Häufige Probleme bei Spanning Tree-Protokollen der Serie ASR 9000

Inhalt

Einleitung

In diesem Dokument werden häufige Probleme beschrieben, die bei der Integration Ihrer aktuellen Layer 2 (L2) Spanning Tree-Netzwerke in Cisco IOS®-Switches mit Cisco Aggregation Services Router (ASR) der Serie 9000, auf denen Cisco IOS XR ausgeführt wird, auftreten.

Problem - PVID-Inkonsistenz (Port VLAN ID)

Cisco IOS-Switches, die Per VLAN Spanning Tree Plus (PVST+) ausführen, blockieren Switch-Ports, wenn sie eine Bridge Protocol Data Unit (BPDU) mit einer inkonsistenten PVID erhalten. Dieses Problem tritt auf, wenn ein Gerät zwischen den Switches die IEEE 802.1Q-Tags auf den PVST+-BPDUs ändert oder übersetzt.

Wenn ein ASR 9000 einen L2VPN-Point-to-Point- oder Multipoint-Service zwischen Switches bereitstellt, die PVST+ ausführen und die VLAN-Tags neu schreiben, werden die folgenden Syslog-Meldungen möglicherweise auf den Cisco IOS-basierten Switches angezeigt:

```
%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent
peer vlan id 10 on GigabitEthernet0/10 VLAN20.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking GigabitEthernet0/10
on VLAN20. Inconsistent local vlan.
```

Dieses Problem ist auf das PVID-Tag zurückzuführen, das zu den PVST+-BPDUs gehört. Dieses Tag wurde entwickelt, um Fehlkonfigurationen zu erkennen und unbeabsichtigte Schleifen zu

vermeiden. In diesem Szenario wird jedoch jedes Ende blockiert, und der Datenverkehr wird nicht weitergeleitet.

Hier ein Beispiel:

Nachfolgend finden Sie die Konfiguration für die Serie ASR 9000 (a9k1):

```
2vpn
bridge group bg1
bridge-domain bd1
interface TenGigE0/0/0/0.10
!
interface TenGigE0/0/0/1.20

interface TenGigE0/0/0/0.10 l2transport
encapsulation dot1q 10
rewrite ingress tag pop 1 symmetric

interface TenGigE0/0/0/1.20 l2transport
encapsulation dot1q 20
rewrite ingress tag pop 1 symmetric
```

Lösung

Um dieses Problem zu vermeiden, können Sie die PVST+-BPDUs blockieren. Diese Aktion deaktiviert Spanning Tree und kann zu Schleifen führen, wenn redundante Verbindungen zwischen den Switches verfügbar sind.

> **Achtung:** Seien Sie vorsichtig, wenn Sie BPDUs blockieren und Spanning Tree effektiv deaktivieren.

BPDU-Filter für Switches

Die BPDUs werden mithilfe der BPDU-Filterfunktion auf den Switches blockiert. Der BPDU-Filter blockiert BPDUs in beide Richtungen, wodurch Spanning Tree auf dem Port effektiv deaktiviert wird. Der BPDU-Filter verhindert ein- und ausgehende BPDUs. Wenn Sie die BPDU-Filterung für eine Schnittstelle aktivieren, ist dies dasselbe wie beim Deaktivieren von Spanning Tree für diese Schnittstelle, was zu Spanning Tree-Schleifen führen kann.

Aktivieren Sie auf Switch1 und Switch2 mit dem folgenden Befehl BPDU-Filter:

```
interface TenGigabitEthernet1/2
spanning-tree bpdufilter enable
```

Sperren von PVST+-BPDUs auf dem ASR 9000

Dieses Problem wird vermieden, wenn Sie den ASR9000 so konfigurieren, dass die PVST+-BPDUs verworfen werden. Dies geschieht mithilfe einer L2-Ethernet-Services-Zugriffsliste, um Pakete abzulehnen, die an die PVST+-BPDU-MAC-Adresse gerichtet sind.

PVST+-BPDUs für das nicht-VLAN 1 (nicht nativ) werden an die PVST+-MAC-Adresse (auch als Shared Spanning Tree Protocol [SSTP]-MAC-Adresse 0100.0ccc.cccd bezeichnet) gesendet und mit einem entsprechenden IEEE 802.1Q-VLAN-Tag versehen.

Diese Zugriffskontrollliste (ACL) kann verwendet werden, um die PVST+-BPDUs zu blockieren:

```
ethernet-services access-list l2acl
10 deny any host 0100.0ccc.cccd
 20 permit any any
```

Wenden Sie die ACL auf die Schnittstelle an, die als l2transport konfiguriert ist:

```
interface TenGigE0/0/0/0.10 l2transport
encapsulation dot1q 10
rewrite ingress tag pop 1 symmetric
ethernet-services access-group l2acl ingress

interface TenGigE0/0/0/1.20 l2transport
encapsulation dot1q 20
rewrite ingress tag pop 1 symmetric
ethernet-services access-group l2acl ingress
```

Problem - Switch-Ports flattern zwischen Blockierung und Weiterleitung, wenn Sie mehrere Typen von Spanning Tree Protocols (STPs) über einen ASR 9000 verwenden.

Der ASR9000 verwendet standardmäßig kein Spanning Tree, wie dies bei den meisten Cisco IOS-Switches der Fall ist. Beim Ethernet Virtual Circuit (EVC)-Modell ist eine BPDU einfach ein anderes L2-Multicast-Paket. Ein häufig auftretendes Problem sind Spanning-Tree-Inkonsistenzen aufgrund verschiedener STP-Typen, die über eine ASR 9000-Bridge-Domäne ausgeführt werden. Dies geschieht auf verschiedene Weise.

Betrachten Sie diese einfache Topologie:

Angenommen, auf Switch1 wird Multiple Spanning Tree (MST) und auf Switch2 PVST+ ausgeführt. Wenn auf a9k1 keine Form von Spanning Tree ausgeführt wird, sieht Switch1 dies als Begrenzungsport. Switch1 wechselt für VLANs, die sich nicht in Common Spanning Tree Instance 0 (CST0) befinden, wieder in den PVST-Modus. Wenn dies das gewünschte Design ist, sollten Sie mit der MST- und PVST-Interaktion vertraut sein, wie im Whitepaper Understanding Multiple Spanning Tree Protocol (802.1s) beschrieben.

Angenommen, Sie führen MST auf Switch1 und auf der Schnittstelle a9k1 aus, die zu Switch1 führt, aber Sie führen weiterhin PVST+ auf Switch2 aus. Die PVST+-BPDUs passieren die Bridge-Domäne und erreichen Switch1. Switch1 erkennt dann sowohl MST-BPDUs von a9k1 als auch die PVST+-BPDUs von Switch2, was dazu führt, dass Spanning Tree auf dem Switch1-Port ständig nicht blockiert, sondern nicht blockiert wird, was zu Datenverkehrsverlusten führt.

Switch1 meldet diese Syslogs:

```
%SPANTREE-SP-2-PVSTSIM_FAIL: Superior PVST BPDU received on VLAN 2 port Gi2/13,
claiming root 2:000b.45b7.1100. Invoking root guard to block the port
%SPANTREE-SP-2-ROOTGUARD_BLOCK: Root guard blocking port GigabitEthernet2/13
on MST1.
%SPANTREE-SP-2-ROOTGUARD_UNBLOCK: Root guard unblocking port GigabitEthernet2/13
on MST0.
%SPANTREE-SP-2-PVSTSIM_FAIL: Superior PVST BPDU received on VLAN 2 port Gi2/13,
claiming root 2:000b.45b7.1100. Invoking root guard to block the port
%SPANTREE-SP-2-ROOTGUARD_BLOCK: Root guard blocking port GigabitEthernet2/13
on MST1.
```

Die Ausgabe des Befehls **show spanning-tree interface** zeigt, dass sich die Ausgabe auf dem Cisco IOS-Gerät switch1 ständig ändert:

```
show spanning-tree interface gig 2/13
Mst Instance Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- -------
MST0 Desg BKN*20000 128.269 P2p Bound(PVST) *ROOT_Inc
MST1 Desg BKN*20000 128.269 P2p Bound(PVST) *ROOT_Inc
MST2 Desg BKN*20000 128.269 P2p Bound(PVST) *ROOT_Inc

show spanning-tree interface gig 2/13
Mst Instance Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- ---------
MST0 Desg FWD 20000 128.269 P2p
MST1 Desg FWD 20000 128.269 P2p
MST2 Desg FWD 20000 128.269 P2p
```

Lösung

Es gibt drei Optionen zu prüfen, um dieses Problem zu verhindern.

- Konfigurieren Sie MST auf Switch2, und aktivieren Sie MST auf den a9k1-Schnittstellen für Switch1 und Switch2.
- Verwenden Sie eine Ethernet-Services-Zugriffsliste auf Switch9k1, um die PVST+-BPDUs entweder beim Eingang von Switch2 oder beim Ausgang von Switch1 zu verwerfen.
- Führen Sie Per VLAN Spanning Tree Access Gateway (PVSTAG) an der Schnittstelle 9001 zu Switch 2 aus. Dadurch verbraucht a9k1 die PVST+-BPDUs von Switch2.

Problem - Spanning-Tree-Ports aufgrund der Erkennung einer Selbst-Schleife blockiert

Wenn ein Switch eine Spanning Tree-BPDU empfängt, die er über dieselbe Schnittstelle gesendet hat, blockiert er dieses VLAN aufgrund einer Self-Loop-Verbindung. Dies ist ein häufiges Problem, das auftritt, wenn ein Switch mit einem Trunk-Port mit einem ASR 9000-Router verbunden ist, der

L2-Multipoint-Dienste bereitstellt, und der ASR 9000 VLAN-Tags an den l2transport-Schnittstellen in derselben Bridge-Domäne nicht umschreibt.

Betrachten wir dieselbe einfache Topologie wie zuvor. Aus Designgründen werden nun auf dem a9k1 mehrere VLANs, die von derselben Switch-Trunk-Schnittstelle kommen, in einer Bridge-Domäne zusammengeführt.

Dies ist die a9k1-Konfiguration:

```
l2vpn
bridge group bg1
bridge-domain bd1
interface GigabitEthernet0/1/0/31.2
!
interface GigabitEthernet0/1/0/31.3
!
interface GigabitEthernet0/1/0/31.4
!
interface GigabitEthernet0/1/0/32.2
!
interface GigabitEthernet0/1/0/32.3
!
interface GigabitEthernet0/1/0/32.4

interface GigabitEthernet0/1/0/31.2 l2transport
encapsulation dot1q 2
!
interface GigabitEthernet0/1/0/31.3 l2transport
encapsulation dot1q 3
!
interface GigabitEthernet0/1/0/31.4 l2transport
encapsulation dot1q 4
```

Dadurch werden die VLANs 2 bis 4 in einer Bridge-Domäne auf a9k1 miteinander verbunden.

Beim EVC-Modell der ASR Serie 9000 werden standardmäßig keine Tags oder Pop-Tags umgeschrieben. Die PVST+-BPDU für **VLAN2** wird mit Interface **Gig 0/1/0/31.2** geliefert und nach **Gig 0/1/0/31.3** und **Gig 0/1/0/31.4** zurückgeleitet. Da es sich bei der Konfiguration nicht um ein Umschreiben einer eingehenden Popup-Aktion handelt, wird die BPDU unverändert zurückgegeben. Der Switch erkennt dies, wenn er seine eigene BPDU zurückerhält, und blockiert dieses VLAN aufgrund einer Self-Loop-Verbindung.

Der Befehl **show spanning-tree interface** gibt an, dass das VLAN blockiert ist:

```
6504-A#show spanning-tree interface gig 2/13

Vlan Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- --------
VLAN0002 Desg BLK 4 128.269 self-looped P2p
VLAN0003 Desg BLK 4 128.269 self-looped P2p
```

```
VLAN0004 Desg BLK 4 128.269 self-looped P2p
```

Lösung

Dieses Problem wird durch die Verwendung des Befehls **ethernet egress-filter strict** an den ASR 9000 l2-Transportschnittstellen behoben.

Dies ist kein empfohlenes Design. Wenn dies jedoch wirklich das gewünschte Design ist, können Sie diese Lösung verwenden, um zu verhindern, dass der Switch die BPDU erhält, die er über dieselbe Schnittstelle zurückgesendet hat.

Sie können den Befehl **ethernet egress-filter strict** auf den a9k1 l2transport-Schnittstellen oder global verwenden. Hier ist das Beispiel unter der Schnittstelle:

```
interface GigabitEthernet0/1/0/31.2 l2transport
encapsulation dot1q 2
ethernet egress-filter strict
!
interface GigabitEthernet0/1/0/31.3 l2transport
encapsulation dot1q 3
ethernet egress-filter strict
!
interface GigabitEthernet0/1/0/31.4 l2transport
encapsulation dot1q 4
ethernet egress-filter strict
```

Der Befehl **ethernet egress-filter strict** ermöglicht die strikte EFP-Filterung (Egress Ethernet Flow Point) an der Schnittstelle. Nur Pakete, die den Eingangs-EFP-Filter der Schnittstelle passieren, werden von dieser Schnittstelle übertragen. Andere Pakete werden am Ausgangsfilter verworfen. Das bedeutet, dass das ausgetretene Paket nicht an das auf der Schnittstelle konfigurierte Kapselungs-**dot1q-**Label gesendet wird, wenn es nicht mit diesem übereinstimmt.

Zugehörige Informationen

- Implementieren des Multiple Spanning Tree Protocol
- Fehlerbehebung bei PVID- und Typ-Inkonsistenzen in Spanning Tree
- Grundlegendes zum Spanning Tree Protocol (802.1s)
- 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.