ein Problem auftritt.

> **Hinweis**: Bei den meisten Schritten zur Fehlerbehebung wird davon ausgegangen, dass eine Verbindung zu den verschiedenen Geräten des Bridge-Netzwerks besteht. Sie benötigen also Konsolenzugriff. Wenn eine Bridging-Schleife vorliegt, können Sie beispielsweise wahrscheinlich keine Telnet-Verbindung herstellen.

Wenn Sie die Ausgabe eines **show-tech support** CLI Analyzer (nur für registrierte Kunden) verwenden, um potenzielle Probleme und Korrekturen anzuzeigen.

Betrachten des Netzwerkdiagramms

Bevor Sie versuchen, eine Bridging-Schleife zu beheben, müssen Ihnen mindestens die folgenden Informationen vorliegen:

- Topologie des Bridge-Netzwerks
- Position der Root-Bridge
- Position der blockierten Ports und redundanten Links

Diese Informationen sind mindestens aus diesen beiden Gründen unerlässlich:

- Um zu wissen, welche Probleme im Netzwerk Sie beheben sollten, müssen Sie wissen, wie das Netzwerk aussieht, wenn es ordnungsgemäß funktioniert.
- Die meisten Schritte zur Fehlerbehebung müssen **show** Befehle, um Fehlerzustände zu identifizieren. Informationen über das Netzwerk helfen Ihnen, sich auf die kritischen Ports der wichtigsten Geräte zu konzentrieren.

Identifizieren einer Bridging-Schleife

Früher konnte ein Broadcast-Sturm verheerende Auswirkungen auf das Netzwerk haben. Heutzutage ist es bei Hochgeschwindigkeitsverbindungen und Geräten, die Switching auf Hardware-Ebene ermöglichen, unwahrscheinlich, dass ein einzelner Host, beispielsweise ein Server, ein Netzwerk durch Broadcasts zum Ausfallen bringt. Der beste Weg, eine Bridging-Schleife zu identifizieren, besteht darin, den Datenverkehr aus einem gesättigten Link zu erfassen und zu überprüfen, ob ähnliche Pakete mehrmals vorkommen. Wenn jedoch alle Benutzer in einer bestimmten Bridge-Domäne gleichzeitig Konnektivitätsprobleme haben, können Sie bereits eine Bridge-Schleife vermuten.

Überprüfen Sie die Port-Auslastung auf Ihren Geräten, und suchen Sie nach abnormalen Werten. Weitere Informationen finden Sie in diesem Dokument im Abschnitt Überprüfen der Port-Auslastung.

Auf den Catalyst Switches, auf denen CatOS ausgeführt wird, können Sie die Verwendung der Rückwandplatine insgesamt mithilfe des **show system** aus. Der Befehl gibt die aktuelle Auslastung der Switch-Backplane sowie die Spitzenauslastung und das Datum der Spitzenauslastung zurück. Eine ungewöhnliche Spitzenauslastung zeigt, ob es jemals eine Bridging-Schleife auf diesem Gerät gegeben hat.

Schnelle Verbindungswiederherstellung und Vorbereitung auf weitere Fehler

Deaktivieren von Ports, um die Schleife zu unterbrechen

Bridging-Schleifen haben äußerst schwerwiegende Folgen für ein Bridge-Netzwerk. Administratoren bleibt im Allgemeinen keine Zeit, um nach der Ursache der Schleife zu suchen. Sie ziehen es daher meist vor, die Verbindung so schnell wie möglich wiederherzustellen. Der einfache Ausweg besteht in diesem Fall darin, jeden Port, der für Redundanz im Netzwerk sorgt, manuell zu deaktivieren. Wenn Sie den am stärksten betroffenen Teil des Netzwerks identifizieren können, deaktivieren Sie die Ports in diesem Bereich zuerst. Deaktivieren Sie nach Möglichkeit zunächst Ports, die blockiert werden können. Überprüfen Sie jedes Mal, wenn Sie einen Port deaktiviert haben, ob die Netzwerkverbindung dadurch wiederhergestellt wurde. Wenn Sie wissen, welchen Port Sie deaktivieren müssen, um die Schleife zu beheben, kennen Sie auch den

redundanten Pfad, auf dem sich dieser Port befindet. Wenn dieser Port blockiert wurde, haben Sie wahrscheinlich den Link gefunden, auf dem der Fehler aufgetreten ist.

Protokollieren von STP-Ereignissen auf Geräten, die blockierte Ports hosten

Wenn Sie die Ursache des Problems nicht genau identifizieren können oder das Problem nur vorübergehend auftritt, aktivieren Sie die Protokollierung von STP-Ereignissen auf den Bridges und Switches des Netzwerks, bei denen der Fehler auftritt. Wenn Sie die Anzahl der zu konfigurierenden Geräte begrenzen möchten, aktivieren Sie diese Protokollierung zumindest für Geräte, die blockierte Ports hosten. Der Übergang eines blockierten Ports erzeugt eine Schleife.

- Cisco IOS-Software - Geben Sie den Befehl exec ein. **debug spanning-tree events** um STP-Debugging-Informationen zu aktivieren. Geben Sie den Befehl für den allgemeinen Konfigurationsmodus ein. **logging buffered** um diese Debugging-Informationen in den Gerätepuffern zu erfassen.
- CatOS **set logging level spantree 7 default** erhöht die Standardstufe von Ereignissen, die sich auf STP beziehen, auf die Debugstufe. Stellen Sie sicher, dass Sie eine maximale Anzahl von Nachrichten in den Switch-Puffern protokollieren, indem Sie die **set logging buffer 500** aus.

Sie können auch versuchen, die Debug-Ausgabe an ein Syslog-Gerät zu senden. Leider bleibt die Verbindung zu einem Syslog-Server selten bestehen, wenn eine Bridging-Schleife auftritt.

Überprüfen der Ports

Die kritischen Ports, die zuerst untersucht werden sollten, sind die blockierenden Ports. Dieser Abschnitt enthält eine Liste der Elemente, auf die Sie bei den verschiedenen Ports achten müssen, sowie eine kurze Beschreibung der Befehle, die für Switches mit CatOS und Cisco IOS-Software ausgeführt werden sollten.

Überprüfen, ob blockierte Ports BPDUs empfangen

Überprüfen Sie insbesondere bei blockierten Ports und Root-Ports, ob diese regelmäßig BPDUs empfangen. Mehrere Probleme können dazu führen, dass der Port keine Pakete oder BPDUs empfängt.

- Cisco IOS Software-In Cisco IOS Software Version 12.0 oder höher, Ausgabe der **show spanning-tree bridge-group #** -Befehls ein `BPDU`-Feld hat. Diesem Feld können Sie die Anzahl der empfangenen BPDUs für jede Schnittstelle entnehmen. Führen Sie den Befehl noch ein- oder zweimal aus, um festzustellen, ob das Gerät BPDUs empfängt.Wenn das `BPDU`-Feld in der Ausgabe von **show spanning-tree** können Sie das STP-Debugging mit dem Befehl **debug spanning-tree** , um den Empfang von BPDUs zu überprüfen.
- CatOS **show mac module/port** anzeigt, wie viele Multicast-Pakete ein bestimmter Port empfängt. Der einfachste Befehl ist jedoch **show spantree statistics module#/port# vlan#** aus. Dieser Befehl gibt die genaue Anzahl der Konfigurations-BPDUs zurück, die ein bestimmter Port in einem bestimmten VLAN empfangen hat. Ein Port kann bei Trunking zu mehreren VLANs gehören. Weitere Informationen finden Sie in diesem Dokument im Abschnitt Ein zusätzlicher CatOS-Befehl.

Überprüfen auf einen Duplexkonflikt

Um mögliche Duplexkonflikte zu ermitteln, müssen Sie jede Seite des Punkt-zu-Punkt-Links überprüfen.

- Cisco IOS Software-Issue der **show interfaces [interface interface-number] status** , um die Geschwindigkeit und den Duplexstatus des jeweiligen Ports zu überprüfen.
- CatOS - Die allerersten Zeilen der Ausgabe des **show port module#/port#** geben Ihnen die Geschwindigkeit und den Duplex-Modus entsprechend der Port-Konfiguration.

Überprüfen der Port-Auslastung

Eine Schnittstelle mit Datenverkehrsüberlastung überträgt möglicherweise wichtige BPDUs nicht. Eine Link-Überlastung weist auch auf eine mögliche Bridging-Schleife hin.

- Cisco IOS-Software: Verwenden Sie den Befehl **show interfaces** um die Auslastung einer Schnittstelle zu ermitteln. Mehrere Felder helfen Ihnen dabei, beispielsweise `load` und `packets input/output`. Im Dokument Troubleshooting Switch Port and Interface Problems (Problembehebung bei Switch-Ports und Schnittstellen) finden Sie eine Erläuterung der **show interfaces** Befehlsausgabe.
- CatOS **show mac module#/port#** zeigt Statistiken zu Paketen an, die ein Port empfängt und sendet. Die Fehlermeldung **show top** evaluiert die Port-Nutzung automatisch über einen Zeitraum von 30 Sekunden und zeigt das Ergebnis an. Bei diesem Befehl werden die Ergebnisse nach prozentualer Bandbreitennutzung klassifiziert. Es sind jedoch auch andere Optionen für die Ergebnisklassifizierung verfügbar. Darüber hinaus **show system** gibt einen Hinweis auf die Backplane-Nutzung, auch wenn der Befehl nicht auf einen bestimmten Port verweist.

Überprüfen auf Paketbeschädigung

- Cisco IOS Software: Suchen Sie nach Fehlerinkrementen im `Eingabefehlerzähler` der **show interfaces** aus. Zu diesen Fehlerzählern gehören runts, giants, no buffer, CRC, frame, overrun und ignored.Im Dokument Troubleshooting Switch Port and Interface Problems (Problembehebung bei Switch-Ports und Schnittstellen) finden Sie eine Erläuterung der **show interfaces** command output.
- CatOS - Der Befehl **show port module#/port#** enthält einige Details zu den Feldern `Align-Err, FCS-Err, Xmit-Err, Rcv-Err` und `Undersize`. Die Fehlermeldung **show counters module#/port#** liefert noch detailliertere Statistiken.

Ein zusätzlicher CatOS-Befehl

Der Befehl **show spantree statistics module#/port# vlan#** liefert sehr genaue Informationen über einen bestimmten Port. Geben Sie diesen Befehl für Ports aus, die Ihnen verdächtig vorkommen, und achten Sie besonders auf folgende Felder:

- `Forward trans count` (Anzahl der Weiterleitungen) - Dieser Zähler merkt sich, wie oft ein Port vom Lernen zum Weiterleiten wechselt. In einer stabilen Topologie zeigt dieser Zähler immer 1 an. Der Zähler wird auf 0 zurückgesetzt, wenn der Port deaktiviert und wieder aktiviert wird. Ein Wert größer als 1 zeigt somit an, dass der Übergang des Ports das Ergebnis einer STP-Neuberechnung ist. Der Übergang ist nicht das Ergebnis eines Ausfalls des direkten Links.

- `Max age expiry count` (Maximales Alter) - Dieser Zähler verfolgt, wie oft das maximale Alter für diesen Link abgelaufen ist. Grundsätzlich wartet ein Port, der BPDUs erwartet, bis zum maximalen Alter, bevor er die designierte Bridge als verloren betrachtet. Der Standardwert für das maximale Alter ist 20 Sekunden. Jedes Mal, wenn dieses Ereignis eintritt, wird der Zähler erhöht. Wenn der Wert nicht 0 ist, bedeutet dies, dass die designierte Bridge für dieses LAN instabil ist oder ein Problem mit der Übertragung von BPDUs besteht.

Suchen nach Ressourcenfehlern

Eine hohe CPU-Auslastung kann für ein System, auf dem der STA ausgeführt wird, riskant sein. Überprüfen Sie mit folgender Methode, ob die CPU-Ressourcen für ein Gerät ausreichen:

- Cisco IOS-Software: Verwenden Sie den Befehl **show processes cpu.** Vergewissern Sie sich, dass die CPU-Auslastung nicht zu hoch ist. Informationen zu Catalyst 4500/4000 Switches, auf denen CatOS oder Cisco IOS-Software ausgeführt wird, finden Sie im Dokument zur CPU-Auslastung auf Catalyst 4500/4000, 2948G, 2980G und 4912G Switches.
- CatOS - Ausgabe des **show proc cpu** command to display CPU utilization information. Check that the CPU utilization is not too high.

Eine Supervisor Engine kann nur eine bestimmte Anzahl an STP-Instanzen unterstützen. Achten Sie darauf, dass die Gesamtanzahl der logischen Ports in allen STP-Instanzen für verschiedene VLANs die maximal unterstützte Anzahl für jeden Supervisor Engine-Typ und jede Arbeitsspeicherkonfiguration nicht überschreitet.

Stellen Sie die **show spantree summary** -Befehl für Switches, auf denen CatOS oder der **show spanning-tree summary totals** -Befehls für Switches, auf denen Cisco IOS-Software ausgeführt wird. In der Spalte `STP Active` (STP aktiv) der Befehlsausgabe ist die Anzahl der logischen Ports oder Schnittstellen pro VLAN zu finden. Die Gesamtanzahl wird unten in dieser Spalte angezeigt. Diese Gesamtanzahl ist die Summe aller logischen Ports in allen STP-Instanzen für die verschiedenen VLANs. Vergewissern Sie sich, dass diese Anzahl die maximal unterstützte Anzahl für jeden Supervisor Engine-Typ nicht überschreitet.

Hinweis: Die Formel zur Berechnung der Summe der logischen Ports auf dem Switch lautet:

```
(number of non-ATM trunks * number of active Vlans on that trunk)
+ 2*(number of ATM trunks * number of active Vlans on that trunk)
+ number of non-trunking ports
```

Eine Zusammenfassung der STP-Einschränkungen für Catalyst Switches finden Sie in diesen Dokumenten:

Plattform	STP-Einschränkungen bei CatOS	STP-Einschränkungen bei Cisco IO Software
Catalyst 6500/6000 Supervisor Engine I und II	Fehlerbehebung bei STP	
Catalyst 6500/6000 Supervisor Engine 720	Fehlerbehebung bei STP	Fehlerbehebung bei Spanning Tre
Catalyst 4500/4000 Catalyst 3750	Spanning Tree	Fehlerbehebung bei Spanning Tre Konfigurieren von STP

Deaktivieren nicht benötigter Funktionen

Bei der Fehlerbehebung versuchen Sie festzustellen, was im Netzwerk derzeit falsch ist. Deaktivieren Sie so viele Funktionen wie möglich. Die Deaktivierung vereinfacht die Netzwerkstruktur und erleichtert die Identifizierung des Problems. EtherChanneling ist beispielsweise eine Funktion, bei der STP mehrere verschiedene Verbindungen logisch zu einer einzigen Verbindung bündeln muss. Die Deaktivierung dieser Funktion während des Fehlerbehebungsprozesses ist sinnvoll. Wenn Sie die Konfiguration so einfach wie möglich gestalten, wird die Fehlerbehebung allgemein vereinfacht.

Nützliche Befehle

Cisco IOS Software-Befehle

- **show interfaces**
- **show spanning-tree**
- **show bridge**
- **show processes cpu**
- **debug spanning-tree**
- **logging buffered**

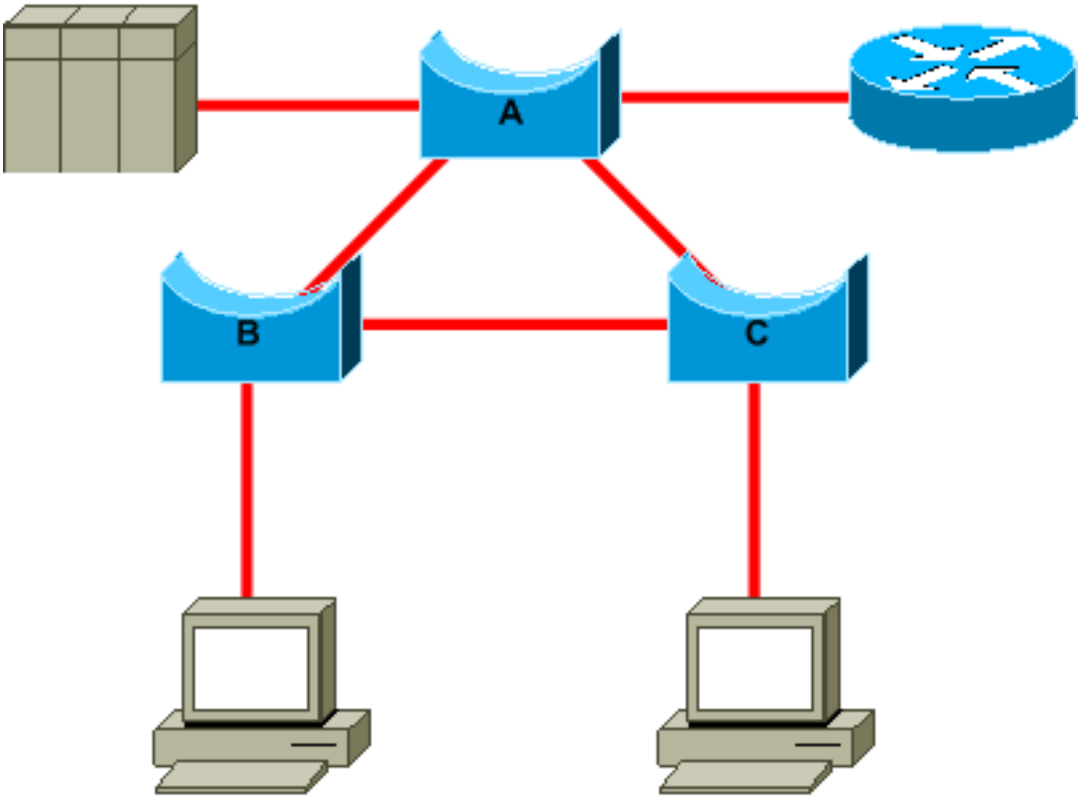
CatOS-Befehle

- **show port**
- **show mac**
- **show spantree**
- **show spantree statistics**
- **show spantree blockedports**
- **show spantree summary**
- **show top**
- **show proc cpu**
- **show system**
- **show counters**
- **set spantree root [secondary]**
- **set spantree uplinkfast**
- **set logging level**
- **set logging buffered**

Gezieltes STP-Design zur Vermeidung von Problemen

Auffinden des Roots

Sehr oft sind Informationen zur Position der Root-Bridge zum Zeitpunkt der Fehlerbehebung nicht verfügbar. Überlassen Sie die Entscheidung, welche Bridge die Root-Bridge ist, nicht dem STP. In der Regel lässt sich für jedes VLAN ermitteln, welcher Switch am besten als Root-Bridge geeignet ist. Dies hängt vom Design des Netzwerks ab. Im Allgemeinen sollten Sie eine leistungsstarke Bridge in der Mitte des Netzwerks auswählen. Wenn Sie die Root-Bridge in der Mitte des Netzwerks mit direkter Verbindung zu den Servern und Routern platzieren, verringern Sie allgemein die durchschnittliche Entfernung von den Clients zu den Servern und Routern.



Dieses Diagramm zeigt:

- Wenn Bridge B die Root-Bridge ist, wird der Link von A zu C auf Bridge A oder Bridge C blockiert. In diesem Fall können Hosts, die sich mit Switch B verbinden, den Server und den Router in zwei Hops erreichen. Hosts, die sich mit Bridge C verbinden, können den Server und den Router in drei Hops erreichen. Die durchschnittliche Entfernung beträgt zweieinhalb Hops.
- Wenn Bridge A die Root-Bridge ist, sind der Router und der Server für beide Hosts, die eine Verbindung zu B und C herstellen, in zwei Hops erreichbar. Die durchschnittliche Entfernung beträgt jetzt zwei Hops.

Die Logik hinter diesem einfachen Beispiel lässt sich auf komplexere Topologien übertragen.

> **Hinweis**: Codieren Sie für jedes VLAN die Root-Bridge und die Backup-Root-Bridge fest, und reduzieren Sie dabei den Wert des STP-Prioritätsparameters. Alternativ können Sie das Makro set spantree root verwenden.

Redundanzplanung

Planen Sie die Organisation Ihrer redundanten Links. Verzichten Sie auf die Plug-and-Play-Funktion von STP. Optimieren Sie den STP-Kostenparameter, um zu entscheiden, welche Ports blockiert werden. Diese Optimierung ist in der Regel nicht erforderlich, wenn Sie ein hierarchisches Design und eine Root-Bridge in geeigneter Position haben.

> **Hinweis:** Wissen Sie für jedes VLAN, welche Ports im stabilen Netzwerk blockiert werden können. Erstellen Sie ein Netzwerkdiagramm, das jede physische Schleife im Netzwerk anzeigt, durch die blockierte Ports die Schleifen unterbrechen.

Wenn Sie die Position redundanter Links kennen, können Sie versehentliche Bridge-Schleifen und

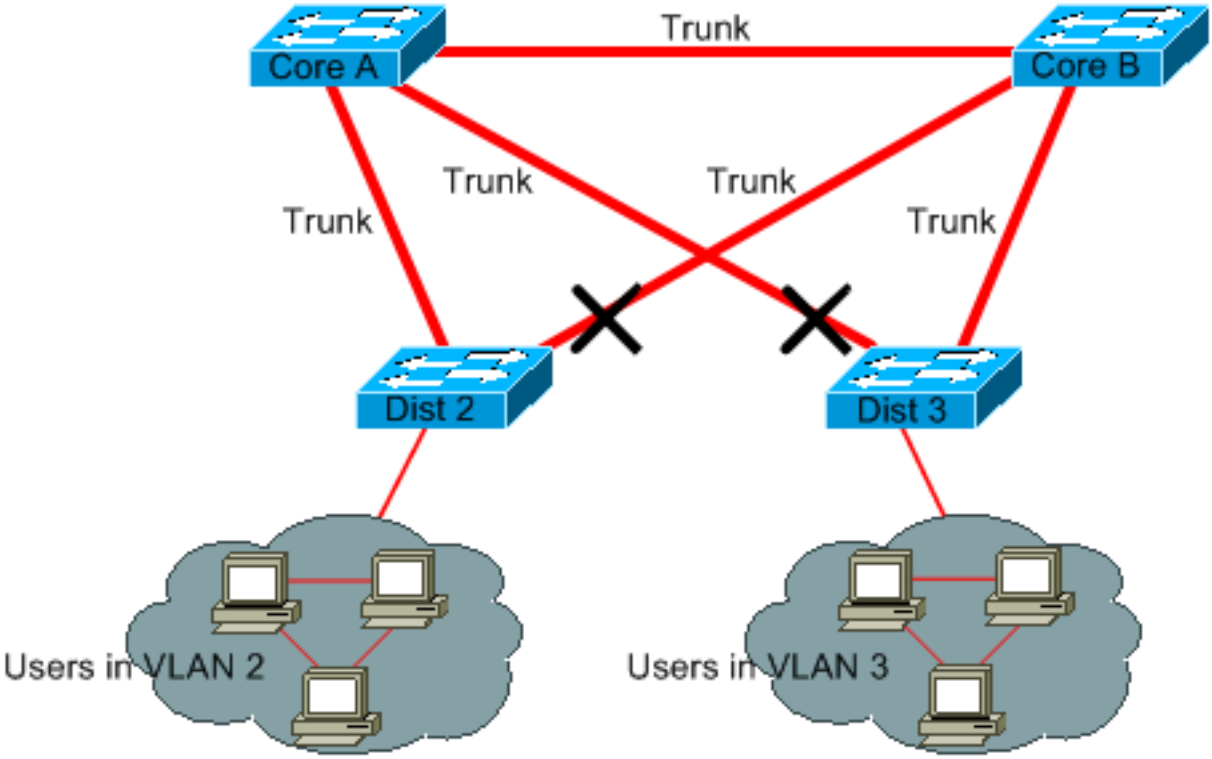
deren Ursache besser identifizieren. Wenn Ihnen zusätzlich die Position der blockierten Ports bekannt ist, können Sie auch den Fehlerort bestimmen.

Minimieren der Anzahl blockierter Ports

Die einzige kritische Aktion, die STP durchführt, ist das Blockieren der Ports. Ein einzelner blockierender Port, der fälschlicherweise zur Weiterleitung übergeht, kann einen großen Teil des Netzwerks zum Ausfallen bringen. Eine gute Möglichkeit, das mit der Verwendung von STP verbundene Risiko zu begrenzen, besteht darin, die Anzahl der blockierten Ports so weit wie möglich zu reduzieren.

Entfernen nicht verwendeter VLANs

Sie benötigen nicht mehr als zwei redundante Links zwischen zwei Knoten in einem Bridge-Netzwerk. Diese Art der Konfiguration ist jedoch üblich:

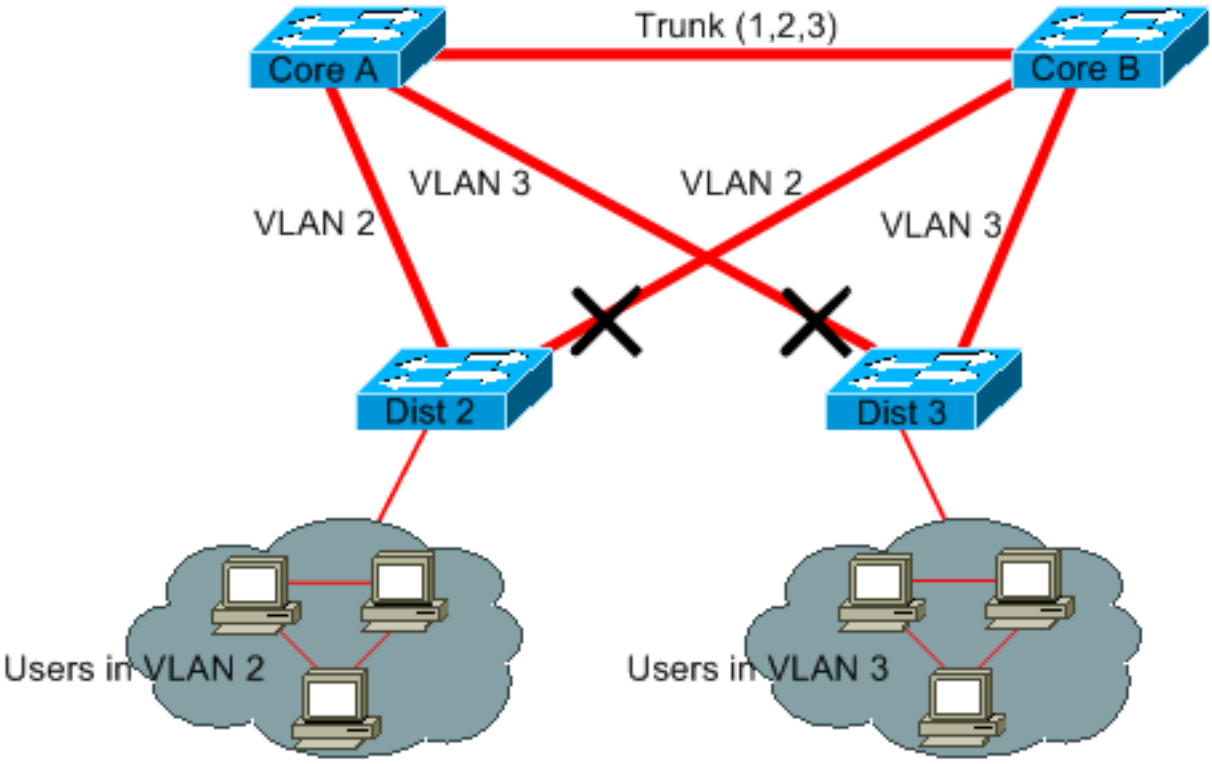


Die Distribution-Switches sind mit zwei Core-Switches verbunden. Benutzer, die eine Verbindung über Distribution-Switches herstellen, gehören nur zu einer Teilmenge der im Netzwerk verfügbaren VLANs. In diesem Beispiel befinden sich alle Benutzer, die eine Verbindung über Dist 2 herstellen, in VLAN 2. Dist 3 verbindet Benutzer nur über VLAN 3. Standardmäßig unterstützen Trunks alle VLANs, die in der VTP-Domäne (VLAN Trunk Protocol) definiert sind. Nur Dist 2 empfängt unnötigen Broadcast- und Multicast-Datenverkehr für VLAN 3, blockiert jedoch auch einen seiner Ports für VLAN 3. Das Ergebnis: drei redundante Pfade zwischen Core A und Core B. Diese Redundanz führt zu mehr blockierten Ports und erhöht die Wahrscheinlichkeit einer Schleife.

Hinweis: Entfernen Sie alle VLANs, die Sie nicht benötigen, von Ihren Trunks.

Die VTP-Bereinigung kann zwar dazu beitragen, aber diese Art von Plug-and-Play-Funktion ist im Netzwerk-Core nicht erforderlich.

In diesem Beispiel wird nur ein Zugriffs-VLAN verwendet, um die Distribution-Switches mit dem Core zu verbinden:



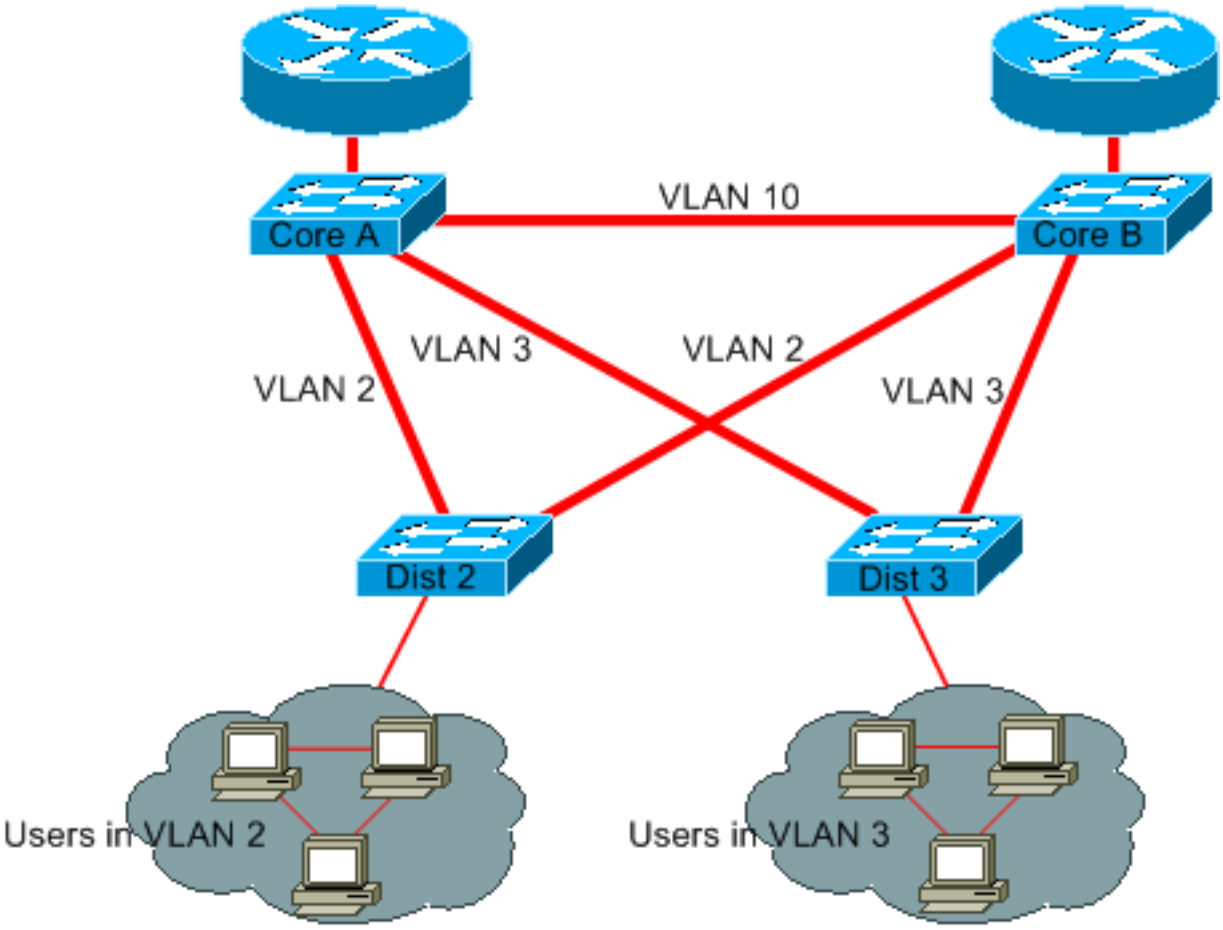
In diesem Design wird nur ein Port pro VLAN blockiert. Außerdem können Sie bei diesem Design alle redundanten Links in nur einem Schritt entfernen, wenn Sie Core A oder Core B herunterfahren.

Verwenden von Layer-3-Switching

Layer-3-Switching-Mittel, die annähernd mit der Switching-Geschwindigkeit routen. Router erfüllen zwei wesentliche Funktionen:

- Router erstellen eine Weiterleitungstabelle. Für dem Informationsaustausch zwischen Routern und Peers werden generell Routing-Protokolle genutzt.
- Router empfangen Pakete und leiten sie basierend auf der Zieladresse an die richtige Schnittstelle weiter.

High-End-Layer-3-Switches von Cisco können diese zweite Funktion jetzt mit derselben Geschwindigkeit wie die Layer-2-Switching-Funktion ausführen. Wenn Sie einen Routing-Hop einführen und eine zusätzliche Segmentierung des Netzwerks erstellen, gibt es keine Geschwindigkeitseinbußen. In diesem Diagramm wird das Beispiel aus dem Abschnitt Entfernen nicht verwendeter VLANs als Grundlage verwendet:



Core A und Core B sind jetzt Layer-3-Switches. Für VLAN 2 und VLAN 3 erfolgt kein Bridging mehr zwischen Core A und Core B, sodass keine STP-Schleife möglich ist.

- Redundanz ist weiterhin gegeben, wobei auf Layer-3-Routing-Protokolle zurückgegriffen wird. Das Design ermöglicht eine Rekonvergenz, die noch schneller erfolgt als die Rekonvergenz mit STP.
- Es gibt keinen einzelnen Port mehr, der von STP blockiert wird. Daher besteht nicht das Risiko einer Bridging-Schleife.
- Es gibt keine Geschwindigkeitseinbußen, da das VLAN durch Layer-3-Switching genauso schnell bleibt wie das Bridging innerhalb des VLAN.

Dieses Design hat nur einen einzigen Nachteil. Die Migration zu dieser Art von Design erfordert im Allgemeinen eine Überarbeitung des Adressierungsschemas.

Beibehalten von STP, auch wenn es unnötig ist

Auch wenn es Ihnen gelungen ist, alle blockierten Ports aus Ihrem Netzwerk zu entfernen, und keine physische Redundanz vorliegt, sollten Sie STP nicht deaktivieren. STP ist im Allgemeinen nicht sehr prozessorintensiv; beim Packet-Switching ist die CPU bei den meisten Cisco Switches nicht involviert. Außerdem reduzieren die wenigen BPDUs, die über die einzelnen Links gesendet werden, die verfügbare Bandbreite nicht wesentlich. Ein Bridge-Netzwerk ohne STP kann jedoch im Bruchteil einer Sekunde ausfallen, wenn ein Bediener beispielsweise an einem Patchpanel einen Fehler macht. Im Allgemeinen ist das Deaktivieren von STP in einem Bridge-Netzwerk zu riskant.

Fernhalten des Datenverkehrs vom administrativen VLAN; kein einzelnes VLAN für das gesamte Netzwerk

Ein Cisco Switch hat in der Regel eine einzelne IP-Adresse, die an ein VLAN gebunden ist, das als administratives VLAN bezeichnet wird. In diesem VLAN verhält sich der Switch wie ein generischer IP-Host. Insbesondere wird jedes Broadcast- oder Multicast-Paket an die CPU weitergeleitet. Ein hohes Maß an Broadcast- oder Multicast-Datenverkehr im administrativen VLAN kann die CPU und die Fähigkeit der CPU zur Verarbeitung wichtiger BPDUs beeinträchtigen. Halten Sie daher den Benutzerdatenverkehr vom administrativen VLAN fern.

Bis vor Kurzem gab es in der Cisco Implementierung keine Möglichkeit, VLAN 1 aus einem Trunk zu entfernen. VLAN 1 dient im Allgemeinen als administratives VLAN, über das auf alle Switches im selben IP-Subnetz zugegriffen werden kann. Diese Art der Einrichtung ist zwar nützlich, kann jedoch riskant sein, da eine Bridging-Schleife in VLAN 1 alle Trunks betrifft, was das gesamte Netzwerk zum Absturz bringen kann. Natürlich besteht dieses Risiko unabhängig vom verwendeten VLAN. Versuchen Sie, die Bridging-Domänen mithilfe von Hochgeschwindigkeits-Layer-3-Switches zu segmentieren.

Ab CatOS Version 5.4 und Cisco IOS-Software Version 12.1(11b)E können Sie VLAN 1 aus Trunks entfernen. VLAN 1 ist dann zwar noch vorhanden, blockiert jedoch den Datenverkehr, sodass keine Schleife entstehen kann.

Zugehörige Informationen

- Tools und Ressourcen – technischer Support und Dokumentation
- Technischer Support und Dokumentation für Cisco Systeme

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.