

# Nexus 9000 vPC mit Best Practices verstehen und konfigurieren

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[vPC - Beschreibung und Terminologie](#)

[Technische Vorteile von vPC](#)

[Betriebliche und architektonische Vorteile von vPC](#)

[Aspekte der vPC-Hardware- und -Software-Redundanz](#)

[Konfigurieren von vPC EVPN VXLAN](#)

[Netzwerkdiagramm](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Konfigurieren von vPC Fabric-Peering](#)

[Netzwerkdiagramm](#)

[Überprüfung](#)

[Konfigurieren von doppelseitigem vPC](#)

[Netzwerkdiagramm](#)

[Konfigurieren von doppelseitigem vPC mit vPC-Fabric-Peering](#)

[Netzwerkdiagramm](#)

[Fehlerbehebung](#)

[Best Practices für ISSU mit vPC](#)

[Strikte Empfehlungen](#)

[Best Practices beim Austausch von vPC-Switches](#)

[Vorprüfungen](#)

[Schritte](#)

[Prüfung nach der Validierung](#)

[Überlegungen zu vPC bei der VXLAN-Bereitstellung](#)

[Strikte Empfehlungen](#)

[Zugehörige Informationen](#)

## Einleitung

Dieses Dokument beschreibt die Best Practices für die Verwendung von vPC (Virtual Port Channels) auf Cisco Nexus Switches der Serie 9000 (9.000).

## Voraussetzungen

## Anforderungen

- NX-OS-Lizenzanforderung für vPC
- Die vPC-Funktion ist in der NX-OS-Basislizenz enthalten.

Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP) und Link Aggregation Control Protocol (LACP) sind ebenfalls in dieser Basislizenz enthalten.

Layer-3-Funktionen wie das OSPF-Protokoll (Open Shortest Path First) oder das ISIS-Protokoll (Intermediate-System-to-Intermediate System) erfordern eine LAN\_ENTERPRISE\_SERVICES\_PKG-Lizenz.

## Verwendete Komponenten

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

Cisco Nexus93180YC-FX mit Version 10.2(3)

Cisco Nexus93180YC-FX mit Version 10.2(3)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Terms	Meaning
vPC	The combined port-channel between the vPC peers and the downstream device. A vPC is a L2 port type: switchport mode trunk or switchport mode access.
vPC peer device	A vPC switch (one of a Cisco Nexus 9000 Series pair).
vPC Domain	Domain containing the 2 peer devices. Only 2 peer devices max can be part of the same vPC domain.
vPC Member port	One of a set of ports (that is. Port-channels) that form a vPC (or port-channel member of a vPC).
vPC Peer-link	Link used to synchronize the state between vPC peer devices. It must be a 10-Gigabit Ethernet Link. vPC peer-link is a L2 trunk carrying vPC VLAN.
vPC Peer-keepalive link	The keepalive link between vPC peer devices; this link is used to monitor the liveness of the peer device.
vPC VLAN	VLAN carried over the peer-link.

vPC Fabric Peering ist eine erweiterte Dual-Homing-Zugriffslösung ohne den Aufwand für vergeudete physische Ports für vPC Peer Link.

## Hintergrundinformationen

Dieses Dokument gilt für:

- Nexus 9000 vPC
- vPC mit VXLAN
- vPC-Fabric-Peering
- Doppelseitiger vPC
- Doppelseitiger virtueller vPC

In diesem Dokument werden auch In-Service-Software-Upgrades (ISSU) im Zusammenhang mit vPC und die neuesten vPC-Verbesserungen (Wiederherstellung mit Verzögerung, NVE-Schnittstellentimer) behandelt.

## **vPC - Beschreibung und Terminologie**

vPC ist eine Virtualisierungstechnologie, bei der die gepaarten Geräte der Cisco Nexus Serie 9000 als eindeutiger logischer Layer-2-Knoten für den Zugriff auf Layer-Geräte oder -Endpunkte dargestellt werden.

vPC gehört zur Multichassis EtherChannel (MCEC)-Technologiefamilie. Mit einem Virtual Port Channel (vPC) können Verbindungen, die physisch mit zwei verschiedenen Cisco Nexus-Geräten der Serie 9000 verbunden sind, für ein drittes Gerät als ein Port-Channel erscheinen.

Beim dritten Gerät kann es sich um einen Switch, einen Server oder ein anderes Netzwerkgerät handeln, das Link-Aggregation unterstützt.

## **Technische Vorteile von vPC**

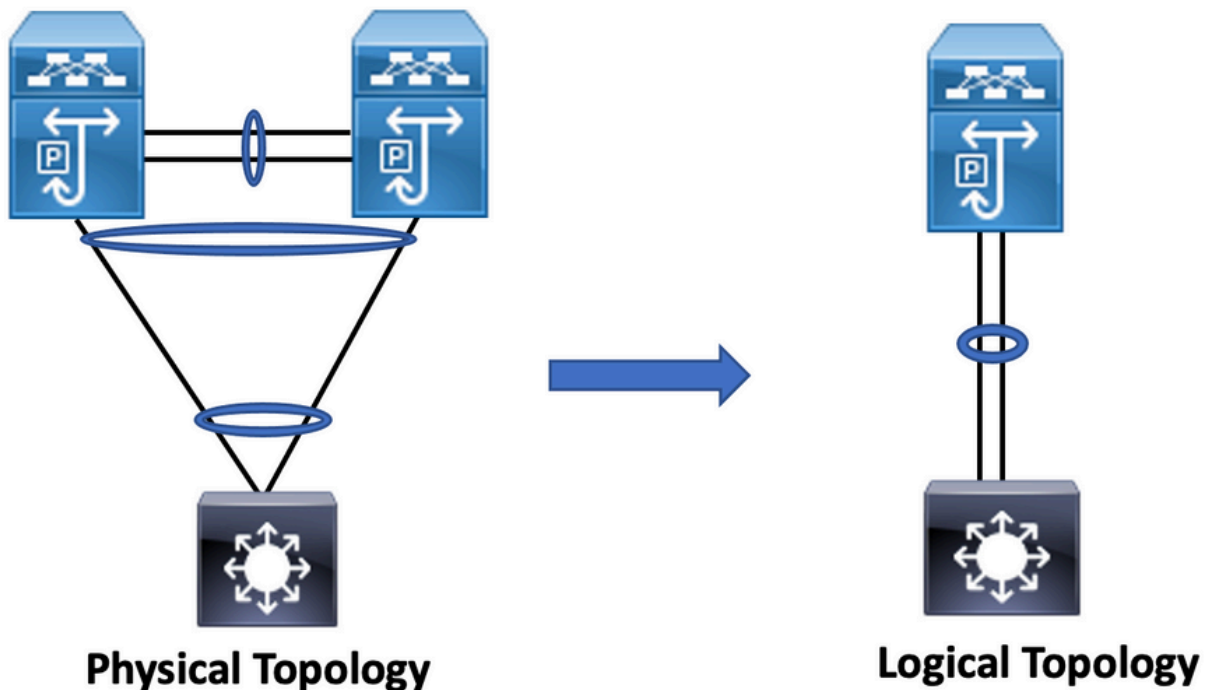
vPC bietet die folgenden technischen Vorteile:

- STP-blockierte Ports werden vermieden
- Verwendet die gesamte verfügbare Uplink-Bandbreite
- Ermöglicht Dual-Homed-Servern den Betrieb im Aktiv-Aktiv-Modus
- Schnelle Konvergenz bei Verbindungs- oder Geräteausfällen
- Duale Active/Active-Standard-Gateways für Server vPC nutzt auch natives Split-Horizon/Loop-Management durch Port-Channeling-Technologie: Ein Paket kommt, ein Port-Channel kann denselben Port-Channel nicht sofort verlassen.

## **Betriebliche und architektonische Vorteile von vPC**

vPC bietet Benutzern sofort die folgenden betrieblichen und architekturbezogenen Vorteile:

- Vereinfachtes Netzwerkdesign
- Aufbau eines ausfallsicheren und robusten Layer-2-Netzwerks
- Nahtlose Mobilität virtueller Systeme und Server-Hochverfügbarkeits-Cluster
- Skalierung der verfügbaren Layer-2-Bandbreite, Erhöhung der bisektionalen Bandbreite
- Vergrößerung des Layer-2-Netzwerks



## Aspekte der vPC-Hardware- und -Software-Redundanz

vPC nutzt Aspekte der Hardware- und Softwareredundanz mithilfe der folgenden Methoden:

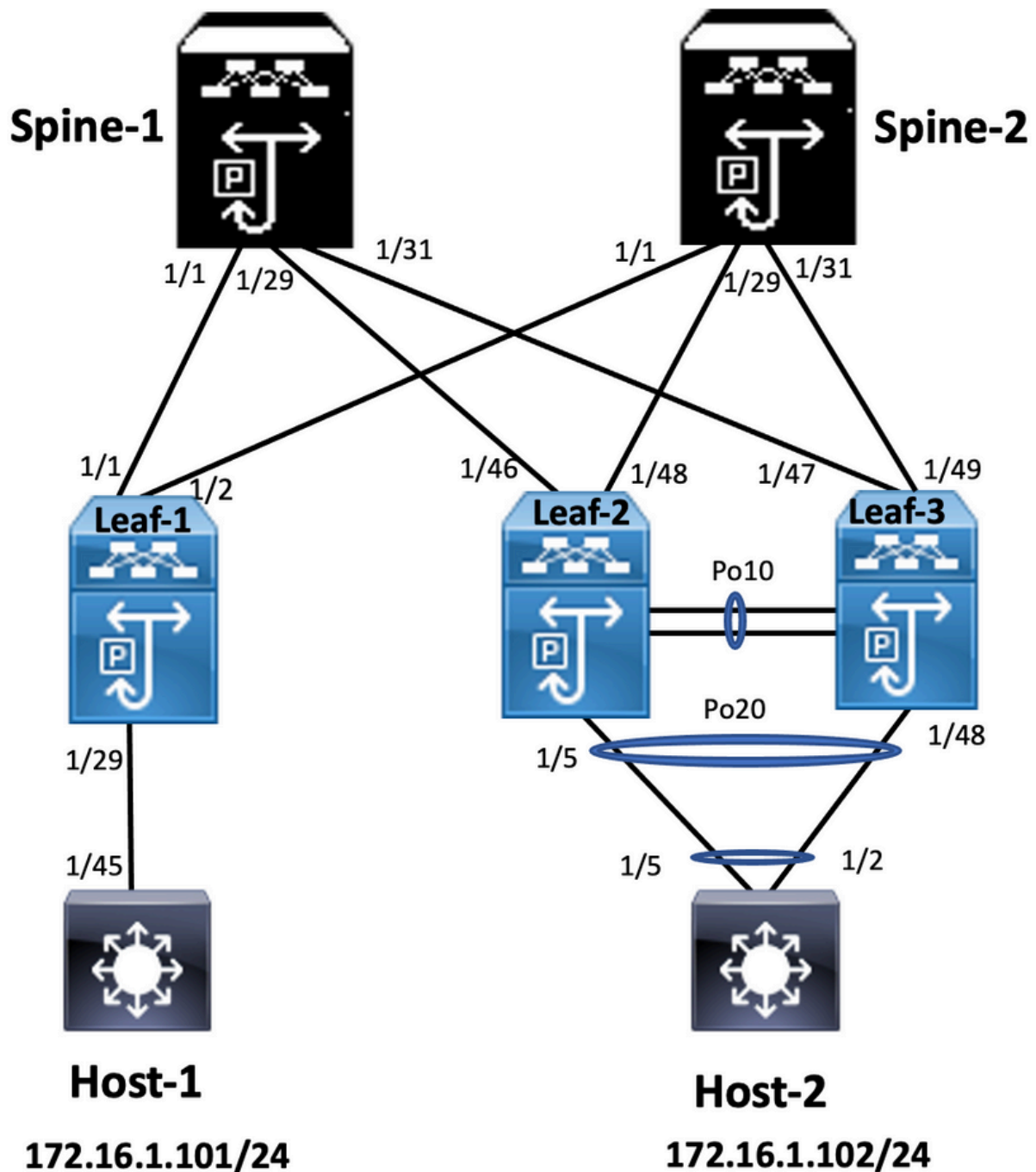
- vPC nutzt alle verfügbaren Port-Channel-Member-Links, sodass im Falle eines Ausfalls einer einzelnen Verbindung der Hash-Algorithmus alle Flows zu den verfügbaren Links umleitet.
- Die vPC-Domäne besteht aus zwei Peer-Geräten. Jedes Peer-Gerät verarbeitet die Hälfte des Datenverkehrs über den Access-Layer. Beim Ausfall eines Peer-Geräts nimmt das andere Peer-Gerät den gesamten Datenverkehr mit minimalen Auswirkungen auf die Konvergenzzeit auf.
- Jedes Peer-Gerät in der vPC-Domäne führt seine eigene Kontrollebene aus, und beide Geräte arbeiten unabhängig voneinander. Potenzielle Probleme auf der Kontrollebene bleiben lokal auf dem Peer-Gerät und wirken sich nicht auf das andere Peer-Gerät aus.

Von STP aus eliminiert vPC die durch STP blockierten Ports und nutzt die gesamte verfügbare Uplink-Bandbreite. STP wird als Ausfallsicherheitsmechanismus verwendet und gibt keinen L2-Pfad für über vPC angeschlossene Geräte vor.

Innerhalb einer vPC-Domäne kann ein Benutzer Zugriffsgeräte auf mehrere Arten verbinden: über vPC verbundene Verbindungen, die ein Aktiv/Aktiv-Verhalten mit Port-Channel nutzen, Aktiv/Standby-Verbindungen umfassen STP und eine einzige Verbindung ohne STP, die auf dem Zugriffsgerät ausgeführt wird.

## Konfigurieren von vPC EVPN VXLAN

### Netzwerkdiagramm



Im Diagramm enthält der Host für die Verbindung mit einem Paar Nexus 9000-Switches die vPC-Domänen-ID, aber auf den als Host konfigurierten Switches wird vPC selbst nicht ausgeführt. Der Access Switch/Host registriert den Uplink als einfachen Port-Channel, ohne dass vPC davon weiß.

```

Leaf-1
vlan 2
vn-segment 10002
vlan 10
vn-segment 10010
route-map PERMIT-ALL permit 10
vrf context test
vni 10002
rd auto
address-family ipv4 unicast
route-target both auto

```

```
route-target both auto evpn
```

```
interface nve1
```

```
no shutdown
```

```
host-reachability protocol bgp
```

```
source-interface loopback1
```

```
member vni 10002 associate-vrf
```

```
member vni 10010
```

```
suppress-arp
```

```
mcast-group 239.1.1.1
```

```
interface loopback0
```

```
ip address 10.1.1.1/32
```

```
ip router ospf 100 area 0.0.0.0
```

```
ip pim sparse-mode
```

```
no shutdown
```

```
interface loopback1
```

```
ip address 10.2.1.1/32
```

```
ip router ospf 100 area 0.0.0.0
```

```
ip pim sparse-mode
```

```
no shutdown
```

## Leaf-2

```
vlan 2
```

```
vn-segment 10002
```

```
vlan 10
```

```
vn-segment 10010
```

```
route-map PERMIT-ALL permit 10
```

```
vrf context test
```

```
vni 10002
```

```
rd auto
```

```
address-family ipv4 unicast
```

```
route-target both auto
```

```
route-target both auto evpn
```

```
interface nve1
```

```
no shutdown
```

```
host-reachability protocol bgp
```

```
advertise virtual-rmac
```

```
source-interface loopback1
```

```
member vni 10002
```

```
associate-vrf member
```

```
vni 10010
```

```
suppress-arp
```

```
mcast-group 239.1.1.1
```

```
interface loopback1
```

```
ip address 10.2.1.4/32
```

```
ip address 10.2.1.10/32 secondary
```

```
ip router ospf 100 area 0.0.0.0
```

```
ip pim sparse-mode
```

```
icam monitor scale
```

```
interface loopback0
```

```
ip address 10.1.1.4/32
```

```
ip router ospf 100 area 0.0.0.0
```

```
ip pim sparse-mode
```

```
no shutdown
```

```
Leaf-2(config-if)# show run vpc
```

```
feature vpc
```

```
vpc domain 1
peer-switch
peer-keepalive destination 10.201.182.26 source 10.201.182.25
peer-gateway
ip arp synchronize
```

```
interface port-channel10
vpc peer-link
```

```
interface port-channel20
vpc 20
```

### **Leaf-3**

```
vlan 2
vn-segment 10002
vlan 10
vn-segment 10010
route-map PERMIT-ALL permit 10
vrf context test
vni 10002
rd auto
address-family ipv4 unicast
route-target both auto
route-target both auto evpn
```

```
interface nve1
no shutdown
```

```
host-reachability protocol bgp
advertise virtual-rmac
source-interface loopback1
member vni 10002
associate-vrf member
vni 10010
suppress-arp
mcast-group 239.1.1.1
```

```
interface loopback1
ip address 10.2.1.3/32
ip address 10.2.1.10/32 secondary
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode
icam monitor scale
```

```
interface loopback0
ip address 10.1.1.3/32
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode
```

```
Leaf-3(config-if)# show run vpc
feature vpc
```

```
vpc domain 1
peer-switch
peer-keepalive destination 10.201.182.25 source 10.201.182.26
peer-gateway
ip arp synchronize
```

```
interface port-channel10
vpc peer-link
```

```
interface port-channel20
vpc 20
```

### Spine-1

```
interface loopback0
ip address 10.3.1.1/32
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode
```

### Host-1

```
interface Vlan10
no shutdown
vrf member test

ip address 172.16.1.101/25
```

### Host-2

```
interface Vlan10
no shutdown
vrf member test

ip address 172.16.1.102/25
```

## Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

```
ip interface Status for VRF "test" (3)
Schnittstellenstatus IP-Adresse
Vlan10 172.16.1.102 Protokoll-Up/Link-Up/Admin-Up
HOST-B(config)# ping 172.16.1.101 VRF-Test
PING 172.16.1.101 (172.16.1.101): 56 Datenbytes
64 Bytes vom 172.16.1.101: icmp_seq=0 ttl=254
time=1,326 ms
64 Bytes vom 172.16.1.101: icmp_seq=1 ttl=254
time=0,54 ms
64 Bytes vom 172.16.1.101: icmp_seq=2 ttl=254
time=0,502 ms
64 Bytes vom 172.16.1.101: icmp_seq=3 ttl=254
time=0,533 ms
64 Bytes vom 172.16.1.101: icmp_seq=4 ttl=254
time=0,47 ms
— 172.16.1.101 Ping-Statistik —
5 übertragene Pakete, 5 empfangene Pakete, Round-
Trip mit 0,00 % Paketverlust (min/avg/max) =
0,47/0,674/1,326 ms HOST-B(config)#
```

```
IP-Schnittstellenstatus für VRF-"Test"(3)
interface IP address Schnittstellenstatus
Vlan10 172.16.1.101 Protokoll-Up/Link-Up/Admin-Up
Host-A(config-if)#
Host-A(config-if)# ping 172.16.1.102 vrf test
PING 172.16.1.102 (172.16.1.102): 56 Datenbyte
64 Bytes vom 172.16.1.102: icmp_seq=0 ttl=254
time=1,069 ms
64 Bytes vom 172.16.1.102: icmp_seq=1 ttl=254
time=0,648 ms
64 Bytes vom 172.16.1.102: icmp_seq=2 ttl=254
time=0,588 ms
64 Bytes vom 172.16.1.102: icmp_seq=3 ttl=254
time=0,521 ms
64 Bytes vom 172.16.1.102: icmp_seq=4 ttl=254
time=0,495 ms
— 172.16.1.102 Ping-Statistiken —
5 übertragene Pakete, 5 empfangene Pakete, Ro
Trip mit 0,00 % Paketverlust (min/avg/max) =
0,495/0,664/1,069 ms Host-A(config-if)#
```

## Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

```
Leaf-2(config-if)# show vpc bri
Legende:
(*) - lokaler vPC ist ausgefallen, Weiterleitung über
```

```
Leaf-3(config-if)# show vpc bri
Legende:
(*) - lokaler vPC ist ausgefallen, Weiterleitung über
```



```

vPC Peer-Link
vPC-Domänen-ID: 1
Peer-Status: Die Peer-Adjacency ist in Ordnung.
vPC-Keep-Alive-Status: Peer ist aktiv
Konfigurationskonsistenzstatus: erfolgreich
Per-VLAN Consistency Status: Success
Typ-2-Konsistenzstatus: Erfolg
vPC-Rolle: primary
Anzahl der konfigurierten vPCs: 1
Peer-Gateway: Aktiviert
Dual-Active ohne VLANs: -
Sichere Konsistenzprüfung: Aktiviert
Status der automatischen Wiederherstellung:
Deaktiviert
Status der Verzögerung-Wiederherstellung: Der Timer
ist ausgeschaltet.(Timeout = 30 s)
Delay-restore SVI-Status: Der Timer ist
ausgeschaltet.(Timeout = 10 s)
Verzögerung-Wiederherstellung des Status des
verwaisten Ports: Der Timer ist ausgeschaltet.(Timeout
= 0 s)
Betriebs-Layer-3-Peer-Router: Deaktiviert
Virtual-Peer-Link-Modus: Deaktiviert
Status der vPC-Peer-Verbindung
—
ID-Port-Status Aktive VLANs
-----
1 Po10 aktiv 1-2,10
vPC-Status
-----
---
ID-Port-Status Konsistenzgrund für aktive VLANs
-----
20 Po20 Up-Erfolge 1-2,10
Bitte überprüfen Sie "show vpc consistency-
parameters vpc <vpc-num>" auf den Konsistenzgrund
für Down-vpc und auf Typ-2-Konsistenzgründe für
beliebige vPCs.

```

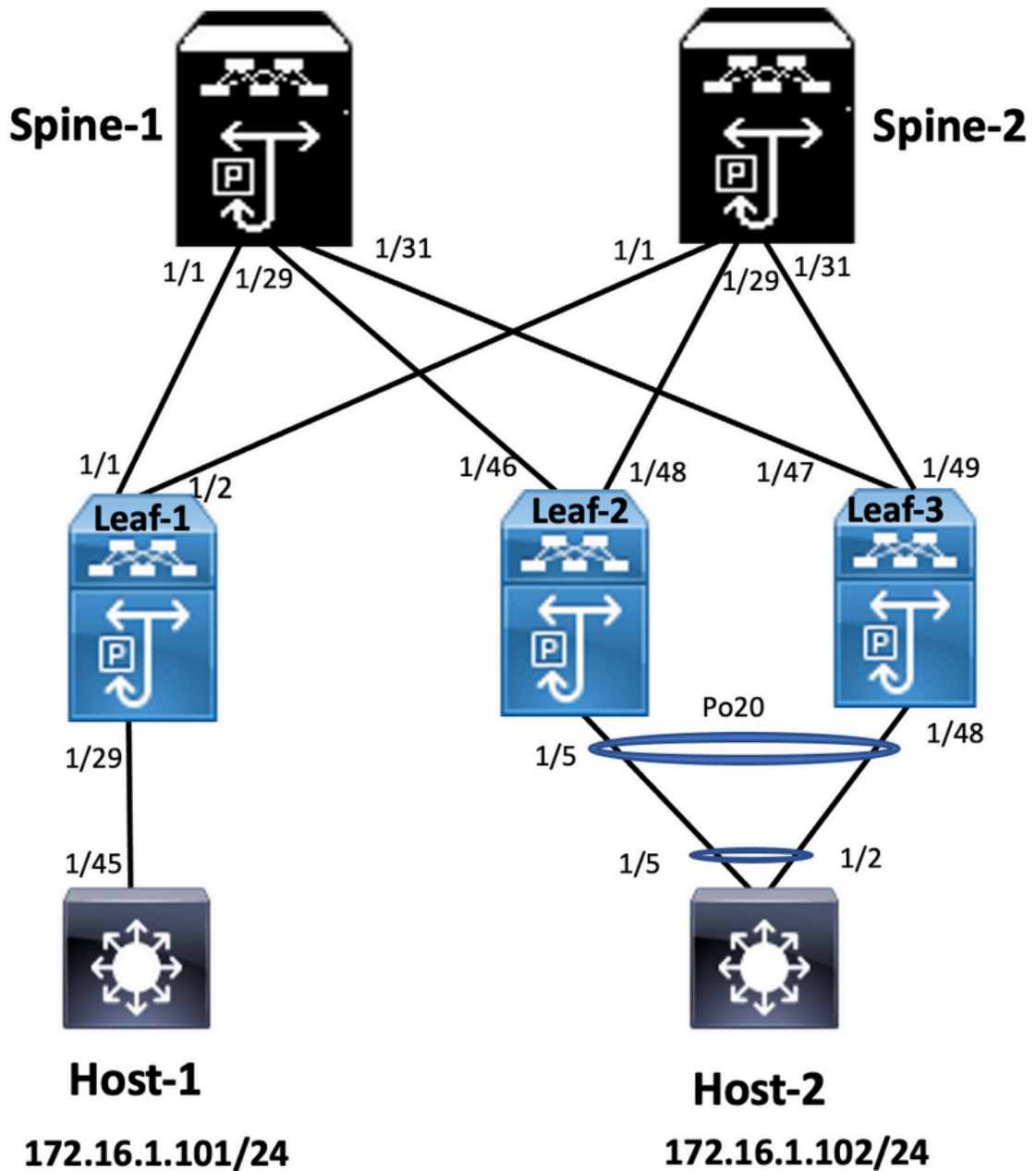
```

vPC Peer-Link
vPC-Domänen-ID: 1
Peer-Status: Die Peer-Adjacency ist in Ordnung.
vPC-Keep-Alive-Status: Peer ist aktiv
Konfigurationskonsistenzstatus: erfolgreich
Per-VLAN Consistency Status: Success
Typ-2-Konsistenzstatus: Erfolg
vPC-Rolle: sekundär
Anzahl der konfigurierten vPCs: 1
Peer-Gateway: Aktiviert
Dual-Active ohne VLANs: -
Sichere Konsistenzprüfung: Aktiviert
Status der automatischen Wiederherstellung:
Deaktiviert
Status der Verzögerung-Wiederherstellung: Der T
ist ausgeschaltet.(Timeout = 30 s)
Delay-restore SVI-Status: Der Timer ist
ausgeschaltet.(Timeout = 10 s)
Verzögerung-Wiederherstellung des Status des
verwaisten Ports: Der Timer ist ausgeschaltet.(Ti
= 0 s)
Betriebs-Layer-3-Peer-Router: Deaktiviert
Virtual-Peer-Link-Modus: Deaktiviert
Status der vPC-Peer-Verbindung
—
ID-Port-Status Aktive VLANs
-----
1 Po10 aktiv 1-2,10
vPC-Status
-----
---
ID-Port-Status Konsistenzgrund für aktive VLANs
-----
20 Po20 Up-Erfolge 1-2,10
Bitte überprüfen Sie "show vpc consistency-
parameters vpc <vpc-num>" auf den Konsistenzg
für Down-vpc und auf Typ-2-Konsistenzgründe fü
beliebige vPCs.

```

## Konfigurieren von vPC Fabric-Peering

### Netzwerkdiagramm



#### Leaf-2

```
Leaf-2(config-vpc-domain)# show run vpc
feature vpc
```

```
vpc domain 1
peer-switch
peer-keepalive destination 10.201.182.26
virtual peer-link destination 10.1.1.3 source 10.1.1.4 dscp 56
peer-gateway
ip arp synchronize
```

```
interface port-channel10
vpc peer-link
```

```
interface Ethernet1/46
mtu 9216
port-type fabric
ip address 192.168.2.1/24
ip ospf network point-to-point
ip router ospf 100 area 0.0.0.0
ip pim sparse-mode
```

```
no shutdown
```

### **Leaf-3**

```
Leaf-3(config-vpc-domain)# show run vpc  
feature vpc
```

```
vpc domain 1  
peer-switch  
peer-keepalive destination 10.201.182.25  
virtual peer-link destination 10.1.1.4 source 10.1.1.3 dscp 56
```

```
peer-gateway  
ip arp synchronize
```

```
interface port-channel10  
vpc peer-link
```

```
interface Ethernet1/47  
mtu 9216  
port-type fabric  
ip address 192.168.1.1/24  
ip ospf network point-to-point  
ip router ospf 100 area 0.0.0.0  
ip pim sparse-mode  
no shutdown
```

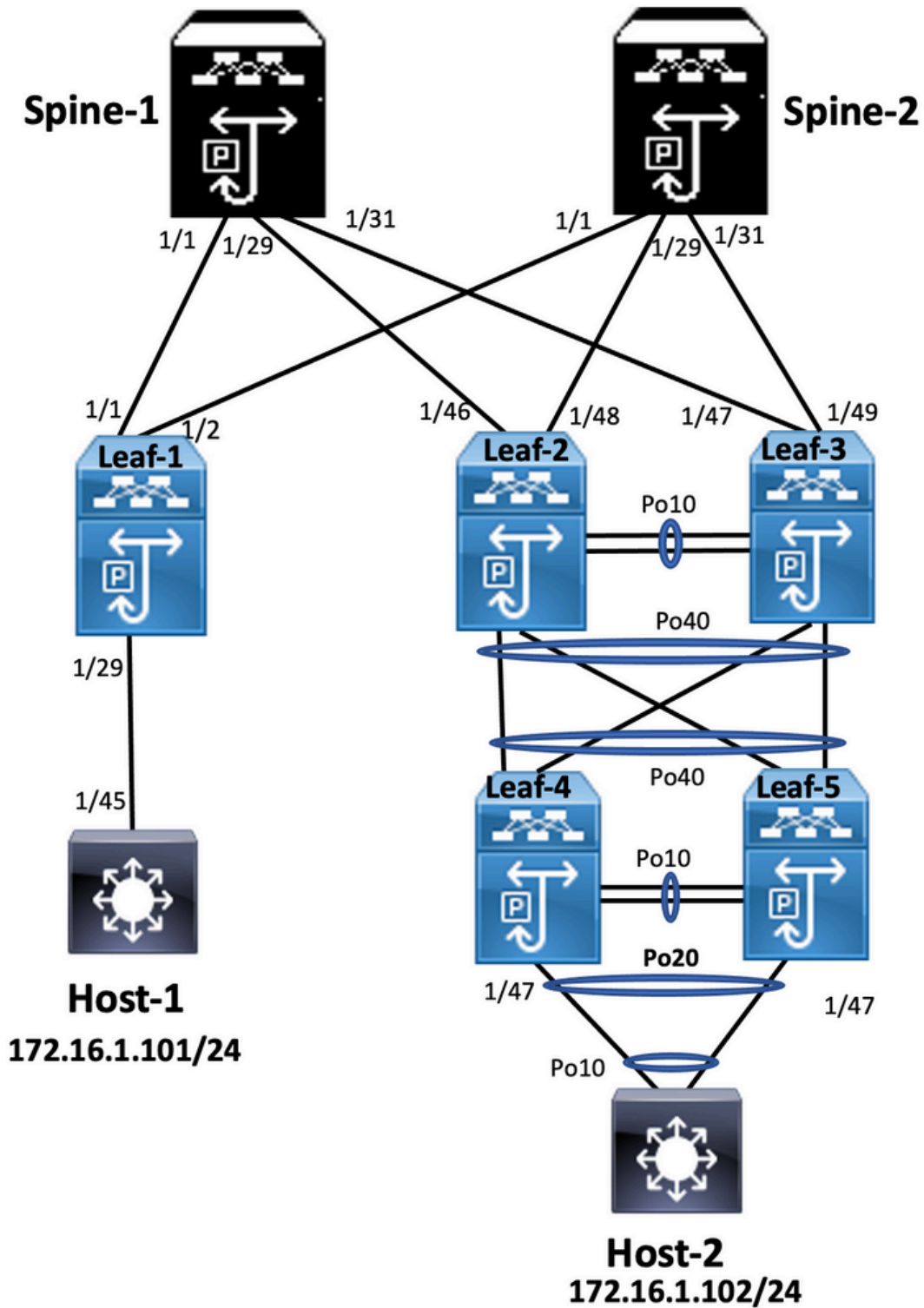
## **Überprüfung**

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

```
show vpc brief  
show vpc role  
show vpc virtual-peerlink vlan consistency  
show vpc fabric-ports  
show vpc consistency-para global  
show nve interface nve 1 detail
```

## **Konfigurieren von doppelseitigem vPC**

### **Netzwerkdiagramm**



#### Leaf-2

```
Leaf-2(config-if-range)# show run vpc
feature vpc
```

```
vpc domain 1
peer-switch
peer-keepalive destination 10.201.182.26 source 10.201.182.25
peer-gateway
ip arp synchronize
```

```
interface port-channel10
vpc peer-link
```

```
interface port-channel20
```

```
vpc 20
```

```
interface port-channel40  
vpc 40
```

### **Leaf-3**

```
Leaf-3(config-if-range)# show run vpc  
feature vpc
```

```
vpc domain 1  
peer-switch  
peer-keepalive destination 10.201.182.25 source 10.201.182.26  
peer-gateway  
ip arp synchronize
```

```
interface port-channel10  
vpc peer-link
```

```
interface port-channel20  
vpc 20
```

```
interface port-channel40  
vpc 40
```

### **Leaf-4**

```
Leaf-4(config-if)# show run vpc  
feature vpc
```

```
vpc domain 2  
peer-switch  
peer-keepalive destination 10.201.182.29 source 10.201.182.28  
peer-gateway
```

```
interface port-channel10  
vpc peer-link
```

```
interface port-channel20  
vpc 20
```

```
interface port-channel40  
vpc 40
```

### **Leaf-5**

```
Leaf-5(config-if)# show running-config vpc  
feature vpc
```

```
vpc domain 2  
peer-switch  
peer-keepalive destination 10.201.182.28 source 10.201.182.29  
peer-gateway
```

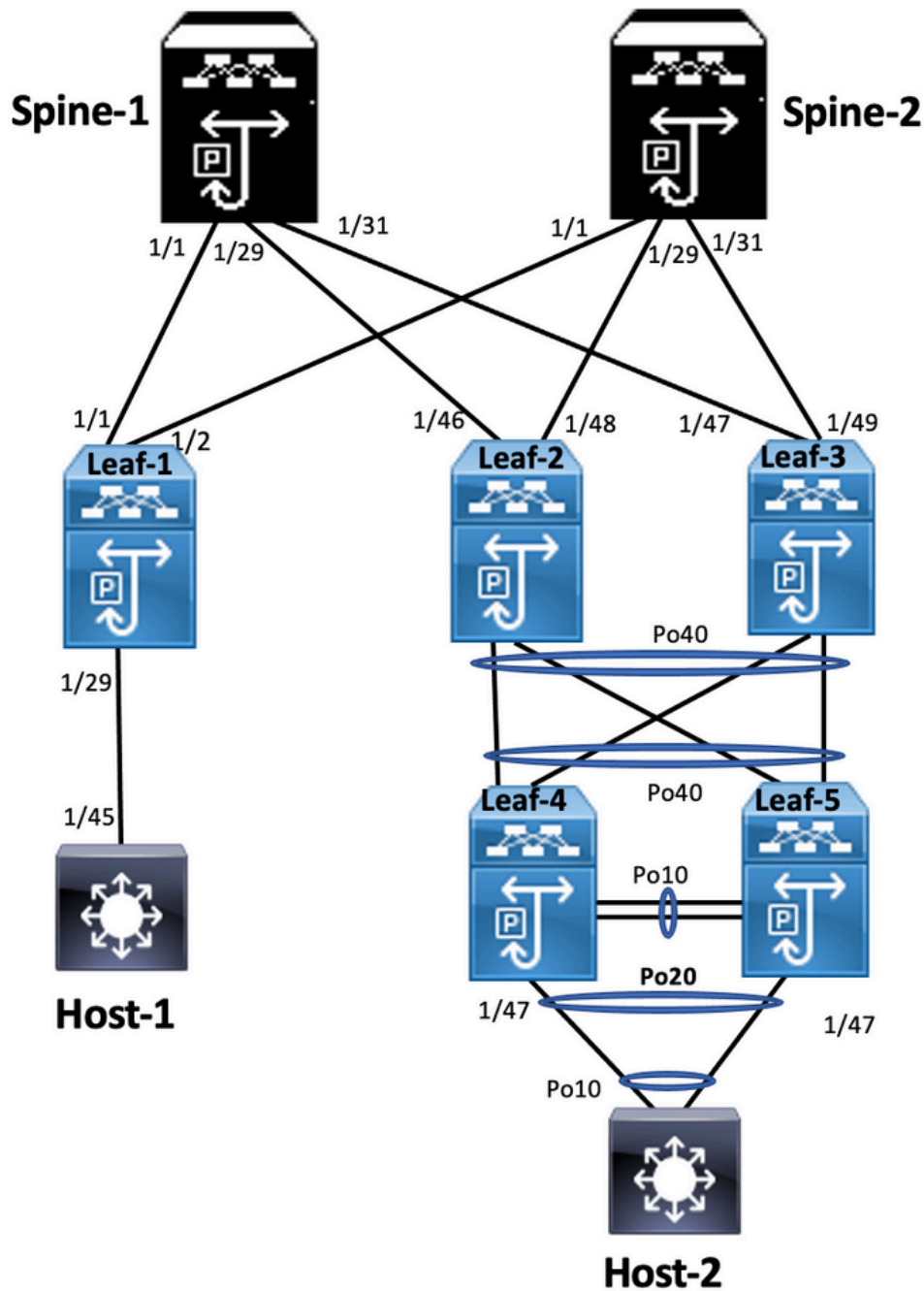
```
interface port-channel10  
vpc peer-link
```

```
interface port-channel20  
vpc 20
```

```
interface port-channel40  
vpc 40
```

## **Konfigurieren von doppelseitigem vPC mit vPC-Fabric-Peering**

# Netzwerkdiagramm



In doppelseitigem vPC wird vPC auf beiden Nexus 9000-Switches ausgeführt. Jedes vPC-Paar der Nexus 9000-Switches ist über einen eindeutigen vPC mit dem Aggregations-vPC-Paar verbunden.

## Leaf-2

```
Leaf-2(config-if-range)# show run vpc  
feature vpc
```

```
vpc domain 1  
peer-switch  
peer-keepalive destination 10.201.182.26  
virtual peer-link destination 10.1.1.3 source 10.1.1.4 dscp 56  
peer-gateway  
ip arp synchronize
```

```
interface port-channel10
```

```
vpc peer-link

interface port-channel20
vpc 20

interface port-channel40
vpc 40
```

### Leaf-3

```
Leaf-3(config-if-range)# show run vpc
feature vpc

vpc domain 1
peer-switch
peer-keepalive destination 10.201.182.25
virtual peer-link destination 10.1.1.4 source 10.1.1.3 dscp 56
peer-gateway
ip arp synchronize

interface port-channel10
vpc peer-link

interface port-channel20
vpc 20

interface port-channel40
vpc 40
```

Leaf-4 and Leaf-5 configuration is similar as double-sided vPC.

## Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

<pre>Leaf-4(config-if)# show spanning-tree VLAN0010 Spanning-Tree-aktiviertes Protokoll rstp Root-ID Priorität 32778     Adresse: 0023.04ee.be01     Kosten 5     Port 4105 (Port-Channel10)     Hello-Zeit 2 Sek. Max. Alter 20 Sek. Vorwärtsverzögerung 15 Sek. Bridge ID Priority 32778 (Priorität 32768 sys-id-ext 10)     Adresse: 0023.04ee.be02     Hello-Zeit 2 Sek. Max. Alter 20 Sek. Vorwärtsverzögerung 15 Sek. Schnittstellenrolle STS-Kosten Prio.NBR-Typ ----- - Po10 Root FWD 4 128.4105 (vPC Peer-Link) Netzwerk P2p Po20 Desg FWD 1 128.4115 (vPC) P2p Po40 Root FWD 1 128.4135 (vPC) P2p VLAN0020</pre>	<pre>Leaf-5(config-if)# show spanning-tree VLAN0010 Spanning-Tree-aktiviertes Protokoll rstp Root-ID Priorität 32778     Adresse: 0023.04ee.be01     Kosten 1     Port 4135 (Port-Channel40)     Hello-Zeit 2 Sek. Max. Alter 20 Sek. Vorwärtsverzögerung 15 Sek. Bridge ID Priority 32778 (Priorität 32768 sys-id-e     Adresse: 0023.04ee.be02     Hello-Zeit 2 Sek. Max. Alter 20 Sek. Vorwärtsverzögerung 15 Sek. Schnittstellenrolle STS-Kosten Prio.NBR-Typ ----- - Po10 Desg FWD 4 128.4105 (vPC Peer-Link) Netzwerk P2p Po20 Desg FWD 1 128.4115 (vPC) P2p Po40 Root FWD 1 128.4135 (vPC) P2p VLAN0020</pre>
--	--

Spanning-Tree-aktiviertes Protokoll rstp  
Root-ID Priorität 32788  
    Adresse: 0023.04ee.be02  
    Diese Bridge ist der Root  
    Hello-Zeit 2 Sek. Max. Alter 20 Sek.  
Vorwärtsverzögerung 15 Sek.  
Bridge ID Priority 32788 (Priorität 32768 sys-id-ext 20)  
    Adresse: 0023.04ee.be02  
    Hello-Zeit 2 Sek. Max. Alter 20 Sek.  
Vorwärtsverzögerung 15 Sek.  
Schnittstellenrolle STS-Kosten Prio.NBR-Typ

---

Spanning-Tree-aktiviertes Protokoll rstp  
Root-ID Priorität 32788  
    Adresse: 0023.04ee.be02  
    Diese Bridge ist der Root  
    Hello-Zeit 2 Sek. Max. Alter 20 Sek.  
Vorwärtsverzögerung 15 Sek.  
Bridge ID Priority 32788 (Priorität 32768 sys-id-e  
    Adresse: 0023.04ee.be02  
    Hello-Zeit 2 Sek. Max. Alter 20 Sek.  
Vorwärtsverzögerung 15 Sek.  
Schnittstellenrolle STS-Kosten Prio.NBR-Typ

---

-  
Po10 Root FWD 4 128.4105 (vPC Peer-Link) Netzwerk  
P2p  
Po20 Desg FWD 1 128.4115 (vPC) P2p  
Po40 Desg FWD 1 128.4135 (vPC) P2p

-  
Po10 Desg FWD 4 128.4105 (vPC Peer-Link)  
Netzwerk P2p  
Po20 Desg FWD 1 128.4115 (vPC) P2p  
Po40 Desg FWD 1 128.4135 (vPC) P2p  
Leaf-5(config-if)#

Leaf-2(config-if-range)# show spanning-tree  
VLAN0001

Spanning-Tree-aktiviertes Protokoll rstp  
Root-ID Priorität 32769  
    Adresse: 0023.04ee.be01  
    Kosten 0  
    Port 0 ()  
    Hello-Zeit 2 Sek. Max. Alter 20 Sek.  
Vorwärtsverzögerung 15 Sek.  
Bridge ID Priority 32769 (Priorität 32768 sys-id-ext 1)  
    Adresse 003a.9c28.2cc7  
    Hello-Zeit 2 Sek. Max. Alter 20 Sek.  
Vorwärtsverzögerung 15 Sek.  
Schnittstellenrolle STS-Kosten Prio.NBR-Typ

---

Leaf-3(config-if-range)# show spanning-tree  
VLAN0010

Spanning-Tree-aktiviertes Protokoll rstp  
Root-ID Priorität 32778  
    Adresse: 0023.04ee.be01  
    Diese Bridge ist der Root  
    Hello-Zeit 2 Sek. Max. Alter 20 Sek.  
Vorwärtsverzögerung 15 Sek.  
Bridge ID Priority 32778 (Priorität 32768 sys-id-e  
    Adresse: 0023.04ee.be01  
    Hello-Zeit 2 Sek. Max. Alter 20 Sek.  
Vorwärtsverzögerung 15 Sek.  
Schnittstellenrolle STS-Kosten Prio.NBR-Typ

---

-  
Eth1/47 Desg FWD 4 128.185 P2p  
VLAN0010  
Spanning-Tree-aktiviertes Protokoll rstp  
Root-ID Priorität 32778  
    Adresse: 0023.04ee.be01  
    Diese Bridge ist der Root  
    Hello-Zeit 2 Sek. Max. Alter 20 Sek.  
Vorwärtsverzögerung 15 Sek.  
Bridge ID Priority 32778 (Priorität 32768 sys-id-ext 10)  
    Adresse: 0023.04ee.be01  
    Hello-Zeit 2 Sek. Max. Alter 20 Sek.  
Vorwärtsverzögerung 15 Sek.  
Schnittstellenrolle STS-Kosten Prio.NBR-Typ

---

-  
Po10 Root FWD 4 128.4105 (vPC Peer-Link) Net  
P2p  
Po40 Desg FWD 1 128.4135 (vPC) P2p  
Leaf-3(config-if-range)#

-  
Po10 Desg FWD 4 128.4105 (vPC Peer-Link)  
Netzwerk P2p  
Po40 Desg FWD 1 128.4135 (vPC) P2p  
Eth1/47 Desg FWD 4 128.185 P2p



Leaf-2(config-if-range)#

## Best Practices für ISSU mit vPC

In diesem Abschnitt werden die Best Practices für unterbrechungsfreie Software-Upgrades beschrieben, bei denen Cisco ISSU verwendet wird, wenn eine vPC-Domäne konfiguriert ist. Die vPC-Funktion für Upgrade (oder Downgrade) des vPC-Systems NX-OS ist vollständig mit Cisco ISSU kompatibel.

In einer vPC-Umgebung stellt ISSU die empfohlene Methode für das Upgrade des Systems dar. Ein unabhängiges Upgrade des vPC-Systems ist ohne Unterbrechung des Datenverkehrs möglich. Das Upgrade ist serialisiert und muss nacheinander ausgeführt werden. Die Konfigurationssperre während des ISSU verhindert synchrone Upgrades auf beiden vPC-Peers (die Konfiguration wird automatisch auf anderen vPC-Peers gesperrt, wenn der ISSU initiiert wird). Zur Durchführung des ISSU-Vorgangs ist ein einziger Knopf erforderlich.

**Hinweis:** vPC mit FEX (Host-vPC) unterstützt ISSU ebenfalls vollständig. Es entsteht kein Paketverlust, wenn ein Upgrade der vPC-Domäne über FEX erfolgt. Server, der über einen standardmäßigen Port-Channel doppelt an zwei verschiedene FEX angeschlossen ist, erkennt den Upgrade-Vorgang im Netzwerk nicht.

```
switch#install all nxos bootflash:
```

### Strikte Empfehlungen

vPC-Peer-Gerät 1, 9001 (lädt den Code zuerst auf primäres oder sekundäres vPC-Peer-Gerät hat keine Bedeutung) verwendet ISSU. Beachten Sie, dass die Konfiguration eines anderen vPC-Peer-Geräts (9K2) gesperrt ist, um einen Betrieb des Switches zu verhindern.

- Verwenden Sie ISSU (In-Service Software Upgrade), um die NX-OS-Codeversion für die vPC-Domäne zu ändern. Führen Sie den Vorgang nacheinander für jeweils ein vPC-Peer-Gerät aus.
- In den NX-OS-Versionshinweisen wird die richtige NX-OS-Zielcodeversion auf Basis des Gerätecodes ausgewählt (ISSU-Kompatibilitätsmatrix). **Hinweis:** Beim Upgrade von 9k1 von 7.x auf 9.3.8/9.3.9 ist der 40G-Port auf vPC ausgefallen. Wenn für den Peer-Link, der mit 40G verbunden ist, ein Upgrade beider Switches auf 9.3.8/9.3.9 empfohlen wird, um 40G zu aktivieren, oder für den Pfad: I7(7) - 9.3(1) - 9.3(9).

## Best Practices beim Austausch von vPC-Switches

```
show version
show module
show spanning-tree summary
show vlan summary
show ip interface brief
show port-channel summary
show vpc
show vpc brief
show vpc role
show vpc peer-keepalives
show vpc statistics peer-keepalive
```

```

show vpc consistency-parameters global
show vpc consistency-parameters interface port-channel<>
show vpc consistency-parameters vlans
show run vpc all
show hsrp brief
show hsrp
show run hsrp
show hsrp interface vlan
Show vrrp
Show vrrp brief
Show vrrp interface vlan
Show run vrrp

```

**Schritte**Fahren Sie alle vPC-Member-Ports einzeln herunter.Alle verwaisten Ports herunterfahren.Fahren Sie alle physischen Layer-3-Verbindungen einzeln herunter.Fahren Sie den vPC Peer Keep Alive (PKA)-Link herunter.Fahren Sie den vPC-Peer-Link herunter.Stellen Sie sicher, dass alle Ports an dem problematischen Switch ausgefallen sind.Stellen Sie sicher, dass der Datenverkehr über gemeinsam genutzte Befehle auf dem redundanten Switch an den redundanten Switch umgeleitet wird.

```

show vpc
show vpc statistics
show ip route vrf all summary
show ip mroute vrf all summary
show ip interface brief
show interface status
show port-channel summary
show hsrp brief
Show vrrp brief

```

Stellen Sie sicher, dass auf dem Ersatzgerät das richtige Image und die richtige Lizenz installiert sind.

```

show version
show module
show diagnostic results module all detail
show license
show license usage
show system internal mts buffer summary/detail
show logging logfile
show logging nvram

```

Konfigurieren Sie den Switch mit der richtigen Backup-Konfiguration.Wenn die automatische Wiederherstellung aktiviert ist, deaktivieren Sie sie während des Ersetzens.

```

Leaf-2(config)# vpc domain 1
Leaf-2(config-vpc-domain)# no auto-recovery
Leaf-2(config-if)# show vpc bri
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id : 1
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role : primary
Number of vPCs configured : 1
Peer Gateway : Enabled
Dual-active excluded VLANs : - Graceful Consistency Check : Enabled

```

```
Auto-recovery status : Disabled
Delay-restore status : Timer is off. (timeout = 30s)
Delay-restore SVI status : Timer is off (timeout = 10s)
Delay-restore Orphan-port status : Timer is off.(timeout = 0s)
Operational Layer3 Peer-router : Disabled
Virtual-peerlink mode : Disabled
```

Stellen Sie sicher, dass das Sticky-Bit auf False festgelegt ist.

```
Leaf-5(config-vpc-domain)# show sys internal vpcm info all | i i stick
OOB Peer Version: 2 OOB peer was alive: TRUE Sticky Master: FALSE
```

Wenn das Sticky-Bit auf True festgelegt ist, konfigurieren Sie die vPC-Rollenpriorität neu. Dies bedeutet, dass die ursprüngliche Konfiguration für die Rollenpriorität erneut angewendet wird.

vPC-Domäne 1 <== 1 ist die auf dem ursprünglichen Switch angegebene vPC-

DomänennummerRollenpriorität 2000 <== Beispiel: wenn 2000 die vPC-Rollenpriorität auf

dem ursprünglichen Switch istRufen Sie die Schnittstellen in dieser Reihenfolge auf: Aufrufen

des Peer-Keep-Alive-LinksAufrufen der vPC Peer-VerbindungBestätigen Sie, dass die vPC-

Rolle korrekt eingerichtet wurde.Rufen Sie die restlichen Schnittstellen auf den Switches

einzel in der folgenden Reihenfolge auf: vPC-Teilnehmer-PortsVerwaiste Ports (Nicht-vPC-

Ports)Physische Layer-3-Schnittstelle**Prüfung nach der Validierung**

```
show version
show module
show diagnostics result module all detail
show environment
show license usage
show interface status
show ip interface brief
show interface status err-disabled
show cdp neighbors
show redundancy status
show spanning-tree summary
show port-channel summary
show vpc
show vpc brief
show vpc role
show vpc peer-keepalives
show vpc statistics peer-keepalive
show vpc consistency-parameters global
show vpc consistency-parameters interface port-channell
show vpc consistency-parameters vlans
show hsrp brief
show vrrp brief
```

## Überlegungen zu vPC bei der VXLAN-Bereitstellung

Für vPC-

VXLAN wird empfohlen, den **delay restore interface-vlan**-Timer in der vPC-Konfiguration zu

erhöhen, wenn die Anzahl der SVIs erhöht wird. Wenn es beispielsweise 1.000 VNIs mit

1.000 SVIs gibt, empfehlen wir, die **Verzögerung** für die **Wiederherstellung des VLAN-**

**Interface**-Timers auf 45 Sekunden zu erhöhen.

```
switch(config-vpc-domain)# delay restore interface-vlan 45
```

Für vPC weist die **Loopback-Schnittstelle** zwei IP-Adressen auf: die **primäre IP-Adresse** und

die **sekundäre IP-Adresse**. Die primäre IP-Adresse ist eindeutig und wird von Layer-3-Protokollen verwendet. Die sekundäre IP-Adresse des Loopbacks ist erforderlich, da sie von der Schnittstelle NVE als VTEP-IP-Adresse verwendet wird. Die sekundäre IP-Adresse muss auf beiden vPC-Peers gleich sein. **Der NVE Hold-Down-Timer** muss höher als der vPC-Verzögerungs-Wiederherstellungs-Timer sein.

```
Leaf-2(config-if-range)# show nve interface nve 1 detail
Interface: nve1, State: Up, encapsulation: VXLAN
VPC Capability: VPC-VIP-Only [notified]
Local Router MAC: 003a.9c28.2cc7
Host Learning Mode: Control-Plane
Source-Interface: loopback1 (primary: 10.1.1.41.1.4, secondary: 10.1.1.10)
Source Interface State: Up
Virtual RMAC Advertisement: Yes
NVE Flags:
Interface Handle: 0x49000001
Source Interface hold-down-time: 180
Source Interface hold-up-time: 30
Remaining hold-down time: 0 seconds
Virtual Router MAC: 0200.1401.010a
Interface state: nve-intf-add-complete
Fabric convergence time: 135 seconds
Fabric convergence time left: 0 seconds
```

Aktivieren Sie für Best Practices die **automatische Wiederherstellung** in Ihrer vPC-Umgebung.

Obwohl selten, gibt es eine Chance, dass vPC Auto-Recovery-Funktion Sie in Dual-Active-Szenario erhalten können. Mit der **vPC-Peer-Switch**-Funktion kann ein Paar von vPC-Peers als einzelner Spanning Tree Protocol-Root in der Layer-2-Topologie angezeigt werden (sie haben dieselbe Bridge-ID). Der vPC-Peer-Switch muss auf beiden vPC-Peers konfiguriert

werden, damit er betriebsbereit ist. Der Befehl lautet:

```
N9K(config-vpc-domain)# peer-switch
```

Mit dem **vPC-Peer-Gateway** kann ein vPC-Peer-Gerät als aktives Gateway für Pakete fungieren, die an die MAC des anderen Peer-Geräterouters adressiert sind. Die Weiterleitung des Datenverkehrs lokal an das vPC-Peer-Gerät wird beibehalten, und die Verwendung des Peer-Links wird vermieden. Wenn die Peer-Gateway-Funktion aktiviert wird, hat dies keine

Auswirkungen auf Datenverkehr und Funktionalität.

```
N9k-1(config)# vpc domain 1
N9k-1(config-vpc-domain)# peer-gateway
```

**Der Layer-3-Peer-Router-Befehl** ermöglicht Routing über den vPC.

```
N9k-1(config)# vpc domain 1
N9k-1(config-vpc-domain)# layer3 peer-router
N9K-1(config-vpc-domain)# exit
```

```
N9K-1# sh vpc
Legend: (*)
- local vPC is down, forwarding via vPC peer-link
vPC domain id : 100
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
```

Configuration consistency status : success  
Per-vlan consistency status : success  
Type-2 consistency status : success  
vPC role : secondary, operational primary  
Number of vPCs configured : 2  
Peer Gateway : Enabled  
Peer gateway excluded VLANs : -  
Peer gateway excluded bridge-domains : -  
Dual-active excluded VLANs and BDs : -  
Graceful Consistency Check : Enabled  
Auto-recovery status : Enabled (timeout = 240 seconds)  
Operational Layer3 Peer-router : Enabled

**Strikte Empfehlungen**Das Peer-Gateway muss vor dem Layer-3-Peer-Router aktiviert werden.Für beide vPC-Peers muss ein Layer-3-Peer-Router konfiguriert sein, damit sie wirksam werden.Aktivieren Sie "Supress-arp" als Best Practice, und verwenden Sie die Multicast-IP-Adresse für VXLAN.Verwenden Sie eine separate Loopback-IP-Adresse für Steuerung und Datenebene in der vPC-VXLAN-Struktur.Bei vPC mit MSTP muss die Bridge-Priorität auf beiden vPC-Peers gleich sein.Für optimale Konvergenzergebnisse optimieren Sie die vPC-Verzögerungswiederherstellung und die NVE-Schnittstellen-Holddown-Timer.

**Zugehörige Informationen**[Nexus Switches der Serie 9000 - Dokumentation Konfigurationsleitfaden für Cisco Nexus NX-OS-Schnittstellen der Serie 9000, Version 9.3\(x\)](#)[Cisco Nexus Serie 9000 - NX-OS Verified Scalability Guide, Version 9.2\(1\) - enthält vPC-Skalierbarkeitsangaben \(CCO\)](#)[Empfohlene Cisco NX-OS-Versionen für Cisco Nexus Switches der Serie 9000](#)[Nexus Switches der Serie 9000 - Versionshinweise](#)[Cisco Nexus Serie 9000 NX-OS VXLAN-Konfigurationsleitfaden, Version 9.2\(x\) - Abschnitt zu vPC Fabric Peering](#)[Konfigurieren des EVPN VXLAN IPV6-Overlay-Konfigurationsbeispiels](#)[Design- und Konfigurationsleitfaden: Best Practices für Virtual Port Channels \(vPC\) auf Cisco Nexus Switches der Serie 7000](#) - Theorie der vPCs N7k und N9k ist ähnlich. In dieser Referenz werden zusätzliche Informationen zu Best Practices behandelt.[Konfigurieren und Überprüfen von doppelseitigem virtuellen vPC](#)

## 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.