Erweiterung des Spanning Tree Protocol mit Root Guard

Inhalt

Einleitung

In diesem Dokument werden die verbesserten STP-Root-Guard-Funktionen beschrieben, die die Zuverlässigkeit, Verwaltbarkeit und Sicherheit von Switched-Netzwerken verbessern.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

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

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

Konventionen

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

Beschreibung

Das Standard-STP bietet dem Netzwerkadministrator keine Möglichkeit, die Topologie des Layer-2-Switched-Netzwerks (L2) sicher durchzusetzen. Eine Möglichkeit zur Durchsetzung der Topologie kann besonders in Netzwerken wichtig sein, in denen eine gemeinsame administrative Kontrolle stattfindet und verschiedene administrative Einheiten oder Unternehmen ein Switch-Netzwerk steuern.

Die Weiterleitungstopologie des Switched-Netzwerks wird berechnet. Die Berechnung basiert u.a. auf der Root-Bridge-Position. Jeder Switch kann die Root-Bridge in einem Netzwerk sein. Eine optimierte Weiterleitungstopologie platziert die Root Bridge jedoch an einem bestimmten vorbestimmten Ort. Beim Standard-STP übernimmt jede Bridge im Netzwerk mit einer niedrigeren Bridge-ID die Rolle der Root-Bridge. Der Administrator kann die Position der Root-Bridge nicht erzwingen.

> **Hinweis**: Der Administrator kann die Root-Bridge-Priorität auf 0 setzen, um die Root-Bridge-Position zu sichern. Eine Bridge mit der Priorität 0 und einer niedrigeren MAC-Adresse ist jedoch nicht garantiert.

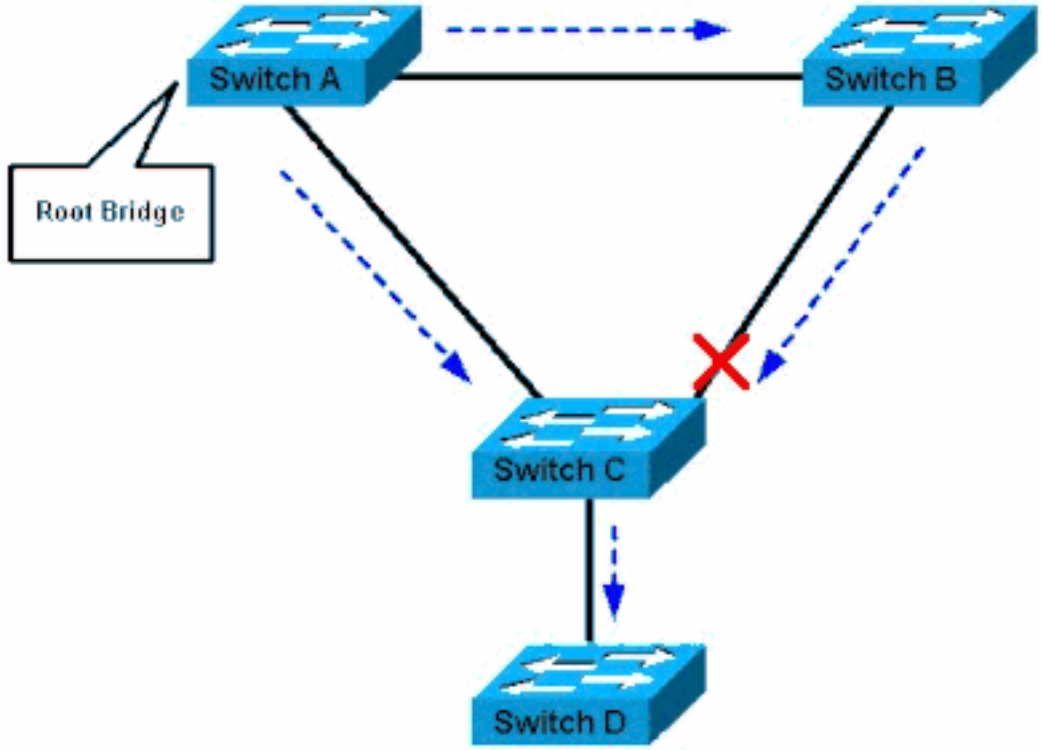
Die Root Guard-Funktion bietet eine Möglichkeit, die Root Bridge-Platzierung im Netzwerk durchzusetzen.

Der Root Guard stellt sicher, dass der Port, auf dem der Root Guard aktiviert ist, der designierte Port ist. In der Regel handelt es sich bei den Root-Bridge-Ports um designierte Ports, es sei denn, zwei oder mehr Ports der Root-Bridge sind miteinander verbunden. Wenn die Bridge überlegene STP Bridge Protocol Data Units (BPDUs) an einem Root Guard-fähigen Port empfängt, verschiebt Root Guard diesen Port in einen Root-inkonsistenten STP-Status. Dieser inkonsistente Stamm-Zustand entspricht im Grunde einem Zuhörzustand. Über diesen Port wird kein Datenverkehr weitergeleitet. Auf diese Weise erzwingt der Root Guard die Position der Root Bridge.

Das Beispiel in diesem Abschnitt zeigt, wie eine nicht autorisierte Root-Bridge Probleme im Netzwerk verursachen kann und wie Root Guard helfen kann.

In Abbildung 1 bilden die Switches A und B den Kern des Netzwerks, und A ist die Root-Bridge für ein VLAN. Switch C ist ein Access Layer Switch. Die Verbindung zwischen B und C ist auf der C-Seite blockiert. Die Pfeile zeigen den Fluss von STP-BPDUs.

Abbildung 1

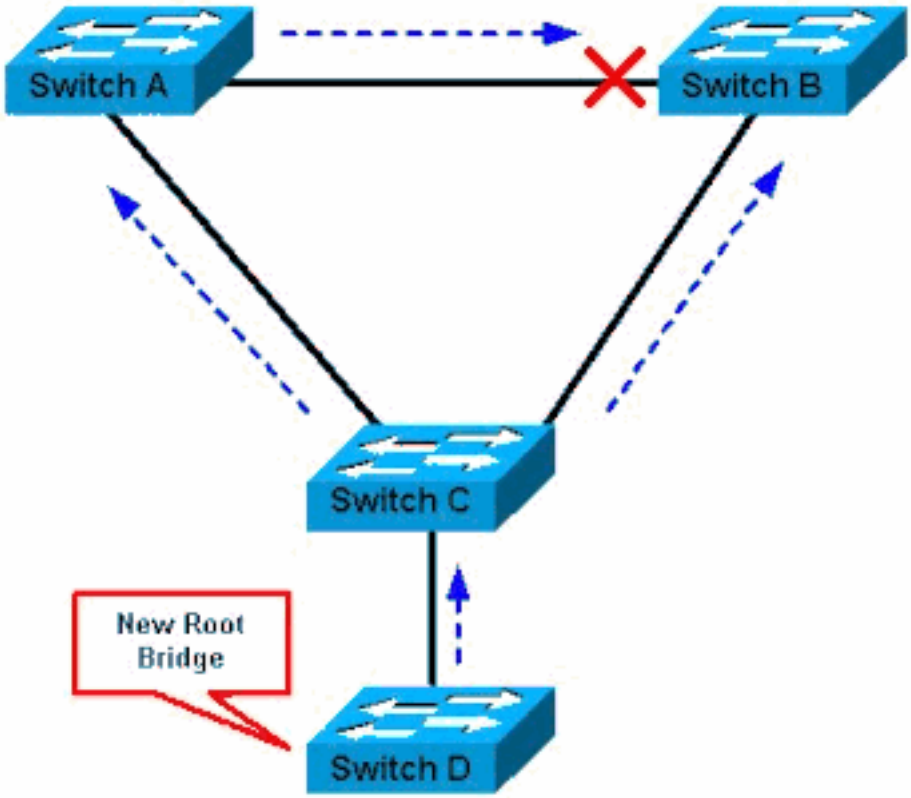


Switch A ist die Root Bridge

In Abbildung 2 nimmt Gerät D am STP teil. Softwarebasierte Bridge-Anwendungen werden beispielsweise auf PCs oder anderen Switches gestartet, die Sie mit einem Service-Provider-Netzwerk verbinden. Wenn die Priorität von Bridge D 0 oder ein beliebiger Wert niedriger als die Priorität der Root-Bridge ist, wird Device D als Root-Bridge für dieses VLAN ausgewählt. Wenn die Verbindung zwischen Gerät A und B 1 Gigabit beträgt und die Verbindungen zwischen A und C sowie zwischen B und C 100 Mbit/s betragen, wird die Gigabit-Ethernet-Verbindung, die die beiden Core-Switches verbindet, durch die Auswahl von D als Root blockiert.

Dieser Block bewirkt, dass alle Daten in diesem VLAN über eine 100-Mbit/s-Verbindung durch den Access Layer fließen. Wenn mehr Daten über den Core in diesem VLAN übertragen werden, als dieser Link aufnehmen kann, werden einige Frames verworfen. Der Frame-Verlust führt zu einem Leistungsverlust oder einem Verbindungsausfall.

Abbildung 2



Switch D ist neue Root Bridge

Die Root-Guard-Funktion schützt das Netzwerk vor solchen Problemen.

Die Konfiguration von Root Guard erfolgt auf Port-Basis. Root Guard verhindert, dass der Port ein STP-Root-Port wird, sodass der Port immer STP-zugewiesen ist. Wenn an diesem Port eine bessere BPDU eingeht, berücksichtigt Root Guard die BPDU nicht und wählt einen neuen STP-Root aus. Stattdessen setzt Root Guard den Port in den Root-inkonsistenten STP-Status. Sie müssen Root Guard auf allen Ports aktivieren, an denen die Root-Bridge nicht angezeigt werden darf. Auf gewisse Weise können Sie einen Perimeter um den Teil des Netzwerks herum konfigurieren, in dem sich der STP-Root befinden kann.

In Abbildung 2 aktivieren Sie den Root Guard am Switch C-Port, der mit Switch D verbunden wird.

Switch C in Abbildung 2 blockiert den Port, der mit Switch D verbunden wird, nachdem der Switch eine überlegene BPDU erhalten hat. Root Guard versetzt den Port in den Root-inkonsistenten STP-Status. In diesem Zustand wird kein Datenverkehr durch den Port geleitet. Nachdem Gerät D die Übertragung besserer BPDUs beendet hat, wird der Port wieder freigegeben. Über STP wechselt der Port vom überwachenden in den lernenden Status und wechselt schließlich in den weiterleitenden Status. Die Erholung erfolgt automatisch; ein menschliches Eingreifen ist nicht erforderlich.

Diese Meldung wird angezeigt, nachdem Root Guard einen Port blockiert:

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated in VLAN 77.
Moved to root-inconsistent state
```

Verfügbarkeit

Root Guard ist in Catalyst 6500/6000 verfügbar, auf dem die Cisco IOS®-Systemsoftware

ausgeführt wird. Diese Funktion wurde erstmals in Version 12.0(7)XE der Cisco IOS-Software eingeführt. Für den Catalyst 4500/4000, auf dem die Cisco IOS-Systemsoftware ausgeführt wird, ist diese Funktion in allen Versionen verfügbar.

Für die Catalyst Switches der Serien 2900XL und 3500XL ist Root Guard ab Version 12.0(5)XU der Cisco IOS Software verfügbar. Die Switches der Serie Catalyst 2950 unterstützen die Root Guard-Funktion in Version 12.0(5.2)WC(1) und höher der Cisco IOS-Software. Die Switches der Serie Catalyst 3550 unterstützen die Root Guard-Funktion in Version 12.1(4)EA1 und höher der Cisco IOS-Software.

Diese Funktion steht auch für neuere Cisco Catalyst Switches zur Verfügung.

Konfiguration

Cisco IOS Software-Konfiguration für Catalyst 6500/6000 und Catalyst 4500/4000

Führen Sie auf den Catalyst Switches der Serien 6500/6000 oder 4500/4000, auf denen Cisco IOS-Systemsoftware ausgeführt wird, diese Befehle aus, um STP Root Guard zu konfigurieren:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
!
Switch#(config)#interface fastethernet 3/1
Switch#(config-if)#spanning-tree guard root
!
```

> **Hinweis:** In Version 12.1(3a)E3 der Cisco IOS Software für den Catalyst 6500/6000, der die Cisco IOS-Systemsoftware ausführt, wurde dieser Befehl von **Spanning-Tree Rootguard** in **"Spanning-Tree Guard Root"** geändert. Der Catalyst 4500/4000, auf dem die Cisco IOS-Systemsoftware ausgeführt wird, verwendet in allen Versionen den Befehl **spanning-tree guard root**.

Cisco IOS Software-Konfiguration für Catalyst 2900XL/3500XL, 2950 und 3550

Konfigurieren Sie auf den Catalyst Switches 2900XL, 3500XL, 2950 und 3550 Switches mit Root Guard im Schnittstellenkonfigurationsmodus, wie in diesem Beispiel gezeigt:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet 0/8
Switch(config-if)# spanning-tree rootguard
Switch(config-if)# ^Z
*Mar 15 20:15:16: %SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Rootguard enabled on
port FastEthernet0/8 VLAN 1.
Switch#
```

Worin besteht der Unterschied zwischen STP BPDU Guard und STP Root Guard?

BPDU Guard und Root Guard sind ähnlich, aber ihre Auswirkungen sind unterschiedlich. BPDU Guard deaktiviert den Port beim BPDU-Empfang, wenn PortFast auf dem Port aktiviert ist. Diese

Deaktivierung verhindert effektiv, dass Geräte hinter solchen Ports an STP teilnehmen. Sie müssen den Port, der in den errdisable-Status versetzt wird, manuell erneut aktivieren oder **errdisable-timeout** konfigurieren.

Root Guard ermöglicht dem Gerät, am STP teilzunehmen, solange es nicht versucht, als Root-Benutzer zu fungieren. Wenn der Root Guard den Port blockiert, erfolgt die anschließende Wiederherstellung automatisch. Die Wiederherstellung erfolgt, sobald das abweichende Gerät keine überlegenen BPDUs mehr sendet.

Weitere Informationen zu BPDU Guard finden Sie unter Spanning Tree PortFast BPDU Guard Enhancement.

Hilft der Root Guard bei dem Problem mit den zwei Wurzeln?

Es kann zu einem unidirektionalen Verbindungsausfall zwischen zwei Bridges in einem Netzwerk kommen. Aufgrund des Fehlers empfängt eine Bridge die BPDUs nicht von der Root-Bridge. Bei einem solchen Fehler empfängt der Root-Switch Frames, die von anderen Switches gesendet werden, die anderen Switches empfangen jedoch nicht die BPDUs, die der Root-Switch sendet. Dies kann zu einer STP-Schleife führen. Da die anderen Switches keine BPDUs vom Root empfangen, sind diese Switches der Meinung, dass sie der Root sind, und senden BPDUs.

Wenn die echte Root-Bridge BPDUs zu empfangen beginnt, verwirft die Root die BPDUs, da sie nicht höherwertig sind. Die Root-Bridge bleibt unverändert. Daher hilft Root Guard nicht, dieses Problem zu lösen. Die Funktionen UniDirectional Link Detection (UDLD) und Loop Guard beheben dieses Problem.

Weitere Informationen zu STP-Fehlerszenarien und zur Fehlerbehebung finden Sie unter Probleme mit dem Spanning Tree Protocol und damit zusammenhängende Designüberlegungen.

Zugehörige Informationen

- Verstehen und Konfigurieren der UDLD-Protokollfunktion
- Wiederherstellen Errdisable Port State auf Cisco IOS-Plattformen
- Technischer Support und Downloads von Cisco

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.