# Kenntnis der Erweiterungen bei Virtual Port Channel (vPC)

## Inhalt

# Einleitung

In diesem Dokument werden häufige Verbesserungen für Virtual Port Channel (vPC) beschrieben, die auf Cisco Nexus-Switches in einer vPC-Domäne konfiguriert wurden.

# Voraussetzungen

## Anforderungen

Cisco empfiehlt, dass Sie mit grundlegenden Informationen zu Anwendungsfall, Konfiguration und Implementierung von Virtual Port Channel (vPC) vertraut sind. Weitere Informationen zu dieser Funktion finden Sie in einem der folgenden Dokumente:

- Konfigurationshandbuch für Cisco Nexus NX-OS-Schnittstellen der Serie 9000, Version 10.1(x)
- Konfigurationsleitfaden für Cisco Nexus NX-OS-Schnittstellen der Serie 9000, Version 9.3(x)
- Konfigurationsleitfaden für Cisco Nexus NX-OS-Schnittstellen der Serie 9000, Version 9.2(x)
- Konfigurationsleitfaden für Cisco Nexus NX-OS-Schnittstellen der Serie 9000, Version 7.x
- Konfigurationsleitfaden für Cisco Nexus 7000 NX-OS-Schnittstellen 8.x
- Konfigurationsleitfaden für Cisco Nexus 7000 NX-OS-Schnittstellen 7.x
- Design- und Konfigurationsleitfaden: Best Practices für Virtual Port Channels (vPC) auf Cisco Nexus Switches der Serie 7000

## Verwendete Komponenten

Die Informationen in diesem Dokument stammen von Geräten in einer bestimmten Laborumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

# Hintergrundinformationen

Seit der Einführung von Cisco NX-OS auf Cisco Nexus-Switches für Rechenzentren wurden zahlreiche Verbesserungen an der Funktion Virtual Port Channel (vPC) vorgenommen, die die Zuverlässigkeit von mit vPC verbundenen Geräten bei Ausfällen verbessern und das Weiterleitungsverhalten beider vPC-Peer-Switches optimieren. Wenn Sie den Zweck jeder Erweiterung, die Verhaltensänderung, die durch die Erweiterung eingeführt wird, und die Fehlerszenarien, die durch die Verbesserung gelöst werden, verstehen, warum und wann eine

Verbesserung in einer vPC-Domäne konfiguriert werden sollte, um die geschäftlichen Anforderungen am besten zu erfüllen.

### Anwendbare Hardware

Das in diesem Dokument beschriebene Verfahren gilt für alle vPC-fähigen Cisco Nexus-Rechenzentrums-Switches.

## vPC-Peer-Switch

In diesem Abschnitt wird die Erweiterung des vPC-Peer-Switches beschrieben, die mit dem Konfigurationsbefehl für die vPC-Domäne des **Peer-Switches** aktiviert wird.

### Überblick

In vielen Umgebungen bilden zwei Nexus Switches in einer vPC-Domäne Aggregations- oder Core-Switches die Grenze zwischen Layer-2-Switched-Ethernet-Domänen und Layer-3-Routing-Domänen. Beide Switches werden mit mehreren VLANs konfiguriert und sind für das Routing des Ost-West- und des Nord-Süd-Datenverkehrs zwischen den VLANs zuständig. In diesen Umgebungen fungieren die Nexus Switches in der Regel auch als Root Bridges aus Sicht des Spanning Tree Protocol.

Normalerweise wird ein vPC-Peer als Root-Bridge des Spanning Tree konfiguriert, indem die Spanning Tree-Priorität auf einen niedrigen Wert, z. B. 0, gesetzt wird. Der andere vPC-Peer ist mit einer etwas höheren Spanning Tree-Priorität konfiguriert, z. B. 4096. Dadurch kann er die Rolle einer Root-Bridge innerhalb des Spanning Tree übernehmen, wenn der vPC-Peer bei einem Ausfall der Root-Bridge agiert. Bei dieser Konfiguration stammt der vPC-Peer, der als Root-Bridge fungiert, von Spanning Tree Bridge Protocol Data Units (BPDUs) mit einer Bridge-ID, die die System-MAC-Adresse enthält.

Wenn jedoch der als Root-Bridge fungierende vPC-Peer ausfällt und den anderen vPC-Peer als Spanning Tree-Root-Bridge übernimmt, generiert der andere vPC-Peer Spanning Tree-BPDUs mit einer Bridge-ID, die seine System-MAC-Adresse enthält, die sich von der System-MAC-Adresse der ursprünglichen Root-Bridge unterscheidet. Je nachdem, wie Downstream-Brücken verbunden sind, variieren die Auswirkungen dieser Änderung und werden in den folgenden Unterabschnitten beschrieben.

#### Redundant verbundene Nicht-vPC-Bridges

Bridges ohne vPC-Verbindung, die mit beiden vPC-Peers über redundante Verbindungen verbunden sind (sodass sich eine Verbindung aus Sicht des Spanning Tree Protocol im Blockierungsstatus befindet), die die Änderung der BPDU (und damit die Änderung der Root-Bridge) erkennen und eine Änderung des Root-Ports beobachten. Andere designierte Weiterleitungsschnittstellen wechseln sofort in den Blockierungsstatus und durchlaufen dann den endlichen Spanning Tree Protocol-Computer (Blockieren, Lernen und Weiterleiten) mit Pausen dazwischen, die dem konfigurierten Spanning Tree Protocol Forward Delay-Timer entsprechen (standardmäßig 15 Sekunden).

Die Änderung des Root-Ports und das anschließende Durchlaufen des endlichen Spanning Tree Protocol-Systems können zu erheblichen Unterbrechungen im Netzwerk führen. Die vPC-Peer-

Switch-Erweiterung wurde in erster Linie eingeführt, um Netzwerkstörungen zu vermeiden, die durch dieses Problem verursacht werden, wenn einer der vPC-Peers offline gehen sollte. Mit der Erweiterung für den vPC-Peer-Switch verfügt die Bridge ohne vPC-Verbindung weiterhin über eine einzelne redundante Verbindung im Blockierungsstatus, wechselt diese Schnittstelle jedoch sofort in den Weiterleitungsstatus, wenn der bestehende Root-Port aufgrund eines Verbindungsfehlers ausfällt. Derselbe Prozess findet statt, wenn der vPC-Peer offline wieder online geht: Die Schnittstelle mit den niedrigsten Kosten für die Root-Bridge übernimmt die Rolle des Root-Ports, und die redundante Verbindung wechselt sofort in den Blockierungsstatus. Der einzige zu beobachtende Effekt auf Datenebene ist der unvermeidliche Verlust übertragener Pakete, die den vPC-Peer durchlaufen haben, als dieser offline ging.

## Über vPC verbundene Bridges

Mit vPC verbundene Bridges in der Spanning Tree-Domäne erkennen die Änderung in der BPDU (und damit die Änderung in der Root-Bridge) und leeren dynamisch ermittelte MAC-Adressen aus ihren lokalen MAC-Adresstabellen. Dieses Verhalten ist in Topologien mit über vPC verbundenen Geräten, die für eine schleifenfreie Topologie nicht auf das Spanning Tree Protocol angewiesen sind, ineffizient und unnötig. vPCs werden aus Sicht des Spanning Tree Protocol wie normale Port-Channels als eine einzige logische Schnittstelle betrachtet, sodass der Verlust eines vPC-Peers dem Verlust einer einzigen Verbindung innerhalb eines Port-Channel-Mitglieds ähnelt. In beiden Szenarien ändert sich der Spanning Tree nicht, sodass das Leeren dynamisch ermittelter MAC-Adressen von Bridges in der Spanning Tree-Domäne (deren Zweck darin besteht, dem "Flood-and-Learn"-Verhalten von Ethernet das erneute Erlernen von MAC-Adressen an neu weiterleitenden Schnittstellen des Spanning Tree zu ermöglichen) nicht erforderlich ist.

Darüber hinaus kann das Leeren dynamisch ermittelter MAC-Adressen zu Unterbrechungen führen. Stellen Sie sich ein Szenario vor, bei dem zwei Hosts einen weitgehend unidirektionalen UDP-basierten Datenfluss haben (z. B. wenn ein TFTP-Client Daten an einen TFTP-Server sendet). In diesem Fluss fließen die Daten meistens vom TFTP-Client zum TFTP-Server - selten sendet der TFTP-Server ein Paket zurück an den TFTP-Client. Daher wird die MAC-Adresse des TFTP-Servers nach einem Leeren der dynamisch abgefragten MAC-Adressen in der Spanning Tree-Domäne einige Zeit nicht abgefragt. Das bedeutet, dass die Daten des TFTP-Clients, die an den TFTP-Server gesendet werden, über das gesamte VLAN geleitet werden, da der Datenverkehr Unicast-unbekannten Datenverkehr ist. Dies kann dazu führen, dass große Datenflüsse an unbeabsichtigte Stellen im Netzwerk gelangen, und Leistungsprobleme verursachen, wenn sie durch überbelegte Bereiche des Netzwerks fließen.

Die vPC-Peer-Switch-Erweiterung wurde eingeführt, um zu verhindern, dass dieses ineffiziente und unnötige Verhalten auftritt, wenn der vPC-Peer als Spanning Tree-Root-Bridge für ein oder mehrere VLANs neu geladen oder ausgeschaltet wird.

Um die vPC-Peer-Switch-Erweiterung zu aktivieren, müssen beide vPC-Peers über identische Spanning Tree Protocol-Konfigurationen verfügen (einschließlich Spanning Tree-Prioritätswerten für alle vPC-VLANs) und als Root Bridge für mindestens ein vPC-VLAN fungieren. Wenn diese Voraussetzungen erfüllt sind, muss der Befehl für die vPC-Domänenkonfiguration des **Peer-Switches** konfiguriert werden, um die vPC-Peer-Switch-Erweiterung zu aktivieren.

> **Hinweis:** Es wird nicht empfohlen, die vPC Peer Switch-Erweiterung in einer vPC-Domäne zu aktivieren, in der keiner der vPC Peer-Switches die Spanning Tree Protocol Root Bridge für ein oder mehrere vPC-VLANs ist. Sie sollten die vPC Peer Switch-Erweiterung nur aktivieren, wenn einer (oder beide) der vPC Peer Switches die Spanning Tree Protocol Root Bridge für ein oder mehrere vPC-VLANs ist/sind.

Sobald die vPC-Peer-Switch-Erweiterung aktiviert ist, beginnen beide vPC-Peers, identische Spanning Tree-BPDUs mit einer Bridge-ID zu generieren, die die MAC-Adresse des vPC-Systems enthält, die von beiden vPC-Peers gemeinsam verwendet wird. Wenn ein vPC-Peer neu geladen wird, ändert sich die Spanning Tree-BPDU, die vom verbleibenden vPC-Peer stammt, nicht, sodass andere Bridges in der Spanning Tree-Domäne keine Änderung in der Root-Bridge erkennen und nicht suboptimal auf die Änderung im Netzwerk reagieren.

## Hinweise

Die vPC Peer Switch-Erweiterung hat einige Probleme, die Sie vor der Konfiguration in einer Produktionsumgebung berücksichtigen sollten.

### Spanning-Tree-Prioritätswerte müssen zwischen vPC-Peers übereinstimmen

Vor der Aktivierung der vPC-Peer-Switch-Erweiterung muss die Spanning Tree-Prioritätskonfiguration für alle vPC-VLANs so geändert werden, dass sie zwischen beiden vPC-Peers identisch ist.

Betrachten Sie die Konfiguration hier, bei der N9K-1 als Spanning Tree-Root-Bridge für die VLANs 1, 10 und 20 mit der Priorität 0 konfiguriert ist. N9K-2 ist die sekundäre Spanning Tree-Root-Bridge für die VLANs 1, 10 und 20 mit der Priorität 4096.

```
N9K-1# show running-config spanning-tree
spanning-tree vlan 1,10,20 priority 0
interface port-channel1
  spanning-tree port type network

N9K-2# show running-config spanning-tree
spanning-tree vlan 1,10,20 priority 4096
interface port-channel1
  spanning-tree port type network
```

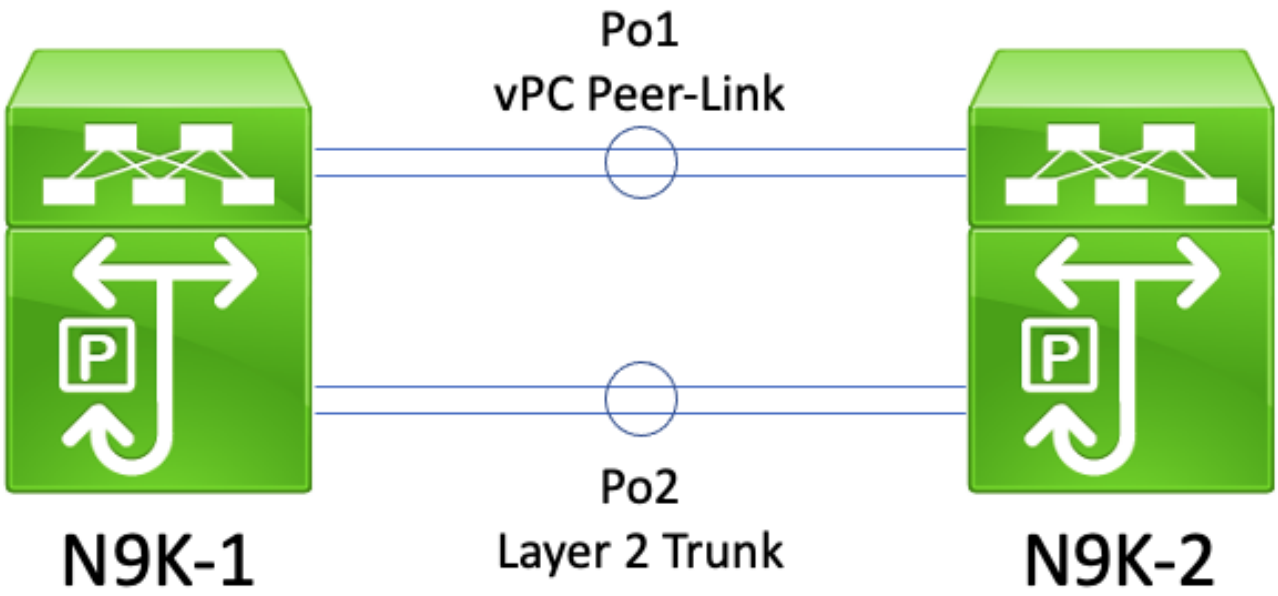
Vor der Aktivierung der vPC Peer Switch-Erweiterung müssen Sie die Spanning Tree-Prioritätskonfiguration für die VLANs 1, 10 und 20 auf N9K-2 ändern, um sie mit der Spanning Tree-Prioritätskonfiguration für dieselben VLANs auf N9K-1 abzustimmen. Ein Beispiel für diese Modifikation ist hier dargestellt.

```
N9K-2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
N9K-2(config)# spanning-tree vlan 1,10,20 priority 0
N9K-2(config)# end
N9K-2# show running-config spanning-tree
spanning-tree vlan 1,10,20 priority 0
interface port-channel1
  spanning-tree port type network

N9K-1# show running-config spanning-tree
spanning-tree vlan 1,10,20 priority 0
interface port-channel1
  spanning-tree port type network
```

### Auswirkungen eines vPC-Peer-Switches auf Nicht-vPC-VLANs

Betrachten Sie die Topologie hier:




In dieser Topologie haben zwei vPC-Peers (N9K-1 und N9K-2) zwei Layer-2-Trunks zwischen sich - Po1 und Po2. Po1 ist der vPC-Peer-Link mit vPC-VLANs, während Po2 ein Layer-2-Trunk mit allen Nicht-vPC-VLANs ist. Wenn die Spanning Tree-Prioritätswerte für Nicht-vPC-VLANs, die über Po2 übertragen werden, auf N9K-1 und N9K-2 identisch sind, stammt jeder vPC-Peer von Spanning Tree-BPDU-Frames, die von der MAC-Adresse des vPC-Systems stammen, die auf beiden Switches identisch ist. Infolgedessen scheint N9K-1 für jedes Nicht-vPC-VLAN seine eigene Spanning Tree-BPDU auf Po2 zu erhalten, obwohl N9K-2 der Switch ist, der die Spanning Tree-BPDU erstellt hat. Aus Sicht von Spanning Tree setzt N9K-1 Po2 für alle Nicht-vPC-VLANs in den Blockierungsstatus.

Dies ist ein erwartungsgemäßes Verhalten. Um dieses Verhalten zu verhindern oder dieses Problem zu umgehen, müssen beide vPC-Peers mit unterschiedlichen Spanning Tree-Prioritätswerten in allen Nicht-vPC-VLANs konfiguriert werden. Auf diese Weise kann ein vPC-Peer als Root-Bridge für das Nicht-vPC-VLAN fungieren und den Layer-2-Trunk zwischen vPC-Peers in den Status "Designated Forwarding" (Ausgewiesene Weiterleitung) versetzen. Auf ähnliche Weise überträgt der Remote-vPC-Peer den Layer-2-Trunk zwischen vPC-Peers in den Status "Designated Root". Dadurch kann Datenverkehr in Nicht-vPC-VLANs über beide vPC-Peers durch den Layer-2-Trunk fließen.

## Konfiguration

Ein Beispiel für die Konfiguration der vPC-Peer-Switch-Funktion finden Sie hier.

In diesem Beispiel ist N9K-1 als Spanning Tree-Root-Bridge für die VLANs 1, 10 und 20 mit der Priorität 0 konfiguriert. N9K-2 ist die sekundäre Spanning Tree-Root-Bridge für die VLANs 1, 10 und 20 mit der Priorität 4096.

```
N9K-1# show running-config vpc
<snip>
vpc domain 1
  role priority 150
  peer-keepalive destination 10.122.190.196

interface port-channel1
```

```
  vpc peer-link

N9K-2# show running-config vpc
<snip>
vpc domain 1
  peer-keepalive destination 10.122.190.195

interface port-channel1
  vpc peer-link

N9K-1# show running-config spanning-tree
spanning-tree vlan 1,10,20 priority 0
interface port-channel1
  spanning-tree port type network

N9K-2# show running-config spanning-tree
spanning-tree vlan 1,10,20 priority 4096
interface port-channel1
  spanning-tree port type network
```

Zunächst muss die Spanning Tree-Prioritätskonfiguration von N9K-2 so geändert werden, dass sie mit der von N9K-1 identisch ist. Dies ist erforderlich, damit die vPC-Peer-Switch-Funktion erwartungsgemäß funktioniert. Wenn die System-MAC-Adresse von N9K-2 niedriger ist als die System-MAC-Adresse von N9K-1, übernimmt N9K-2 die Rolle der Root-Bridge für die Spanning-Tree-Domäne, was dazu führt, dass andere Bridges in der Spanning-Tree-Domäne ihre lokalen MAC-Adresstabellen für alle betroffenen VLANs leeren. Ein Beispiel für dieses Phänomen ist hier dargestellt.

```
N9K-1# show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    1
             Address     689e.0baa.dea7
             This bridge is the root
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    1      (priority 0 sys-id-ext 1)
             Address     689e.0baa.dea7
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po1              Desg FWD 1         128.4096 (vPC peer-link) Network P2p
Po10             Desg FWD 1         128.4105 (vPC) P2p
Po20             Desg FWD 1         128.4115 (vPC) P2p

N9K-2# show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    1
             Address     689e.0baa.dea7
             Cost        1
             Port        4096 (port-channel1)
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     689e.0baa.de07
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po1              Root FWD 1         128.4096 (vPC peer-link) Network P2p
Po10             Desg FWD 1         128.4105 (vPC) P2p
Po20             Desg FWD 1         128.4115 (vPC) P2p

N9K-2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
N9K-2(config)# spanning-tree vlan 1,10,20 priority 0
N9K-2(config)# end
N9K-2# show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    1
             Address     689e.0baa.de07
             This bridge is the root
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    1      (priority 0 sys-id-ext 1)
             Address     689e.0baa.de07
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po1              Desg FWD 1         128.4096 (vPC peer-link) Network P2p
Po10             Desg FWD 1         128.4105 (vPC) P2p
Po20             Desg FWD 1         128.4115 (vPC) P2p
```

Als Nächstes können wir die vPC-Peer-Switch-Funktion über den Konfigurationsbefehl für die vPC-Domäne des **Peer-Switches** aktivieren. Dadurch wird die Bridge-ID innerhalb der Spanning Tree-BPDUs geändert, die von beiden vPC-Peers generiert wurden. Dies führt dazu, dass andere Bridges in der Spanning Tree-Domäne ihre lokalen MAC-Adresstabellen für alle betroffenen VLANs leeren.

```
N9K-1# configure terminal
N9K-1(config)# vpc domain 1
N9K-1(config-vpc-domain)# peer-switch
N9K-1(config-vpc-domain)# end
N9K-1#

N9K-2# configure terminal
N9K-2(config)# vpc domain 1
N9K-2(config-vpc-domain)# peer-switch
N9K-2(config-vpc-domain)# end
N9K-2#
```

Sie können überprüfen, ob die vPC-Peer-Switch-Funktion wie erwartet funktioniert, indem Sie mit dem Befehl **show spanning-tree summary** beide vPC-Peers als Root-Bridge für vPC-VLANs validieren. Diese Ausgabe sollte außerdem den Status anzeigen, dass die vPC-Peer-Switch-Funktion aktiviert und betriebsbereit ist.

```
N9K-1# show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001, VLAN0010, VLAN0020
L2 Gateway STP                          is disabled
Port Type Default                       is disable
```

```
Edge Port [PortFast] BPDU Guard Default  is disabled
Edge Port [PortFast] BPDU Filter Default is disabled
Bridge Assurance                         is enabled
Loopguard Default                        is disabled
Pathcost method used                     is short
vPC peer-switch                          is enabled (operational)
STP-Lite                                 is disabled

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                     0         0        0          3          3
VLAN0010                     0         0        0          3          3
VLAN0020                     0         0        0          3          3
---------------------- -------- --------- -------- ---------- ----------
3 vlans                      0         0        0          9          9

N9K-2# show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001, VLAN0010, VLAN0020
L2 Gateway STP                           is disabled
Port Type Default                        is disable
Edge Port [PortFast] BPDU Guard Default  is disabled
Edge Port [PortFast] BPDU Filter Default is disabled
Bridge Assurance                         is enabled
Loopguard Default                        is disabled
Pathcost method used                     is short
vPC peer-switch                          is enabled (operational)
STP-Lite                                 is disabled

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                     0         0        0          3          3
VLAN0010                     0         0        0          3          3
VLAN0020                     0         0        0          3          3
---------------------- -------- --------- -------- ---------- ----------
3 vlans                      0         0        0          9          9
```

Verwenden Sie den Befehl **show spanning-tree vlan {x}**, um detailliertere Informationen zu einem bestimmten VLAN anzuzeigen. Der Switch mit der primären oder operativen primären vPC-Rolle hat alle seine Schnittstellen im Status "Designated Forwarding". Der Switch mit der sekundären oder operativen sekundären vPC-Rolle hat alle zugehörigen Schnittstellen mit Ausnahme des vPC-Peer-Links, der sich im Root-Weiterleitungsstatus befindet, den Status "Designated Forwarding". Beachten Sie, dass die in der Ausgabe von **show vpc role** angezeigte MAC-Adresse des vPC-Systems mit der Root Bridge-ID und der Bridge-ID jedes vPC-Peers identisch ist.

```
N9K-1# show vpc role

vPC Role status
----------------------------------------------------
vPC role                        : primary
Dual Active Detection Status    : 0
vPC system-mac                  : 00:23:04:ee:be:01
vPC system-priority             : 32667
vPC local system-mac            : 68:9e:0b:aa:de:a7
vPC local role-priority         : 150
vPC local config role-priority  : 150
vPC peer system-mac             : 68:9e:0b:aa:de:07
vPC peer role-priority          : 32667
vPC peer config role-priority   : 32667
```

```
N9K-1# show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    1
             Address     0023.04ee.be01
             This bridge is the root
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    1      (priority 0 sys-id-ext 1)
             Address     0023.04ee.be01
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po1              Desg FWD 1         128.4096 (vPC peer-link) Network P2p
Po10             Desg FWD 1         128.4105 (vPC) P2p
Po20             Desg FWD 1         128.4115 (vPC) P2p

N9K-2# show vpc role

vPC Role status
----------------------------------------------------
vPC role                        : secondary
Dual Active Detection Status    : 0
vPC system-mac                  : 00:23:04:ee:be:01
vPC system-priority             : 32667
vPC local system-mac            : 68:9e:0b:aa:de:07
vPC local role-priority         : 32667
vPC local config role-priority  : 32667
vPC peer system-mac             : 68:9e:0b:aa:de:a7
vPC peer role-priority          : 150
vPC peer config role-priority   : 150

N9K-2# show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    1
             Address     0023.04ee.be01
             This bridge is the root
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    1      (priority 0 sys-id-ext 1)
             Address     0023.04ee.be01
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po1              Root FWD 1         128.4096 (vPC peer-link) Network P2p
Po10             Desg FWD 1         128.4105 (vPC) P2p
Po20             Desg FWD 1         128.4115 (vPC) P2p
```

Schließlich können wir das Dienstprogramm zur Paketerfassung auf der Ethanalyzer-Kontrollebene auf jedem vPC-Peer verwenden, um zu bestätigen, dass beide vPC-Peers Spanning-Tree-BPDUs mit einer Bridge-ID und einer Root-Bridge-ID, die die von beiden vPC-Peers gemeinsam genutzte MAC-Adresse des vPC-Systems enthalten, erzeugen.

```
N9K-1# ethanalyzer local interface inband display-filter stp limit-captured-frames 0
<snip>
Capturing on inband
```

```
2021-05-13 01:59:51.664206 68:9e:0b:aa:de:d4 -> 01:80:c2:00:00:00 STP RST. Root =
0/1/00:23:04:ee:be:01  Cost = 0  Port = 0x9000

N9K-2# ethanalyzer local interface inband display-filter stp limit-captured-frames 0
<snip>
Capturing on inband
2021-05-13 01:59:51.777034 68:9e:0b:aa:de:34 -> 01:80:c2:00:00:00 STP RST. Root =
0/1/00:23:04:ee:be:01  Cost = 0  Port = 0x9000
```

## Auswirkungen

Die Auswirkungen der Aktivierung der vPC-Peer-Switch-Erweiterung variieren je nachdem, ob andere Bridges in der Spanning Tree-Domäne über einen vPC mit beiden vPC-Peers verbunden sind oder ob diese redundant mit beiden vPC-Peers ohne vPC verbunden sind.

### Redundant verbundene Nicht-vPC-Bridges

Wenn eine Bridge ohne vPC-Verbindung mit redundanten Verbindungen zu beiden vPC-Peers (sodass sich eine Verbindung aus Sicht des Spanning Tree Protocol im Blockierungsstatus befindet) eine Änderung der Spanning Tree-Root-Bridge erkennt, die in Spanning Tree-BPDUs angekündigt wird, kann sich der Root-Port der Bridge zwischen den beiden redundanten Schnittstellen ändern. Dies wiederum kann dazu führen, dass andere Designated Forwarding-Schnittstellen sofort in den Blocking-Zustand übergehen und dann den Endstatus-Rechner des Spanning Tree Protocol (Blocking, Learning und Forwarding) mit Pausen durchlaufen, die dem konfigurierten Spanning Tree Protocol Forward Delay-Timer entsprechen (standardmäßig 15 Sekunden). Die Änderung des Root-Ports und das anschließende Durchlaufen des endlichen Spanning Tree Protocol-Systems können zu erheblichen Unterbrechungen im Netzwerk führen.

Es sollte erwähnt werden, dass diese Auswirkungen immer dann auftreten, wenn der vPC-Peer, der derzeit die Root-Bridge für die Spanning-Tree-Domäne ist, offline geht (z. B. bei Stromausfall, Hardwareausfall oder einem Neuladen). Dieses Verhalten ist nicht spezifisch für die vPC-Peer-Switch-Erweiterung, da die Aktivierung der vPC-Peer-Switch-Erweiterung aus Sicht eines Spanning-Tree-Servers ein ähnliches Verhalten wie ein vPC-Peer verursacht, der offline geht.

### Über vPC verbundene Bridges

Wenn eine über vPC verbundene Bridge eine Änderung in der Spanning Tree-Root-Bridge erkennt, die in Spanning Tree-BPDUs angekündigt wird, löscht die Bridge dynamisch ermittelte MAC-Adressen aus ihrer MAC-Adresstabelle. Beim Konfigurieren der vPC-Peer-Switch-Funktion können Sie dieses Verhalten in den folgenden beiden Szenarien beobachten:

1. Wenn Spanning Tree-Prioritätswerte so konfiguriert sind, dass sie zwischen beiden vPC-Peers übereinstimmen, kann die Spanning Tree-Root-Bridge von einem vPC-Peer zu einem anderen wechseln, wenn der vPC-Peer, der zuvor nicht die Root-Bridge war, eine niedrigere System-MAC-Adresse hat als der vPC-Peer, der zuvor die Root-Bridge war. Ein Beispiel für dieses Szenario finden Sie im Abschnitt zur Konfiguration von vPC-Peer-Switches in diesem Dokument.
2. Wenn die vPC-Peer-Switch-Funktion über den Konfigurationsbefehl für die vPC-Domäne des **Peer-Switches** aktiviert wird, beginnen beide vPC-Peers als Root Bridges der Spanning Tree-Domäne zu funktionieren. Beide vPC-Peers beginnen mit der Erstellung identischer Spanning Tree-BPDUs, die sich selbst als Root-Bridge der Spanning Tree-Domäne

behaupten.

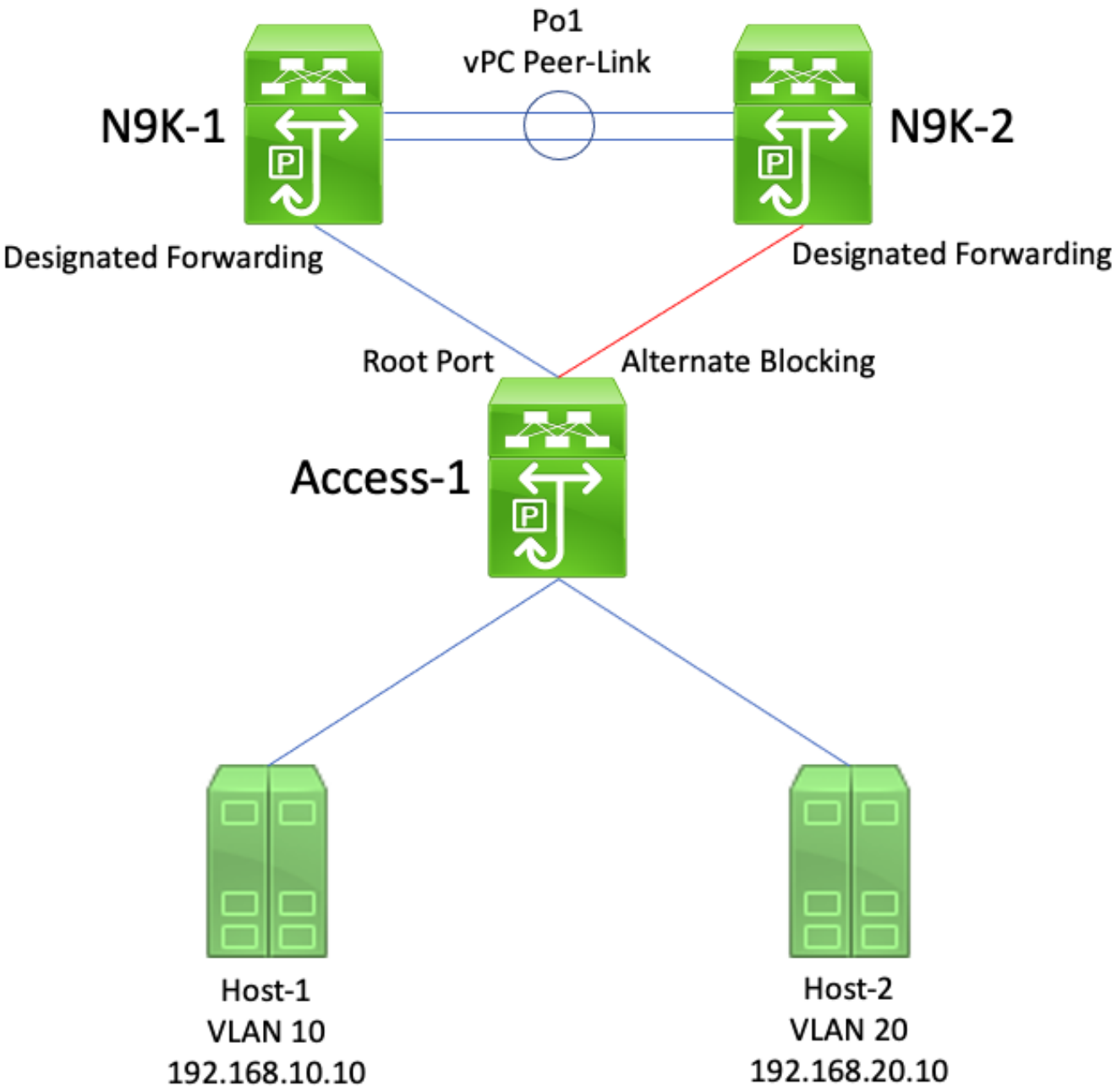
In den meisten Szenarien und Topologien wurden keine Auswirkungen auf die Datenebene beobachtet. Kurzfristig wird der Datenverkehr auf Datenebene jedoch innerhalb eines VLAN durch unbekanntes Unicast-Flooding geflutet, da die Ziel-MAC-Adresse von Frames auf keinem Switch-Port als direktes Ergebnis der Leerung dynamisch ermittelter MAC-Adressen erfasst wird. In einigen Topologien kann dies zu kurzzeitigen Leistungsproblemen oder Paketverlusten führen, wenn der Datenverkehr auf Datenebene an überbelegte Netzwerkgeräte im VLAN geleitet wird. Dies kann auch zu Problemen mit bandbreitenintensiven, unidirektionalen Datenverkehrsflüssen oder stillen Hosts führen (Hosts, die primär Pakete empfangen und selten Pakete senden), da dieser Datenverkehr über einen längeren Zeitraum innerhalb des VLAN geleitet wird, anstatt wie üblich direkt zum Ziel-Host zu wechseln.

Es sollte erwähnt werden, dass diese Auswirkungen mit der Leerung dynamisch ermittelter MAC-Adressen aus der MAC-Adresstabelle der Bridges innerhalb des betroffenen VLAN zusammenhängen. Dieses Verhalten ist nicht spezifisch für die vPC-Peer-Switch-Erweiterung oder eine Änderung der Root-Bridge - es kann auch durch eine Benachrichtigung über eine Topologieänderung verursacht werden, die aufgrund eines Nicht-Edge-Ports im VLAN generiert wird.

## Beispiele für Fehlerszenarien

### Redundant verbundene Nicht-vPC-Bridges, die den Finite-State-Rechner neu starten

Betrachten Sie die Topologie hier:




In dieser Topologie sind N9K-1 und N9K-2 vPC-Peers in einer vPC-Domäne. N9K-1 ist mit einem Spanning Tree-Prioritätswert von 0 für alle VLANs konfiguriert, sodass N9K-1 die Root-Bridge für alle VLANs ist. N9K-2 ist mit einem Spanning Tree-Prioritätswert von 4096 für alle VLANs konfiguriert, sodass N9K-2 die sekundäre Root-Bridge für alle VLANs ist. Access-1 ist ein Switch, der redundant über Layer-2-Switch-Ports mit N9K-1 und N9K-2 verbunden ist. Diese Switch-Ports sind nicht in einem Port-Channel gebündelt. Das Spanning Tree Protocol setzt daher die mit N9K-1 verbundene Verbindung in den Status "Designated Root" (Designierte Root) und die mit N9K-2 verbundene Verbindung in den Status "Alternate Blocking" (Alternative Blockierung).

Stellen Sie sich ein Fehlerszenario vor, bei dem N9K-1 aufgrund eines Hardware- oder Stromausfalls oder eines erneuten Ladens des Switches offline geht. N9K-2 behauptet sich selbst als Root-Bridge für alle VLANs, indem es Spanning Tree-BPDUs unter Verwendung seiner System-MAC-Adresse als Bridge-ID meldet. Access-1 erkennt eine Änderung in der Root-Bridge-ID. Darüber hinaus wechselt der designierte Root-Port in einen Down/Down-Status, was bedeutet, dass der neue designierte Root-Port die Verbindung ist, die sich in einem alternativen Blockierungsstatus gegenüber N9K-2 befand.

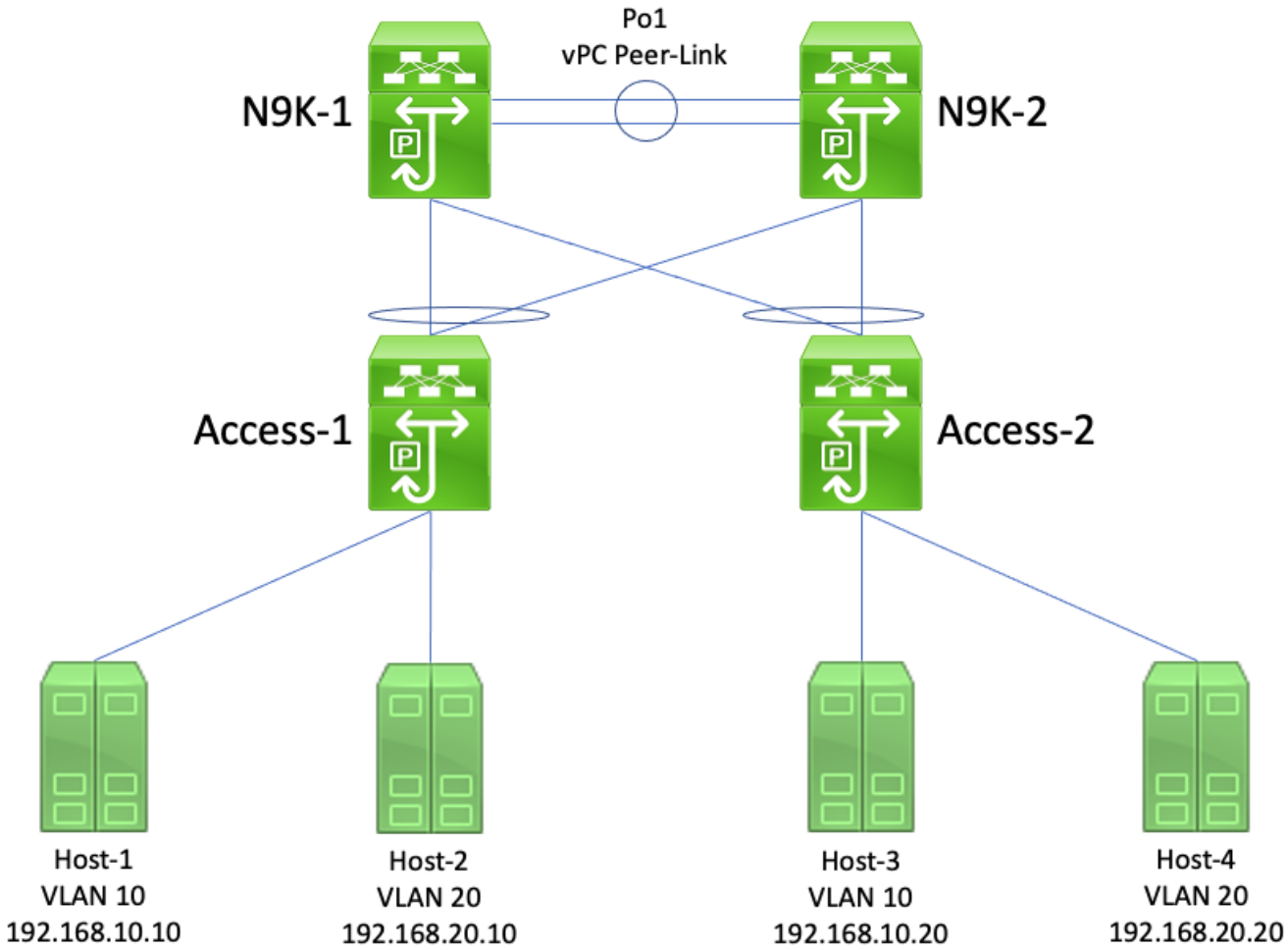
Diese Änderung bei den designierten Root-Ports bewirkt, dass alle Nicht-Edge-Spanning-Tree-

Ports den Spanning Tree Protocol Finite State Machine (Blocking, Learning und Forwarding) mit Pausen dazwischen durchlaufen, die dem konfigurierten Spanning Tree Protocol Forward Delay-Timer (standardmäßig 15 Sekunden) entsprechen. Dieser Prozess kann das Netzwerk erheblich beeinträchtigen.

Im gleichen Fehlerszenario mit aktivierter vPC-Peer-Switch-Erweiterung übertragen sowohl N9K-1 als auch N9K-2 identische Spanning Tree-BPDUs, wobei die gemeinsam genutzte MAC-Adresse des vPC-Systems als Bridge-ID verwendet wird. Wenn N9k-1 ausfällt, setzt N9K-2 die Übertragung derselben Spanning-Tree-BPDU fort. Infolgedessen wechselt Access-1 sofort die Alternative Blocking-Verbindung zu N9K-2 in den Designated Root-Status und beginnt mit der Weiterleitung des Datenverkehrs über die Verbindung. Da sich die Spanning Tree-Root-Bridge-ID nicht ändert, können Nicht-Edge-Ports das Spanning Tree Protocol Finite State Machine nicht passieren, wodurch die im Netzwerk beobachtete Unterbrechung verringert wird.

### VPC-verbundene Bridges löschen dynamisch ermittelter MAC-Adressen

Betrachten Sie die Topologie hier:




In dieser Topologie sind N9K-1 und N9K-2 vPC-Peers in einer vPC-Domäne, die Inter-VLAN-Routing zwischen VLAN 10 und VLAN 20 durchführen. N9K-1 ist mit einem Spanning Tree-Prioritätswert von 0 für VLAN 10 und VLAN 20 konfiguriert, sodass N9K-1 die Root-Bridge für beide VLANs ist. N9K-2 ist mit einem Spanning Tree-Prioritätswert von 4096 für VLAN 10 und VLAN 20 konfiguriert, wodurch N9K-2 die sekundäre Root-Bridge für beide VLANs ist. Host-1, Host-2, Host-3 und Host-4 kommunizieren kontinuierlich miteinander.

Stellen Sie sich ein Fehlerszenario vor, bei dem N9K-1 aufgrund eines Hardware- oder

Stromausfalls oder eines erneuten Ladens des Switches offline geht. N9K-2 behauptet sich selbst als die Root-Bridge für VLAN 10 und VLAN 20, indem es Spanning Tree-BPDUs unter Verwendung seiner System-MAC-Adresse als Bridge-ID meldet. Access-1 und Access-2 sehen eine Änderung in der Root-Bridge-ID, und obwohl der Spanning Tree gleich bleibt (d. h. der vPC mit N9K-1 und N9K-2 bleibt ein designierter Root-Port), leeren Access-1 und Access-2 ihre MAC-Adressen aller dynamisch bezogenen MAC-Adressen in VLAN 10 und VLAN 20.

In den meisten Umgebungen ist die Leerung dynamisch ermittelter MAC-Adressen mit minimalen Auswirkungen verbunden. Es gehen keine Pakete verloren (abgesehen von Paketen, die verloren gingen, als sie bei einem Fehler an N9K-1 übertragen wurden). Der Datenverkehr wird jedoch vorübergehend innerhalb jeder Broadcast-Domäne als unbekannter Unicast-Datenverkehr geflutet, während alle Switches in der Broadcast-Domäne dynamische MAC-Adressen neu lernen.

Im gleichen Fehlerszenario mit aktivierter vPC-Peer-Switch-Erweiterung würden N9K-1 und N9K-2 identische Spanning-Tree-BPDUs übertragen, wobei die gemeinsam genutzte MAC-Adresse des vPC-Systems als Bridge-ID verwendet wird. Wenn N9k-1 ausfällt, setzt N9K-2 die Übertragung derselben Spanning-Tree-BPDU fort. Infolgedessen ist Access-1 und Access-2 nicht bewusst, dass eine Änderung der Spanning Tree-Topologie stattgefunden hat. Aus ihrer Sicht sind die Spanning Tree-BPDUs der Root-Bridge identisch, sodass es nicht erforderlich ist, dynamisch ermittelte MAC-Adressen aus relevanten VLANs zu leeren. Dadurch wird in diesem Fehlerszenario das Flooding von unbekanntem Unicast-Datenverkehr in jeder Broadcast-Domäne verhindert.

# vPC-Peer-Gateway

In diesem Abschnitt wird die Erweiterung des vPC-Peer-Gateways beschrieben, die mit dem Konfigurationsbefehl für die vPC-Domäne des **Peer-Gateways** aktiviert wird.

## Überblick

In einer vPC-Domäne konfigurierte Nexus-Switches leiten das First Hop Redundancy Protocol (FHRP) standardmäßig doppelt aktiv weiter. Das bedeutet, dass, wenn einer der vPC-Peers ein Paket mit einer Ziel-MAC-Adresse empfängt, die zu einer auf dem Switch konfigurierten HSRP- (Hot Standby Router Protocol) oder VRRP-Gruppe (Virtual Router Redundancy Protocol) gehört, der Switch das Paket gemäß der lokalen Routing-Tabelle weiterleitet, und zwar unabhängig vom Status der HSRP- oder VRRP-Kontrollebene. Mit anderen Worten: Es wird erwartet, dass ein vPC-Peer im HSRP-Standby- oder VRRP-Backup-Status Pakete weiterleitet, die an die virtuelle HSRP- oder VRRP-MAC-Adresse gerichtet sind.

Wenn ein vPC-Peer ein Paket an eine virtuelle FHRP-MAC-Adresse weiterleitet, schreibt er das Paket mit einer neuen Quell- und Ziel-MAC-Adresse neu. Die Quell-MAC-Adresse ist die MAC-Adresse der Switched Virtual Interface (SVI) des vPC-Peers innerhalb des VLAN, in das das Paket geroutet wird. Die Ziel-MAC-Adresse ist die MAC-Adresse, die der Next-Hop-IP-Adresse für die Ziel-IP-Adresse des Pakets entsprechend der lokalen Routing-Tabelle des vPC-Peers zugeordnet ist. Bei Inter-VLAN-Routing-Szenarien ist die Ziel-MAC-Adresse des Pakets nach dem Umschreiben die MAC-Adresse des Hosts, an den das Paket letztendlich gerichtet ist.

Bei einigen Hosts wird das Standardweiterleitungsverhalten nicht als Optimierungsfunktion verwendet. Bei diesem Verhalten führt der Host keine Routing-Tabelle und/oder ARP-Cache-Suche durch, wenn er auf ein eingehendes Paket antwortet. Stattdessen kippt der Host die Quell- und Ziel-MAC-Adressen des eingehenden Pakets für das Antwortpaket. Mit anderen Worten, die

Quell-MAC-Adresse des eingehenden Pakets wird zur Ziel-MAC-Adresse des Antwortpakets, und die Ziel-MAC-Adresse des eingehenden Pakets wird zur Quell-MAC-Adresse des Antwortpakets. Dieses Verhalten unterscheidet sich von einem Host, der dem Standardweiterleitungsverhalten folgt. Dieser würde eine lokale Routing-Tabelle und/oder eine ARP-Cache-Suche durchführen und die Ziel-MAC-Adresse des Antwortpakets auf die virtuelle FHRP-MAC-Adresse setzen.

Dieses vom Standard abweichende Verhalten des Hosts kann gegen die vPC-Schleifenvermeidungsregel verstoßen, wenn das vom Host generierte Antwortpaket an einen vPC-Peer adressiert wird, den vPC jedoch an den anderen vPC-Peer weiterleitet. Der andere vPC-Peer empfängt das Paket, das an eine MAC-Adresse seines vPC-Peers gerichtet ist, und leitet das Paket aus dem vPC-Peer-Link an den vPC-Peer weiter, der die im MAC-Zieladressfeld des Pakets vorhandene MAC-Adresse besitzt. Der vPC-Peer, der Eigentümer der MAC-Adresse ist, versucht, das Paket lokal weiterzuleiten. Wenn das Paket einen vPC auslassen muss, verwirft der vPC-Peer dieses Paket, um gegen die vPC-Schleifenvermeidungsregel zu verstoßen. Daher können Sie bei einigen Datenströmen, die von einem Host stammen oder an einen Host gerichtet sind, unter Verwendung dieses nicht standardmäßigen Verhaltens Verbindungsprobleme oder Paketverluste feststellen.

Die vPC-Peer-Gateway-Erweiterung wurde eingeführt, um den Paketverlust zu vermeiden, der von Hosts mit diesem nicht standardmäßigen Verhalten eingeführt wurde. Dies geschieht dadurch, dass ein vPC-Peer Pakete, die an die MAC-Adresse des anderen vPC-Peers gerichtet sind, lokal weiterleiten kann, sodass Pakete, die an den entfernten vPC-Peer gerichtet sind, nicht aus dem vPC-Peer-Link ausgetreten werden müssen, um geroutet zu werden. Mit anderen Worten: Die Erweiterung des vPC-Peer-Gateways ermöglicht es einem vPC-Peer, Pakete "im Namen" des entfernten vPC-Peers weiterzuleiten. Die vPC-Peer-Gateway-Erweiterung kann mit dem Konfigurationsbefehl **für** die **vPC-**Domäne des **Peer-Gateways** aktiviert werden.

## Hinweise

### Flapping von Unicast Routing Protocol-Adjacencies über vPCs oder vPC-VLANs

Wenn dynamische Unicast-Routing-Protokoll-Adjacencies zwischen zwei vPC-Peers und einem über einen verwaisten vPC-Port verbundenen Router oder Router gebildet werden, beginnen die Routing-Protokoll-Adjacencies möglicherweise kontinuierlich zu flapping, nachdem die vPC-Peer-Gateway-Erweiterung aktiviert wurde, wenn die Routing-/Layer-3-over-vPC-Erweiterung nicht unmittelbar danach konfiguriert wird. Diese Fehlerszenarien werden ausführlich in den Abschnitten zu Unicast Routing Protocol Adjacencies over a vPC with vPC Peer Gateway Example Failure Scenario und Unicast Routing Protocol Adjacencies over a vPC VLAN with vPC Peer Gateway beschrieben.

Um dieses Problem zu beheben, aktivieren Sie die Erweiterung Routing/Layer 3 über vPC mit dem Befehl **layer3 peer-router** vPC domain configuration, unmittelbar nachdem Sie die Erweiterung vPC Peer Gateway mit dem Befehl **peer-gateway** vPC domain configuration aktiviert haben.

### Automatische Deaktivierung von ICMP- und ICMPv6-Umleitungen

Wenn die vPC-Peer-Gateway-Erweiterung aktiviert ist, wird die Generierung von ICMP- und ICMPv6-Weiterleitungspaketen automatisch auf allen vPC-VLAN-SVIs deaktiviert (d. h. jeder SVI, die einem VLAN zugeordnet ist, das über den vPC-Peer-Link verbunden ist). Hierzu konfiguriert der Switch **keine IP-Umleitungen** und **keine IPv6-Umleitungen** auf allen vPC-VLAN-SVIs. Dadurch

wird verhindert, dass ein Switch ICMP-Umleitungspakete als Reaktion auf Pakete generiert, die den Switch erreichen, aber eine Ziel-MAC- und IP-Adresse des vPC-Peers des Switches haben.

Wenn in Ihrer Umgebung innerhalb eines bestimmten VLAN ICMP- oder ICMPv6-Weiterleitungspakete erforderlich sind, müssen Sie dieses VLAN mithilfe des Konfigurationsbefehls **peer-gateway exclude-vlan <vlan-id>** vPC-Domain von der Nutzung der vPC Peer-Gateway-Erweiterung ausschließen.

> **Hinweis**: Der Befehl **peer-gateway exclude-vlan <vlan-id>** vPC domain configuration wird auf Switches der Serie Nexus 9000 nicht unterstützt.

## Konfiguration

Ein Beispiel für die Konfiguration der vPC-Peer-Gateway-Funktion finden Sie hier.

In diesem Beispiel sind N9K-1 und N9K-2 vPC-Peers in einer vPC-Domäne. Für beide vPC-Peers ist eine HSRP-Gruppe für VLAN 10 konfiguriert. N9K-1 ist der aktive HSRP-Router mit einer Priorität von 150, während N9K-2 der HSRP-Standby-Router mit der Standardpriorität von 100 ist.

```
N9K-1# show running-config vpc
<snip>
vpc domain 1
  role priority 150
  peer-keepalive destination 10.82.140.43

interface port-channel1
  vpc peer-link

N9K-2# show running-config vpc
<snip>
vpc domain 1
  peer-keepalive destination 10.82.140.42

interface port-channel1
  vpc peer-link

N9K-1# show running-config interface vlan 10
<snip>
interface Vlan10
  no shutdown
  ip address 192.168.10.2/24
  hsrp 10
    preempt
    priority 150
    ip 192.168.10.1

N9K-2# show running-config interface vlan 10
<snip>
interface Vlan10
  no shutdown
  ip address 192.168.10.3/24
  hsrp 10
    ip 192.168.10.1

N9K-1# show hsrp interface vlan 10 brief
*:IPv6 group   #:group belongs to a bundle
                      P indicates configured to preempt.
```

```
                    |
 Interface   Grp  Prio P State    Active addr      Standby addr     Group addr
  Vlan10      10   150  P Active   local            192.168.10.3     192.168.10.1    (conf)

N9K-2# show hsrp interface vlan 10 brief
*:IPv6 group   #:group belongs to a bundle
                     P indicates configured to preempt.
                    |
 Interface   Grp  Prio P State    Active addr      Standby addr     Group addr
  Vlan10      10   100    Standby  192.168.10.2     local            192.168.10.1    (conf)
```

VLAN 10 SVI von N9K-1 hat die MAC-Adresse 00ee.ab67.db47, und die VLAN 10 SVI von N9K-2 hat die MAC-Adresse 00ee.abd8.747f. Die virtuelle HSRP-MAC-Adresse für VLAN 10 lautet 0000.0c07.ac0a. In diesem Zustand sind die VLAN 10-SVI-MAC-Adresse und die virtuelle HSRP-MAC-Adresse in der MAC-Adresstabelle jedes Switches vorhanden. Die VLAN 10-SVI-MAC-Adresse und die virtuelle HSRP-MAC-Adresse jedes Switches haben das Gateway-Flag (G), das anzeigt, dass der Switch lokal Pakete weiterleitet, die an diese MAC-Adresse gerichtet sind.

Beachten Sie, dass in der MAC-Adresstabelle von N9K-1 nicht das Gateway-Flag für die VLAN 10-SVI-MAC-Adresse von N9K-2 vorhanden ist. Ebenso ist in der MAC-Adresstabelle von N9K-2 das Gateway-Flag für die VLAN 10-SVI-MAC-Adresse von N9K-1 nicht vorhanden.

```
N9K-1# show mac address-table vlan 10
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan
   VLAN     MAC Address      Type      age     Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
G   10     0000.0c07.ac0a   static   -         F      F    sup-eth1(R)
G   10     00ee.ab67.db47   static   -         F      F    sup-eth1(R)
*   10     00ee.abd8.747f   static   -         F      F    vPC Peer-Link(R)

N9K-2# show mac address-table vlan 10
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan
   VLAN     MAC Address      Type      age     Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
G   10     0000.0c07.ac0a   static   -         F      F    vPC Peer-Link(R)
*   10     00ee.ab67.db47   static   -         F      F    vPC Peer-Link(R)
G   10     00ee.abd8.747f   static   -         F      F    sup-eth1(R)
```

Wir können die Erweiterung des vPC-Peer-Gateways über den Konfigurationsbefehl für die vPC-Domäne des **Peer-Gateways** aktivieren. Auf diese Weise kann der Switch empfangene Pakete mit einer MAC-Zieladresse, die zur MAC-Adresse des vPC-Peers gehört, die er über den vPC-Peer-Link bezogen hat, lokal weiterleiten. Hierzu wird die Gateway-Markierung für die MAC-Adresse des vPC-Peers in der MAC-Adresstabelle des Switches festgelegt.

```
N9K-1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
N9K-1(config)# vpc domain 1
N9K-1(config-vpc-domain)# peer-gateway
N9K-1(config-vpc-domain)# end
N9K-1#
```

```
N9K-2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
N9K-2(config)# vpc domain 1
N9K-2(config-vpc-domain)# peer-gateway
N9K-2(config-vpc-domain)# end
N9K-2#
```

Sie können überprüfen, ob die vPC-Peer-Gateway-Erweiterung wie erwartet funktioniert, indem Sie überprüfen, ob das Gateway-Flag in der MAC-Adresstabelle für die vPC-Peer-MAC vorhanden ist.

```
N9K-1# show mac address-table vlan 10
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan
   VLAN     MAC Address      Type      age     Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
G   10     0000.0c07.ac0a   static    -         F      F    sup-eth1(R)
G   10     00ee.ab67.db47   static    -         F      F    sup-eth1(R)
G   10     00ee.abd8.747f   static    -         F      F    vPC Peer-Link(R)

N9K-2# show mac address-table vlan 10
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan
   VLAN     MAC Address      Type      age     Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
G   10     0000.0c07.ac0a   static    -         F      F    vPC Peer-Link(R)
G   10     00ee.ab67.db47   static    -         F      F    vPC Peer-Link(R)
G   10     00ee.abd8.747f   static    -         F      F    sup-eth1(R)
```

## Auswirkungen

Die Auswirkungen der Aktivierung der vPC Peer Gateway-Erweiterung können je nach umgebender Topologie und dem Verhalten verbundener Hosts variieren, wie in den folgenden Unterabschnitten beschrieben. Wenn keiner der folgenden Unterabschnitte auf Ihre Umgebung zutrifft, führt die Aktivierung der vPC Peer Gateway-Erweiterung nicht zu Unterbrechungen und hat keine Auswirkungen auf Ihre Umgebung.

### Flapping von Unicast Routing Protocol-Adjacencies über vPCs oder vPC-VLANs

Wenn dynamische Unicast-Routing-Protokoll-Adjacencies zwischen zwei vPC-Peers und einem über einen verwaisten vPC-Port verbundenen Router oder Router gebildet werden, beginnen die Routing-Protokoll-Adjacencies möglicherweise kontinuierlich zu flapping, nachdem die vPC-Peer-Gateway-Erweiterung aktiviert wurde, wenn die Routing-/Layer-3-over-vPC-Erweiterung nicht unmittelbar danach konfiguriert wird. Diese Fehlerszenarien werden ausführlich in den Abschnitten zu Unicast Routing Protocol Adjacencies over a vPC with vPC Peer Gateway Example Failure Scenario und Unicast Routing Protocol Adjacencies over a vPC VLAN with vPC Peer Gateway beschrieben.

Um dieses Problem zu beheben, aktivieren Sie die Erweiterung Routing/Layer 3 über vPC mit dem Befehl **layer3 peer-router** vPC domain configuration, unmittelbar nachdem Sie die Erweiterung vPC Peer Gateway mit dem Befehl **peer-gateway** vPC domain configuration aktiviert haben.

### Automatische Deaktivierung von ICMP- und ICMPv6-Umleitungen

Wenn die vPC-Peer-Gateway-Erweiterung aktiviert ist, wird die Generierung von ICMP- und ICMPv6-Weiterleitungspaketen automatisch auf allen vPC-VLAN-SVIs deaktiviert (d. h. jeder SVI, die einem VLAN zugeordnet ist, das über den vPC-Peer-Link verbunden ist). Hierzu konfiguriert der Switch **keine IP-Umleitungen** und **keine IPv6-Umleitungen** auf allen vPC-VLAN-SVIs. Dadurch wird verhindert, dass ein Switch ICMP-Umleitungspakete als Reaktion auf Pakete generiert, die den Switch erreichen, aber eine Ziel-MAC- und IP-Adresse des vPC-Peers des Switches haben.

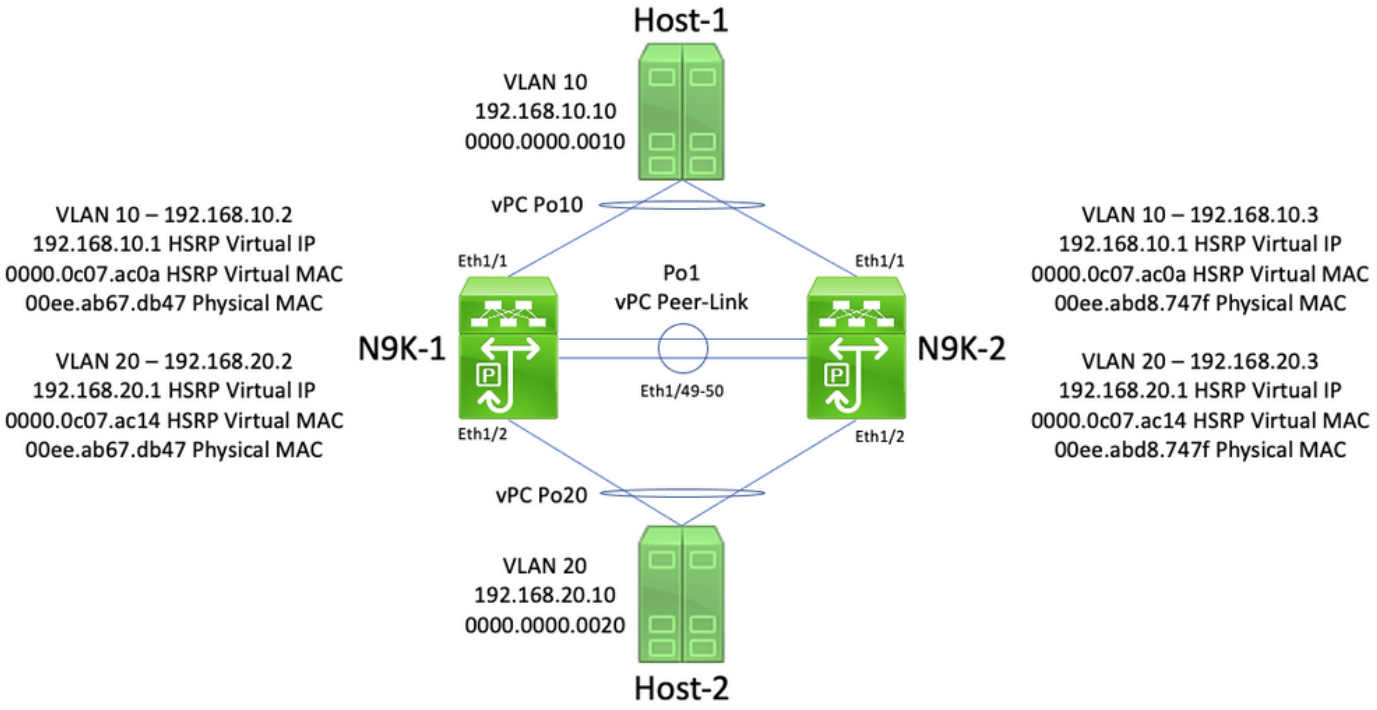
Wenn in Ihrer Umgebung innerhalb eines bestimmten VLAN ICMP- oder ICMPv6-Weiterleitungspakete erforderlich sind, müssen Sie dieses VLAN mithilfe des Konfigurationsbefehls **peer-gateway exclude-vlan <vlan-id>** vPC-Domain von der Nutzung der vPC Peer-Gateway-Erweiterung ausschließen.

> **Hinweis**: Der Befehl **peer-gateway exclude-vlan <vlan-id>** vPC domain configuration wird auf Switches der Serie Nexus 9000 nicht unterstützt.

## Beispiele für Fehlerszenarien

### Mit vPC verbundene Hosts mit nicht standardmäßigem Weiterleitungsverhalten

Betrachten Sie die Topologie hier:

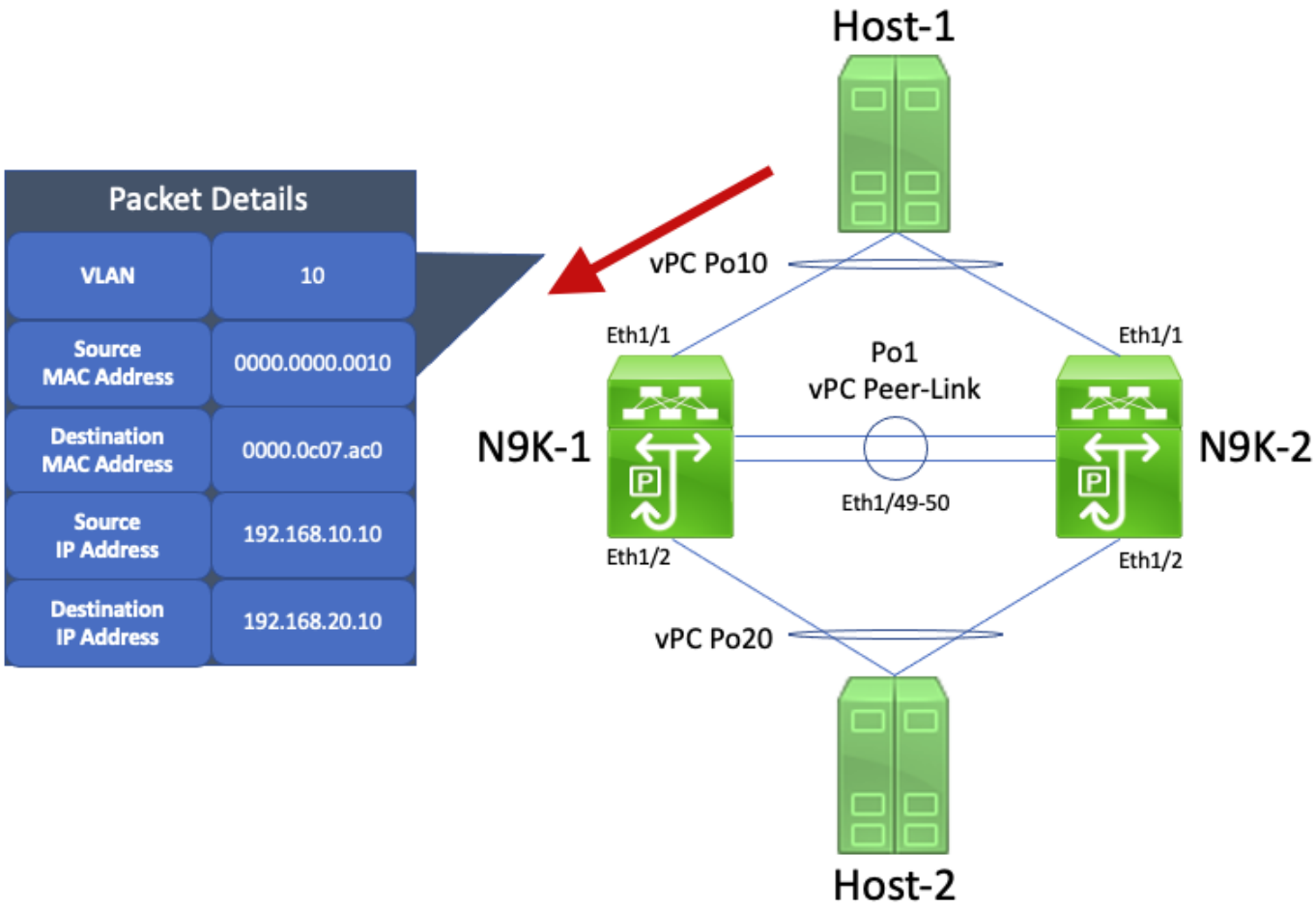



In dieser Topologie sind N9K-1 und N9K-2 vPC-Peers in einer vPC-Domäne, die Inter-VLAN-Routing zwischen VLAN 10 und VLAN 20 durchführen. Die Schnittstelle Po1 ist der vPC-Peer-Link. Ein Host mit dem Namen Host-1 ist über vPC Po10 mit N9K-1 und N9K-2 in VLAN 10 verbunden. Host-1 besitzt die IP-Adresse 192.168.10.10 mit der MAC-Adresse 0000.000.0010. Ein Host mit dem Namen Host-2 ist über vPC Po20 mit N9K-1 und N9K-2 in VLAN 20 verbunden. Host-2 besitzt die IP-Adresse 192.168.20.10 mit der MAC-Adresse 0000.0000.0020.

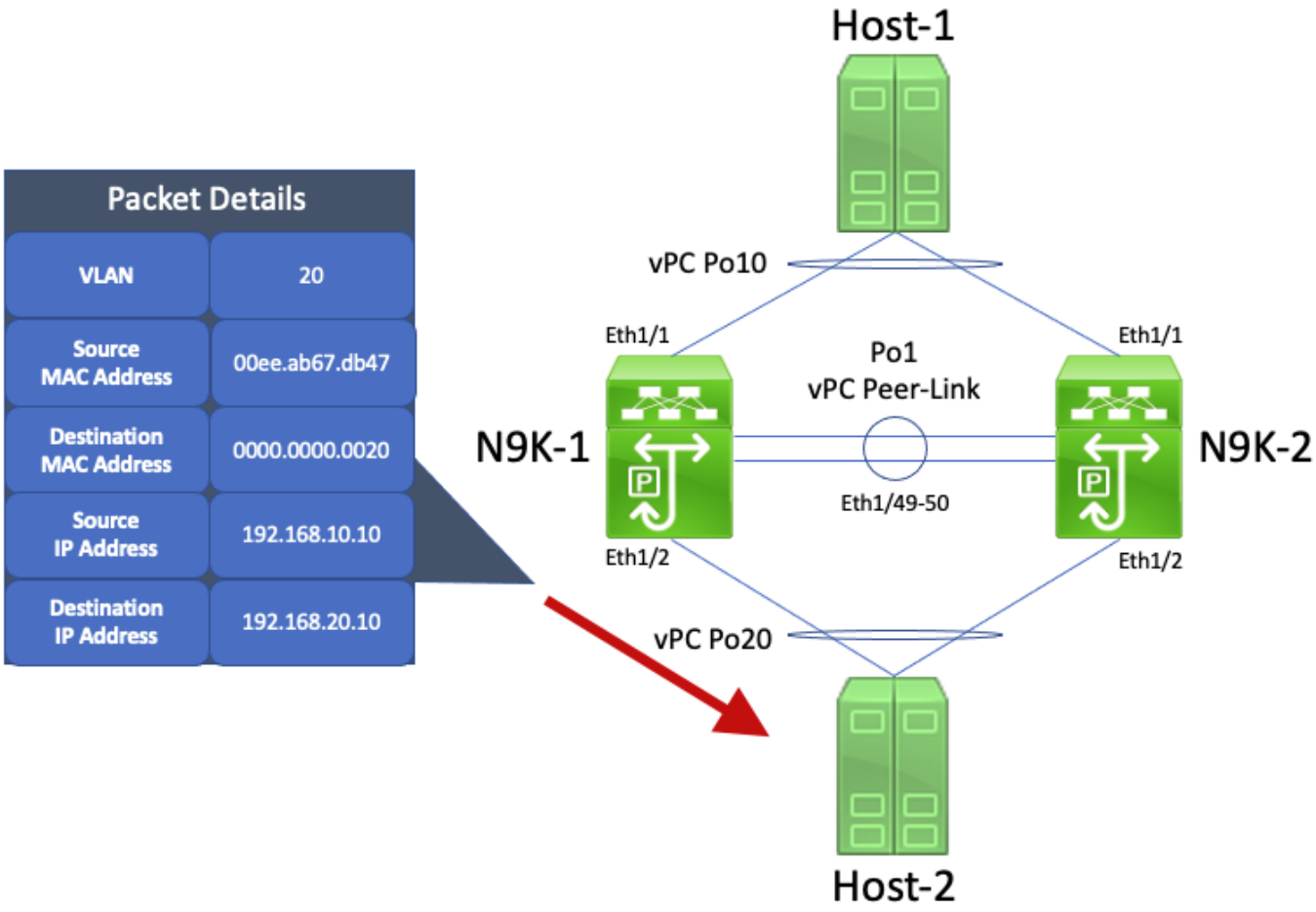
N9K-1 und N9K-2 verfügen beide über SVIs in VLAN 10 und VLAN 20, wobei HSRP unter jeder

SVI aktiviert ist. Die VLAN 10-Schnittstelle von N9K-1 hat die IP-Adresse 192.168.10.2, und die VLAN 20-Schnittstelle von N9K-1 hat die IP-Adresse 192.168.20.2. Beide SVIs von N9K-1 haben die physische MAC-Adresse 00ee.ab67.db47. Die VLAN 10-Schnittstelle von N9K-2 hat die IP-Adresse 1921.68.10.3, und die VLAN 20-Schnittstelle von N9K-2 hat die IP-Adresse 192.168.20.3. Beide SVIs von N9K-2 haben die physische MAC-Adresse 00ee.abd8.747f. Die virtuelle HSRP-IP-Adresse für VLAN 10 lautet 192.168.10.1, die virtuelle HSRP-MAC-Adresse 0000.0c07.ac0a. Die virtuelle HSRP-IP-Adresse für VLAN 20 lautet 192.168.20.1, die virtuelle HSRP-MAC-Adresse 0000.0c07.ac14.

Stellen Sie sich ein Szenario vor, in dem Host-1 ein ICMP-Echoanforderungspaket an Host-2 sendet. Nachdem Host-1 ARP für sein Standard-Gateway (die virtuelle HSRP-IP-Adresse) aufgelöst hat, folgt Host-1 dem Standardweiterleitungsverhalten und generiert ein ICMP-Echoanforderungspaket mit der Quell-IP-Adresse 192.168.10.10 und der Ziel-IP-Adresse 192.168.20.10. 00.0000.0010 und die MAC-Zieladresse 0000.0c07.ac0a. Dieses Paket geht an N9K-1 aus. Ein visuelles Beispiel hierfür ist hier dargestellt.

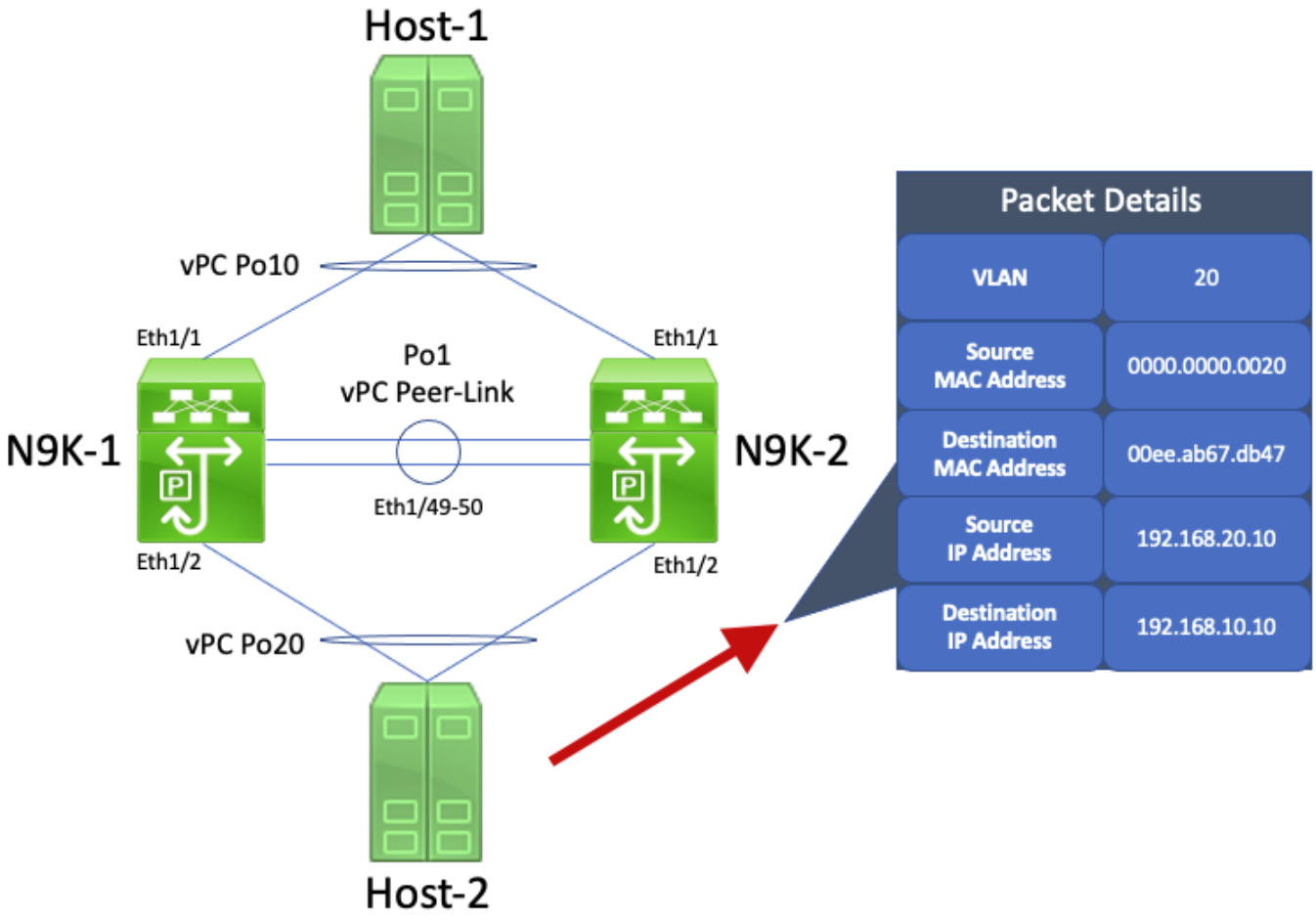



N9K-1 empfängt dieses Paket. Da dieses Paket für die virtuelle HSRP-MAC-Adresse bestimmt ist, kann N9K-1 dieses Paket unabhängig vom Status der HSRP-Kontrollebene entsprechend der lokalen Routing-Tabelle weiterleiten. Dieses Paket wird von VLAN 10 in VLAN 20 geroutet. Beim Routing des Pakets führt N9K-1 eine Umschreibung des Pakets durch, indem die Quell- und Ziel-MAC-Adressfelder des Pakets neu adressiert werden. Die neue Quell-MAC-Adresse des Pakets ist die physische MAC-Adresse, die mit der VLAN 20 SVI von N9K-1 (00ee.ab67.db47) verknüpft ist, und die neue Ziel-MAC-Adresse ist die MAC-Adresse, die Host-2 (0000.000.0020) zugeordnet ist. Ein visuelles Beispiel hierfür ist hier dargestellt.

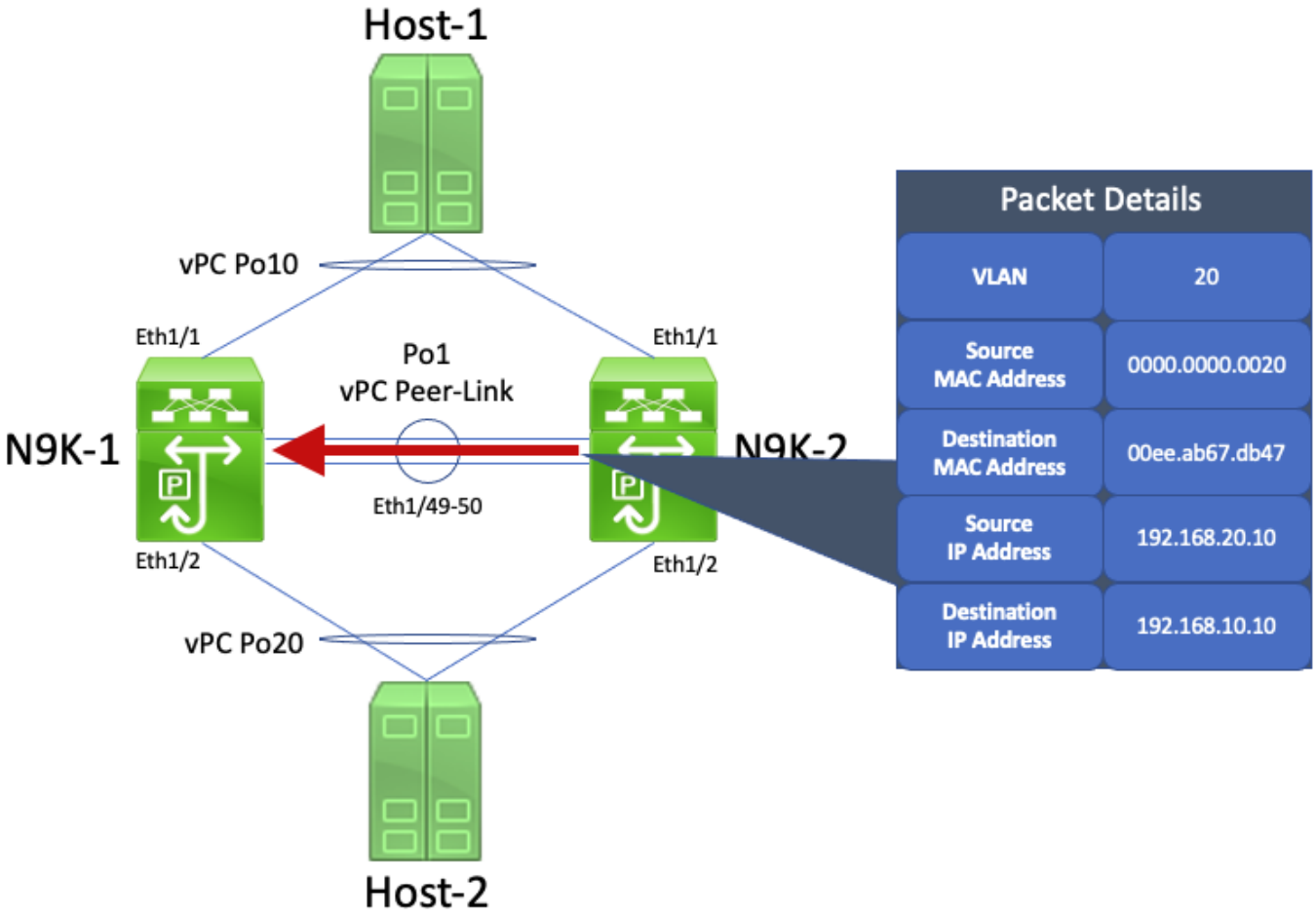



Host-2 empfängt dieses Paket und generiert ein ICMP-Echo-Reply-Paket als Antwort auf das ICMP-Echo-Request-Paket von Host-1. Wenn Host-2 jedoch nicht dem Standardweiterleitungsverhalten folgt. Zur Optimierung der Weiterleitung führt Host-2 keine Routing-Tabelle oder ARP-Cache-Suche nach der IP-Adresse von Host-1 (192.168.10.10) durch, sondern invertiert die Quell-MAC-Adresse und die Ziel-MAC-Adressfelder des ursprünglich empfangenen ICMP-Echoanforderungspakets Host-2. Das von Host-2 generierte ICMP-Echo-Reply-Paket weist daher die Quell-IP-Adresse 192.168.20.10, die Ziel-IP-Adresse 192.168.10.10, die Quell-MAC-Adresse 0000.0000.0020 auf. MAC-Zieladresse: 00ee.ab67.db47.

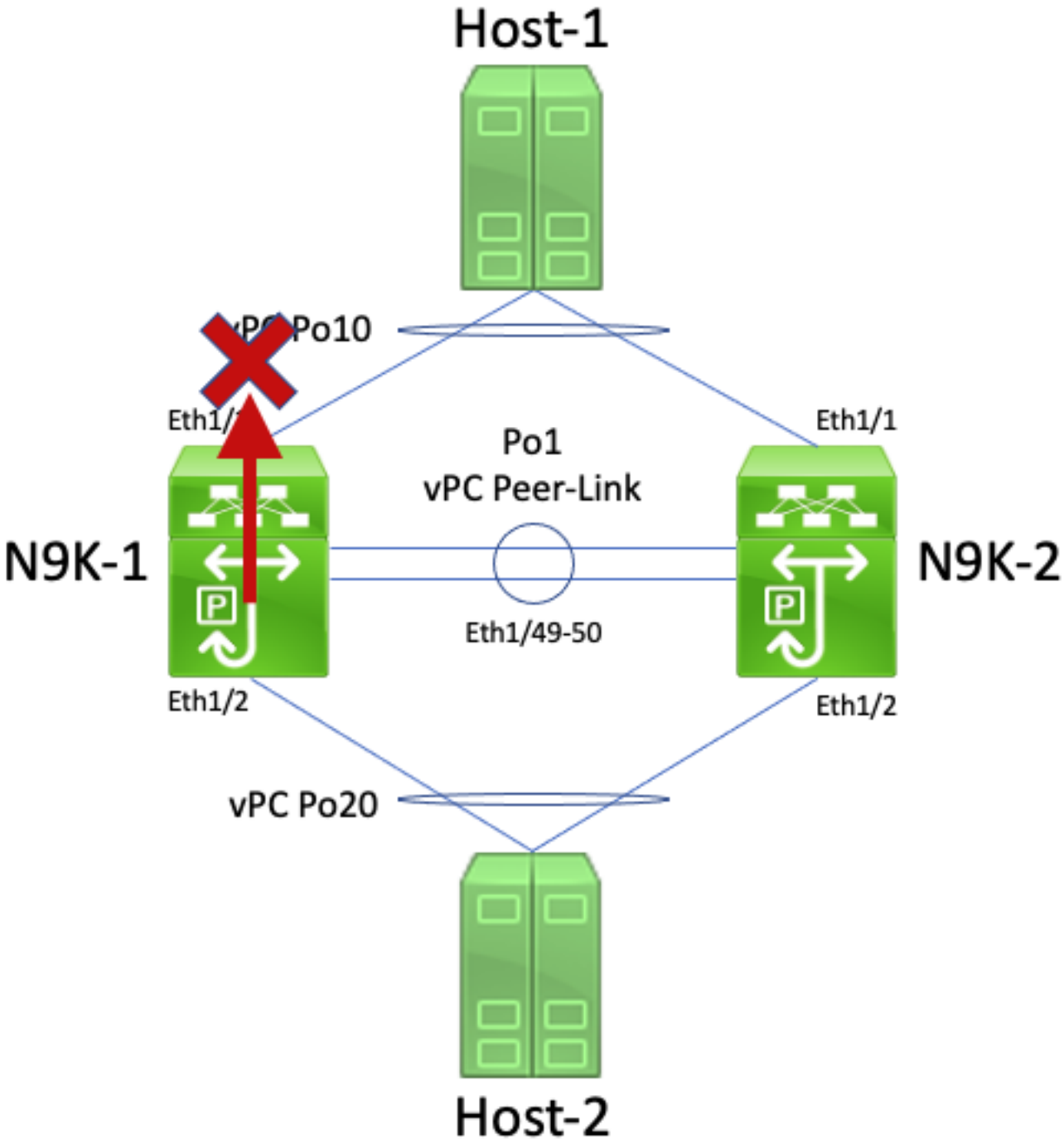
Wenn dieses ICMP-Echoantwortpaket an N9K-1 ausgeht, wird dieses Paket problemlos an Host-1 weitergeleitet. Beachten Sie jedoch ein Szenario, bei dem das ICMP-Echo-Reply-Paket in Richtung N9K-2 ausgeht, wie hier gezeigt.




N9K-2 empfängt dieses Paket. Da dieses Paket für die physische MAC-Adresse der VLAN 20 SVI von N9K-1 bestimmt ist, leitet N9K-2 dieses Paket über den vPC-Peer-Link an N9K-1 weiter, da N9K-2 dieses Paket nicht für N9K-1 weiterleiten kann. Ein visuelles Beispiel hierfür ist hier dargestellt.




N9K-1 empfängt dieses Paket. Da dieses Paket für die physische MAC-Adresse der VLAN 20 SVI von N9K-1 bestimmt ist, kann N9K-1 dieses Paket entsprechend der lokalen Routing-Tabelle routen, unabhängig vom Status der HSRP-Kontrollebene. Dieses Paket wird von VLAN 20 in VLAN 10 geroutet. Die Ausgangsschnittstelle für diese Route wird jedoch zu vPC Po10 aufgelöst, der auf N9K-2 verfügbar ist.  Dies stellt einen Verstoß gegen die Regel zur Vermeidung von vPC-Schleifen dar: Wenn N9K-1 ein Paket über den vPC-Peer-Link empfängt, kann N9K-1 dieses Paket nicht von einer vPC-Schnittstelle weiterleiten, wenn dieselbe vPC-Schnittstelle auf N9K-2 aktiv ist. N9K-1 verwirft dieses Paket aufgrund dieser Verletzung. Ein visuelles Beispiel hierfür ist hier dargestellt.




Sie können dieses Problem beheben, indem Sie die vPC-Peer-Gateway-Erweiterung mit dem Konfigurationsbefehl für die vPC-Domäne **Peer-Gateway** aktivieren. Dadurch kann N9K-2 das ICMP-Echo-Reply-Paket (und andere Pakete, die ähnlich adressiert sind) im Auftrag von N9K-1 weiterleiten, obwohl die Ziel-MAC-Adresse des Pakets N9K-1 gehört und nicht N9K-2. Daher kann N9K-2 dieses Paket von seiner vPC-Po10-Schnittstelle weiterleiten, anstatt es über den vPC-Peer-Link weiterzuleiten.

## Routing/Layer 3 über vPC (Layer 3-Peer-Router)

In diesem Abschnitt wird die Verbesserung von Routing/Layer 3 über vPC beschrieben, die mit dem Konfigurationsbefehl **für die vPC-**Domäne des **Layer-3-Peer-Routers** aktiviert wird.

**Hinweis:** Das Bilden von Multicast-Routing-Protokoll-Adjacencies (namentlich Protocol Independent Multicast [PIM] Adjacencies) über einen vPC wird bei aktivierter Routing-/Layer 3-over-vPC-Erweiterung nicht unterstützt.

## Überblick

In einigen Umgebungen möchten Kunden einen Router über vPC mit einem Paar Nexus-Switches verbinden und über den vPC mit beiden vPC-Peers Unicast-Routing-Protokoll-Nachbarschaften bilden. Alternativ können Kunden einen Router über ein vPC-VLAN mit einem einzelnen vPC-Peer verbinden und über das vPC-VLAN mit beiden vPC-Peers Unicast-Routing-Protokoll-Nachbarschaften bilden. Daher hätte der mit vPC verbundene Router Equal-Cost Multi-Path (ECMP) für Präfixe, die von beiden Nexus-Switches angekündigt werden. Dies ist möglicherweise besser als die Verwendung dedizierter Routing-Verbindungen zwischen dem mit vPC verbundenen Router und beiden vPC-Peers, um die Nutzung von IP-Adressen zu sparen (3 IP-Adressen anstelle von 4 IP-Adressen erforderlich) oder die Konfigurationskomplexität zu verringern (geroutete Schnittstellen neben SVIs, insbesondere in VRF-Lite-Umgebungen, die Subschnittstellen erfordern).

Bislang wurde die Bildung von Unicast-Routing-Protokoll-Nachbarschaften über einen vPC auf Cisco Nexus-Plattformen nicht unterstützt. Es ist jedoch möglich, dass Kunden eine Topologie implementiert haben, in der Unicast-Routing-Protokoll-Nachbarschaften über einen vPC ohne Probleme entstehen, auch wenn diese nicht unterstützt werden. Nach einigen Änderungen im Netzwerk (z. B. einem Software-Upgrade des mit vPC verbundenen Routers oder der vPC-Peers selbst, einem Firewall-Failover usw.) funktionieren die Nachbarschaften des Unicast-Routing-Protokolls über einen vPC nicht mehr. Dies führt entweder zu Paketverlusten für den Datenverkehr auf Datenebene oder zu Unicast-Routing-Protokoll-Nachbarschaften, bei denen ein oder beide vPC-Peers nicht verfügbar sind. Die technischen Details, warum diese Szenarien fehlschlagen und nicht unterstützt werden, werden im Abschnitt Beispielszenarien dieses Dokuments behandelt.

Die Routing/Layer 3 over vPC-Erweiterung wurde eingeführt, um die Unterstützung für die Bildung von Unicast-Routing-Protokoll-Nachbarschaften über einen vPC hinzuzufügen. Zu diesem Zweck können Unicast-Routing-Protokollpakete mit einer TTL von 1 über den vPC-Peer-Link weitergeleitet werden, ohne dass die TTL des Pakets herabgesetzt wird. Dadurch können Unicast-Routing-Protokoll-Nachbarschaften problemlos über einen vPC oder ein vPC-VLAN gebildet werden. Die Erweiterung "Routing/Layer 3 over vPC" kann mit dem Konfigurationsbefehl **layer3 peer-router** vPC domain aktiviert werden, nachdem die Erweiterung "vPC Peer Gateway" mit dem Befehl "**peer-gateway** vPC domain configuration" aktiviert wurde.

NX-OS-Softwareversionen, mit denen die Unterstützung der Routing/Layer 3 over vPC-Erweiterung für jede Cisco Nexus-Plattform eingeführt wurde, sind in Tabelle 2 ("Routing Protocols Adjacencies Support over vPC VLANs") im Dokument "Supported Topology for Routing over Virtual Port Channel on Nexus Platforms" aufgeführt.

## Hinweise

### Gelegentliche VPC-2-L3_VPC_UNEQUAL_WEIGHT-Syslogs

Wenn die Erweiterung "Routing/Layer 3 über vPC" aktiviert ist, beginnen beide vPC-Peers einmal stündlich Syslogs zu generieren, die einem der folgenden ähneln:

```
2021 May 26 19:13:47.079 switch %VPC-2-L3_VPC_UNEQUAL_WEIGHT: Layer3 peer-router is enabled.
Please make sure both vPC peers have the same L3 routing configuration.
2021 May 26 19:13:47.351 switch %VPC-2-L3_VPC_UNEQUAL_WEIGHT: Unequal weight routing is not
supported in L3 over vPC. Please make sure both vPC peers have equal link cost configuration
```

Keines dieser Syslogs weist auf ein Problem mit dem Switch hin. Bei diesen Syslogs handelt es sich um Warnungen an den Administrator, dass Routing-Konfiguration, Kosten und Gewichtung auf beiden vPC-Peers identisch sein sollten, wenn die Erweiterung Routing/Layer 3 über vPC aktiviert ist, um sicherzustellen, dass beide vPC-Peers den Datenverkehr identisch weiterleiten können. Es weist nicht unbedingt darauf hin, dass eine falsche Routing-Konfiguration, falsche Kosten oder falsche Gewichtung auf einem vPC-Peer vorhanden sind.

Diese Syslogs können mithilfe der hier gezeigten Konfiguration deaktiviert werden.

```
switch# configure terminal
switch(config)# vpc domain 1
switch(config-vpc-domain)# no layer3 peer-router syslog
switch(config-vpc-domain)# end
switch#
```

Diese Konfiguration muss auf beiden vPC-Peers durchgeführt werden, um das Syslog auf beiden vPC-Peers zu deaktivieren.

### Datenverkehr auf Datenebene mit TTL von 1 Software aufgrund von Cisco Bug-ID CSCvs82183 weitergeleitet und Cisco Bug-ID CSCvw16965

Wenn die Erweiterung für Routing/Layer 3 über vPC auf Switches der Serie Nexus 9000 aktiviert ist, die mit einem Cloud Scale ASIC ausgestattet sind, auf dem eine NX-OS-Softwareversion vor der NX-OS-Softwareversion 9.3(6) ausgeführt wird, wird Datenverkehr auf Datenebene, der keinem Unicast-Routing-Protokoll mit einer TTL von 1 zugeordnet ist, an den Supervisor gesendet und in der Software anstatt in der Hardware weitergeleitet. Je nachdem, ob es sich bei dem Nexus-Switch um einen fest konfigurierten Switch (auch "Top of Rack" genannt) oder einen modularen Chassis-Switch (auch "End of Row" genannt) handelt und ob es sich um die aktuelle NX-OS-Softwareversion des Switches handelt, kann die Ursache für dieses Problem auf den Softwarefehler Cisco Bug-ID CSCvs82183 zurückgeführt werden. oder Softwarefehler Cisco Bug-ID CSCvw16965 . Beide Softwarefehler betreffen nur Switches der Serie Nexus 9000 mit einem Cloud Scale ASIC. Für andere Cisco Nexus Hardwareplattformen ist keines der beiden Probleme relevant. Weitere Informationen zu den einzelnen Softwarefehlern finden Sie in den entsprechenden Informationen.

Um diese Softwarefehler zu vermeiden, empfiehlt Cisco das Upgrade auf NX-OS Softwareversion 9.3(6) oder höher. Als allgemeine Empfehlung empfiehlt Cisco, regelmäßig ein Upgrade auf die aktuelle empfohlene NX-OS-Softwareversion für den Nexus Switch der Serie 9000 durchzuführen, wie im Dokument Empfohlene Cisco NX-OS-Versionen für Cisco Nexus Switches der Serie 9000 beschrieben.

## Konfiguration

Ein Beispiel für die Konfiguration der Routing-/Layer 3-over-vPC-Erweiterung finden Sie hier.

In diesem Beispiel sind N9K-1 und N9K-2 vPC-Peers in einer vPC-Domäne. Für beide vPC-Peers ist die vPC-Peer-Gateway-Erweiterung bereits aktiviert. Dies ist erforderlich, um die Erweiterung Routing/Layer 3 over vPC zu aktivieren. Beide vPC-Peers verfügen über eine SVI im VLAN 10, die

unter OSPF-Prozess 1 aktiviert ist. N9K-1 und N9K-3 sind in einem OSPF-EXSTART/EXCHANGE-Status mit einem über vPC verbundenen OSPF-Router mit der IP-Adresse und der Nachbar-ID 192.168.10.3 stecken.

```
N9K-1# show running-config vpc
<snip>
vpc domain 1
  role priority 150
  peer-keepalive destination 10.122.190.196
  peer-gateway

interface port-channel1
  vpc peer-link

N9K-2# show running-config vpc
<snip>
vpc domain 1
  peer-keepalive destination 10.122.190.195
  peer-gateway

interface port-channel1
  vpc peer-link

N9K-1# show running-config interface Vlan10

interface Vlan10
  no shutdown
  no ip redirects
  ip address 192.168.10.1/24
  no ipv6 redirects
  ip router ospf 1 area 0.0.0.0

N9K-2# show running-config interface Vlan10

interface Vlan10
  no shutdown
  no ip redirects
  ip address 192.168.10.2/24
  no ipv6 redirects
  ip router ospf 1 area 0.0.0.0

N9K-1# show running-config ospf

feature ospf

router ospf 1

interface Vlan10
  ip router ospf 1 area 0.0.0.0

N9K-2# show running-config ospf

feature ospf

router ospf 1

interface Vlan10
  ip router ospf 1 area 0.0.0.0

N9K-1# show ip ospf neighbors
 OSPF Process ID 1 VRF default
 Total number of neighbors: 3
```

```
 Neighbor ID     Pri State            Up Time  Address         Interface
 192.168.10.2      1 TWOWAY/DROTHER   00:08:10 192.168.10.2    Vlan10
 192.168.10.3      1 EXCHANGE/BDR     00:07:43 192.168.10.3    Vlan10

N9K-2# show ip ospf neighbors
 OSPF Process ID 1 VRF default
 Total number of neighbors: 3
 Neighbor ID     Pri State            Up Time  Address         Interface
 192.168.10.1      1 TWOWAY/DROTHER   00:08:21 192.168.10.1    Vlan10
 192.168.10.3      1 EXSTART/BDR      00:07:48 192.168.10.3    Vlan10
```

Wir können die Erweiterung Routing/Layer 3 over vPC über den Konfigurationsbefehl **layer3 peer-router** vPC domain aktivieren. Dadurch wird verhindert, dass ein vPC-Peer die TTL von Unicast-Routing-Protokollpaketen herabsetzt, die als Folge der Aktivierung der vPC-Peer-Gateway-Erweiterung geroutet werden.

```
N9K-1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
N9K-1(config)# vpc domain 1
N9K-1(config-vpc-domain)# layer3 peer-router
N9K-1(config-vpc-domain)# end
N9K-1#

N9K-2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
N9K-2(config)# vpc domain 1
N9K-2(config-vpc-domain)# layer3 peer-router
N9K-2(config-vpc-domain)# end
N9K-2#
```

Sie können überprüfen, ob die Erweiterung für Routing/Layer 3 über vPC erwartungsgemäß funktioniert, indem Sie validieren, ob die OSPF-Adjacency mit dem über vPC verbundenen OSPF-Nachbarn in den FULL-Status wechselt, kurz nachdem die Erweiterung für Routing/Layer 3 über vPC aktiviert wurde.

```
N9K-1# show ip ospf neighbors
 OSPF Process ID 1 VRF default
 Total number of neighbors: 3
 Neighbor ID     Pri State            Up Time  Address         Interface
 192.168.10.2      1 TWOWAY/DROTHER   00:12:17 192.168.10.2    Vlan10
 192.168.10.3      1 FULL/BDR         00:00:29 192.168.10.3    Vlan10

N9K-2# show ip ospf neighbors
 OSPF Process ID 1 VRF default
 Total number of neighbors: 3
 Neighbor ID     Pri State            Up Time  Address         Interface
 192.168.10.1      1 TWOWAY/DROTHER   00:12:27 192.168.10.1    Vlan10
 192.168.10.3      1 FULL/BDR         00:00:19 192.168.10.3    Vlan10
```

## Auswirkungen

Die Aktivierung der Erweiterung Routing/Layer 3 über vPC hat keine inhärenten Auswirkungen auf die vPC-Domäne. Wenn Sie also die Erweiterung Routing/Layer 3 über vPC aktivieren, werden vPCs weder vom vPC-Peer ausgesetzt noch der Datenverkehr auf Datenebene durch die Aktivierung dieser Erweiterung beeinträchtigt.

Wenn jedoch dynamische Routing-Protokoll-Adjacencies, die zuvor deaktiviert waren, weil die Routing/Layer 3 over vPC-Erweiterung nicht aktiviert war, plötzlich aktiviert werden, weil diese Erweiterung aktiviert wurde, dann kann es je nach Rolle der betroffenen Routing-Protokoll-Adjacencies, der über diese Adjacencies gemeldeten spezifischen Präfixe und des aktuellen Status der Unicast-Routing-Tabelle zu Unterbrechungen kommen, wenn Routing/Layer 3 über v PC-Erweiterung.

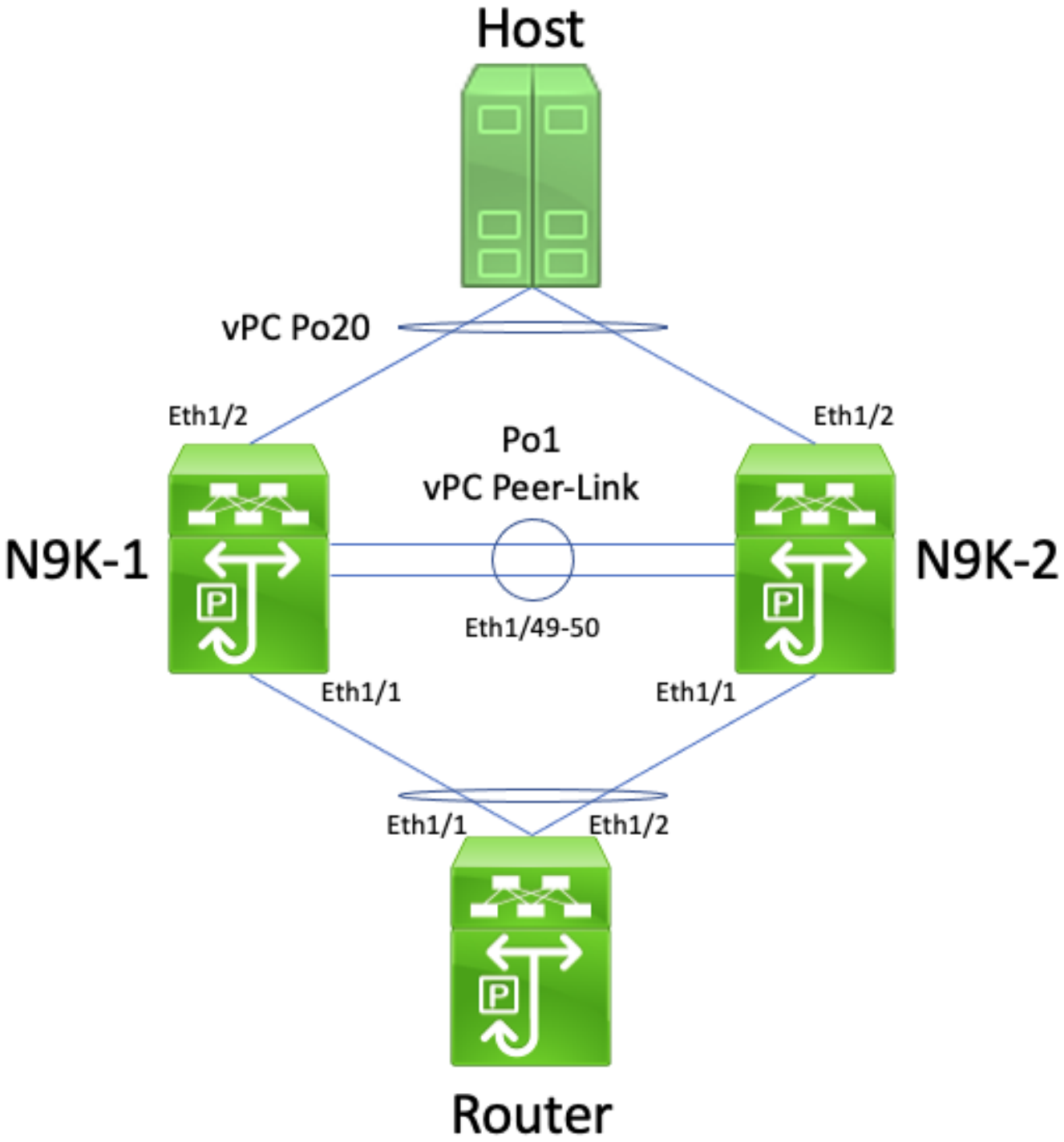
Aus diesem Grund empfiehlt Cisco, dass Kunden diese Erweiterung während eines Wartungsfensters aktivieren. Dabei wird davon ausgegangen, dass es zu Unterbrechungen auf der Kontroll- und Datenebene kommen kann, es sei denn, die Kunden sind äußerst zuversichtlich, dass die betroffenen Routing-Protokoll-Nachbarschaften den Betrieb des Netzwerks nicht wesentlich beeinträchtigen.

Cisco empfiehlt außerdem, den Abschnitt "Hinweise" in diesem Dokument eingehend auf Softwarefehler zu überprüfen, die sich auf Ihre NX-OS-Softwareversion auswirken und dazu führen können, dass Datenverkehr auf natürlicher Datenebene mit einem TTL von 1 nicht in der Hardware, sondern in der Software verarbeitet wird.

## Beispiele für Fehlerszenarien

### Unicast-Routing-Protokoll-Adjacencies über vPC ohne vPC-Peer-Gateway

Betrachten Sie die hier abgebildete Topologie:




In dieser Topologie sind die Nexus Switches N9K-1 und N9K-2 vPC-Peers in einer vPC-Domäne, in der die vPC-Peer-Gateway-Erweiterung nicht aktiviert ist. Die Schnittstelle Po1 ist der vPC-Peer-Link. Ein Router mit dem Hostnamen Router ist über vPC Po10 mit N9K-1 und N9K-2 verbunden. Ein Host ist über vPC Po20 mit N9K-1 und N9K-2 verbunden. Die Po10-Schnittstelle des Routers ist ein gerouteter Port-Channel, der unter einem Unicast-Routing-Protokoll aktiviert wird. Für N9K-1 und N9K-2 sind SVI-Schnittstellen unter demselben Unicast-Routing-Protokoll aktiviert und befinden sich in derselben Broadcast-Domäne wie der Router.

Unicast-Routing-Protokoll-Nachbarschaften über einen vPC, bei denen die vPC-Peer-Gateway-Erweiterung nicht aktiviert ist, werden nicht unterstützt, da die ECMP-Hashing-Entscheidung des vPC-verbundenen Routers und die Layer-2-Port-Channel-Hashing-Entscheidung voneinander abweichen können. In dieser Topologie würden sich erfolgreich Routing-Protokoll-Nachbarschaften zwischen Router, N9K-1 und N9K-2 bilden. Berücksichtigen Sie den Datenverkehrsfluss zwischen Router und Host. Datenverkehr auf Datenebene, der den Router

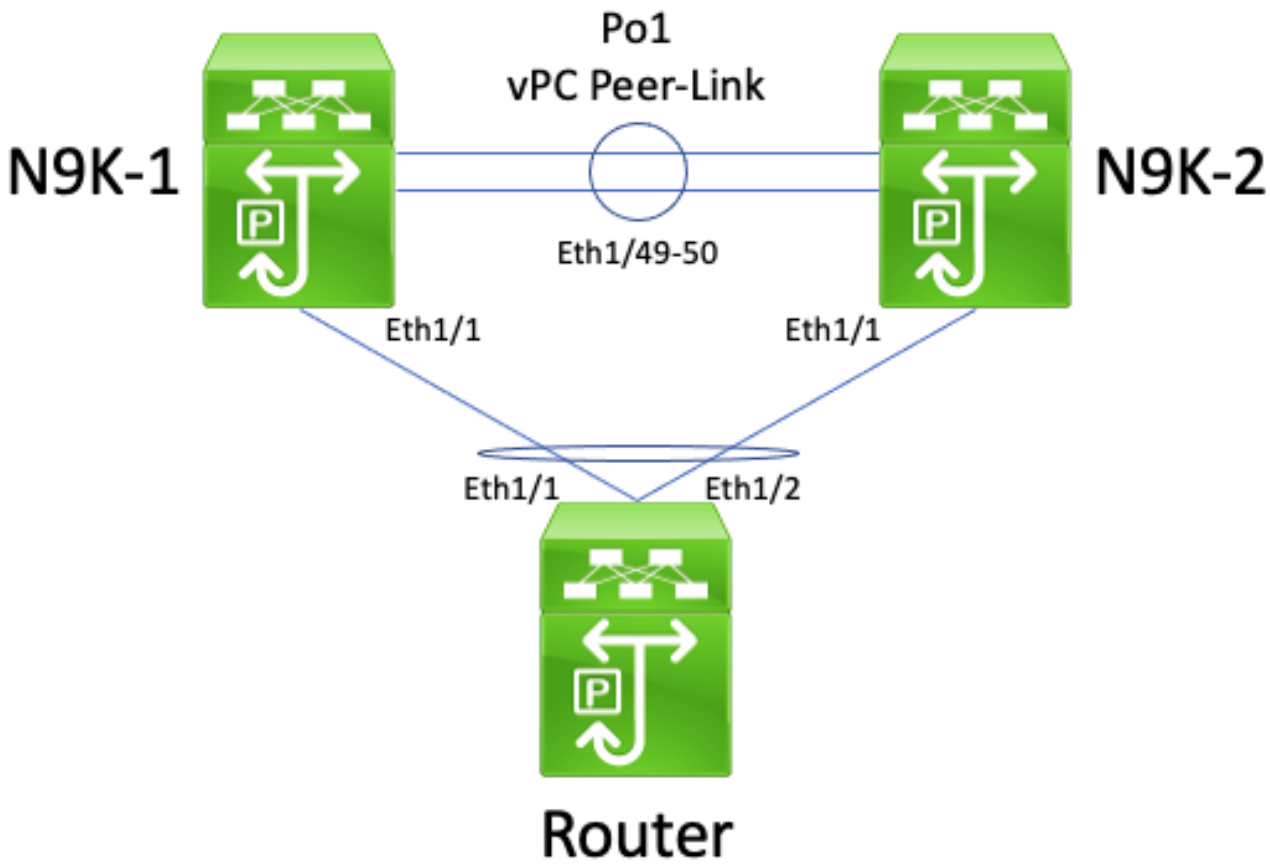
zum Host durchquert, kann mit einer MAC-Zieladresse neu geschrieben werden, die zur SVI-MAC-Adresse von N9K-1 gehört (aufgrund der vom Router getroffenen ECMP-Hashing-Entscheidung), jedoch ausgehend von der Schnittstelle Ethernet1/2 (aufgrund der vom Router getroffenen Layer-2-Port-Channel-Hashing-Entscheidung).

N9K-2 empfängt dieses Paket und leitet es über den vPC-Peer-Link weiter, da die Ziel-MAC-Adresse zu N9K-1 gehört und die vPC-Peer-Gateway-Erweiterung (mit der N9K-2 das Paket für N9K-1 weiterleiten kann) nicht aktiviert ist. N9K-1 empfängt dieses Paket über den vPC-Peer-Link und erkennt, dass es aus seinem Ethernet1/2 in vPC Po20 weitergeleitet werden muss. Dies verstößt gegen die vPC-Schleifenvermeidungsregel, d. h. N9K-1 verwirft das Paket in der Hardware. Daher können Sie bei einigen Datenströmen, die in dieser Topologie die vPC-Domäne durchlaufen, Verbindungsprobleme oder Paketverluste beobachten.

Sie können dieses Problem beheben, indem Sie die vPC-Peer-Gateway-Erweiterung mit dem vPC-Domänenkonfigurationsbefehl **Peer-Gateway** und dann die Erweiterung Routing/Layer 3 über vPC mit dem Befehl **layer3 Peer-Router** vPC-Domänenkonfiguration aktivieren. Um Unterbrechungen auf ein Minimum zu reduzieren, sollten Sie beide vPC-Erweiterungen in schneller Folge aktivieren, sodass das Fehlerszenario, das in den Unicast Routing Protocol-Nachbarschaften über einen vPC mit vPC-Peer-Gateway beschrieben wird, keine Zeit hat.

### Unicast Routing Protocol-Adjacencies über einen vPC mit vPC-Peer-Gateway

Betrachten Sie die hier abgebildete Topologie:




In dieser Topologie sind die Nexus Switches N9K-1 und N9K-2 vPC-Peers in einer vPC-Domäne, in der die vPC-Peer-Gateway-Erweiterung aktiviert ist. Die Schnittstelle Po1 ist der vPC-Peer-Link. Ein Router mit dem Hostnamen Router ist über vPC Po10 mit N9K-1 und N9K-2 verbunden. Die

Po10-Schnittstelle des Routers ist ein gerouteter Port-Channel, der unter einem Unicast-Routing-Protokoll aktiviert wird. Für N9K-1 und N9K-2 sind SVI-Schnittstellen unter demselben Unicast-Routing-Protokoll aktiviert und befinden sich in derselben Broadcast-Domäne wie der Router.

Unicast-Routing-Protokoll-Nachbarschaften über einen vPC mit aktivierter vPC-Peer-Gateway-Erweiterung werden nicht unterstützt, da die vPC-Peer-Gateway-Erweiterung verhindern könnte, dass Unicast-Routing-Protokoll-Nachbarschaften zwischen dem mit vPC verbundenen Router und beiden vPC-Peers entstehen. In dieser Topologie kann es vorkommen, dass eine Routing-Protokoll-Adjacency zwischen dem Router und N9K-1 oder N9K-2 nicht wie erwartet verfügbar ist, je nachdem, wie die Unicast-Routing-Protokollpakete vom Router an den N9K-1- oder N9K-2-Hash über vPC-Po10 gesendet wurden.

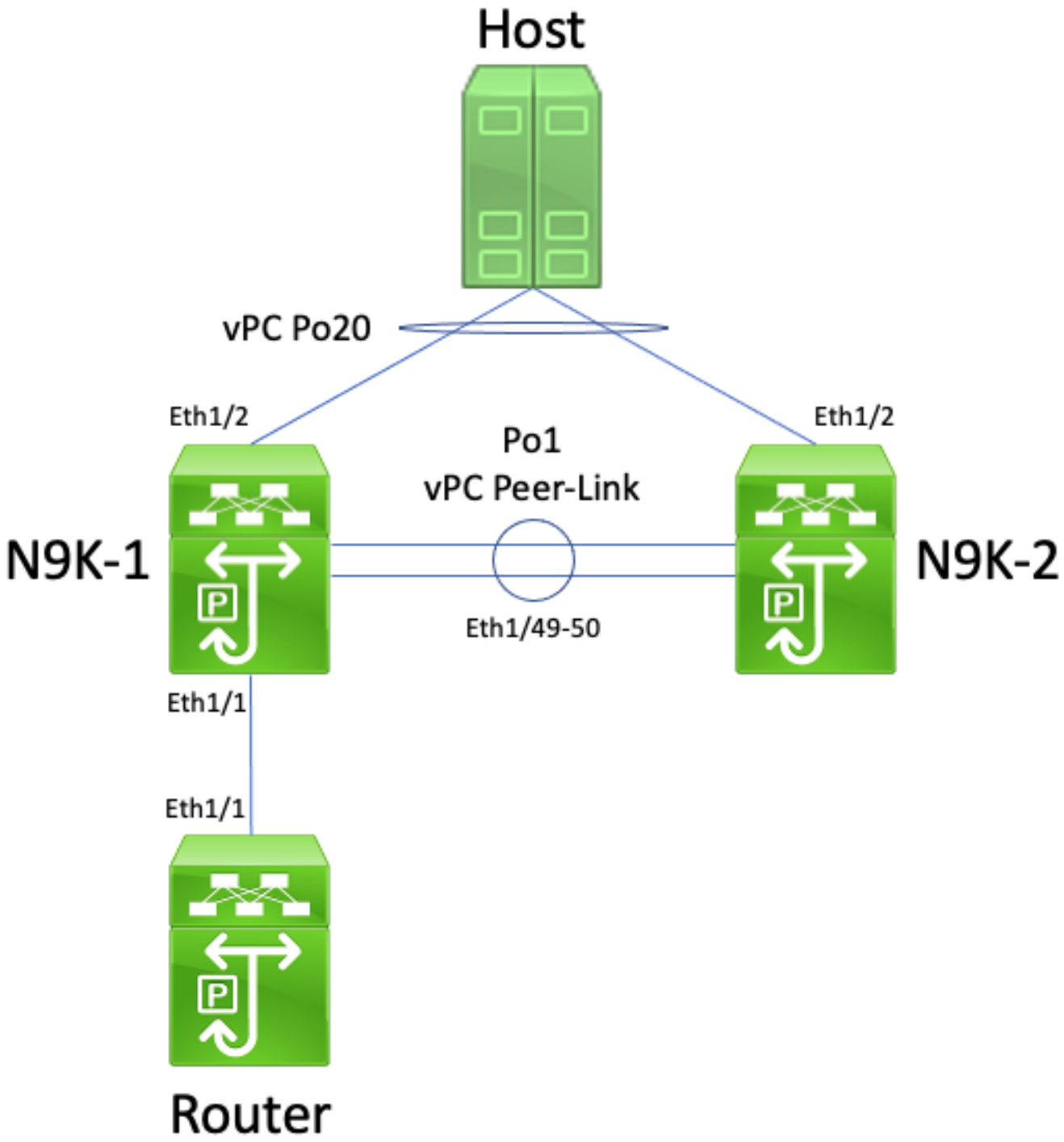
Alle Router können verbindungslokale Multicast-Routing-Protokollpakete (allgemein als "Hello"-Pakete bezeichnet) problemlos senden und empfangen, da diese Pakete erfolgreich an das vPC-VLAN geflutet werden. Stellen Sie sich jedoch ein Szenario vor, in dem ein vom Router stammendes Unicast-Routing-Protokollpaket, das für N9K-1 bestimmt ist, aufgrund der Layer-2-Port-Channel-Hashing-Entscheidung des Routers Ethernet1/2 in Richtung N9K-2 verlässt. Dieses Paket ist an die SVI-MAC-Adresse von N9K-1 gerichtet, aber an die Ethernet1/1-Schnittstelle von N9K-2. N9K-2 erkennt, dass das Paket an die SVI-MAC-Adresse von N9K-1 gerichtet ist, die in der MAC-Adresstabelle von N9K-2 mit dem Kennzeichen "G" oder "Gateway" installiert ist, da die vPC-Peer-Gateway-Erweiterung aktiviert ist. Daher versucht N9K-2, das Unicast-Routing-Protokollpaket im Auftrag von N9K-1 lokal zu routen.

Beim Routing des Pakets wird jedoch die Time to Live (TTL) des Pakets dekrementiert, und die TTL der meisten Unicast-Routing-Protokollpakete ist 1. Dadurch wird die TTL des Pakets auf 0 dekrementiert und von N9K-2 verworfen. Aus Sicht von N9K-1 empfängt N9K-1 verbindungslokale Multicast-Routing-Protokollpakete vom Router und ist in der Lage, Unicast-Routing-Protokollpakete an den Router zu senden, empfängt jedoch keine Unicast-Routing-Protokollpakete vom Router. Dadurch wird die Routing-Protokoll-Adjacency zum Router von N9K-1 entfernt, und der lokale Finite-State-Computer für das Routing-Protokoll wird neu gestartet. Entsprechend startet der Router seinen lokalen Finite-State-Computer für das Routing-Protokoll neu.

Sie können dieses Problem beheben, indem Sie die Erweiterung Routing/Layer 3 über vPC mit dem Konfigurationsbefehl für die vPC-Domäne des **Layer-3-Peer-Routers** aktivieren. Auf diese Weise können Unicast-Routing-Protokollpakete mit einer TTL von 1 über den vPC-Peer-Link weitergeleitet werden, ohne dass die TTL des Pakets herabgesetzt werden muss. Dadurch können Unicast-Routing-Protokoll-Nachbarschaften problemlos über einen vPC oder ein vPC-VLAN gebildet werden.

### Unicast-Routing-Protokoll-Adjacencies über ein vPC-VLAN ohne vPC-Peer-Gateway

Betrachten Sie die hier abgebildete Topologie:




In dieser Topologie sind die Nexus Switches N9K-1 und N9K-2 vPC-Peers in einer vPC-Domäne, in der die vPC-Peer-Gateway-Erweiterung nicht aktiviert ist. Die Schnittstelle Po1 ist der vPC-Peer-Link. Ein Router mit dem Hostnamen Router ist über Ethernet1/1 mit Ethernet1/1 von N9K-1 verbunden. Die Ethernet1/1-Schnittstelle des Routers ist eine geroutete Schnittstelle, die unter einem Unicast-Routing-Protokoll aktiviert wird. Für N9K-1 und N9K-2 sind SVI-Schnittstellen unter demselben Unicast-Routing-Protokoll aktiviert und befinden sich in derselben Broadcast-Domäne wie der Router.

Unicast-Routing-Protokoll-Adjacencies über ein vPC-VLAN, ohne dass die vPC-Peer-Gateway-Erweiterung aktiviert ist, werden nicht unterstützt, da die ECMP-Hashing-Entscheidung des vPC-VLAN-verbundenen Routers N9K-2 dazu veranlassen kann, Datenverkehr auf Datenebene wegen Verletzung der vPC-Schleifenvermeidungsregel zu verwerfen. In dieser Topologie würden sich erfolgreich Routing-Protokoll-Nachbarschaften zwischen Router, N9K-1 und N9K-2 bilden. Berücksichtigen Sie den Datenverkehrsfluss zwischen Router und Host. Datenverkehr auf

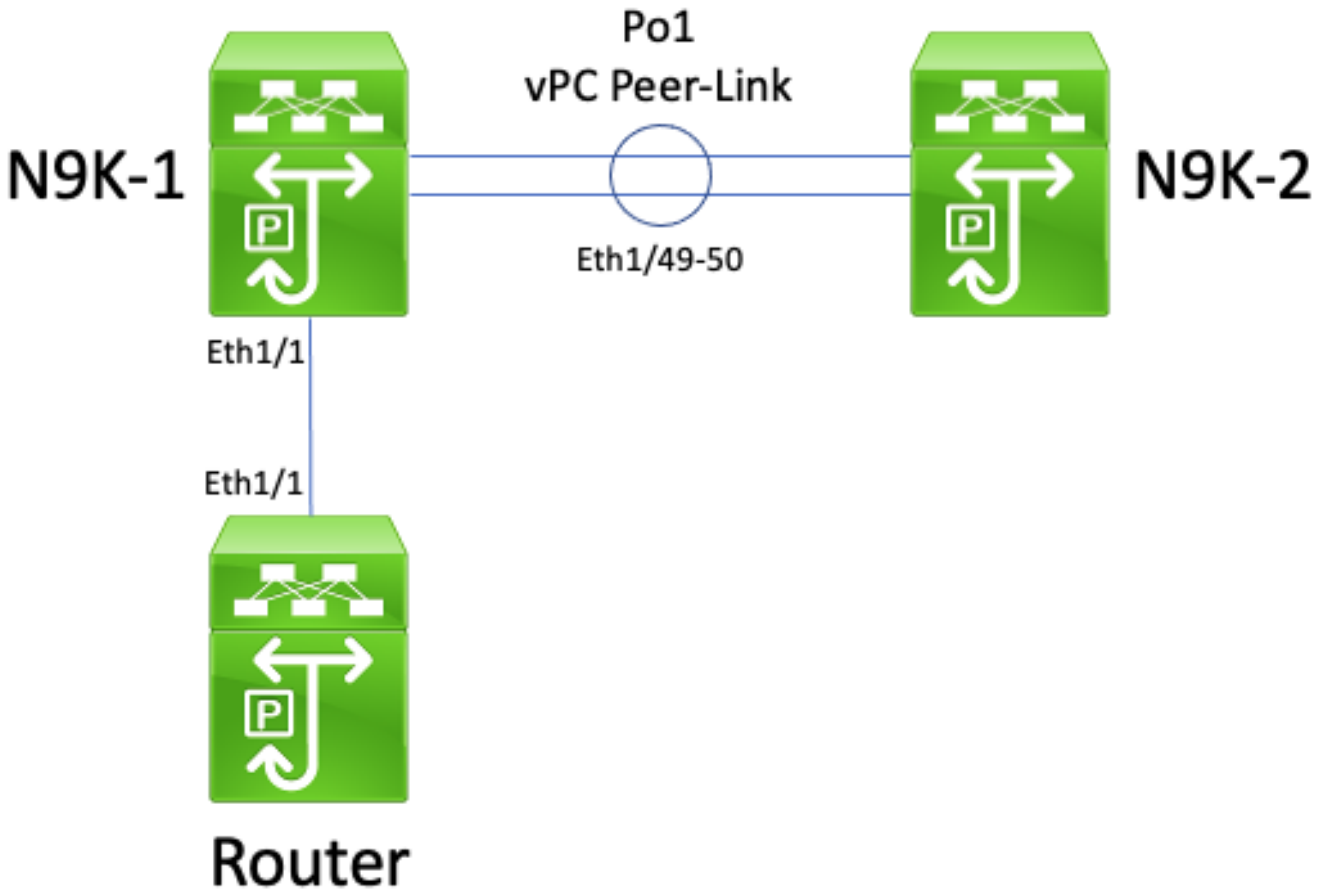
Datenebene, der den Router durchquert und für den Host bestimmt ist, kann mit einer MAC-Zieladresse, die zur SVI-MAC-Adresse von N9K-2 gehört (aufgrund der vom Router getroffenen ECMP-Hashing-Entscheidung), neu geschrieben werden und von der Schnittstelle Ethernet1/1 zu N9K-1 ausgehen.

N9K-1 empfängt dieses Paket und leitet es über den vPC-Peer-Link weiter, da die Ziel-MAC-Adresse zu N9K-2 gehört und die vPC-Peer-Gateway-Erweiterung (die es N9K-1 ermöglicht, das Paket für N9K-2 weiterzuleiten) nicht aktiviert ist. N9K-2 empfängt dieses Paket über den vPC-Peer-Link und erkennt, dass es aus seinem Ethernet1/2 in vPC Po20 weitergeleitet werden muss. Dies verstößt gegen die vPC-Schleifenvermeidungsregel, d. h. N9K-2 verwirft das Paket in der Hardware. Daher können Sie bei einigen Datenströmen, die in dieser Topologie die vPC-Domäne durchlaufen, Verbindungsprobleme oder Paketverluste beobachten.

Sie können dieses Problem beheben, indem Sie die vPC-Peer-Gateway-Erweiterung mit dem vPC-Domänenkonfigurationsbefehl **Peer-Gateway** und dann die Erweiterung Routing/Layer 3 über vPC mit dem Befehl **layer3 Peer-Router** vPC-Domänenkonfiguration aktivieren. Um Unterbrechungen auf ein Minimum zu reduzieren, sollten Sie beide vPC-Erweiterungen in schneller Folge aktivieren, sodass das Fehlerszenario, das in den Unicast Routing Protocol-Nachbarschaften über einen vPC mit vPC-Peer-Gateway beschrieben wird, keine Zeit hat.

### Unicast-Routing-Protokoll-Adjacencies über ein vPC-VLAN mit vPC-Peer-Gateway

Betrachten Sie die hier abgebildete Topologie:




In dieser Topologie sind die Nexus Switches N9K-1 und N9K-2 vPC-Peers in einer vPC-Domäne, in der die vPC-Peer-Gateway-Erweiterung aktiviert ist. Die Schnittstelle Po1 ist der vPC-Peer-Link. Ein Router mit dem Hostnamen Router ist über Ethernet1/1 mit Ethernet1/1 von N9K-1 verbunden.

Die Ethernet1/1-Schnittstelle des Routers ist eine geroutete Schnittstelle, die unter einem Unicast-Routing-Protokoll aktiviert wird. Für N9K-1 und N9K-2 sind SVI-Schnittstellen unter demselben Unicast-Routing-Protokoll aktiviert und befinden sich in derselben Broadcast-Domäne wie der Router.

Unicast-Routing-Protokoll-Nachbarschaften über ein vPC-VLAN mit aktivierter vPC-Peer-Gateway-Erweiterung werden nicht unterstützt, da die vPC-Peer-Gateway-Erweiterung verhindert, dass sich zwischen dem mit dem vPC-VLAN verbundenen Router und dem vPC-Peer, mit dem der mit dem vPC-VLAN verbundene Router nicht direkt verbunden ist, Unicast-Routing-Protokoll-Nachbarschaften bilden. In dieser Topologie wird eine Routing-Protokoll-Adjacency zwischen Router und N9K-2 nicht wie erwartet angezeigt, da Pakete des Routing-Unicast-Routing-Protokolls vom Typ N9K-1, die an die SVI MAC-Adresse von N9K-2 gerichtet sind, aufgrund der Aktivierung der vPC-Peer-Gateway-Erweiterung nicht verfügbar sind. Da die Pakete geroutet werden, muss ihre Time To Live (TTL) verringert werden. Unicast-Routing-Protokollpakete haben in der Regel eine TTL von 1, und ein Router, der die TTL eines Pakets auf 0 herabsetzt, muss dieses Paket verwerfen.

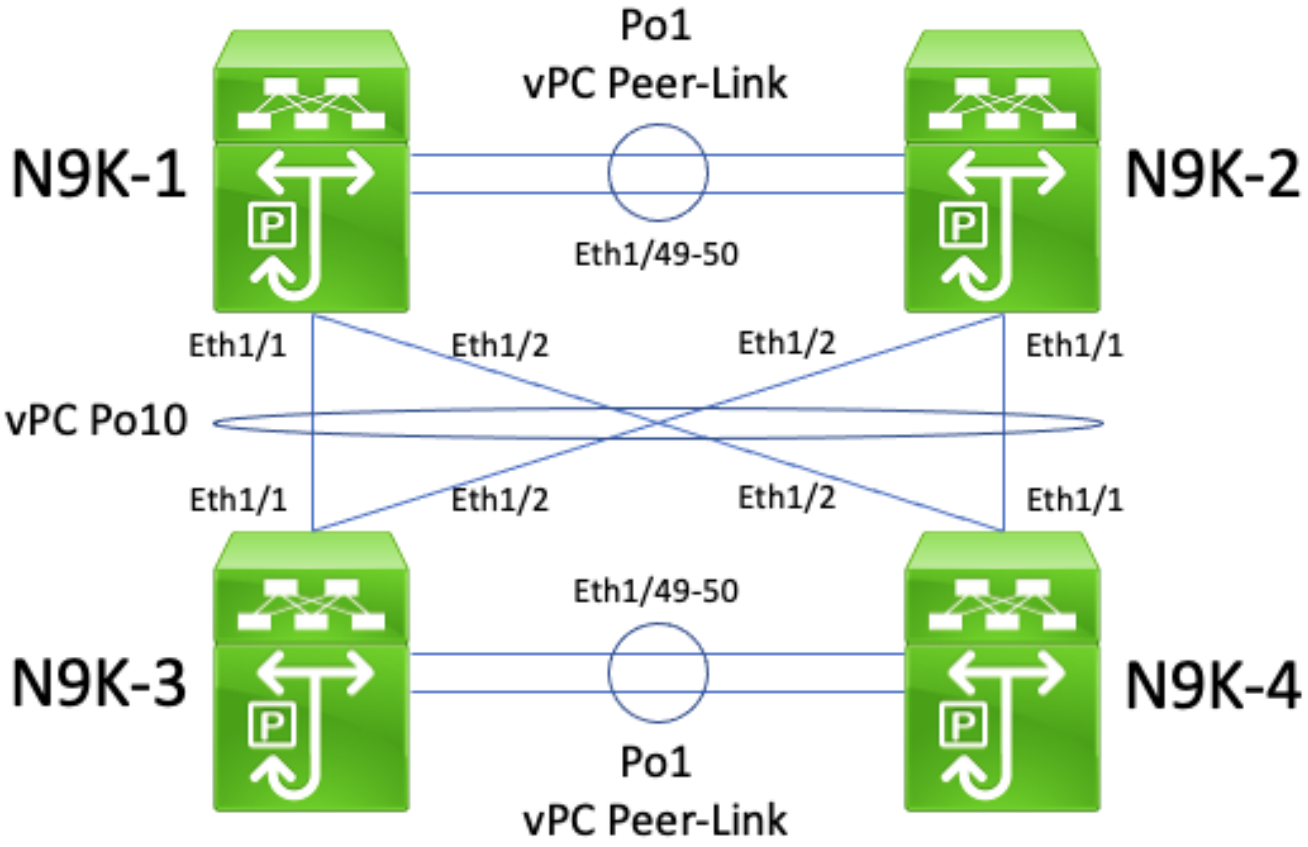
Alle Router können verbindungslokale Multicast-Routing-Protokollpakete (allgemein als "Hello"-Pakete bezeichnet) problemlos senden und empfangen, da diese Pakete erfolgreich an das vPC-VLAN geflutet werden. Stellen Sie sich jedoch ein Szenario vor, in dem ein vom Router stammendes Unicast-Routing-Protokollpaket, das für N9K-2 bestimmt ist, Ethernet1/1 in Richtung N9K-1 verlässt. Dieses Paket ist für die SVI-MAC-Adresse von N9K-2 bestimmt, jedoch für die Ethernet1/1-Schnittstelle von N9K-1. N9K-1 erkennt, dass das Paket an die SVI-MAC-Adresse von N9K-2 gerichtet ist, die in der MAC-Adresstabelle von N9K-1 mit dem Kennzeichen "G" oder "Gateway" installiert ist, da die vPC-Peer-Gateway-Erweiterung aktiviert ist. Daher versucht N9K-1, das Unicast-Routing-Protokollpaket im Auftrag von N9K-2 lokal zu routen.

Beim Routing des Pakets wird jedoch die TTL des Pakets dekrementiert, und die TTL der meisten Unicast-Routing-Protokollpakete ist 1. Dadurch wird die TTL des Pakets auf 0 dekrementiert und von N9K-1 verworfen. Aus Sicht von N9K-2 empfängt N9K-2 verbindungslokale Multicast-Routing-Protokollpakete vom Router und ist in der Lage, Unicast-Routing-Protokollpakete an den Router zu senden, empfängt jedoch keine Unicast-Routing-Protokollpakete vom Router. Als Ergebnis trennt N9K-2 die Routing-Protokoll-Adjacency mit dem Router und startet seinen lokalen Finite-State-Computer für das Routing-Protokoll neu. Entsprechend startet der Router seinen lokalen Finite-State-Computer für das Routing-Protokoll neu.

Sie können dieses Problem beheben, indem Sie die Erweiterung Routing/Layer 3 über vPC mit dem Konfigurationsbefehl für die vPC-Domäne des **Layer-3-Peer-Routers** aktivieren. Auf diese Weise können Unicast-Routing-Protokollpakete mit einer TTL von 1 über den vPC-Peer-Link weitergeleitet werden, ohne dass die TTL des Pakets herabgesetzt werden muss. Dadurch können Unicast-Routing-Protokoll-Nachbarschaften problemlos über einen vPC oder ein vPC-VLAN gebildet werden.

### Unicast Routing Protocol-Adjacencies über Back-to-Back-vPC mit vPC-Peer-Gateway

Betrachten Sie die hier abgebildete Topologie:



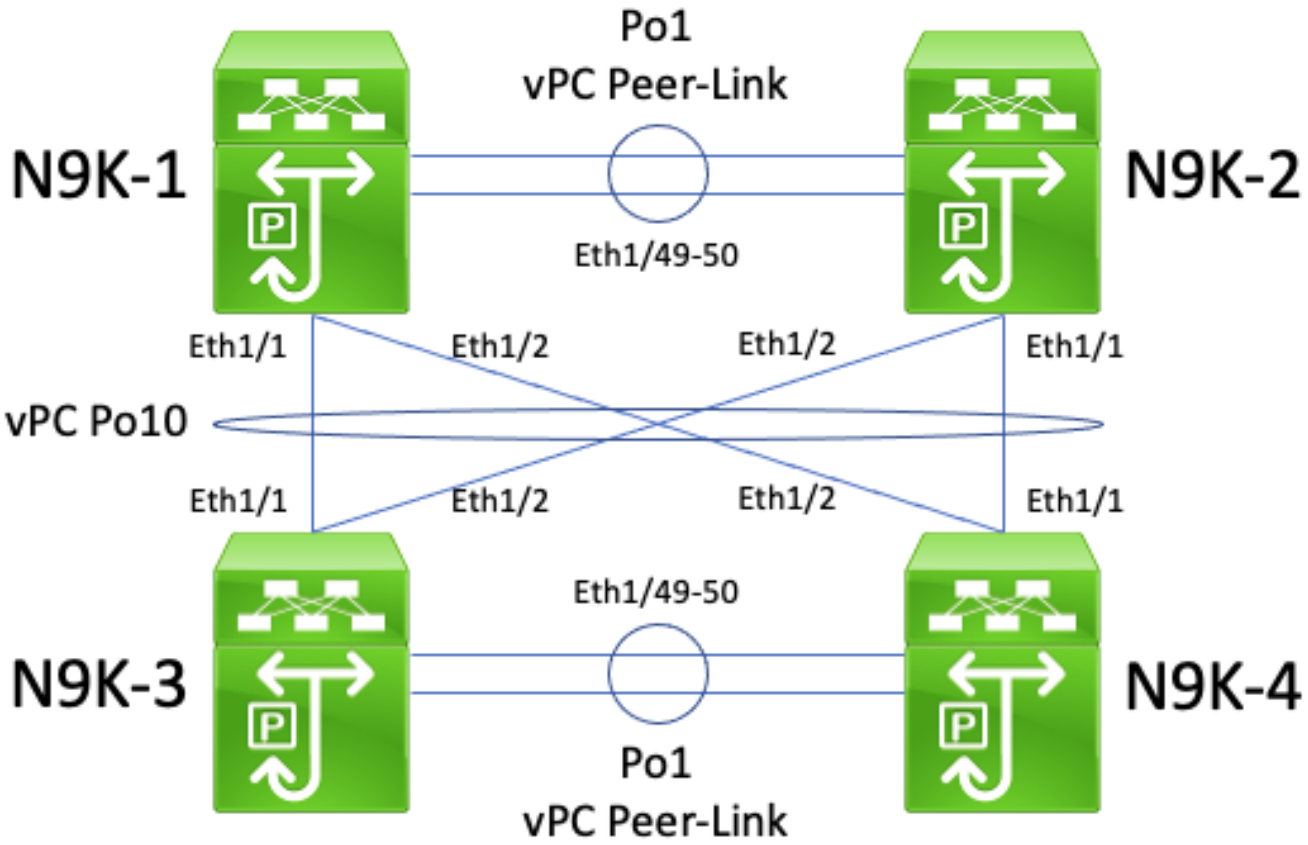

In dieser Topologie sind die Nexus Switches N9K-1 und N9K-2 vPC-Peers in einer vPC-Domäne, in der die vPC-Peer-Gateway-Erweiterung aktiviert ist. Die Nexus Switches N9K-3 und N9K-4 sind vPC-Peers innerhalb einer vPC-Domäne, in der die vPC-Peer-Gateway-Erweiterung aktiviert ist. Beide vPC-Domänen sind über einen Back-to-Back-vPC-Po10 miteinander verbunden. Alle vier Switches verfügen über SVI-Schnittstellen, die unter einem Unicast-Routing-Protokoll aktiviert sind, und befinden sich in derselben Broadcast-Domäne.

Unicast-Routing-Protokoll-Adjacencies in Back-to-Back-vPCs mit aktivierter vPC-Peer-Gateway-Erweiterung werden nicht unterstützt, da die vPC-Peer-Gateway-Erweiterung verhindern kann, dass Unicast-Routing-Protokoll-Adjacencies zwischen einer vPC-Domäne und einer anderen vPC-Domäne entstehen. In dieser Topologie kann eine Routing-Protokoll-Adjacency zwischen N9K-1 und entweder N9K-3 oder N9K-4 (oder beiden) nicht wie erwartet verfügbar sein. Ebenso kann eine Routing-Protokoll-Adjacency zwischen N9K-2 und entweder N9K-3 oder N9K-4 (oder beiden) erwartungsgemäß fehlschlagen. Dies liegt daran, dass Unicast-Routing-Protokollpakete an einen Router (z. B. N9K-3) gerichtet, aber an einen anderen Router (z. B. N9K-4) weitergeleitet werden können, basierend auf der Layer 2-Port-Channel-Hashing-Entscheidung des ursprünglichen Routers.

Die Ursache dieses Problems ist mit der im Abschnitt "Unicast Routing Protocol Adjacencies over a vPC with vPC Peer Gateway" dieses Dokuments beschriebenen Ursache identisch. Sie können dieses Problem beheben, indem Sie die Erweiterung Routing/Layer 3 über vPC mit dem Konfigurationsbefehl für die vPC-Domäne des **Layer-3-Peer-Routers** aktivieren. Auf diese Weise können Unicast-Routing-Protokollpakete mit einer TTL von 1 über den vPC-Peer-Link weitergeleitet werden, ohne dass die TTL des Pakets herabgesetzt werden muss. Dadurch können Unicast-Routing-Protokoll-Nachbarschaften problemlos über einen Back-to-Back-vPC gebildet werden.

**OSPF-Adjacencies über vPC mit vPC-Peer-Gateway, bei denen das Präfix in OSPF LSDB, aber nicht in der Routing-Tabelle vorhanden ist**

Betrachten Sie die hier abgebildete Topologie:




In dieser Topologie sind die Nexus Switches N9K-1 und N9K-2 vPC-Peers in einer vPC-Domäne, in der die vPC-Peer-Gateway-Erweiterung aktiviert ist. Die Nexus Switches N9K-3 und N9K-4 sind vPC-Peers innerhalb einer vPC-Domäne, in der die vPC-Peer-Gateway-Erweiterung aktiviert ist. Beide vPC-Domänen sind über einen Back-to-Back-vPC-Po10 miteinander verbunden. Alle vier Switches verfügen über SVI-Schnittstellen, die unter einem Unicast-Routing-Protokoll aktiviert sind, und befinden sich in derselben Broadcast-Domäne. N9K-4 ist der OSPF Designated Router (DR) für die Broadcast-Domäne, während N9K-3 der OSPF Backup Designated Router (BDR) für die Broadcast-Domäne ist.

In diesem Szenario wechselt eine OSPF-Adjacency zwischen N9K-1 und N9K-3 in den FULL-Status, da Unicast-OSPF-Pakete Ethernet1/1 beider Switches verlieren. Entsprechend wechselt eine OSPF-Adjacency zwischen N9K-2 und N9K-3 in den Status "FULL", da Unicast-OSPF-Pakete Ethernet1/2 beider Switches verlieren.

Eine OSPF-Adjacency zwischen N9K-1 und N9K-4 befindet sich jedoch im EXSTART- oder EXCHANGE-Zustand, da Unicast-OSPF-Pakete Ethernet1/1 beider Switches verlassen und von N9K-2 und N9K-4 verworfen werden, wie in den Unicast Routing Protocol-Adjacencies über Back-to-Back-vPC mit vPC Peak beschrieben. Weitere Informationen finden Sie im Abschnitt Gateway dieses Dokuments. Ähnlich ist eine OSPF-Adjacency zwischen N9K-2 und N9K-4 im EXSTART- oder EXCHANGE-Zustand blockiert, da Unicast-OSPF-Pakete Ethernet1/2 beider Switches verlassen und von N9K-1 und N9K-3 verworfen werden, wie im Abschnitt "Unicast Routing Protocol-Adjacencies over Back-to-Back vPC with vPC Peer Gateway" von beschrieben. dieses Dokuments.

Infolgedessen befinden sich N9K-1 und N9K-2 in einem VOLLSTÄNDIGEN Zustand mit dem BDR für die Broadcast-Domäne, jedoch in einem EXSTART- oder EXCHANGE-Zustand mit dem DR für die Broadcast-Domäne. Sowohl der DR als auch der BDR einer Broadcast-Domäne behalten eine

vollständige Kopie der OSPF Link State Data Base (LSDB) bei. OSPF-DROTHER-Router müssen jedoch den Zustand "FULL" mit dem DR für die Broadcast-Domäne aufweisen, um Präfixe zu installieren, die über OSPF vom DR oder BDR bezogen werden. Infolgedessen scheinen sowohl N9K-1 als auch N9K-2 Präfixe zu haben, die von N9K-3 und N9K-4 gelernt wurden, die in der OSPF-LSDB vorhanden sind. Diese Präfixe werden jedoch erst in der Unicast-Routing-Tabelle installiert, wenn N9K-1 und N9K-2 in den FULL-Zustand mit N9K-4 (der DR für die Broadcast-Domäne) übergehen.

Sie können dieses Problem beheben, indem Sie die Erweiterung Routing/Layer 3 über vPC mit dem Konfigurationsbefehl für die vPC-Domäne des **Layer-3-Peer-Routers** aktivieren. Auf diese Weise können Unicast-Routing-Protokollpakete mit einer TTL von 1 über den vPC-Peer-Link weitergeleitet werden, ohne dass die TTL des Pakets herabgesetzt werden muss. Dadurch können Unicast-Routing-Protokoll-Nachbarschaften problemlos über einen Back-to-Back-vPC gebildet werden. Infolgedessen werden N9K-1 und N9K-2 mit N9K-4 (dem DR für die Broadcast-Domäne) in den FULL-Status überführt und die von N9K-3 und N9K-4 bezogenen Präfixe über OSPF erfolgreich in die jeweiligen Unicast-Routing-Tabellen installiert.

# Zugehörige Informationen

- Konfigurationshandbuch für Cisco Nexus NX-OS-Schnittstellen der Serie 9000, Version 10.1(x)
- Konfigurationsleitfaden für Cisco Nexus NX-OS-Schnittstellen der Serie 9000, Version 9.3(x)
- Konfigurationsleitfaden für Cisco Nexus NX-OS-Schnittstellen der Serie 9000, Version 9.2(x)
- Konfigurationsleitfaden für Cisco Nexus NX-OS-Schnittstellen der Serie 9000, Version 7.x
- Konfigurationsleitfaden für Cisco Nexus 7000 NX-OS-Schnittstellen 8.x
- Konfigurationsleitfaden für Cisco Nexus 7000 NX-OS-Schnittstellen 7.x
- Design- und Konfigurationsleitfaden: Best Practices für Virtual Port Channels (vPC) auf Cisco Nexus Switches der Serie 7000
- Unterstützte Topologien für das Routing über virtuellen Port-Channel auf Nexus-Plattformen

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.