Fehlerbehebung: ACI Intra-Fabric Forwarding - zeitweilige Unterbrechungen

Inhalt

Einleitung

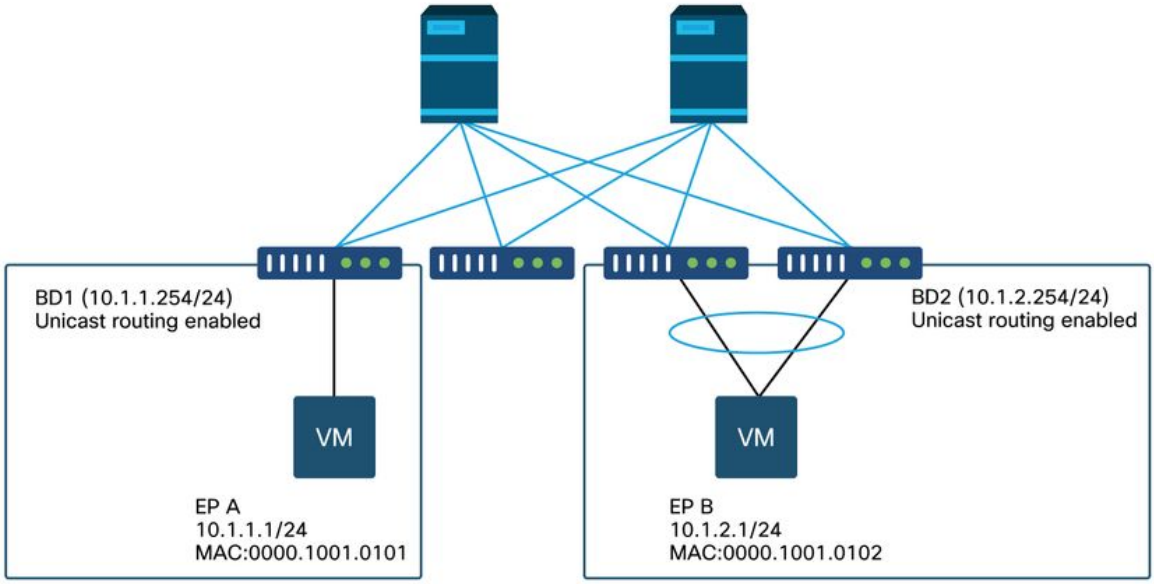
In diesem Dokument werden die Schritte zur Fehlerbehebung bei zeitweiligen Verlusten in der ACI beschrieben.

Hintergrundinformationen

Das Material aus diesem Dokument wurde aus dem Buch "Troubleshooting Cisco Application Centric Infrastructure, Second Edition" extrahiert, insbesondere aus dem Kapitel "**Intra-Fabric Forwarding - Intermittent Drops**".

Fehlerbehebung: ACI Intra-Fabric Forwarding - zeitweilige Unterbrechungen

Topologiebeispiel



In diesem Beispiel erfolgt der Ping-Vorgang von EP A (10.1.1.1) zu EP B (10.1.2.1) mit den intermittierenden Tropfen.

```
[EP-A ~]$ ping 10.1.2.1 -c 10
PING 10.1.2.1 (10.1.2.1) 56(84) bytes of data.
64 bytes from 10.1.2.1: icmp_seq=1 ttl=231 time=142 ms
64 bytes from 10.1.2.1: icmp_seq=2 ttl=231 time=141 ms
                                <-- missing icmp_seq=3

64 bytes from 10.1.2.1: icmp_seq=4 ttl=231 time=141 ms
64 bytes from 10.1.2.1: icmp_seq=5 ttl=231 time=141 ms
64 bytes from 10.1.2.1: icmp_seq=6 ttl=231 time=141 ms
                                 <-- missing icmp_seq=7

64 bytes from 10.1.2.1: icmp_seq=8 ttl=231 time=176 ms
```

```
64 bytes from 10.1.2.1: icmp_seq=9 ttl=231 time=141 ms
64 bytes from 10.1.2.1: icmp_seq=10 ttl=231 time=141 ms

--- 10.1.2.1 ping statistics ---
10 packets transmitted, 8 received, 20% packet loss, time 9012ms
```

Problembehebungs-Workflow

1. Bestimmen Sie, welche Richtung die intermittierenden Tropfen verursacht

Führen Sie eine Paketerfassung (tcpdump, Wireshark usw.) auf dem Zielhost (EP B) durch. Konzentrieren Sie sich bei ICMP auf die Sequenznummer, um zu sehen, dass die intermittierend verworfenen Pakete auf EP B beobachtet werden.

```
[admin@EP-B ~]$ tcpdump -ni eth0 icmp
11:32:26.540957 IP 10.1.1.1 > 10.1.2.1: ICMP echo request, id 3569, seq 1, length 64
11:32:26.681981 IP 10.1.2.1 > 10.1.1.1: ICMP echo reply, id 3569, seq 1, length 64
11:32:27.542175 IP 10.1.1.1 > 10.1.2.1: ICMP echo request, id 3569, seq 2, length 64
11:32:27.683078 IP 10.1.2.1 > 10.1.1.1: ICMP echo reply, id 3569, seq 2, length 64
11:32:28.543173 IP 10.1.1.1 > 10.1.2.1: ICMP echo request, id 3569, seq 3, length 64   <---
11:32:28.683851 IP 10.1.2.1 > 10.1.1.1: ICMP echo reply, id 3569, seq 3, length 64     <---
11:32:29.544931 IP 10.1.1.1 > 10.1.2.1: ICMP echo request, id 3569, seq 4, length 64
11:32:29.685783 IP 10.1.2.1 > 10.1.1.1: ICMP echo reply, id 3569, seq 4, length 64
11:32:30.546860 IP 10.1.1.1 > 10.1.2.1: ICMP echo request, id 3569, seq 5, length 64
...
```

- Muster 1 - Alle Pakete werden bei der EP B-Paketerfassung beobachtet.

Drops sollten in ICMP-Echoantwort (EP B bis EP A) erfolgen.

- Muster 2 - Bei der Paketerfassung mit EP B werden zeitweilige Verluste beobachtet.

Drops sollten das ICMP-Echo (EP A bis EP B) aufweisen.

2. Überprüfen Sie, ob bei einem anderen Protokoll mit derselben Quell-/Ziel-IP-Adresse das gleiche Problem auftritt.

Versuchen Sie, wenn möglich, die Verbindung zwischen den beiden Endpunkten mit einem anderen Protokoll zu testen, das der Vertrag zwischen den Endpunkten zulässt (z. B. ssh, telnet, http, ...).

- Muster 1 - Bei anderen Protokollen erfolgt die Ablage zeitweilig genauso.

Das Problem kann wie unten gezeigt beim Flapping des Endpunkts oder beim Queuing/Puffern auftreten.

- Muster 2 - Nur bei ICMP tritt der zeitweilige Abfall auf.

Die Weiterleitungstabellen (z. B. die Endpunkttabelle) sollten problemlos sein, da die Weiterleitung auf MAC und IP basiert. Warteschlangen/Pufferung sollten ebenfalls nicht der Grund sein, da sich dies auf andere Protokolle auswirken würde. Der einzige Grund, warum die ACI eine andere, protokollbasierte Weiterleitungsentscheidung treffen würde, ist der PBR-Anwendungsfall.

Eine Möglichkeit ist, dass einer der Spine-Knoten ein Problem hat. Wenn ein Protokoll anders ist, kann die Last des Pakets mit derselben Quelle und demselben Ziel durch den Eingangs-Leaf auf einen anderen Uplink/Fabric-Port (d. h. einen anderen Spine) verteilt werden.

Mit Atomic Counters kann sichergestellt werden, dass Pakete nicht auf Spine-Knoten verworfen

werden und bis zum Ausgangs-Leaf reichen. Falls die Pakete den Ausgangs-Leaf nicht erreichen, überprüfen Sie den ELAM auf dem Eingangs-Leaf, um festzustellen, welcher Fabric-Port die Pakete versendet. Um das Problem auf einen bestimmten Spine zu isolieren, können Leaf-Uplinks deaktiviert werden, um den Datenverkehr auf einen anderen Spine zu zwingen.

3. Überprüfen Sie, ob es mit einem Endpunkt-Lernproblem zusammenhängt.

Die ACI leitet Pakete von einem Endpunkt an einen anderen Endpunkt über eine Endpunkttabelle weiter. Ein vorübergehendes Erreichbarkeitsproblem kann durch Flapping des Endpunkts verursacht werden, da unangemessene Endpunktinformationen dazu führen, dass das Paket an ein falsches Ziel gesendet oder als Vertrag verworfen wird, der in die falsche EPG eingestuft wird. Auch wenn das Ziel ein L3Out anstelle einer Endpunktgruppe sein sollte, stellen Sie sicher, dass die IP nicht als Endpunkt in derselben VRF-Instanz über alle Leaf-Switches hinweg gelernt wird.

Weitere Informationen zur Fehlerbehebung beim Flapping von Endpunkten finden Sie im Unterabschnitt "Endpoint Flapping" in diesem Abschnitt.

4. Überprüfen Sie, ob es mit Pufferungsproblemen zusammenhängt, indem Sie die Verkehrsfrequenz ändern.

Vergrößern oder verkleinern Sie das Ping-Intervall, um festzustellen, ob sich das Abwurfverhältnis ändert. Der Intervallunterschied sollte groß genug sein.

In Linux kann die Option '-i' verwendet werden, um das Intervall (Sek.) zu ändern:

```
[EP-A ~]$ ping 10.1.2.1 -c 10 -i 5     -- Increase it to 5 sec
[EP-A ~]$ ping 10.1.2.1 -c 10 -i 0.2   -- Decrease it to 0.2 msec
```

Wenn sich die Verlustrate erhöht, wenn das Intervall verringert wird, ist dies wahrscheinlich auf Warteschlangen oder Pufferung auf Endpunkten oder Switches zurückzuführen.

Die zu berücksichtigende Verlustrate ist (Anzahl der Drops/insgesamt gesendete Pakete) anstelle von (Anzahl der Drops/Zeit).

In einem solchen Szenario sollten Sie Folgendes überprüfen.

1. Überprüfen Sie, ob die Zähler für das Zurücksetzen an den Switch-Schnittstellen mit dem Ping zunehmen. Weitere Informationen finden Sie im Abschnitt "Schnittstellenverluste" im Kapitel "Intra-Fabric-Weiterleitung".
2. Überprüfen Sie, ob der Rx-Zähler zusammen mit den Paketen am Zielendpunkt zunimmt. Wenn der Rx-Zähler um die gleiche Anzahl wie die übertragenen Pakete erhöht wird, werden Pakete wahrscheinlich auf dem Endpunkt selbst verworfen. Dies kann auf Endgerätepufferung im TCP/IP-Stack zurückzuführen sein.

Wenn beispielsweise 100000 Pings in einem möglichst kurzen Intervall gesendet werden, kann der Rx-Zähler am Endpunkt beobachtet werden, wenn er um 100000 erhöht wird.

```
[EP-B ~]$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 10.1.2.1  netmask 255.255.255.0  broadcast 10.1.2.255
      ether 00:00:10:01:01:02  txqueuelen 1000  (Ethernet)
      RX packets 101105  bytes 1829041
```

```
RX errors 0  dropped 18926930  overruns 0  frame 0
TX packets 2057  bytes 926192
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

5. Überprüfen Sie, ob die ACI die Pakete sendet oder das Ziel die Pakete empfängt.

Nehmen Sie eine SPAN-Erfassung am Ausgangsport des Leaf-Switches vor, um die ACI-Fabric aus dem Fehlerbehebungspfad zu entfernen.

Rx-Zähler am Ziel können ebenfalls nützlich sein, um den Fehlerbehebungspfad für alle Netzwerk-Switches zu deaktivieren, wie in den vorherigen Schritten für die Pufferung gezeigt.

Flapping

In diesem Abschnitt wird erläutert, wie Sie auf Endpunkt-Flapping prüfen. Weitere Informationen finden Sie in folgenden Dokumenten:

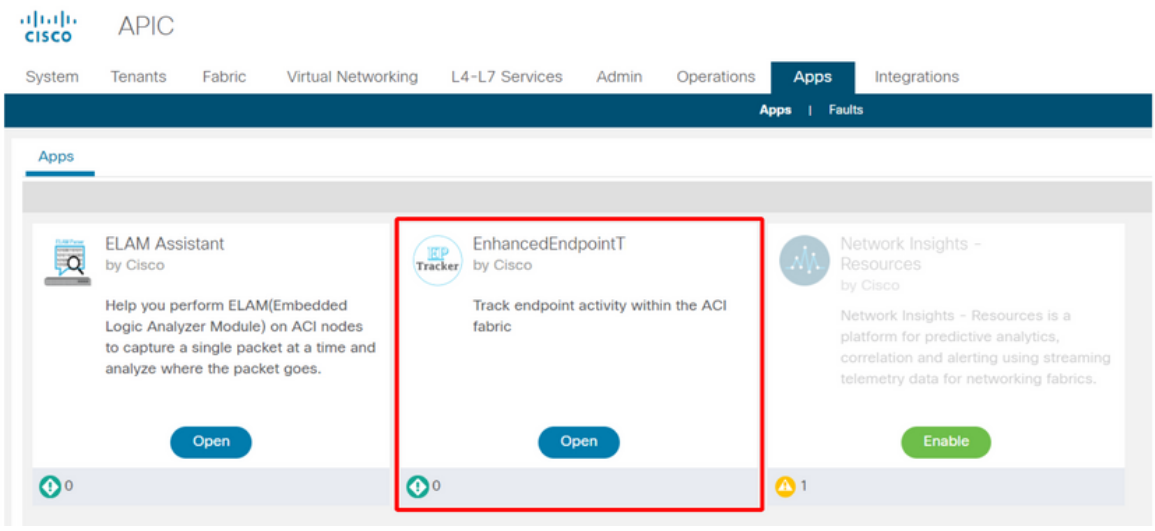
- "ACI Fabric Endpoint Learning Whitepaper" auf www.cisco.com
- "Cisco Live BRKACI-2641 ACI Troubleshooting: Endpoints" auf www.ciscolive.com

Wenn die ACI dieselbe MAC- oder IP-Adresse an mehreren Standorten ermittelt, sieht es so aus, als ob sich das Endgerät bewegt hätte. Dies kann auch durch eine Spoofing-Vorrichtung oder eine Fehlkonfiguration verursacht werden. Dieses Verhalten wird als Endpunkt-Flapping bezeichnet. In einem solchen Szenario fällt der Datenverkehr zum beweglichen/flapping-Endpunkt (MAC-Adresse für überbrückten Datenverkehr, IP-Adresse für gerouteten Datenverkehr) intermittierend aus.

Die effektivste Methode zur Erkennung von Flapping-Ereignissen auf Endpunkten ist der Enhanced Endpoint Tracker. Diese Anwendung kann als ACI AppCenter-Anwendung oder als eigenständige Anwendung auf einem externen Server ausgeführt werden, falls eine deutlich größere Fabric verwaltet werden muss.

Erweiterte Endgeräte-Nachverfolgung

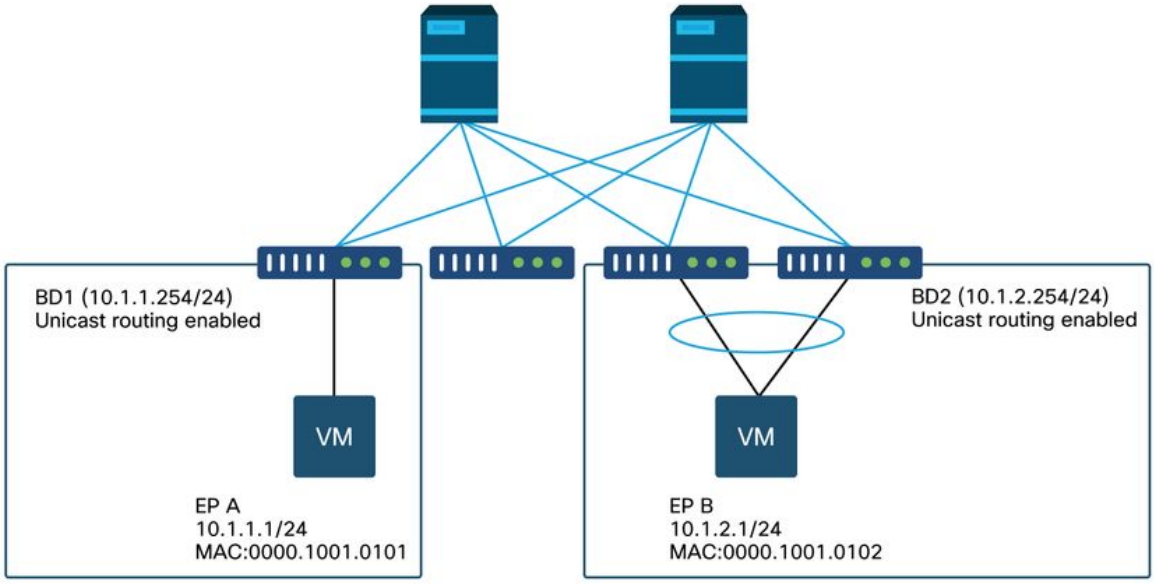
ABWERTUNG WARNUNG! Dieser Leitfaden wurde am 4.2 verfasst. Seitdem wurde die Enhanced Endpoint Tracker-App veraltet und steht nun für die Funktionalität in Nexus Dashboard Insights. Weitere Informationen finden Sie unter Cisco Bug-ID CSCvz59365. .



Das obige Bild zeigt den Enhanced Endpoint Tracker im AppCenter. Im folgenden Beispiel wird

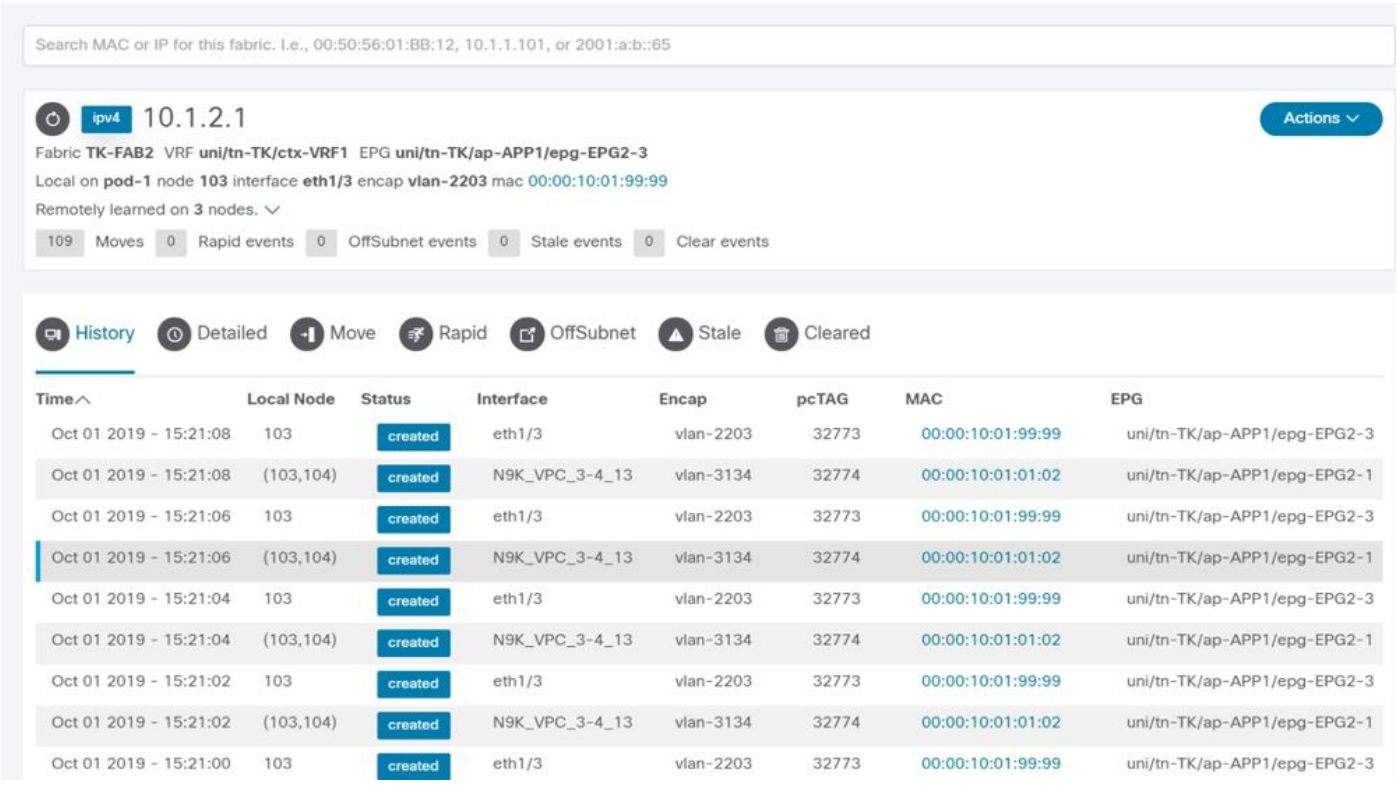
veranschaulicht, wie flapping-fähige Endpunkte mit dem Enhanced Endpoint Tracker gefunden werden.

Beispiel für Endpunkt-Flapping



In diesem Beispiel sollte IP 10.1.2.1 zu EP B mit MAC 0000.1001.0102 gehören. Ein EP X mit MAC 0000.1001.9999 bezieht Datenverkehr mit IP 10.1.2.1 jedoch aufgrund einer mis-config oder möglicherweise IP-Spoofing.

Erweiterte Endpoint Tracker-Ausgabe - Verschiebungen

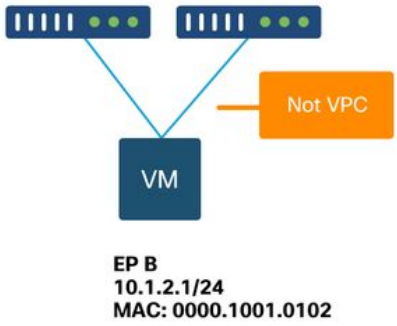


Der Enhanced Endpoint Tracker zeigt an, wann und wo IP 10.1.2.1 abgerufen wurde. Wie im

obigen Screenshot gezeigt, flattert 10.1.2.1 zwischen zwei Endpunkten mit MAC 0000.1001.0102 (erwartet) und 0000.1001.9999 (nicht erwartet). Dies führt zu einem Erreichbarkeitsproblem in Richtung IP 10.1.2.1, da das Paket über die falsche Schnittstelle an ein falsches Gerät gesendet wird, wenn es an der falschen MAC-Adresse erkannt wird. Um dieses Problem zu beheben, müssen Sie Schritte ergreifen, um zu verhindern, dass die unerwartete VM Datenverkehr mit einer unangemessenen IP-Adresse bezieht.

Im Folgenden finden Sie ein typisches Beispiel für ein Flapping eines Endpunkts aufgrund einer ungeeigneten Konfiguration.

Topologiebeispiel, das Flapping des Endpunkts verursachen kann



Wenn ein Server oder eine VM über zwei Schnittstellen ohne VPC mit ACI-Leaf-Knoten verbunden ist, muss der Server das Active/Standby NIC-Teaming verwenden. Andernfalls erfolgt ein Lastenausgleich für die Pakete auf beide Uplinks, und es sieht so aus, als würden die Endpunkte aus Sicht eines ACI-Leaf-Switches zwischen zwei Schnittstellen hin- und herwechseln. In diesem Fall ist ein Active/Standby- oder ein gleichwertiger NIC-Teaming-Modus erforderlich, oder es wird nur eine vPC auf ACI-Seite verwendet.

Schnittstellen-Drops

In diesem Kapitel wird beschrieben, wie Sie die wichtigsten Zähler für das Verwerfen der Eingangsschnittstelle überprüfen.

Hardware-Drop-Counter-Typen

Auf Nexus 9000-Switches, die im ACI-Modus ausgeführt werden, gibt es drei Haupt-Hardwarezähler für Eingangsschnittstellen.

Weiterleiten

Die wichtigsten Gründe für den Rückgang sind:

- SECURITY_GROUP_DENY: Ein Verlust aufgrund fehlender Verträge, um die Kommunikation zu ermöglichen.
- VLAN_XLATE_MISS: Ein Ausfall aufgrund eines ungeeigneten VLAN. Beispiel: Ein Frame gelangt über ein 802.1Q VLAN 10 in die Fabric. Wenn der Switch über VLAN 10 am Port verfügt, überprüft er den Inhalt und trifft eine Weiterleitungsentscheidung auf Basis der Ziel-

MAC. Wenn VLAN 10 auf dem Port jedoch nicht zulässig ist, wird er gelöscht und als VLAN_XLATE_MISS gekennzeichnet.
- ACL_DROP: Ein Verlust aufgrund von SUP-TCAM. Der SUP-TCAM in ACI-Switches enthält spezielle Regeln, die zusätzlich zur normalen L2/L3-Weiterleitungsentscheidung anzuwenden sind. Die Regeln im SUP-TCAM sind integriert und können nicht vom Benutzer konfiguriert werden. Das Ziel der SUP-TCAM-Regeln besteht hauptsächlich darin, einige Ausnahmen oder einen Teil des Datenverkehrs auf der Kontrollebene zu verarbeiten und nicht von Benutzern überprüft oder überwacht zu werden. Wenn ein Paket die SUP-TCAM-Regeln erfüllt und das Paket verworfen werden soll, wird das verworfene Paket als ACL_DROP gezählt, und der Zähler für die Weiterleitung wird erhöht.

Weiterleitungsverweigerungen sind im Wesentlichen Pakete, die aus einem gültigen bekannten Grund verworfen wurden. Sie können im Allgemeinen ignoriert werden und verursachen keine Leistungseinbußen, im Gegensatz zu echten Datenverkehrseinbrüchen.

Fehler

Wenn der Switch einen ungültigen Frame empfängt, wird er als Fehler verworfen. Beispiele hierfür sind Frames mit FCS- oder CRC-Fehlern. Weitere Informationen finden Sie im Abschnitt "CRC - FCS - Cut-Through Switching".

Puffer

Wenn ein Switch einen Frame empfängt und es keine Puffer für Eingang oder Ausgang gibt, wird der Frame mit "Puffer" verworfen. Dies weist in der Regel auf eine Überlastung irgendwo im Netzwerk hin. Die Verbindung, die den Fehler anzeigt, ist möglicherweise voll, oder die Verbindung mit dem Ziel ist überlastet.

Erfassen von Zählern mithilfe der API

Es ist erwähnenswert, dass der Benutzer durch die Nutzung der API und des Objektmodells schnell alle Instanzen dieser Drops im Fabric abfragen kann (diese über ein apic ausführen) -

```
# FCS Errors (non-stomped CRC errors)
moquery -c rmonDot3Stats -f 'rmon.Dot3Stats.fCSErrors>="1"' | egrep "dn|fCSErrors"

# FCS + Stomped CRC Errors
moquery -c rmonEtherStats -f 'rmon.EtherStats.cRCAlignErrors>="1"' | egrep "dn|cRCAlignErrors"

# Output Buffer Drops
moquery -c rmonEgrCounters -f 'rmon.EgrCounters.bufferdroppkts>="1"' | egrep "dn|bufferdroppkts"

# Output Errors
moquery -c rmonIfOut -f 'rmon.IfOut.errors>="1"' | egrep "dn|errors"
```

Anzeigen von Drop-Statistiken in der CLI

Wenn Fehler festgestellt werden oder Paketverluste an Schnittstellen mithilfe der CLI überprüft werden müssen, empfiehlt es sich, die Plattformzähler in der Hardware anzuzeigen. Nicht alle Zähler werden mit "show interface" angezeigt. Die drei Hauptgründe für das Verwerfen können nur mithilfe der Plattformzähler angezeigt werden. So zeigen Sie diese an:

Blatt

SSH auf dem Leaf und führen Sie diese Befehle aus. Dieses Beispiel gilt für Ethernet 1/31.

```
ACI-LEAF# vsh_lc
module-1# show platform internal counters port 31
Stats for port 31
(note: forward drops includes sup redirected packets too)
IF          LPort                    Input                        Output
                                Packets       Bytes          Packets    Bytes
eth-1/31    31  Total          400719   286628225      2302918    463380330
                Unicast     306610   269471065       453831     40294786
                Multicast        0           0      1849091    423087288
                Flood        56783     8427482            0            0
              Total Drops     37327                        0
                Buffer            0                       0
                Error             0                       0
                Forward      37327
                LB                0
                AFD RED                                    0
...
```

Spine

Ein fester Spine (N9K-C9332C und N9K-C9364C) kann mit der gleichen Methode wie die Leaf-Switches überprüft werden.

Bei einem modularen Spine (N9K-C9504 usw.) muss die Linecard angeschlossen werden, bevor die Plattformzähler angezeigt werden können. SSH auf den Spine und führen Sie diese Befehle aus. Dieses Beispiel gilt für Ethernet 2/1.

```
ACI-SPINE# vsh
ACI-SPINE# attach module 2
module-2# show platform internal counters port 1
Stats for port 1
(note: forward drops include sup redirected packets too)
IF          LPort                    Input                        Output
                                Packets       Bytes          Packets    Bytes
eth-2/1      1  Total        85632884  32811563575     126611414   25868913406
                Unicast   81449096  32273734109     104024872   23037696345
                Multicast  3759719   487617769     22586542   2831217061
                Flood            0           0            0            0
              Total Drops         0                        0
                Buffer            0                       0
                Error             0                       0
                Forward           0
                LB                0
                AFD RED                                    0
...
```

Zähler für Warteschlangenstatus werden mithilfe von "show queuing interface" angezeigt. Dieses Beispiel gilt für Ethernet 1/5.

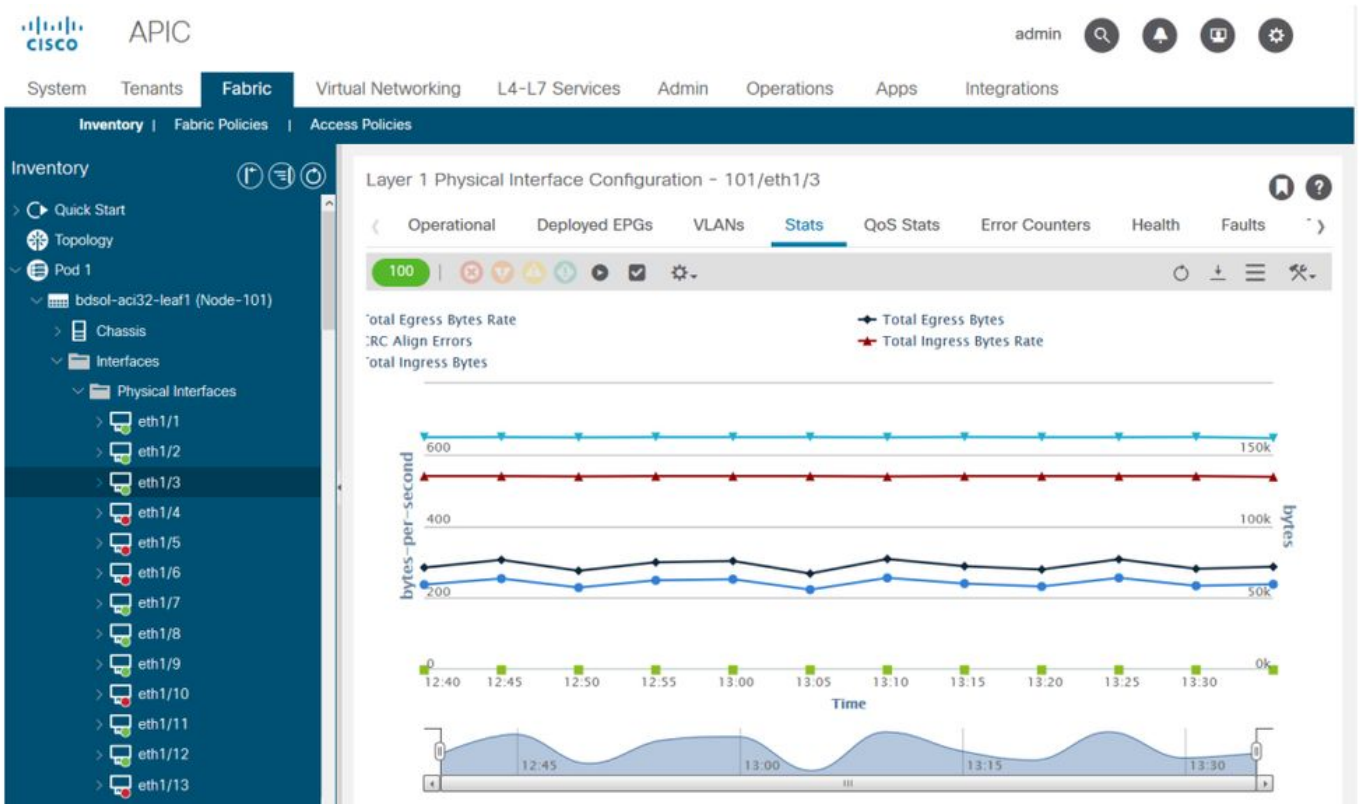
```
ACI-LEAF# show queuing interface ethernet 1/5
================================================================================
               Queuing stats for ethernet 1/5
================================================================================
================================================================================
```

```
                Qos Class level1
================================================================================
Rx Admit Pkts :  0                      Tx Admit Pkts :  0
Rx Admit Bytes:  0                      Tx Admit Bytes:  0
Rx Drop Pkts  :  0                      Tx Drop Pkts  :  0
Rx Drop Bytes :  0                      Tx Drop Bytes :  0

================================================================================
                Qos Class level2
================================================================================
Rx Admit Pkts :  0                      Tx Admit Pkts :  0
Rx Admit Bytes:  0                      Tx Admit Bytes:  0
Rx Drop Pkts  :  0                      Tx Drop Pkts  :  0
Rx Drop Bytes :  0                      Tx Drop Bytes :  0

================================================================================
                Qos Class level3
================================================================================
Rx Admit Pkts :  1756121                Tx Admit Pkts :  904909
Rx Admit Bytes:  186146554              Tx Admit Bytes:  80417455
Rx Drop Pkts  :  0                      Tx Drop Pkts  :  22
Rx Drop Bytes :  0                      Tx Drop Bytes :  3776

...
```

Anzeigen von Statistiken in der Benutzeroberfläche

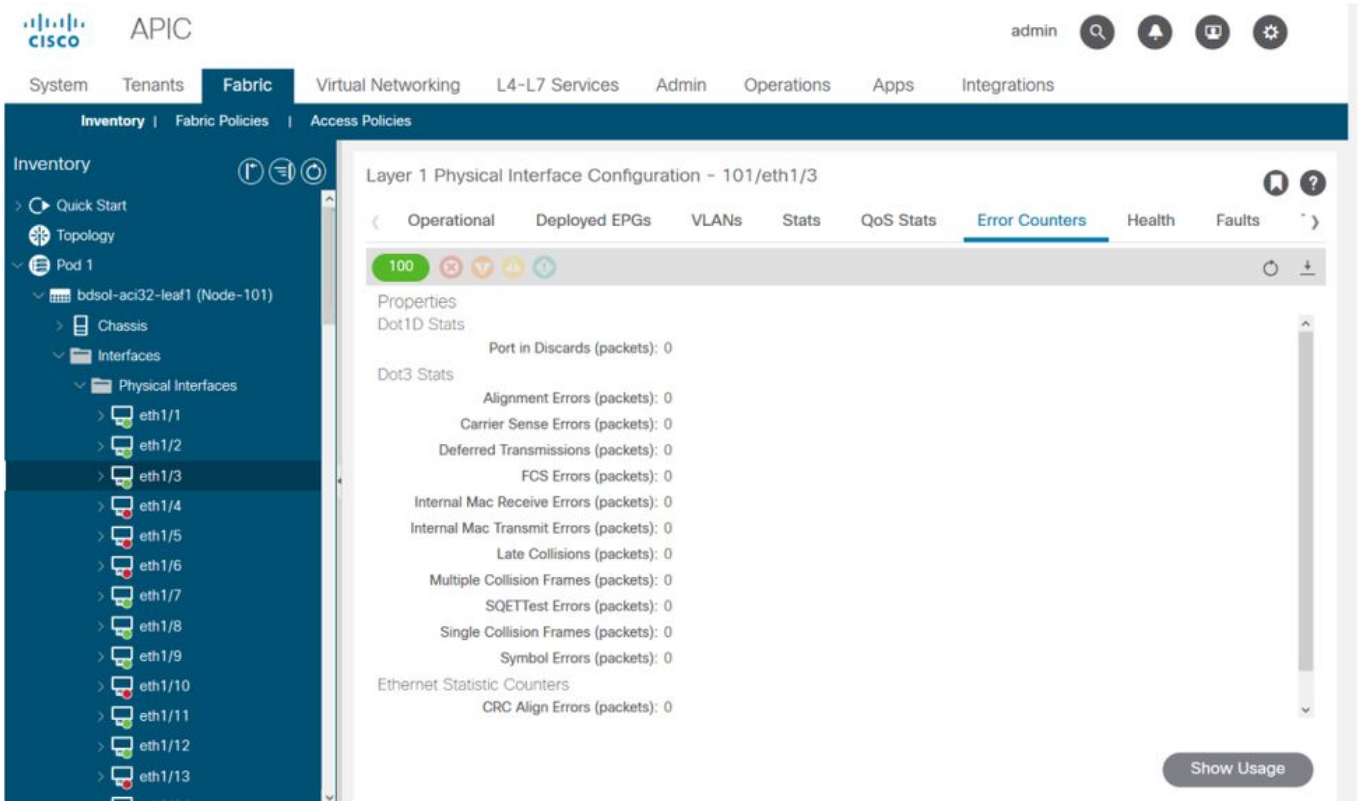
Der Speicherort lautet "Fabric > Inventory > Leaf/Spine > Physical interface > Stats" (Fabric > Bestand > Leaf/Spine > Physische Schnittstelle > Statistiken).

Statistiken der GUI-Schnittstelle



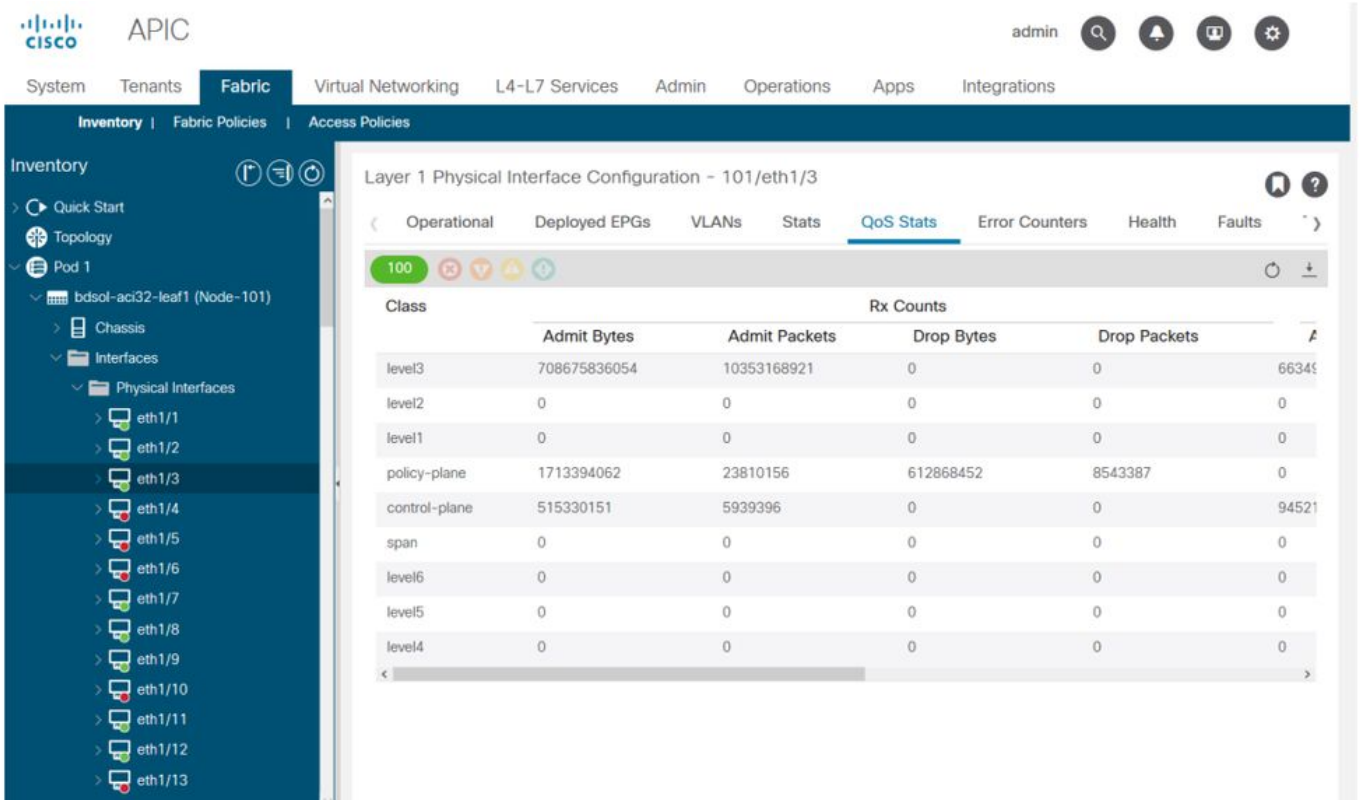
Die Fehlerstatistiken können am gleichen Ort angezeigt werden:

GUI-Schnittstellenfehler



Und schließlich kann die GUI QoS-Statistiken pro Schnittstelle anzeigen:

QoS-Zähler für die GUI-Schnittstelle



CRC — FCS — Cut-Through Switching

Was ist eine zyklische Redundanzprüfung (CRC)?

CRC ist eine Polynomfunktion auf dem Frame, die eine 4B-Nummer in Ethernet zurückgibt. Es erfasst alle Einzelbitfehler und einen guten Prozentsatz an Doppelbitfehlern. Damit soll sichergestellt werden, dass der Rahmen beim Transport nicht beschädigt wurde. Wenn der CRC-Fehlerzähler ansteigt, bedeutet dies, dass, wenn die Hardware die Polynomfunktion auf dem Frame ausgeführt hat, eine 4B-Zahl resultierte, die sich von der 4B-Zahl auf dem Frame selbst unterschied. Frames können aus verschiedenen Gründen beschädigt werden, z. B. aufgrund von Duplexungleichheit, fehlerhafter Verkabelung und defekter Hardware. Es ist jedoch davon auszugehen, dass CRC-Fehler in gewissem Umfang vorliegen, und der Standard ermöglicht eine Ethernet-Fehlerrate von bis zu 10-12 Bit (1 Bit von 1012 kann umgeschaltet werden).

Store-and-forward- und Cut-Through-Switching

Sowohl Store-and-Forward- als auch Cut-Through-Layer-2-Switches basieren ihre Weiterleitungsentscheidungen auf der MAC-Zieladresse von Datenpaketen. Sie lernen auch MAC-Adressen, während sie die Quell-MAC-Felder (SMAC) von Paketen untersuchen, während Stationen mit anderen Knoten im Netzwerk kommunizieren.

Ein Store-and-Forward-Switch trifft eine Weiterleitungsentscheidung für ein Datenpaket, nachdem er den gesamten Frame empfangen und seine Integrität überprüft hat. Ein Cut-Through-Switch wird unmittelbar nach der Überprüfung der Ziel-MAC-Adresse (DMAC) eines eingehenden Frames an den Weiterleitungsprozess weitergeleitet. Ein Cut-Through-Switch muss jedoch warten, bis er das gesamte Paket angezeigt hat, bevor er die CRC-Prüfung durchführt. Das bedeutet, dass das Paket bis zur Validierung der CRC bereits weitergeleitet wurde und nicht verworfen werden kann, wenn die Überprüfung fehlschlägt.

Bisher basierten die meisten Netzwerkgeräte auf Store-and-Forward-Funktionen. Cut-Through-Switching-Technologien werden häufig in Hochgeschwindigkeitsnetzwerken eingesetzt, die Weiterleitungen mit geringer Latenz erfordern.

Insbesondere in Bezug auf ACI-Hardware der 2. Generation und später erfolgt das Cut-Through-Switching, wenn die Eingangsschnittstelle eine höhere und die Ausgangsschnittstelle dieselbe oder eine geringere Geschwindigkeit aufweist. Das Store-and-Forward-Switching erfolgt, wenn die Eingangsschnittstellengeschwindigkeit niedriger ist als die Ausgangsschnittstelle.

Stampfen

Pakete mit einem CRC-Fehler müssen gelöscht werden. Wird der Frame auf einem Cut-Through-Pfad vermittelt, erfolgt die CRC-Validierung, nachdem das Paket bereits weitergeleitet wurde. Daher besteht die einzige Möglichkeit darin, die Ethernet-Frame-Check-Sequenz (FCS) zu stempeln. Beim **Stempeln eines Frames wird der FCS auf einen bekannten Wert gesetzt, der keine CRC-Prüfung besteht**. Aus diesem Grund kann ein fehlerhafter Frame, der bei der CRC-Funktion ausfällt, auf jeder durchlaufenden Schnittstelle als CRC angezeigt werden, bis er einen Store-and-Forward-Switch erreicht, der ihn verwirft.

ACI und CRC: Suche nach fehlerhaften Schnittstellen

- Wenn ein Leaf CRC-Fehler an einem Downlink-Port erkennt, liegt dies meistens am Downlink-SFP oder an Komponenten auf dem externen Gerät/Netzwerk.
- Wenn ein Spine CRC-Fehler erkennt, liegt dies meistens an diesem lokalen Port, SFP, Fiber oder Neighbor SFP. CRC-fehlerhafte Pakete von Leaf-Downlinks werden nicht zu den Spines geleitet. Als wären seine Header lesbar, ist er VXLAN-gekapselt, und die neue CRC wird

berechnet. Wenn die Header aufgrund einer Frame-Beschädigung nicht lesbar sind, wird das Paket verworfen.
- Erkennt ein Leaf CRC-Fehler auf Fabric-Verbindungen, kann dies entweder: Ein Problem mit dem lokalen Glasfaser-/SFP-Paar, der Eingangsfaser des Spine oder dem SFP-Paar.Ein gestampfter Rahmen, der sich seinen Weg durch den Stoff bahnt.

Stampfen: Fehlerbehebung Stampfen

- Suchen Sie nach Schnittstellen mit FCS-Fehlern in der Fabric. Da FCS lokal an einem Port stattfindet, handelt es sich höchstwahrscheinlich um die Glasfaser oder das SFP an beiden Enden.
- CRC-Fehler in der Ausgabe von 'show interface' geben den FCS+Stomp-Gesamtwert wieder.\

Sehen Sie sich ein Beispiel an:

Überprüfen Sie einen Port mit dem Befehl

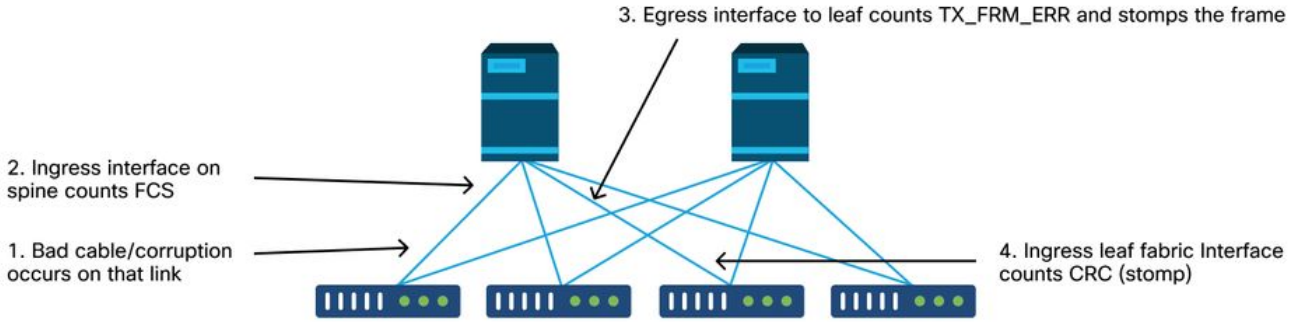
```
vsh_lc: 'show platform internal counter port <X>'
```

In diesem Befehl sind drei Werte wichtig:

- RX_FCS_ERR - FCS-Fehler.
- RX_CRCERR - Empfangener gestempelter CRC-Fehler-Frame.
- TX_FRM_ERROR - Gepuffertes CRC-Fehler-Frame.

```
module-1# show platform internal counters port 1 | egrep ERR
       RX_FCS_ERR           0     ---- Real error local between the devices and its direct
neighbor
       RX_CRCERR            0     ---- Stomped frame --- so likely stomped by underlying devices
and generated further down the network
       TX_FRM_ERROR         0     ---- Packet received from another interface that was stomp on
Tx direction
```

CRC-Fehlerbehebungsszenario



Wenn eine beschädigte Verbindung eine große Anzahl beschädigter Frames generiert, können diese Frames an alle anderen Leaf-Knoten übertragen werden, und es ist sehr gut möglich, CRC am Eingang der Fabric-Uplinks der meisten Leaf-Knoten im Fabric zu finden. Diese würden wahrscheinlich alle von einer einzigen beschädigten Verbindung stammen.

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.