Fehlerbehebung bei Verbindungs-Flap-Problemen auf dem Nexus 9000

Inhalt

Einleitung

Dieses Dokument gbeschreiben wie Sie das Layer-1-Link-Flap-Problem auf Nexus 9000-Switches beheben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit dem Cisco Nexus-Betriebssystem (NX-OS) und der grundlegenden Nexus-Architektur vertraut zu machen, bevor Sie mit den in diesem Dokument beschriebenen Informationen fortfahren.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- N9K-C93180YC-FX
- nxos64-cs.10.2.6.M

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.

Analyse der Ursachen von Verbindungs-Flap

Ein Link-Flap ist ein Netzwerkproblem, bei dem eine physische Schnittstelle an einem Switch, z. B. der Nexus 9000, ständig zwischen aktiv und inaktiv wechselt. Diese Beeinträchtigung kann die Netzwerkleistung beeinträchtigen, das Netzwerk destabilisieren und die Kommunikation unterbrechen. Dies kann erhebliche Unannehmlichkeiten mit sich bringen. Link-Flaps entstehen im Allgemeinen durch fehlerhafte physische Schichten oder Probleme bei der Protokollsynchronisierung.

- Durch Protokoll ausgelöste Verbindungs-Flap

Protokollgesteuerte Verbindungs-Flaps treten auf, wenn ein Problem mit der Protokoll-Synchronisierung auftritt. Dies kann Protokolle wie das Link Aggregation Control Protocol (LACP), Virtual Port-Channel und andere umfassen. Das Problem kann durch falsche Protokollkonfigurationen oder Paketverluste entstehen, die zu einer Instabilität der Verbindung führen. Regelmäßige Überwachung und rechtzeitige Software-Updates können helfen, diese Art von Link-Flapping zu verhindern.

- Physisches Layer-1-Problem

Link-Flaps können auch von Layer 1, der physischen Schicht des Netzwerks, ausgehen. Dies erfordert häufig physische Komponenten wie Kabel und Schnittstellen. Beschädigte, lose oder veraltete Kabel und fehlerhafte Schnittstellen können zu Klappen der Verbindung führen. Regelmäßige physische Inspektionen und Wartungsarbeiten, einschließlich Kabelprüfungen und Schnittstellentests, können dabei helfen, diese Probleme zu identifizieren und zu beheben, bevor es zu Verbindungsunterbrechungen kommt.

Dieser Artikel konzentriert sich auf die Fehlerbehebung bei physischen Layer-1-Problemen.

Identifizieren der Link-Flap

Link-Flaps können einfach aus Protokollen erkannt werden. Im Beispiel wird ein Link-Flap-Ereignis an Port E1/5 angezeigt, bei dem der Port ausfällt und später wieder verfügbar ist.

<#root>

```
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-FOP_CHANGED: port-channel100: first operational
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-PORT_DOWN: port-channel100: Ethernet1/5 is down
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-channel
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_BANDWIDTH_CHANGE: Interface port-channel100,bandwidth
```

2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_LINK_FAILURE: Interface Ethernet1/5 is down (Lin

```
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-channel
2024 Jan 21 05:27:58 N9K-C93180YC-FX %ETHPORT-5-SPEED: Interface Ethernet1/5, operational speed changed
2024 Jan 21 05:27:58 N9K-C93180YC-FX %ETHPORT-5-IF_DUPLEX: Interface Ethernet1/5, operational duplex mo
2024 Jan 21 05:27:58 N9K-C93180YC-FX %ETHPORT-5-IF_RX_FLOW_CONTROL: Interface Ethernet1/5, operational
2024 Jan 21 05:27:58 N9K-C93180YC-FX %ETHPORT-5-IF_TX_FLOW_CONTROL: Interface Ethernet1/5, operational
2024 Jan 21 05:27:58 N9K-C93180YC-FX %ETHPORT-5-SPEED: Interface port-channel100, operational speed cha
2024 Jan 21 05:27:58 N9K-C93180YC-FX %ETHPORT-5-IF_DUPLEX: Interface port-channel100, operational duple
2024 Jan 21 05:27:58 N9K-C93180YC-FX %ETHPORT-5-IF_RX_FLOW_CONTROL: Interface port-channel100, operatio
2024 Jan 21 05:27:58 N9K-C93180YC-FX %ETHPORT-5-IF_TX_FLOW_CONTROL: Interface port-channel100, operatio
```

2024 Jan 21 05:28:02 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-PORT_UP: port-channel100: Ethernet1/5 is up

```
2024 Jan 21 05:28:02 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-FOP_CHANGED: port-channel100: first operational
2024 Jan 21 05:28:02 N9K-C93180YC-FX %ETHPORT-5-IF_BANDWIDTH_CHANGE: Interface port-channel100,bandwidth
2024 Jan 21 05:28:02 N9K-C93180YC-FX %ETHPORT-5-IF_UP: Interface Ethernet1/5 is up in mode access
2024 Jan 21 05:28:02 N9K-C93180YC-FX %ETHPORT-5-IF_UP: Interface port-channel100 is up in mode access
```

Identifizieren von Layer-1-Link-Flap oder von Protokollen ausgelöster Link-Flap

Der Ethernet Port Manager (Ethpm) ist ein Prozess, der Ethernet-Schnittstellen verwaltet. Der Ethpm-Ereignisverlauf kann verwendet werden, um die Ursache einer Link-Flap zu identifizieren.

Beispiel für Layer-1-Flap

Bei E1/5 tritt um 05:28:35 Uhr ein Verbindungsausfall auf, wobei der EthPM-Übergang von ETH_PORT_FSM_EV_LINK_DOWN ausgelöst wird. Dies zeigt eine Layer-1-Klappe an.

<#root>

```
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-channel
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_BANDWIDTH_CHANGE: Interface port-channel100,bandwidth
```

2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_LINK_FAILURE: Interface Ethernet1/5 is down (Lin

```
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-channel
```

N9K-C93180YC-FX# show system internal ethpm event-history interface e1/5

```
[143] 2024-01-21T05:26:02.100255000+00:00 [-] FSM:<Ethernet1/5> Transition:
Previous state: [ETH_PORT_FSM_ST_WAIT_BUNDLE_MEMBER_BRINGUP]
Triggered event: [ETH_PORT_FSM_EV_FIRST_BRINGUP_BUNDLE_MEMBER_DONE]
Next state: [ETH_PORT_FSM_ST_BUNDLE_MEMBER_UP]
```

[144]

2024-01-21T05:27:35.

783495000+00:00 [-] FSM:<Ethernet1/5> Transition:
Previous state: [ETH_PORT_FSM_ST_BUNDLE_MEMBER_UP]

Triggered event: [ETH_PORT_FSM_EV_LINK_DOWN]

Next state: [FSM_ST_NO_CHANGE]

LACP Triggered Flap - Beispiel

E1/8 geht um 07:40:07 in einen inaktiven Initialisierungszustand über, wobei der EthPM-Übergang durch ETH_PORT_FSM_EV_EXTERNAL_REINIT_NO_FLAP_REQ ausgelöst wird. Dies zeigt ein Link-Flap an, das durch das Link Aggregation Control Protocol (LACP) ausgelöst wird.

<#root>

2024 Jan 21 07:37:20 N9K-C93180YC-FX %ETHPORT-5-IF_UP: Interface port-channel200 is up in Layer3
2024 Jan 21 07:40:07 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-chann
2024 Jan 21 07:40:07 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-FOP_CHANGED: port-channel200: first operationa
2024 Jan 21 07:40:07 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-PORT_DOWN: port-channel200: Ethernet1/8 is dow
2024 Jan 21 07:40:07 N9K-C93180YC-FX %ETHPORT-5-IF_BANDWIDTH_CHANGE: Interface port-channel200,bandwidt

2024 Jan 21 07:40:07 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_INITIALIZING: Interface Ethernet1/8 is down (Ini

<#root>

N9K-C93180YC-FX# show system internal ethpm event-history interface e1/8

[218] 2024-01-21T07:37:20.551880000+00:00 [-] FSM:<Ethernet1/8> Transition:
Previous state: [ETH_PORT_FSM_ST_WAIT_BUNDLE_MEMBER_BRINGUP]
Triggered event: [ETH_PORT_FSM_EV_FIRST_BRINGUP_BUNDLE_MEMBER_DONE]
Next state: [ETH_PORT_FSM_ST_BUNDLE_MEMBER_UP]

[219]

2024-01-21T07:40:07.104339000

+00:00 [-] FSM:<Ethernet1/8> Transition:
Previous state: [ETH_PORT_FSM_ST_BUNDLE_MEMBER_UP]
Triggered event:

[ETH_PORT_FSM_EV_EXTERNAL_REINIT_NO_FLAP_REQ]

Next state: [FSM_ST_NO_CHANGE]

Fehlerbehebung bei Layer-1-Link-Flap

Cisco bietet eine breite Palette an optischen Modulen für eine Vielzahl von Geschwindigkeiten, Medien und Entfernungen. Stellen Sie vor dem Herstellen einer Verbindung mit dem Nexus 9000 sicher, dass SFP und Kabel mit Ihrer aktuellen Software und Hardware kompatibel sind. Sie können dies überprüfen durch:

Kompatibilitätsmatrix für optische Verbindungen zu Geräten von Cisco

Interoperabilitätsmatrix für optische Verbindungen von Cisco

Layer-1-Problem bei NX-OS 10.2.1 und höheren Versionen

Ab NX-OS 10.2.1 wird die Platform Insights Engine (PIE) auf allen Cloudscale-ToR- und EoR-Plattformen unterstützt. PIE ist eine Echtzeit-Ursachenanalyse-Anwendung, die während des Switches ausgeführt wird.

Drei PIEs unterstützen Sie bei der Lösung des Problems mit Layer-1-Link-Flaps.

Link Flap PIE

Der Link-Flap-PIE analysiert Link-Flap-Ereignisse, die von User Space Drivers (USDs) veröffentlicht werden, und bestimmt die Ursache für einen Link-Flap. Der PIE veröffentlicht dem Broker die Erkenntnisse zur Ursachenanalyse. Link-Flapping-Ereignisse werden von den USDs (PIE-Client) veröffentlicht, wenn ein Link flaps. Die USDs sammeln alle relevanten Daten vom ASIC und USD, die für die Ursachenanalyse erforderlich sind, und veröffentlichen die Daten an den Broker. Die Link-Flap-PIE analysiert die Daten und kommt zur wahrscheinlichsten Ursache für die Flap.

PIE nach unten verknüpfen

Der Link nach unten PIE findet die Ursache für einen Link, der nicht hochkommt. Das USD sammelt Daten zu einer Schnittstelle, wenn diese für "up" (aktiv) konfiguriert ist, der Betriebsstatus der Schnittstelle jedoch nicht "up" (aktiv) ist. Diese Daten werden in der PIE-Anwendung veröffentlicht. Der Link-Down-PIE abonniert diese Ereignisse, empfängt die Daten vom Broker und analysiert die Daten, um die Ursache zu ermitteln.

Optische PIE

Die Optik PIE ist eine kontinuierliche Überwachungs-Engine, die eine Zeitreihenanalyse der in regelmäßigen Abständen gesammelten DOM-Daten durchführt. Durch die Verfolgung verschiedener Parameter im DOM über einen bestimmten Zeitraum erreicht der PIE eine Metrik, die den Zustand der optischen Verbindungen für jeden optischen Port beschreibt. Die Metrik ist eine Erkenntnis über den Gesundheitszustand eines optischen Transceivers.

Weitere Informationen finden Sie in diesem PIE-Dokument:

Cisco Nexus Serie 9000 NX-OS Platform Insights Engine Guide, Version 10.2(x)

PIE-Beispiel: Link-Flap verursacht durch Herunterfahren und erneutes Aktivieren des Ports auf der Peer-Seite

<#root>

```
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-FOP_CHANGED: port-channel100: first operational
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-PORT_DOWN: port-channel100: Ethernet1/5 is down
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-channel
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_BANDWIDTH_CHANGE: Interface port-channel100,bandwidth

2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_LINK_FAILURE: Interface Ethernet1/5 is down (Link

2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-channel
2024 Jan 21 05:27:58 N9K-C93180YC-FX %ETHPORT-5-SPEED: Interface Ethernet1/5, operational speed changed
<snip>
2024 Jan 21 05:28:02 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-PORT_UP: port-channel100: Ethernet1/5 is up

N9K-C93180YC-FX# show pie interface ethernet 1/5 link-flap-rca

2024-01-21 05:27:35

 Event Id: 00000068 Ethernet1/5 Source Id: 436209664 RCA Code: 41   >>>PIE event time

Reason: Link flapped/down due to Local Fault, check peer

 >>>PIE link flap reason

N9K-C93180YC-FX# show pie interface ethernet 1/5 transceiver-insights

2024-01-21 05:30:12 Event Id: 00000080 Event Class: xcvr DOM DB Event Interface: Ethernet1/5 Health Met
2024-01-21 05:28:12 Event Id: 00000072 Event Class: xcvr DOM DB Event Interface: Ethernet1/5 Health Met
```

PIE-Beispiel: Link Down durch Herunterfahren des Ports auf der Peer-Seite

<#root>

```
2024 Jan 21 05:48:38 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-FOP_CHANGED: port-channel100: first operational
2024 Jan 21 05:48:38 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-PORT_DOWN: port-channel100: Ethernet1/5 is down
2024 Jan 21 05:48:38 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-channel
2024 Jan 21 05:48:38 N9K-C93180YC-FX %ETHPORT-5-IF_BANDWIDTH_CHANGE: Interface port-channel100,bandwidth

2024 Jan 21 05:48:38 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_LINK_FAILURE: Interface Ethernet1/5 is down (Link

2024 Jan 21 05:48:38 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-channel

N9K-C93180YC-FX# show pie interface ethernet 1/5 link-down-rca

2024-01-21 05:48:48
```

```
 Event Id: 00000197 Ethernet1/5 Source Id: 436209664 RCA Code: 16           >>>PIE event time
```

Reason: No PCS alignment detected. Please check Fec, speed, Autoneg configurations with peer

```
   >>>Physical layer failed
```

N9K-C93180YC-FX# show pie interface ethernet 1/5 transceiver-insights

```
2024-01-21 05:50:12 Event Id: 00000199 Event Class: xcvr DOM DB Event Interface: Ethernet1/5 Health Met
2024-01-21 05:48:12 Event Id: 00000187 Event Class: xcvr DOM DB Event Interface: Ethernet1/5 Health Met
```

Ersetzen defekter Teile

Basierend auf der PIE-Ausgabe wird empfohlen, die potenziell fehlerhafte Komponente zu ersetzen und die Überwachung fortzusetzen. Besteht die Verbindungsklappe weiter, ist ein Austauschtest erforderlich, um das fehlerhafte Teil einzugrenzen. Ein Swap-Test kann durchgeführt werden, indem eine Komponente nach der anderen gewechselt wird, während alle anderen Komponenten unverändert bleiben. Letztlich stabilisiert sich die Verbindung nach dem Austauschen der spezifischen fehlerhaften Komponente.

Layer-1-Problem bei NX-OS 10.1.2 und früheren Versionen

Für NX-OS-Softwareversionen vor 10.2(1) ist kein PIE-Support verfügbar. Für die Überprüfung der Layer-1-Link-Flap sind mehrere manuelle Schritte erforderlich.

Überprüfen des Port-Client-Ereignisverlaufs

Hier werden alle Linkereignisse im angeschlossenen Modul aufgelistet. Debouncing-Zeit bezieht sich auf die Dauer, die eine Schnittstelle wartet, bevor sie den Supervisor über den Ausfall einer Verbindung informiert. Während dieses Zeitraums wartet die Schnittstelle, bis der Link wieder verfügbar ist. Diese wird verwendet, um festzustellen, ob die Verbindung ausgefallen ist oder nur eine kleine Klappe auftritt.

<#root>

N9K-C93180YC-FX# attach module 1

module-1# show system internal port-client link-event

```
*************** Port Client Link Events Log ***************
---- ------ ----- ----- ------
Time PortNo Speed Event Stsinfo
---- ------ ----- ----- ------
```

Jan 21 05:48:38 2024 00122142 Ethernet1/5 ---- DOWN Link down debounce timer stopped and link is down

Jan 21 05:48:37 2024 00993003 Ethernet1/5 ---- DOWN Link down debounce timer started(0x40e50006)

Jan 21 05:45:14 2024 00432606 Ethernet1/5 10G UP SUCCESS(0x0)

Überprüfen der ASIC-Ereignisse

Diese Ereignisse liefern detaillierte Informationen zu den einzelnen Verbindungsereignissen.

<#root>

N9K-C93180YC-FX# attach module 1
module-1# show hardware internal tah link-events fp-port 5

324) Jan 21 05:48:37 2024 uSec 992843: Fp 5 : tahusd_isr.c #8469
Port Down with an ASIC interrupt
------------- ASIC MAC/PCS/Serdes REGS (Mac Channel 0) -------------

Link flapped due to Local Fault, check peer

>>>Local Fault means the local

device detected the issue on the receive path.

>>>

Remote Fault means a Local Fault is detected across the link.

Intr Regs 00:0x0000, 01:0x0000, 02:0x0000, 03:0x0010, 07:0x0000, 11:0x0000, 15:0x0000
sts2.bercount : 0x0f00 sts2.erroredblocks : 0x0000
bercounthi : 0x0000 erroredblockhi : 0x0000
counters0.syncloss : 0x0001 counters0.blocklockloss: 0x0001
counters1.highber : 0x0000 counters1.vlderr : 0x0000
counters2.unkerr : 0x0012 counters2.invlderr : 0x0000

Fehlercode	Erläuterung
st2,fehlerhafteBlöcke	Zählt fehlerhafte Blöcke (Bits höherer Ordnung).
st2.bercount	Zählt ungültige Synchronisierungsheader (niedrigere Bit-Reihenfolge).

Bercounthi	Zählt ungültige Synchronisierungsheader (Bits höherer Ordnung).
erroredblockhi	Zählt fehlerhafte Blöcke (Bits höherer Ordnung).
Zähler0.synclos	Synchronisierungsverlust
Zähler0.blocklockloss	Blockierverlust
Zähler1.highber	Hoher BER
Zähler1.vlderr	Gültiger Fehler
Zähler2.unkerr	Unbekannter Fehler
counter2.invlderr	Ungültiger Fehler

Überprüfen der DOM-Informationen auf beiden Seiten

Diese Ausgabe enthält mehrere Informationen zu SFP (Small Form-factor Pluggable). Wenn ein Wert außerhalb des akzeptablen Bereichs bei der SFP-Diagnose liegt, gilt der SFP als potenziell beschädigte Komponente und muss ersetzt werden. In diesem Beispiel ist alles in Ordnung.

<#root>

```
N9K-C93180YC-FX# show interface e1/5 transceiver details


Ethernet1/5
transceiver is present
type is 10Gbase-SR                    >>>SFP type
name is CISCO-OPLINK                  >>>SFP vendor
part number is TPP4XGDS0CCISE2G
revision is 02
serial number is OPMXXXXXXXX          >>>SFP SN
nominal bitrate is 10300 MBit/sec     >>>SFP bitrate
Link length supported for 50/125um OM2 fiber is 82 m
Link length supported for 62.5/125um fiber is 26 m
Link length supported for 50/125um OM3 fiber is 300 m
cisco id is 3
cisco extended id number is 4
cisco part number is 10-2415-03
cisco product id is SFP-10G-SR        >>>SFP PID
cisco version id is V03

SFP Detail Diagnostics Information (internal calibration)
```

```
--------------------------------------------------------------------------------
            Current                 Alarms       Warnings
          Measurement           High    Low    High    Low
--------------------------------------------------------------------------------
Temperature

 36.52 C           75.00 C -5.00 C 70.00 C 0.00 C

Voltage

     3.28 V             3.63 V  2.97 V  3.46 V 3.13 V

Current

     6.61 mA          12.00 mA 0.50 mA 11.50 mA 1.00 mA

Tx Power

   -2.70 dBm        1.99 dBm -11.30 dBm -1.00 dBm -7.30 dBm

Rx Power

   -2.40 dBm        1.99 dBm -13.97 dBm -1.00 dBm -9.91 dBm
Transmit Fault Count = 0
--------------------------------------------------------------------------------
Note: ++ high-alarm; + high-warning; -- low-alarm; - low-warning
peer side information is snipped.
```

Test und Austausch defekter Teile wechseln

Wenn bei den vorherigen Prüfungen alles in Ordnung zu sein scheint, ist ein Swap-Test erforderlich, um das fehlerhafte Teil einzugrenzen. Ein Swap-Test kann durchgeführt werden, indem eine Komponente nach der anderen gewechselt wird, während alle anderen Komponenten unverändert bleiben. Schließlich stabilisiert sich die Verbindung, nachdem die jeweilige fehlerhafte Komponente ausgetauscht wurde.

Zugehörige Informationen

Datenblatt für Nexus 9000

Konfigurationsleitfaden für Nexus 9000-Schnittstellen

Nexus Serie 9000 - NX-OS Platform Insights Engine-Leitfaden

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.