Fehlerbehebung für Layer-2-Loops

Inhalt

Einleitung

In diesem Dokument werden Informationen beschrieben, die bei der Identifizierung der Quelle von Layer-2-Schleifen helfen und Schutzmaßnahmen zu deren Verhinderung in der Zukunft vorsehen.

Voraussetzungen

Es wird empfohlen, dass Sie Kenntnisse über STP-Konzepte haben.

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 kennen.

Verwendete Befehle

- show interfaces | include ist up|Eingaberate
- show cdp neighbors <Schnittstelle>
- show spanning-tree
- show logging

Theorie der Fehlerbehebung

Unabhängig von der Topologie und vom Ausgangspunkt (dem Switch, mit dem Sie zuerst verbunden sind) ist der Ansatz zum Verfolgen der Problemursache identisch.

Verwenden Sie den zuvor bereitgestellten Befehl show interface. Wir konzentrieren uns auf die Schnittstelle oder Schnittstellen mit hohen Eingangsraten.

Hohe Produktionsraten sind ein Symptom,... keine Ursache.

Wenn die Schnittstellen mit hoher Eingangsrate identifiziert werden, verwenden Sie einen CDP-Nachbarn, um die Verbindungen für angeschlossene Switches zu überprüfen. Wenn Sie einen Host-Port finden, versuchen Sie, den Port herunterzufahren, um das Problem zu beheben.

Wenn Sie Switches mit zwei verbundenen Verbindungen verwenden, bestätigen Sie mithilfe der Spanning Tree-Befehle den Blockierungs- und Weiterleitungsstatus. Dies hilft bei der Identifizierung eines defekten Ports/Switches.

Topology Change Notifications (TCN) (Benachrichtigungen zu Topologieänderungen (TCN)): Diese werden bei der Arbeit an Loops ignoriert.

Ältere Switches verfügen nicht über COPP oder können die BPDU-Verarbeitung nicht verarbeiten, was zu zufälligen TCNs führt.

Wenn Sie den Port finden, von dem Sie glauben, dass er das Problem darstellt, schalten Sie ihn aus, und warten Sie mindestens 30 Sekunden. Wenn das Problem dadurch nicht behoben wird, fahren Sie fort und schließen Sie diese Schnittstelle noch nicht.

Anwendung

```
DistroSwitch#show interfaces | include is up|input rate
GigabitEthernet1/0/1 is up, line protocol is up
 5 minute input rate 1482600 bits/sec, 2739 packets/sec
GigabitEthernet1/0/2 is up, line protocol is up
 5 minute input rate 291658000 bits/sec, 366176 packets/sec <------------
TenGigabitEthernet1/1/1 is up, line protocol is up
 5 minute input rate 1339000 bits/sec, 2614 packets/sec
```

```
DistroSwitch#show cdp neighbors gigabitEthernet 1/0/1
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
 S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
 D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID Local Intrfce Holdtme Capability Platform Port ID
access Gig 1/0/2 158 S I C9300-48P Gig 2/0/2 <-----------------
```

<#root>

DistroSwitch#show logging

```
*May 3 18:33:45.885: %SW_MATM-4-MACFLAP_NOTIF: Host 0cd0.f8dc.dc47 in vlan 1 is flapping between port G
*May 3 18:33:58.841: %SW_MATM-4-MACFLAP_NOTIF: Host 0cd0.f8dc.dc47 in vlan 1 is flapping between port T
*May 3 18:34:13.842: %SW_MATM-4-MACFLAP_NOTIF: Host 0cd0.f8dc.dc47 in vlan 1 is flapping between port G
*May 3 18:34:28.839: %SW_MATM-4-MACFLAP_NOTIF: Host 0cd0.f8dc.dc47 in vlan 1 is flapping between port T
*May 3 18:34:43.840: %SW_MATM-4-MACFLAP_NOTIF: Host 0cd0.f8dc.dc47 in vlan 1 is flapping between port T
*May 3 18:34:58.839: %SW_MATM-4-MACFLAP_NOTIF: Host 0cd0.f8dc.dc47 in vlan 1 is flapping between port T
```

```
access#show spanning-tree vlan 1
Spanning tree instance(s) for vlan 1 does not exist.
```

Prävention

STP - Best Practices

BPDU Guard: deaktiviert Schnittstellen, wenn sie BPDU Guard erhalten, anstatt es weiterzuleiten.

Root Guard - In der Regel für Distro-Geräte, die auf den Access Switch zeigen - Auf der Schnittstelle, auf die dies angewendet wird, wird niemals eine übergeordnete BPDU oder eine untergeordnete BPDU angezeigt.

Loop Guard - Normalerweise für alle Switches weltweit - Wenn ein Switch eine BPDU auf einer Schnittstelle empfängt, überwacht er diese Schnittstelle, um zu überprüfen, ob er alle

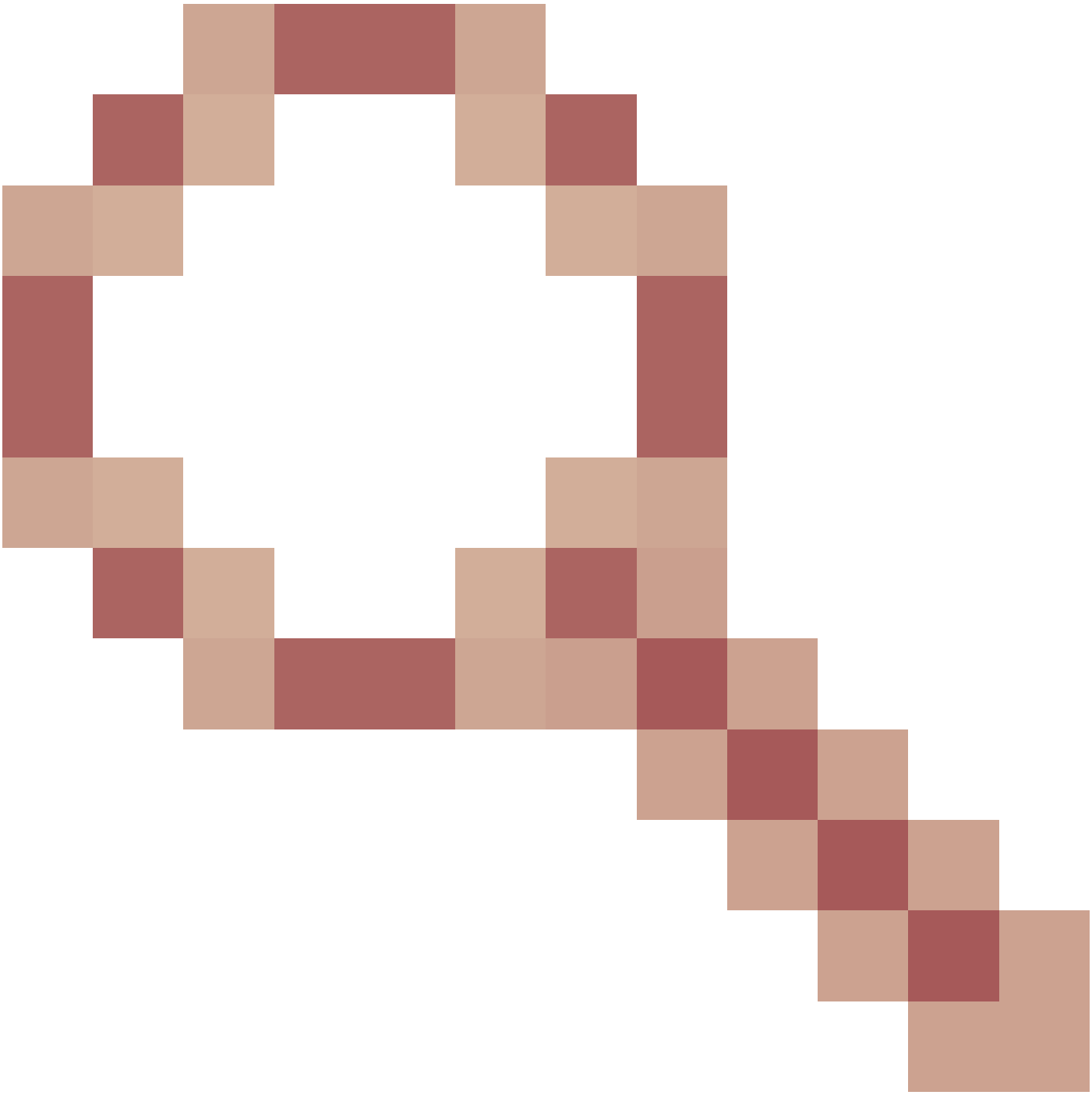
2 Sekunden danach. Wenn nicht, wird die Loop-Inkonsistenz erreicht.

BPDU-Filter - Deaktiviert STP. BPDUs werden nach Eingang weder gesendet noch verarbeitet. Gängig von Service Providern, nicht unbedingt Enterprise Networks

EMPFEHLEN SIE NICHT ALLE STP-FUNKTIONEN - z. B. "bpdufilter" triumphiert über "bpduguard"

UDLD aggressiv

Sturmkontrolle - festgelegt auf 1 % (nicht höher oder niedriger) - Cisco Bug IDCSCvt85758



CoPP und QoS für bestimmte Szenarien sind nützlich, aber nicht gängig.

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.