Fehlerbehebung bei MAC Flaps/Loop auf Cisco Catalyst Switches

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung bei MAC Flaps/Loop auf Cisco Catalyst Switches beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über grundlegende Kenntnisse der Switching-Konzepte verfügen und mit dem Spanning Tree Protocol (STP) und seinen Funktionen auf Cisco Catalyst-Switches vertraut sind.

Verwendete Komponenten

Die in diesem Dokument enthaltenen Informationen basieren auf Cisco Catalyst Switches mit allen Versionen (dieses Dokument ist nicht auf bestimmte Software- oder Hardwareversionen 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.

Hintergrundinformationen

Dieses Dokument dient als Leitfaden zur systematischen Behebung von MAC-Flaps oder Schleifenproblemen bei Cisco Catalyst-Switches. MAC-Flaps/Loops sind Störungen in einem Netzwerk, die durch Inkonsistenzen in den MAC-Adresstabellen von Switches verursacht werden. Dieses Dokument enthält nicht nur Schritte zur Identifizierung und Lösung dieser Probleme, sondern auch praktische Beispiele für ein besseres Verständnis.

Was ist MAC Flapping?

Eine MAC-Klappe tritt auf, wenn ein Switch einen Frame mit der gleichen MAC-Quelladresse, jedoch von einer anderen Schnittstelle empfängt als der, von dem er ihn ursprünglich empfangen hat. Dadurch wechselt der Switch zwischen den Ports und aktualisiert seine MAC-Adresstabelle mit der neuen Schnittstelle. Diese Situation kann zu Instabilitäten im Netzwerk und Leistungsproblemen führen.

Bei einem Cisco Switch wird das MAC-Flapping in der Regel wie folgt protokolliert:

```
"%SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan x is flapping between port (1) and port (2)"
```

In diesem Beispiel wurde die MAC-Adresse`xxxx.xxxx.xxxx`zuerst an Schnittstellenport (1) ermittelt und dann an Schnittstellenport (2) erkannt, wodurch ein MAC-Flapping auftrat.

Die häufigste Ursache für MAC-Flapping ist eine Layer-2-Schleife im Netzwerk, die häufig auf eine fehlerhafte STP-Konfiguration oder auf Probleme mit redundanten Verbindungen zurückzuführen ist. Andere Ursachen können fehlerhafte Hardware, Softwarefehler oder sogar Sicherheitsprobleme wie MAC-Spoofing sein.

Die Fehlerbehebung bei MAC-Flaps umfasst häufig das Identifizieren und Beheben von Schleifen im Netzwerk, das Überprüfen von Gerätekonfigurationen oder das Aktualisieren der Firmware/Software der Geräte.

Allgemeine Richtlinien zur Fehlerbehebung

- Identifizieren des MAC-Flapping: Suchen Sie nach Protokollen in Ihrem Switch, die ein MAC-

Flapping anzeigen. Bei einem Cisco Switch sieht die Protokollmeldung beispielsweise wie folgt aus:

```
%SW_MATM-4-MACFLAP_NOTIF: Host [mac_address] in vlan [vlan_id] is flapping between port [port_id_
```

- Beachten Sie die MAC-Adresse und die Schnittstellen: Die Protokollmeldung gibt die MAC-Adresse an, bei der Flapping auftritt, und die Schnittstellen, zwischen denen Flapping auftritt. Notieren Sie sich diese, da sie Ihnen bei Ihren Nachforschungen helfen.
- Affected Interfaces (Betroffene Schnittstellen) untersuchen: Verwenden Sie die CLI des Switches, um die beteiligten Schnittstellen zu untersuchen. Mithilfe von Befehlen wie`show interfaces`oder können Sie`show mac address-table`sehen, welche Geräte mit den Schnittstellen verbunden sind und wo die MAC-Adresse abgefragt wird.
- Trace the Flapping MAC Address (Flapping-MAC-Adresse): MAC lernt über die Ports X und Y. Ein Port führt uns zu dem Punkt, an dem diese MAC angeschlossen ist, und der andere führt uns zum Loop. `show mac address-table`Wählen Sie einen Port aus, und beginnen Sie mit der Ausführung des Befehls für jeden Layer-2-Switch im Pfad.
- Auf physische Schleifen prüfen: Überprüfen Sie Ihre Netzwerktopologie, um festzustellen, ob es physische Schleifen gibt. Diese können auftreten, wenn mehrere Pfade zwischen Switches vorhanden sind. Wenn eine Schleife gefunden wird, müssen Sie Ihr Netzwerk neu konfigurieren, um die Schleife zu entfernen.
- STP überprüfen: STP wurde entwickelt, um Schleifen in Ihrem Netzwerk zu verhindern, indem bestimmte Pfade blockiert werden. Wenn das STP falsch konfiguriert ist, werden Schleifen nicht wie gewünscht verhindert. Verwenden Sie Befehle wie`show spanning-tree`, um die STP-Konfiguration zu überprüfen. Überprüfen Sie außerdem mithilfe des Befehls`show spanning-tree detail | include ieee|occur|from|is`auf Benachrichtigungen zu Topologieänderungen (TCNs).
- Prüfen Sie, ob doppelte MAC-Adressen vorhanden sind: Wenn zwei Geräte im Netzwerk über dieselbe MAC-Adresse verfügen (was meistens in der Hochverfügbarkeits-Konfiguration und bei mehreren Netzwerkschnittstellen-Controllern bzw. Netzwerkkarten (NICs) der Fall ist), kann dies zu MAC-Flapping führen. Verwenden Sie den`show mac address-table`Befehl, um nach doppelten MAC-Adressen in Ihrem Netzwerk zu suchen.
- Überprüfen Sie, ob Hardware oder Kabel defekt sind: Defekte Netzwerkkabel oder Hardware kann dazu führen, dass Frames an die falschen Schnittstellen gesendet werden, was zu MAC-Flapping führt. Überprüfen Sie den physischen Zustand der Kabel, und ziehen Sie einen Hardwareaustausch in Betracht, um festzustellen, ob das Problem weiterhin besteht. Schnittstellen-Flapping kann auch MAC-Flapping auf Switches verursachen.
- Suchen Sie nach Software-Bugs: Manchmal kann MAC-Flapping durch Fehler in der Software Ihrer Netzwerkgeräte verursacht werden. Suchen Sie im Bug-Such-Tool nach.

Bug Search Tool: https://bst.cloudapps.cisco.com/bugsearch

Hilfe zum Bug Search Tool:
https://www.cisco.com/c/en/us/support/web/tools/bst/bsthelp/index.html#search

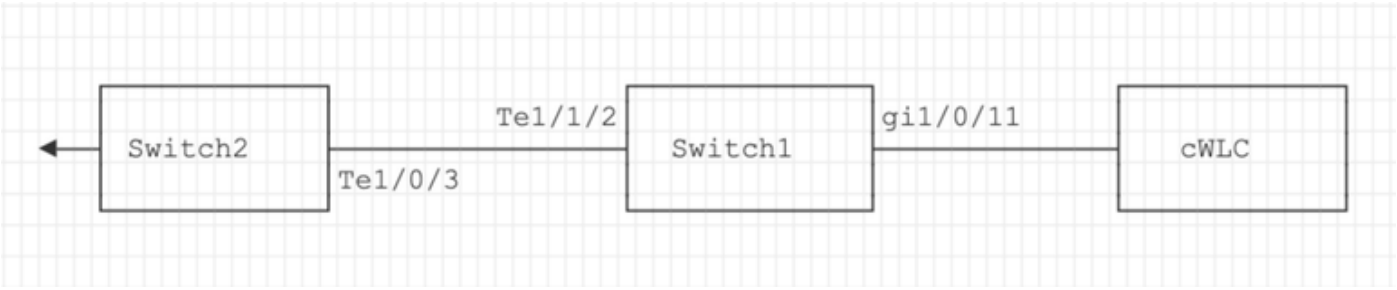
- TAC-Support kontaktieren: Wenn Sie alles versucht haben und das Problem weiterhin besteht, können Sie sich an den Cisco TAC-Support wenden. Sie können weitere Hilfe leisten.

Anwenderbericht 1

Problembeschreibung

Beim eWLC-Controller besteht ein Verbindungsverlust zum Gateway, und durch Paketverluste wird verhindert, dass APs dem Controller beitreten.

Topologie



Schritte zur Fehlerbehebung

MAC-Flapping wurde auf dem Switch (Switch1) erkannt, der mit dem eWLC verbunden ist.

```
*Aug  5 05:52:50.750: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
*Aug  5 05:53:03.327: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
*Aug  5 05:53:21.466: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
```

MAC-Schulung:

Geben Sie den Befehl`show mac address-table address`
ein, um die vom Port bezogene MAC-Adresse zu überprüfen.

<#root>

```
Switch1#show mac address-table address 0000.5e00.0101

          Mac Address Table
-------------------------------------------
```

```
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   4    0000.5e00.0101    DYNAMIC     Gi1/0/11


   4    0000.5e00.0101    DYNAMIC     Te1/1/2
```

Konfiguration der Ports Gi1/0/11 und Te1/1/2:

Geben Sie den Befehlshow running-config interface
ein, um die Schnittstellenkonfiguration zu überprüfen.

<#root>

```
interface GigabitEthernet1/0/11


 switchport trunk native vlan 4
 switchport mode trunk
end


interface TenGigabitEthernet1/1/2


 switchport mode trunk
end
```

CDP-Nachbarn der Ports Gi1/0/11 und Te1/1/2:

Geben Sie den Befehlshow cdp neighbors
ein, um die Details der verbundenen Geräte zu überprüfen.

<#root>

```
Switch1#show cdp neighbors gi1/0/11


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

eWLC            Gig 1/0/11        130              R T   C9115AXI- Gig 0 < ----- eWLC Controller



Switch1#show cdp neighbors gi1/1/2


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
```

Switch2

Ten 1/1/2 163 R S I C9500-16X Ten 1/0/3 < ----- Uplink Switch

MAC Learning auf Switch2 (Uplink-Switch):

Geben Sie den Befehlshow mac address-table address
ein, um die vom Port bezogene MAC-Adresse zu überprüfen.

<#root>

Switch2#show mac address-table address 0000.5E00.0101

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   4    0000.5e00.0101    STATIC
```

Vl4 < ----- VRRP MAC of Vlan4

```
   4    0000.5e00.0101    DYNAMIC
```

Te1/0/13 < ----- Learning from Switch1 (eWLC connected Switch)

<#root>

Switch2#show vrrp vlan 4

Vlan4 - Group 1

```
 - Address-Family IPv4
  State is MASTER
  State duration 5 days 4 hours 22 mins
  Virtual IP address is x.x.x.x
```

Virtual MAC address is 0000.5E00.0101 < ------ VRRP MAC of Vlan4

```
  Advertisement interval is 1000 msec
```

Ursache

Es wurde überprüft, ob die VRRP-ID (Virtual Router Redundancy Protocol) von Switch 2 und der eWLC identisch waren, was zur Generierung derselben virtuellen MAC durch den VRRP führte.

Auflösung

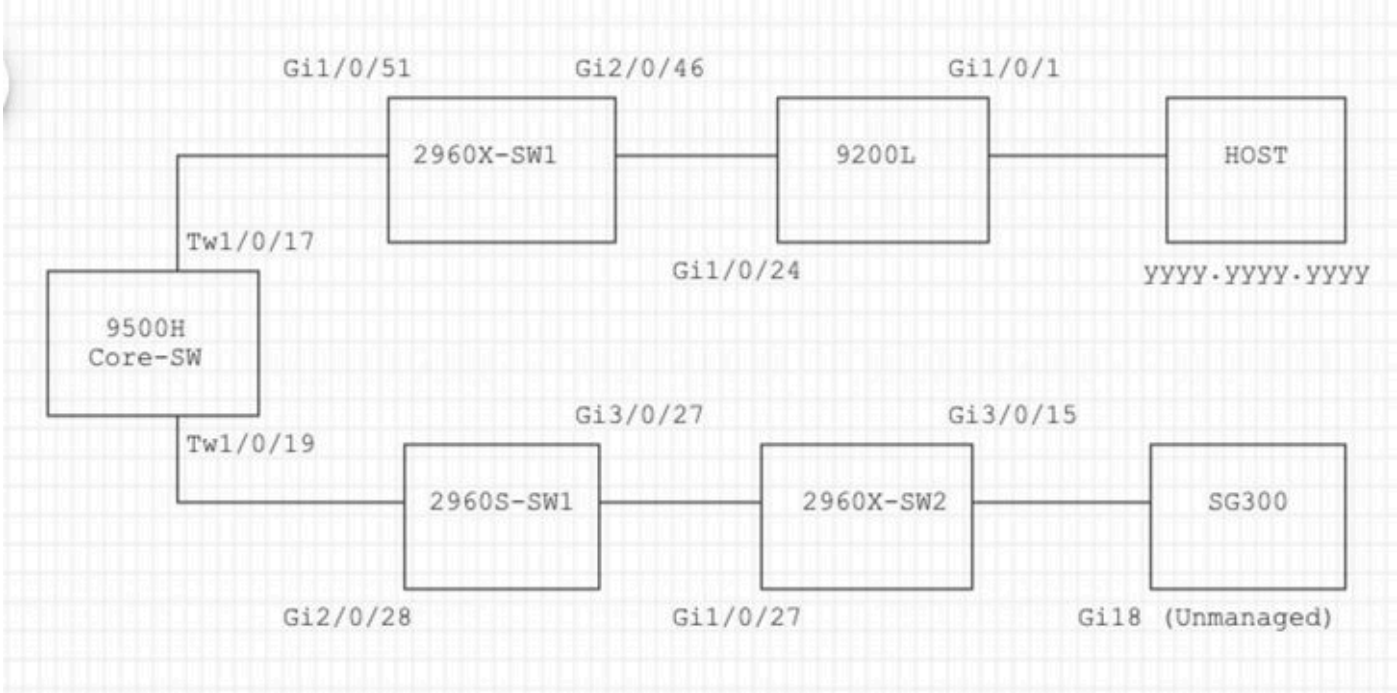
Das Problem wurde behoben, nachdem die VRRP-Instanz auf dem WLC geändert wurde. Dies verursachte ein Duplikat der MAC-Adresse auf dem Switch, das zu einem Verbindungsverlust mit dem Gateway und Paketverlusten führte, wodurch verhindert wurde, dass die APs dem Controller beitreten konnten.

Anwenderbericht 2

Problembeschreibung

Einige Server sind entweder nicht zugänglich oder es kommt zu erheblichen Latenzen/Verlusten.

Topologie



Schritte zur Fehlerbehebung

1. Auf dem Core-Switch tritt ein MAC-Flapping auf.

```
Nov 14 08:36:34.637: %SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan 1 is flapping between port Tw
Nov 14 08:36:34.838: %SW_MATM-4-MACFLAP_NOTIF: Host yyyy.yyyy.yyyy in vlan 1 is flapping between port Tw
Nov 14 08:36:34.882: %SW_MATM-4-MACFLAP_NOTIF: Host zzzz.zzzz.zzzz in vlan 1 is flapping between port Po
```

2. Wählen Sie die MAC-Adresse`yyyy.yyyy.yyyy`für die Fehlerbehebung aus.

MAC-Schulung:

Geben Sie den Befehl`show mac address-table address`
ein, um die vom Port bezogene MAC-Adresse zu überprüfen.

<#root>

```
Core-SW#show mac address-table address yyyy.yyyy.yyyy


          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy    DYNAMIC     Twe1/0/17
```

CDP-Nachbarn der Ports Twe 1/0/17 und Twe 1/0/17:

Geben Sie den Befehl`show cdp neighbors`
ein, um die Details der verbundenen Geräte zu überprüfen.

<#root>

```
Core-SW#show cdp neighbors Twe 1/0/17


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

2960X-SW1


                 Twe 1/0/17        162              S I   WS-C2960X Gig 1/0/51



Core-SW#show cdp neighbors Twe 1/0/19


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

2960S-SW1


                 Twe 1/0/19        120              S I   WS-C2960S Gig 2/0/28
```

Protokolle von 2960X-SW1 verbunden mit Core-SW Twe1/0/17:

MAC$_{yyyy.yyyy.yyyy}$flattert zwischen Port Gi1/0/51 und Gi2/0/46 (9200L).

<#root>

```
2960X-SW1#show mac address-table address yyyy.yyyy.yyyy


          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy    DYNAMIC     Gi1/0/51



2960X-SW1#show mac address-table address yyyy.yyyy.yyyy


          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy DYNAMIC     Gi2/0/46



2960X-SW1#show run interface gi 1/0/51


Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet1/0/51
switchport mode trunk
end


2960X-SW1#show run interface gi 2/0/46


Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet2/0/46
switchport mode trunk
end
```

Protokolle von 9200L:

(Dies scheint der gültige Port für diese MAC-Adresse zu sein.)

<#root>

```
9200L#show mac address-table address yyyy.yyyy.yyyy


          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy DYNAMIC     Gi1/0/1



9200L#show run interface gi 1/0/1


Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet1/0/1
switchport mode access
end
```

2960S-SW1 Angeschlossen an Core-SW Twe1/0/19:

(Scheint ein Schleifenpfad zu sein.) Der Port am Core-SW wurde heruntergefahren, um den Loop zu reduzieren.

Auf der Core-SW wurden jedoch weiterhin MAC-Flaps beobachtet.

Protokolle von 2960S-SW1:

<#root>

```
Nov 14 08:36:34.637: %SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan 1 is flapping between port G
Nov 14 08:36:34.838: %SW_MATM-4-MACFLAP_NOTIF: Host yyyy.yyyy.yyyy in vlan 1 is flapping between port G
Nov 14 08:36:34.882: %SW_MATM-4-MACFLAP_NOTIF: Host zzzz.zzzz.zzzz in vlan 1 is flapping between port G


2960S-SW1#show run interface gi 3/0/27


Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet3/0/27
switchport mode trunk
end


2960S-SW1#show cdp neighbor gi 3/0/27


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
```

```
2960X-SW2

                Gig 3/0/27        176              S I   WS-C2960X Gig 1/0/27
```

Protokolle von 2960X-SW2:

<#root>

```
2960X-SW2#show run interface gi 3/0/15


Building configuration...

Current configuration : 39 bytes
!
interface GigabitEthernet3/0/15
end


2960X-SW2#show cdp neighbor gi 3/0/15


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

SG300     Gig 3/0/15        157              S I   SG300-28P gi18




2960X-SW2#config terminal


2960X-SW2(config)#interface gi 3/0/15


2960X-SW2(config-if)#shutdown
```

Ursache

MAC-Flaps traten auf, nachdem der SG300-Switch (nicht verwaltet) mit dem Netzwerk verbunden war.

Auflösung

Das Flapping-Problem mit der MAC-Adresse wurde behoben, indem der mit dem Unmanaged Switch SG300 verbundene Port heruntergefahren wurde.

Prävention

STP-PortFast:

STP PortFast veranlasst einen Layer-2-LAN-Port, sofort in den Weiterleitungsstatus zu wechseln, und umgeht dabei den Status "Zuhören" und "Lernen". STP PortFast verhindert die Generierung von STP-TCNs, die für Ports, die keine STP Bridge Protocol Data Units (BPDUs) empfangen, nicht sinnvoll sind. Konfigurieren Sie STP PortFast nur auf Ports, die mit End-Host-Geräten verbunden sind, die VLANs terminieren und von denen der Port niemals STP-BPDUs empfangen darf, z. B. Workstations, Server, Ports auf Routern, die nicht für die Unterstützung von Bridging konfiguriert sind.

BPDU Guard:

STP BPDU Guard ergänzt die Funktionen von STP PortFast. Auf STP PortFast-fähigen Ports schützt STP BPDU Guard Layer-2-Schleifen, die STP nicht bereitstellen kann, wenn STP PortFast aktiviert ist. STP BPDU Guard sperrt Ports, die BPDUs empfangen.

Root Guard

Root Guard verhindert, dass Ports zu STP-Root-Ports werden. Verwenden Sie STP Root Guard, um zu verhindern, dass ungeeignete Ports zu STP-Root-Ports werden. Ein Beispiel für einen ungeeigneten Port ist ein Port, der mit einem Gerät verbunden ist, das sich außerhalb der direkten Netzwerkadministrationskontrolle befindet.

Loop Guard:

Loop Guard ist eine proprietäre STP-Optimierung von Cisco. Loop Guard schützt Layer-2-Netzwerke vor Loops, die auftreten, wenn eine Ursache die normale Weiterleitung von BPDUs auf Point-to-Point-Verbindungen verhindert (z. B. eine Fehlfunktion der Netzwerkschnittstelle oder eine ausgelastete CPU). Loop Guard ergänzt den Schutz vor unidirektionalen Verbindungsausfällen durch Unidirectional Link Detection (UDLD). Loop Guard isoliert Ausfälle und ermöglicht die Konvergierung von STP in eine stabile Topologie, wobei die ausgefallene Komponente aus der STP-Topologie ausgeschlossen wird.

BPDU-Filter:

Dadurch wird STP deaktiviert. BPDUs werden nach Eingang weder gesendet noch verarbeitet. Dies ist bei Service Providern üblich, nicht unbedingt bei Unternehmensnetzwerken.

Aggressiver UDLD-Test:

Das proprietäre UDLD-Protokoll von Cisco überwacht die physische Konfiguration der Verbindungen zwischen Geräten und Ports, die UDLD unterstützen. UDLD erkennt unidirektionale Verbindungen. UDLD kann im normalen oder im aggressiven Modus betrieben werden. Im Normalmodus klassifiziert UDLD eine Verbindung als unidirektional, wenn die empfangenen UDLD-Pakete keine Informationen enthalten, die für das Nachbargerät richtig sind. Zusätzlich zur Funktionalität des UDLD im Normalmodus versetzt das UDLD im aggressiven Modus die Ports in

den Status "err-disabled" (deaktiviert), wenn die Beziehung zwischen zwei zuvor synchronisierten Nachbarn nicht wiederhergestellt werden kann.

Sturmkontrolle:

Traffic Storm Control ist in der Hardware implementiert und beeinträchtigt nicht die Gesamtleistung des Switches. In der Regel sind Endgeräte wie PCs und Server die Quelle für Broadcast-Datenverkehr, der unterdrückt werden kann. Um eine unnötige Verarbeitung von übermäßigem Broadcast-Datenverkehr zu vermeiden, aktivieren Sie die Traffic Storm Control für den Broadcast-Datenverkehr an den Access Ports, die mit den Endgeräten verbunden sind, und an den Ports, die mit den wichtigsten Netzwerkknoten verbunden sind.

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.