# Prevenzione dei loop VPC Nexus

## Sommario



## Introduzione

In questo documento vengono descritti gli scenari in cui la prevenzione dei loop vPC può influire sull'inoltro del traffico nelle progettazioni di reti di layer 3 basate su Nexus.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CLI del sistema operativo Nexus
- Concetti su vPC

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software 10.4(4)

- Hardware N9K-C9364C-GX

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Premesse

Negli attuali ambienti di data center, la tecnologia vPC (Virtual Port Channel) di Cisco Nexus è essenziale per consentire ridondanza e bilanciamento del carico. Consentendo alle connessioni a due switch Nexus distinti di funzionare come un singolo canale di porta logica, vPC semplifica l'architettura di rete e migliora l'affidabilità per i dispositivi downstream. Tuttavia, alcuni dettagli di configurazione possono introdurre complessità operative.

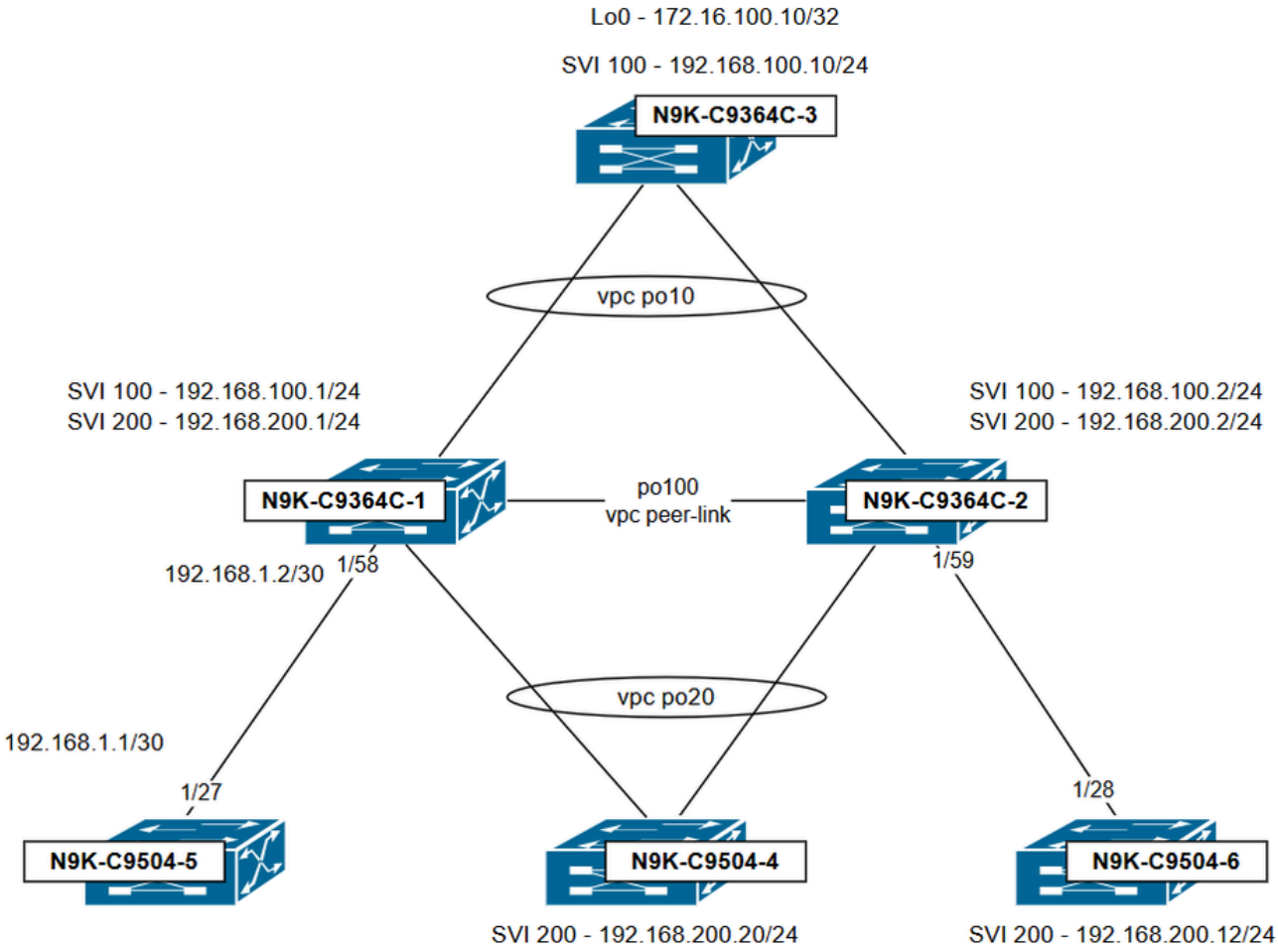
In questo documento vengono esaminati gli scenari in cui la prevenzione dei loop vPC diventa importante e viene esaminato il relativo impatto sull'inoltro del traffico. Una chiara comprensione di questo meccanismo è fondamentale per i tecnici di rete che desiderano progettare e mantenere una connettività di layer 3 robusta ed efficiente nelle infrastrutture basate su Nexus, contribuendo a prevenire interruzioni del traffico e a mantenere prestazioni di rete ottimali.

# Problema

In un ambiente Cisco Nexus che utilizza vPC, gli operatori di rete possono osservare un comportamento imprevisto di inoltro del traffico causato dalla regola di prevenzione del loop vPC. Quando il traffico passa da un peer vPC all'altro attraverso il collegamento peer vPC, non può attraversare alcun canale di porta vPC attivo su entrambi gli switch. Di conseguenza, i dispositivi che dipendono da questo percorso per la connettività possono subire la perdita di pacchetti o la perdita di connettività, anche se tutti i collegamenti fisici risultano attivi.

La comprensione e l'accounting per la regola di prevenzione dei loop vPC è essenziale per la progettazione e la risoluzione dei problemi relativi a topologie di rete resilienti, in quanto ignorare questo comportamento può causare interruzioni impreviste del servizio e rendere i problemi di rete più difficili da diagnosticare.

# Esempio di rete




In questa topologia, il dominio vPC è composto da N9K-C9364C-1 e N9K-C9364C-2. Entrambi gli switch sono configurati con le VLAN 100 e 200 come VLAN vPC e le SVI sono configurate per ciascuna VLAN. Il dominio vPC è responsabile del routing tra VLAN tra queste VLAN. Se non diversamente specificato, l'IP virtuale (VIP) HSRP condiviso tra gli switch peer vPC viene usato come hop successivo per il routing predefinito dagli altri switch della topologia.

- Configurazione N9K-C9364C-1 SVI

```
interface Vlan100
nessuna chiusura
no ip redirects
indirizzo ip 192.168.100.1/24
nessun reindirizzamento ipv6
hsrp 100
ip 192.168.100.254

interface Vlan200
nessuna chiusura
no ip redirects
indirizzo ip 192.168.200.1/24
nessun reindirizzamento ipv6
hsrp 200
```

ip 192.168.200.254

- Configurazione N9K-C9364C-2 SVI

interface Vlan100
nessuna chiusura
no ip redirects
indirizzo ip 192.168.100.2/24
nessun reindirizzamento ipv6
hsrp 100
ip 192.168.100.254

interface Vlan200
no ip redirects
indirizzo ip 192.168.200.2/24
nessun reindirizzamento ipv6
hsrp 200
ip 192.168.200.254

# Scenari

## Scenario 1: La SVI per la VLAN vPC è chiusa manualmente sul peer vPC

a) Il traffico indirizzato da vPC a vPC è interessato

In uno scenario di lavoro, N9K-C9504-4 (VLAN 200) può eseguire correttamente il ping di N9K-C9364C-3 (VLAN 100). Traceroute indica che il percorso di connessione passa per 192.168.200.2, che è assegnato a N9K-C9364C-2.

<#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
```

A questo punto, il flusso del traffico funziona nel modo seguente:

- N9K-C9364C-2 riceve il traffico da 192.168.200.20 destinato a 192.168.100.10, con l'indirizzo MAC di destinazione impostato sul MAC virtuale HSRP (VMAC) condiviso all'interno del dominio vPC.
- Poiché HSRP funziona in modalità attivo-attivo da una prospettiva di piano dati sul vPC, N9K-C9364C-2 instrada il traffico dalla VLAN 200 alla VLAN 100 e lo inoltra attraverso vPC 10.

Si consideri uno scenario in cui SVI 200 viene chiuso sul N9K-C9364C-2, ma rimane attivo sul N9K-C9364C-1:

```
<#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#
```

A causa della differenza nello stato operativo delle SVI tra i peer vPC, viene rilevata un'incoerenza di tipo 2 all'interno del dominio vPC:

<#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#
```

A questo punto, il traffico tra le ore 192.168.200.20 e 192.168.100.10 non ha più esito positivo:

<#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#
```

Per tracciare il percorso del traffico, viene usato un ping colorato (un ping con una dimensione MTU specificata):

<#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#

In base ai contatori di interfaccia del N9K-C9364C-2, questo traffico viene ricevuto sul canale porta 20 e inoltrato al canale porta 100 (il collegamento peer vPC):

<#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#
```

Questo comportamento si verifica perché SVI 200 è spento sulla scheda N9K-C9364C-2, impedendo il routing locale del traffico sulla VLAN 200. In questo scenario, il traffico viene instradato attraverso il collegamento peer vPC alla scheda N9K-C9364C-1, in modo che il dispositivo esegua il routing tra VLAN.

Osservando i contatori di interfaccia sul N9K-C9364C-1, si conferma che i pacchetti raggiungono questo dispositivo tramite il collegamento peer vPC. Tuttavia, non sono stati osservati pacchetti in uscita sul canale porta 10 vPC, che si connette a 192.168.100.10.

<#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#
```

Anche se il traffico arriva alla N9K-C9364C-1 attraverso il collegamento peer vPC, non viene inoltrato al canale porta 10 vPC. Ciò è dovuto al fatto che il bit exit_vsl_drop per questo vPC è impostato su 1, il che accade quando lo stesso canale porta vPC è in funzione sullo switch peer (in questo caso 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:

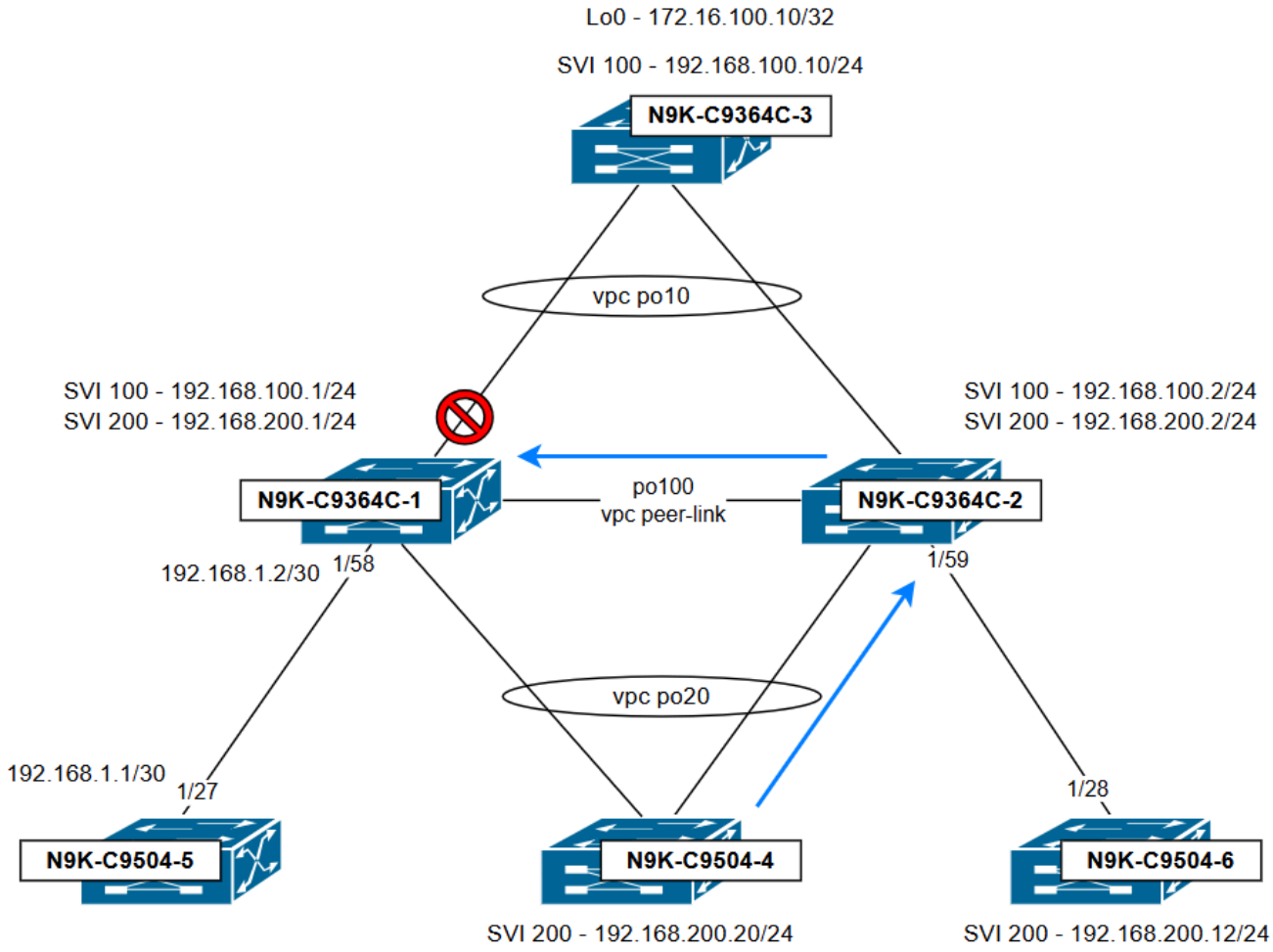
**vPC state: Up Old Compat Status: Pass**

vPC Peer Information:

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

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

Topologia che illustra il flusso del traffico e il punto in cui viene rilasciato:




Conclusione:

N9K-C9364C-1 riduce il traffico a causa della regola di prevenzione del loop vPC: Il traffico ricevuto sul collegamento peer vPC non può essere inoltrato su nessun canale della porta vPC attivo su entrambi gli switch."Per evitare questo problema, verificare che lo stato amministrativo delle SVI sia coerente su entrambi gli switch e che le loro configurazioni siano simmetriche.

b) Il traffico indirizzato dall'host orfano all'host vPC è interessato

Considerando lo stesso scenario in cui SVI 200 viene chiuso sul N9K-C9364C-2, ma rimane attivo sul N9K-C9364C-1. Il ping tra N9K-C9504-6 (VLAN 200) e N9K-C9364C-3 (VLAN 100) non ha esito positivo.

<#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#
```

Per tracciare il percorso del traffico, viene usato un ping colorato (un ping con una dimensione MTU specificata):

<#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
```

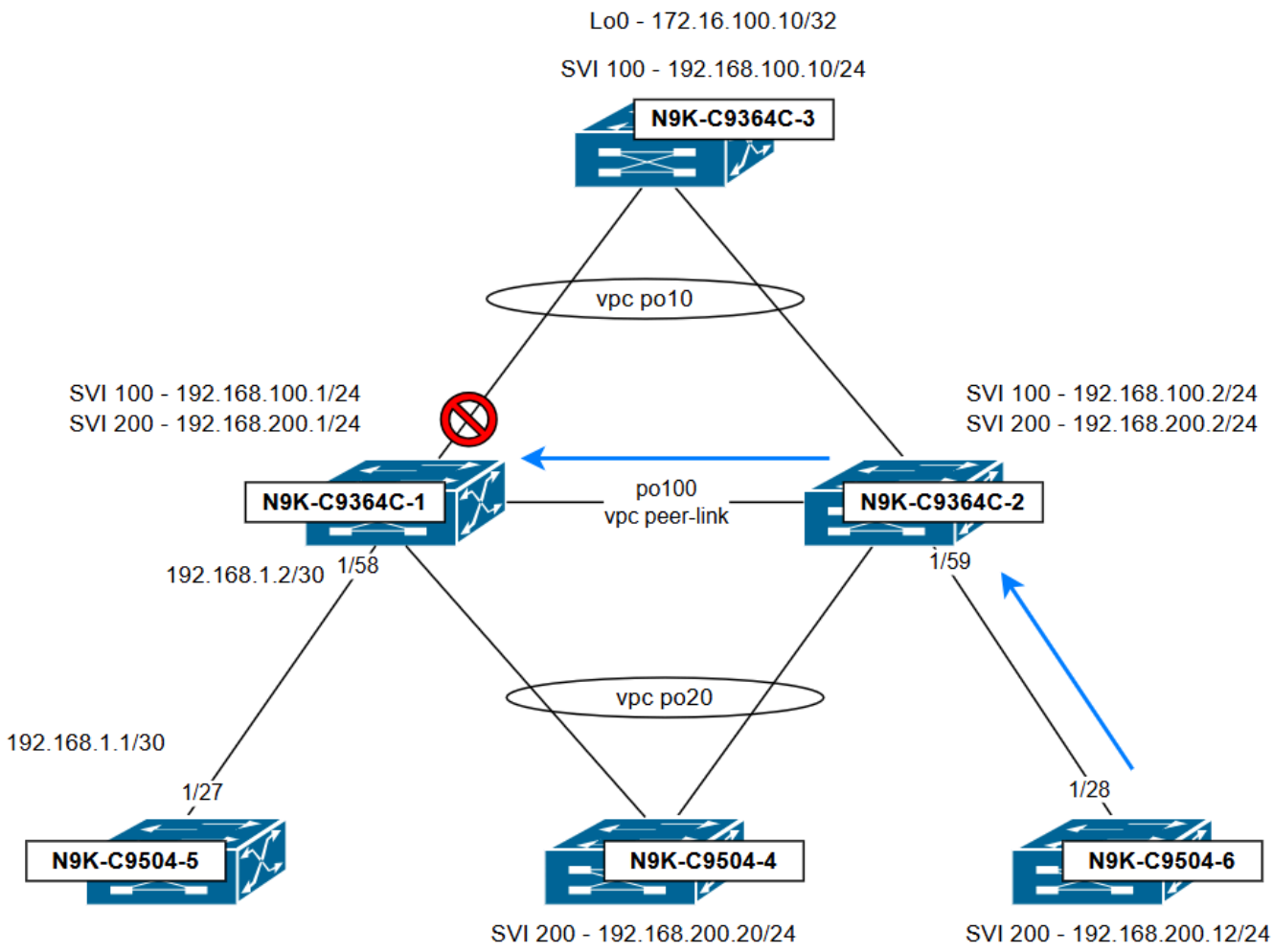
```
N9K-C9364C-1#
```

Anche se il traffico arriva alla N9K-C9364C-1 attraverso il collegamento peer vPC, non viene inoltrato al canale porta 10 vPC. Ciò è dovuto al fatto che il bit exit_vsl_drop per questo vPC è impostato su 1, il che accade quando lo stesso canale porta vPC è in funzione sullo switch peer (in questo caso 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#
```

Topologia che illustra il flusso del traffico e il punto in cui viene interrotto:




Conclusione:

Anche se il traffico proviene da un host orfano collegato all'N9K-C9364C-2, viene scartato dall'N9K-C9364C-1 a causa della regola vPC per evitare i loop: Il traffico ricevuto tramite il collegamento peer vPC non può essere inoltrato ad alcun canale della porta vPC attivo su entrambi gli switch. se la porta in entrata sullo switch peer è una porta vPC o una porta orfana è irrilevante; l'elemento importante è che il traffico entri attraverso il collegamento peer vPC ed è destinato a un vPC attivo su entrambi gli switch. Per evitare questo problema, verificare che lo stato amministrativo delle SVI sia coerente su entrambi gli switch e che le loro configurazioni siano simmetriche.

## Scenario 2: tutti i vPC e le SVI sono attivi - Next Hop Point per il peer vPC

In questo scenario, tutte le porte SVI e i canali vPC all'interno del dominio vPC sono attivi. Tuttavia, il N9K-C9504-5, collegato al N9K-C9364C-1 tramite un'interfaccia di layer 3, non è in grado di eseguire il ping tra Loopback 0 e N9K-C9364C-3.

Un traceroute da N9K-C9504-5 indica che il pacchetto raggiunge prima l'hop successivo immediato a 192.168.1.2, quindi procede verso 192.168.100.2, che è associato a N9K-C9364C-2.

```
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#
```

La verifica dell'hop successivo da N9K-C9364C-1 (l'hop iniziale per questo traffico) mostra che la destinazione è raggiungibile tramite 192.168.100.2, che corrisponde a SVI 100 su N9K-C9364C-2.

<#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#
```

Per tracciare il percorso del traffico, viene usato un ping colorato (un ping con una dimensione MTU specificata):

<#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#
```

Anche se il traffico arriva alla N9K-C9364C-2 attraverso il collegamento peer vPC, non viene inoltrato al canale porta 10 vPC. Ciò è dovuto al fatto che il bit exit_vsl_drop per questo vPC è impostato su 1, il che accade quando lo stesso canale porta vPC è in funzione sullo switch peer (in questo caso N9K-C9364C-1).

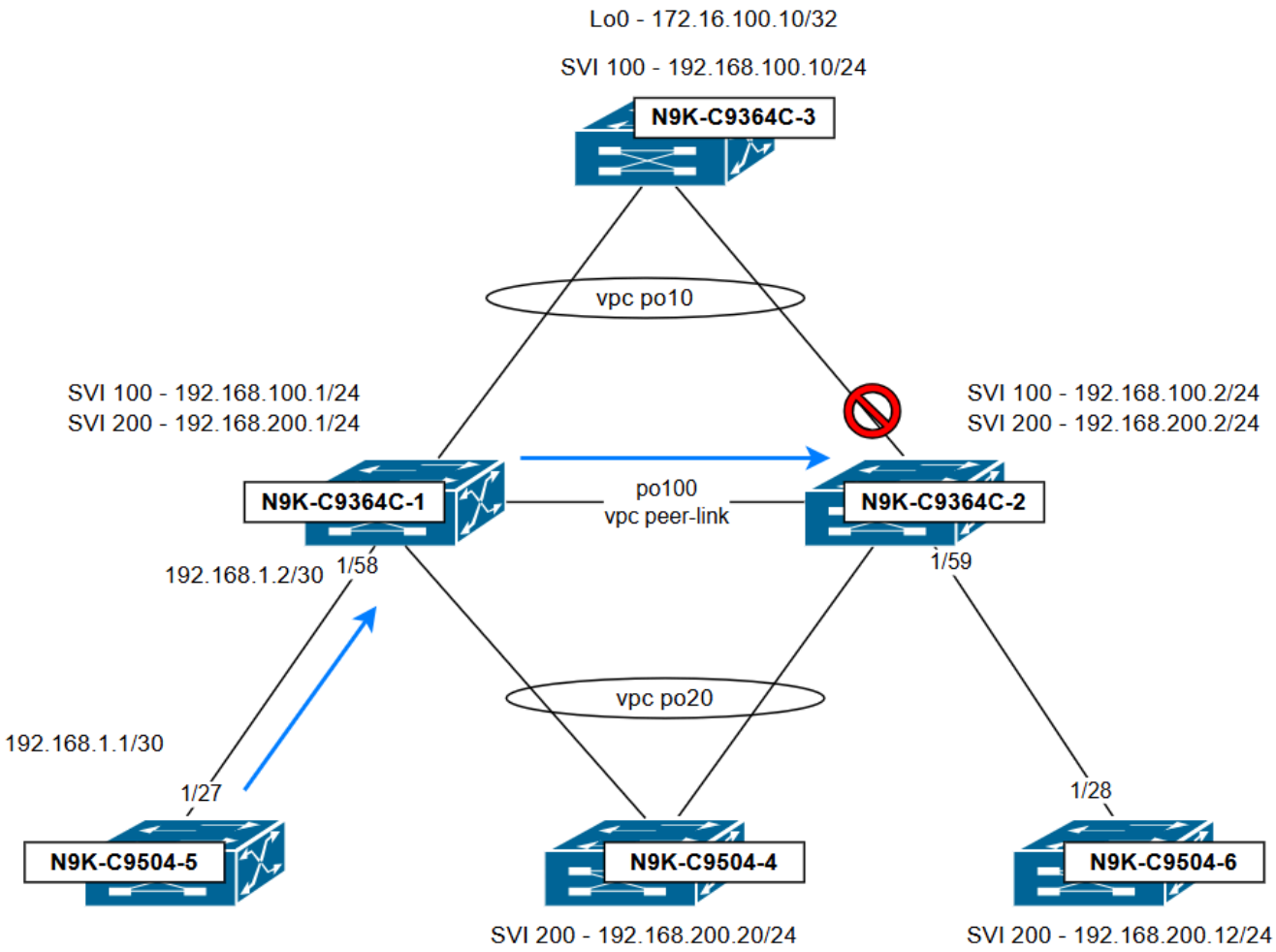
<#root>

```
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#
```

Topologia che illustra il flusso del traffico e il punto in cui viene interrotto:



Conclusione:

Il problema è dovuto al fatto che N9K-C9364C-1 utilizza N9K-C9364C-2 come hop successivo, inviando il traffico attraverso il collegamento peer vPC prima di tentare l'uscita da vPC 10. Il traffico viene scartato a causa della regola per evitare i loop nel vPC: Il traffico ricevuto tramite il collegamento peer vPC non può essere inoltrato ad alcun canale della porta vPC attivo su entrambi gli switch. Per evitare il problema, verificare che le route (dinamiche o statiche) con hop successivo tramite un canale della porta vPC siano configurate su entrambi gli switch peer vPC, in modo che il traffico non debba attraversare il collegamento peer vPC ed uscire da un vPC.

## Scenario 3: tutti i vPC e le SVI sono attivi - la funzione VPC Peer-Gateway è disattivata

In questo scenario tutti i canali porte SVI e vPC sono attivi sul dominio vPC; tuttavia, la funzione peer-gateway vPC è disattivata. A questo punto, N9K-C9504-4 (VLAN 200) non è in grado di eseguire il ping tra N9K-C9364C-3 (VLAN 100).

```
<#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#
```

La verifica dell'hop successivo da N9K-C9504-4 mostra che la destinazione è raggiungibile tramite 192.168.200.2, che corrisponde a SVI 200 su N9K-C9364C-2 e connessa tramite la porta vPC-canale 20.

```
<#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
```

Un ping colorato (un ping con una dimensione MTU specificata) viene usato per tracciare il percorso preso da questo traffico. Qui i contatori di interfaccia rivelano che N9K-C9364C-1 riceve il traffico da 192.168.200.20 a 192.168.100.10 sulla porta-canale 20 e lo invia al vPC peer-link (port-channel100)

<#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 riceve il traffico sul collegamento peer vPC (port-channel100), ma non lo inoltra al canale porta 10 vPC.

```
<#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#
```

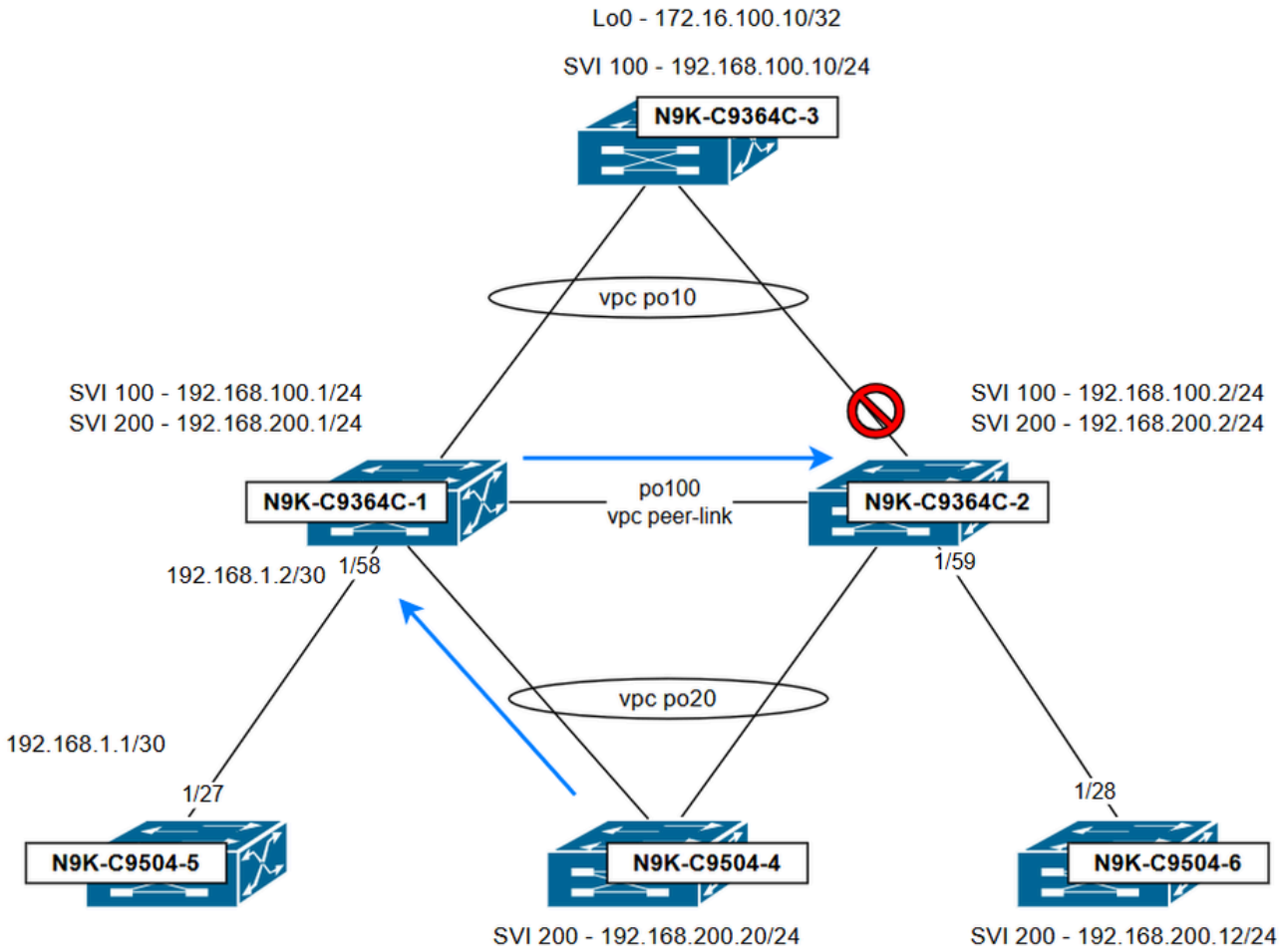
Anche se il traffico arriva alla N9K-C9364C-2 attraverso il collegamento peer vPC, non viene inoltrato al canale porta 10 vPC. Ciò è dovuto al fatto che il bit exit_vsl_drop per questo vPC è impostato su 1, il che accade quando lo stesso canale porta vPC è in funzione sullo switch peer (in questo caso N9K-C9364C-1).

Poiché il gateway peer è disabilitato, N9K-C9364C-1 può instradare solo i pacchetti indirizzati al proprio indirizzo MAC locale. Di conseguenza, i pacchetti destinati a a478.06de.7edb (MAC da N9K-C9364C-2) vengono inoltrati da N9K-C9364C-1 tramite il collegamento peer vPC.

```
<#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#
```

Topologia che illustra il flusso del traffico e il punto in cui viene interrotto:




Conclusione:

Se il gateway peer è abilitato, il traffico indirizzato destinato all'indirizzo MAC del peer vPC viene elaborato localmente programmando l'indirizzo MAC del peer come gateway. In questo modo si impedisce l'utilizzo del collegamento peer vPC nel percorso del traffico ed evita le cadute causate dalla regola di prevenzione del loop vPC. Per evitare tali problemi, verificare che la funzionalità gateway peer vPC sia abilitata nel dominio vPC.

## Panoramica della soluzione

- Configurazione SVI coerente sulle VLAN vPC.

Le configurazioni SVI (Asymmetric Switched Virtual Interface) tra switch peer vPC possono causare problemi critici di inoltro del traffico, tra cui la sospensione delle attività. Una pratica comune, ma non supportata, che contribuisce a questa condizione è il test del failover tra peer vPC chiudendo le SVI da un lato. Questo metodo crea uno stato SVI asimmetrico non supportato dall'architettura Nexus vPC, con conseguente blocco del traffico e errori di inoltro. Verificare che la configurazione SVI sia sempre coerente su tutte le VLAN vPC per cui è necessario il routing.

- Abilitare il gateway peer nel dominio vPC.

La funzionalità peer-gateway rappresenta un miglioramento fondamentale nelle implementazioni di Cisco Nexus vPC. Se abilitato sul dominio vPC, consente a ogni switch peer vPC di accettare ed elaborare i pacchetti destinati all'indirizzo MAC virtuale del peer vPC. Ciò significa che entrambi i peer vPC possono rispondere al traffico associato al gateway, a prescindere dallo switch che ha ricevuto originariamente il pacchetto.  Se non è abilitato il gateway peer, alcuni tipi di traffico, ad esempio i pacchetti inviati all'indirizzo MAC del gateway predefinito, possono essere scartati se arrivano su un peer e se in caso contrario devono attraversare il collegamento peer e uscire da una porta membro del vPC. Verificare che il gateway peer vPC sia configurato nel dominio vPC.

## Informazioni correlate

Miglioramenti apportati al vPC (Virtual Port Channel)

Best practice per i canali porte virtuali (vPC) su Nexus

Funzione Peer Gateway su Nexus 7000

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).