Comprensión de Nexus VPC Loop Avoidance

Contenido

Introducción

Este documento describe situaciones en las que la prevención de bucles vPC puede afectar al reenvío de tráfico en diseños de red de capa 3 basados en Nexus.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- CLI del sistema operativo Nexus
- Conceptos de vPC

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

En los entornos de Data Center actuales, la tecnología Cisco Nexus Virtual Port Channel (vPC) es esencial para habilitar la redundancia y el equilibrio de carga. Al permitir que las conexiones a dos switches Nexus independientes funcionen como un único canal de puerto lógico, vPC simplifica la arquitectura de red y mejora la fiabilidad de los dispositivos de flujo descendente. Sin embargo, algunos detalles de la configuración pueden introducir complejidades operativas.

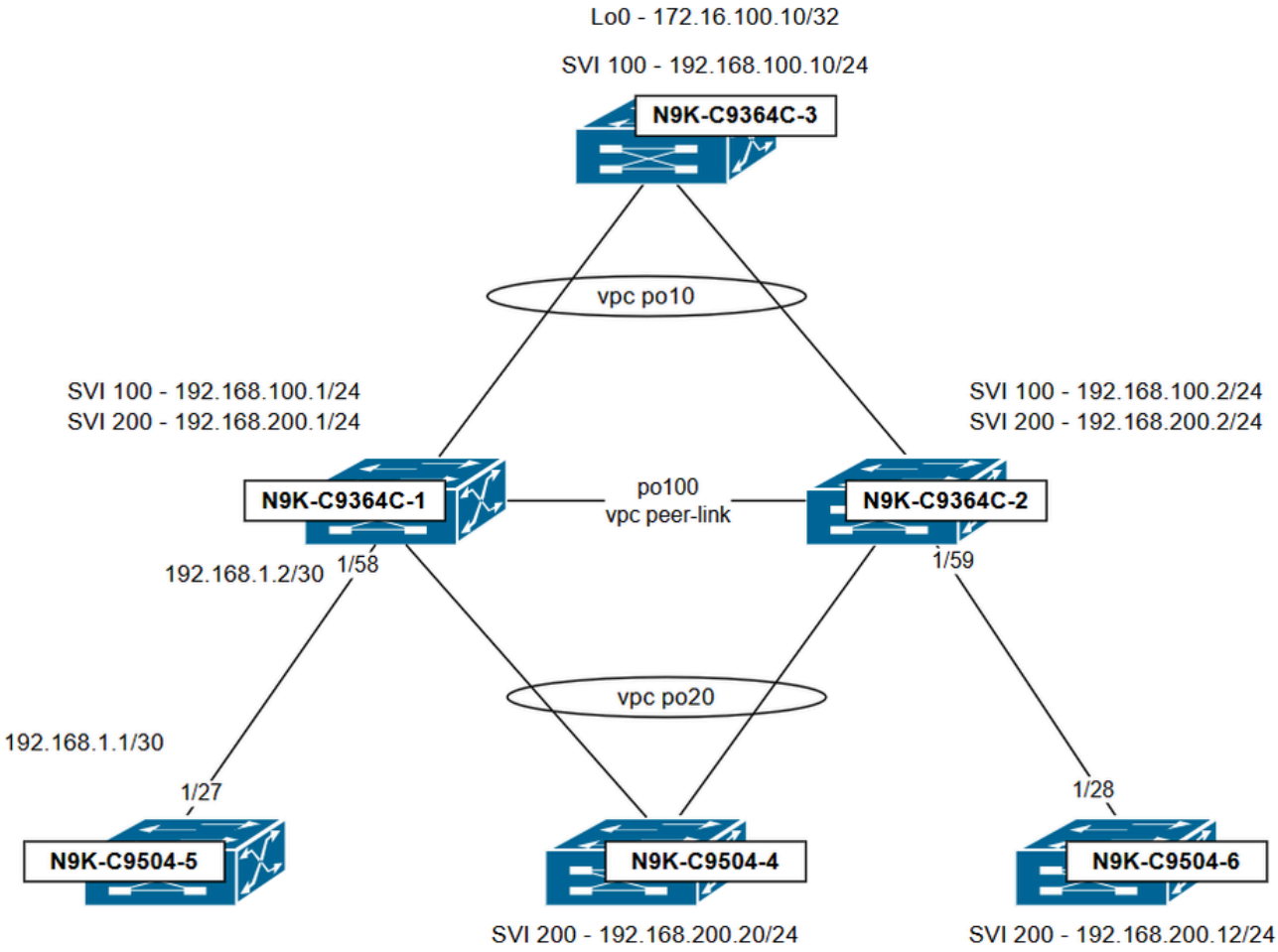
Este documento explora escenarios donde la prevención de loops vPC se vuelve significativa y examina su impacto en el reenvío de tráfico. Un conocimiento claro de este mecanismo es fundamental para los ingenieros de redes que desean diseñar y mantener una conectividad de capa 3 sólida y eficiente en una infraestructura basada en Nexus, lo que ayuda a evitar las interrupciones del tráfico y a mantener un rendimiento óptimo de la red.

Problema

En un entorno Cisco Nexus con vPC, los operadores de red pueden observar el comportamiento inesperado de reenvío de tráfico provocado por la regla de prevención de bucles de vPC. Cuando el tráfico viaja de un par vPC a otro a través del enlace de par vPC, no puede salir a través de ningún canal de puerto vPC que esté activo en ambos switches. Como resultado, los dispositivos que dependen de esta ruta para la conectividad pueden experimentar paquetes perdidos o pérdida de conectividad, incluso si todos los enlaces físicos parecen estar activos.

Comprender y dar cuenta de la regla de prevención de bucles de vPC es esencial para diseñar y solucionar problemas de topologías de red resistentes, ya que pasar por alto este comportamiento puede provocar interrupciones de servicio inesperadas y dificultar el diagnóstico de problemas de red.

Diagrama de la red



En esta topología, el dominio vPC lo crean N9K-C9364C-1 y N9K-C9364C-2. Ambos switches se configuran con VLAN 100 y 200 como VLAN vPC y se configuran SVI para cada VLAN. El dominio vPC es responsable del routing entre VLAN entre estas VLAN. A menos que se especifique lo contrario, la IP virtual (VIP) de HSRP compartida entre los switches de par vPC se utiliza como salto siguiente para la ruta predeterminada por parte de los otros switches de la topología.

- Configuración de SVI N9K-C9364C-1

```
interface Vlan100
no shutdown
no ip redirects
ip address 192.168.100.1/24
no ipv6 redirects
HSRP 100
ip 192.168.100.254

interface Vlan200
no shutdown
no ip redirects
ip address 192.168.200.1/24
no ipv6 redirects
```

HSRP 200
ip 192.168.200.254

- Configuración de SVI N9K-C9364C-2

interface Vlan100
no shutdown
no ip redirects
ip address 192.168.100.2/24
no ipv6 redirects
HSRP 100
ip 192.168.100.254

interface Vlan200
no ip redirects
ip address 192.168.200.2/24
no ipv6 redirects
HSRP 200
ip 192.168.200.254

Escenarios

Escenario 1: SVI para VLAN vPC se apaga administrativamente en el par vPC

a) El tráfico enrutado de vPC a vPC se ve afectado

En un escenario de trabajo, N9K-C9504-4 (VLAN 200) puede hacer ping correctamente a N9K-C9364C-3 (VLAN 100). Traceroute indica que la ruta de conexión pasa a través de 192.168.200.2, que está asignado 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

En este punto, el flujo de tráfico funciona de la siguiente manera:

- N9K-C9364C-2 recibe tráfico de 192.168.200.20 destinado a 192.168.100.10, con la dirección MAC de destino establecida en la dirección MAC virtual (VMAC) HSRP compartida dentro del dominio vPC.
- Dado que HSRP funciona en modo Activo-Activo desde una perspectiva de plano de datos en el vPC, N9K-C9364C-2 enruta el tráfico de VLAN 200 a VLAN 100 y lo reenvía a través de vPC 10.

Considere una situación en la que SVI 200 se apaga en N9K-C9364C-2, pero permanece activo en 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#
```

Debido a la diferencia en el estado operativo de las SVI entre los pares vPC, se detecta una incoherencia de tipo 2 dentro 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#
```

En esta etapa, el tráfico de 192.168.200.20 a 192.168.100.10 ya no es exitoso:

<#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#
```

Un ping coloreado (un ping con un tamaño de MTU especificado) se utiliza para rastrear la trayectoria tomada por este tráfico:

<#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#
```

Según los contadores de interfaz en N9K-C9364C-2, este tráfico se recibe en el canal de puerto 20 y se reenvía al canal de puerto 100 (el enlace de par 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#
```

Este comportamiento ocurre porque SVI 200 se apaga en N9K-C9364C-2, lo que evita el ruteo local del tráfico para VLAN 200. En este escenario, el tráfico se puentea a través del link de par vPC al N9K-C9364C-1, de modo que el dispositivo realice el ruteo entre VLAN.

Si observamos los contadores de interfaz en N9K-C9364C-1, se confirma que los paquetes llegan a este dispositivo a través del enlace de par vPC; sin embargo, no se han observado paquetes salientes en el canal de puerto 10 vPC, que se conecta 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#
```

Aunque el tráfico llega a N9K-C9364C-1 a través del enlace de par vPC, no se reenvía al canal de puerto 10 vPC. Esto se debe a que el bit egress_vsl_drop está configurado en 1 para este vPC, lo que sucede cuando el mismo canal de puerto vPC está operativo en el switch de par (en este 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:
```

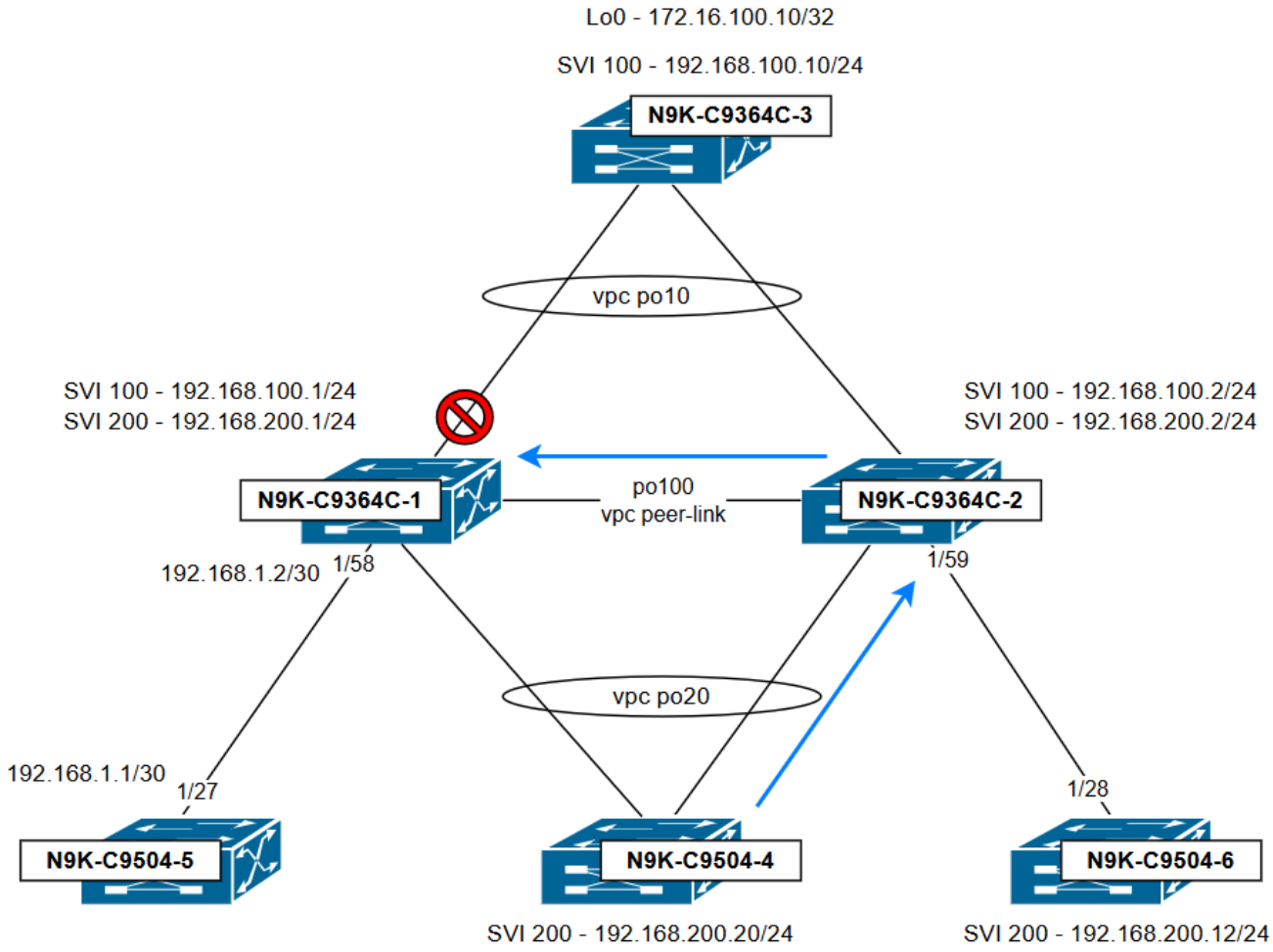
vPC state: Up Old Compat Status: Pass

```
vPC Peer Information:
```

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

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

Topología que ilustra el flujo de tráfico y el punto en el que se descarta:



Conclusión:

N9K-C9364C-1 descarta el tráfico debido a la regla de prevención de bucles de vPC: El tráfico recibido a través del enlace de par vPC no se puede reenviar a ningún canal de puerto vPC que esté activo en ambos switches."Para evitar este problema, asegúrese de que el estado administrativo de las SVI sea coherente en ambos switches y de que sus configuraciones sean simétricas.

b) El tráfico enrutado de huérfano a host vPC se ve afectado

Teniendo en cuenta el mismo escenario en el que SVI 200 se cierra en N9K-C9364C-2, pero permanece activo en N9K-C9364C-1. Un ping de N9K-C9504-6 (VLAN 200) a N9K-C9364C-3 (VLAN 100) no es satisfactorio.

<#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#
```

Un ping coloreado (un ping con un tamaño de MTU especificado) se utiliza para rastrear la trayectoria tomada por este tráfico:

<#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)
```

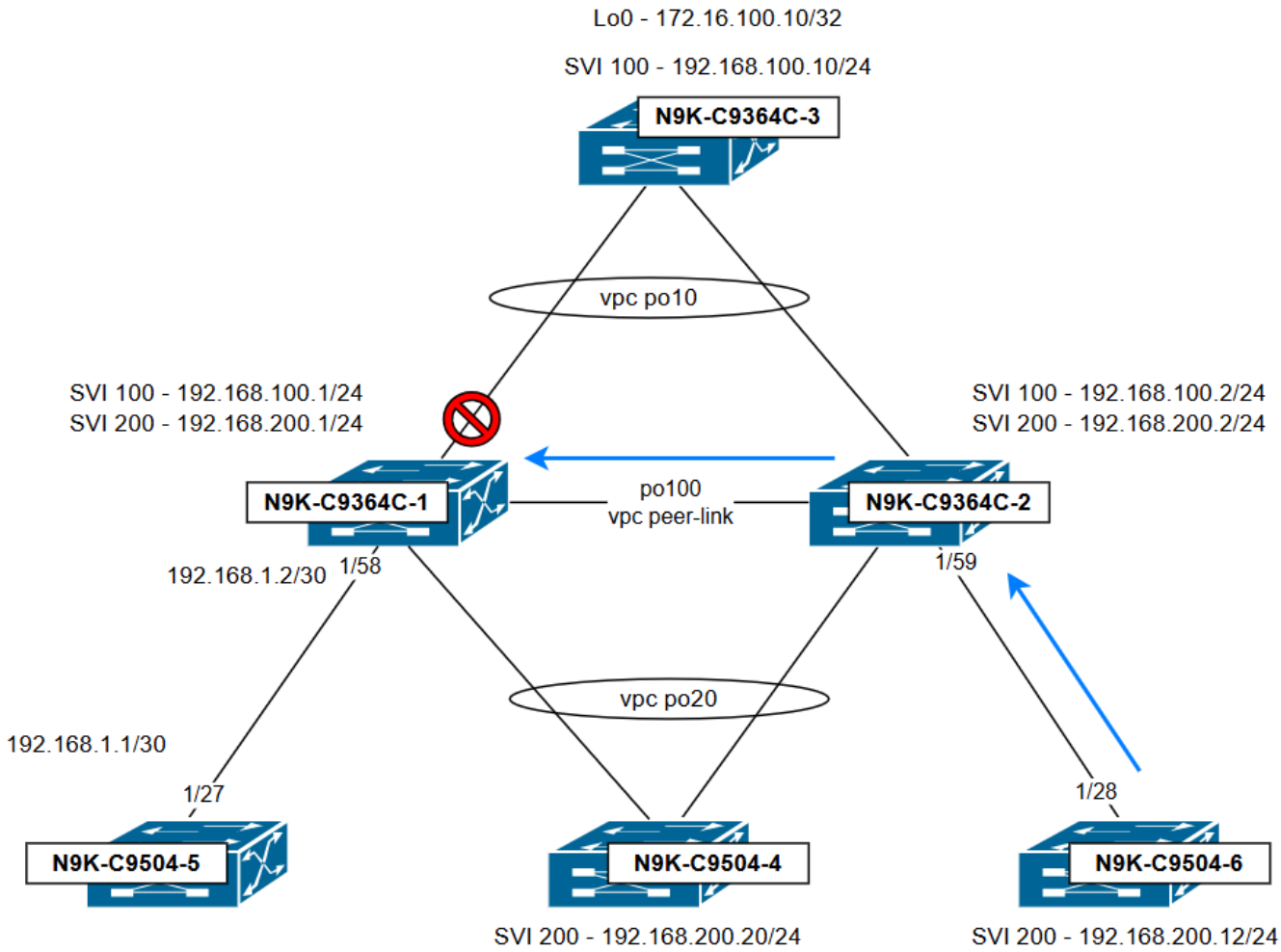
```
60. Tx Packets from 1024 to 1518 bytes: = 0
N9K-C9364C-1#
```

Aunque el tráfico llega a N9K-C9364C-1 a través del enlace de par vPC, no se reenvía al canal de puerto 10 vPC. Esto se debe a que el bit egress_vsl_drop está configurado en 1 para este vPC, lo que sucede cuando el mismo canal de puerto vPC está operativo en el switch de par (en este 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#
```

Topología que ilustra el flujo de tráfico y el punto en el que se descarta:



Conclusión:

Aunque el tráfico se origina en un host huérfano conectado a N9K-C9364C-2, N9K-C9364C-1 lo descarta debido a la regla de prevención de bucles de vPC: El tráfico recibido a través del enlace de par vPC no se puede reenviar fuera de ningún canal de puerto vPC que esté activo en ambos switches. Si el puerto de ingreso en el switch par es un vPC o un puerto huérfano es irrelevante; lo que importa es que el tráfico entra a través del link de par vPC y está destinado a un vPC que está activo en ambos switches. Para evitar este problema, asegúrese de que el estado administrativo de las SVI sea consistente en ambos switches y que sus configuraciones sean simétricas.

Situación 2: Todos los vPC y SVI están activos: puntos de salto siguientes al par vPC

En esta situación, todas las SVI y los canales de puerto vPC del dominio vPC están activos. Sin embargo, N9K-C9504-5, que está conectado a N9K-C9364C-1 a través de una interfaz de capa 3, no puede hacer ping al bucle invertido 0 en N9K-C9364C-3.

Un traceroute de N9K-C9504-5 indica que el paquete alcanza primero su próximo salto inmediato en 192.168.1.2 y luego continúa a 192.168.100.2, que está asociado con N9K-C9364C-2.

```
<#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#
```

La verificación de siguiente salto de N9K-C9364C-1 (el salto inicial para este tráfico) muestra que el destino es alcanzable a través de 192.168.100.2, que corresponde a SVI 100 en 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#
```

Un ping coloreado (un ping con un tamaño de MTU especificado) se utiliza para rastrear la trayectoria tomada por este tráfico:

```
<#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#
```

Aunque el tráfico llega al N9K-C9364C-2 a través del enlace de par vPC, no se reenvía al canal de puerto 10 vPC. Esto se debe a que el bit egress_vsl_drop está configurado en 1 para este vPC, lo que sucede cuando el mismo canal de puerto vPC está operativo en el switch de par (en este caso, N9K-C9364C-1).

<#root>

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

show system internal eltm info interface Po10 | i i vsl

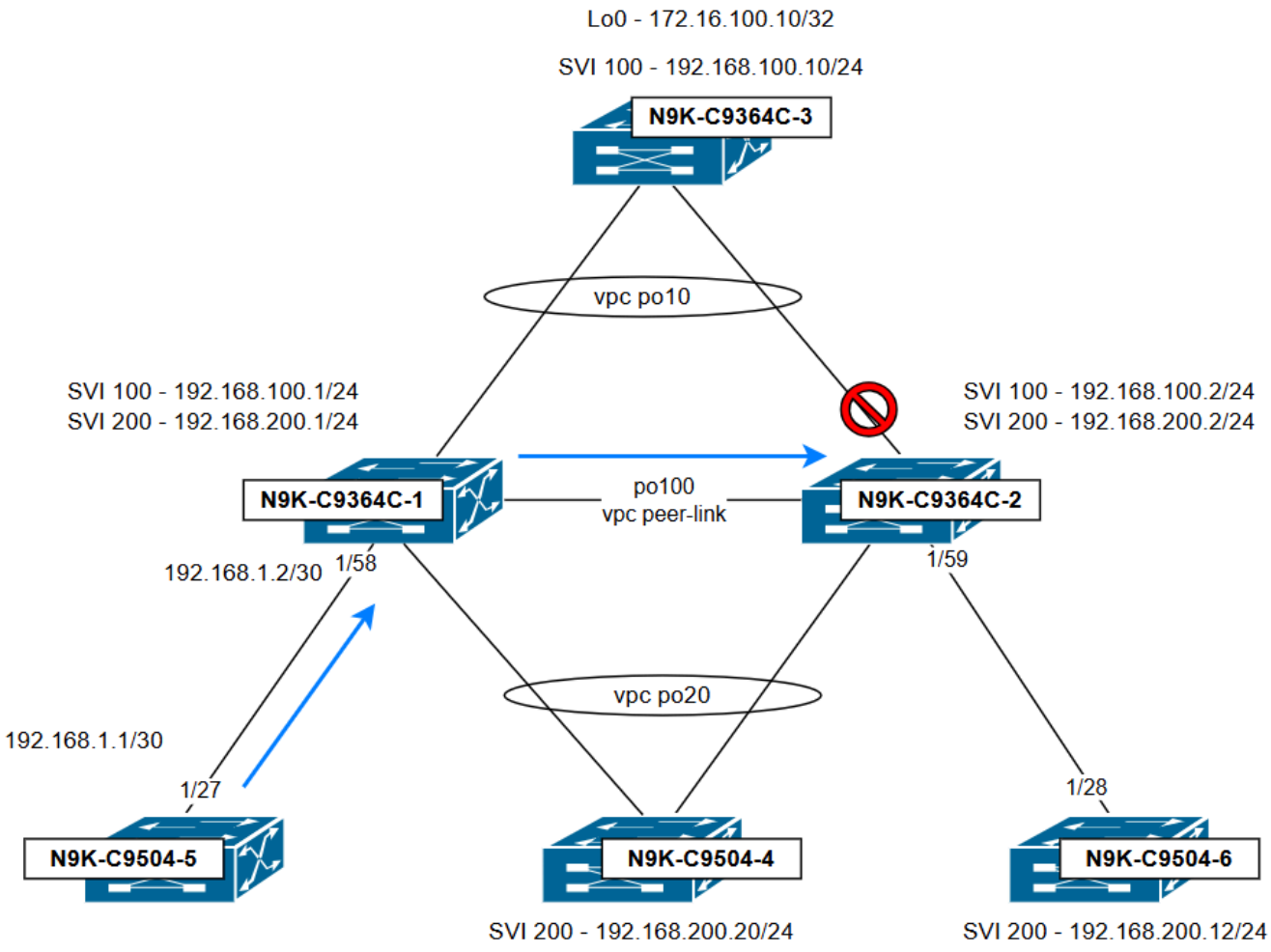
egress_vsl_drop = 1

```
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#
```

Topología que ilustra el flujo de tráfico y el punto en el que se descarta:



Conclusión:

El problema se observa porque N9K-C9364C-1 utiliza N9K-C9364C-2 como salto siguiente, enviando tráfico a través del enlace de par vPC antes de que intente salir a través de vPC 10. El tráfico se descarta debido a la regla de prevención de bucles vPC: El tráfico recibido a través del enlace de par vPC no se puede reenviar a ningún canal de puerto vPC que esté activo en ambos switches. Para evitar este problema, asegúrese de que las rutas (dinámicas o estáticas) con un salto siguiente a través de un canal de puerto vPC estén configuradas en ambos switches de par vPC, de modo que el tráfico no tenga que cruzar el enlace de par vPC y salir a través de un vPC.

Situación 3: Todos los vPC y SVI están activos; la función de gateway de par VPC está desactivada

En esta situación, todas las SVI y los canales de puerto vPC están activos en el dominio vPC; sin embargo, la función de gateway de par vPC está desactivada. En este momento, N9K-C9504-4 (VLAN 200) no puede hacer ping a 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 verificación de salto siguiente de N9K-C9504-4 muestra que el destino es alcanzable a través de 192.168.200.2, que corresponde a SVI 200 en N9K-C9364C-2 y está conectado a través del canal de puerto vPC 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 coloreado (un ping con un tamaño de MTU especificado) se utiliza para rastrear la trayectoria tomada por este tráfico. Aquí los contadores de interfaz revelan que N9K-C9364C-1 recibe el tráfico de 192.168.200.20 a 192.168.100.10 a través del canal de puerto 20 y lo envía al link de par vPC (canal de puerto 100)

<#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 recibe el tráfico a través del enlace de par vPC (canal de puerto100), pero no lo reenvía al canal de puerto 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#
```

Aunque el tráfico llega a N9K-C9364C-2 a través del enlace de par vPC, no se reenvía al canal de puerto 10 vPC. Esto se debe a que el bit egress_vsl_drop está configurado en 1 para este vPC, lo que sucede cuando el mismo canal de puerto vPC está operativo en el switch de par (en este caso, N9K-C9364C-1).

Dado que la gateway de peer está inhabilitada, N9K-C9364C-1 solo puede rutear paquetes dirigidos a su propia dirección MAC local. Como resultado, los paquetes destinados a a a478.06de.7edb (MAC desde N9K-C9364C-2) son reenviados por N9K-C9364C-1 a través del enlace de par vPC.

<#root>

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

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

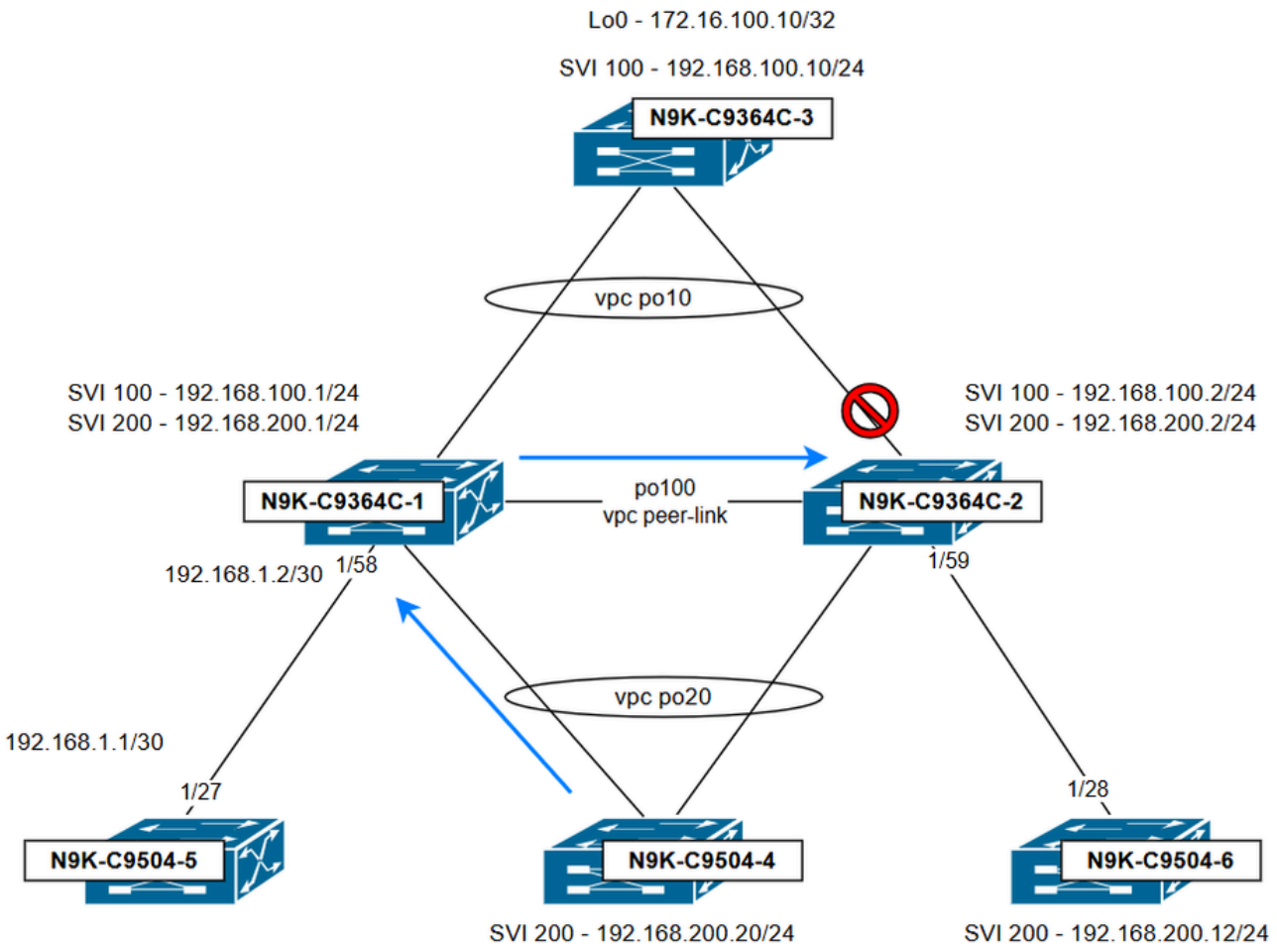
```
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan
VLAN MAC Address Type age Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
* 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#
```

Topología que ilustra el flujo de tráfico y el punto en el que se descarta:



Conclusión:

Si se activa la puerta de enlace de par, el tráfico enrutado destinado a la dirección MAC del par vPC se procesa localmente mediante la programación de la puerta de enlace MAC de par. Esto evita que el enlace de par vPC se utilice en la ruta de tráfico y evita las caídas causadas por la regla de evitación de bucles vPC. Para evitar estos problemas, asegúrese de que la función de gateway de par vPC está activada en el dominio vPC.

Descripción general de soluciones

- Mantenga la configuración de SVI uniforme en las VLAN vPC.

Las configuraciones asimétricas de la interfaz virtual conmutada (SVI) entre switches de par vPC pueden provocar problemas críticos de reenvío de tráfico, incluido el bloqueo del tráfico. Una práctica común pero no admitida que contribuye a esta condición es probar la conmutación por error entre los pares vPC apagando las SVI en un lado. Este método crea un estado de SVI asimétrico que la arquitectura vPC de Nexus no admite, lo que da como resultado fallos de reenvío y agujeros negros del tráfico. Asegúrese de que la configuración de SVI sea siempre uniforme en todas las VLAN vPC para las que se necesita routing.

- Active la puerta de enlace de par en el dominio vPC.

La función de gateway de par es una mejora fundamental en las implementaciones de vPC de Cisco Nexus. Cuando está habilitado en el dominio vPC, permite que cada switch de par vPC acepte y procese paquetes destinados a la dirección MAC virtual del par vPC. Esto significa que cualquiera de los pares vPC puede responder al tráfico enlazado a la gateway, independientemente del switch que haya recibido originalmente el paquete. Sin la puerta de enlace de par habilitada, ciertos tipos de tráfico, como los paquetes enviados a la dirección MAC de la puerta de enlace predeterminada, se pueden descartar si llegan a un par y, de lo contrario, tendrían que atravesar el enlace de par y salir de un puerto miembro de vPC. Asegúrese de que el gateway de par vPC está configurado en el dominio vPC.

Información Relacionada

Comprender las mejoras del canal de puerto virtual (vPC)

Prácticas recomendadas para Virtual Port Channels (vPC) en Nexus

Función Peer Gateway en Nexus 7000

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).