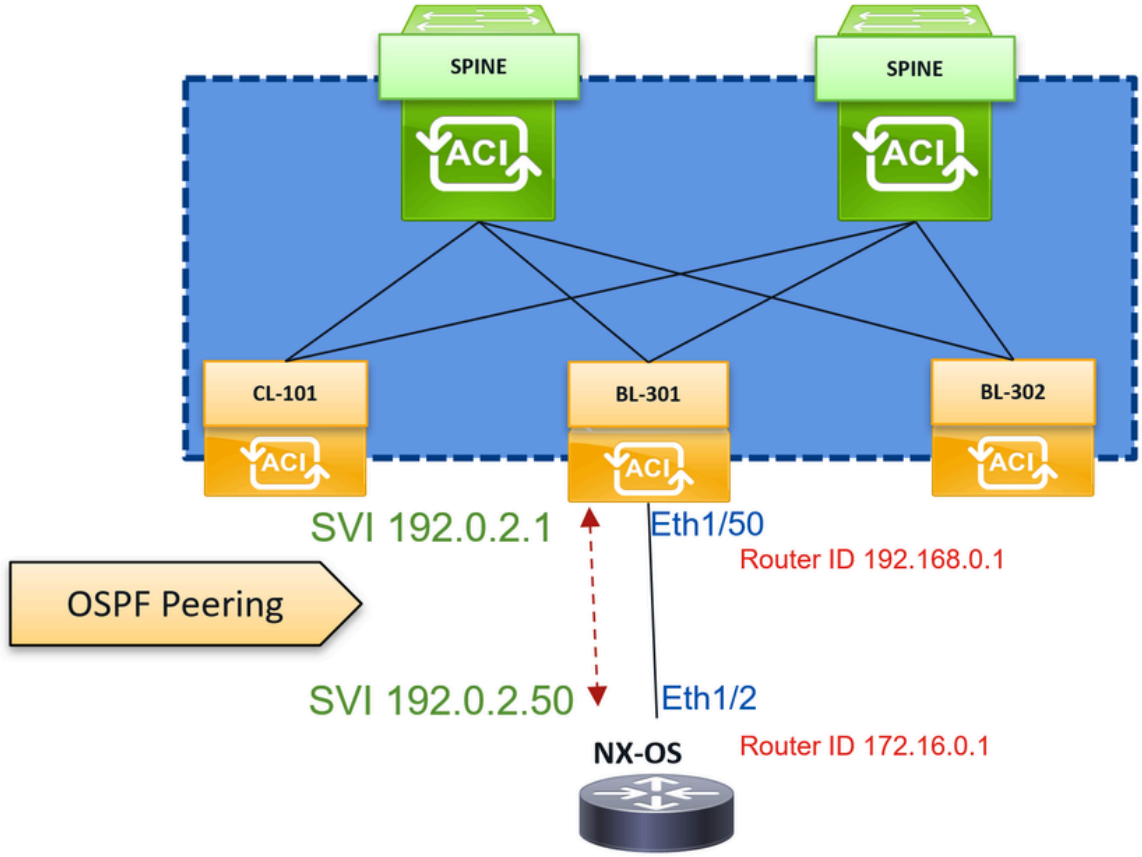
Fehlerbehebung bei ACI OSPF-Adjacencies

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung für OSPF-Adjacencies (Open Shortest Path First) der Application Centric Infrastructure (ACI) beschrieben.

Topologie



Topologie

Konfigurationsanforderungen für das OSPF-Peering

OSPF ist eines der Protokolle, die Sie zwischen der Cisco ACI und einem externen Router aktivieren können. Die Cisco ACI unterstützt alle gängigen Optionen, wie z. B. den OSPF-Bereich einschließlich Backbone, verschiedene Stub-Optionen, Authentifizierung von Nachbarn und andere ähnliche Optionen.

Ein L3Out umfasst die Routing-Protokolloptionen, die Switch-spezifische Konfiguration (ein Knotenprofil) und die schnittstellenspezifischen Einstellungen (ein Schnittstellenprofil). Die OSPF-bezogenen Parameter können wie ein normaler Router hauptsächlich an zwei Stellen konfiguriert werden. Die erste Option ist Virtual Routing and Forwarding (VRF)-weite oder knotenweite Konfiguration, z. B. Area-ID und Area Type, die auf dem L3Out selbst konfiguriert werden können. Der zweite Parameter bezieht sich auf Schnittstellenebenen wie das OSPF-Hello-Intervall oder den Schnittstellentyp (Broadcast, Point-to-Point(P2P)).

Für die Einrichtung der OSPF-Adjacency zwischen dem ACI-Border-Leaf und dem externen Router müssen folgende Voraussetzungen erfüllt sein:

1. OSPF-Bereich-ID und -Typ müssen übereinstimmen
2. Die OSPF-Router-ID muss eindeutig sein
3. Die maximale Übertragungseinheit (Maximum Transmission Unit, MTU) muss übereinstimmen (sie wird standardmäßig von der Fabric auf 9.000 und von den meisten

Cisco IOS®/NXOS auf 1.500 festgelegt).
4. OSPF-Authentifizierungsschlüssel und -typ müssen übereinstimmen (falls verwendet)
5. OSPF-Hello- und Dead-Intervalle müssen übereinstimmen
6. OSPF-Netzwerktyp muss übereinstimmen

Das Whitepaper enthält eine detaillierte Erläuterung der Designkonzepte und -optionen für die ACI L3Out für die unterstützten Routing-Protokolle.

Wenn Sie mit der L3Out-Konfiguration und anderen grundlegenden Anforderungen nicht vertraut sind, lesen Sie das Whitepaper.

Fehlerbehebung bei OSPF-Adjacency - Allgemeine Checkliste

Unabhängig davon, ob die OSPF-Adjacency zuvor verfügbar war oder nie genutzt wurde, sollten zunächst die grundlegenden Anforderungen validiert werden.

Schritt 1: Pingen Sie die Remote-End-Schnittstelle. Dies hilft bei der Bestätigung, ob die IP-Verbindung zum anderen Ende des Netzwerks möglich ist, was eine Hauptanforderung für die Aktivierung von OSPF ist.

```
iping -V <vrf> <remote_end_IP>
example:
BL-301# iping -V abc1:vrf-1 192.0.2.50
```

Schritt 2: Validieren Sie die grundlegenden Konfigurationsparameter:

1. OSPF-Bereich-ID und -Typ müssen übereinstimmen
2. Die OSPF-Router-ID muss eindeutig sein
3. Die MTU muss übereinstimmen (in der Fabric ist standardmäßig 9.000 eingestellt, in den meisten Fällen 1.500 für Cisco IOS/NX).
4. OSPF-Authentifizierungsschlüssel und -typ müssen übereinstimmen (falls verwendet)
5. OSPF-Hello- und Dead-Intervalle müssen übereinstimmen
6. OSPF-Netzwerktyp muss übereinstimmen

Die Befehlsausgaben zeigen die Konfigurationsattribute an, die auf das Leaf übertragen werden.

<#root>

```
BL-301# show ip int bri vrf abc1:vrf-1
IP Interface Status for VRF "abc1:vrf-1"(137)
Interface            Address              Interface Status
vlan1                192.0.2.1/24         protocol-up/link-up/admin-up  --> l3out SVI
lo9                  192.168.0.1/32       protocol-up/link-up/admin-up  --> Router ID SVI

BL-301#
```

show ip ospf interface vlan 1

```
Vlan1 is up, line protocol is up
IP address
192.0.2.1/24
, Process ID default VRF
abc1:vrf-1
,
area backbone

Enabled by interface configuration
State P2P,
Network type P2P
, cost 4
Index 84, Transmit delay 1 sec
1 Neighbors, flooding to 1, adjacent with 1
Timer intervals:
Hello 10, Dead 40
, Wait 40, Retransmit 5
Hello timer due in 00:00:03
No authentication

Number of opaque link LSAs: 0, checksum sum 0

BL-301#
show int vlan
1 | egrep "MTU"



MTU
9000
 bytes, BW 10000000 Kbit, DLY 1 usec

BL-301#
show ip ospf vrf abc1:vrf-1 | grep Routing

Routing Process default with ID
192.168.0.1
 VRF abc1:vrf-1 -->
Router ID
```

Notieren Sie sich alle hervorgehobenen Details, und vergewissern Sie sich, dass die entsprechenden Parameter am Remote-Ende synchronisiert sind.

Fehlerbehebung: OSPF-Adjacency - Faults

<#root>

[+]From the border Leaf we can identify the state of the neighbor state
BL-301# show ip ospf neighbors vrf

abc1:vrf-

1

<<EMPTY>>

[+] You can check the associated faults to the VRF.
BL-301# moquery -c faultInst -x 'query-target-filter=wcard(faultInst.dn,"

abc1:vrf-1

")' | egrep "code|rule|dn|descr|lastTransition"

<<EMPTY>>

Es gibt einige Szenarien ohne aktive Fehler in der Umgebung, aber es kann einen Fehler Record F1385 (protocol-ospf-adjacency-down) auf dem Leaf geben, der uns auf das letzte Mal verweist, als diese Nachbarschaft aktiv war oder wenn sie nie voll war.
Sie können dies mit dem moquery -c faultRecord -f 'fault.Inst.code=="F1385"' -x 'query-target-filter=wcard(faultRecord.dn,"abc1:vrf-1")' | grep dn Befehl identifizieren.

Überprüfen Sie mit dem Befehl die Anzahl der Fehlerdatensätze für ein bestimmtes Datummoquery -c faultRecord -f 'fault.Inst.code=="F1385"' -x 'query-target-filter=wcard(faultRecord.dn,"abc1:vrf-1")' -x 'query-target-filter=wcard(faultRecord.created,"2024-01-01")' | egrep "dn" | wc -l.

Sie müssen die OSPF-Schnittstelle und die lokal und remote konfigurierten IP-Adressen identifizieren.

<#root>

[+] Identify the IP applied on the external device from the ARP associated to the interface
BL-301# moquery -c arpAdjEp -x 'query-target-filter=wcard(arpAdjEp.ifId,"

vlan1

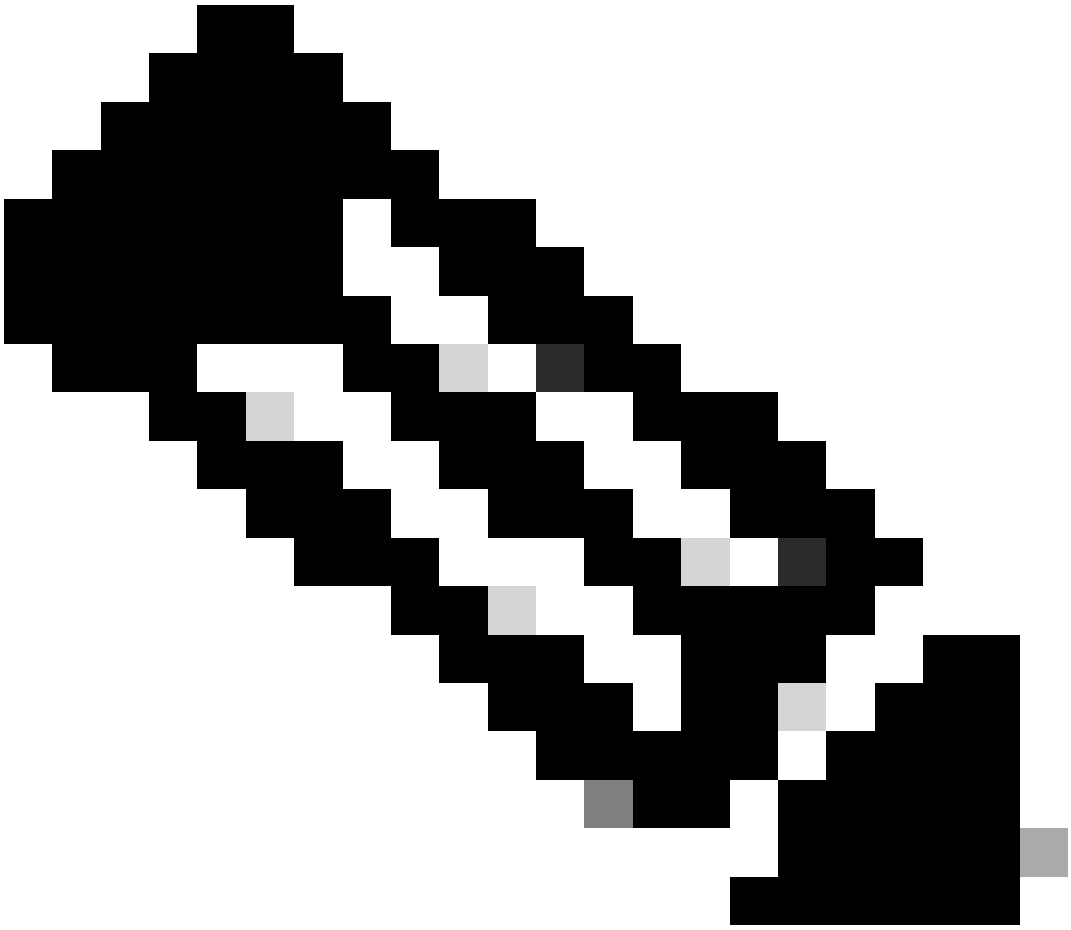
")' | grep "ip "
ip   :

192.0.2.50

Erfassen des Datenverkehrs auf der Kontrollebene auf dem Knoten

Mit der erwarteten virtuellen Quell- und Ziel-Switch-Schnittstelle (SVI) des Grenz-Leaf können Sie das tcpdump-Dienstprogramm zur

Überprüfung verwenden.



Hinweis: Hierfür wird die Schnittstelle kpm_inb verwendet, mit der Sie den gesamten Netzwerkverkehr der CPU-In-Band-Kontrollebene anzeigen können.

<#root>

[+] Capture a single OSPF hello packet using TCPDUMP coming for local BL OSPF IP 192.0.2.1
BL-301# tcpdump src host 192.0.2.1 -vv -e -i kpm_inb
tcpdump: listening on kpm_inb, link-type EN10MB (Ethernet), capture size 262144 bytes
  192.0.2.1 > ospf-all.mcast.net:

0SPFv2

, Hello, length 44
        Router-ID 192.168.0.1,

Backbone Area

,

Authentication Type: none (0)

        Options [

External

]

Hello Timer 10s, Dead Timer 40s,

Mask 255.255.255.0, Priority 1

[+] Capture a single OSPF hello packet using TCPDUMP coming from external device OSPF IP 192.0.2.50
BL-301# tcpdump src host 192.0.2.50 -vv -e -i kpm_inb
tcpdump: listening on kpm_inb, link-type EN10MB (Ethernet), capture size 262144 bytes
    192.0.2.50 > ospf-all.mcast.net:

OSPFv2

, Hello, length 44
        Router-ID 172.16.0.1,

Backbone Area, Authentication Type: none (0)

        Options [

External

]

Hello Timer 10s, Dead Timer 40s,

Mask 255.255.255.0, Priority 1

Wireshark-Verifizierung

Sie können OSPF- und HOST-spezifischen Datenverkehr erfassen, um ihn in Wireshark zu analysieren.

BL-301# tcpdump -i kpm_inb proto ospf -vv -e -w - | tee /data/techsupport/Node-XXX_OSPF.pcap | tcpdump -r - host any

BL-301# tcpdump -xxxvi kpm_inb 'proto ospf and (host <<X.X.X.X>> or host <<Y.Y.Y.Y>>)' -w /data/techsupport/Node-XXX_OSPF_HOST.pcap

BL-301# tcpdump -i kpm_inb proto ospf -vv -e -w - | tee /data/techsupport/Node-XXX_OSPF_HOST.pcap | tcpdump -r - host X.X.X.X

Für pcap-Aufnahmen können Sie Wireshark-Filter verwenden, indem Sie **Analyze > Apply as a Column** verwenden.

ospf.area_id = zur Identifizierung von AreaID

ospf.auth.type = zur Überprüfung des konfigurierten Auth Type auf Übereinstimmung

ospf.hello.hello_interval = zur Überprüfung auf unterschiedliche MTUs

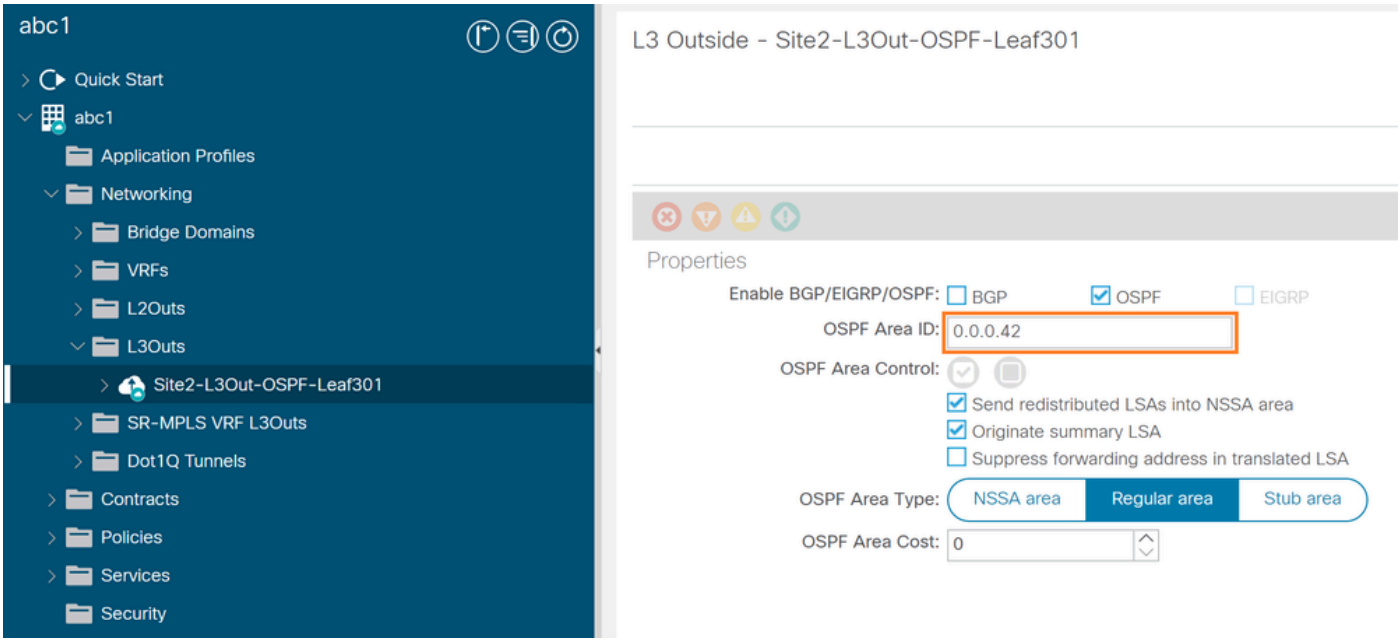
ospf.hello.router_dead_interval = zur Überprüfung auf unterschiedliche Dead-Intervall-Konfiguration

ospf.srcrouter = Router-ID

Fehlerbehebungsszenarien

Fehlerbehebung der OSPF-Adjacency: Area ID Mismatch

Navigieren Sie in der APIC-Konfiguration mit der Area-ID 0.0.0.42 zu **Fabric > Tenants > Networking > L3Outs > <<L3outName>> Policy > Main**.



Falsche OSPF-Bereichs-ID konfiguriert 0.0.0.42

Aus dem Randblatt:

<#root>

[+] Check OSPF interface details to confirm current area

BL-301# show ip ospf interface vlan 1 | grep area
IP address 192.0.2.1/24, Process ID default VRF abc1:vrf-1, area

0.0.0.42

Or

```
BL-301# moquery -c ospfIf -x 'query-target-filter=wcard(ospfIf.id,"vlan1")' | grep area
area         :
```

0.0.0.42

```
[+] Capture a single packet TCPDUMP for local BL OSPF IP
BL-301# tcpdump src host 192.0.2.1 -vv -e -i kpm_inb -c 1
    192.0.2.1 > ospf-all.mcast.net: OSPFv2, Hello, length 44
        Router-ID 192.168.0.1,
```

Area

0.0.0.42

```
, Authentication Type: none (0)
        Options [External]
          Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1

[+] Capture a single OSPF hello packet using TCPDUMP coming from external device OSPF IP
BL-301# tcpdump src host 192.0.2.50 -vv -e -i kpm_inb -c 1
    192.0.2.50 > ospf-all.mcast.net: OSPFv2, Hello, length 44
        Router-ID 172.16.0.1,
```

Backbone Area

```
, Authentication Type: none (0)
        Options [External]
          Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
```

Von externem Gerät:

<#root>

NX-OS# show logging log | tail -n 100 | grep ospf-bootcamp
2023 Dec 28 15:17:09 NX-OS %OSPF-4-AREA_ERR: ospf-bootcamp [22263] (301-l3-abc1) Packet from 192.0.2.1 on Ethernet1/2 received for wrong are

0.0.0.42

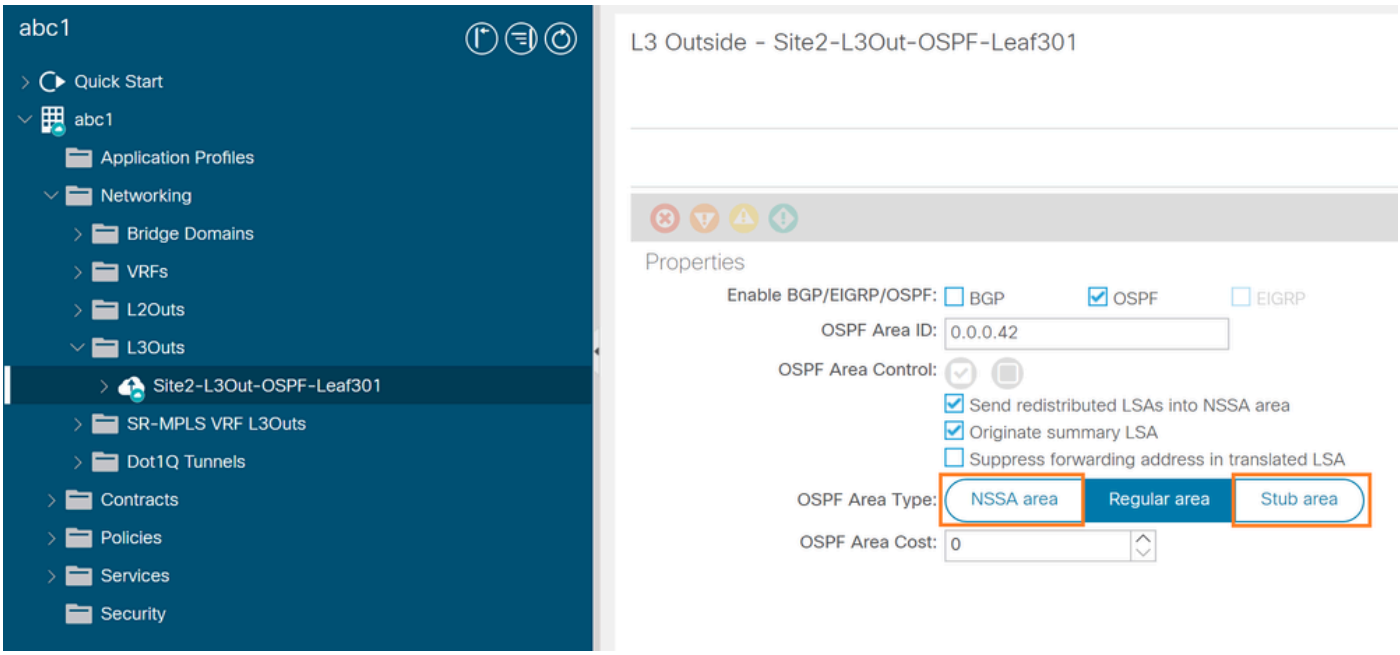
```
NX-OS# show ip ospf interface Ethernet1/2 | grep area
    Process ID bootcamp VRF 301-l3-abc1,
```

area 0.0.0.0

Lösung: Ordnen Sie die OSPF-Area 0.0.0.0 oder dem Backbone auf BL oder 0.0.0.42 auf dem externen Gerät zu.

Fehlerbehebung der OSPF-Adjacency: Area Type Mismatch

Navigieren Sie in der ACI-GUI bei der Konfiguration mit dem Bereichstyp NSSA oder Stub zu **Fabric** > **Tenants** > **Networking** > **L3Outs** > **"L3outName"** > **Policy** > **Main**.



NSSA- oder Stub Area-Konfiguration.

Aus dem Randblatt:

<#root>

```
[+] Capture a single packet TCPDUMP for local BL OSPF IP
BL-301# moquery -c ospfArea -x 'query-target-filter=wcard(ospfArea.dn,"abc1:vrf-1")' | egrep "type"
type                :
```

nssa

```
BL-301# tcpdump src host 192.0.2.1 -vv -e -i kpm_inb -c 1
    192.0.2.1 > ospf-all.mcast.net: OSPFv2, Hello, length 44
        Router-ID 192.168.0.1, Area 0.0.0.42, Authentication Type: none (0)
        Options [
```

NSSA

```
]
          Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
```

or

```
BL-301# moquery -c ospfArea -x 'query-target-filter=wcard(ospfArea.dn,"abc1:vrf-1")' | egrep "type"
type               :
```

stub

```
BL-301# tcpdump src host 192.0.2.1 -vv -e -i kpm_inb -c 1
    192.0.2.1 > ospf-all.mcast.net: OSPFv2, Hello, length 44
        Router-ID 192.168.0.1, Area 0.0.0.42, Authentication Type: none (0)
        Options [
```

none

```
]
          Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1

[+] Capture a single OSPF hello packet using TCPDUMP coming from external device OSPF IP
BL-301# tcpdump src host 192.0.2.50 -vv -e -i kpm_inb -c 1
    192.0.2.50 > ospf-all.mcast.net: OSPFv2, Hello, length 44
        Router-ID 172.16.0.1, Area 0.0.0.42, Authentication Type: none (0)
        Options [
```

External

```
]
          Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
```

Von externem Gerät:

<#root>

```
[+] Check OSPF interfaces con vrf
```

```
NX-OS# show ip int bri vrf 301-l3-abc1
IP Interface Status for VRF "301-l3-abc1"(21)
Interface            IP Address      Interface Status
Lo1001               110.1.0.1       protocol-up/link-up/admin-up
Eth1/2.1120          192.0.2.50      protocol-up/link-up/admin-up

NX-OS# show ip ospf interface Ethernet1/2 | grep area
    Process ID bootcamp VRF 301-l3-abc1,
```

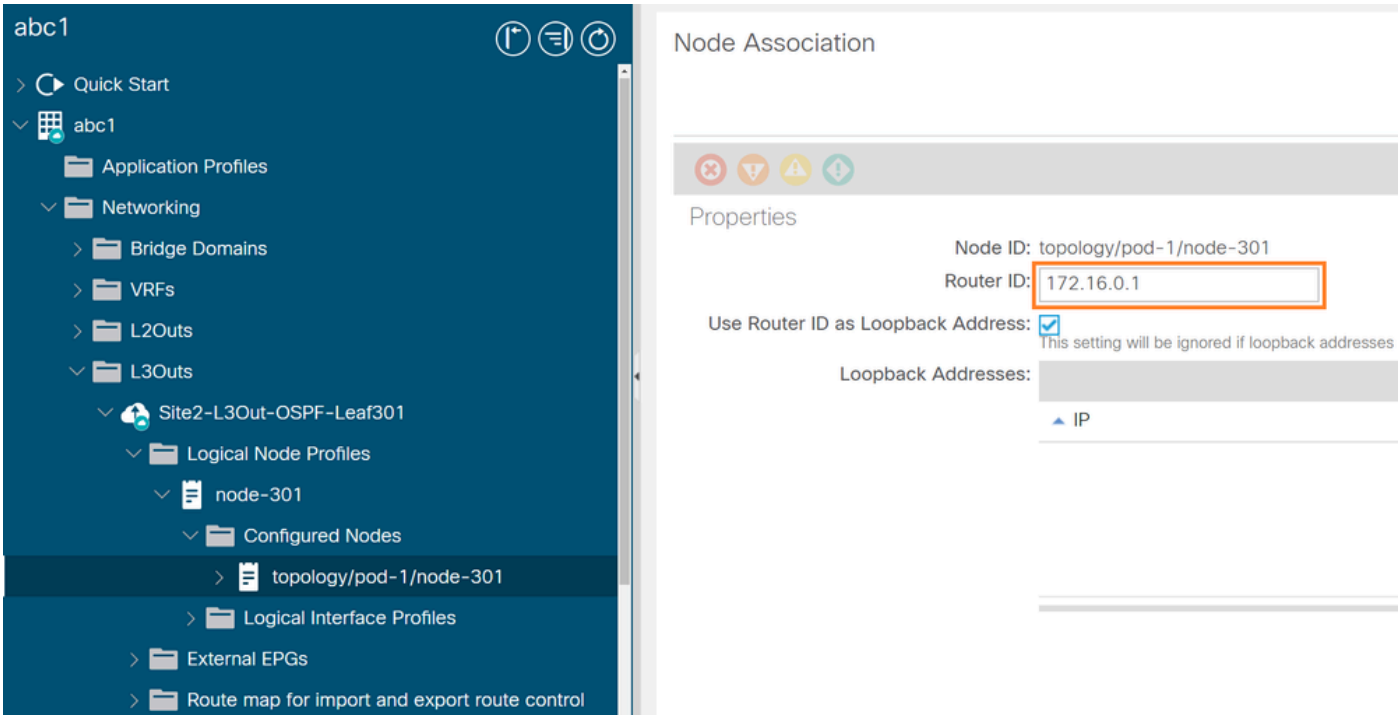
area 0.0.0.0

Lösung: Passen Sie den OSPF-Bereichstyp regelmäßig auf L3Out oder vom externen Gerät an.

Fehlerbehebung der OSPF-Adjacency: Doppelte Router-ID

Eine duplizierte Router-ID verhindert die Bildung der OSPF-Adjacency. Nach der Konfiguration der OSPF-Router-ID erstellt das Leaf in der ACI-Fabric ein Loopback mit der Router-ID-IP-Adresse. Da diese Adresse für Loopback verwendet wird, darf sie sich nicht mit der Schnittstellen-IP überschneiden, da sie fehlschlägt.
In diesem Beispiel können Sie überprüfen, ob die Router-ID des Nachbargeräts falsch konfiguriert wurde.

Navigieren Sie über die ACI-GUI zu Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Configured Nodes > topology/pod-Y/node-X.



die Router-ID vom Nachbargerät falsch konfiguriert wurde.

Aus dem Randblatt:

<#root>

```
[+] Check OSPF interfaces associated with the VRF
BL-301# show ip int bri vrf  abc1:vrf-1
IP Interface Status for VRF "abc1:vrf-1"(137)
Interface            Address              Interface Status
vlan1                192.0.2.1/24         protocol-up/link-up/admin-up
lo9
```

172.16.0.1

```
/32       protocol-up/link-up/admin-up

[+] Capture a single packet TCPDUMP for local BL OSPF IP
BL-301# tcpdump src host 192.0.2.1 -vv -e -i kpm_inb -c 1
    192.0.2.1 > ospf-all.mcast.net: OSPFv2, Hello, length 44
```

Router-ID

172.16.0.1

```
, Backbone Area, Authentication Type: none (0)
        Options [External]
          Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1

[+] Capture a single OSPF hello packet using TCPDUMP coming from external device OSPF IP
BL-301# tcpdump src host 192.0.2.50 -vv -e -i kpm_inb -c 1
    192.0.2.50 > ospf-all.mcast.net: OSPFv2, Hello, length 48
```

Router-ID

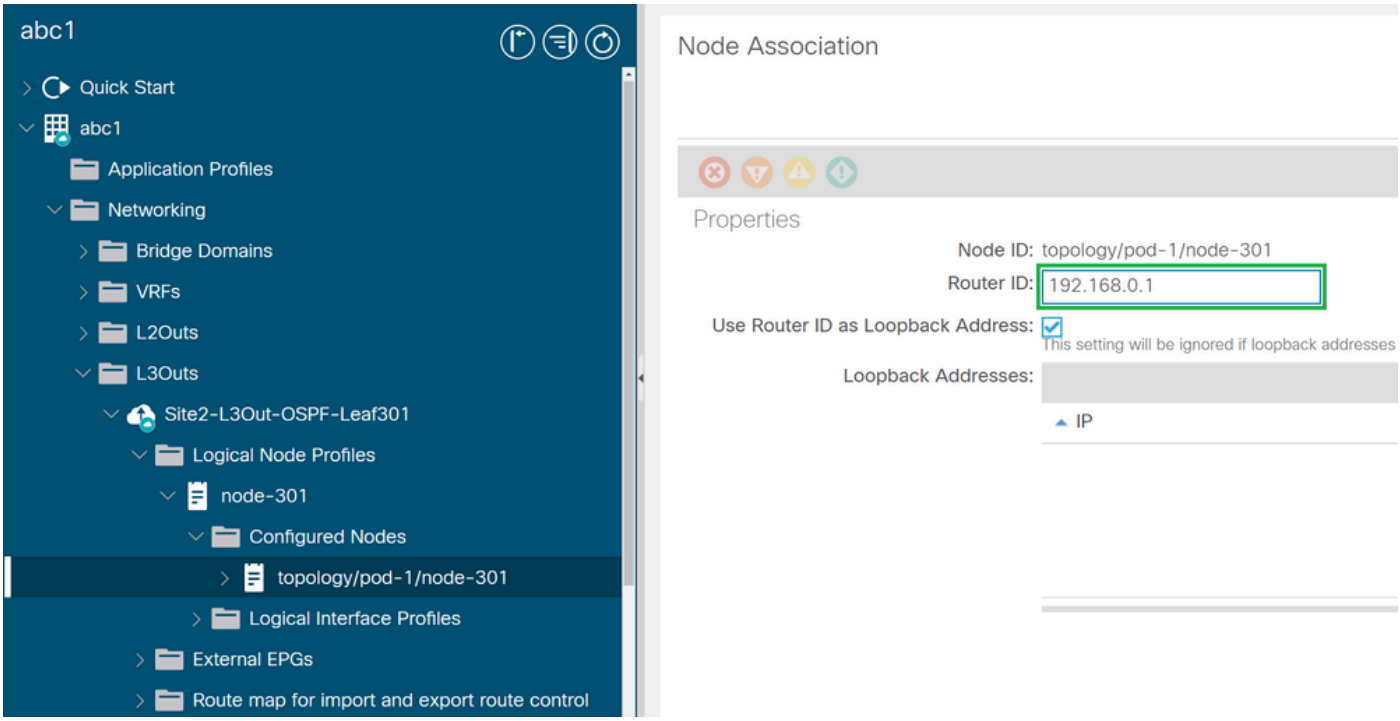
172.16.0.1

```
, Backbone Area, Authentication Type: none (0)
        Options [External]
          Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
```

Von externem Gerät

```
NX-OS# show logging log | tail -n 100 | grep ospf-bootcamp
2024 Jan  4 13:55:36 NX-OS %OSPF-4-DUPRID:  ospf-bootcamp [22263] (301-l3-abc1) Router 192.0.2.1 on int
```

Lösung: Verwenden Sie für beide Geräte unterschiedliche Router-IDs.



Verwendung unterschiedlicher Router-IDs auf beiden Geräten

Fehlerbehebung der OSPF-Adjacency: MTU-Diskrepanz

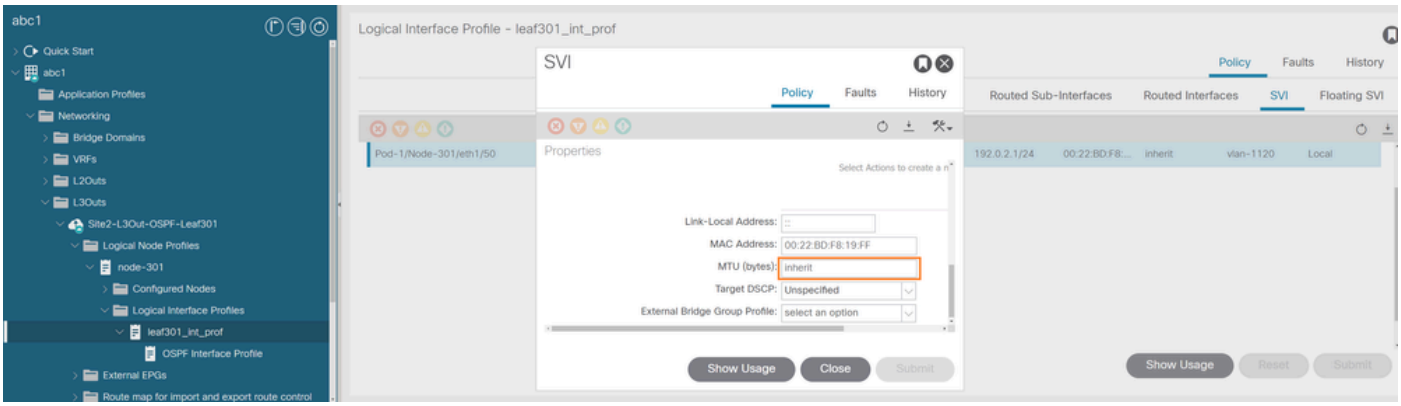
Nachdem zwei benachbarte OSPF-Router eine bidirektionale Kommunikation eingerichtet und die Auswahl von Designated Router (DR)/BDR

(in Broadcast-Netzwerken) abgeschlossen haben, wechseln die Router in den Exstart-Status. In diesem Zustand stellen die benachbarten Router eine Aktiv/Standby-Beziehung her und bestimmen die Sequenznummer des ursprünglichen Datenbankdeskriptors (DBD), die beim Austausch von DBD-Paketen verwendet werden soll.

Sobald die Aktiv/Standby-Beziehung ausgehandelt wurde (der Router mit der höchsten Router-ID wird zum aktiven Router), wechseln die benachbarten Router in den Austauschstatus. In diesem Zustand tauschen die Router DBD-Pakete aus, die ihre gesamte Link-State-Datenbank beschreiben. Die Router senden außerdem Link-State-Anforderungspakete, die aktuellere Link-State-Advertisements (LSAs) von Nachbarn anfordern.

Wenn die MTU-Einstellungen für benachbarte Router-Schnittstellen nicht übereinstimmen, bleiben die Router im Exstart-/Exchange-Status stecken. Der Grund hierfür ist, dass der Router mit der höheren MTU ein Paket sendet, das größer ist als die auf dem benachbarten Router festgelegte MTU, sodass der benachbarte Router das Paket ignoriert.

Navigieren Sie in der APIC-GUI-Konfiguration mit der Standard-Vererbungskonfiguration zu Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile.



Standardmäßig setzt die ACI-Fabric die Layer-3-Schnittstellen-MTU auf 9.000 anstatt auf 1.500.

Standardmäßig legt die ACI-Fabric die Layer-3-Schnittstellen-MTU auf 9.000 anstatt auf 1.500 fest. Da die ACI eine höhere MTU aufweist, akzeptiert sie weiterhin die DBD-Pakete vom externen Router und versucht, sie zu bestätigen.

Wenn der externe Router eine niedrigere oder höhere MTU hat, ignoriert er die DBD-Pakete zusammen mit ACK von der ACI, sendet das ursprüngliche DBD-Paket weiter und bleibt im Exstart-/Exchange-Status.

Aus dem Randblatt:

<#root>

[+]From the border Leaf we can identify the state of the neighborship relation
BL-301# show ip ospf neighbors vrf abc1:vrf-1
OSPF Process ID default VRF abc1:vrf-1
Total number of neighbors: 1
Neighbor ID Pri State Up Time Address Interface
172.16.0.1 1

EXCHANGE

/ - 01:10:05 192.0.2.50

Vlan1

[+] You can check the associated faults to the Tenant:VRF / OSPF interface
BL-301# moquery -c faultInst -x 'query-target-filter=wcard(faultInst.dn,"

abc1:vrf-1

\/if-\[

vlan1

\]")' | egrep "code|rule|dn|descr|lastTransition"
code   :

F1385

descr   :

OSPF adjacency is not full, current state Exchange

dn   : topology/pod-1/node-301/sys/ospf/inst-default/dom-abc1:vrf-1/if-[vlan1]/adj-172.16.0
lastTransition   : 2023-12-28T12:26:23.369-05:00
rule   : ospf-adj-ep-failed
title   : OSPF Adjacency Down

code   :

F3592

descr   :

OSPF interface vlan1 mtu is different than neighbor mtu

dn   : topology/pod-1/node-301/sys/ospf/inst-default/dom-abc1:vrf-1/if-[vlan1]/fault-F3592
lastTransition   : 2023-12-28T12:26:23.369-05:00
rule   : ospf-if-mtu-config-mismatch-err

[+] Identify the MTU applied on the OSPF interface
BL-301# show int vlan 1 | egrep "MTU"

MTU

9000

 bytes, BW 10000000 Kbit, DLY 1 usec

[+] If the default configuration is on place there will be a missmatch with the 1500 default
BL-301# show ip ospf event-history adjacency | grep "neighbor mtu"
2023-12-28T12:24:31.986149000-05:00 ospf default [20751]: TID 21885:ospfv2_check_ddesc_for_nbr_state:49

neighbor mtu [

1500] is smaller than if mtu 9000

[+] Or if the locally configured MTU is lower tham external router
[2023-12-28T14:05:48.495659000-05:00:T:ospfv2_check_ddesc_for_nbr_state:478] abc1:vrf-1DBD from 192.0.2

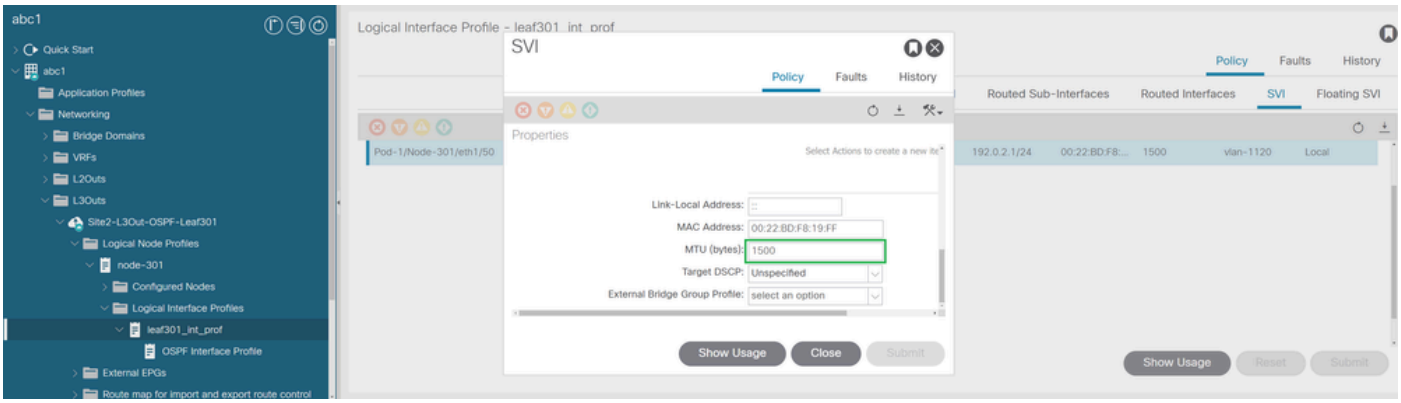
mtu [1500] is large than if mtu 1200

Mögliche Lösungen:

- MTU auf beiden Geräten anpassen

Wenn eine MTU auf einer der beiden Seiten geändert wird, bleibt sie bis zur nächsten Aushandlung unverändert, da die Mitgliedschaft bereits besteht. Sie kann aus mehreren Gründen ausgelöst werden. Beispiel: physische Schnittstelle ausgefallen, Neubereitstellung von Richtlinien, Leaf-Neuladen, Upgrade usw.

Navigieren Sie Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile wie im Bild dargestellt zu.



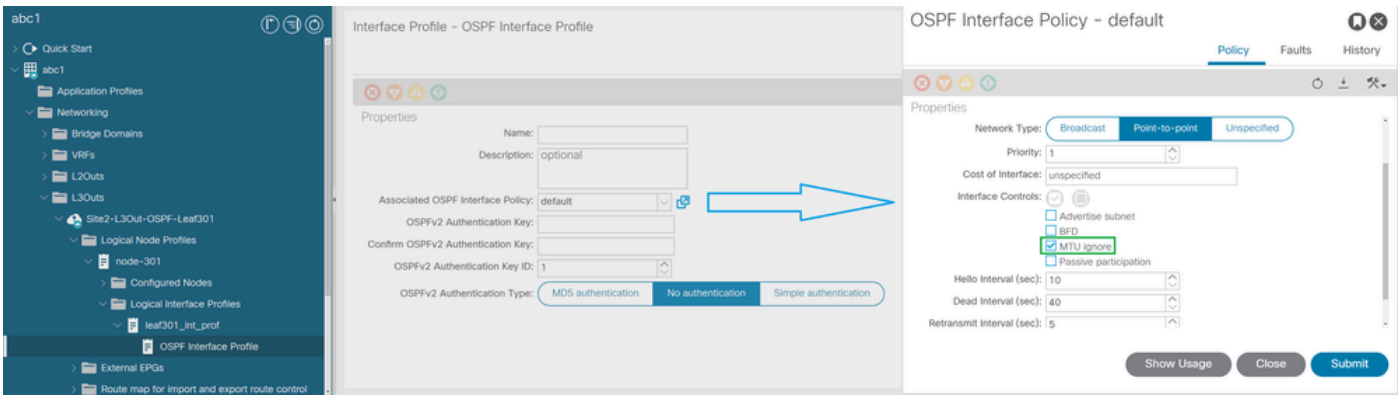
MTU auf 1500 konfiguriert

- Die MTU-Ignorierung in der Richtlinie für die zugeordnete OSPF-Schnittstelle stellt die Verbindung wieder her.

Das Problem mit der MTU-Ignorierung kann auftreten, wenn die OSPF-Datenbank wächst. Wenn sich die MTUs nur um einige Byte unterscheiden, kann die Einrichtung eine lange Zeit dauern, bis Sie über die richtige Kombination von LSAs stolpern, die das DBD generieren oder ein Paket mit der richtigen Größe aktualisieren.

Die Tests in einer kleinen Übung funktionieren einwandfrei, aber das Produktionsnetzwerk kann unerwartete Verhaltensweisen feststellen.

Navigieren Sie Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile > Associated OSPF Interface Policy wie im Bild dargestellt zu.



MTU-Ignorierungskonfiguration

Fehlerbehebung der OSPF-Adjacency: Authentication Mismatch

Sie können die Authentifizierung in OSPF aktivieren, um Routing-Aktualisierungsinformationen sicher auszutauschen. Die OSPF-Authentifizierung kann none (oder null), simple (Einfach) oder MD5 sein. Die Authentifizierungsmethode "none" bedeutet, dass keine Authentifizierung für OSPF verwendet wird und dass es sich um die Standardmethode handelt. Bei der einfachen Authentifizierung wird das Passwort im Klartext über das Netzwerk übertragen. Bei MD5-Authentifizierung wird das Kennwort nicht über das Netzwerk weitergeleitet.

Dies sind die drei verschiedenen Authentifizierungstypen, die von OSPF unterstützt werden.

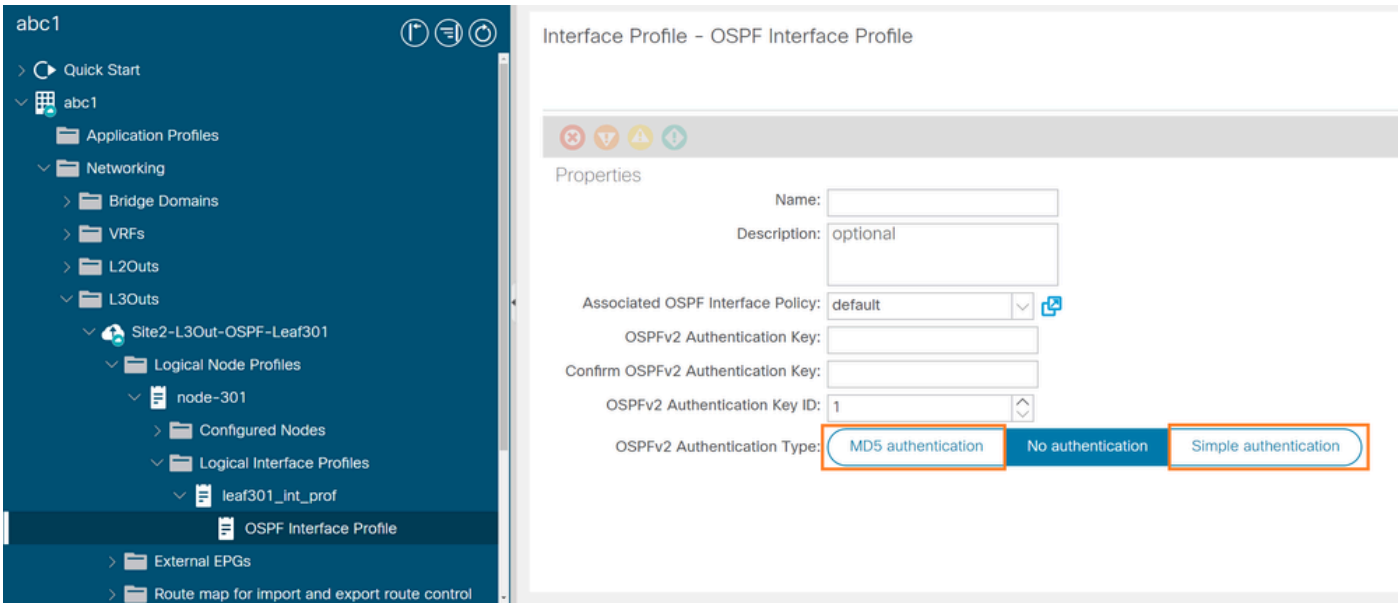
Null-Authentifizierung - Dies wird auch als Typ 0 bezeichnet und bedeutet, dass im Paket-Header keine Authentifizierungsinformationen enthalten sind. Dies ist die Standardeinstellung.

Einfache Authentifizierung - Dies wird auch als Typ 1 bezeichnet und verwendet einfache unverschlüsselte Kennwörter.

MD5-Authentifizierung - Dies wird auch als Typ 2 bezeichnet und verwendet kryptografische MD5-Kennwörter.

Die Authentifizierung muss nicht festgelegt werden. Wenn sie jedoch festgelegt ist, müssen alle Peer-Router im gleichen Segment über das gleiche Kennwort und die gleiche Authentifizierungsmethode verfügen.

Navigieren Sie in der ACI-GUI zu, Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile wie im Bild dargestellt.



Konfiguration von MD5 oder einfachen Authentifizierungen

Aus CLI:

<#root>

```
[+] Check Authentication type configured
APIC# moquery -c ospfIfP -x 'query-target-filter=wcard(ospfIfP.dn,"tn-abc1\/out-Site2-L3Out-OSPF-BL-301
```

```
authType     :
```

simple

```
[+] Capture a single packet TCPDUMP for local BL OSPF IP
BL-301# tcpdump src host 192.0.2.1 -vv -e -i kpm_inb -c 1
    192.0.2.1 > ospf-all.mcast.net: OSPFv2, Hello, length 44
        Router-ID 192.168.0.1, Backbone Area, Authentication Type:
```

simple (

1)

```
        Simple text password: cisco
        Options [External]
          Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
or

[+] Check Authentication type configured
APIC# moquery -c ospfIfP -x 'query-target-filter=wcard(ospfIfP.dn,"tn-abc1\/out-Site2-L3Out-OSPF-BL-301
authType     :
```

md5

```
[+] Capture a single packet TCPDUMP for local BL OSPF IP
```

```
BL-301# tcpdump src host 192.0.2.1 -vv -e -i kpm_inb -c 1
192.0.2.1 > ospf-all.mcast.net: OSPFv2, Hello, length 44
        Router-ID 192.168.0.1, Backbone Area, Authentication Type:
```

MD5 (2)

```
        Key-ID: 1, Auth-Length: 16, Crypto Sequence Number: 0x026c0a34
        Options [External]
          Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
```

```
[+] Capture a single OSPF hello packet using TCPDUMP coming from external device OSPF IP
BL-301# tcpdump src host 192.0.2.50 -vv -e -i kpm_inb -c 1
    192.0.2.50 > ospf-all.mcast.net: OSPFv2, Hello, length 48
     Router-ID 172.16.0.1, Backbone Area, Authentication Type:
```

none (0)

```
        Options [External]
          Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1

[+] Live OSPF trace Decode for VRF
BL-301# log_trace_bl_print_tool /var/sysmgr/tmp_logs/ospfv2_1_trace.bl | tail -n 250 | grep abc1:vrf-1
[2024-01-04T16:23:29.650806000-05:00:T:ospfv2_set_authentication:70] abc1:vrf-1out pkt on Vlan1:
```

auth simple text: key cisco

```
or
[2024-01-04T16:24:22.794682000-05:00:T:ospfv2_set_authentication:96] abc1:vrf-1out pkt on Vlan1:
```

auth md5: key cisco

```
, key id 1 Seq 40635829 (time 1704403462)
```

Von externem Gerät:

```
NX-OS#  show logging log | tail -n 100 | grep ospf-bootcamp
2024 Jan  4 16:55:01 NX-OS %OSPF-4-AUTH_ERR:  ospf-bootcamp [22263] (301-l3-abc1) Received packet from
or
2024 Jan  4 16:55:20 NX-OS %OSPF-4-AUTH_ERR:  ospf-bootcamp [22263] (301-l3-abc1) Received packet from
```

Lösung: Authentifizierungen abgleichen.

Fehlerbehebung der OSPF-Adjacency: Hello/Dead Timer Mismatch

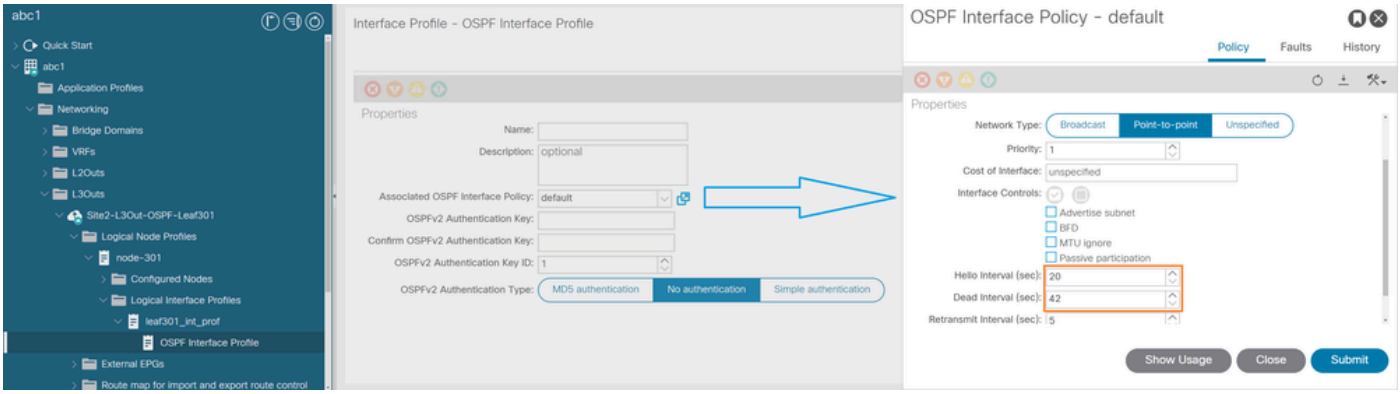
OSPF-Hello-Pakete sind Pakete, die ein OSPF-Prozess an seine OSPF-Nachbarn sendet, um die Verbindung mit diesen Nachbarn aufrechtzuerhalten. Die Hello-Pakete werden in einem konfigurierbaren Intervall (in Sekunden) gesendet. Die Standardeinstellung ist 10 Sekunden für eine Ethernet-Verbindung (für P2P und Broadcast Network Type). Hello-Pakete enthalten eine Liste aller Nachbarn, für die innerhalb des Dead-Intervalls ein Hello-Paket empfangen wurde. Das Ausfallintervall kann ebenfalls konfiguriert werden (in Sekunden) und ist standardmäßig auf das Vierfache des Hello-Intervalls festgelegt. Der Wert aller Hello-Intervalle muss innerhalb eines Netzwerks gleich sein. Ebenso muss der Wert aller Dead-Intervalle innerhalb eines Netzwerks gleich sein.

Diese beiden Intervalle arbeiten zusammen, um die Verbindung aufrechtzuerhalten, indem sie anzeigen, dass die Verbindung betriebsbereit ist. Wenn ein Router innerhalb des Dead-Intervalls kein Hello-Paket von einem Nachbarn empfängt, wird dieser Nachbarn als ausgefallen deklariert.

Wenn die standardmäßigen OSPF-Hello- und Dead-Timer in der ACI-Fabric geändert werden, müssen sie mit dem externen Router

übereinstimmen.

Navigieren Sie in der ACI-GUI zu, Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile > Associated OSPF Interface Policy wie im Bild dargestellt.



Benutzerdefinierte Hello-/Dead-Timer

Aus dem Randblatt:

<#root>

```
[+] Check OSPF interface configuration
BL-301# show ip ospf interface vlan 1 | egrep "Timer|Network"
State P2P, Network type P2P, cost 4
Timer intervals: Hello
```

20

```
, Dead
```

42

```
, Wait 42, Retransmit 5
```

```
Or
```

```
BL-301# moquery -c ospfIf -x 'query-target-filter=wcard(ospfIf.id,"vlan1")' | egrep "deadIntvl|helloInt
```

deadIntvl   : 42

helloIntvl   : 20

nwT   : p2p

Or

```
APIC# moquery -c ospfRsIfPol -x 'query-target-filter=wcard(ospfIfP.dn,"abc1\/out-Site2-L3Out-OSPF-BL-30
tnOspfIfPolName  : Custom_OSPF_Interface_Policy

APIC# moquery -c ospfIfPol -x 'query-target-filter=wcard(ospfIfPol.name,"Custom_OSPF_Interface_Policy")
deadIntvl    :
```

42

helloIntvl   :

2

0

nwT   : p2p

```
[+] Capture a single packet TCPDUMP for local BL OSPF IP
BL-301# tcpdump src host 192.0.2.1 -vv -e -i kpm_inb -c 1
192.0.2.1 > ospf-all.mcast.net: OSPFv2, Hello, length 44
        Router-ID 192.168.0.1, Backbone Area, Authentication Type: none (0)
        Options [External]
```

Hello Timer 20s

,

Dead Timer 42s

, Mask 255.255.255.0, Priority 1

[+] Capture a single OSPF hello packet using TCPDUMP coming from external device OSPF IP
BL-301# tcpdump src host 192.0.2.50 -vv -e -i kpm_inb -c 1
192.0.2.50 > ospf-all.mcast.net: OSPFv2, Hello, length 44
        Router-ID 172.16.0.1, Backbone Area, Authentication Type: none (0)
        Options [External]

Hello Timer 10s

,

Dead Timer 40s

, Mask 255.255.255.0, Priority 1

Von externem Gerät:

<#root>

```
[+] Check OSPF interfaces con vrf
NX-OS# show ip int bri vrf 301-l3-abc1
IP Interface Status for VRF "301-l3-abc1"(21)
Interface            IP Address      Interface Status
Lo1001               110.1.0.1       protocol-up/link-up/admin-up
Eth1/2.1120          192.0.2.50      protocol-up/link-up/admin-up

[+] Check OSPF configuration by default Dead timer on NX-OS devices is 4 times hello interval
NX-OS# show run ospf all | section Ethernet1/2.1120 | grep hello
```

ip ospf hello-interval

10

```
[+] Check OSPF interface advertized parameters
NX-OS# show ip ospf interface Ethernet1/2.1120 | grep Timer
    Timer intervals:
```

Hello

10

,

Dead

40

, Wait 40, Retransmit 5

Lösung: Übereinstimmung mit OSPF-Timern

Fehlerbehebung der OSPF-Adjacency: Interface Type Mismatch

In diesem Abschnitt wird die Fehlerbehebung beschrieben, wenn auf der ACI "Broadcast" oder "Unspecified" konfiguriert ist und das externe Gerät den Status P2P hat.

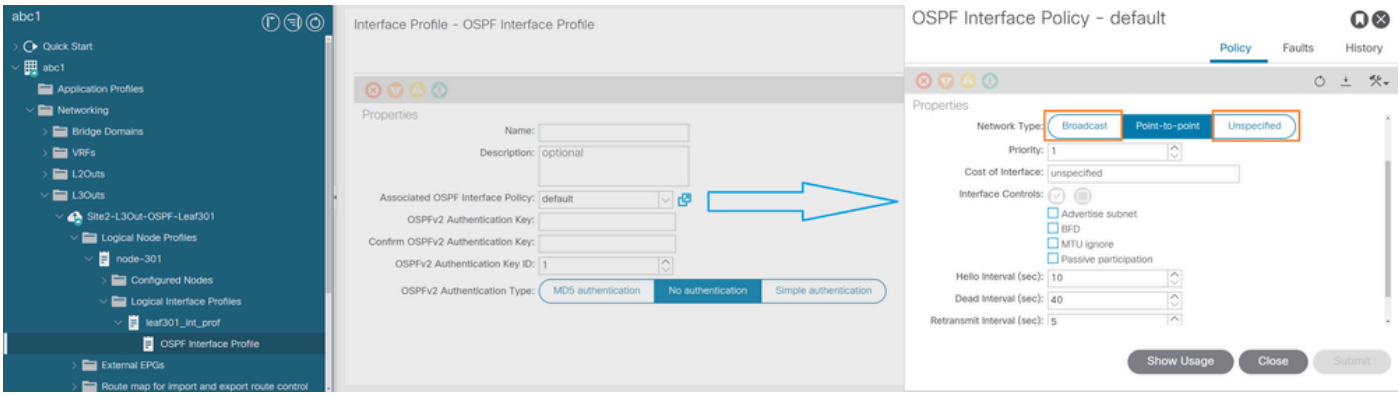
Senden

- Der Broadcast-Netzwerktyp ist der Standard für eine OSPF-fähige Ethernet-Schnittstelle.
- Für den Broadcast-Netzwerktyp muss eine Verbindung Layer-2-Broadcast-Funktionen unterstützen.
- Der Broadcast-Netzwerktyp verfügt über einen 10-sekündigen Hello- und 40-sekündigen Dead-Timer (identisch mit P2P).
- Für einen OSPF-Broadcast-Netzwerktyp muss ein DR/BDR verwendet werden.

Point-to-Point

- Ein P2P OSPF-Netzwerktyp unterhält keine DR/BDR-Beziehung.
- Der P2P-Netzwerktyp verfügt über einen 10-Sekunden-Hello- und einen 40-Sekunden-Dead-Timer.
- P2P-Netzwerktypen sollen zwischen zwei direkt verbundenen Routern verwendet werden.

Navigieren Sie in der ACI-GUI zu, Fabric > Tenants > Networking > L3Outs > "L3outName" > "Node-X" > Logical Interface Profiles > OSPF Interface Profile > Associated OSPF Interface Policy wie im Bild dargestellt.



Broadcast- oder nicht spezifizierter Netzwerktyp konfiguriert

Aus dem Randblatt:

<#root>

```
[+] Check OSPF neighborship relation
BL-301# show ip ospf neighbors vrf abc1:vrf-1
 OSPF Process ID default VRF abc1:vrf-1
 Total number of neighbors: 1
 Neighbor ID     Pri State            Up Time  Address         Interface
 172.16.0.1        1
```

INITIALIZING/DROTHER

```
 00:06:42 192.0.2.50      Vlan1

[+] Check OSPF interface configuration
BL-301# moquery -c ospfIf -x 'query-target-filter=wcard(ospfIf.id,"vlan1")' | egrep "deadIntvl|helloInt
deadIntvl    : 40
helloIntvl   : 10
nwT          :
```

bcast

or

```
BL-301# moquery -c ospfIf -x 'query-target-filter=wcard(ospfIf.id,"vlan1")' | egrep "deadIntvl|helloInt
deadIntvl    : 40
```

```
helloIntvl   : 10
nwT          :
```

unspecified

Or

```
APIC# moquery -c ospfRsIfPol -x 'query-target-filter=wcard(ospfIfP.dn,"abc1\/out-Site2-L3Out-OSPF-BL-30
tnOspfIfPolName  : Custom_OSPF_Interface_Policy

APIC# moquery -c ospfIfPol -x 'query-target-filter=wcard(ospfIfPol.name,"Custom_OSPF_Interface_Policy")
deadIntvl    : 40
helloIntvl   : 10
nwT          :
```

bcast

```
APIC# moquery -c ospfIfPol -x 'query-target-filter=wcard(ospfIfPol.name,"Custom_OSPF_Interface_Policy")
deadIntvl    : 40
helloIntvl   : 10
nwT          :
```

unspecified

```
[+] Whether it is bcast or unspecified the interface will show as Broadcast
BL-301#  show ip ospf interface vlan 1 | egrep "Timer|Network"
    State DR, Network type
```

BROADCAST

```
, cost 4
    Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5

[+] Capture a single packet TCPDUMP for local BL OSPF IP
BL-301# tcpdump src host 192.0.2.1 -vv -e -i kpm_inb -c 1
192.0.2.1 > ospf-all.mcast.net: OSPFv2, Hello, length 48
        Router-ID 192.168.0.1, Backbone Area, Authentication Type: none (0)
        Options [External]
          Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
```

Designated Router

192.0.2.1

```
          Neighbor List:
            172.16.0.1

[+] Capture a single OSPF hello packet using TCPDUMP coming from external device OSPF IP
BL-301# tcpdump src host 192.0.2.50 -vv -e -i kpm_inb -c 1
192.0.2.50 > ospf-all.mcast.net: OSPFv2, Hello, length 44
        Router-ID 172.16.0.1, Backbone Area, Authentication Type: none (0)
        Options [External]
          Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
```

Von externem Gerät:

<#root>

```
[+] Check OSPF interfaces con vrf
NX-OS# show ip int bri vrf 301-l3-abc1
IP Interface Status for VRF "301-l3-abc1"(21)
Interface            IP Address      Interface Status
Lo1001               110.1.0.1       protocol-up/link-up/admin-up
Eth1/2.1120          192.0.2.50      protocol-up/link-up/admin-up

[+] Check OSPF configuration by default Dead timer on NX-OS devices is 4 times hello interval
NX-OS# show run ospf all | section Ethernet1/2 | grep network
  ip ospf network
```

point-to-point

```
[+] Check OSPF interface advertized parameters
NX-OS# show ip ospf interface Ethernet1/2 | grep type
    State P2P, Network type
```

P2P

```
, cost 1
```

Überprüfungsbefehl - Cheatsheet

Auf diese Befehle wurde in diesem Dokument Bezug genommen, um die verschiedenen Szenarien zu beheben.

Knoten	Befehle	Zweck
ACI-Switch	show ip ospf neighbors vrf <<TNT:VRF>>	Überprüfen der Nachbarschaftsbeziehung auf VRF
	show ip ospf interface brief vrf <<TNT:VRF>>	Überprüfung der mit der VRF-Instanz verbundenen OSPF-Schnittstellen
	moquery -c faultInst -x 'query-target-filter=wcard(faultInst.dn,"<<TNT:VRF>>")'	Sie können die zugehörigen Fehler der VRF-Instanz überprüfen.
	moquery -c ospfIf -x 'query-target-filter=wcard(ospfIf.dn,"<<TNT:VRF>>")'	Überprüfen Sie alle mit der VRF-Instanz verknüpften OSPF-Schnittstellendetails.

	moquery -c ospfIf -x 'query-target-filter=wcard(ospfIf.id,"<<vlanX>>")'	Überprüfen der OSPF-Schnittstellenkonfiguration
	moquery -c arpAdjEp -x 'query-target-filter=wcard(arpAdjEp.ifId,"<<vlanX>>")' | grep ip	Überprüfen Sie die IP-Adresse des externen Geräts von dem mit der Schnittstelle verknüpften ARP.
	log_trace_bl_print_tool /var/sysmgr/tmp_logs/ospfv2_1_trace.bl | tail -n 250 | grep <<TNT:VRF>>	Live-OSPF-Trace-Dekodierung für VRF
	tcpdump -i kpm_inb proto ospf -vv -e -w - | tee /data/techsupport/Node-XXX_OSPF.pcap | tcpdump -r - host any	Erfassung von OSPF-Datenverkehr für die Analyse in Wireshark
	tcpdump -i kpm_inb proto ospf -vv -e -w - | tee /data/techsupport/Node-XXX_OSPF_HOST.pcap | tcpdump -r - host <<X.X.X.X>>	Erfassung von spezifischem Datenverkehr von HOST zur Analyse von Wireshark
	tcpdump -xxxvi kpm_inb 'proto ospf and (host <<X.X.X.X>> or host <<Y.Y.Y.Y>>)' -w /data/techsupport/Node-XXX_OSPF_HOST.pcap	Erfassung von SRC- und DST-spezifischem Datenverkehr von HOST zur Analyse von Wireshark
	tcpdump src host <<X.X.X.X>> -vv -e -i kpm_inb -c 1	Erfassung einer In-Band-Kontrollebene für einen bestimmten Host
ACI-APIC	moquery -c ospfIfP -x 'query-target-filter=wcard(ospfIfP.dn,"<<TNT>>\/out-<<L3outName>>")'	Überprüfen Sie den konfigurierten Authentifizierungstyp.
	moquery -c l3ext.RsPathL3OutAtt -x 'query-target-filter=wcard(l3extRsPathL3OutAtt.dn,"<<TNT>>\/out-<<L3outName>>")'	Konfiguration des L3out-Pfads überprüfen
	moquery -c faultRecord -f 'fault.Inst.code=="F1385"' -x 'query-target-filter=wcard(faultRecord.dn,"<<TNT:VRF>>")'	Überprüfen Sie die Fehlerverlaufsdatensätze auf Fehler F1385 protocol-ospf-adjacency-

		down.
	moquery -c ospfRsIfPol -x 'query-target-filter=wcard(ospfIfP.dn,"<<TNT>>\/out-<<L3outName>>")' | grep tnOspfIfPolName	Überprüfen Sie L3out auf benutzerdefinierte Richtlinie für zugeordnete OSPF-Schnittstellen.
	moquery -c ospfIfPol -x 'query-target-filter=wcard(ospfIfPol.name,"Custom_OSPF_Interface_Policy")'	Überprüfen Sie, ob benutzerdefinierte Details für die zugeordnete OSPF-Schnittstellenrichtlinie vorliegen.
NX-Switch	show ip int bri vrf <<VRF>>	OSPF-Schnittstellen mit VRF überprüfen
	show run ospf all | section EthernetX/Y	OSPF-Konfiguration überprüfen
	show ip ospf interface EthernetX/Y	Überprüfen der über die OSPF-Schnittstelle gemeldeten Parameter

Zugehörige Informationen

- Fehlerbehebung: ACI External Forwarding
- Technischer Support und Downloads von Cisco

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.