Nexus vPC-Schleifenvermeidung

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Hintergrundinformationen

Problem

Netzwerkdiagramm

Szenarien

- Szenario 1: SVI für vPC-VLAN wird auf vPC-Peer administrativ heruntergefahren
  - a) Gerouteter Datenverkehr von vPC zu vPC ist betroffen
  - Fazit:
  - b) Gerouteter Datenverkehr vom verwaisten vPC-Host ist betroffen
  - Fazit:
- Szenario 2: Alle vPCs und SVIs sind aktiv - Next-Hop-Punkte auf den vPC-Peer
  - Fazit:
- Szenario 3: Alle vPCs und SVIs sind aktiv - VPC-Peer-Gateway-Funktion ist deaktiviert
  - Fazit:

Lösungsüberblick

Zugehörige Informationen

Einleitung

In diesem Dokument werden Szenarien beschrieben, in denen sich die vPC-Schleifenvermeidung auf die Weiterleitung von Datenverkehr in Nexus-basierten Layer-3-Netzwerkdesigns auswirken kann.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kommandozeile des Nexus-Betriebssystems
- vPC-Konzepte

Verwendete Komponenten

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

- Software 10.4(4)
- Hardware N9K-C9364C-GX

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

Hintergrundinformationen

In modernen Rechenzentrumsumgebungen ist die Cisco Nexus Virtual Port Channel (vPC)-Technologie unverzichtbar, um Redundanz und Lastenausgleich zu ermöglichen. Da Verbindungen zu zwei separaten Nexus Switches als ein einziger logischer Port-Channel fungieren, vereinfacht vPC die Netzwerkarchitektur und verbessert die Zuverlässigkeit für nachgeschaltete Geräte. Bestimmte Konfigurationsdetails können jedoch zu einer Komplexität der Betriebsabläufe führen.

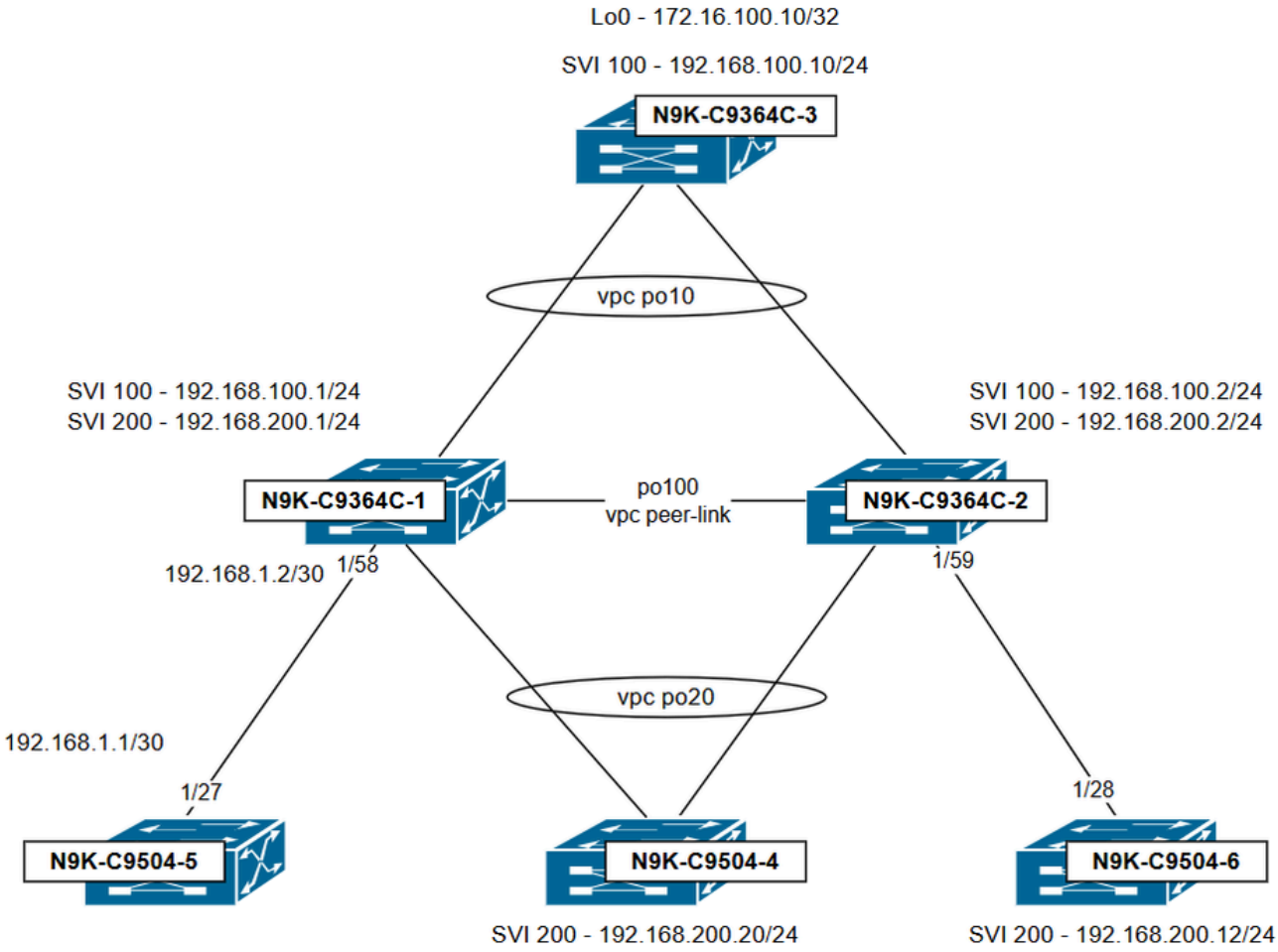
In diesem Dokument werden Szenarien untersucht, in denen die vPC-Schleifenvermeidung eine wichtige Rolle spielt. Außerdem werden die Auswirkungen auf die Weiterleitung von Datenverkehr untersucht. Ein klares Verständnis dieses Mechanismus ist für Netzwerktechniker, die robuste, effiziente Layer-3-Verbindungen in Nexus-basierten Infrastrukturen konzipieren und aufrechterhalten möchten, unerlässlich, um Datenverkehrsunterbrechungen zu verhindern und eine optimale Netzwerkleistung aufrechtzuerhalten.

Problem

In einer Cisco Nexus-Umgebung, die vPC verwendet, können Netzwerkbetreiber ein unerwartetes Weiterleitungsverhalten beobachten, das durch die vPC-Schleifenvermeidungsregel verursacht wird. Wenn Datenverkehr von einem vPC-Peer zu einem anderen über den vPC-Peer-Link übertragen wird, kann er nicht über einen vPC-Port-Channel geleitet werden, der auf beiden Switches aktiv ist. Auf Geräten, die für eine Verbindung auf diesen Pfad angewiesen sind, können daher Pakete verworfen werden oder die Verbindung wird unterbrochen, selbst wenn alle physischen Verbindungen aktiv zu sein scheinen.

Um ausfallsichere Netzwerktopologien zu entwerfen und zu beheben, ist es wichtig, die vPC-Regel zur Vermeidung von Schleifen zu verstehen und zu berücksichtigen, da ein Übersehen dieses Verhaltens zu unerwarteten Serviceunterbrechungen führen und die Diagnose von Netzwerkproblemen schwieriger machen kann.

Netzwerkdiagramm



In dieser Topologie besteht die vPC-Domäne aus N9K-C9364C-1 und N9K-C9364C-2. Beide Switches werden mit den VLANs 100 und 200 als vPC-VLANs konfiguriert, und für jedes VLAN werden SVIs eingerichtet. Die vPC-Domäne ist für das VLAN-übergreifende Routing zwischen diesen VLANs zuständig. Sofern nicht anders angegeben, wird die virtuelle HSRP-IP (VIP), die von den vPC-Peer-Switches gemeinsam verwendet wird, von den anderen Switches in der Topologie als nächster Hop für die Standardroute verwendet.

- N9K-C9364C-1 SVI-Konfiguration

  Schnittstelle Vlan100
  Kein Herunterfahren
  no ip redirects
  ip address 192.168.100.1/24
  Keine IPv6-Umleitungen
  SRP 100
  IP 192.168.100.254

  Schnittstelle Vlan200
  Kein Herunterfahren
  no ip redirects
  ip address 192.168.200.1/24
  Keine IPv6-Umleitungen

SRP 200
IP 192.168.200.254

- N9K-C9364C-2 SVI-Konfiguration

Schnittstelle Vlan100
Kein Herunterfahren
no ip redirects
ip address 192.168.100.2/24
Keine IPv6-Umleitungen
SRP 100
IP 192.168.100.254

Schnittstelle Vlan200
no ip redirects
ip address 192.168.200.2/24
Keine IPv6-Umleitungen
SRP 200
IP 192.168.200.254

Szenarien

Szenario 1: SVI für vPC-VLAN wird auf vPC-Peer administrativ heruntergefahren

a) Gerouteter Datenverkehr von vPC zu vPC ist betroffen

In einem Arbeitsszenario kann N9K-C9504-4 (VLAN 200) erfolgreich einen Ping an N9K-C9364C-3 (VLAN 100) senden. Traceroute gibt an, dass der Verbindungspfad 192.168.200.2 durchläuft, der N9K-C9364C-2 zugewiesen ist.

```
<#root>

N9K-C9504-4#

ping 192.168.100.10


PING 192.168.100.10 (192.168.100.10): 56 data bytes
64 bytes from 192.168.100.10: icmp_seq=0 ttl=253 time=8.48 ms
64 bytes from 192.168.100.10: icmp_seq=1 ttl=253 time=0.618 ms
64 bytes from 192.168.100.10: icmp_seq=2 ttl=253 time=0.582 ms
64 bytes from 192.168.100.10: icmp_seq=3 ttl=253 time=0.567 ms
64 bytes from 192.168.100.10: icmp_seq=4 ttl=253 time=0.55 ms

--- 192.168.100.10 ping statistics ---

5 packets transmitted, 5 packets received, 0.00% packet loss


round-trip min/avg/max = 0.55/2.159/8.48 ms
N9K-C9504-4#
```

```
<#root>

N9K-C9504-4#

traceroute 192.168.100.10


traceroute to 192.168.100.10 (192.168.100.10), 30 hops max, 40 byte packets

1 192.168.200.2 (192.168.200.2) 1.129 ms 0.602 ms 0.724 ms    <<<---- SVI 200 on N9K-C9364C-2


2 192.168.100.10 (192.168.100.10) 1.001 ms 0.657 ms 0.588 ms
```

Der Datenverkehrsfluss funktioniert derzeit wie folgt:

- N9K-C9364C-2 empfängt Datenverkehr von 192.168.200.20, der für 192.168.100.10 bestimmt ist, wobei die Ziel-MAC-Adresse auf die gemeinsam genutzte virtuelle HSRP-MAC (VMAC) in der vPC-Domäne festgelegt ist.
- Da HSRP auf dem vPC aus Sicht der Datenebene im Aktiv-Aktiv-Modus betrieben wird, leitet N9K-C9364C-2 den Datenverkehr von VLAN 200 an VLAN 100 weiter und leitet ihn über vPC 10 weiter.

Stellen Sie sich ein Szenario vor, in dem SVI 200 auf N9K-C9364C-2 heruntergefahren wird, aber auf N9K-C9364C-1 aktiv bleibt:

```
<#root>

N9K-C9364C-1#

show ip interface brief



IP Interface Status for VRF "default"(1)
Interface IP Address Interface Status
Vlan100 192.168.100.1 protocol-up/link-up/admin-up

Vlan200 192.168.200.1 protocol-up/link-up/admin-up <<<---- SVI 200 is up


N9K-C9364C-1#
```

```
<#root>

N9K-C9364C-2#

show ip interface brief



IP Interface Status for VRF "default"(1)
Interface IP Address Interface Status
Vlan100 192.168.100.2 protocol-up/link-up/admin-up
```

```
Vlan200 192.168.200.2 protocol-down/link-down/admin-down  <<<---- SVI 200 is down

N9K-C9364C-2#
```

Aufgrund des unterschiedlichen Betriebsstatus der SVIs zwischen den vPC-Peers wird eine Typ-2-Inkonsistenz in der vPC-Domäne erkannt:

<#root>

```
N9K-C9364C-1#

show 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 : failed

Type-2 inconsistency reason : SVI type-2 configuration incompatible


vPC role : primary
Number of vPCs configured : 2
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

vPC Peer-link status
---------------------------------------------------------------------
id Port Status Active vlans
-- ---- ------ --------------------------------------------------
1 Po100 up 1,100,200

vPC status
----------------------------------------------------------------------------
Id Port Status Consistency Reason Active vlans
-- ------------ ------ ----------- ------ ---------------
10 Po10 up success success 1,100,200
20 Po20 up success success 1,100,200
N9K-C9364C-1#
```

<#root>

```
N9K-C9364C-2#
```

```
show 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 : failed

Type-2 inconsistency reason : SVI type-2 configuration incompatible


vPC role : secondary
Number of vPCs configured : 2
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)
Operational Layer3 Peer-router : Disabled
Virtual-peerlink mode : Disabled

vPC Peer-link status
---------------------------------------------------------------------
id Port Status Active vlans
-- ---- ------ --------------------------------------------------
1 Po100 up 1,100,200

vPC status
----------------------------------------------------------------------------
Id Port Status Consistency Reason Active vlans
-- ------------ ------ ----------- ------ ---------------
10 Po10 up success success 1,100,200
20 Po20 up success success 1,100,200

N9K-C9364C-2#
```

Zum gegenwärtigen Zeitpunkt ist der Datenverkehr vom 192.168.200.20 bis zum 192.168.100.10 nicht mehr erfolgreich:

<#root>

```
N9K-C9504-4#

ping 192.168.100.10


PING 192.168.100.10 (192.168.100.10): 56 data bytes
Request 0 timed out
Request 1 timed out
Request 2 timed out
Request 3 timed out
Request 4 timed out
```

```
--- 192.168.100.10 ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss
N9K-C9504-4#
```

Ein farbiger Ping (ein Ping mit einer angegebenen MTU-Größe) wird verwendet, um den Pfad zu verfolgen, der von diesem Datenverkehr verwendet wird:

<#root>

```
N9K-C9504-4#
```

ping 192.168.100.10 count 100 timeout 0 packet-size 1030

```
PING 192.168.100.10 (192.168.100.10): 1030 data bytes
Request 0 timed out
Request 1 timed out
---- snip -----
Request 98 timed out
Request 99 timed out

--- 192.168.100.10 ping statistics ---
```

100 packets transmitted, 0 packets received, 100.00% packet loss

```
N9K-C9504-4# ^C
N9K-C9504-4#
```

Den Schnittstellenzählern auf N9K-C9364C-2 zufolge wird dieser Datenverkehr auf Port-Channel 20 empfangen und an Port-Channel 100 (den vPC-Peer-Link) weitergeleitet:

<#root>

```
N9K-C9364C-2#
```

show interface port-channel 20 counters detailed all | i "1024 to|po" ; sh int port-channel 10 counters

port-channel20

```
52.
```

Rx Packets from 1024 to 1518 bytes: = 100   <<<----- Ingress vPC po20

```
60. Tx Packets from 1024 to 1518 bytes: = 0
port-channel10
52. Rx Packets from 1024 to 1518 bytes: = 0
60. Tx Packets from 1024 to 1518 bytes: = 0
```

port-channel100

```
52. Rx Packets from 1024 to 1518 bytes: = 0
```

```
60.
Tx Packets from 1024 to 1518 bytes: = 100 <<<----- Egress po100 (vPC peer-link)

N9K-C9364C-2#
```

Dieses Verhalten tritt auf, weil SVI 200 auf dem N9K-C9364C-2 heruntergefahren wird, wodurch das lokale Routing des Datenverkehrs für VLAN 200 verhindert wird. In diesem Szenario wird der Datenverkehr über den vPC-Peer-Link zu N9K-C9364C-1 überbrückt, sodass das Gerät das Inter-VLAN-Routing durchführt.

Wenn Sie sich die Schnittstellenzähler auf N9K-C9364C-1 ansehen, wird bestätigt, dass die Pakete dieses Gerät über die vPC Peer-Verbindung erreichen. Auf dem vPC-Port-Channel 10, der mit 192.168.100.10 verbunden ist, wurden jedoch keine ausgehenden Pakete beobachtet.

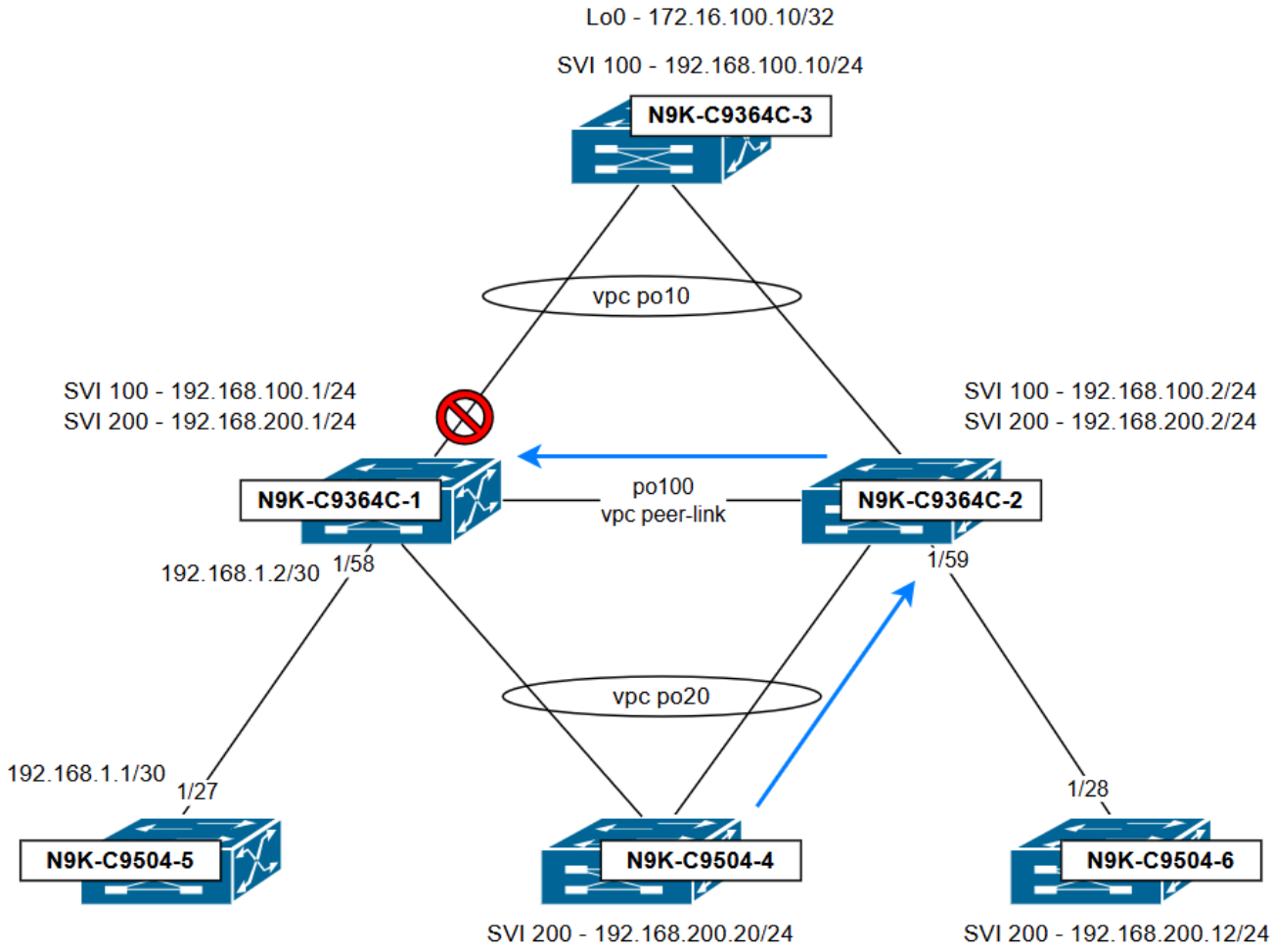
```
<#root>
N9K-C9364C-1#
show interface port-channel 20 counters detailed all | i "1024 to|po" ; sh int port-channel 10 counters


port-channel20
52. Rx Packets from 1024 to 1518 bytes: = 0
60. Tx Packets from 1024 to 1518 bytes: = 0
port-channel10
52. Rx Packets from 1024 to 1518 bytes: = 0
60.
Tx Packets from 1024 to 1518 bytes: = 0  <<<----- Expected egress vPC po10. No packets!!!


port-channel100
52.
Rx Packets from 1024 to 1518 bytes: = 100 <<<----- Ingress po100 (vPC peer-link)


60. Tx Packets from 1024 to 1518 bytes: = 0
N9K-C9364C-1#
```

Obwohl der Datenverkehr über die vPC-Peer-Verbindung an N9K-C9364C-1 ankommt, wird er nicht an den vPC-Port-Channel 10 weitergeleitet. Dies liegt daran, dass das egress_vsl_drop-Bit für diesen vPC auf 1 festgelegt ist, was geschieht, wenn derselbe vPC-Port-Channel auf dem Peer-Switch betriebsbereit ist (in diesem Fall N9K-C9364C-2)

```
<#root>
N9K-C9364C-1#
show system internal eltm info interface Po10 | i i vsl
```

```
egress_vsl_drop = 1


N9K-C9364C-1#



<#root>

N9K-C9364C-1#

show system internal vPCm info interface Po10 | i "Peer stat|Inform|vPC sta"


IF Elem Information:
MCECM DB Information:

vPC state: Up Old Compat Status: Pass


vPC Peer Information:

Peer state: Up         <<<------------- vPC 10 up on peer


PSS Information:

vPC state: Up Old Compat Status: Pass


vPC Peer Information:

Peer state: Up         <<<------------- vPC 10 up on peer


Shared Database Information:
Application database Information:
Lock Information:
N9K-C9364C-1#
```

Topologie, die den Datenverkehrsfluss und den Punkt veranschaulicht, an dem er verworfen wird:



Fazit:

N9K-C9364C-1 verwirft Datenverkehr aufgrund der vPC-Schleifenvermeidungsregel: Der über den vPC Peer-Link empfangene Datenverkehr kann nicht über einen vPC-Port-Channel weitergeleitet werden, der auf beiden Switches aktiv ist."Um dieses Problem zu vermeiden, stellen Sie sicher, dass der administrative Status der SVIs auf beiden Switches konsistent ist und dass ihre Konfigurationen symmetrisch sind.

b) Gerouteter Datenverkehr vom verwaisten zum vPC-Host ist betroffen

Im selben Szenario wird SVI 200 auf N9K-C9364C-2 heruntergefahren, bleibt aber auf N9K-C9364C-1 aktiv. Ein Ping von N9K-C9504-6 (VLAN 200) an N9K-C9364C-3. (VLAN 100) fehlgeschlagen.

<#root>

```
N9K-C9504-6#

ping 192.168.100.10 packet-size 1030 count 100 timeout 0


PING 192.168.100.10 (192.168.100.10): 1030 data bytes
Request 0 timed out
```

```
Request 1 timed out
Request 2 timed out
---- snip -----
Request 97 timed out
Request 98 timed out
Request 99 timed out

--- 192.168.100.10 ping statistics ---

100 packets transmitted, 0 packets received, 100.00% packet loss


N9K-C9504-6#
```

Ein farbiger Ping (ein Ping mit einer angegebenen MTU-Größe) wird verwendet, um den Pfad zu verfolgen, der von diesem Datenverkehr verwendet wird:

<#root>

```
N9K-C9364C-2#

show interface eth1/59 counters detailed all | i "1024 to|Eth" ; sh int port-channel 10 counters detaile


Ethernet1/59

52. Rx Packets from 1024 to 1518 bytes: = 100 <<<----- Ingress port to N9K-C9504-6


60. Tx Packets from 1024 to 1518 bytes: = 0
port-channel10
52. Rx Packets from 1024 to 1518 bytes: = 0
60. Tx Packets from 1024 to 1518 bytes: = 0
port-channel100
52. Rx Packets from 1024 to 1518 bytes: = 0

60. Tx Packets from 1024 to 1518 bytes: = 100 <<<----- Egress po100 (vPC peer-link)


N9K-C9364C-2#
```

<#root>

```
N9K-C9364C-1#

show interface port-channel 10 counters detailed all | i "1024 to|po" ; sh int port-channel 100 counters


port-channel10
52. Rx Packets from 1024 to 1518 bytes: = 0

60. Tx Packets from 1024 to 1518 bytes: = 0 <<<----- Expected egress vPC po10. No packets!!!


port-channel100

52. Rx Packets from 1024 to 1518 bytes: = 100 <<<----- Ingress po100 (vPC peer-link)
```

```
60. Tx Packets from 1024 to 1518 bytes: = 0
N9K-C9364C-1#
```

Obwohl der Datenverkehr über die vPC-Peer-Verbindung an N9K-C9364C-1 ankommt, wird er nicht an den vPC-Port-Channel 10 weitergeleitet. Dies liegt daran, dass das egress_vsl_drop-Bit für diesen vPC auf 1 festgelegt ist, was geschieht, wenn derselbe vPC-Port-Channel auf dem Peer-Switch betriebsbereit ist (in diesem Fall N9K-C9364C-2)

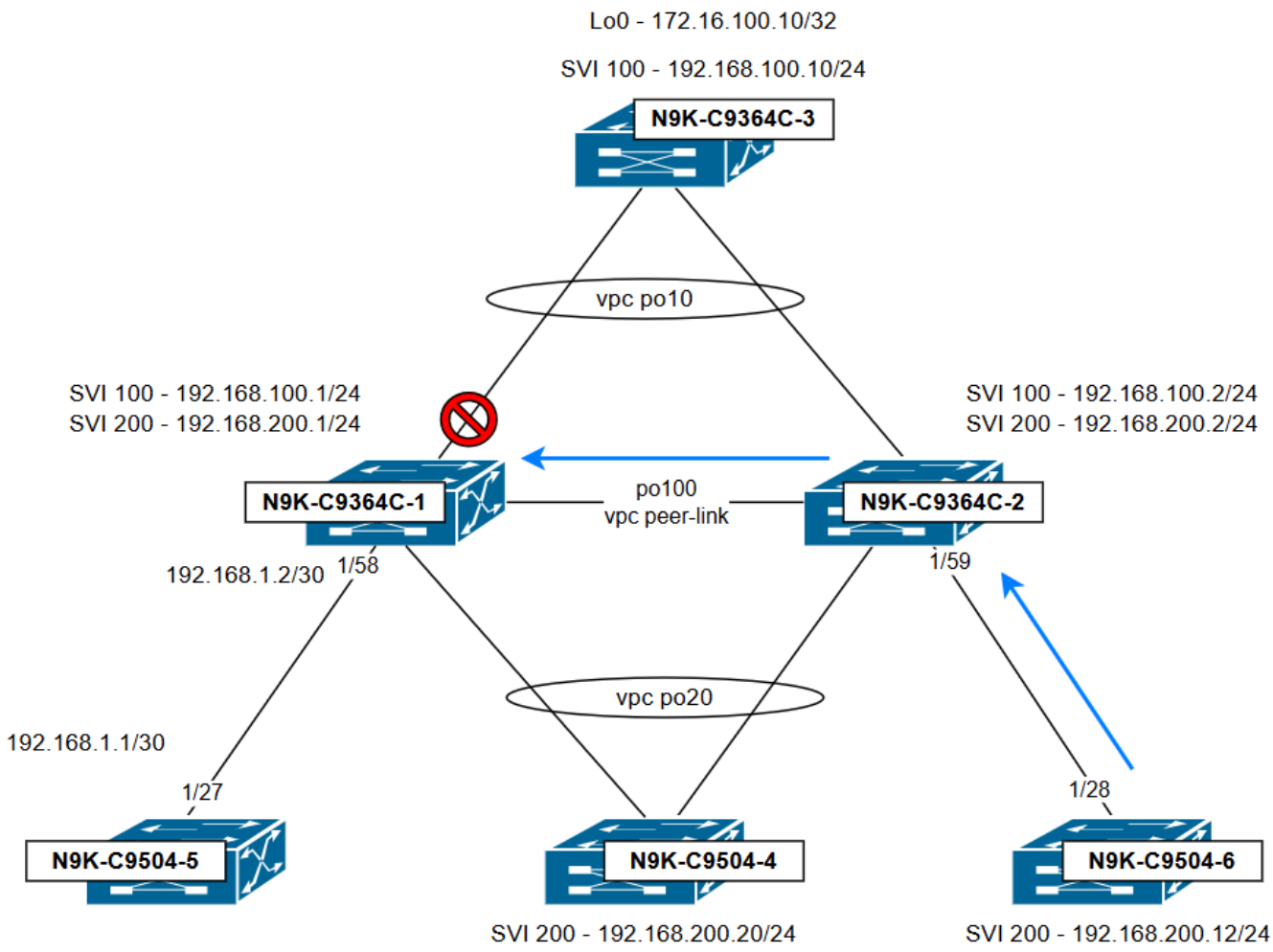
<#root>

```
N9K-C9364C-1#
show system internal eltm info interface Po10 | i i vsl


egress_vsl_drop = 1


N9K-C9364C-1#
```

<#root>

```
N9K-C9364C-1#
show system internal vpcm info interface Po10 | i "Peer stat|Inform|vPC sta"


IF Elem Information:
MCECM DB Information:
vPC state: Up Old Compat Status: Pass


vPC Peer Information:
Peer state: Up <<<------------- vPC 10 up on peer


PSS Information:
vPC state: Up Old Compat Status: Pass


vPC Peer Information:
Peer state: Up <<<------------- vPC 10 up on peer


Shared Database Information:
Application database Information:
Lock Information:
N9K-C9364C-1#
```

Topologie, die den Datenverkehrsfluss und den Punkt, an dem er verworfen wird, veranschaulicht:



Fazit:

Obwohl der Datenverkehr von einem verwaisten Host stammt, der mit N9K-C9364C-2 verbunden ist, wird er von N9K-C9364C-1 aufgrund der vPC-Schleifenvermeidungsregel verworfen: Der über den vPC Peer-Link empfangene Datenverkehr kann nicht über einen vPC-Port-Channel weitergeleitet werden, der auf beiden Switches aktiv ist. Ob der Eingangs-Port auf dem Peer-Switch ein vPC oder ein verwaister Port ist, spielt keine Rolle. Wichtig ist, dass der Datenverkehr über die vPC Peer-Verbindung eingeht und für einen vPC bestimmt ist, der auf beiden Switches aktiv ist. Um dieses Problem zu vermeiden, stellen Sie sicher, dass der administrative Status der SVIs auf beiden Switches konsistent ist und dass ihre Konfigurationen symmetrisch sind.

Szenario 2: Alle vPCs und SVIs sind aktiv - Next-Hop-Punkte für den vPC-Peer

In diesem Szenario sind alle SVIs und vPC-Port-Channels in der vPC-Domäne aktiv. N9K-C9504-5, das über eine Layer-3-Schnittstelle mit N9K-C9364C-1 verbunden ist, kann jedoch keinen Ping für Loopback 0 auf N9K-C9364C-3 senden.

Eine Traceroute von N9K-C9504-5 gibt an, dass das Paket zuerst seinen unmittelbaren nächsten Hop bei 192.168.1.2 erreicht und dann zu 192.168.100.2 weitergeht, der mit N9K-C9364C-2 verknüpft ist.

<#root>

N9K-C9504-5#

traceroute 172.16.100.10

traceroute to 172.16.100.10 (172.16.100.10), 30 hops max, 40 byte packets
1 192.168.1.2

(192.168.1.2)

 1.338 ms 0.912 ms 0.707 ms
2 192.168.100.2

(192.168.100.2)

 0.948 ms 0.751 ms 0.731 ms
3 * * *
4 * * *
N9K-C9504-5#

Die Next-Hop-Verifizierung von N9K-C9364C-1 (dem ersten Hop für diesen Datenverkehr) zeigt, dass das Ziel bis 192.168.100.2 erreichbar ist, was SVI 100 auf N9K-C9364C-2 entspricht.

<#root>

N9K-C9364C-1#

 show ip route 172.16.100.10

IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

172.16.100.0/24, ubest/mbest: 1/0
*

via 192.168.100.2

, [1/0], 00:05:05, static
N9K-C9364C-1#

Ein farbiger Ping (ein Ping mit einer angegebenen MTU-Größe) wird verwendet, um den Pfad zu verfolgen, der von diesem Datenverkehr verwendet wird:

<#root>

N9K-C9364C-1#

show interface e1/58 counters detailed all | i "1024 to|Eth" ; sh int port-channel 100 counters detailed

Ethernet1/58
52.

Rx Packets from 1024 to 1518 bytes: = 100 <<<----- Ingress Eth1/58

60. Tx Packets from 1024 to 1518 bytes: = 0
port-channel100
52. Rx Packets from 1024 to 1518 bytes: = 0
60.

Tx Packets from 1024 to 1518 bytes: = 100 <<<----- Egress po100 (vPC peer-link)

port-channel10
52. Rx Packets from 1024 to 1518 bytes: = 0
60. Tx Packets from 1024 to 1518 bytes: = 0
N9K-C9364C-1#

<#root>

N9K-C9364C-2# sh int port-channel 100 counters detailed all | i "1024 to|po" ; sh int port-channel 10 c
port-channel100
52.

Rx Packets from 1024 to 1518 bytes: = 100 <<<----- Ingress po100 (vPC peer-link)

60. Tx Packets from 1024 to 1518 bytes: = 0
port-channel10
52. Rx Packets from 1024 to 1518 bytes: = 0
60.

Tx Packets from 1024 to 1518 bytes: = 0 <<<----- Egress vPC po10, no packets!!!

N9K-C9364C-2#

Obwohl der Datenverkehr über den vPC-Peer-Link an N9K-C9364C-2 ankommt, wird er nicht an den vPC-Port-Channel 10 weitergeleitet. Dies liegt daran, dass das Bit "egress_vsl_drop" für diesen vPC auf "1" festgelegt ist, was geschieht, wenn derselbe vPC-Port-Channel auf dem Peer-Switch betriebsbereit ist (in diesem Fall N9K-C9364C-1).

<#root>

N9K-C9364C-2#

show system internal eltm info interface Po10 | i i vsl

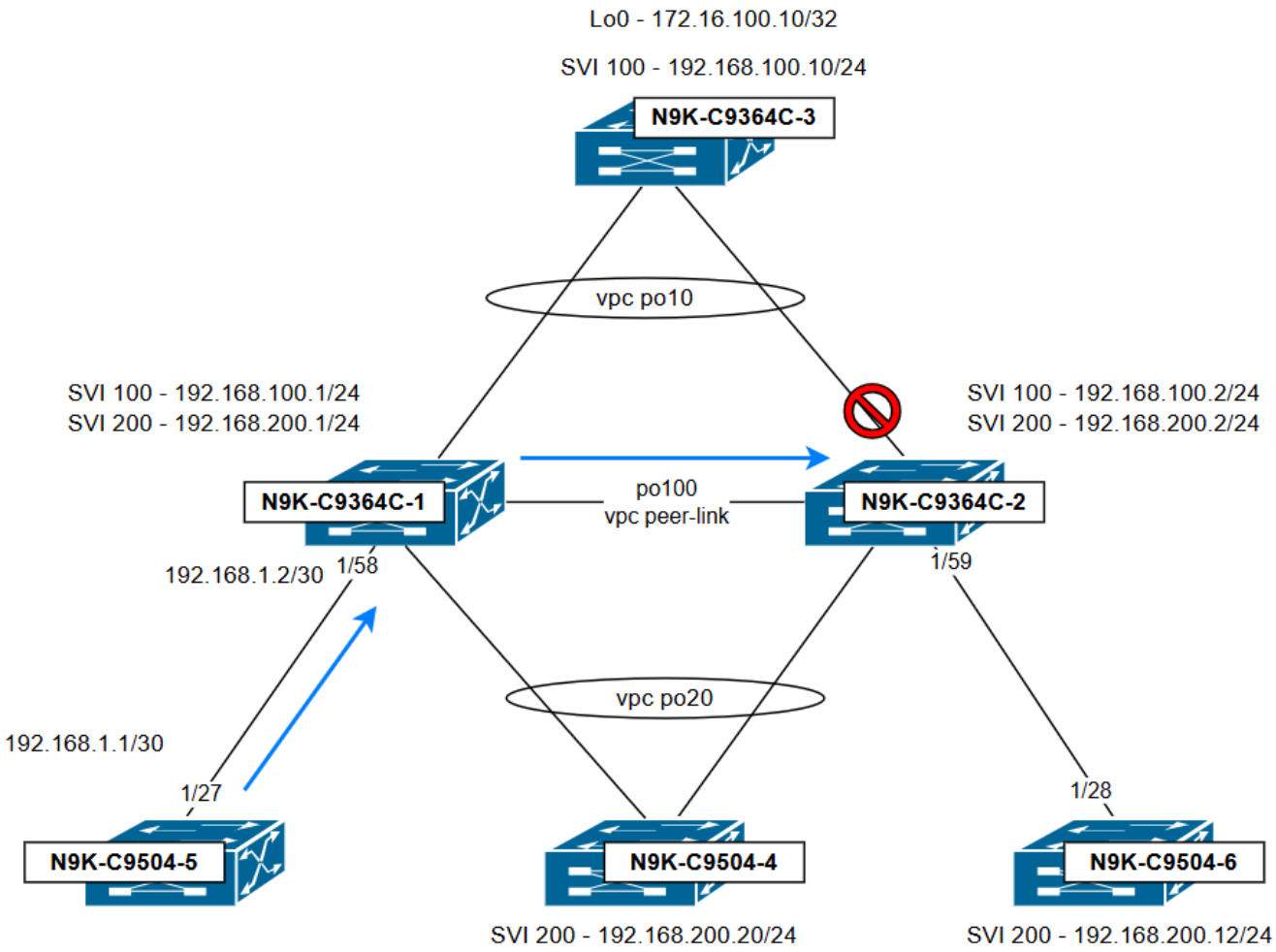
egress_vsl_drop = 1

N9K-C9364C-2#

<#root>

```
N9K-C9364C-2# show system internal vPCm info interface Po10 | i "Peer stat|Inform|vPC sta"
IF Elem Information:
MCECM DB Information:

vPC state: Up Old Compat Status: Pass


vPC Peer Information:

Peer state: Up <<<------------ vPC 10 up on peer


PSS Information:
vPC state: Up Old Compat Status: Pass
vPC Peer Information:

Peer state: Up <<<------------ vPC 10 up on peer


Shared Database Information:
Application database Information:
Lock Information:
N9K-C9364C-2#
```

Topologie, die den Datenverkehrsfluss und den Punkt, an dem er verworfen wird, veranschaulicht:



Fazit:

Das Problem wurde beobachtet, da N9K-C9364C-1 N9K-C9364C-2 als nächsten Hop verwendet und Datenverkehr über die vPC Peer-Verbindung sendet, bevor dieser versucht, über vPC 10 den Datenverkehr zu verlassen. Der Datenverkehr wird aufgrund der vPC-Schleifenvermeidungsregel verworfen: Der über den vPC-Peer-Link empfangene Datenverkehr kann nicht über einen vPC-Port-Channel weitergeleitet werden, der auf beiden Switches aktiv ist. Um dieses Problem zu vermeiden, stellen Sie sicher, dass Routen (dynamisch oder statisch) mit einem nächsten Hop über einen vPC-Port-Channel auf beiden vPC-Peer-Switches konfiguriert sind, sodass Datenverkehr nicht über den vPC-Peer-Link übertragen und über einen vPC ausgehen muss.

Szenario 3: Alle vPCs und SVIs sind aktiv - VPC-Peer-Gateway-Funktion ist deaktiviert

In diesem Szenario befinden sich alle SVIs und vPC-Port-Channels in der vPC-Domäne. Die vPC-Peer-Gateway-Funktion ist jedoch deaktiviert. An diesem Punkt kann N9K-C9504-4 (VLAN 200) keinen Ping an N9K-C9364C-3 (VLAN 100) senden.

<#root>

```
N9K-C9504-4#
```

ping 192.168.100.10

```
PING 192.168.100.10 (192.168.100.10): 56 data bytes
Request 0 timed out
Request 1 timed out
Request 2 timed out
Request 3 timed out
Request 4 timed out

--- 192.168.100.10 ping statistics ---
```

5 packets transmitted, 0 packets received, 100.00% packet loss

```
N9K-C9504-4#
```

Die Next-Hop-Verifizierung von N9K-C9504-4 zeigt, dass das Ziel bis 192.168.200.2 erreichbar ist. Dies entspricht SVI 200 auf N9K-C9364C-2 und ist über den vPC-Port-Channel 20 verbunden.

<#root>

```
N9K-C9504-4#
```

show ip route 192.168.100.10

```
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
```

```
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

0.0.0.0/0, ubest/mbest: 1/0
*via
```

192.168.200.2

```
, [1/0], 01:22:46, static
N9K-C9504-4#
```

<#root>

```
N9K-C9504-4#
```

show ip arp detail | i 192.168.200.2

192.168.200.2

```
 00:08:05
```

a478.06de.7edb

```
 Vlan200 port-channel20 default
```

Ein farbiger Ping (ein Ping mit einer angegebenen MTU-Größe) wird verwendet, um den Pfad zu verfolgen, der von diesem Datenverkehr verwendet wird. Hier zeigen die Schnittstellenzähler an, dass N9K-C9364C-1 den Datenverkehr von 192.168.200.20 bis 192.168.100.10 über Port-Channel 20 empfängt und an die vPC Peer-Verbindung (Port-Channel100) sendet.

<#root>

```
N9K-C9364C-1#
```

show interface port-channel 20 counters detailed all | i "1024 to|po" ; sh int port-channel 10 counters

```
port-channel20
52.
```

Rx Packets from 1024 to 1518 bytes: = 100   <<<----- Ingress vPC 20

```
60. Tx Packets from 1024 to 1518 bytes: = 0
port-channel10
52. Rx Packets from 1024 to 1518 bytes: = 0
60. Tx Packets from 1024 to 1518 bytes: = 0
port-channel100
52. Rx Packets from 1024 to 1518 bytes: = 0
60.
```

Tx Packets from 1024 to 1518 bytes: = 100   <<<----- Egress po100 (vPC peer-link)

```
N9K-C9364C-1#
```

N9K-C9364C-2 empfängt den Datenverkehr über die vPC Peer-Verbindung (Port-Channel 100), leitet ihn jedoch nicht an vPC Port-Channel 10 weiter.

```
<#root>

N9K-C9364C-2#

show int port-channel 20 counters detailed all | i "1024 to|po" ; sh int port-channel 10 counters detail


port-channel20
52. Rx Packets from 1024 to 1518 bytes: = 0
60. Tx Packets from 1024 to 1518 bytes: = 0
port-channel10
52. Rx Packets from 1024 to 1518 bytes: = 0
60. Tx Packets from 1024 to 1518 bytes: = 0

   <<<----- Egress vPC po10, no packets!!!


port-channel100

52. Rx Packets from 1024 to 1518 bytes: = 100  <<<----- Ingress po100 (vPC peer-link)


60. Tx Packets from 1024 to 1518 bytes: = 0
N9K-C9364C-2#
```

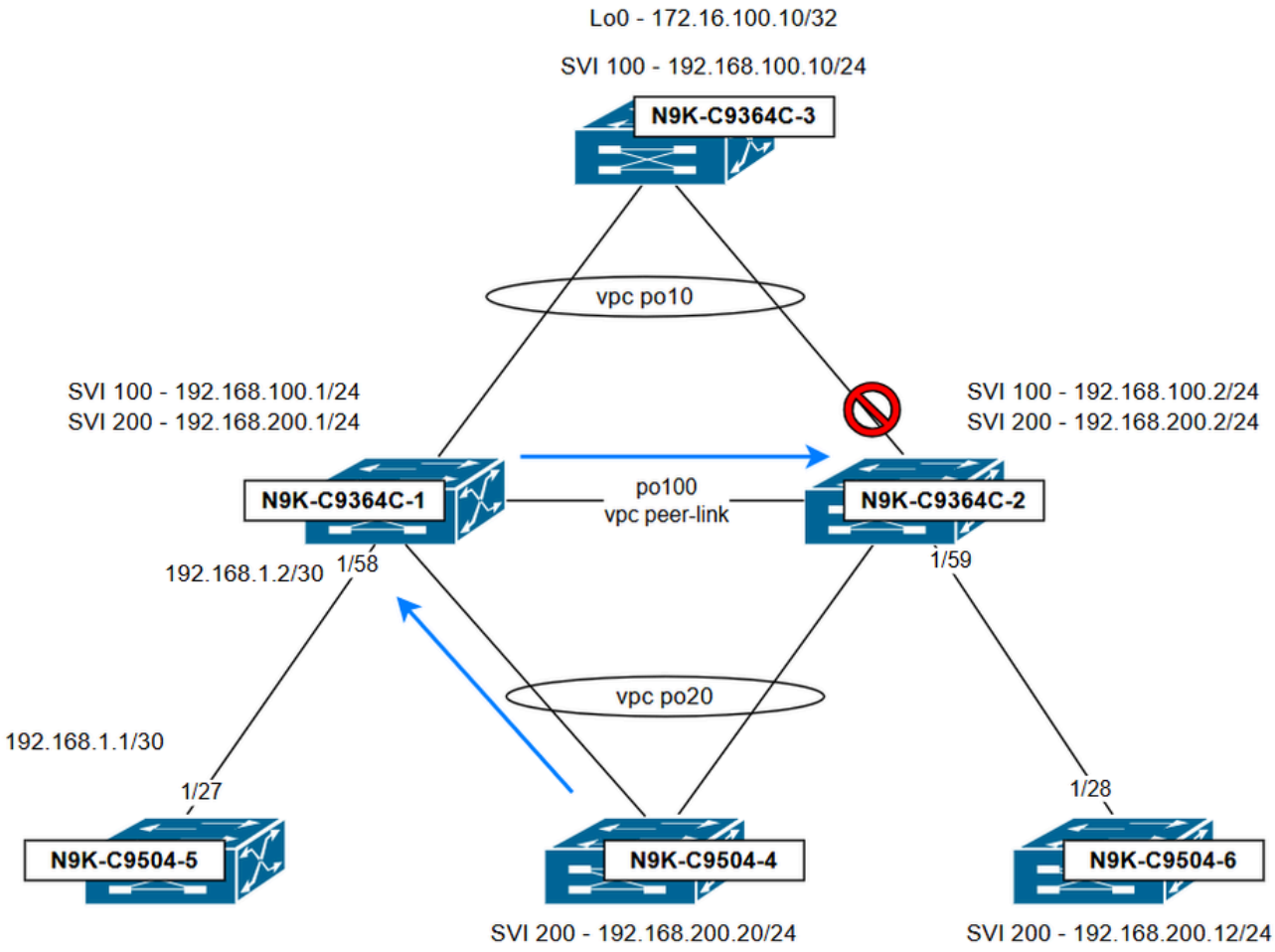
Obwohl der Datenverkehr über die vPC-Peer-Verbindung an N9K-C9364C-2 ankommt, wird er nicht an den vPC-Port-Channel 10 weitergeleitet. Dies liegt daran, dass das egress_vsl_drop-Bit für diesen vPC auf 1 festgelegt ist, was geschieht, wenn derselbe vPC-Port-Channel auf dem Peer-Switch betriebsbereit ist (in diesem Fall N9K-C9364C-1).

Da das Peer-Gateway deaktiviert ist, kann N9K-C9364C-1 nur Pakete weiterleiten, die an die eigene lokale MAC-Adresse adressiert sind. Daher werden Pakete, die an a478.06de.7edb (MAC von N9K-C9364C-2) gerichtet sind, von N9K-C9364C-1 über die vPC-Peer-Verbindung weitergeleitet.

```
<#root>

N9K-C9364C-1#

show mac address-table add a478.06de.7edb


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
---------+-----------------+--------+---------+------+----+------------------
* 100

a478.06de.7edb

 static - F F
```

```
vPC Peer-Link

(R)
* 200

a478.06de.7edb

 static - F F

vPC Peer-Link

(R)
N9K-C9364C-1#
```

Topologie, die den Datenverkehrsfluss und den Punkt, an dem er verworfen wird, veranschaulicht:



Fazit:

Wenn das Peer-Gateway aktiviert ist, wird der für die MAC-Adresse des vPC-Peers bestimmte geroutete Datenverkehr lokal verarbeitet, indem die Peer-MAC als Gateway programmiert wird. Dadurch wird verhindert, dass der vPC-Peer-Link im Datenverkehrspfad verwendet wird, und durch die vPC-Schleifenvermeidungsregel verursachte Datenverluste werden vermieden. Um solche Probleme zu vermeiden, stellen Sie sicher, dass die vPC Peer-Gateway-Funktion in der vPC-Domäne aktiviert ist.

Lösungsüberblick

- Konsistente SVI-Konfiguration in vPC-VLANs

Asymmetric Switched Virtual Interface (SVI)-Konfigurationen zwischen vPC-Peer-Switches können zu kritischen Problemen bei der Weiterleitung des Datenverkehrs führen, einschließlich Blackholing des Datenverkehrs. Eine gängige, jedoch nicht unterstützte Vorgehensweise, die zu dieser Bedingung beiträgt, ist das Testen des Failovers zwischen vPC-Peers durch das Herunterfahren von SVIs auf einer Seite. Durch diese Methode wird ein asymmetrischer SVI-Status erstellt, der von der Nexus vPC-Architektur nicht unterstützt wird. Dies führt zu Datenverkehrs-Blackholing und Weiterleitungsfehlern. Stellen Sie sicher, dass die SVI-Konfiguration in allen vPC-VLANs, für die Routing erforderlich ist, immer konsistent ist.

- Aktivieren Sie Peer-Gateway in der vPC-Domäne.

Die Peer-Gateway-Funktion stellt eine wichtige Erweiterung bei Cisco Nexus vPC-Bereitstellungen dar. Wenn diese Funktion in der vPC-Domäne aktiviert ist, kann jeder vPC-Peer-Switch Pakete akzeptieren und verarbeiten, die für die virtuelle MAC-Adresse des vPC-Peers bestimmt sind. Dies bedeutet, dass jeder vPC-Peer auf Gateway-gebundenen Datenverkehr reagieren kann, unabhängig davon, welcher Switch das Paket ursprünglich empfangen hat. Ohne Aktivierung des Peer-Gateways können bestimmte Datenverkehrstypen - z. B. an die Standard-Gateway-MAC-Adresse gesendete Pakete - verworfen werden, wenn sie auf einem Peer eintreffen und andernfalls den Peer-Link durchlaufen und einen vPC-Member-Port verlassen müssten. Stellen Sie sicher, dass das vPC-Peer-Gateway in der vPC-Domäne konfiguriert ist.

Zugehörige Informationen

Informationen zu Verbesserungen bei Virtual Port Channel (vPC)

Best Practices für Virtual Port Channels (vPC) auf Nexus

Peer-Gateway-Funktion auf dem Nexus 7000

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.