Comprender las mejoras del canal de puerto virtual (vPC)

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Hardware aplicable
Switch de par vPC
Overview
Puentes no vPC conectados de forma redundante
Puentes conectados a vPC
Advertencias
Los valores de prioridad de árbol de expansión deben coincidir entre pares vPC
El switch de par vPC afecta a las VLAN no vPC
Configuración
Impacto
Puentes no vPC conectados de forma redundante
Puentes conectados a vPC
Ejemplos de situaciones de falla
Puentes no vPC conectados de forma redundante que reinician la máquina de estados finitos
Puentes conectados a vPC que vacían direcciones MAC aprendidas dinámicamente
Gateway de par vPC
Overview
Advertencias
Intermitencia de adyacencias de protocolo de routing de unidifusión sobre vPC o VLAN vPC
Desactivación automática de redireccionamientos ICMP e ICMPv6
Configuración
Impacto
Intermitencia de adyacencias de protocolo de routing de unidifusión sobre vPC o VLAN vPC
Desactivación automática de redireccionamientos ICMP e ICMPv6
Ejemplos de situaciones de falla
Hosts conectados a vPC con comportamiento de reenvío no estándar
Routing/Capa 3 a través de vPC (router par de Capa3)
Overview
Advertencias
Syslogs ocasionales VPC-2-L3_VPC_UNEQUAL_WEIGHT
Tráfico del plano de datos con TTL de 1 software reenviado debido al ID de bug de Cisco CSCvs82183 y al ID de bug de Cisco CSCvw16965
Configuración
Impacto

Ejemplos de situaciones de falla
Adyacencias de protocolo de routing de unidifusión a través de un vPC sin gateway de par vPC
Adyacencias de protocolo de routing de unidifusión a través de un vPC con gateway de par vPC
Adyacencias de protocolo de routing de unidifusión a través de una VLAN vPC sin gateway de par vPC
Adyacencias de protocolo de routing de unidifusión a través de una VLAN vPC con gateway de par vPC
Adyacencias de protocolo de routing de unidifusión a través de un vPC adosado con gateway de par vPC
Adyacencias OSPF a través de vPC con gateway de par vPC donde el prefijo está presente en la LSDB de OSPF pero no en la tabla de routing
Información Relacionada

Introducción

Este documento describe las mejoras comunes del canal de puerto virtual (vPC) configuradas en los switches Cisco Nexus en un dominio vPC.

Prerequisites

Requirements

Cisco recomienda que comprenda la información básica sobre el caso de uso, la configuración y la implementación del canal de puertos virtual (vPC). Para obtener más información sobre esta función, consulte uno de estos documentos aplicables:

- Guía de configuración de las interfaces NX-OS de Cisco Nexus 9000 Series, versión 10.1(x)
- Guía de configuración de las interfaces NX-OS de Cisco Nexus 9000 Series, versión 9.3(x)
- Guía de configuración de las interfaces NX-OS de Cisco Nexus 9000 Series, versión 9.2(x)
- Guía de configuración de las interfaces NX-OS de Cisco Nexus 9000 Series, versión 7.x
- Guía de configuración de las interfaces NX-OS de Cisco Nexus 7000 Series, versión 8.x
- Guía de configuración de las interfaces NX-OS de Cisco Nexus 7000 Series, versión 7.x
- Guía de diseño y configuración: Prácticas recomendadas para Virtual Port Channels (vPC) en switches Nexus de Cisco serie 7000

Componentes Utilizados

La información de este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Desde el inicio de Cisco NX-OS en switches de centro de datos Cisco Nexus, la función del canal de puertos virtual (vPC) ha recibido numerosas mejoras que favorecen la fiabilidad de los dispositivos conectados a vPC durante situaciones de falla y optimizan el comportamiento de reenvío de ambos switches de par vPC. Comprender el propósito de cada mejora, el cambio de

comportamiento que introduce la mejora y las situaciones de falla que soluciona la mejora puede ayudarle a comprender por qué y cuándo debe configurarse una mejora dentro de un dominio vPC para ayudar a satisfacer mejor las necesidades y los requisitos empresariales.

Hardware aplicable

El procedimiento descrito en este documento se aplica a todos los switches de centro de datos Cisco Nexus con capacidad para vPC.

Switch de par vPC

Esta sección describe la mejora del switch de par vPC, que se activa con el comando de configuración de dominio vPC **peer-switch**.

Overview

En muchos entornos, un par de switches Nexus en un dominio vPC son switches de agregación o de núcleo que actúan como el límite entre dominios ethernet conmutados de Capa 2 y dominios enrutados de Capa 3. Ambos switches se configuran con varias VLAN y son responsables del routing del tráfico horizontal entre VLAN y tráfico vertical. En estos entornos, los switches Nexus también actúan normalmente como puente de ruta desde la perspectiva del protocolo de árbol de expansión.

Normalmente, un par vPC se configura como el puente de ruta del árbol de expansión estableciendo su prioridad de árbol de expansión en un valor bajo, como 0. El otro par vPC se configura con una prioridad de árbol de expansión ligeramente más alta, como 4096, que le permite asumir la función de puente de ruta dentro del árbol de expansión si el par vPC que actúa como puente de ruta falla. Con esta configuración, el par vPC que actúa como puente de ruta origina unidades de datos de protocolo puente (BPDU) de árbol de expansión con un ID de puente que contiene su dirección MAC del sistema.

Sin embargo, si el par vPC que actúa como puente raíz falla y hace que el otro par vPC tome el control como puente raíz del árbol de expansión, el otro par vPC origina BPDU del árbol de expansión con un ID de puente que contiene su dirección MAC del sistema, que es diferente de la dirección MAC del sistema del puente raíz original. Dependiendo de cómo estén conectados los puentes descendentes, el impacto de este cambio varía y se describe en las subsecciones siguientes.

Puentes no vPC conectados de forma redundante

Los puentes no conectados a vPC que están conectados a ambos pares vPC con links redundantes (como que un link está en estado de bloqueo desde una perspectiva de protocolo de árbol de expansión) que detectan el cambio en la BPDU (y, por lo tanto, el cambio en el puente raíz) observan un cambio en el puerto raíz. Otras interfaces de reenvío designadas pasan inmediatamente a un estado de bloqueo y, a continuación, atraviesan la máquina de estado finito del protocolo de árbol de extensión (bloqueo, aprendizaje y reenvío) con pausas entre ellas equivalentes al temporizador de retraso de reenvío del protocolo de árbol de extensión configurado (15 segundos de forma predeterminada).

El cambio en el puerto raíz y la posterior inversión de la máquina de estado finito del protocolo de

árbol de expansión pueden causar una cantidad significativa de interrupciones dentro de la red. La mejora del switch de par vPC se introdujo principalmente para evitar la interrupción de la red causada por este problema si uno de los pares vPC se desconectaba. Con la mejora del switch de par vPC, el puente no conectado a vPC todavía tiene un único enlace redundante que está en estado de bloqueo, pero inmediatamente pasa esa interfaz a un estado de reenvío si el puerto raíz existente deja de funcionar debido a una falla de link. El mismo proceso ocurre cuando el par vPC sin conexión vuelve a estar en línea: la interfaz con el menor costo para el puente raíz asume la función de puerto raíz y el link redundante pasa inmediatamente a un estado de bloqueo. El único impacto del plano de datos que se observa es la pérdida inevitable de paquetes en vuelo que atravesaban el par vPC cuando se desconectaban.

Puentes conectados a vPC

Los puentes conectados a vPC en el dominio de árbol de expansión detectan el cambio en la BPDU (y, por lo tanto, el cambio en el puente raíz) y purgan las direcciones MAC aprendidas dinámicamente de sus tablas de direcciones MAC locales. Este comportamiento es ineficaz e innecesario en topologías con dispositivos conectados a vPC que no dependen del protocolo de árbol de extensión para una topología sin bucles. Los vPC se ven como una única interfaz lógica desde la perspectiva del protocolo de árbol de extensión, al igual que los canales de puerto normales, por lo que la pérdida de un par vPC es similar a la pérdida de un único enlace dentro de un miembro de canal de puerto. En cualquier situación, el árbol de expansión no cambia, por lo que es innecesario el vaciado de direcciones MAC aprendidas dinámicamente de los puentes en el dominio del árbol de expansión (cuyo propósito es permitir que el comportamiento de inundación y aprendizaje de ethernet vuelva a aprender las direcciones MAC en las interfaces de reenvío nuevo del árbol de expansión).

Además, el vaciado de direcciones MAC aprendidas dinámicamente podría ser potencialmente disruptivo. Considere una situación donde dos hosts tienen un flujo basado en UDP mayormente unidireccional (como un cliente TFTP que envía datos a un servidor TFTP). En este flujo, los datos fluyen principalmente del cliente TFTP al servidor TFTP; rara vez el servidor TFTP envía un paquete de vuelta al cliente TFTP. Como resultado, después de un vaciado de direcciones MAC aprendidas dinámicamente en el dominio de árbol de expansión, la MAC del servidor TFTP no se aprende durante algún tiempo. Esto significa que los datos del cliente TFTP enviados hacia el servidor TFTP se inundan a través de la VLAN, ya que el tráfico es tráfico unicast desconocido. Esto puede hacer que los flujos de datos de gran tamaño viajen a lugares no deseados dentro de la red y puede causar problemas de rendimiento si fluyen a través de secciones de la red con exceso de suscriptores.

La mejora del switch de par vPC se introdujo para evitar que este comportamiento ineficiente e innecesario se produjera en el caso de que se recargue o apague el par vPC que actúa como puente de ruta del árbol de expansión para una o más VLAN.

Para activar la mejora del switch de par vPC, ambos pares vPC deben tener la misma configuración del protocolo de árbol de expansión (incluidos los valores de prioridad del árbol de expansión para todas las VLAN vPC) y ser el puente de ruta para al menos una VLAN vPC. Una vez que se cumplen estos requisitos previos, el comando de configuración de dominio vPC **peer-switch** debe configurarse para activar la mejora del switch de par vPC.

> **Nota**: No se recomienda habilitar la mejora del switch de par vPC en un dominio vPC donde ninguno de los switches de par vPC es el puente raíz del protocolo de árbol de extensión para una o más VLAN vPC. Solo debe activar la mejora del switch de par vPC si uno (o ambos) de los switches de par vPC son el puente de ruta del protocolo de árbol de

expansión para una o más VLAN vPC.

Una vez habilitada la mejora del switch de par vPC, ambos pares vPC comienzan a originar BPDU de árbol de extensión idénticas con una ID de puente que contiene la dirección MAC del sistema vPC compartida por ambos pares vPC. Si se vuelve a cargar un par vPC, la BPDU del árbol de expansión originada por el par vPC restante no cambia, de modo que otros puentes del dominio del árbol de expansión no ven ningún cambio en el puente raíz y no reaccionan de forma subóptima al cambio en la red.

Advertencias

La mejora del switch de par vPC tiene algunas advertencias que debe tener en cuenta antes de configurarlo en un entorno de producción.

Los valores de prioridad de árbol de expansión deben coincidir entre pares vPC

Antes de activar la mejora del switch de par vPC, se debe modificar la configuración de prioridad del árbol de expansión para todas las VLAN vPC de modo que sea idéntica entre ambos pares vPC.

Considere la configuración aquí, donde N9K-1 está configurado para ser el puente de ruta del árbol de expansión para las VLAN 1, 10 y 20 con una prioridad de 0. N9K-2 es el puente de ruta del árbol de expansión secundario para las VLAN 1, 10 y 20 con una prioridad de 4096.

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

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

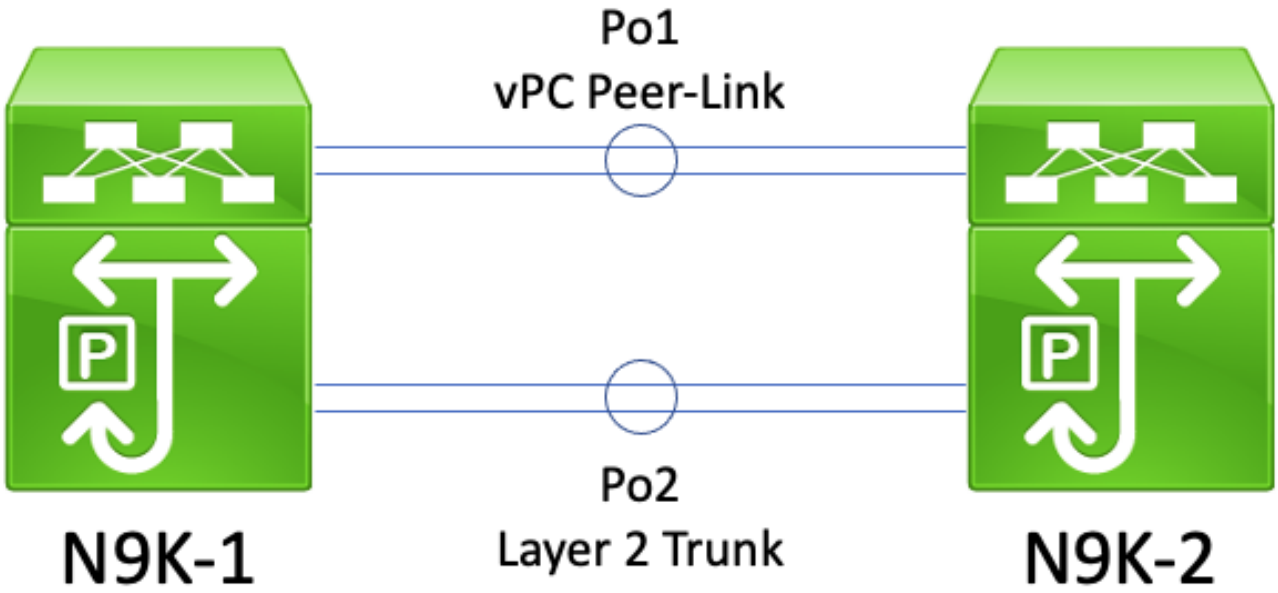
Antes de activar la mejora del switch de par vPC, debe modificar la configuración de prioridad del árbol de expansión para las VLAN 1, 10 y 20 en N9K-2 para que coincidan con la configuración de prioridad del árbol de expansión para las mismas VLAN en N9K-1. Aquí se muestra un ejemplo de esta modificación.

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

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

El switch de par vPC afecta a las VLAN no vPC

Considere la topología aquí:



En esta topología, dos pares vPC (N9K-1 y N9K-2) tienen dos enlaces troncales de Capa 2 entre ellos: Po1 y Po2. Po1 es el enlace de par vPC que transporta VLAN vPC, mientras que Po2 es un enlace troncal de Capa 2 que transporta todas las VLAN que no son vPC. Si los valores de prioridad del árbol de expansión para las VLAN que no son vPC transportadas a través de Po2 son idénticos en N9K-1 y N9K-2, cada par vPC origina tramas BPDU del árbol de expansión originadas en la dirección MAC del sistema vPC, que es idéntica en ambos switches. Como resultado, N9K-1 parece recibir su propia BPDU de Spanning Tree en Po2 para cada VLAN que no es vPC, aunque N9K-2 es el switch que originó la BPDU de Spanning Tree. Desde la perspectiva del árbol de extensión, N9K-1 coloca el Po2 en estado de bloqueo para todas las VLAN que no sean vPC.

Debe ocurrir lo siguiente. Para evitar que este comportamiento ocurra o para solucionar este problema, ambos pares vPC deben configurarse con diferentes valores de prioridad de árbol de expansión en todas las VLAN que no sean vPC. Esto permite que un par vPC se convierta en el puente raíz de la VLAN que no es vPC y que el enlace troncal de capa 2 entre pares vPC pase a un estado de reenvío designado. De forma similar, el par vPC remoto realiza la transición del troncal de capa 2 entre los pares vPC a un estado de raíz designada. Esto permite que el tráfico en las VLAN que no son vPC fluya a través de ambos pares vPC a través del troncal de Capa 2.

Configuración

Aquí puede encontrar un ejemplo de cómo configurar la función de switch de par vPC.

En este ejemplo, N9K-1 se configura para que sea el puente de ruta del árbol de expansión para las VLAN 1, 10 y 20 con una prioridad de 0. N9K-2 es el puente de ruta del árbol de expansión secundario para las VLAN 1, 10 y 20 con una prioridad de 4096.

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

```
interface port-channel1
  vpc peer-link

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

interface port-channel1
  vpc peer-link

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

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

En primer lugar, debe cambiarse la configuración de prioridad del árbol de expansión de N9K-2 para que sea idéntica a la de N9K-1. Se trata de un requisito para que la función de switch de par vPC funcione según lo esperado. Si la dirección MAC del sistema de N9K-2 es inferior a la dirección MAC del sistema de N9K-1, N9K-2 usurpa la función de puente raíz para el dominio de árbol de extensión, lo que hace que otros puentes en el dominio de árbol de extensión vacíen sus tablas de direcciones MAC locales para todas las VLAN afectadas. Aquí se muestra un ejemplo de este fenómeno.

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

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

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

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

N9K-2# show spanning-tree vlan 1

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

  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
```

```
             Address     689e.0baa.de07
             Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec

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

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

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

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

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

A continuación, podemos activar la función switch de par vPC a través del comando de configuración de dominio vPC **peer-switch**. Esto cambia el ID de puente dentro de las BPDU del Spanning Tree originadas por ambos peers vPC, lo que hace que otros bridges en el dominio del Spanning Tree vacíen sus tablas de direcciones MAC locales para todas las VLAN afectadas.

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

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

Puede verificar que la función del switch de par vPC funciona como se esperaba validando ambos pares vPC que afirman ser el puente de ruta para las VLAN vPC con el comando **show spanning-tree summary**. Este resultado también debe indicar que la función de switch de par vPC está activada y en funcionamiento.

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

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

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

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

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

Utilice el comando **show spanning-tree vlan{x}** para ver información más detallada sobre una VLAN específica. El switch que desempeña la función vPC principal u operativa principal tiene todas sus interfaces en un estado de reenvío designado. El switch que desempeña la función vPC secundaria u operativa secundaria tiene todas sus interfaces en un estado de reenvío designado, excepto el enlace de par vPC, que se encuentra en un estado de reenvío raíz. Tenga en cuenta que la dirección MAC del sistema vPC que se muestra en la salida de **show vpc role** es idéntica al ID de puente de ruta y el ID de puente de cada par vPC.

```
N9K-1# show vpc role

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

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

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

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

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

N9K-2# show vpc role

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

N9K-2# show spanning-tree vlan 1

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

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

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

Por último, podemos utilizar la utilidad de captura de paquetes del plano de control EthAnalyzer en cualquiera de los pares vPC para confirmar que ambos pares vPC están originando BPDU de árbol de expansión con un ID de puente y un ID de puente de ruta que contienen la dirección MAC del sistema vPC compartida entre ambos pares vPC.

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

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

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

Impacto

El impacto de habilitar la mejora del switch de par vPC varía en función de si otros puentes del dominio de árbol de extensión están conectados a ambos pares vPC a través de un vPC o si están conectados de forma redundante a ambos pares vPC sin un vPC.

Puentes no vPC conectados de forma redundante

Si un puente no conectado a vPC con enlaces redundantes a ambos pares vPC (de modo que un enlace se encuentre en estado de bloqueo desde una perspectiva de protocolo de árbol de expansión) detecta un cambio en el puente de ruta de árbol de expansión anunciado en las BPDU de árbol de expansión, el puente de ruta del puente puede cambiar entre las dos interfaces redundantes. A su vez, esto puede hacer que otras interfaces de reenvío designadas pasen inmediatamente a un estado de bloqueo y, a continuación, atraviesen la máquina de estado finito del protocolo de árbol de expansión (bloqueo, aprendizaje y reenvío) con pausas intermedias equivalentes al temporizador de retardo de reenvío del protocolo de árbol de expansión configurado (15 segundos de forma predeterminada). El cambio en el puerto raíz y la posterior inversión de la máquina de estado finito del protocolo de árbol de expansión pueden causar una cantidad significativa de interrupciones dentro de la red.

Cabe mencionar que este impacto se produce siempre que el par vPC que es actualmente el puente raíz del dominio de árbol de extensión se desconecta (por ejemplo, en caso de fallo de alimentación, fallo de hardware o recarga). Este comportamiento no es específico de la mejora del switch de par vPC; al activar la mejora del switch de par vPC, simplemente se produce un comportamiento similar al de un par vPC que se desconecta desde la perspectiva del árbol de expansión.

Puentes conectados a vPC

Si un puente conectado a vPC detecta un cambio en el puente raíz del árbol de expansión anunciado en las BPDU del árbol de expansión, el puente vacía las direcciones MAC aprendidas dinámicamente de su tabla de direcciones MAC. Al configurar la función de switch de par vPC, puede observar este comportamiento en los dos escenarios siguientes:

1. Cuando se configuran los valores de prioridad del árbol de expansión para que coincidan entre ambos pares de vPC, el puente de ruta del árbol de expansión puede cambiar de un par vPC a otro si el par vPC que antes no era el puente de ruta tiene una dirección MAC del sistema menor que la del par vPC anteriormente era el puente raíz. Un ejemplo de esta situación se muestra en la sección Configuración del switch de par vPC de este documento.
2. Cuando la función de switch de par vPC está habilitada a través del comando de configuración de dominio **vPC peer-switch**, ambos pares vPC comienzan a funcionar como puentes raíz del dominio de árbol de extensión. Ambos pares vPC comienzan a originar

BPDU de árbol de expansión idénticas que se afirman a sí mismos como el puente raíz del dominio de árbol de expansión.

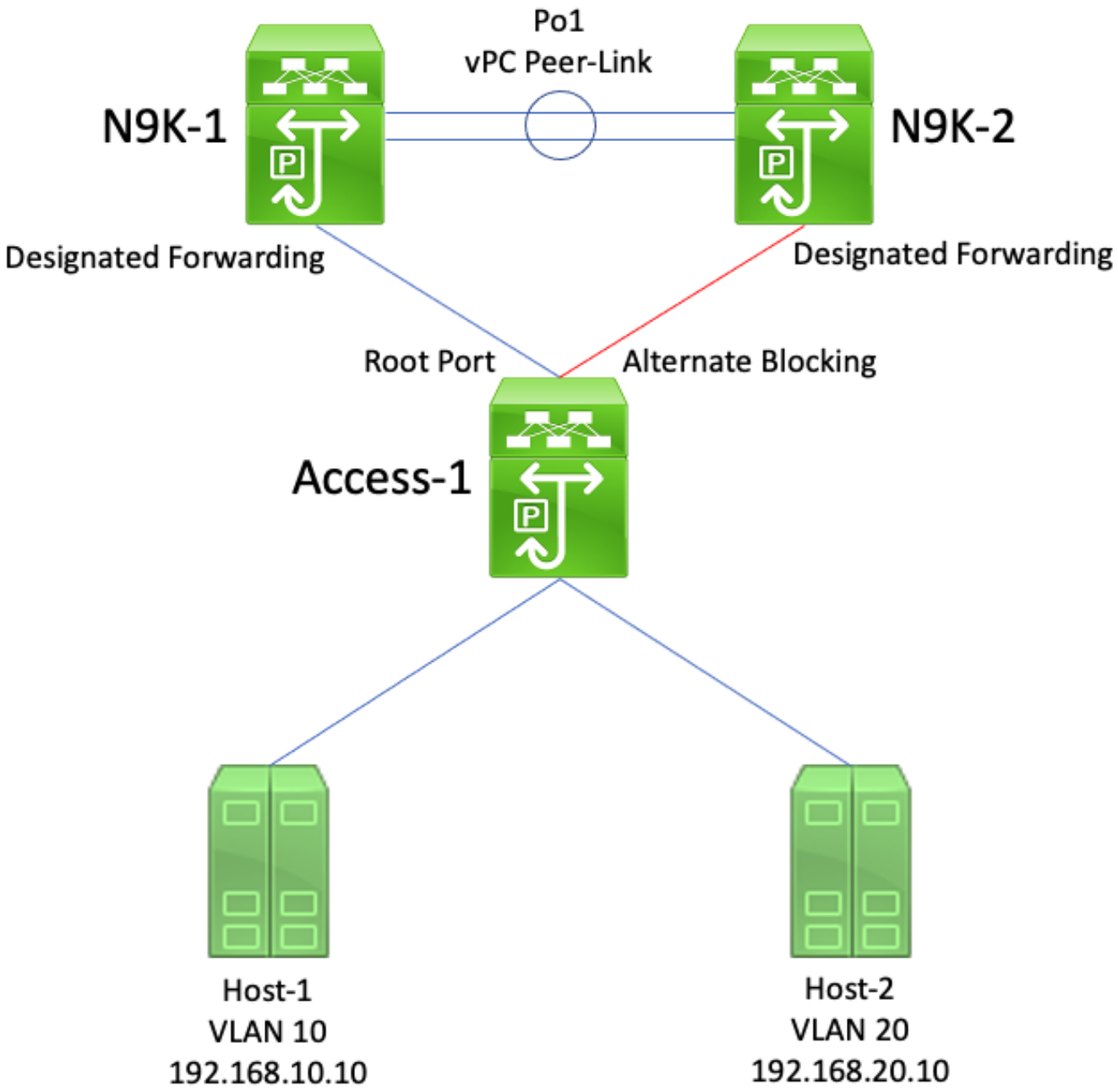
En la mayoría de los escenarios y topologías, no se observa ningún impacto en el plano de datos como resultado de ninguno de estos dos escenarios. Sin embargo, durante un corto período de tiempo, el tráfico del plano de datos se inunda dentro de una VLAN debido a la inundación de unidifusión desconocida, ya que la dirección MAC de destino de las tramas no se aprende en ningún puerto de switch como resultado directo del vaciado de las direcciones MAC aprendidas dinámicamente. En algunas topologías, esto puede causar breves períodos de problemas de rendimiento o pérdida de paquetes si el tráfico del plano de datos se desborda en dispositivos de red con suscripción excesiva dentro de la VLAN. Esto también puede causar problemas con los flujos de tráfico unidireccional de gran ancho de banda o los hosts silenciosos (hosts que reciben principalmente paquetes y rara vez envían paquetes), ya que este tráfico se inunda dentro de la VLAN durante un período de tiempo prolongado en lugar de conmutarse directamente al host de destino como es normal.

Vale la pena mencionar que este impacto está relacionado con el vaciado de direcciones MAC aprendidas dinámicamente de la tabla de direcciones MAC de los puentes dentro de la VLAN afectada. Este comportamiento no es específico de la mejora del switch de par vPC ni de un cambio en el puente de ruta; también puede ser causado por una notificación de cambio de topología generada debido a que un puerto no perimetral aparece dentro de la VLAN.

Ejemplos de situaciones de falla

Puentes no vPC conectados de forma redundante que reinician la máquina de estados finitos

Considere la topología aquí:



En esta topología, N9K-1 y N9K-2 son pares vPC en un dominio vPC. N9K-1 se configura con un valor de prioridad de árbol de expansión de 0 para todas las VLAN, lo que convierte a N9K-1 en el puente de ruta para todas las VLAN. N9K-2 se configura con un valor de prioridad de árbol de expansión de 4096 para todas las VLAN, lo que convierte a N9K-2 en el puente de ruta secundario para todas las VLAN. Access-1 es un switch que está conectado de forma redundante a los puertos de switch N9K-1 y N9K-2 a través de la Capa 2. Estos puertos de switch no se agrupan en un canal de puerto, por lo que el protocolo de árbol de expansión coloca el enlace conectado a N9K-1 en un estado de raíz designada y el enlace conectado a N9K-2 en un estado de bloqueo alternativo.

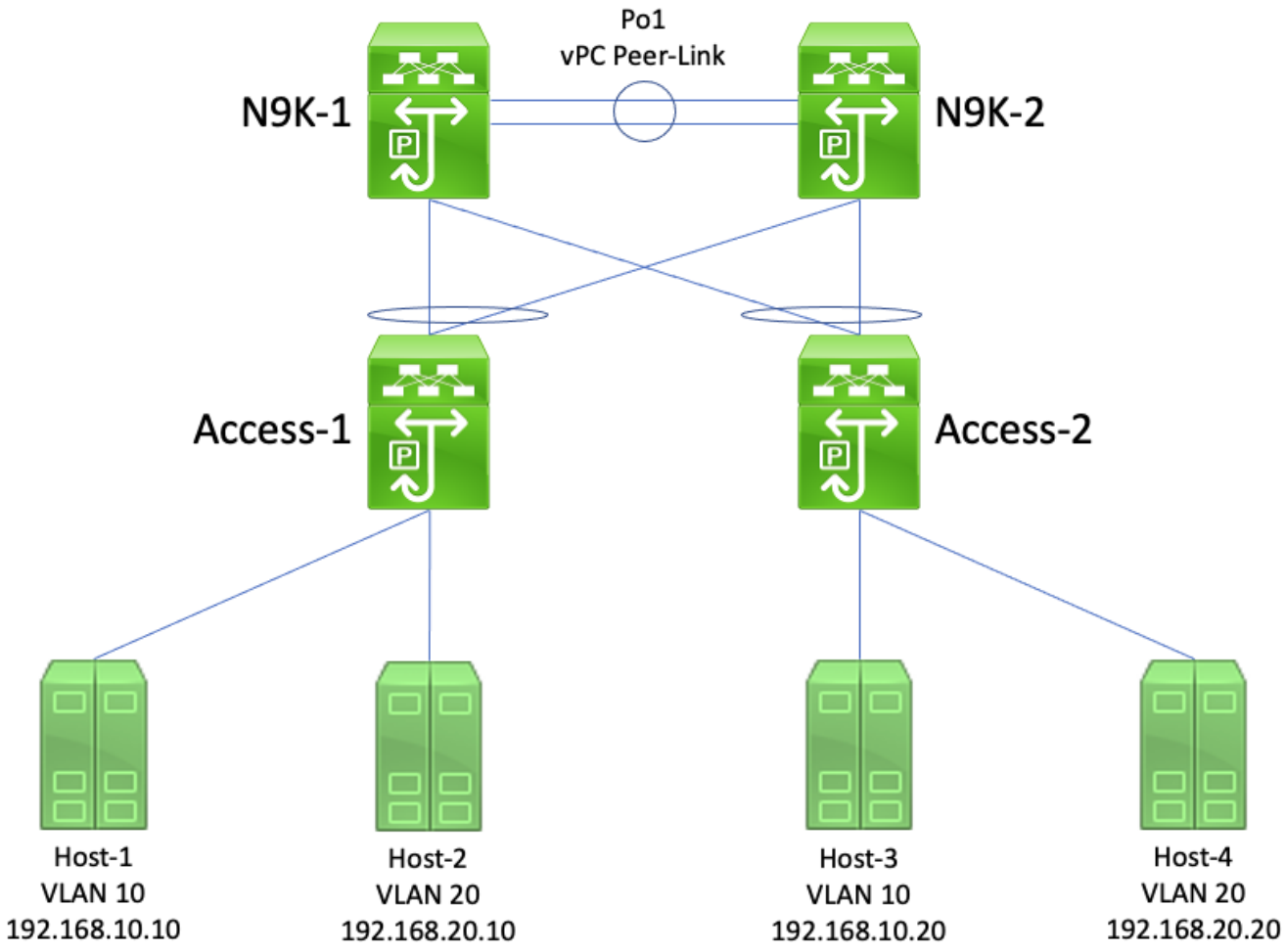
Considere una situación de falla en la que N9K-1 se desconecta debido a una falla de hardware, una falla de alimentación o una recarga del switch. N9K-2 se afirma como el puente raíz para todas las VLAN anunciando las BPDU del árbol de expansión usando su dirección MAC del sistema como el ID del puente. Access-1 ve un cambio en el ID del puente raíz. Además, se trata de transiciones de puerto de raíz designada a un estado de inactividad/inactividad, lo que significa que el nuevo puerto de raíz designada es el link que estaba en un estado de bloqueo alternativo frente a N9K-2.

Este cambio en los puertos raíz designados hace que todos los puertos de árbol de extensión no perimetral pasen a través de la máquina de estado finito del protocolo de árbol de extensión (bloqueo, aprendizaje y reenvío) con pausas entre ellas equivalentes al temporizador de retraso de reenvío del protocolo de árbol de extensión configurado (15 segundos de forma predeterminada). Este proceso puede ser extremadamente perjudicial para la red.

En el mismo escenario de falla con la mejora del switch de par vPC habilitada, tanto N9K-1 como N9K-2 transmiten BPDU de árbol de expansión idénticas usando la dirección MAC del sistema vPC compartida como ID del puente. Si N9k-1 falla, N9K-2 continúa transmitiendo esta misma BPDU de árbol de expansión. Como resultado, Access-1 pasa inmediatamente el link de bloqueo alternativo hacia N9K-2 a un estado de raíz designada y comienza a reenviar tráfico a través del link. Además, el hecho de que el ID de puente de ruta del árbol de expansión no cambie impide que los puertos no perimetrales pasen a través de la máquina de estado finito del protocolo de árbol de expansión, lo que reduce la cantidad de interrupciones observadas en la red.

Puentes conectados a vPC que vacían direcciones MAC aprendidas dinámicamente

Considere la topología aquí:



En esta topología, N9K-1 y N9K-2 son pares vPC en un dominio vPC que realizan routing entre las VLAN entre VLAN 10 y VLAN 20. N9K-1 se configura con un valor de prioridad de árbol de expansión de 0 para VLAN 10 y VLAN 20, lo que convierte a N9K-1 en el puente de ruta para ambas VLAN. N9K-2 se configura con un valor de prioridad de árbol de expansión de 4096 para VLAN 10 y VLAN 20, lo que convierte a N9K-2 en el puente de ruta secundario para ambas VLAN. Host-1, Host-2, Host-3 y Host-4 se comunican continuamente entre sí.

Considere una situación de falla en la que N9K-1 se desconecta debido a una falla de hardware, una falla de alimentación o una recarga del switch. N9K-2 se afirma a sí mismo como el puente raíz para VLAN 10 y VLAN 20 anunciando las BPDU del árbol de expansión usando su dirección MAC del sistema como el ID del puente. Access-1 y Access-2 ven un cambio en el ID del puente raíz, y aunque el spanning tree permanece igual (lo que significa que el vPC que se enfrenta a N9K-1 y N9K-2 sigue siendo un puerto raíz designado), tanto Access-1 como Access-2 purgan su dirección MAC de todas las direcciones MAC aprendidas dinámicamente en VLAN 10 y VLAN 20.

En la mayoría de los entornos, el vaciado de direcciones MAC aprendidas dinámicamente causa un impacto mínimo. No se pierden paquetes (aparte de los que se perdieron cuando se transmitieron a N9K-1 cuando falló), pero el tráfico se inunda temporalmente dentro de cada dominio de difusión como tráfico unidifusión desconocido mientras que todos los switches en el dominio de difusión vuelven a aprender las direcciones MAC dinámicas.

En la misma situación de error con la mejora del switch de par vPC activada, tanto N9K-1 como N9K-2 transmitirían BPDU de árbol de expansión idénticas utilizando la dirección MAC del sistema vPC compartido como el ID de puente. Si N9k-1 falla, N9K-2 continúa transmitiendo esta misma BPDU de árbol de expansión. Como resultado, Access-1 y Access-2 no son conscientes de que se ha producido ningún cambio en la topología del árbol de expansión; desde su perspectiva, las BPDU del árbol de expansión del puente raíz son idénticas, por lo que no hay necesidad de vaciar las direcciones MAC aprendidas dinámicamente de las VLAN relevantes. Esto evita el desborde del tráfico unidifusión desconocido en cada dominio de difusión en esta situación de falla.

Gateway de par vPC

Esta sección describe la mejora del gateway de par vPC, que se activa con el comando de configuración de dominio vPC **peer-gateway**.

Overview

Los switches Nexus configurados en un dominio vPC realizan el reenvío de protocolo FHRP activo dual de forma predeterminada. Esto significa que si un par vPC recibe un paquete con una dirección MAC de destino perteneciente a un grupo de protocolo de router en espera en caliente (HSRP) o protocolo de redundancia de router virtual (VRRP) configurado en el switch, el switch enruta el paquete de acuerdo con su tabla de routing local independientemente de su estado de plano de control HSRP o VRRP. En otras palabras, se espera un comportamiento para un par vPC en un estado HSRP de reserva o estado de copia de respaldo de VRRP para enrutar paquetes destinados a la dirección MAC virtual HSRP o VRRP.

Cuando un par vPC enruta un paquete destinado a una dirección MAC virtual FHRP, reescribe el paquete con una nueva dirección MAC de origen y destino. La dirección MAC de origen es la dirección MAC de la interfaz virtual conmutada (SVI) del par vPC dentro de la VLAN a la que se enruta el paquete. La dirección MAC de destino es la dirección MAC asociada con la dirección IP de siguiente salto para la dirección IP de destino del paquete de acuerdo con la tabla de ruteo local del par vPC. En escenarios de ruteo entre VLAN, la dirección MAC de destino del paquete después de que el paquete haya sido reescrito es la dirección MAC del host al que el paquete está destinado en última instancia.

Algunos hosts no siguen el comportamiento de reenvío estándar como función de optimización. Con este comportamiento, el host no realiza una tabla de routing ni una búsqueda de caché ARP

cuando responde a un paquete entrante. En cambio, el host da vuelta las direcciones MAC de origen y destino del paquete entrante para el paquete de respuesta. En otras palabras, la dirección MAC de origen del paquete entrante se convierte en la dirección MAC de destino del paquete de respuesta, y la dirección MAC de destino del paquete entrante se convierte en la dirección MAC de origen del paquete de respuesta. Este comportamiento difiere de un host que sigue el comportamiento de reenvío estándar, que realizaría una tabla de enrutamiento local o búsqueda de caché ARP y definiría la dirección MAC de destino del paquete de respuesta en la dirección MAC virtual FHRP.

Este comportamiento de host no estándar puede incumplir la regla de prevención de bucle de vPC si el paquete de respuesta generado por el host se dirige a un par vPC, pero envía el vPC hacia el otro par vPC. El otro par vPC recibe el paquete destinado a una dirección MAC propiedad de su par vPC y reenvía el paquete fuera del enlace de par vPC hacia el par vPC que posee la dirección MAC presente en el campo de dirección MAC de destino del paquete. El par vPC que posee la dirección MAC intenta rutear el paquete localmente. Si el paquete necesita salir de un vPC, el par vPC descarta este paquete por infringir la regla de prevención de bucles vPC. Como resultado, puede observar problemas de conectividad o pérdida de paquetes para algunos flujos originados o destinados a un host utilizando este comportamiento no estándar.

Se introdujo la mejora del gateway de par vPC para eliminar la pérdida de paquetes introducida por los hosts que utilizan este comportamiento no estándar. Esto se logra al permitir que un par vPC enrute localmente los paquetes destinados a la dirección MAC del otro par vPC, de modo que los paquetes destinados al par vPC remoto no necesiten salir del enlace de par vPC para enrutarse. En otras palabras, la mejora del gateway de par vPC permite que un par vPC enrute paquetes "en nombre" del par vPC remoto. La mejora del gateway de par vPC se puede activar con el comando de configuración de dominio vPC **peer-gateway**.

Advertencias

Intermitencia de adyacencias de protocolo de routing de unidifusión sobre vPC o VLAN vPC

Si se forman adyacencias de protocolo de routing de unidifusión dinámica entre dos pares vPC y un router conectado a vPC o un router conectado a través de un puerto vPC huérfano, las adyacencias de protocolo de routing pueden comenzar con intermitencias continuas después de activar la mejora del gateway de par vPC si la mejora de Routing/Capa 3 a través de vPC no se configura inmediatamente después. Estas situaciones de falla se describen en detalle en las secciones Ejemplos de situaciones de falla de adyacencias de protocolo de routing de unidifusión a través de un vPC con gateway de par vPC y Adyacencias de protocolo de routing de unidifusión a través de una VLAN vPC con gateway de par vPC de este documento.

Para resolver este problema, active la mejora de Routing/Capa 3 a través de vPC con el comando de configuración de dominio vPC **layer3 peer-router** inmediatamente después de activar la mejora del gateway de par vPC con el comando de configuración de dominio vPC **peer-gateway**.

Desactivación automática de redireccionamientos ICMP e ICMPv6

Cuando se habilita la mejora de la puerta de enlace de par vPC, la generación de paquetes de redirección ICMP e ICMPv6 se deshabilita automáticamente en todas las SVI de VLAN vPC (es decir, cualquier SVI asociada a una VLAN que se conecta mediante trunking a través del enlace de par vPC). El switch hace esto al configurar **no ip redirects** y **no ipv6 redirects** en todas las SVI de VLAN vPC. Esto evita que un switch genere paquetes de redirección ICMP en respuesta a los

paquetes que ingresan al switch, pero tienen una dirección MAC de destino y una dirección IP del par vPC del switch.

Si los paquetes de redirección ICMP o ICMPv6 son necesarios en su entorno dentro de una VLAN específica, debe excluir esta VLAN de las ventajas de la mejora de vPC Peer Gateway mediante el comando de configuración de dominio **vPC peer-gateway exclude-vlan <vlan-id>**.

> **Nota**: el comando de configuración de dominio **peer-gateway exclude-vlan <vlan-id>** vPC no es compatible con los switches Nexus serie 9000.

Configuración

Aquí puede encontrar un ejemplo de cómo configurar la función de gateway de par vPC.

En este ejemplo, N9K-1 y N9K-2 son pares vPC en un dominio vPC. Ambos pares vPC tienen un grupo HSRP configurado para la VLAN 10. N9K-1 es el router HSRP activo con una prioridad de 150, mientras que N9K-2 es el router de reserva de HSRP con la prioridad predeterminada de 100.

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

interface port-channel1
  vpc peer-link

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

interface port-channel1
  vpc peer-link

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

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

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

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

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

La SVI de VLAN 10 de N9K-1 tiene una dirección MAC de 00ee.ab67.db47 y la SVI de VLAN 10 de N9K-2 tiene una dirección MAC de 00ee.abd8.747f. La dirección MAC virtual HSRP para VLAN 10 es 0000.0c07.ac0a. En este estado, la dirección MAC de la SVI de VLAN 10 de cada switch y la dirección MAC virtual HSRP están presentes en la tabla de direcciones MAC de cada switch. La dirección MAC SVI VLAN 10 de cada switch y la dirección MAC virtual HSRP tienen presente el indicador Gateway (G), que indica que el switch enruta localmente los paquetes destinados a esta dirección MAC.

Tenga en cuenta que la tabla de direcciones MAC de N9K-1 no tiene el indicador de puerta de enlace presente para la dirección MAC de la SVI de VLAN 10 de N9K-2. De manera similar, la tabla de direcciones MAC de N9K-2 no tiene el indicador de Gateway para la dirección MAC de la SVI de VLAN 10 de N9K-1.

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

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

Podemos activar la mejora del gateway de par vPC a través del comando de configuración de dominio vPC **peer-gateway**. Esto permite que el switch enrute localmente los paquetes recibidos con una dirección MAC de destino perteneciente a la dirección MAC de su par vPC aprendida en el enlace de par vPC. Esto se logra al definir el indicador de gateway en la dirección MAC del par vPC dentro de la tabla de direcciones MAC del switch.

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

```
N9K-1#

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

Puede verificar que la mejora del gateway de par vPC funcione como se espera al validar que el indicador de gateway esté presente en la tabla de direcciones MAC para el MAC del par vPC.

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

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

Impacto

El impacto de habilitar la mejora de la puerta de enlace par vPC puede variar en función de la topología circundante y del comportamiento de los hosts conectados, tal y como se describe en las siguientes subsecciones. Si ninguna de las siguientes subsecciones se aplica a su entorno, la activación de la mejora de la puerta de enlace de par vPC no es perjudicial ni tiene impacto en su entorno.

Intermitencia de adyacencias de protocolo de routing de unidifusión sobre vPC o VLAN vPC

Si se forman adyacencias de protocolo de routing de unidifusión dinámica entre dos pares vPC y un router conectado a vPC o un router conectado a través de un puerto vPC huérfano, las adyacencias de protocolo de routing pueden comenzar con intermitencias continuas después de activar la mejora del gateway de par vPC si la mejora de Routing/Capa 3 a través de vPC no se configura inmediatamente después. Estas situaciones de falla se describen en detalle en las secciones Ejemplos de situaciones de falla de adyacencias de protocolo de routing de unidifusión a través de un vPC con gateway de par vPC y Adyacencias de protocolo de routing de unidifusión a través de una VLAN vPC con gateway de par vPC de este documento.

Para resolver este problema, active la mejora de Routing/Capa 3 a través de vPC con el comando de configuración de dominio vPC **layer3 peer-router** inmediatamente después de activar la mejora del gateway de par vPC con el comando de configuración de dominio vPC **peer-gateway**.

Desactivación automática de redireccionamientos ICMP e ICMPv6

Cuando se habilita la mejora de la puerta de enlace de par vPC, la generación de paquetes de redirección ICMP e ICMPv6 se deshabilita automáticamente en todas las SVI de VLAN vPC (es decir, cualquier SVI asociada a una VLAN que se conecta mediante trunking a través del enlace de par vPC). El switch hace esto al configurar **no ip redirects** y **no ipv6 redirects** en todas las SVI de VLAN vPC. Esto evita que un switch genere paquetes de redirección ICMP en respuesta a los paquetes que ingresan al switch, pero tienen una dirección MAC de destino y una dirección IP del par vPC del switch.

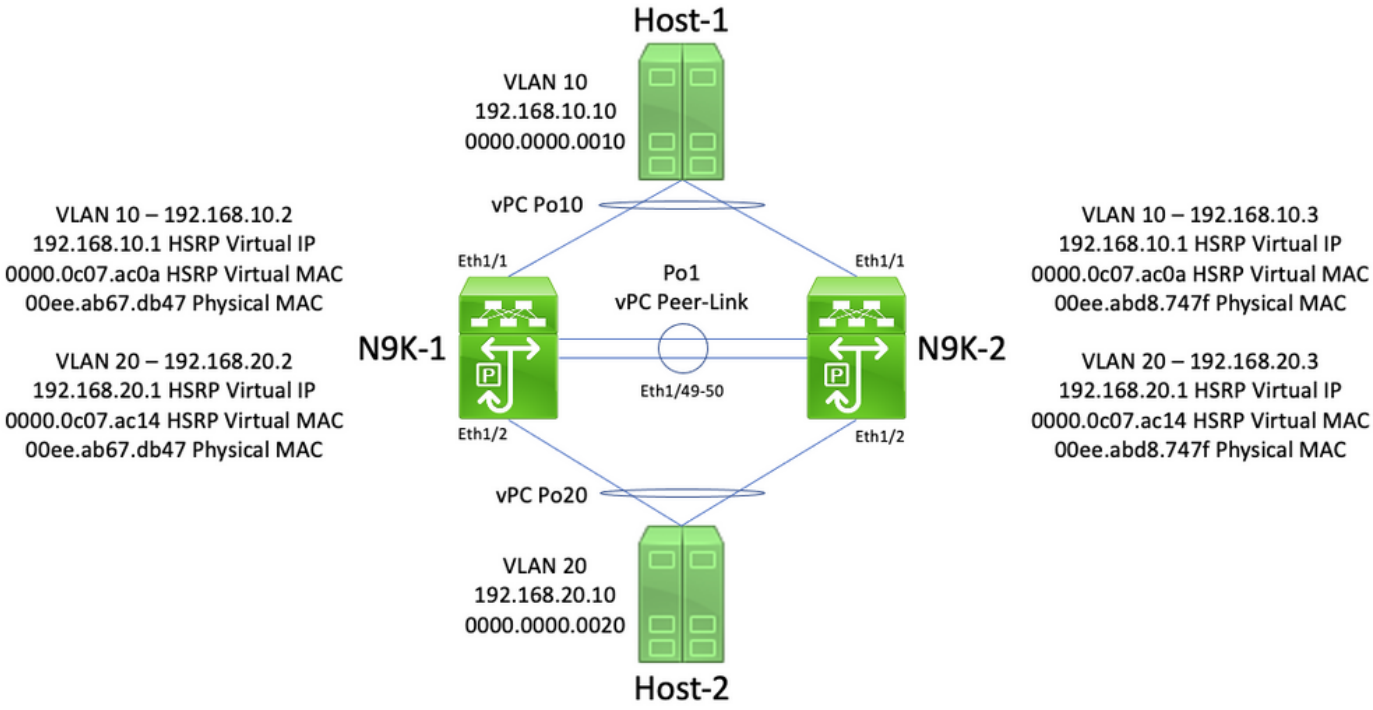
Si los paquetes de redirección ICMP o ICMPv6 son necesarios en su entorno dentro de una VLAN específica, debe excluir esta VLAN de las ventajas de la mejora de vPC Peer Gateway mediante el comando de configuración de dominio **vPC peer-gateway exclude-vlan <vlan-id>**.

> **Nota**: el comando de configuración de dominio **peer-gateway exclude-vlan <vlan-id>** vPC no es compatible con los switches Nexus serie 9000.

Ejemplos de situaciones de falla

Hosts conectados a vPC con comportamiento de reenvío no estándar

Considere la topología aquí:

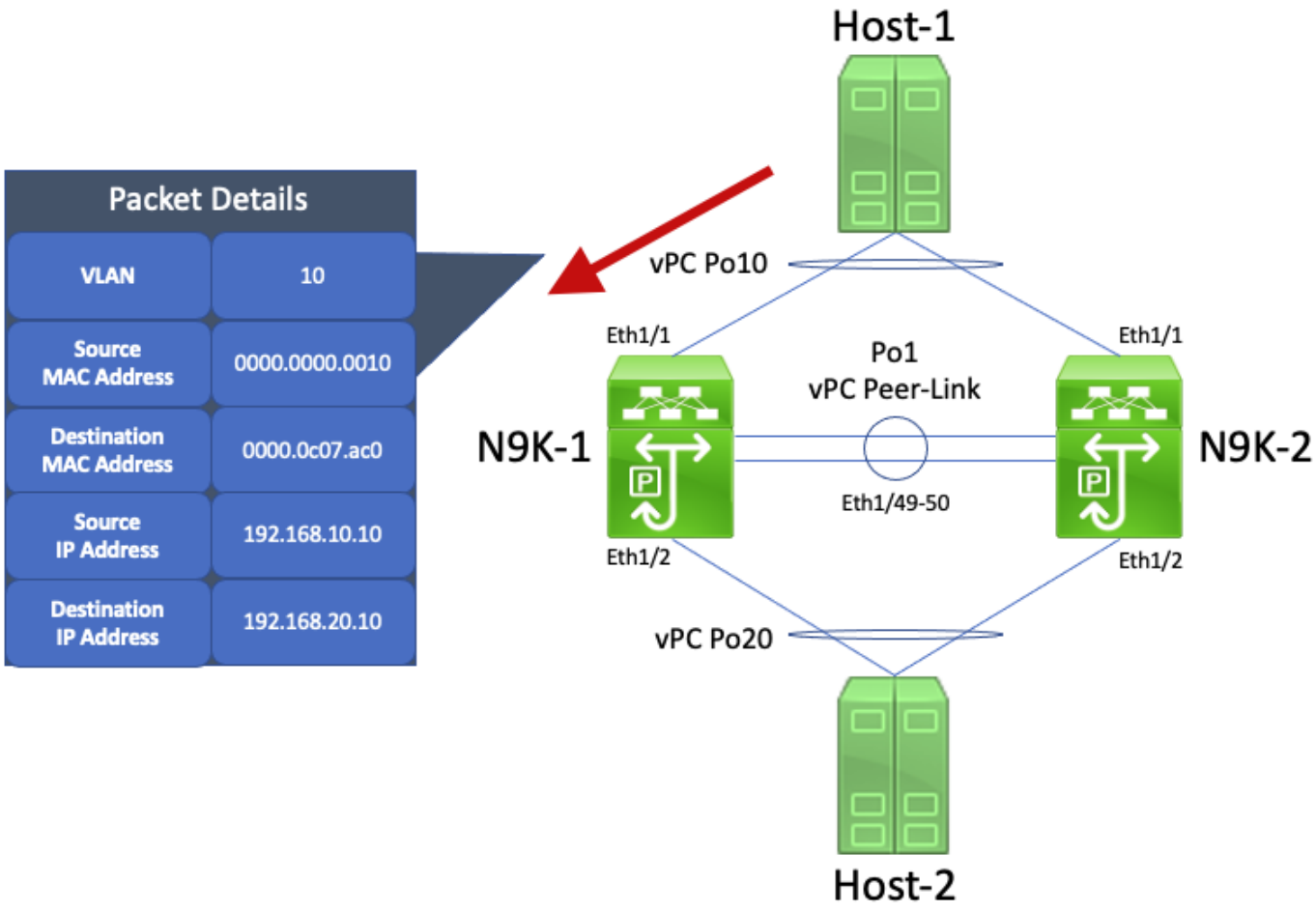


En esta topología, N9K-1 y N9K-2 son pares vPC en un dominio vPC que realizan routing entre las VLAN entre VLAN 10 y VLAN 20. La interfaz Po1 es el enlace de par vPC. Un host denominado Host-1 se conecta a través de vPC Po10 a N9K-1 y N9K-2 en VLAN 10. El Host-1 posee una dirección IP de 192.168.10.10 con una dirección MAC de 0000.0000.0010. Un host denominado Host-2 se conecta a través de vPC Po20 a N9K-1 y N9K-2 en VLAN 20. El host 2 posee una dirección IP de 192.168.20.10 con una dirección MAC de 0000.0000.0020.

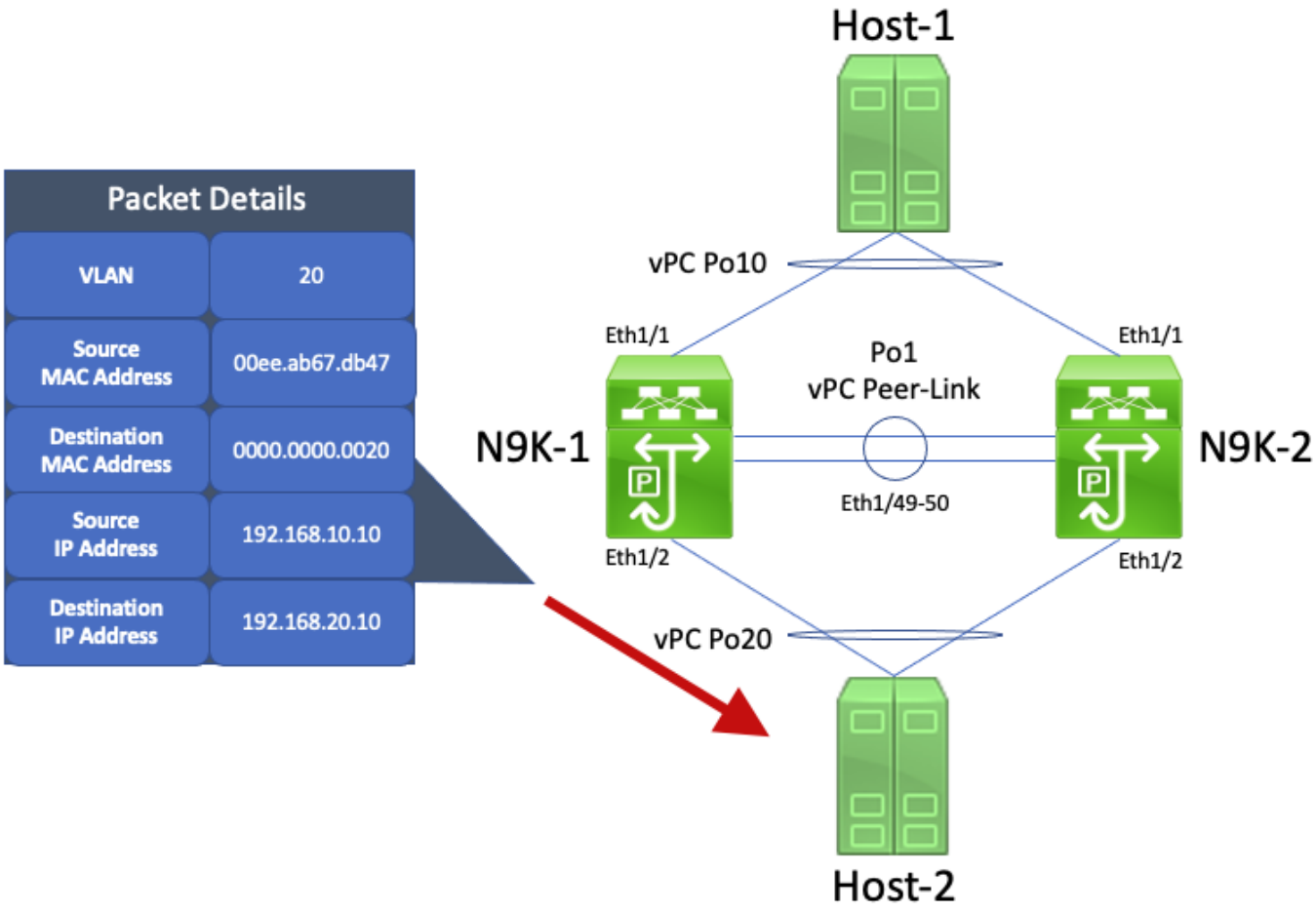
N9K-1 y N9K-2 tienen SVI en VLAN 10 y VLAN 20 con HSRP activado en cada SVI. La interfaz

VLAN 10 de N9K-1 tiene una dirección IP de 192.168.10.2 y la interfaz VLAN 20 de N9K-1 tiene una dirección IP de 192.168.20.2. Ambas SVI de N9K-1 tienen una dirección MAC física de 00ee.ab67.db47. La interfaz VLAN 10 de N9K-2 tiene una dirección IP de 1921.68.10.3 y la interfaz VLAN 20 de N9K-2 tiene una dirección IP de 192.168.20.3. Ambas SVI de N9K-2 tienen una dirección MAC física de 00ee.abd8.747f. La dirección IP virtual HSRP para VLAN 10 es 192.168.10.1 y la dirección MAC virtual HSRP es 0000.0c07.ac0a. La dirección IP virtual de HSRP para la VLAN 20 es 192.168.20.1, y la dirección MAC virtual de HSRP es 0000.0c07.ac14.

Considere una situación en la que el Host-1 envía un paquete de solicitud de eco ICMP al Host-2. Después de que el Host-1 resuelve ARP para su gateway predeterminado (la dirección IP virtual HSRP), el Host-1 sigue el comportamiento de reenvío estándar y genera un paquete de solicitud de eco ICMP con una dirección IP de origen de 192.168.10.10, una dirección IP de destino de 192.168.20.10, una dirección MAC de origen de 0000.0000.0010 y una dirección MAC de destino de 0000.0c07.ac0a. Este paquete se dirige hacia N9K-1. Aquí se muestra un ejemplo visual de esto.

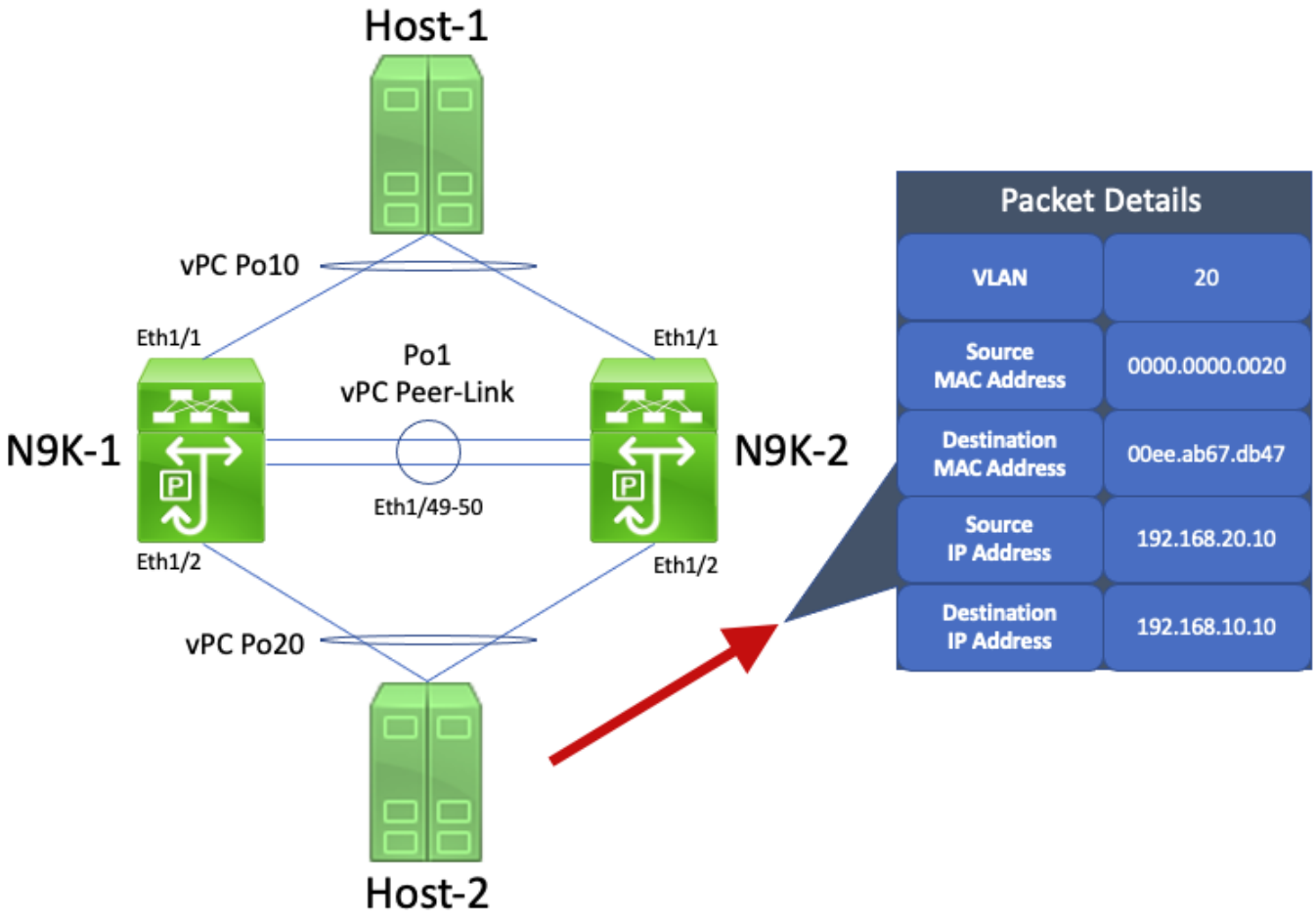


N9K-1 recibe este paquete. Dado que este paquete está destinado a la dirección MAC virtual HSRP, N9K-1 puede enrutar este paquete según su tabla de routing local independientemente de su estado de plano de control HSRP. Este paquete se enruta desde la VLAN 10 a la VLAN 20. Como parte del ruteo del paquete, N9K-1 realiza la reescritura del paquete redireccionando los campos de dirección MAC de origen y destino del paquete. La nueva dirección MAC de origen del paquete es la dirección MAC física asociada con la VLAN 20 SVI (00ee.ab67.db47) de N9K-1 y la nueva dirección MAC de destino es la dirección MAC asociada con Host-2 (0000.0000.0020). Aquí se muestra un ejemplo visual de esto.

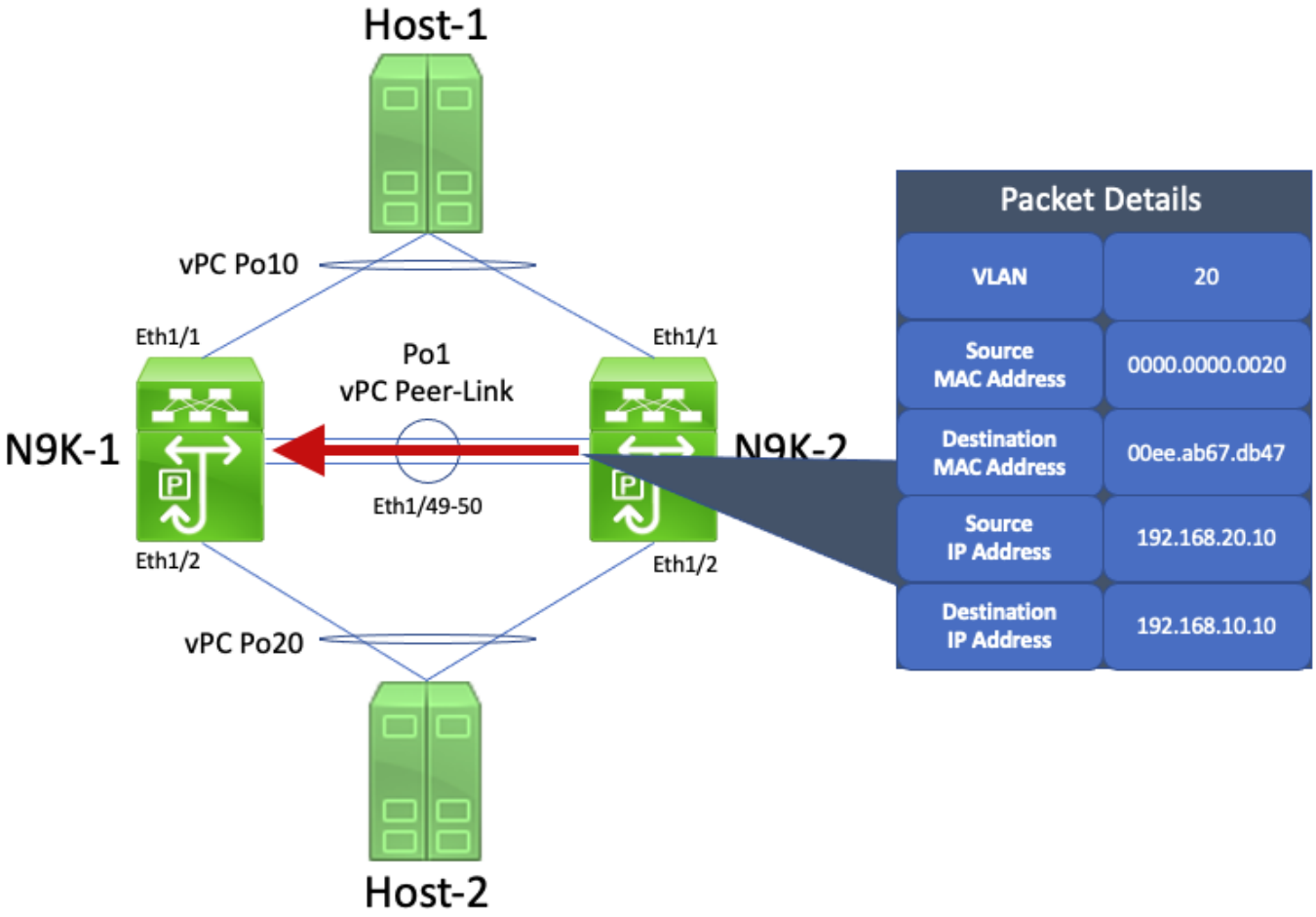


El Host 2 recibe este paquete y genera un paquete de respuesta de eco ICMP en respuesta al paquete de solicitud de eco ICMP del Host-1. Sin embargo, cuando el Host-2 no sigue el comportamiento de reenvío estándar. Para optimizar su reenvío, el Host-2 no realiza una tabla de routing ni una búsqueda de caché ARP para la dirección IP del Host-1 (192.168.10.10); en cambio, invierte los campos de dirección MAC de origen y dirección MAC de destino del Host-2 del paquete de solicitud de eco ICMP recibido originalmente. Como resultado, el paquete de respuesta de eco ICMP generado por Host-2 tiene una dirección IP de origen de 192.168.20.10, una dirección IP de destino de 192.168.10.10, una dirección MAC de origen de 0000.0000.0020 y una dirección MAC de destino de 00ee.ab67.db47.

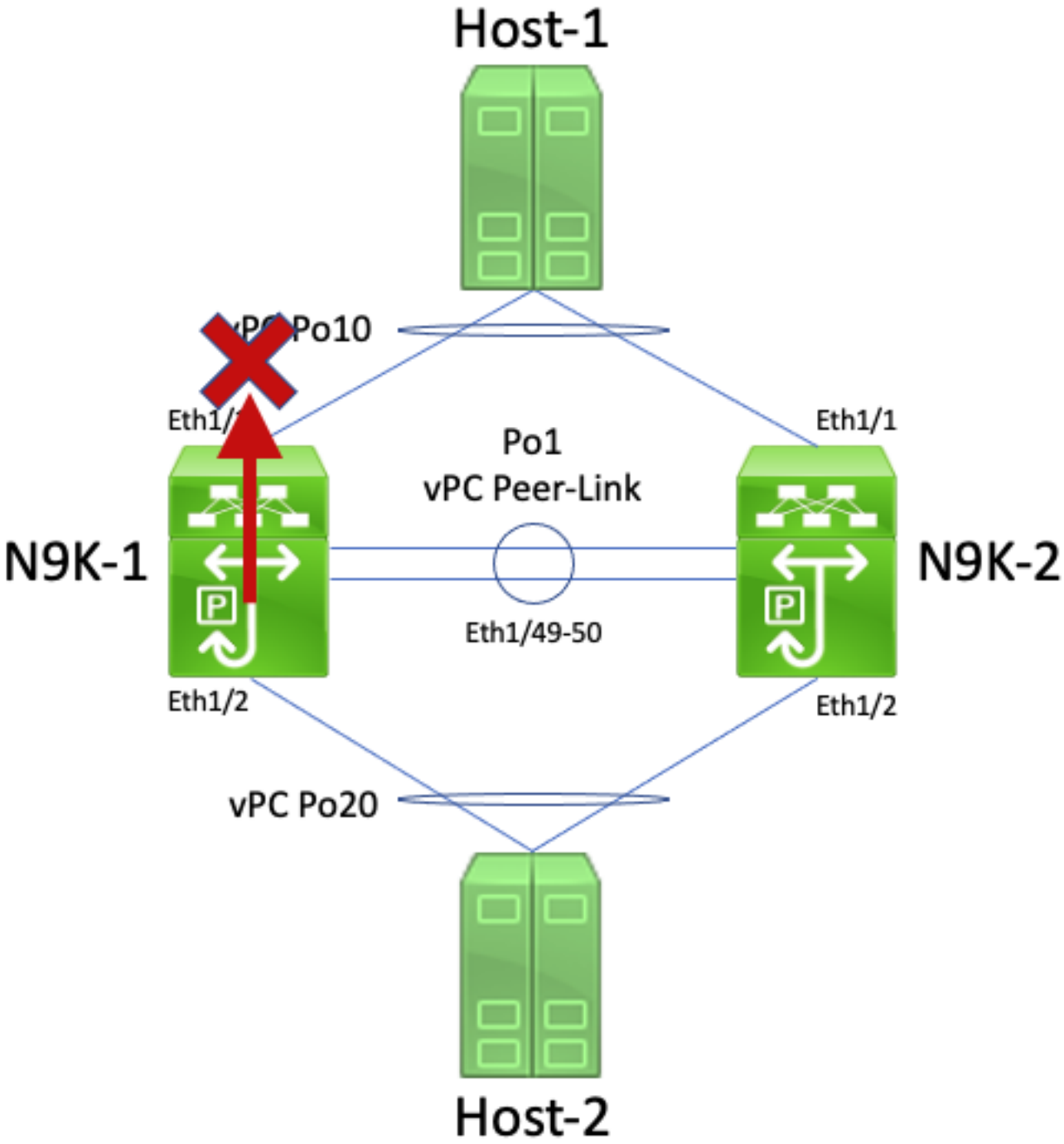
Si este paquete de respuesta de eco ICMP egresa hacia N9K-1, este paquete se reenvía hacia el Host-1 sin problemas. Sin embargo, considere una situación donde este paquete de respuesta de eco ICMP se dirige hacia N9K-2, como se muestra aquí.



N9K-2 recibe este paquete. Dado que este paquete está destinado a la dirección MAC física de la VLAN 20 SVI de N9K-1, N9K-2 reenvía este paquete a través del enlace de par vPC hacia N9K-1, ya que N9K-2 no puede rutear este paquete en nombre de N9K-1. Aquí se muestra un ejemplo visual de esto.



N9K-1 recibe este paquete. Dado que este paquete está destinado a la dirección MAC física de la SVI de VLAN 20 de N9K-1, N9K-1 puede enrutar este paquete según su tabla de routing local, independientemente del estado del plano de control de HSRP. Este paquete se enruta desde la VLAN 20 a la VLAN 10. Sin embargo, la interfaz de salida para esta ruta se resuelve en vPC Po10, que está activado en N9K-2. Se trata de una infracción de la regla de prevención de bucles de vPC. Si N9K-1 recibe un paquete a través del enlace de par de vPC, N9K-1 no puede reenviar ese paquete fuera de una interfaz vPC si la misma interfaz vPC está activada en N9K-2. N9K-1 descarta este paquete como resultado de esta infracción. Aquí se muestra un ejemplo visual de esto.



Puede resolver este problema activando la mejora del gateway de par vPC con el comando de configuración de dominio de vPC **peer-gateway**. Esto permite que N9K-2 enrute el paquete de respuesta de eco ICMP (y otros paquetes que se dirigen de manera similar) en nombre de N9K-1, aunque la dirección MAC de destino del paquete es propiedad de N9K-1 y no de N9K-2. Como resultado, N9K-2 puede reenviar este paquete desde su interfaz vPC Po10 en lugar de reenviarlo a través del enlace de par vPC.

Routing/Capa 3 a través de vPC (router par de Capa3)

Esta sección describe la mejora de Routing/Capa 3 sobre vPC, que se activa con el comando de configuración de dominio de vPC **layer3 peer-router**.

Nota: La formación de adyacencias de protocolo de routing multidifusión (es decir, adyacencias de multidifusión independiente del protocolo [PIM]) a través de vPC no es compatible con la mejora de routing/capa 3 a través de vPC activada.

Overview

En algunos entornos, los clientes desean conectar un router a un par de switches Nexus a través de vPC y formar adyacencias de protocolo de routing unidifusión a través de vPC con ambos pares vPC. De manera alternativa, los clientes pueden conectar un router a un único par vPC a través de una VLAN vPC y formar adyacencias de protocolo de routing unidifusión con ambos pares vPC a través de la VLAN vPC. Como resultado, el router conectado a vPC tendría rutas múltiples de igual costo (ECMP) para los prefijos anunciados por ambos switches Nexus. Esto puede ser preferible a utilizar enlaces de routing dedicados entre el router conectado a vPC y ambos pares vPC para conservar la utilización de direcciones IP (se necesitan 3 direcciones IP en lugar de 4 direcciones IP) o reducir la complejidad de la configuración (interfaces enrutadas junto con SVI, especialmente en entornos VRF-Lite que requerirían subinterfaces).

Tradicionalmente, las plataformas Cisco Nexus no admitían la formación de adyacencias de protocolo de routing unidifusión sobre un vPC. Sin embargo, es posible que los clientes hayan implementado una topología en la que las adyacencias del protocolo de routing unidifusión se forman sobre un vPC sin problemas, aunque no sean compatibles. Después de algunos cambios en la red (como una actualización de software del router conectado a vPC o los propios pares vPC, una conmutación por error de firewall, etc.), las adyacencias del protocolo de routing unidifusión sobre un vPC dejan de funcionar, lo que da como resultado la pérdida de paquetes para el tráfico del plano de datos o adyacencias del protocolo de routing unidifusión que no pueden aparecer con uno o ambos pares vPC. Los detalles técnicos detrás de por qué fallan y no se admiten estas situaciones se analizan en la sección Ejemplos de situaciones de falla de este documento.

La mejora de Routing/Capa 3 sobre vPC se introdujo para agregar soporte para formar adyacencias de protocolo de routing unidifusión sobre un vPC. Esto se logra permitiendo que los paquetes del protocolo de routing de unidifusión con un TTL de 1 se reenvíen a través del enlace de par vPC sin disminuir el TTL del paquete. Como resultado, pueden formarse adyacencias de protocolo de routing de unidifusión sobre una vLAN vPC o vPC sin problemas. La mejora de Routing/Capa 3 sobre vPC se puede activar con el comando de configuración de dominio vPC **layer3 peer-router** después de activar la mejora de gateway de par vPC con el comando de configuración de dominio de vPC **peer-gateway**.

Las versiones de software NX-OS que introdujeron la compatibilidad con la mejora de Routing/Capa 3 sobre vPC para cada plataforma Cisco Nexus se documentan en la tabla 2 ("Compatibilidad de adyacencias de protocolos de routing sobre VLAN vPC") dentro del documento Topologías compatibles para routing sobre canal de puerto virtual en plataformas Nexus.

Advertencias

Syslogs ocasionales VPC-2-L3_VPC_UNEQUAL_WEIGHT

Una vez habilitada la mejora del routing/capa 3 en vPC, ambos pares vPC comienzan a generar registros del sistema similares a uno de los siguientes una vez cada hora:

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

Ninguno de estos syslogs indica un problema con el switch. Estos syslogs son advertencias para el administrador de que la configuración de routing, el costo y el peso deben ser idénticos en ambos pares vPC cuando está activada la mejora de Routing/Capa 3 sobre vPC para asegurarse de que ambos pares vPC puedan enrutar el tráfico de forma idéntica. No indica necesariamente que la configuración de routing, el costo o el peso no coincidan en ninguno de los pares vPC.

Estos syslogs se pueden desactivar mediante la configuración que se muestra aquí.

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

Esta configuración debe realizarse en ambos pares vPC para inhabilitar el syslog en ambos pares vPC.

Tráfico del plano de datos con TTL de 1 software reenviado debido a la identificación de error de Cisco CSCvs82183 y Cisco bug ID CSCvw16965

Cuando la mejora del routing/capa 3 en vPC se habilita en los switches Nexus serie 9000 equipados con un ASIC a escala de nube que ejecuta una versión de software NX-OS anterior a la versión 9.3(6) del software NX-OS, el tráfico del plano de datos que no esté asociado con un protocolo de routing unidifusión que tenga un TTL de 1 se envía al supervisor y se reenvía en el software en lugar de en el hardware. En función de si el switch Nexus es un switch de chasis fijo (también denominado "parte superior del rack") o un switch de chasis modular (también denominado "final de la fila"), así como de la versión actual del software NX-OS del switch, la causa principal de este problema se puede atribuir a cualquiera de los defectos del software ID de error de Cisco CSCvs82183 o defecto de software ID de bug de Cisco CSCvw16965 . Ambos defectos de software solo afectan a los switches Nexus de la serie 9000 con un ASIC en la nube; ningún otro problema afecta a ninguna otra plataforma de hardware Cisco Nexus. Para obtener más detalles, consulte la información de cada defecto de software individual.

Para evitar estos defectos de software, Cisco recomienda actualizar a la versión 9.3(6) o posterior del software NX-OS. Como recomendación general, Cisco recomienda actualizar periódicamente la versión de software NX-OS recomendada actualmente para el switch Nexus de la serie 9000 al que hace referencia el documento Versiones recomendadas de Cisco NX-OS para los switches Cisco Nexus de la serie 9000.

Configuración

Aquí puede encontrar un ejemplo de cómo configurar la mejora de Routing/Capa 3 sobre vPC.

En este ejemplo, N9K-1 y N9K-2 son pares vPC en un dominio vPC. Ambos pares vPC ya tienen activada la mejora de gateway de par vPC, que es necesaria para activar la mejora de Routing/Capa 3 sobre vPC. Ambos pares vPC tienen una SVI en la VLAN 10, que se activa en el proceso OSPF 1. N9K-1 y N9K-3 están atascados en un estado OSPF EXSTART/EXCHANGE con un router OSPF conectado a vPC con una dirección IP e ID de vecino de 192.168.10.3.

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

interface port-channel1
  vpc peer-link

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

interface port-channel1
  vpc peer-link

N9K-1# show running-config interface Vlan10

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

N9K-2# show running-config interface Vlan10

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

N9K-1# show running-config ospf

feature ospf

router ospf 1

interface Vlan10
  ip router ospf 1 area 0.0.0.0

N9K-2# show running-config ospf

feature ospf

router ospf 1

interface Vlan10
  ip router ospf 1 area 0.0.0.0

N9K-1# show ip ospf neighbors
 OSPF Process ID 1 VRF default
 Total number of neighbors: 3
 Neighbor ID     Pri State            Up Time  Address         Interface
 192.168.10.2      1 TWOWAY/DROTHER   00:08:10 192.168.10.2    Vlan10
 192.168.10.3      1 EXCHANGE/BDR     00:07:43 192.168.10.3    Vlan10
```

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

Podemos activar la mejora de Routing/Capa 3 sobre vPC a través del comando de configuración de dominio vPC **layer3 peer-router**. Esto evita que un par vPC disminuya el TTL de los paquetes de protocolo de routing unidifusión enrutados como resultado de la activación de la mejora de la puerta de enlace de par vPC.

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

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

Puede verificar que la mejora de routing/Capa 3 sobre vPC funciona como se esperaba validando que la adyacencia OSPF con el vecino OSPF conectado a vPC pasa al estado FULL poco después de activar la mejora de routing/Capa 3 sobre vPC.

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

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

Impacto

La activación del Routing/Capa 3 sobre la mejora de vPC no causa ningún impacto inherente en el dominio vPC. Esto significa que cuando se habilita el routing/capa 3 en la mejora de vPC, ni el par vPC suspende ningún vPC ni se ve afectado de forma inherente ningún tráfico del plano de datos al habilitar esta mejora.

Sin embargo, si las adyacencias de protocolo de routing dinámico que anteriormente estaban inactivas como resultado de no tener activada la mejora de Routing/Capa 3 sobre vPC repentinamente como resultado de activar esta mejora, entonces dependiendo del rol de las adyacencias de protocolo de routing afectadas, los prefijos específicos anunciados a través de

esas adyacencias y el estado actual de la tabla de routing unidifusión, puede observarse alguna interrupción cuando se activa el Routing/Capa 3 sobre la mejora de vPC.

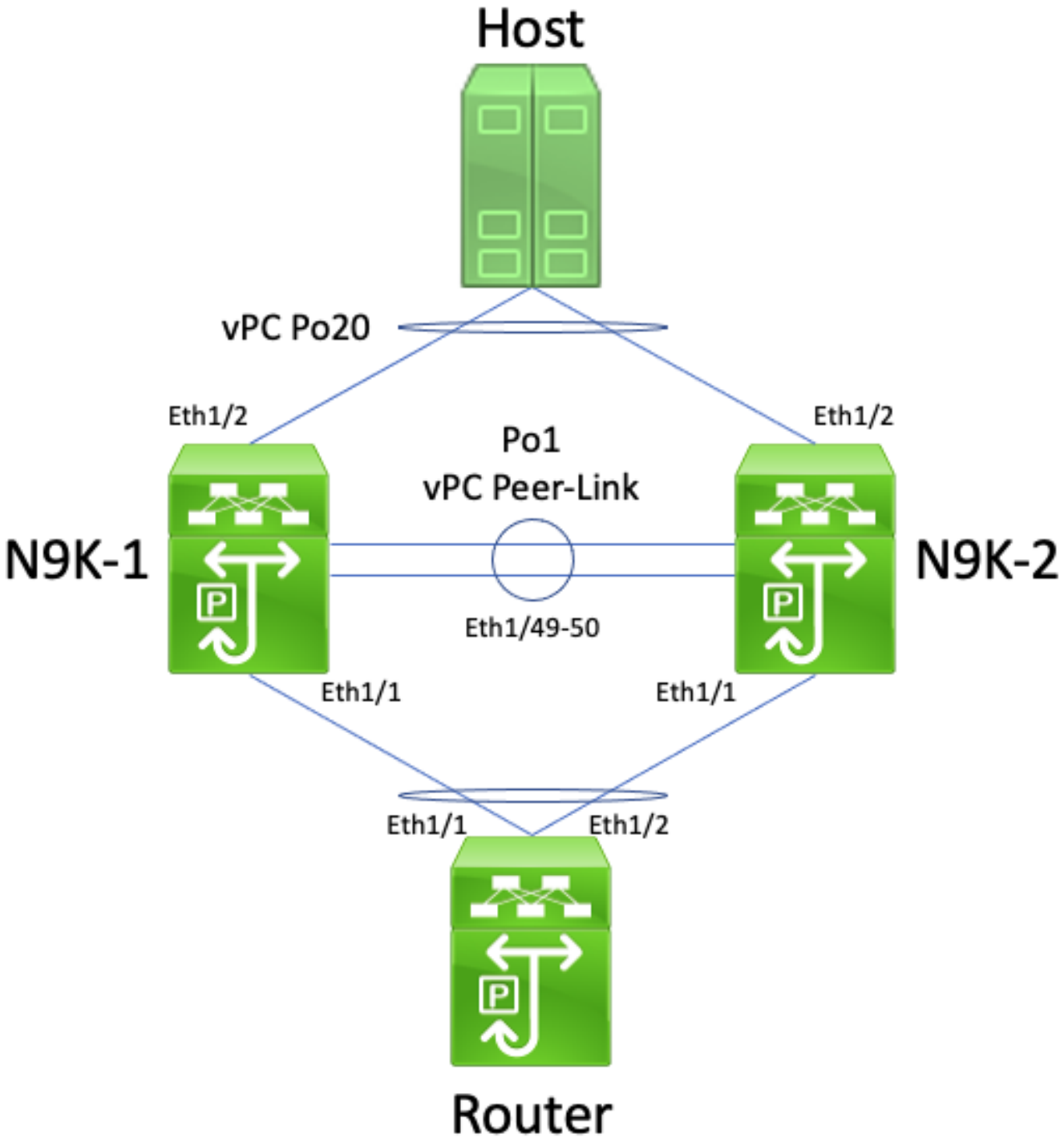
Por este motivo, Cisco aconseja a los clientes que habiliten esta mejora durante un período de mantenimiento con la expectativa de que pueda haber una interrupción en el plano de control y el plano de datos, a menos que los clientes estén extremadamente seguros de que las adyacencias del protocolo de routing afectadas no afectan significativamente al funcionamiento de la red.

Cisco también recomienda revisar detenidamente la sección Advertencias de este documento para detectar cualquier defecto de software que afecte su versión de software NX-OS que pueda causar que el tráfico natural del plano de datos con un TTL de 1 se procese en software en lugar de hardware.

Ejemplos de situaciones de falla

Adyacencias de protocolo de routing de unidifusión a través de un vPC sin gateway de par vPC

Considere la topología que se muestra aquí:



En esta topología, los switches Nexus N9K-1 y N9K-2 son pares de vPC dentro de un dominio de vPC donde la mejora del gateway de pares de vPC no está activada. La interfaz Po1 es el enlace de par vPC. Un router con el nombre de host Router está conectado a través de vPC Po10 a N9K-1 y N9K-2. Un host está conectado a N9K-1 y N9K-2 a través de vPC Po20. La interfaz Po10 del router es un canal de puerto enrutado que se activa con un protocolo de routing unidifusión. N9K-1 y N9K-2 tienen interfaces SVI activadas con el mismo protocolo de routing unidifusión y están en el mismo dominio de difusión que el router.

Las adyacencias del protocolo de routing unidifusión a través de un vPC sin la mejora de la puerta de enlace de par vPC activada no son compatibles porque la decisión de hash ECMP del router conectado a vPC y su decisión de hashing de canal de puerto de Capa 2 podrían diferir. En esta topología, las adyacencias del protocolo de routing se formarían correctamente entre el router, N9K-1 y N9K-2. Considere el flujo de tráfico entre el router y el host. El tráfico del plano de datos que atraviesa el router destinado al host puede reescribirse con una dirección MAC de destino

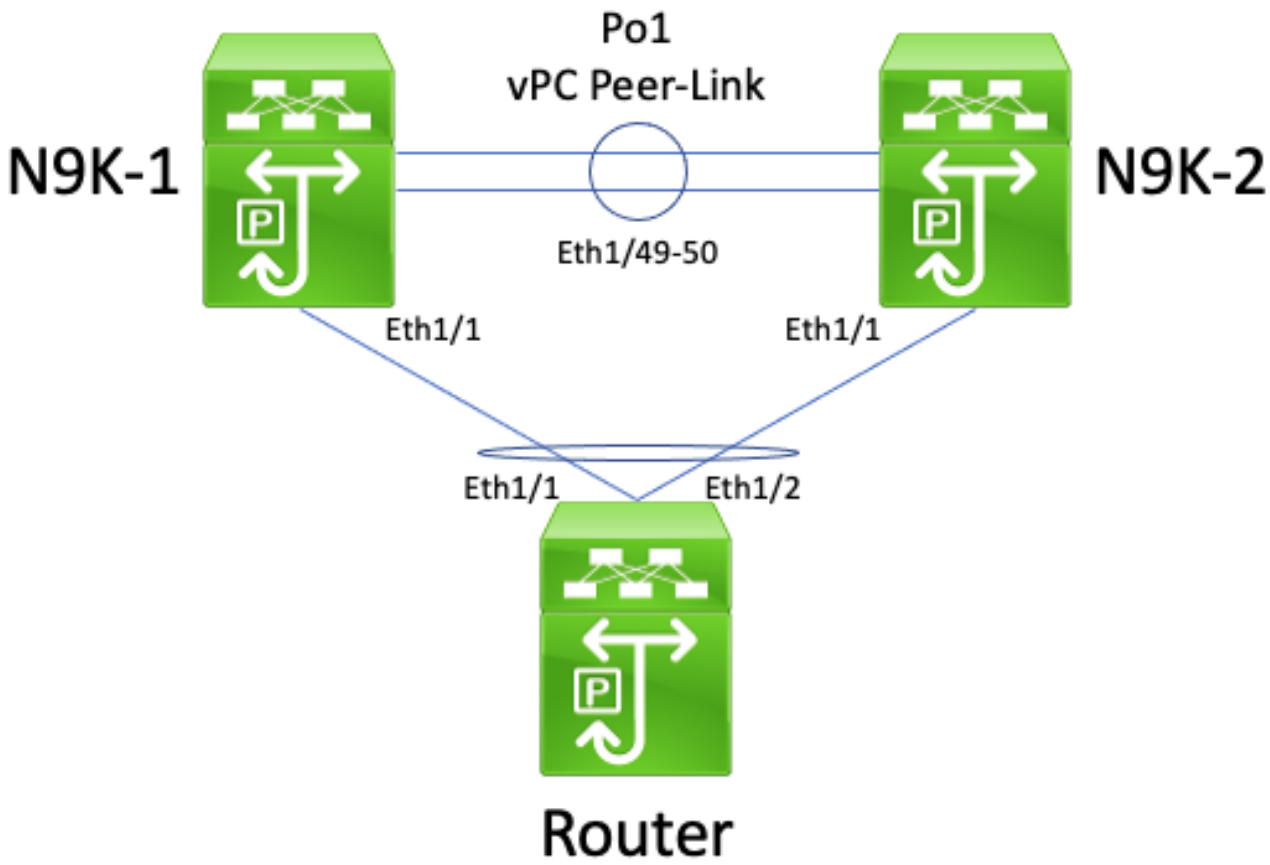
perteneciente a la dirección MAC de SVI de N9K-1 (debido a la decisión de hash ECMP tomada por el router), pero la salida de la interfaz Ethernet1/2 (debido a la decisión de hash de canal de puerto de Capa 2 tomada por el router).

N9K-2 recibe este paquete y lo reenvía a través de vPC Peer-Link, ya que la dirección MAC de destino pertenece a N9K-1 y la mejora de vPC Peer Gateway (que permite que N9K-2 rutee el paquete en nombre de N9K-1) no está habilitada. N9K-1 recibe este paquete en el enlace de par vPC y reconoce que necesitaría reenviar el paquete fuera de su Ethernet1/2 en vPC Po20. Esto infringe la regla de prevención de bucle de vPC, por lo que N9K-1 descarta el paquete en el hardware. Como resultado, puede observar problemas de conectividad o pérdida de paquetes para algunos flujos que atraviesan el dominio vPC en esta topología.

Puede resolver este problema al activar la mejora del gateway de par vPC con el comando de configuración de dominio de vPC **peer-gateway** y, a continuación, activar la mejora de Routing/Capa 3 sobre vPC con el comando de configuración de dominio vPC **layer3 peer-router**. Para minimizar las interrupciones, debe activar ambas mejoras de vPC en sucesión rápida para que la situación de falla descrita en las Adyacencias de protocolo de routing de unidifusión a través de un vPC con gateway de par vPC no pueda ocurrir.

Adyacencias de protocolo de routing de unidifusión a través de un vPC con gateway de par vPC

Considere la topología que se muestra aquí:



En esta topología, los switches Nexus N9K-1 y N9K-2 son pares de vPC dentro de un dominio de vPC donde la mejora del gateway de pares de vPC está activada. La interfaz Po1 es el enlace de par vPC. Un router con el nombre de host Router está conectado a través de vPC Po10 a N9K-1 y N9K-2. La interfaz Po10 del router es un canal de puerto enrutado que se activa con un protocolo

de routing unidifusión. N9K-1 y N9K-2 tienen interfaces SVI activadas con el mismo protocolo de routing unidifusión y están en el mismo dominio de difusión que el router.

No se admiten las adyacencias de protocolo de routing de unidifusión sobre un vPC con la mejora de gateway de par vPC activada porque la mejora del gateway de par vPC podría evitar que se formen adyacencias de protocolo de routing de unidifusión entre el router conectado a vPC y ambos pares vPC. En esta topología, una adyacencia de protocolo de ruteo entre el router y N9K-1 o N9K-2 puede fallar en aparecer como se esperaba, dependiendo de cómo los paquetes de protocolo de ruteo unicast originados por el router al hash N9K-1 o N9K-2 a través del vPC Po10.

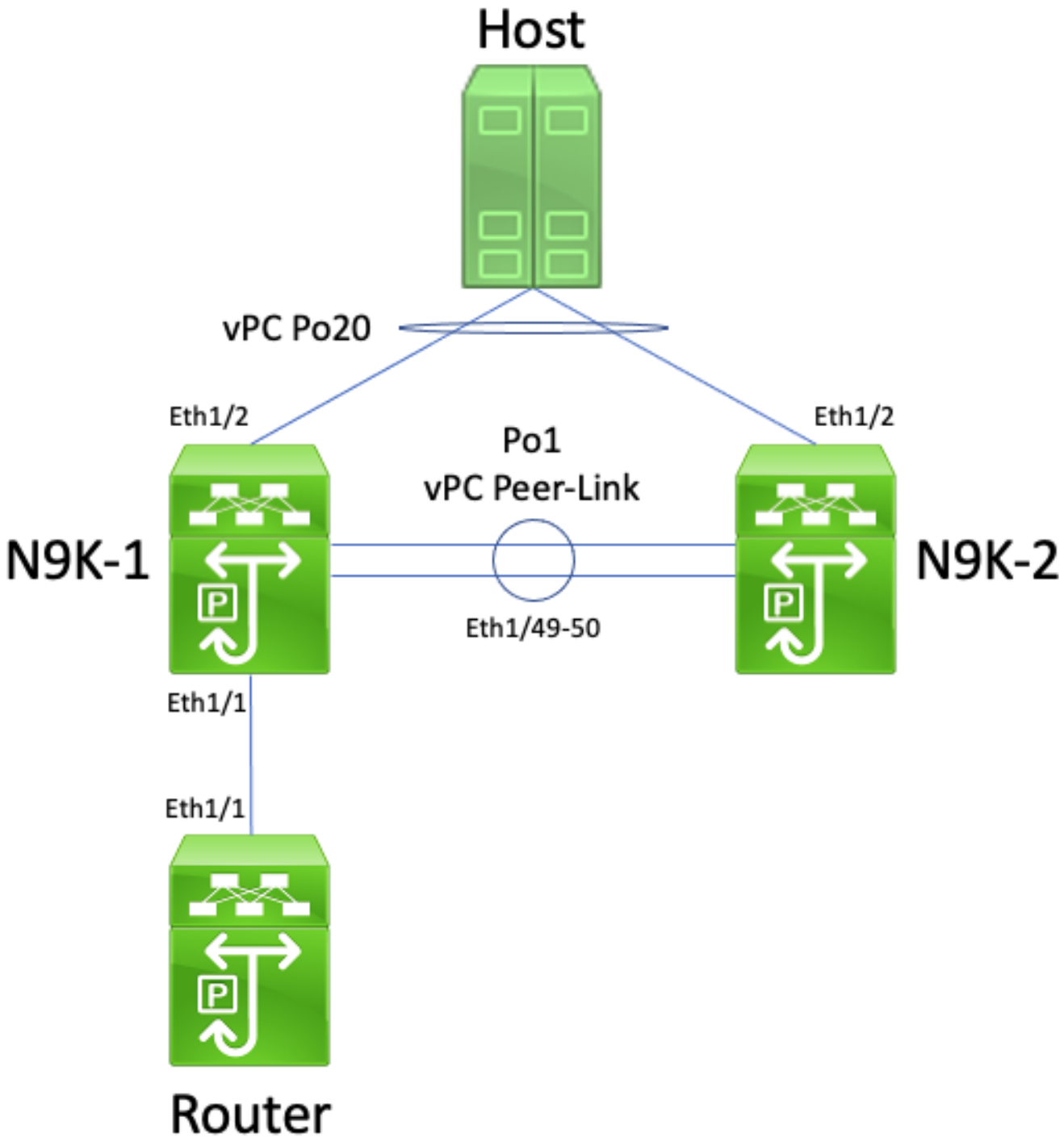
Todos los routers pueden enviar y recibir paquetes de protocolo de routing de multidifusión local de enlace (comúnmente llamados paquetes "Hello") sin problemas, ya que estos paquetes se desbordan correctamente en la VLAN de vPC. Sin embargo, considere una situación en la que un paquete de protocolo de routing de unidifusión proveniente del router destinado a N9K-1 sale de Ethernet1/2 hacia N9K-2 debido a la decisión de hash de canal de puertos de Capa 2 del router. Este paquete está destinado a la dirección MAC SVI de N9K-1, pero ingresa a la interfaz Ethernet1/1 de N9K-2. N9K-2 ve que el paquete está destinado a la dirección MAC SVI de N9K-1, que está instalada en la tabla de direcciones MAC de N9K-2 con el indicador "G", o "Gateway", debido a que la mejora de la puerta de enlace par vPC está habilitada. Como resultado, N9K-2 intenta rutear localmente el paquete de protocolo de ruteo unicast en nombre de N9K-1.

Sin embargo, al rutear el paquete, el tiempo de vida (TTL) del paquete disminuye, y el TTL de la mayoría de los paquetes de protocolo de ruteo unicast es 1. Como resultado, el TTL del paquete se reduce a 0 y es eliminado por N9K-2. Desde la perspectiva de N9K-1, N9K-1 recibe paquetes de protocolo de routing de multidifusión local de enlace del router y puede enviar paquetes de protocolo de routing de unidifusión al router, pero no recibe paquetes de protocolo de routing de unidifusión del router. Como resultado, N9K-1 elimina la adyacencia del protocolo de ruteo con el router y reinicia su máquina de estado finito local para el protocolo de ruteo. De manera similar, el router reinicia su máquina de estado finito local para el protocolo de ruteo.

Puede resolver este problema activando la mejora de Routing/Capa 3 sobre vPC con el comando de configuración de dominio de vPC **peer-router 3**. Esto permite que los paquetes del protocolo de routing de unidifusión con un TTL de 1 se reenvíen a través del enlace de par vPC sin disminuir el TTL del paquete. Como resultado, pueden formarse adyacencias de protocolo de routing de unidifusión sobre una vLAN vPC o vPC sin problemas.

Adyacencias de protocolo de routing de unidifusión a través de una VLAN vPC sin gateway de par vPC

Considere la topología que se muestra aquí:



En esta topología, los switches Nexus N9K-1 y N9K-2 son pares de vPC dentro de un dominio de vPC donde la mejora del gateway de pares de vPC no está activada. La interfaz Po1 es el enlace de par vPC. Un router con un nombre de host del router se conecta a través de Ethernet1/1 a Ethernet1/1 de N9K-1. La interfaz Ethernet1/1 del router es una interfaz enrutada que se activa con un protocolo de routing unidifusión. N9K-1 y N9K-2 tienen interfaces SVI activadas con el mismo protocolo de routing unidifusión y están en el mismo dominio de difusión que el router.

No se admiten las adyacencias de protocolo de routing de unidifusión sobre una VLAN vPC sin la mejora de gateway de par vPC activada porque la decisión de hash ECMP del router conectado a VLAN vPC puede hacer que N9K-2 elimine el tráfico del plano de datos por infringir la regla de prevención de bucles de vPC. En esta topología, las adyacencias del protocolo de routing se formarían correctamente entre el router, N9K-1 y N9K-2. Considere el flujo de tráfico entre el router y el host. El tráfico del plano de datos que atraviesa el router destinado al host puede reescribirse con una dirección MAC de destino perteneciente a la dirección MAC de SVI de N9K-2

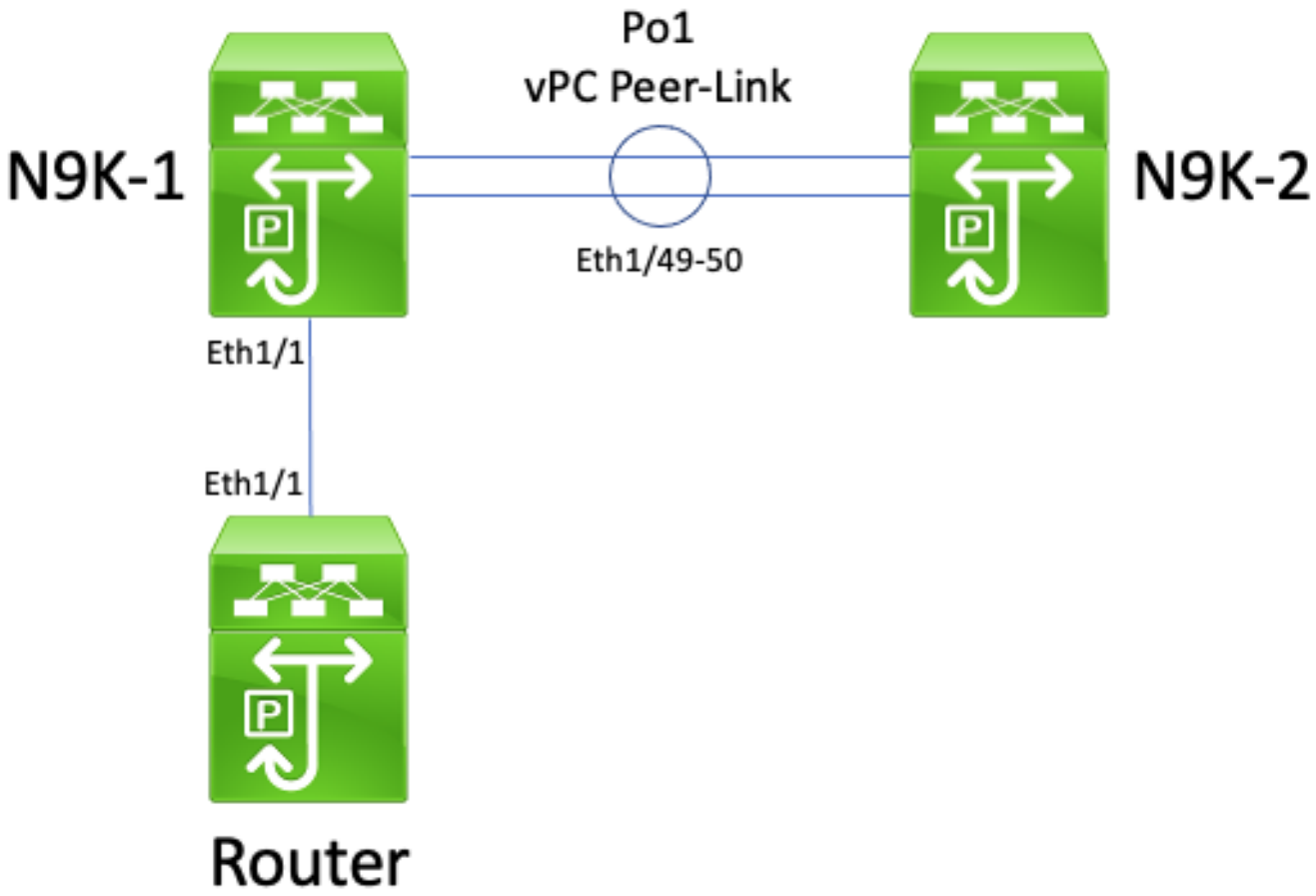
(debido a la decisión de hash ECMP tomada por el router) y salir de la interfaz Ethernet1/1 a N9K-1.

N9K-1 recibe este paquete y lo reenvía a través del enlace de par vPC, ya que la dirección MAC de destino pertenece a N9K-2 y la mejora de la puerta de enlace de par vPC (que permite que N9K-1 enrute el paquete en nombre de N9K-2) no está habilitada. N9K-2 recibe este paquete en el enlace de par vPC y reconoce que necesitaría reenviar el paquete fuera de su Ethernet1/2 en vPC Po20. Esto infringe la regla de prevención de bucle de vPC, por lo que N9K-2 descarta el paquete en el hardware. Como resultado, puede observar problemas de conectividad o pérdida de paquetes para algunos flujos que atraviesan el dominio vPC en esta topología.

Puede resolver este problema al activar la mejora del gateway de par vPC con el comando de configuración de dominio de vPC **peer-gateway** y, a continuación, activar la mejora de Routing/Capa 3 sobre vPC con el comando de configuración de dominio vPC **layer3 peer-router**. Para minimizar las interrupciones, debe activar ambas mejoras de vPC en sucesión rápida para que la situación de falla descrita en las Adyacencias de protocolo de routing de unidifusión a través de un vPC con gateway de par vPC no pueda ocurrir.

Adyacencias de protocolo de routing de unidifusión a través de una VLAN vPC con gateway de par vPC

Considere la topología que se muestra aquí:



En esta topología, los switches Nexus N9K-1 y N9K-2 son pares de vPC dentro de un dominio de vPC donde la mejora del gateway de pares de vPC está activada. La interfaz Po1 es el enlace de par vPC. Un router con un nombre de host del router se conecta a través de Ethernet1/1 a Ethernet1/1 de N9K-1. La interfaz Ethernet1/1 del router es una interfaz enrutada que se activa

con un protocolo de routing unidifusión. N9K-1 y N9K-2 tienen interfaces SVI activadas con el mismo protocolo de routing unidifusión y están en el mismo dominio de difusión que el router.

No se admiten las adyacencias de protocolo de routing unidifusión en una VLAN vPC con la mejora de la puerta de enlace de par vPC activada porque la mejora de la puerta de enlace de par vPC impide que se formen adyacencias de protocolo de routing unidifusión entre el router conectado a la VLAN vPC y el par vPC al que el router conectado a la VLAN vPC no está conectado directamente. En esta topología, una adyacencia de protocolo de ruteo entre el router y N9K-2 no se activa como se esperaba como resultado del ruteo N9K-1 de paquetes de protocolo de ruteo unicast destinados a la dirección MAC SVI de N9K-2 debido a que la mejora de vPC Peer Gateway está habilitada. Dado que los paquetes se están enrutando, se debe reducir su tiempo de duración (TTL). Los paquetes de protocolo de routing de unidifusión normalmente tienen un TTL de 1 y un router que reduce el TTL de un paquete a 0 debe descartar ese paquete.

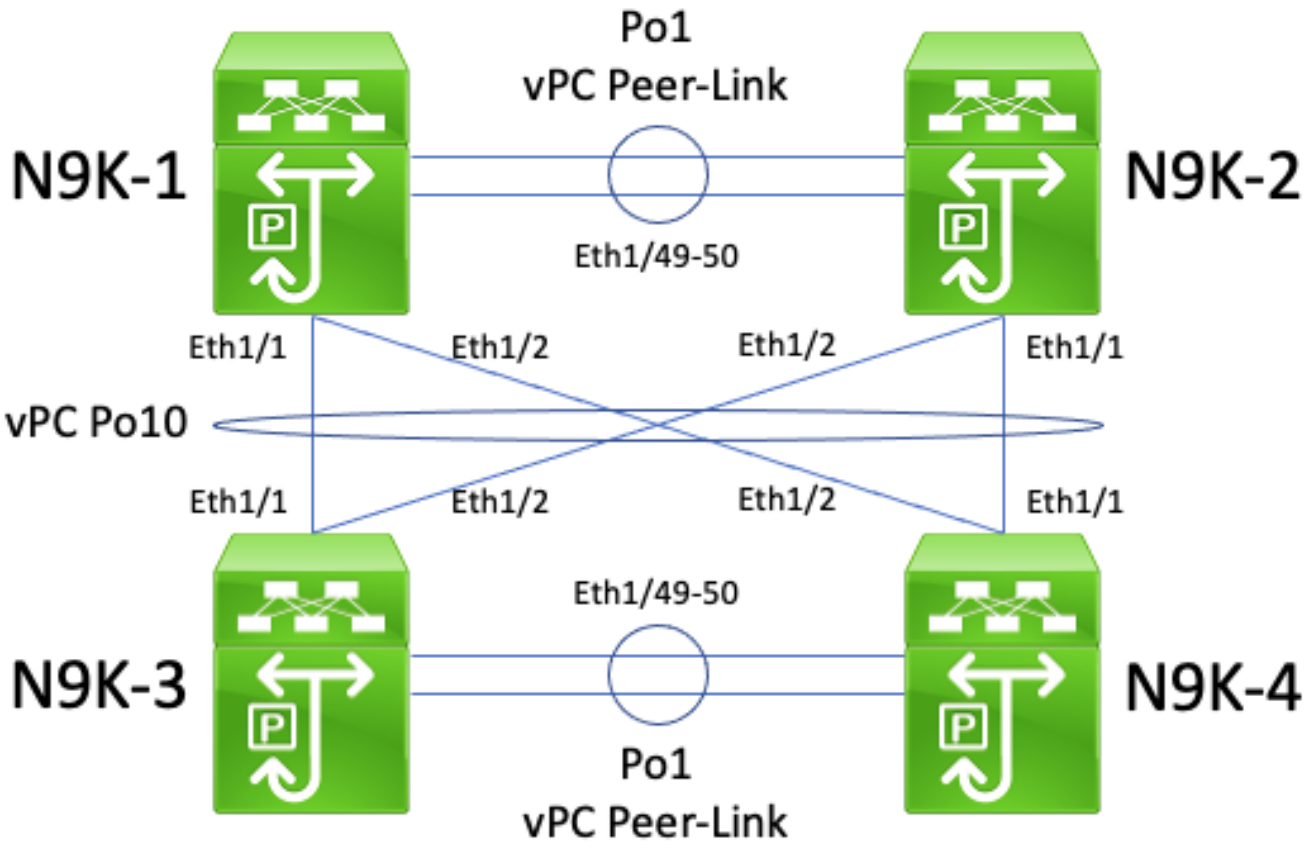
Todos los routers pueden enviar y recibir paquetes de protocolo de routing de multidifusión local de enlace (comúnmente llamados paquetes "Hello") sin problemas, ya que estos paquetes se desbordan correctamente en la VLAN de vPC. Sin embargo, considere una situación en la que un paquete de protocolo de routing de unidifusión proveniente del router destinado a N9K-2 sale de Ethernet1/1 hacia N9K-1. Este paquete está destinado a la dirección MAC SVI de N9K-2, pero ingresa a la interfaz Ethernet1/1 de N9K-1. N9K-1 ve que el paquete está destinado a la dirección MAC SVI de N9K-2, que está instalada en la tabla de direcciones MAC de N9K-1 con el indicador "G", o "Gateway", debido a que la mejora de la puerta de enlace par vPC está habilitada. Como resultado, N9K-1 intenta rutear localmente el paquete de protocolo de ruteo unicast en nombre de N9K-2.

Sin embargo, al rutear el paquete, el TTL del paquete disminuye, y el TTL de la mayoría de los paquetes de protocolo de ruteo unicast es 1. Como resultado, el TTL del paquete se reduce a 0 y N9K-1 lo descarta. Desde la perspectiva de N9K-2, N9K-2 recibe paquetes de protocolo de routing de multidifusión local de enlace del router y puede enviar paquetes de protocolo de routing de unidifusión al router, pero no recibe paquetes de protocolo de routing de unidifusión del router. Como resultado, N9K-2 elimina la adyacencia del protocolo de ruteo con el router y reinicia su máquina de estado finito local para el protocolo de ruteo. De manera similar, el router reinicia su máquina de estado finito local para el protocolo de ruteo.

Puede resolver este problema activando la mejora de Routing/Capa 3 sobre vPC con el comando de configuración de dominio de vPC **peer-router 3**. Esto permite que los paquetes del protocolo de routing de unidifusión con un TTL de 1 se reenvíen a través del enlace de par vPC sin disminuir el TTL del paquete. Como resultado, pueden formarse adyacencias de protocolo de routing de unidifusión sobre una vLAN vPC o vPC sin problemas.

Adyacencias de protocolo de routing de unidifusión a través de un vPC adosado con gateway de par vPC

Considere la topología que se muestra aquí:



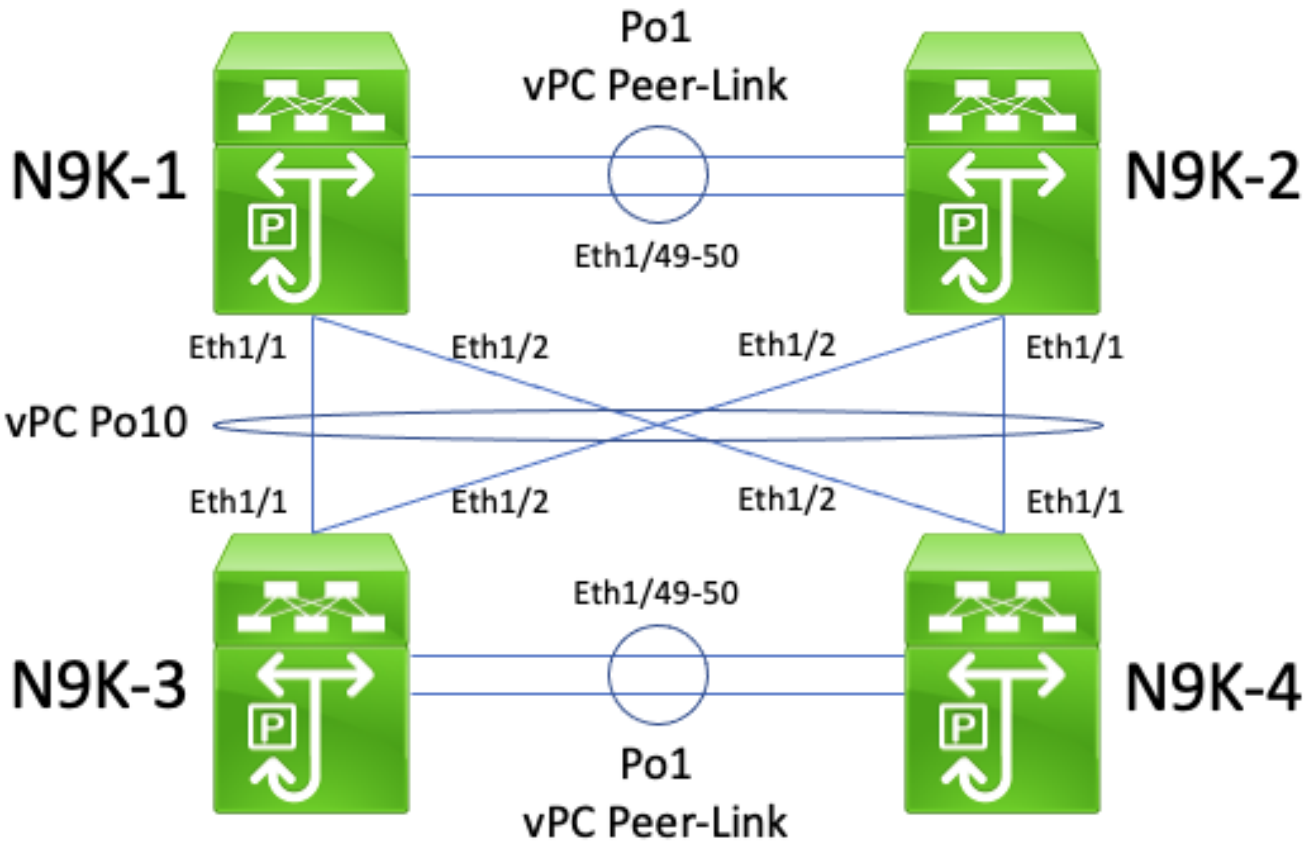
En esta topología, los switches Nexus N9K-1 y N9K-2 son pares de vPC dentro de un dominio de vPC donde la mejora del gateway de pares de vPC está activada. Los switches Nexus N9K-3 y N9K-4 son pares vPC dentro de un dominio vPC en el que está activada la mejora del gateway de par vPC. Ambos dominios vPC se conectan entre sí a través de un vPC Po10 adosado. Los cuatro switches tienen interfaces SVI activadas con un protocolo de routing unidifusión y están en el mismo dominio de difusión.

No se admiten las adyacencias de protocolo de routing de unidifusión en vPC adosados con la mejora de gateway de par vPC activada porque la mejora del gateway de par vPC puede evitar que se formen adyacencias de protocolo de routing de unidifusión entre un dominio vPC y otro. En esta topología, una adyacencia de protocolo de ruteo entre N9K-1 y N9K-3 o N9K-4 (o ambos) puede fallar en aparecer como se esperaba. De manera similar, una adyacencia de protocolo de routing entre N9K-2 y N9K-3 o N9K-4 (o ambos) puede no aparecer como se espera. Esto se debe a que los paquetes de protocolo de routing de unidifusión pueden estar destinados a un router (por ejemplo, N9K-3) pero reenviarse a otro router (por ejemplo, N9K-4) según la decisión de hash de canal de puertos de Capa 2 del router de origen.

La causa raíz de este problema es idéntica a la causa raíz que se describe en las sección Adyacencias del protocolo de routing de unidifusión sobre una de vPC con gateway de pares vPC de este documento. Puede resolver este problema activando la mejora de Routing/Capa 3 sobre vPC con el comando de configuración de dominio de vPC **peer-router 3**. Esto permite que los paquetes del protocolo de routing de unidifusión con un TTL de 1 se reenvíen a través del enlace de par vPC sin disminuir el TTL del paquete. Como resultado, pueden formarse adyacencias de protocolo de routing de unidifusión sobre un vPC adosado sin problemas.

Adyacencias OSPF a través de vPC con gateway de par vPC donde el prefijo está presente en la LSDB de OSPF pero no en la tabla de routing

Considere la topología que se muestra aquí:



En esta topología, los switches Nexus N9K-1 y N9K-2 son pares de vPC dentro de un dominio de vPC donde la mejora del gateway de pares de vPC está activada. Los switches Nexus N9K-3 y N9K-4 son pares vPC dentro de un dominio vPC en el que está activada la mejora del gateway de par vPC. Ambos dominios vPC se conectan entre sí a través de un vPC Po10 adosado. Los cuatro switches tienen interfaces SVI activadas con un protocolo de routing unidifusión y están en el mismo dominio de difusión. N9K-4 es el router designado (DR) de OSPF para el dominio de difusión, mientras que N9K-3 es el router designado de respaldo (BDR) de OSPF para el dominio de difusión.

En esta situación, una adyacencia OSPF entre N9K-1 y N9K-3 pasa a un estado FULL debido a los paquetes OSPF unidifusión que salen de Ethernet1/1 de ambos switches. De manera similar, una adyacencia OSPF entre N9K-2 y N9K-3 pasa a un estado FULL debido a los paquetes OSPF unidifusión que salen de Ethernet1/2 de ambos switches.

Sin embargo, una adyacencia OSPF entre N9K-1 y N9K-4 está atascada en un estado EXSTART o EXCHANGE debido a paquetes OSPF de unidifusión que salen de Ethernet1/1 de ambos switches y son descartados por N9K-2 y N9K-4 como se describe en la sección Adyacencias del protocolo de routing de unidifusión sobre vPC adosado con gateway de par vPC de este documento. De manera similar, una adyacencia OSPF entre N9K-2 y N9K-4 está atascada en un estado EXSTART o EXCHANGE debido a paquetes OSPF de unidifusión que salen de Ethernet1/2 de ambos switches y son descartados por N9K-1 y N9K-3 como se describe en la sección Adyacencias del protocolo de routing de unidifusión sobre vPC adosado con gateway de par vPC de este documento.

Como resultado, N9K-1 y N9K-2 están en estado FULL con el BDR para el dominio de difusión, pero están en estado EXSTART o EXCHANGE con el DR para el dominio de difusión. Tanto el DR como el BDR de un dominio de difusión conservan una copia completa de la Base de datos de estados de enlace (LSDB) de OSPF, pero los routers DROTHER de OSPF deben estar en estado FULL con el DR para el dominio de difusión a fin de instalar los prefijos aprendidos a

través de OSPF desde el DR o el BDR. Como resultado, tanto N9K-1 como N9K-2 parecen tener prefijos aprendidos de N9K-3 y N9K-4 presentes en OSPF LSDB, pero esos prefijos no se instalan en la tabla de ruteo unicast hasta que N9K-1 y N9K-2 transitan a un estado FULL con N9K-4 (el DR para el dominio de broadcast).

Puede resolver este problema activando la mejora de Routing/Capa 3 sobre vPC con el comando de configuración de dominio de vPC **peer-router 3**. Esto permite que los paquetes del protocolo de routing de unidifusión con un TTL de 1 se reenvíen a través del enlace de par vPC sin disminuir el TTL del paquete. Como resultado, pueden formarse adyacencias de protocolo de routing de unidifusión sobre un vPC adosado sin problemas. Como resultado, N9K-1 y N9K-2 pasan a un estado FULL con N9K-4 (el DR para el dominio de broadcast) e instala los prefijos aprendidos de N9K-3 y N9K-4 a través de OSPF en sus respectivas tablas de ruteo unicast exitosamente.

Información Relacionada

- Guía de configuración de las interfaces NX-OS de Cisco Nexus 9000 Series, versión 10.1(x)
- Guía de configuración de las interfaces NX-OS de Cisco Nexus 9000 Series, versión 9.3(x)
- Guía de configuración de las interfaces NX-OS de Cisco Nexus 9000 Series, versión 9.2(x)
- Guía de configuración de las interfaces NX-OS de Cisco Nexus 9000 Series, versión 7.x
- Guía de configuración de las interfaces NX-OS de Cisco Nexus 7000 Series, versión 8.x
- Guía de configuración de las interfaces NX-OS de Cisco Nexus 7000 Series, versión 7.x
- Guía de diseño y configuración: Prácticas recomendadas para Virtual Port Channels (vPC) en switches Nexus de Cisco serie 7000
- Topologías admitidas para el routing por canal de puertos virtuales en plataformas Nexus

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).