Inzicht in verbeteringen in Virtual Port Channels (vPC)

Inhoud

Inleiding

In dit document worden de gebruikelijke verbeteringen beschreven voor Virtual Port Channel (vPC) die op Cisco Nexus-switches in een vPC-domein zijn geconfigureerd.

Voorwaarden

Vereisten

Cisco raadt u aan om uzelf vertrouwd te maken met de basisinformatie met betrekking tot de use cases, configuratie en implementatie van vPC. Raadpleeg een van de volgende toepasselijke documenten voor meer informatie over deze functie:

- Configuratiehandleiding voor Cisco Nexus 9000 Series NX-OS-interfaces, release 10.1(x)
- Configuratiehandleiding voor Cisco Nexus 9000 Series NX-OS-interfaces, release 9.3(x)
- Configuratiehandleiding voor Cisco Nexus 9000 Series NX-OS-interfaces, release 9.2(x)
- Configuratiehandleiding voor Cisco Nexus 9000 Series NX-OS-interfaces, release 7.x
- Configuratiehandleiding voor Cisco Nexus 7000 Series NX-OS-interfaces 8.x
- Configuratiehandleiding voor Cisco Nexus 7000 Series NX-OS-interfaces 7.x
- Design and Configuration Guide: Best Practices voor Virtual Port Channel (vPC) op Cisco Nexus 7000 Series Switches

Gebruikte componenten

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Sinds de introductie van Cisco NX-OS op Cisco Nexus-datacenterswitches heeft de functie vPC (Virtual Port Channel) talrijke verbeteringen ondergaan die de betrouwbaarheid van via vPC verbonden apparaten tijdens foutscenario's ten goede komt en het doorschakelgedrag van beide vPC-peerswitches optimaliseren. Als u inzicht krijgt in het doel van elke verbetering, de wijziging in het gedrag als gevolg van de verbetering en de foutscenario's die worden opgelost door de verbetering begrijpt u beter waarom en wanneer een verbetering moet worden geconfigureerd binnen een vPC-domein om zo goed mogelijk aan de bedrijfsbehoeften en -vereisten te voldoen.

Toepasselijke hardware

De procedure in dit document is van toepassing op alle vPC-compatibele Cisco Nexus-datacenterswitches.

vPC-peerswitch

In deze sectie wordt de vPC-peerswitch beschreven, een verbetering die wordt ingeschakeld met de configuratieopdracht **peer-switch** voor het vPC-domein.

Overzicht

In veel omgevingen zijn een paar Nexus-switches in een vPC-domein aggregatie- of core-switches die de grens vormen tussen via Layer 2 geswitchte Ethernet-domeinen en via Layer 3 gerouteerde domeinen. Beide switches worden geconfigureerd met meerdere VLAN's en zijn verantwoordelijk voor de routering van oost-west verkeer tussen VLAN's, maar ook noord-zuid verkeer. In deze omgevingen fungeren de Nexus-switches vanuit een Spanning Tree Protocol-perspectief doorgaans ook als root-bruggen.

Normaal gesproken is één vPC-peer ingesteld als de root-brug van de Spanning Tree door de Spanning Tree-prioriteit in te stellen op een lage waarde, zoals 0. De andere vPC peer is geconfigureerd met een iets hogere Spanning Tree-prioriteit, zoals 4096, die het mogelijk maakt de rol van root-brug binnen de Spanning Tree over te nemen als de vPC-peer die als root-brug fungeert, mislukt. Met deze configuratie genereert de vPC-peer die optreedt als de root-brug BPDU's (Bridge Protocol Data Units) voor de Spanning Tree, met een brug-id die het MAC-adres van het systeem bevat.

Als de vPC-peer die als root-brug fungeert echter faalt en ervoor zorgt dat de andere vPC-peer de Spanning Tree-root-brug overneemt, ontstaat de andere vPC-peer Spanning Tree BPDU's met een Bridge ID met het systeemMAC-adres van de oorspronkelijke root-brug. Afhankelijk van de manier waarop stroomafwaartse bruggen zijn verbonden, varieert het effect van deze wijziging en wordt deze in de volgende subparagrafen beschreven.

Redundant verbonden niet-vPC-bruggen

Niet-vPC-verbonden bruggen die zijn verbonden met zowel vPC-peer als redundante links (zodat één link zich in een blokkerende staat bevindt vanuit het perspectief van Spanning Tree Protocol) die de wijziging in de BPDU (en dus de wijziging in root-brug) detecteren, zien een wijziging in Root Port. Andere toegewezen Forwarding-interfaces, onmiddellijk overgang naar een blokkerende toestand, en vervolgens de machine met de eindige status Spanning Tree Protocol (blokkering, leren en doorsturen) met pauzes tussen de equivalent van de geconfigureerde Spanning Tree Protocol Forward Delay-timer (standaard 15 seconden).

De wijziging van de root-poort en het daaropvolgende doorlopen van de eindigetoestandsautomaat van het Spanning Tree Protocol kan een aanzienlijke verstoring binnen het netwerk veroorzaken. De vPC-peerswitch is vooral geïntroduceerd om netwerkverstoringen door dit probleem te voorkomen als een van de vPC-peers offline gaat. Dankzij de verbetering van de vPC Peer Switch heeft de niet-vPC-aangesloten brug nog steeds één redundante link die zich in een blokkerende toestand bevindt, maar onmiddellijk overgangen die naar een doorsturen status interfaceren als de bestaande Root Port uitvalt vanwege een koppelingsfout. Hetzelfde proces gebeurt wanneer de offline vPC peer online terugkomt - de root-brug met de laagste

kosten neemt de rol Root Port over, en de redundante link gaat onmiddellijk over naar een blokkerende staat. De enige impact die wordt waargenomen is het onvermijdelijke verlies van pakketten tijdens de vlucht die de vPC-peer passeerden terwijl deze offline ging.

Via vPC verbonden bruggen

Met vPC verbonden bruggen in het Spanning Tree-domein detecteren de wijziging in de BPDU (en dus de wijziging in root-brug) en spoelen dynamisch aangeleerde MAC-adressen uit hun lokale MAC-adrestabellen. Dit gedrag is inefficiënt en onnodig in topologieën met vPC-verbonden apparaten die niet afhankelijk zijn van Spanning Tree Protocol voor een lusvrije topologie. vPC's worden gezien als één logische interface vanuit een Spanning Tree Protocol-perspectief, net zoals normale poortkanalen, zodat het verlies van een vPC-peer vergelijkbaar is met het verlies van één enkele link binnen een poortkanaallid. In beide scenario's verandert de Spanning Tree niet, dus is het verwijderen van dynamisch geleerde MAC-adressen van bruggen in het Spanning Tree-domein (waarvan het doel is om het flood-en-leer-gedrag van Ethernet toe te staan om MAC-adressen opnieuw te leren op nieuwe doorsturende interfaces van de Spanning Tree) onnodig.

Bovendien kan het verwijderen van dynamisch geleerde MAC-adressen ontwrichtend zijn. Denk aan een scenario waarin twee hosts een grotendeels unidirectionele, op UDP gebaseerde stroom hebben (zoals een TFTP-client die data naar een TFTP-server zendt). In deze stroom stromen data meestal van de TFTP-client naar de TFTP-server. De TFTP-server stuurt zelden een pakket terug naar de TFTP-client. Dientengevolge, na een vloed van dynamisch-geleerde MAC-adressen in het Spanning Tree-domein, wordt de MAC van de TFTP-server enige tijd niet geleerd. Dit betekent dat de gegevens van de TFTP-client die naar de TFTP-server worden verzonden, door het VLAN worden overspoeld, aangezien het verkeer onbekend-unicastverkeer is. Dit kan leiden tot grote datastromen naar onbedoelde plaatsen in het netwerk en kan prestatieproblemen veroorzaken als de stromen door overbelaste delen van het netwerk gaan.

De vPC-peerswitch is geïntroduceerd om dit inefficiënte en overbodige gedrag te voorkomen als de vPC-peer die fungeert als root-brug voor de Spanning Tree voor een of meer VLAN's opnieuw wordt geladen of wordt uitgeschakeld.

Om de vPC-peerswitch in te schakelen, moeten beide vPC-peers een identieke Spanning Tree Protocol-configuratie hebben (inclusief Spanning Tree-prioriteitswaarden voor alle vPC-VLAN's) en de root-brug zijn voor ten minste één vPC-VLAN. Als aan deze voorwaarden wordt voldaan, moet de configuratieopdracht **peer-switch** voor het vPC-domein worden geconfigureerd om de vPC-peerswitch in te schakelen.

> **Opmerking**: de verbetering van de vPC-peer Switch inschakelen in een vPC-domein waar geen van de vPC-peer switches de Spanning Tree Protocol-Root-brug voor een of meer vPC VLAN's zijn, wordt niet aanbevolen. Schakel de vPC-peerswitch alleen in als een of beide vPC-peerswitches de root-brug voor het Spanning Tree Protocol is voor een of meer vPC-VLAN's.

Nadat de verbetering van de vPC Peer Switch is ingeschakeld, beginnen beide vPC-peers met identieke Spanning Tree BPDU's met een Bridge ID die het MAC-adres van het vPC-systeem bevat dat door beide vPC-peers wordt gedeeld. Als een vPC-peer opnieuw wordt geladen, verandert de Spanning Tree BPDU die is gegenereerd door de resterende vPC-peer niet, zodat andere bruggen in het Spanning Tree-domein geen wijzigingen in de root-brug zien en niet suboptimaal reageren op de wijziging in het netwerk.

Voorbehouden

De vPC-peerswitch kent wel enkele beperkingen waarvan u zich bewust moet zijn voordat u deze configureert in een productieomgeving.

Prioriteitswaarden voor de Spanning Tree moeten overeenkomen tussen vPC-peers

Voordat u de vPC-peerswitch inschakelt, moet u de Spanning Tree-prioriteitsconfiguratie voor alle vPC-VLAN's wijzigen zodat deze identiek is tussen beide vPC-peers.

Overweeg hier de configuratie, waarbij N9K-1 is geconfigureerd als de Spanning Tree root-brug voor VLAN's 1, 10 en 20 met een prioriteit van 0. N9K-2 is de secundaire Spanning Tree-root-brug voor VLAN's 1, 10 en 20 met een prioriteit van 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
```

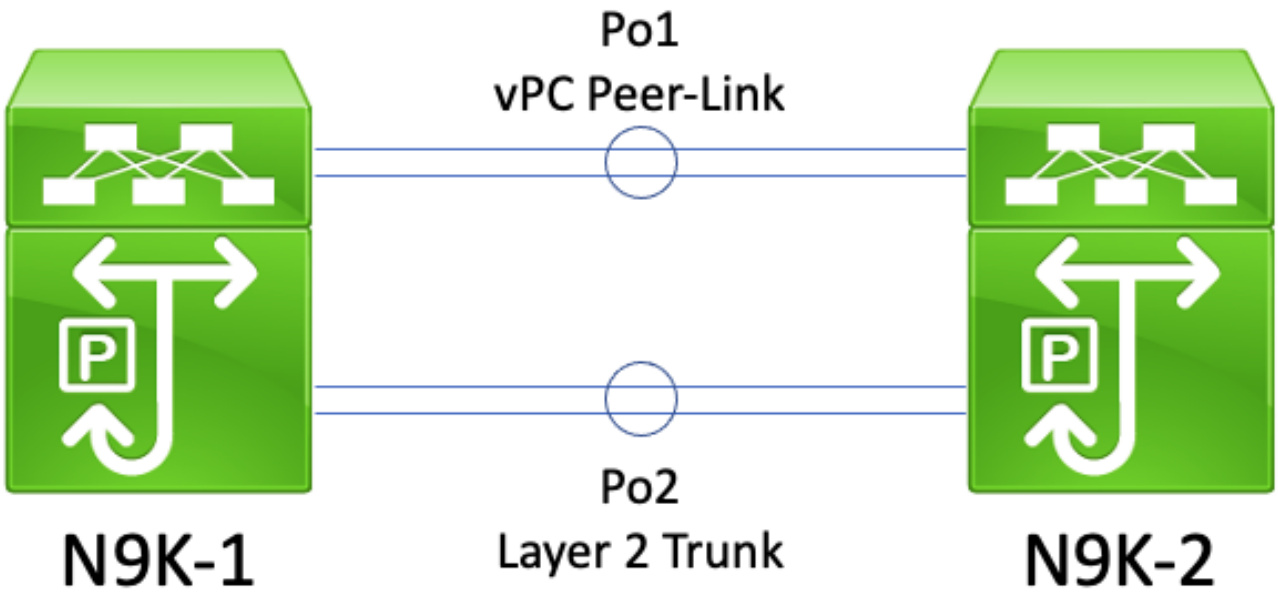
Voorafgaand aan het inschakelen van de Verbetering in vPC Peer Switch, moet u de prioriteitsconfiguratie van Spanning Tree voor VLAN's 1, 10 en 20 op N9K-2 aanpassen om de prioriteitsconfiguratie van Spanning Tree aan te passen voor dezelfde VLAN's op N9K-1. Hier wordt een voorbeeld van deze wijziging gegeven.

```
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
```

Effect van vPC-peerswitch op niet-vPC-VLAN's

Bekijk deze topologie:



In deze topologie hebben twee vPC peers (N9K-1 en N9K-2) twee Layer 2 trunks tussen hen - Po1 en Po2. Po1 is de vPC Peer-Link met vPC VLAN's, terwijl Po2 een Layer 2-trunk is met alle niet-vPC VLAN's. Als de Spanning Tree-prioriteitswaarden voor niet-vPC VLAN's die over Po2 worden gedragen, identiek zijn op N9K-1 en N9K-2, dan komt elke vPC-peer uit Spanning Tree BPDU-frames afkomstig van het vPC-systeem MAC-adres, dat op beide switches identiek is. Hierdoor lijkt N9K-1 zijn eigen Spanning Tree BPDU te ontvangen op Po2 voor elk niet-vPC VLAN, ook al is N9K-2 de switch die is ontstaan uit de Spanning Tree BPDU. Vanuit een Spanning Tree-perspectief plaatst N9K-1 Po2 in een blokkerende status voor alle niet-vPC VLAN's.

Dit is verwacht gedrag. Als u dit gedrag wilt voorkomen of dit probleem wilt omzeilen, moeten beide vPC-peers met verschillende Spanning Tree-prioriteitswaarden worden geconfigureerd op alle niet-vPC-VLAN's. Hierdoor kan één vPC-peer de root-brug worden voor het niet-vPC VLAN en kan Layer 2-trunk tussen vPC-peers worden overgezet naar een toegewezen Forwarding-status. Op dezelfde manier wordt Layer 2 trunk tussen vPC-peers door de externe vPC-peer naar een toegewezen rootstatus overgezet. Hierdoor kan verkeer in niet-vPC VLAN's over beide vPC-peers door Layer 2-trunk stromen.

Configuratie

Hier vindt u een voorbeeld van hoe de functie voor de vPC-peerswitch kan worden geconfigureerd.

In dit voorbeeld is N9K-1 geconfigureerd als de Spanning Tree root-brug voor VLAN's 1, 10 en 20 met een prioriteit van 0. N9K-2 is de secundaire Spanning Tree-root-brug voor VLAN's 1, 10 en 20 met een prioriteit van 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
```

Eerst moet de prioriteitsconfiguratie voor Spanning Tree voor N9K-2 worden gewijzigd, zodat deze identiek is aan die van N9K-1. Dit is een vereiste voor de vPC-peerswitch om te functioneren zoals verwacht. Als het MAC-adres van het systeem van N9K-2 lager is dan het MAC-adres van het systeem van N9K-1, dan maakt N9K-2 gebruik van de rol van root-brug voor het Spanning Tree-domein, dat ervoor zorgt dat andere bruggen in het Spanning Tree-domein hun lokale MAC-adrestabellen voor alle betrokken VLAN's doorspoelen. Een voorbeeld van dit verschijnsel ziet u hier.

```
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
```

Vervolgens kunnen we de functie vPC-peerswitch inschakelen via de configuratieopdracht **peer-switch** voor het vPC-domein. Dit verandert de Bridge ID binnen Spanning Tree BPDU's die door beide vPC-peers zijn gegenereerd, waardoor andere bruggen in het Spanning Tree-domein hun lokale MAC-adrestabellen voor alle getroffen VLAN's moeten doorspoelen.

```
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#
```

U kunt verifiëren of de functie vPC-peerswitch aan de verwachtingen voldoet door met de opdracht **show spanning-tree summary** te controleren of beide vPC-peers claimen de root-brug voor vPC-VLAN’s te zijn. Uit deze output moet ook blijken dat de functie vPC-peerswitch is ingeschakeld en operationeel is.

```
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
```

Gebruik de opdracht **show spanning-tree vlan {x}** om meer gedetailleerde informatie over een specifieke VLAN weer te geven. De switch met de rol Primary of Operational Primary vPC heeft alle interfaces in een Toegewezen Forwarding-staat. De switch die de secundaire of operationele secundaire vPC-rol heeft, heeft al zijn interfaces in een aangewezen doorsturen-status, behalve de vPC Peer-Link, die zich in een Root Forwarding-status bevindt. Het MAC-adres van het vPC-systeem dat in de output van **show vpc role** wordt weergegeven, is identiek aan de root-brug-id en brug-id van elke vPC-peer.

```
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
```

Ten slotte kunnen we het [hulpprogramma Ethanalyzer voor pakketvastlegging voor de besturingsplane] op een van beide vPC's gebruiken om te controleren of beide vPC-peers Spanning Tree-BPDU's genereren met een brug-id en root-brug-id die het MAC-adres van het vPC-systeem bevatten dat tussen beide vPC-peers wordt gedeeld.

```
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
```

Impact

De invloed van het inschakelen van de verbeteringen in de vPC Peer-Switch hangt af van de vraag of andere bruggen in het Spanning Tree-domein via een vPC met beide vPC-peers zijn verbonden of van de redundante verbinding met beide vPC-peers zonder vPC.

Redundant verbonden niet-vPC-bruggen

Als een niet via vPC verbonden brug met redundante links naar beide vPC-peers (zodat één link zich vanuit het perspectief van het Spanning Tree Protocol in een blokkeertoestand bevindt) een wijziging in de Spanning Tree-root-brug detecteert die wordt aangekondigd in Spanning Tree-BPDU's, kan de root-poort van de brug wisselen tussen de twee redundante interfaces. Dit kan er weer toe leiden dat andere aangewezen doorstuurinterfaces onmiddellijk overgaan in een blokkeertoestand en vervolgens de eindigetoestandsautomaat van het Spanning Tree Protocol doorlopen (blokkeren, leren en doorsturen) met onderbrekingen die het equivalent zijn van de geconfigureerde timer voor doorstuurvertraging voor het Spanning Tree Protocol (standaard 15 seconden). De wijziging van de root-poort en het daaropvolgende doorlopen van de eindigetoestandsautomaat van het Spanning Tree Protocol kan een aanzienlijke verstoring binnen het netwerk veroorzaken.

Het is vermeldenswaard dat deze impact optreedt wanneer de vPC peer die momenteel de root-brug is voor het Spanning Tree-domein offline gaat (zoals bij stroomuitval, hardwarestoringen of herladen). Dit gedrag heeft niet specifiek betrekking op de vPC-peerswitch. Het inschakelen van de vPC-peerswitch veroorzaakt alleen gedrag dat vanuit het perspectief van een Spanning Tree lijkt op het gedrag van een vPC-peer die offline gaat.

Via vPC verbonden bruggen

Als een met vPC verbonden bridge een wijziging in de Spanning Tree root-brug detecteert die wordt geadverteerd in Spanning Tree BPDU's, spoelt de bridge dynamisch aangeleerde MAC-adressen uit de MAC-adrestabel. Tijdens het configureren van de functie vPC Peer Switch kunt u dit gedrag waarnemen in de volgende twee scenario's:

1. Als Spanning Tree-prioriteitswaarden zijn geconfigureerd om overeen te komen tussen beide vPC-peers, kan de Spanning Tree-root-brug veranderen als de vPC-peer die daarvoor niet de root-brug was een lager MAC-adres heeft dan de vPC-peer die de root-brug was. Een voorbeeld van dit scenario wordt weergegeven in de sectie Configuratie van vPC-peerswitch van dit document.
2. Wanneer de functie voor vPC peer Switch is ingeschakeld via de opdracht voor **peer-switch** vPC-domeinconfiguratie, beginnen beide vPC-peers te werken als root-bruggen van het Spanning Tree-domein. Beide vPC-peers beginnen identieke Spanning Tree BPDU's te produceren die zichzelf bevestigen als de root-brug van het Spanning Tree-domein.

In de meeste scenario's en topologieën wordt geen dataplaat-impact waargenomen als resultaat van een van deze twee scenario's. Echter, voor een korte periode, data vliegtuig verkeer wordt

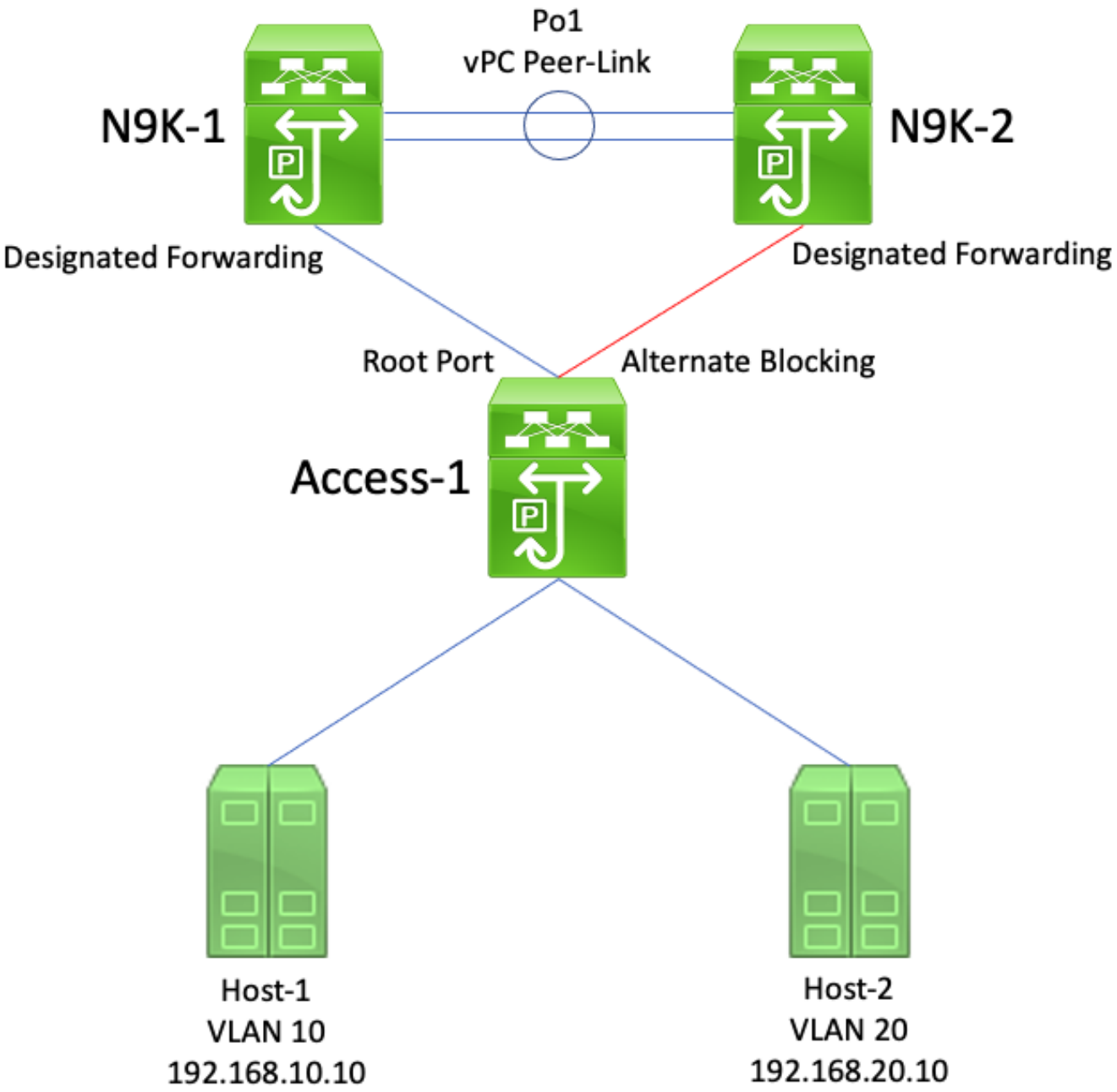
overstroomd binnen een VLAN als gevolg van onbekende unicast overstroming, als het doel MAC-adres van frames worden niet geleerd op een switchport als een direct resultaat van de flush van dynamisch-geleerde MAC-adressen. In sommige topologieën kan dit voor kortere perioden tot prestatieproblemen of pakketverlies leiden als dataplane-verkeer wordt geflood naar overbelaste netwerkapparaten binnen het VLAN. Dit kan ook problemen opleveren met bandbreedte-intensieve unidirectionele verkeersstromen of stille hosts (hosts die voornamelijk pakketten ontvangen en zelden pakketten verzenden), omdat dit verkeer binnen het VLAN voor een langere periode wordt overspoeld in plaats van dat het als normaal rechtstreeks naar de doelhost wordt geschakeld.

Het is de moeite waard om te vermelden dat deze impact gerelateerd is aan de flush van dynamisch geleerde MAC-adressen uit de MAC-adrestabel van bruggen binnen het aangetaste VLAN. Dit gedrag hoort niet specifiek bij de vPC-peerswitch of een wijziging in root-brug, maar kan ook worden veroorzaakt door een melding van een topologiewijziging die wordt gegenereerd omdat een niet-edge-poort wordt geactiveerd in het VLAN.

Voorbeelden van foutscenario's

Redundant verbonden niet-vPC-bruggen die de eindigetoestandsautomaat opnieuw opstarten

Bekijk deze topologie:



In deze topologie zijn N9K-1 en N9K-2 vPC-peers in een vPC-domein. N9K-1 is geconfigureerd met een Spanning Tree-prioriteitswaarde van 0 voor alle VLAN's waardoor het de root-brug is voor alle VLAN's. Omdat N9K-2 is geconfigureerd met een Spanning Tree-prioriteitswaarde van 4096 voor alle VLAN's, is dit de secundaire root-brug voor alle VLAN's. Access-1 is een switch die redundant met N9K-1 en N9K-2 is verbonden via een Layer 2-switchpoort. Omdat deze switchpoorten niet zijn gebundeld in een poortkanaal, plaatst het Spanning Tree Protocol de link verbonden met N9K-1 in een aangewezen root-toestand en de link verbonden met N9K-2 in een alternatieve blokkeertoestand.

Stelt u zich een storingsscenario voor waarbij N9K-1 offline gaat als gevolg van een hardwarestoring, stroomuitval of een reload van de switch. N9K-2 bevestigt zichzelf als de root-brug voor alle VLAN's door Spanning Tree BPDU's te adverteren met zijn systeem MAC-adres als de bridge-id. Access-1 ziet een wijziging in de ID van de root-brug. Bovendien is het de aangewezen Root poort overgangen naar een down/down staat, wat betekent dat de nieuwe toegewezen Root poort is de link die was in een alternatieve blokkerende staat tegenover N9K-2.

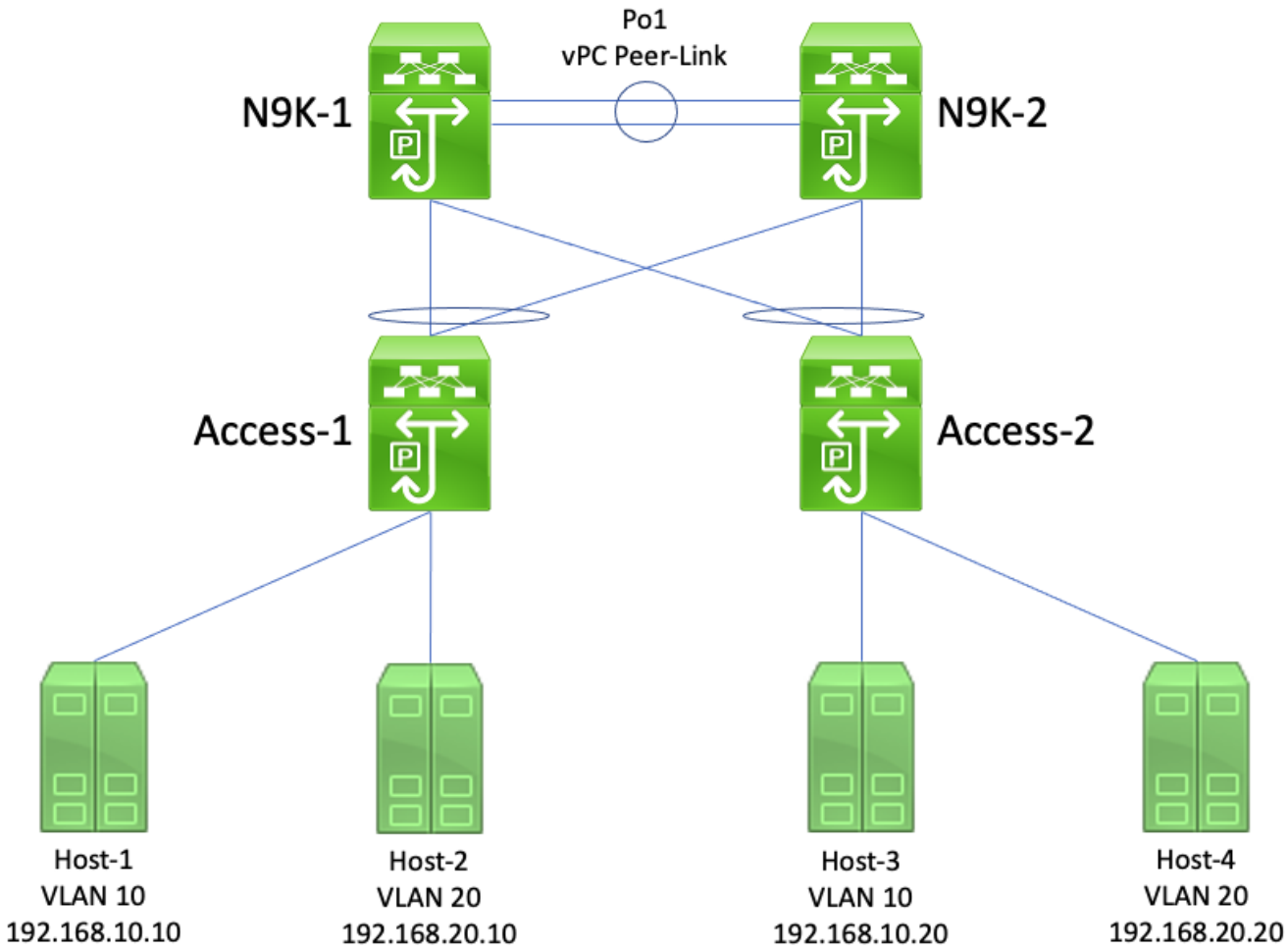
Deze verandering in de Toegewezen Poorten van de Root veroorzaakt alle niet-rand het Overspannen - de Poorten van de Boom aan stap door de Eindige staatsmachine van het

Spanning Tree Protocol (het Blokkeren, het Leren, en het Door:sturen) met pauzes binnen - tussen equivalent aan de gevormde Spanning Tree Protocol voorwaartse vertragingstimer (15 seconden door gebrek). Dit proces kan het netwerk ernstig ontwrichten.

In hetzelfde storingsscenario met de ingeschakelde verbetering van de vPC Peer Switch, verzenden zowel N9K-1 als N9K-2 identieke Spanning Tree BPDU's met behulp van het gedeelde vPC-systeem MAC-adres als de bridge-id. Als N9k-1 mislukt, blijft N9K-2 dezelfde Spanning Tree BPDU verzenden. Dientengevolge, overgaat access-1 onmiddellijk de Alternate Blocking link naar N9K-2 naar een Toegewezen Root staat en begint het doorsturen van verkeer over de link. Omdat de id van de Spanning Tree-root-brug niet verandert, hoeven niet-edge-poorten de eindigetoestandsautomaat van het Spanning Tree Protocol niet te doorlopen, waardoor de mate van ontwrichting in het netwerk beperkt blijft.

Via vPC verbonden bruggen die dynamisch geleerde MAC-adressen wissen

Bekijk deze topologie:



In deze topologie zijn N9K-1 en N9K-2 vPC-peers in een vPC-domein die routing tussen VLAN 10 en VLAN 20 uitvoeren. N9K-1 is geconfigureerd met een Spanning Tree-prioriteitswaarde van 0 voor VLAN 10 en VLAN 20, waardoor N9K-1 de root-brug voor beide VLAN's is. N9K-2 is geconfigureerd met een Spanning Tree-prioriteitswaarde van 4096 voor VLAN 10 en VLAN 20, waardoor het de secundaire root-brug is voor beide VLAN's. Host-1, Host-2, Host-3 en Host-4 communiceren allemaal doorlopend met elkaar.

Stelt u zich een storingsscenario voor waarbij N9K-1 offline gaat als gevolg van een hardwarestoring, stroomuitval of een reload van de switch. N9K-2 bevestigt zichzelf als de root-

brug voor VLAN 10 en VLAN 20 door Spanning Tree BPDU's te adverteren met behulp van zijn systeem MAC-adres als de bridge-id. Access-1 en Access-2 zien een wijziging in de ID van de root-brug, en hoewel de overspanningsboom hetzelfde blijft (wat betekent dat de vPC met betrekking tot N9K-1 en N9K-2 een toegewezen Root-poort blijft), vouwen zowel Access-1 als Access-2 hun MAC-adres van alle dynamisch aangeleerde MAC-adressen in VLAN 10 en VLAN 20.

In de meeste omgevingen heeft het wissen van dynamisch geleerde MAC-adressen minimale impact. Er gaan geen pakketten verloren (behalve die pakketten die naar N9K-1 werden verzonden terwijl het uitviel), maar verkeer wordt tijdelijk in elk broadcastdomein geflood als onbekend unicast verkeer terwijl alle switches in het broadcastdomein dynamische MAC-adressen opnieuw moeten leren.

Als in hetzelfde foutscenario de vPC-peerswitch is ingeschakeld, verzenden N9K-1 en N9K-2 identieke Spanning Tree-BPDU's, waarbij het gedeelde MAC-adres van het vPC-systeem als de brug-id dient. Als N9k-1 mislukt, blijft N9K-2 dezelfde Spanning Tree BPDU verzenden. Dientengevolge, zijn access-1 en access-2 zich er niet van bewust dat enige verandering in de Spanning Tree topologie heeft plaatsgevonden - vanuit hun perspectief, zijn de Spanning Tree BPDU's van de root-brug identiek, zodat is er geen behoefte om dynamisch-geleerde MAC-adressen van relevante VLAN's te spoelen. Zo wordt in dit foutscenario voorkomen dat er onbekend unicast verkeer in elk broadcastdomein wordt geflood.

vPC-peergateway

In deze sectie wordt de vPC-peergateway beschreven, een verbetering die wordt ingeschakeld met de configuratieopdracht **peer-gateway** voor het vPC-domein.

Overzicht

Nexus-switches die zijn geconfigureerd in een vPC-domein voeren doorstuurbewerkingen standaard uit met het dual-active First Hop Redundancy Protocol (FHRP). Dit betekent dat als een vPC-peer een pakket ontvangt met een MAC-adres van een Hot Standby Router Protocol (HSRP)- of Virtual Router Redundancy Protocol (VRRP)-groep die op de switch is geconfigureerd, de switch het pakket routeert volgens zijn lokale routeringstabel, ongeacht de status van het HSRP- of VRRP-besturingsplane. Met andere woorden, dit is verwacht gedrag voor een vPC-peer in een HSRP-standby- of VRRP-back-uptoestand om pakketten te routeren die bestemd zijn voor het virtuele MAC-adres voor HSRP of VRRP.

Wanneer een vPC peer een pakket routeert dat bestemd is voor een FHRP virtueel MAC-adres, herschrijft het pakket met een nieuw bron- en doelMAC-adres. Het MAC-adres van de bron is het MAC-adres van de Switched Virtual Interface (SVI) van de vPC-peer in het VLAN waarin het pakket wordt gerouteerd. Het MAC-adres van de bestemming is het MAC-adres dat gekoppeld is aan het IP-adres van de volgende hop voor het IP-adres van de bestemming van het pakket volgens de lokale routeringstabel van de vPC-peer. In inter-VLAN-routeringsscenario's is het MAC-adres van de bestemming van het pakket nadat het pakket is herschreven het MAC-adres van de host waarnaar het pakket uiteindelijk is bestemd.

Sommige hosts volgen niet het standaardgedrag voor doorsturen als een optimalisatiefunctie. Bij dit gedrag voert de host bij het beantwoorden van een inkomend pakket geen lookup uit op een routingtabel en/of ARP-cache. In plaats daarvan verwisselt de host het bron- en bestemmings-MAC-adres van het inkomende pakket voor het antwoordpakket. Met andere woorden, het bron-

MAC-adres van het inkomende pakket wordt het bestemmings-MAC-adres van het antwoordpakket en het bestemmings-MAC-adres van het inkomende pakket wordt het bron-MAC-adres van het antwoordpakket. Dit gedrag verschilt van een host die het standaardgedrag voor doorsturen volgt, waarbij een lookup in een lokale routingtabel en/of ARP-cache wordt uitgevoerd en het bestemmings-MAC-adres van het antwoordpakket wordt ingesteld op het virtuele MAC-adres voor FHRP.

Dit niet-standaardgedrag van de host kan de vPC-regel voor het voorkomen van lussen schenden als het gegenereerde antwoordpakket door de host is geadresseerd aan één vPC-peer, maar de vPC wordt uitgevoerd naar de andere vPC-peer. De andere vPC-peer ontvangt het pakket dat bestemd is voor een MAC-adres dat eigendom is van de vPC-peer en stuurt het pakket door vanuit de vPC-peer-link naar de vPC-peer die eigenaar is van het MAC-adres in het doelveld van het MAC-adres van het pakket. De vPC peer die eigenaar is van het MAC-adres probeert het pakket lokaal te beheren. Als het pakket een vPC moet verlaten, laat de vPC peer dit pakket vallen voor het overtreden van de vPC-loopvermijdingsregel. Als gevolg daarvan kunnen zich connectiviteitsproblemen voordoen of kan er pakketverlies optreden voor sommige stromen die afkomstig zijn van of bestemd zijn voor een host die gebruikmaakt van dit niet-standaardgedrag.

De vPC-peergateway is geïntroduceerd om het pakketverlies te voorkomen als gevolg van hosts die dit niet-standaardgedrag vertonen. Dit wordt gedaan door het één vPC-peer toe te staan om pakketten bestemd voor het MAC-adres van de andere vPC-peer lokaal te routeren, zodat pakketten bestemd voor de externe vPC-peer de vPC-peerlink niet hoeven te verlaten om gerouteerd te worden. Met andere woorden, met de vPC-peergateway kan één vPC-peer pakketten namens de externe vPC-peer routeren. De vPC-peergateway kan worden ingeschakeld met de configuratieopdracht **peer-gateway** voor het vPC-domein.

Voorbehouden

Fluctuatie van aangrenzingen van unicast routingprotocollen via vPC's of vPC-VLAN's

Als dynamische aangrenzingen van unicast routingprotocollen worden gevormd tussen twee vPC-peers en een via vPC verbonden router of een router die is verbonden via een vPC-orphan-poort, kunnen de aangrenzingen van routingprotocollen na inschakeling van de vPC-peergateway voortdurend fluctueren als niet ook direct daarna routing/Layer 3 via vPC wordt geconfigureerd. Deze foutscenario's worden gedetailleerd beschreven in de secties Voorbeeld van foutscenario met aangrenzingen van unicast routingprotocollen via een vPC met vPC-peergateway en Aangrenzingen van unicast routingprotocollen via een vPC-VLAN met vPC-peergateway van dit document.

U lost dit probleem op door routing/Layer 3 via vPC in te schakelen met de configuratieopdracht **layer3 peer-router** voor het vPC-domein, direct nadat u de vPC-peergateway heeft ingeschakeld met de configuratieopdracht **peer-gateway** voor het vPC-domein.

Automatische uitschakeling van ICMP- en ICMPv6-omleidingen

Wanneer de verbetering van de vPC Peer Gateway is ingeschakeld, wordt de generatie van ICMP- en ICMPv6 Redirect-pakketten automatisch uitgeschakeld op alle vPC VLAN SVI's (dat wil zeggen, elke SVI die is gekoppeld aan een VLAN dat via de vPC Peer-Link is getrunkt). De switch doet dit door **no ip redirects** en **no ipv6 redirects** te configureren op alle SVI's voor vPC-VLAN's. Zo wordt voorkomen dat een switch ICMP-omleidingspakketten genereert in antwoord op pakketten die binnenkomen bij de switch, maar een bestemmings-MAC- en IP-adres van de vPC-

peer van de switch hebben.

Als ICMP- of ICMPv6 Redirect-pakketten nodig zijn in uw omgeving binnen een specifiek VLAN, moet u dit VLAN uitsluiten van voordeel te halen uit de verbetering van de vPC Peer Gateway met behulp van de opdracht voor de configuratie van het vPC-domein voor **peer-gateway exclusiviteit-VLAN <vlan-id>** vPC.

> **Opmerking**: de opdracht voor **configuratie van** vPC-domeinen met **peer-gateway** uitsluitings-**VLAN** wordt niet ondersteund op Nexus 9000 Series switches.

Configuratie

Hier vindt u een voorbeeld van hoe de functie voor de vPC-peergateway kan worden geconfigureerd.

In dit voorbeeld zijn N9K-1 en N9K-2 vPC-peers in een vPC-domein. Beide vPC-peers hebben een HSRP-groep geconfigureerd voor VLAN 10. N9K-1 is de HSRP Active router met een prioriteit van 150, terwijl N9K-2 de HSRP Standby router is met de standaardprioriteit van 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)
```

De SVI van VLAN 10 van N9K-1 heeft het MAC-adres 00ee.ab67.db47 en de SVI van VLAN 10 van N9K-2 heeft als MAC-adres 00ee.abd8.747f. Het virtuele HSRP MAC-adres voor VLAN 10 is 0000.0c07.ac0a. In deze staat zijn het MAC-adres van de SVI voor VLAN 10 van elke switch en het virtuele MAC-adres voor HSRP aanwezig in de MAC-adrestabel van elke switch. Het VLAN 10 SVI MAC-adres van elke switch en het HSRP Virtual MAC-adres bevatten de Gateway (G)-vlag, die aangeeft dat de switch lokaal pakketten routeert die bestemd zijn voor dit MAC-adres.

In de MAC-adrestabel van N9K-1 ontbreekt de Gateway-markering voor het MAC-adres van de SVI voor VLAN 10 van N9K-2. En in de MAC-adrestabel van N9K-2 ontbreekt de Gateway-markering voor het MAC-adres van de SVI voor VLAN 10 van 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)
```

We kunnen de vPC-peergateway inschakelen met de configuratieopdracht peer-gateway voor het vPC-domein. Hierdoor kan de switch de ontvangen pakketten lokaal routeren met een doeladres van MAC dat behoort tot het MAC-adres van hun vPC-peer dat op de vPC Peer-Link is geleerd. Hiervoor moet de Gateway-markering voor het MAC-adres van de vPC-peer worden ingesteld in de MAC-adrestabel van de 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#
```

U kunt controleren of de vPC-peergateway werkt zoals verwacht door te controleren of de Gateway-markering aanwezig is in de MAC-adrestabel voor de vPC-peer.

```
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)
```

Impact

De gevolgen van het inschakelen van de verbetering van de vPC Peer Gateway kunnen verschillen afhankelijk van de omliggende topologie en het gedrag van verbonden hosts zoals beschreven in de volgende subsecties. Als geen van de volgende subsecties van toepassing is op uw omgeving, dan is de verbetering van de vPC Peer Gateway niet storend en heeft deze geen invloed op uw omgeving.

Fluctuatie van aangrenzingen van unicast routingprotocollen via vPC's of vPC-VLAN's

Als dynamische aangrenzingen van unicast routingprotocollen worden gevormd tussen twee vPC-peers en een via vPC verbonden router of een router die is verbonden via een vPC-orphan-poort, kunnen de aangrenzingen van routingprotocollen na inschakeling van de vPC-peergateway voortdurend fluctueren als niet ook direct daarna routing/Layer 3 via vPC wordt geconfigureerd. Deze foutscenario's worden gedetailleerd beschreven in de secties Voorbeeld van foutscenario met aangrenzingen van unicast routingprotocollen via een vPC met vPC-peergateway en Aangrenzingen van unicast routingprotocollen via een vPC-VLAN met vPC-peergateway van dit document.

U lost dit probleem op door routing/Layer 3 via vPC in te schakelen met de configuratieopdracht **layer3 peer-router** voor het vPC-domein, direct nadat u de vPC-peergateway heeft ingeschakeld met de configuratieopdracht **peer-gateway** voor het vPC-domein.

Automatische uitschakeling van ICMP- en ICMPv6-omleidingen

Wanneer de verbetering van de vPC Peer Gateway is ingeschakeld, wordt de generatie van ICMP- en ICMPv6 Redirect-pakketten automatisch uitgeschakeld op alle vPC VLAN SVI's (dat wil zeggen, elke SVI die is gekoppeld aan een VLAN dat via de vPC Peer-Link is getrunkt). De switch doet dit door **no ip redirects** en **no ipv6 redirects** te configureren op alle SVI's voor vPC-VLAN's. Zo wordt voorkomen dat een switch ICMP-omleidingspakketten genereert in antwoord op pakketten die binnenkomen bij de switch, maar een bestemmings-MAC- en IP-adres van de vPC-peer van de switch hebben.

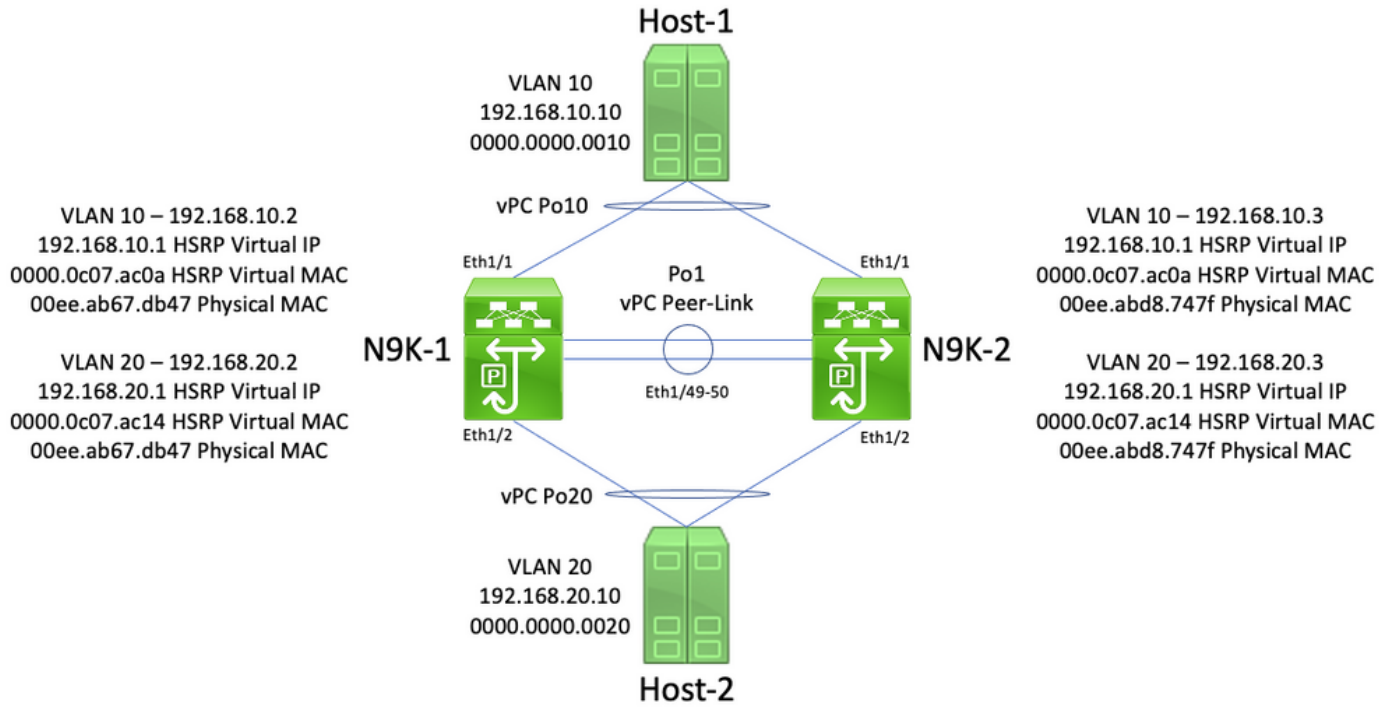
Als ICMP- of ICMPv6 Redirect-pakketten nodig zijn in uw omgeving binnen een specifiek VLAN, moet u dit VLAN uitsluiten van voordeel te halen uit de verbetering van de vPC Peer Gateway met behulp van de opdracht voor de configuratie van het vPC-domein voor **peer-gateway exclusiviteit-VLAN <vlan-id>** vPC.

> **Opmerking**: de opdracht voor **configuratie van** vPC-domeinen met **peer-gateway** uitsluitings-**VLAN** wordt niet ondersteund op Nexus 9000 Series switches.

Voorbeelden van foutscenario's

Via vPC verbonden hosts met niet-standaardgedrag bij doorsturen

Bekijk deze topologie:

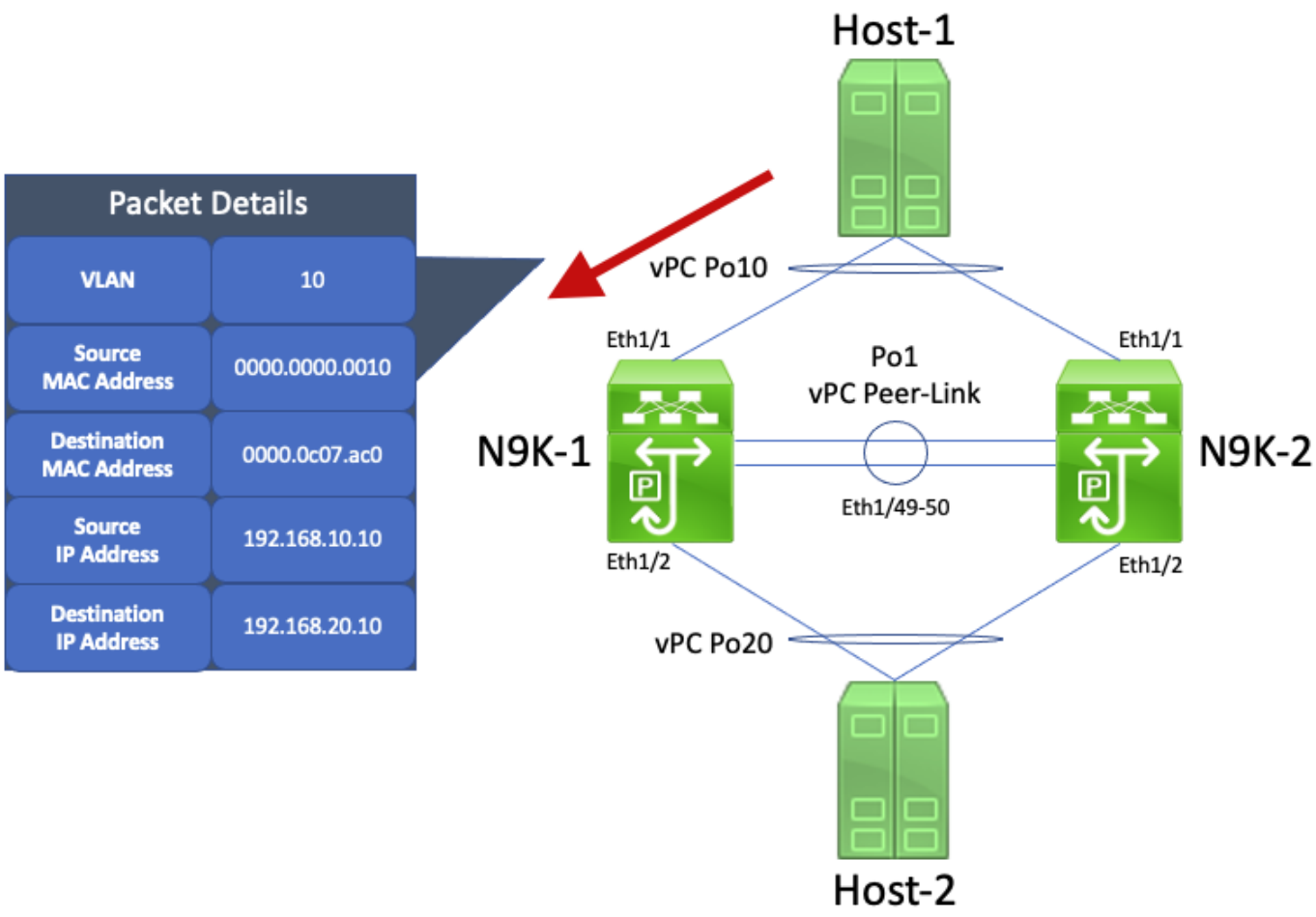


In deze topologie zijn N9K-1 en N9K-2 vPC-peers in een vPC-domein die routing tussen VLAN 10 en VLAN 20 uitvoeren. Interface Po1 is de vPC-peerlink. Een host met de naam Host-1 wordt aangesloten via vPC Po10 met N9K-1 en N9K-2 in VLAN 10. Host-1 bezit een IP-adres van 192.168.10.10 met een MAC-adres van 0000.000.0010. Een host met de naam Host-2 wordt via vPC Po20 verbonden met N9K-1 en N9K-2 in VLAN 20. Host-2 heeft een IP-adres van 192.168.20.10 met een MAC-adres van 0000.000.0020.

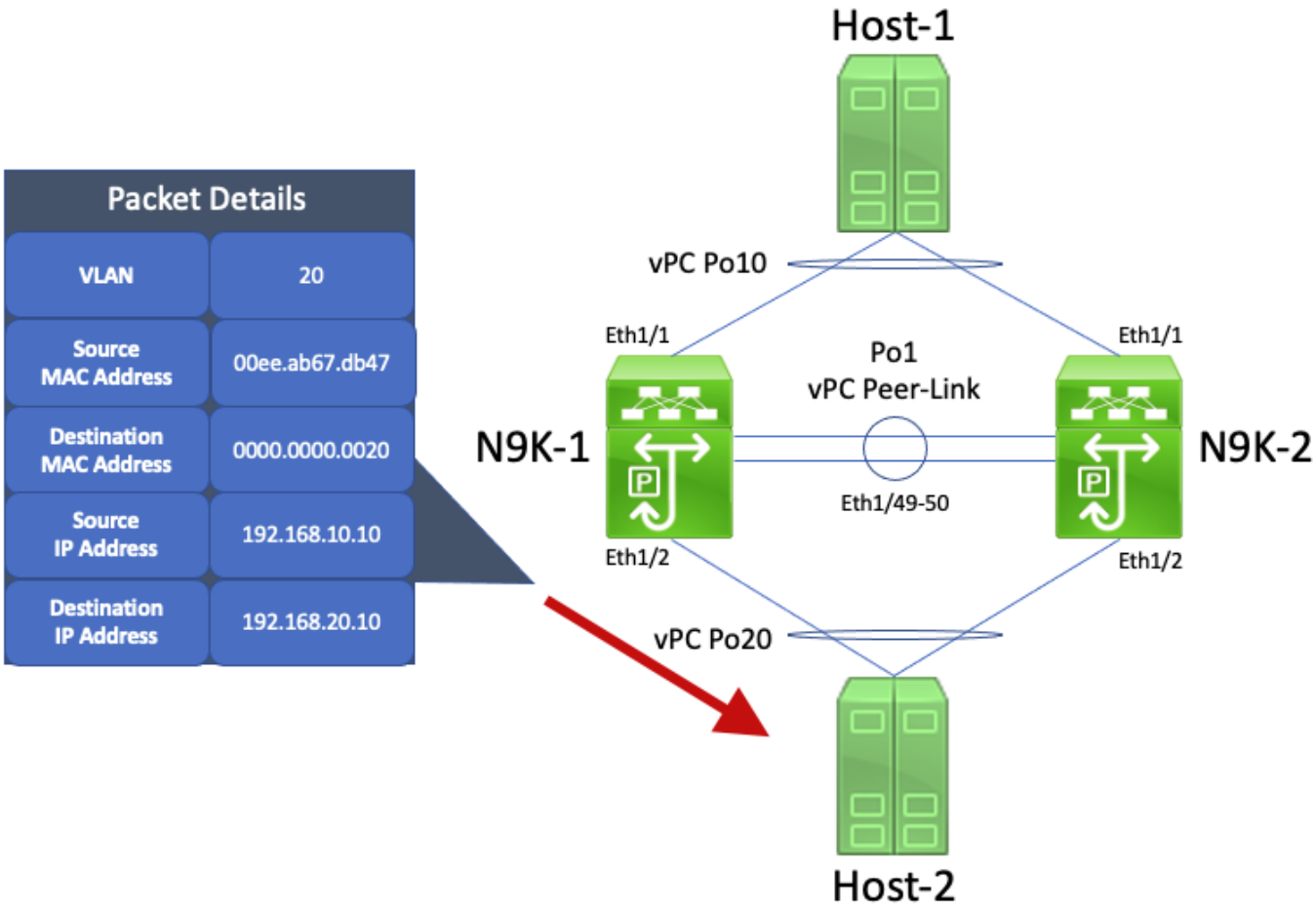
N9K-1 en N9K-2 hebben beide SVI's in VLAN 10 en VLAN 20, en onder elke SVI is HSRP geactiveerd. De VLAN 10-interface van N9K-1 heeft een IP-adres van de VLAN 20-interface met

192.168.10.2 en de VLAN 20-interface met N9K-1 heeft een IP-adres van 192.168.20.2. Beide SVI's van N9K-1 hebben een fysiek MAC-adres van 00ee.ab67.db47. De VLAN 10-interface van N9K-2 heeft een IP-adres van de VLAN 20-interface van 1921.68.10.3 en de VLAN 20-interface van N9K-2 heeft een IP-adres van 192.168.20.3. Beide SVI's van N9K-2 hebben een fysiek MAC-adres van 00ee.abd8.747f. Het virtuele HSRP IP-adres voor VLAN 10 is 192.168.10.1, het virtuele MAC-adres voor HSRP is 0000.0c07.ac0a. Het virtuele HSRP IP-adres voor VLAN 20 is 192.168.20.1, het virtuele MAC-adres voor HSRP is 0000.0c07.ac14.

Overweeg een scenario waar host-1 een ICMP Echo-verzoekpakket naar host-2 stuurt. Nadat Host-1 ARP oplost voor zijn standaardgateway (het virtuele IP-adres van HSRP), volgt Host-1 standaard doorsturen gedrag en genereert een ICMP Echo request-pakket met een IP-bronadres van 192.168.10.10, een IP-adres van bestemming van 192.168.20.10, een MAC-adres van bron van 000.000.0010 en een MAC-adres van bestemming van 0000.0c07.ac0a0a0a0a0a0a0a Dit pakket gaat naar N9K-1. Een visueel voorbeeld hiervan ziet u hier.

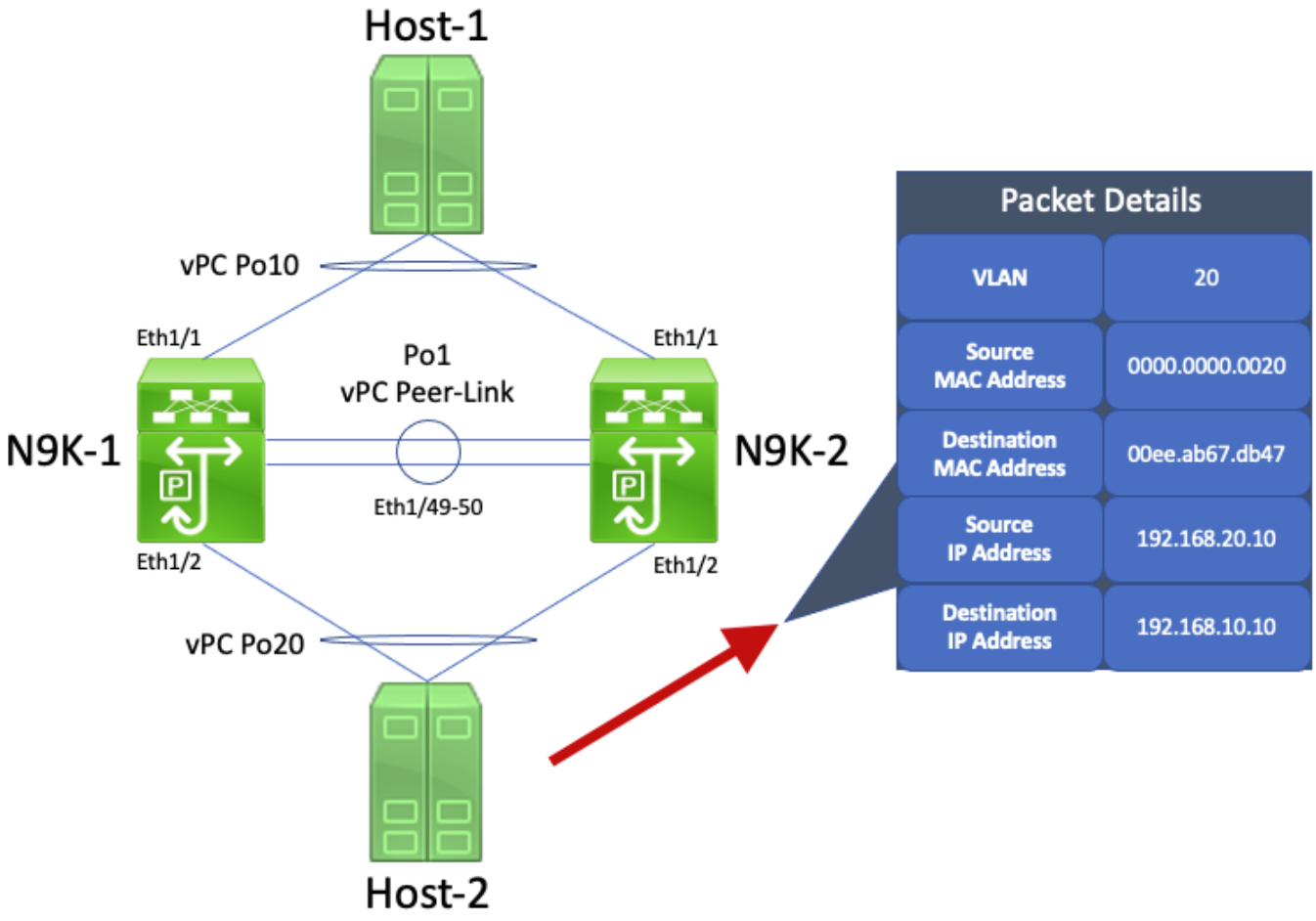


N9K-1 ontvangt dit pakket. Aangezien dit pakket bestemd is voor het virtuele MAC-adres voor HSRP, kan N9K-1 dit pakket routeren op basis van de lokale routingtabel, ongeacht de staat van de HSRP-besturingsplane. Dit pakket wordt van VLAN 10 naar VLAN 20 gerouteerd. Als deel van het routeren van het pakket, voert N9K-1 pakketherschrijven uit door de bron en de bestemmingsMAC- adresvelden van het pakket opnieuw te richten. Het nieuwe MAC-adres van de bron van het pakket is het fysieke MAC-adres dat is gekoppeld aan N9K-1 VLAN 20 SVI (00ee.ab67.db47) en het nieuwe MAC-adres van de bestemming is het MAC-adres dat is gekoppeld aan host-2 (000.000.0020). Een visueel voorbeeld hiervan ziet u hier.

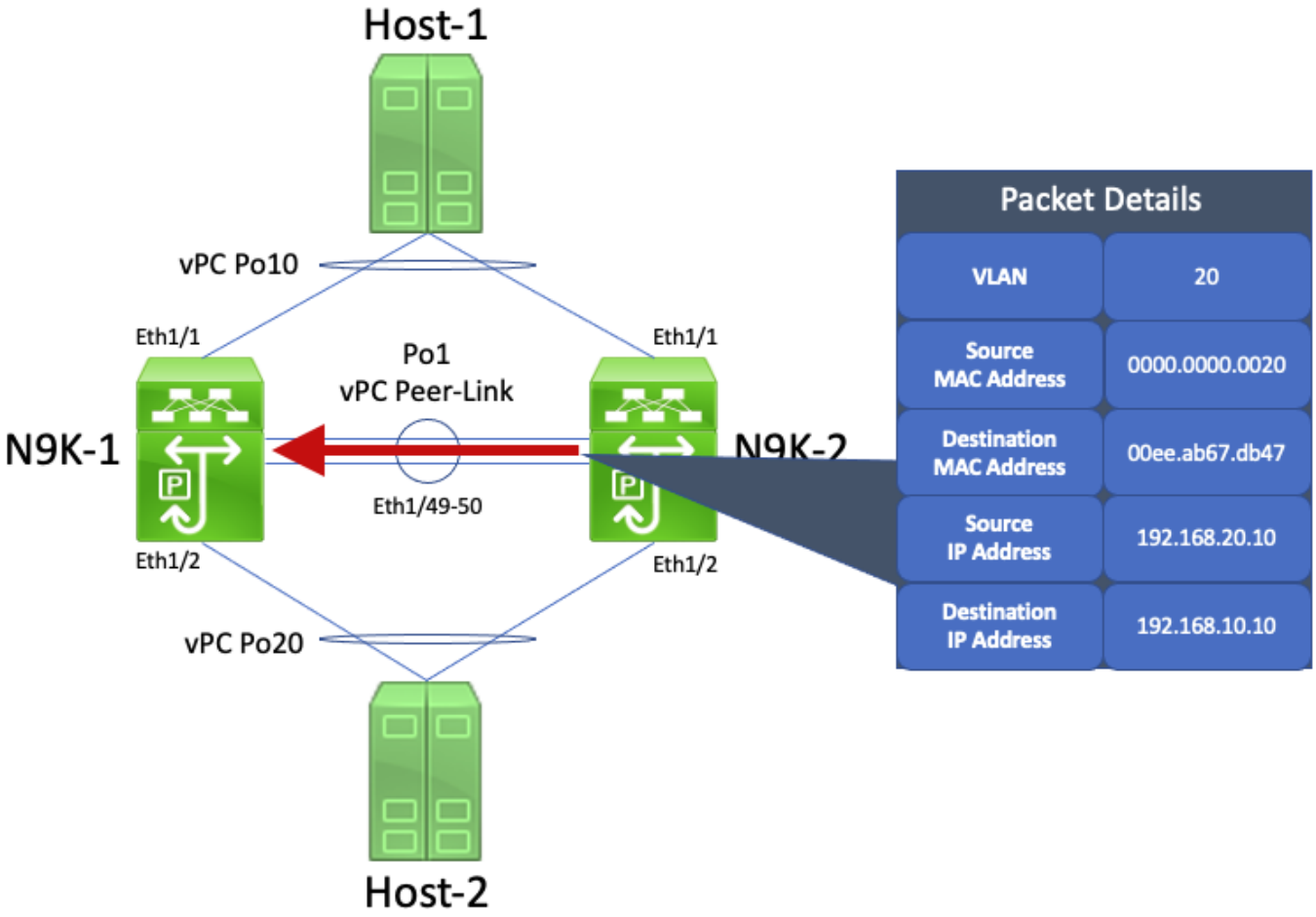


Host-2 ontvangt dit pakket en genereert een ICMP-pakket met een echoantwoord voor het ICMP-pakket met een echoaanvraag van Host-1. Host-2 volgt echter niet altijd het standaardgedrag voor doorsturen. Om het doorsturen te optimaliseren, voert Host-2 geen lookup in de routingtabel of ARP-cache uit voor het IP-adres van Host-1 (192.168.10.10). In plaats daarvan worden de velden voor het bron- en bestemmings-MAC-adres van het ICMP-pakket met de echoaanvraag dat Host-2 oorspronkelijk ontving, omgewisseld. Dientengevolge, heeft het pakket van het Antwoord van de ICMP-Echo dat door host-2 wordt geproduceerd een bronIP adres van 192.168.20.10, een bestemmingsIP adres van 192.168.10.10, een adres bron van MAC van 0000.0000.0020, en een adres van bestemmingsMAC van 00ee.ab67.db47.

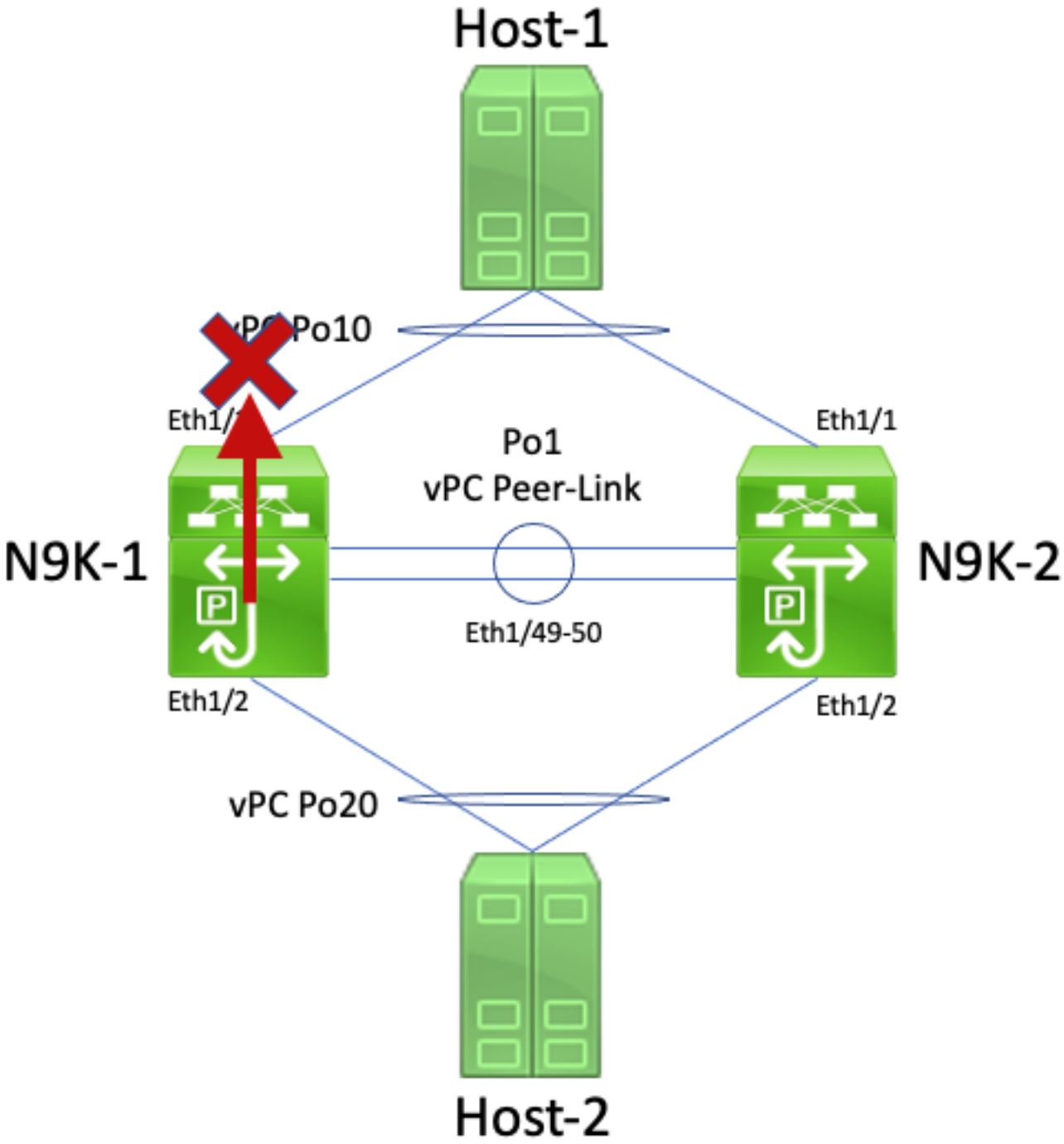
Als dit pakket van het Antwoord van ICMP Echo naar N9K-1 gaat, wordt dit pakket door:sturen naar host-1 zonder probleem. Het is een ander verhaal als dit ICMP-pakket met de echoaanvraag wordt uitgevoerd naar N9K-2, zoals hier wordt weergegeven.



N9K-2 ontvangt dit pakket. Aangezien dit pakket bestemd is voor het fysieke MAC-adres van N9K-1's VLAN 20 SVI, stuurt N9K-2 dit pakket door via de vPC Peer-Link naar N9K-1, aangezien N9K-2 dit pakket niet kan routeren namens N9K-1. Een visueel voorbeeld hiervan ziet u hier.



N9K-1 ontvangt dit pakket. Aangezien dit pakket bestemd is voor het fysieke MAC-adres van de SVI van VLAN 20 van N9K-1, kan N9K-1 dit pakket routeren op basis van de lokale routingtabel, ongeacht de staat van de HSRP-besturingsplane. Dit pakket wordt van VLAN 20 naar VLAN 10 gerouteerd. De uitgangsinterface voor deze route gaat echter over op vPC Po10, dat is ingesteld op N9K-2. Dit is een schending van de vPC Loop Avoidance-regel - als N9K-1 een pakket ontvangt via de vPC Peer-Link, kan N9K-1 dat pakket niet doorsturen vanuit een vPC-interface als dezelfde vPC-interface actief is op N9K-2. N9K-1 laat dit pakket vallen als gevolg van deze overschrijding. Een visueel voorbeeld hiervan ziet u hier.



U kunt dit probleem oplossen door de vPC-peergateway in te schakelen met de configuratieopdracht **peer-gateway** voor het vPC-domein. Hierdoor kan N9K-2 het ICMP Echo Reply-pakket (en andere op dezelfde manier geadresseerde pakketten) namens N9K-1 sturen, ook al is het doeladres van het MAC van het pakket eigendom van N9K-1 en niet van N9K-2. Hierdoor kan N9K-2 dit pakket doorsturen vanuit de vPC Po10 interface in plaats van het door te sturen via de vPC Peer-Link.

Routing/Layer 3 via vPC (Layer3 peer-router)

In deze sectie wordt de functie voor routing/Layer 3 via vPC beschreven, een verbetering die wordt ingeschakeld met de configuratieopdracht **layer3 peer-router** voor het vPC-domein.

Opmerking: Het vormen van nabijheid van multicast-routingprotocollen (namelijk Protocol Independent Multicast [PIM]-nabijheid) over een vPC wordt niet ondersteund met de ingeschakeld verbetering van Routing/Layer 3 over vPC.

Overzicht

In sommige cloudomgevingen willen klanten een router via vPC verbinden met een paar Nexus-switches en via de vPC aangrenzingen van unicast routingprotocollen vormen met beide vPC-peers. Als alternatief kunnen klanten een router via een vPC-VLAN verbinden met een enkele vPC-peer en via het vPC-VLAN aangrenzingen van unicast routingprotocollen vormen met beide vPC-peers. Als gevolg daarvan maakt de via vPC verbonden router gebruik van ECMP (Equal-Cost Multi-Path) voor voorvoegsels die door beide Nexus-switches worden aangekondigd. Dit kan de voorkeur verdienen boven het gebruik van speciale routinglinks tussen de vPC-router en beide vPC-peers om op IP-adresgebruik te besparen (drie IP-adressen nodig in plaats van vier) of de complexiteit van de configuratie te beperken (gerouteerde interfaces naast SVI's, vooral in VRF-Lite-omgevingen die subinterfaces nodig hebben).

Tot voor kort werd het vormen van aangrenzingen van unicast routingprotocollen via een vPC niet ondersteund op Cisco Nexus-platforms. Klanten kunnen echter een topologie hebben geïmplementeerd waarbij zonder probleem via een vPC aangrenzingen van unicast routingprotocollen worden gevormd, ook al worden ze niet ondersteund. Na een wijziging in het netwerk, zoals een software-upgrade van de via vPC verbonden router of de vPC-peers zelf, een firewall-failover, enzovoort, werken de aangrenzingen van unicast routingprotocollen via een vPC niet meer, wat resulteert in pakketverlies voor dataplane-verkeer of ertoe leidt dat aangrenzingen van unicast routingprotocollen met één of beide vPC-peers niet meer online komen. In de sectie Voorbeelden van foutscenario's van dit document worden de technische details achter deze foutscenario's beschreven en wordt aangegeven waarom deze scenario's niet worden ondersteund.

De functie voor routing/Layer 3 via vPC is geïntroduceerd om ondersteuning te bieden voor het vormen van aangrenzingen van unicast routingprotocollen via een vPC. Dit wordt gedaan door toe te staan dat unicast routingprotocolpakketten met een TTL van 1 via de vPC-peerlink worden doorgestuurd zonder de TTL van het pakket te verlagen. Het resultaat is dat zonder problemen aangrenzingen van unicast routingprotocollen kunnen worden gevormd via een vPC of vPC-VLAN. Direct nadat u de vPC-peergateway heeft ingeschakeld met de configuratieopdracht **peer-gateway**, kunt u routing/Layer 3 via vPC inschakelen met de configuratieopdracht **layer3 peer-router** voor het vPC-domein.

In tabel 2, Routing Protocols Adjacencies Support over vPC VLANs (Ondersteuning voor aangrenzingen van routingprotocollen via vPC-VLAN's), van het document Supported Topologies for Routing over Virtual Port Channel on Nexus Platforms (Ondersteunde topologieën voor routing via virtueel poortkanaal op Nexus-platforms) wordt aangegeven in welke NX-OS-softwarereleases ondersteuning voor routing/Layer 3 via vPC is toegevoegd voor elk Cisco Nexus-platform.

Voorbehouden

Incidentele VPC-2-L3_VPC_UNEQUAL_WEIGHT-syslogs

Nadat de verbetering van Routing/Layer 3 over vPC is ingeschakeld, beginnen beide vPC-peers elk uur systemen te genereren die vergelijkbaar zijn met een van de volgende:

```
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
```

Geen van deze syslogs duidt op een probleem met de switch. Deze syslogs zijn waarschuwingen voor de beheerder dat de configuratie, kosten en het gewicht van de routing op beide vPC-peers identiek moeten zijn als routing/Layer 3 via vPC is ingeschakeld om te kunnen waarborgen dat vPC-peers verkeer op identieke wijze kunnen routeren. Het hoeft niet te betekenen dat de configuratie, kosten of het gewicht op een van beide vPC-peers onjuist is geconfigureerd.

Deze syslogs kunnen via de onderstaande configuratie worden uitgeschakeld.

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

Deze configuratie moet op beide vPC-peers worden uitgevoerd om de syslog op beide vPC-peers uit te schakelen.

Gegevensverkeer met TTL van 1-software doorgestuurd vanwege Cisco-bug-id CSCvs82183 en Cisco-bug-id CSCvw16965

Wanneer Routing/Layer 3 over vPC-verbetering is ingeschakeld op Nexus 9000 Series switches die zijn uitgerust met een Cloud Scale ASIC die voorafgaand aan NX-OS softwarerelease 9.3(6) een NX-OS-softwarerelease uitvoert, wordt dataplaat-verkeer dat niet is gekoppeld aan een unicast-routingprotocol met een TTL van 1 naar de supervisor gestraft en in software in plaats van hardware doorgestuurd. Afhankelijk van het feit of de Nexus-switch een vaste chassiskabel (ook wel "Rackmontage" genoemd) of een modulaire switch switch (ook "Einde van Rij" genoemd) is, evenals de huidige NX-OS softwarerelease van de switch, kan de oorzaak van dit probleem worden toegeschreven aan een softwarestoring Cisco bug ID CSCvs82183 Voor softwaredefect Cisco-bug-id CSCvw16965 . Beide softwaredefecten hebben alleen invloed op Nexus 9000 Series switches die zijn uitgerust met een Cloud Scale ASIC - geen van de andere Cisco Nexus hardwareplatforms wordt beïnvloed door een van beide problemen. Raadpleeg de specifieke informatie voor de afzonderlijke softwaredefecten voor meer informatie.

Cisco raadt u aan een upgrade naar NX-OS-softwarerelease 9.3(6) of hoger uit te voeren om deze softwarefouten te voorkomen. Cisco raadt u aan regelmatig te upgraden naar de momenteel aanbevolen NX-OS-softwarerelease voor de Nexus 9000 Series switch waarnaar wordt verwezen in het document Aanbevolen Cisco NX-OS-releases voor Cisco Nexus 9000 Series switches.

Configuratie

Hier vindt u een voorbeeld van hoe routing/Layer 3 via vPC kan worden geconfigureerd.

In dit voorbeeld zijn N9K-1 en N9K-2 vPC-peers in een vPC-domein. Voor beide vPC-peers is de vPC-peergateway al ingeschakeld, een vereiste om routing/Layer 3 via vPC te kunnen inschakelen. Beide vPC-peers hebben een SVI in VLAN 10, die is ingeschakeld onder OSPF-proces 1. N9K-1 en N9K-3 zitten vast in een OSPF EXSTART/EXCHANGE-status met een vPC-verbonden OSPF-router met een IP-adres en buurid van 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
```

We kunnen routing/Layer 3 via vPC inschakelen met de configuratieopdracht **layer3 peer-router** voor het vPC-domein. Dit voorkomt dat een vPC-peer de TTL van unicast Routing Protocol-pakketten verlaagt die zijn gerouteerd als gevolg van het feit dat de vPC Peer Gateway-verbetering is ingeschakeld.

```
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#
```

U kunt verifiëren of routing/Layer 3 via vPC naar behoren werkt door te controleren of de OSPF-aangrenzing met de via vPC verbonden OSPF-neighbor kort na het inschakelen van routing/Layer 3 via vPC overgaat in de toestand FULL.

```
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
```

Impact

Het inschakelen van routing/Layer 3 via vPC heeft geen inherente impact op het vPC-domein. Dit betekent dat wanneer u de verbetering Routing/Layer 3 over vPC inschakelt, geen vPC-peer eventuele vPC's opschort of enig verkeer van dataplane inherent wordt beïnvloed door het inschakelen van deze verbetering.

Als aangrenzingen van protocollen voor dynamische routing die voorheen niet actief waren omdat routing/Layer 3 via vPC niet was ingeschakeld, plotseling wel actief worden als gevolg van het inschakelen van deze verbetering, kan er sprake zijn van enige ontwrichting bij het inschakelen van routing/Layer 3 via vPC, afhankelijk van de rol van de betreffende aangrenzingen van het

routingprotocol, de specifieke voorvoegsels die via deze aangrenzingen worden aangekondigd en de huidige toestand van de unicast routingtabel.

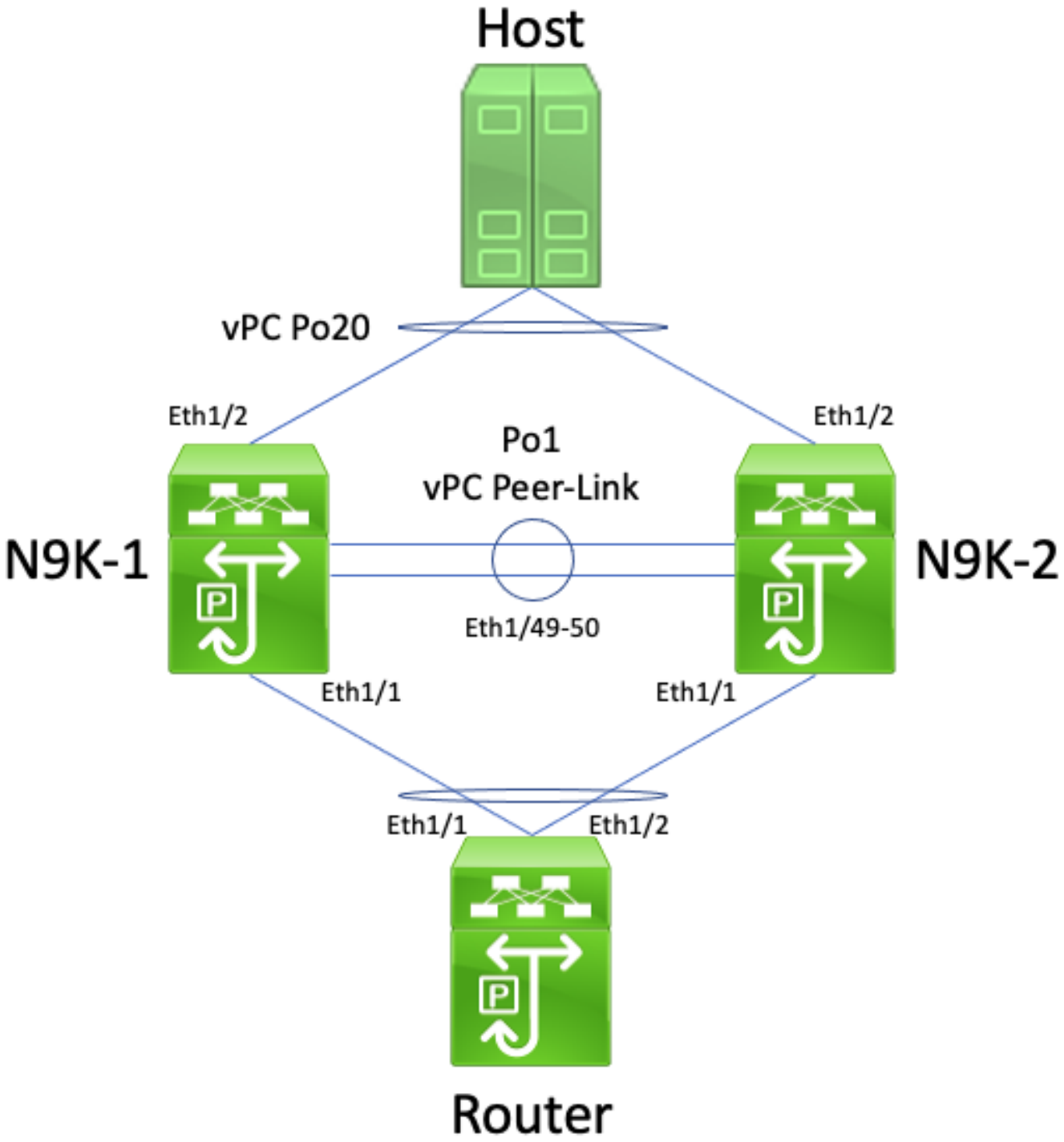
Om deze reden adviseert Cisco dat klanten deze verbetering tijdens een onderhoudsvenster mogelijk maken in de verwachting dat er sprake kan zijn van ontwrichting van besturingsplane en dataplane, tenzij klanten er zeer zeker van zijn dat de gevolgen van de aangetaste routingprotocolnabijheid geen aanzienlijke invloed hebben op de werking van het netwerk.

Cisco raadt u ook aan de sectie Voorbehouden van dit document zorgvuldig te controleren op softwarefouten die van invloed kunnen zijn op uw NX-OS-softwarerelease en ertoe kunnen leiden dat natuurlijk dataplane-verkeer met een TTL van 1 in software wordt verwerkt in plaats van in hardware.

Voorbeelden van foutscenario's

Aangrenzingen van unicast routingprotocollen via een vPC zonder vPC-peergateway

Bekijk de topologie die hier wordt weergegeven:



In deze topologie zijn de Nexus-switches N9K-1 en N9K-2 vPC-peers in een vPC-domein waarin de vPC-peergateway niet is ingeschakeld. Interface Po1 is de vPC-peerlink. Een router met een hostnaam van Router wordt aangesloten via vPC Po10 met N9K-1 en N9K-2. Een host is verbonden met N9K-1 en N9K-2 via vPC Po20. De Po10-interface van de router is een gerouteerd poortkanaal dat wordt geactiveerd onder een unicast-routeringsprotocol. Voor N9K-1 en N9K-2 zijn SVI-interfaces geactiveerd onder hetzelfde unicast routingprotocol. De switches bevinden zich in hetzelfde broadcastdomein als Router.

Aangrenzingen van unicast routingprotocollen via een vPC waarvoor de vPC-peergateway niet is ingeschakeld, worden niet ondersteund omdat de hashing-beslissing voor ECMP van de via vPC verbonden router en de hashing-beslissing van het bijbehorende Layer 2-poortkanaal kunnen verschillen. In deze topologie, zou het verpletteren van protocolnabijheid met succes tussen Router, N9K-1, en N9K-2 vormen. Overweeg de stroom van verkeer tussen router en host. Verkeer van de dataplane dat via Router naar Host stroomt, kan worden herschreven met een

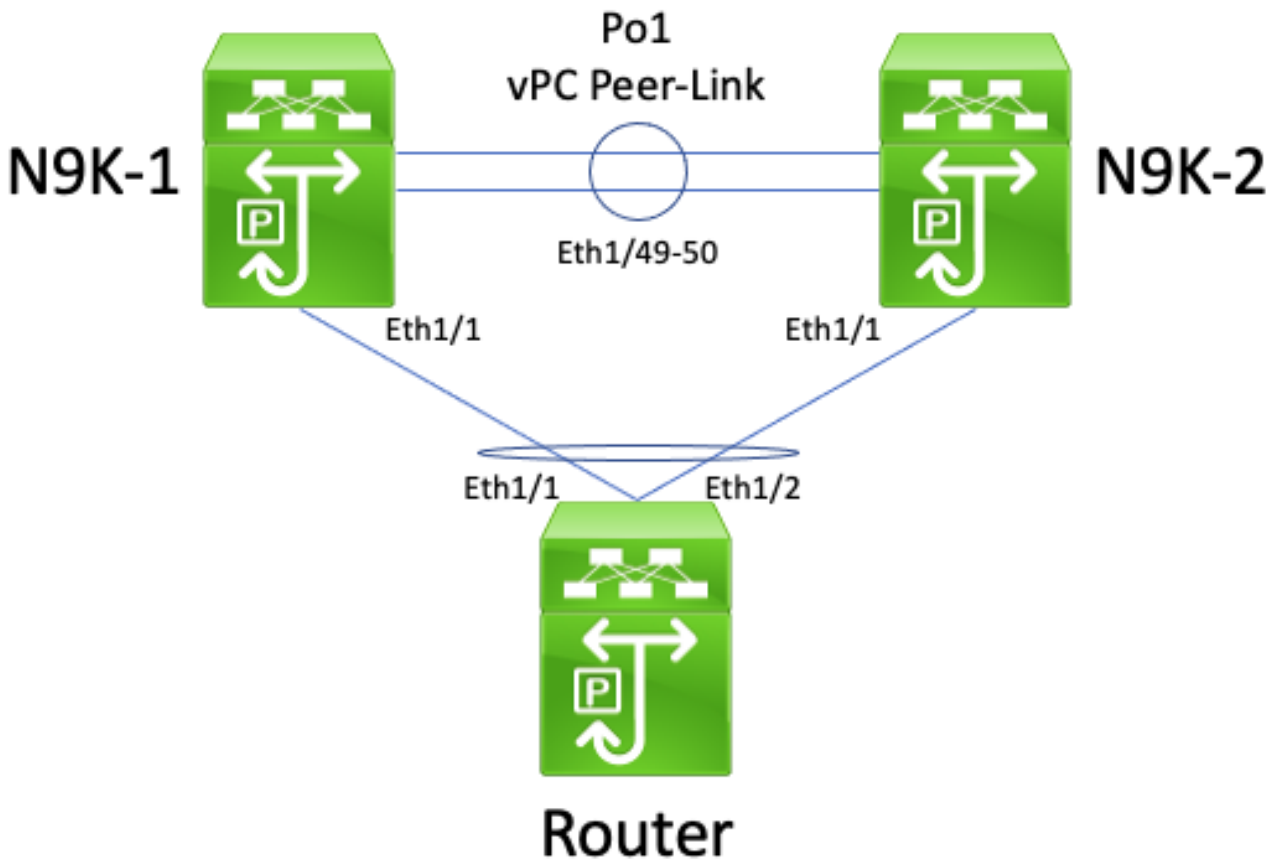
bestemmings-MAC-adres dat hoort bij het MAC-adres van de SVI van N9K-1 (vanwege de hashing-beslissing voor ECMP van de router), maar worden uitgevoerd vanuit interface Ethernet1/2 (vanwege de hashing-beslissing voor het Layer 2-poortkanaal van de router).

N9K-2 ontvangt dit pakket en doorstuurt het over de vPC Peer-Link, omdat het MAC-adres van de bestemming tot N9K-1 behoort en de verbetering in de vPC Peer Gateway (die N9K-2 toestaat om het pakket te leiden namens N9K-1) niet is ingeschakeld. N9K-1 ontvangt dit pakket via de vPC Peer-Link en erkent dat het pakket moet doorsturen vanuit zijn Ethernet1/2 in vPC Po20. Dit is in strijd met de vPC Loop Avoidance regel, dus N9K-1 laat het pakket vallen in hardware. Als gevolg daarvan kunnen zich connectiviteitsproblemen voordoen of kan er pakketverlies optreden voor sommige stromen die het vPC-domein passeren in deze topologie.

U lost dit probleem op door de vPC-peergateway in te schakelen met de configuratieopdracht **peer-gateway** voor het vPC-domein en vervolgens routing/Layer 3 via vPC in te schakelen met de configuratieopdracht **layer3 peer-router** voor het vPC-domein. Om onderbrekingen te voorkomen, moet u beide vPC-verbeteringen kort achter elkaar inschakelen, zodat er niet voldoende tijd is voor het foutscenario beschreven in Aangrenzingen van unicast routingprotocollen via een vPC met vPC-peergateway om zich voor te doen.

Aangrenzingen van unicast routingprotocollen via een vPC met vPC-peergateway

Bekijk de topologie die hier wordt weergegeven:



In deze topologie zijn de Nexus-switches N9K-1 en N9K-2 vPC-peers in een vPC-domein waarin de vPC-peergateway is ingeschakeld. Interface Po1 is de vPC-peerlink. Een router met een hostnaam van Router wordt aangesloten via vPC Po10 met N9K-1 en N9K-2. De Po10-interface van de router is een gerouteerd poortkanaal dat wordt geactiveerd onder een unicast-

routeringsprotocol. Voor N9K-1 en N9K-2 zijn SVI-interfaces geactiveerd onder hetzelfde unicast routingprotocol. De switches bevinden zich in hetzelfde broadcastdomein als Router.

Aangrenzingen van unicast routingprotocollen via een vPC waarvoor de vPC-peergateway is ingeschakeld, worden niet ondersteund omdat de vPC-peergateway kan verhinderen dat er aangrenzingen van unicast routingprotocollen worden gevormd tussen de via vPC verbonden router en beide vPC-peers. In deze topologie, kan een routeringsprotocol nabijheid tussen router en N9K-1 of N9K-2 er niet in slagen om op de verwachte manier tevoorschijn te komen afhankelijk van hoe de unicast routeringsprotocol pakketten voortkwamen uit router aan of N9K-1 of N9K-2 hash over vPC Po10.

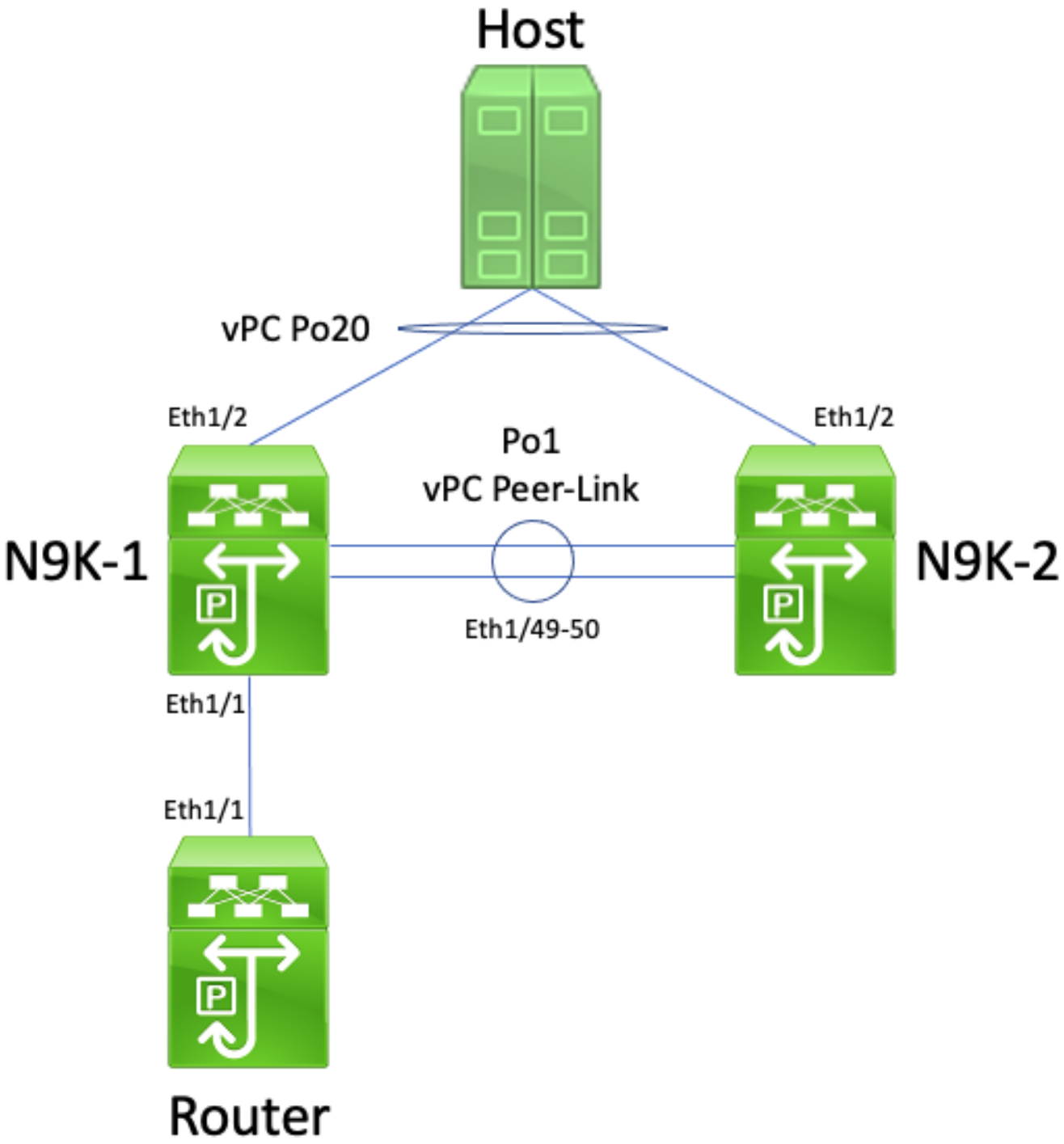
Alle routers kunnen zonder probleem link-local multicast routingprotocolpakketten (ook wel Hello-pakketten) verzenden en ontvangen omdat deze worden geflood naar het vPC-VLAN. Er kan zich echter ook een situatie voordoen waarin een unicast routingprotocolpakket afkomstig van de router en bestemd voor N9K-1 in plaats daarvan via Ethernet1/2 wordt uitgevoerd naar N9K-2 vanwege de hashing-beslissing van het Layer 2-poortkanaal van de router. Dit pakket is bestemd voor het SVI MAC-adres van N9K-1, maar komt in de Ethernet1/1-interface van N9K-2. N9K-2 ziet dat het pakket bestemd is voor het SVI MAC-adres van N9K-1, dat geïnstalleerd is in de MAC-adrestabel van N9K-2 met de "G", of "Gateway", vlag als gevolg van de vPC Peer Gateway-verbetering die is ingeschakeld. Dientengevolge, probeert N9K-2 het unicast routingprotocolpakket namens N9K-1 plaatselijk te leiden.

Door het pakket te routeren wordt echter de tijd om te leven (TTL) van het pakket verkleind en de TTL van de meeste unicast routingprotocolpakketten is 1. Hierdoor wordt de TTL van het pakket verlaagd naar 0 en verlaagd door N9K-2. Vanuit het perspectief van N9K-1, ontvangt N9K-1 link-lokale multicast routing protocolpakketten van router en kan het unicast routing protocolpakketten naar router verzenden, maar ontvangt het geen unicast routing protocolpakketten van router. Dientengevolge, scheurt N9K-1 onderaan de routeringsprotocolnabijheid met router en begint zijn lokale eindige toestandsmachine voor het routeringsprotocol opnieuw. Op dezelfde manier begint de router zijn lokale eindige staatsmachine voor het routeringsprotocol opnieuw.

U lost dit probleem op door routing/Layer 3 via vPC in te schakelen met de configuratieopdracht **layer 3 peer-router** voor het vPC-domein. Unicast routingprotocolpakketten met een TTL van 1 kunnen dan via de vPC-peerlink worden doorgestuurd zonder de TTL van het pakket te verlagen. Het resultaat is dat zonder problemen aangrenzingen van unicast routingprotocollen kunnen worden gevormd via een vPC of vPC-VLAN.

Aangrenzingen van unicast routingprotocollen via een vPC-VLAN zonder vPC-peergateway

Bekijk de topologie die hier wordt weergegeven:



In deze topologie zijn de Nexus-switches N9K-1 en N9K-2 vPC-peers in een vPC-domein waarin de vPC-peergateway niet is ingeschakeld. Interface Po1 is de vPC-peerlink. Een router met een hostnaam van Router is via Ethernet1/1 verbonden met N9K-1's Ethernet1/1. De Ethernet1/1-interface van de router is een gerouteerde interface die wordt geactiveerd onder een unicast-routeringsprotocol. Voor N9K-1 en N9K-2 zijn SVI-interfaces geactiveerd onder hetzelfde unicast routingprotocol. De switches bevinden zich in hetzelfde broadcastdomein als Router.

Aangrenzingen van unicast routingprotocollen via een vPC-VLAN waarvoor de vPC-peergateway niet is ingeschakeld, worden niet ondersteund omdat de hashing-beslissing voor ECMP van de via het vPC-VLAN verbonden router ertoe kan leiden dat dataplane-verkeer door N9K-2 wordt afgewezen vanwege het schenden van de vPC-regel voor het voorkomen van lussen. In deze topologie, zou het verpletteren van protocolnabijheid met succes tussen Router, N9K-1, en N9K-2 vormen. Overweeg de stroom van verkeer tussen router en host. Verkeer van de dataplane dat via Router naar Host stroomt, kan worden herschreven met een bestemmings-MAC-adres dat hoort

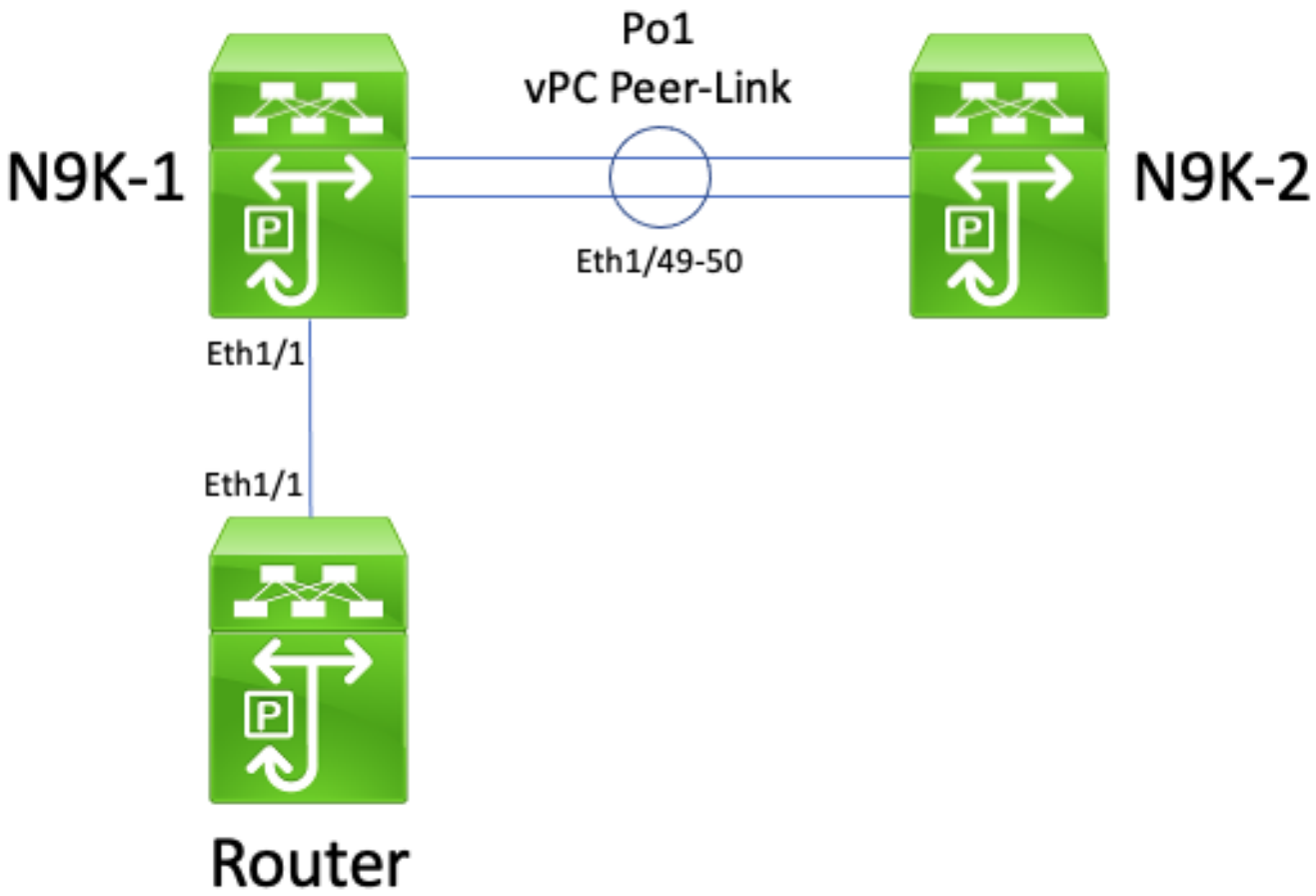
bij het MAC-adres van de SVI van N9K-2 (vanwege de hashing-beslissing voor ECMP van de router) en van interface Ethernet1/1 worden uitgevoerd naar N9K-1.

N9K-1 ontvangt dit pakket en doorstuurt het over de vPC Peer-Link, omdat het MAC-adres van de bestemming tot N9K-2 behoort en de verbetering in de vPC Peer Gateway (die N9K-1 in staat stelt om het pakket te leiden namens N9K-2) niet is ingeschakeld. N9K-2 ontvangt dit pakket via de vPC Peer-Link en erkent dat het pakket moet doorsturen vanuit zijn Ethernet1/2 in vPC Po20. Dit is in strijd met de vPC Loop Avoidance regel, dus N9K-2 laat het pakket vallen in hardware. Als gevolg daarvan kunnen zich connectiviteitsproblemen voordoen of kan er pakketverlies optreden voor sommige stromen die het vPC-domein passeren in deze topologie.

U lost dit probleem op door de vPC-peergateway in te schakelen met de configuratieopdracht **peer-gateway** voor het vPC-domein en vervolgens routing/Layer 3 via vPC in te schakelen met de configuratieopdracht **layer3 peer-router** voor het vPC-domein. Om onderbrekingen te voorkomen, moet u beide vPC-verbeteringen kort achter elkaar inschakelen, zodat er niet voldoende tijd is voor het foutscenario beschreven in Aangrenzingen van unicast routingprotocollen via een vPC met vPC-peergateway om zich voor te doen.

Aangrenzingen van unicast routingprotocollen via een vPC-VLAN met vPC-peergateway

Bekijk de topologie die hier wordt weergegeven:



In deze topologie zijn de Nexus-switches N9K-1 en N9K-2 vPC-peers in een vPC-domein waarin de vPC-peergateway is ingeschakeld. Interface Po1 is de vPC-peerlink. Een router met een hostnaam van Router is via Ethernet1/1 verbonden met N9K-1's Ethernet1/1. De Ethernet1/1-interface van de router is een gerouteerde interface die wordt geactiveerd onder een unicast-routeringsprotocol. Voor N9K-1 en N9K-2 zijn SVI-interfaces geactiveerd onder hetzelfde unicast

routingprotocol. De switches bevinden zich in hetzelfde broadcastdomein als Router.

Unicast-routingprotocolnabijheid via vPC VLAN met de ingeschakelde verbetering van de vPC Peer Gateway wordt niet ondersteund omdat de verbetering van de vPC Peer Gateway voorkomt dat unicast-routingprotocolnabijheid zich vormt tussen de met vPC VLAN verbonden router en de vPC-peer waarmee de met vPC VLAN verbonden router niet rechtstreeks is verbonden. In deze topologie, slaagt een routeringsprotocol nabijheid tussen router en N9K-2 er niet in om op te duiken zoals verwacht als resultaat van N9K-1 routing unicast routeringsprotocol pakketten bestemd voor N9K-2's SVI MAC-adres dankzij de vPC Peer Gateway-verbetering die wordt ingeschakeld. Omdat de pakketten worden gerouteerd, moet hun TTL worden verlaagd. Unicast routingprotocolpakketten hebben doorgaans een TTL van 1. Een router die de TTL van een pakket verlaagt naar 0, moet dat pakket afwijzen.

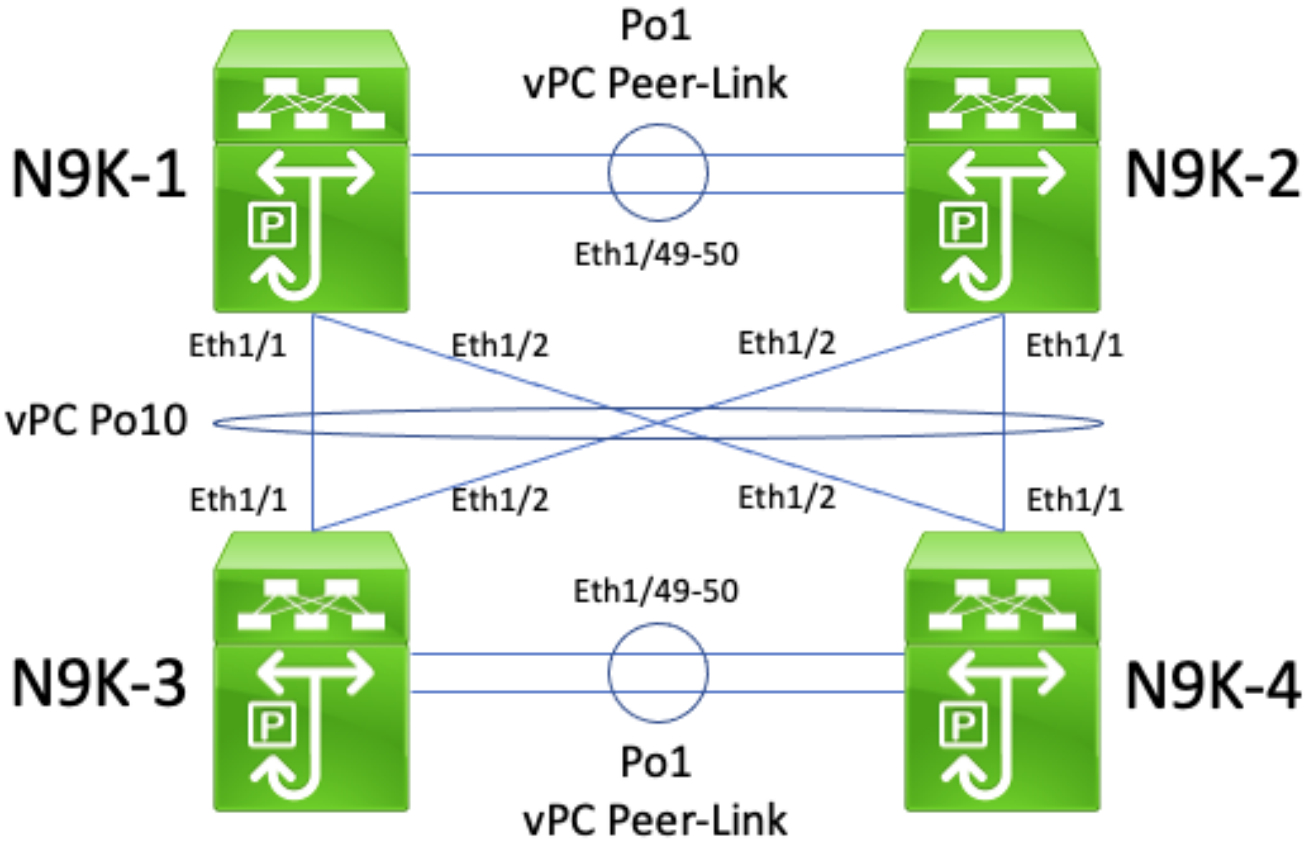
Alle routers kunnen zonder probleem link-local multicast routingprotocolpakketten (ook wel Hello-pakketten) verzenden en ontvangen omdat deze worden geflood naar het vPC-VLAN. Overweeg echter een scenario waarin een unicast routingprotocol-pakketbron van router bestemd voor N9K-2 Ethernet1/1 naar N9K-1 betrekt. Dit pakket is bestemd voor het SVI MAC-adres van N9K-2, maar komt in de Ethernet1/1-interface van N9K-1. N9K-1 ziet dat het pakket is bestemd voor het SVI MAC-adres van N9K-2, dat is geïnstalleerd in de MAC-adrestabel van N9K-1 met de "G", of "Gateway", vlag als gevolg van de vPC Peer Gateway-verbetering die is ingeschakeld. Dientengevolge, probeert N9K-1 het unicast routeringsprotocol pakket namens N9K-2 lokaal te leiden.

Door het pakket te routeren wordt de TTL van het pakket echter verlaagd en de TTL van de meeste unicast-routingprotocolpakketten is 1. Hierdoor wordt de TTL van het pakket verlaagd naar 0 en verlaagd door N9K-1. Vanuit het perspectief van N9K-2, ontvangt N9K-2 link-lokale multicast routingprotocolpakketten van router en kan het unicast routingprotocolpakketten naar router verzenden, maar ontvangt het geen unicast routingprotocolpakketten van router. Dientengevolge, scheurt N9K-2 onderaan de routeringsprotocolnabijheid met router en begint zijn lokale eindige toestandsmachine voor het routeringsprotocol opnieuw. Op dezelfde manier begint de router zijn lokale eindige staatsmachine voor het routeringsprotocol opnieuw.

U lost dit probleem op door routing/Layer 3 via vPC in te schakelen met de configuratieopdracht **layer 3 peer-router** voor het vPC-domein. Unicast routingprotocolpakketten met een TTL van 1 kunnen dan via de vPC-peerlink worden doorgestuurd zonder de TTL van het pakket te verlagen. Het resultaat is dat zonder problemen aangrenzingen van unicast routingprotocollen kunnen worden gevormd via een vPC of vPC-VLAN.

Aangrenzingen van unicast routingprotocollen via back-to-back vPC met vPC-peergateway

Bekijk de topologie die hier wordt weergegeven:



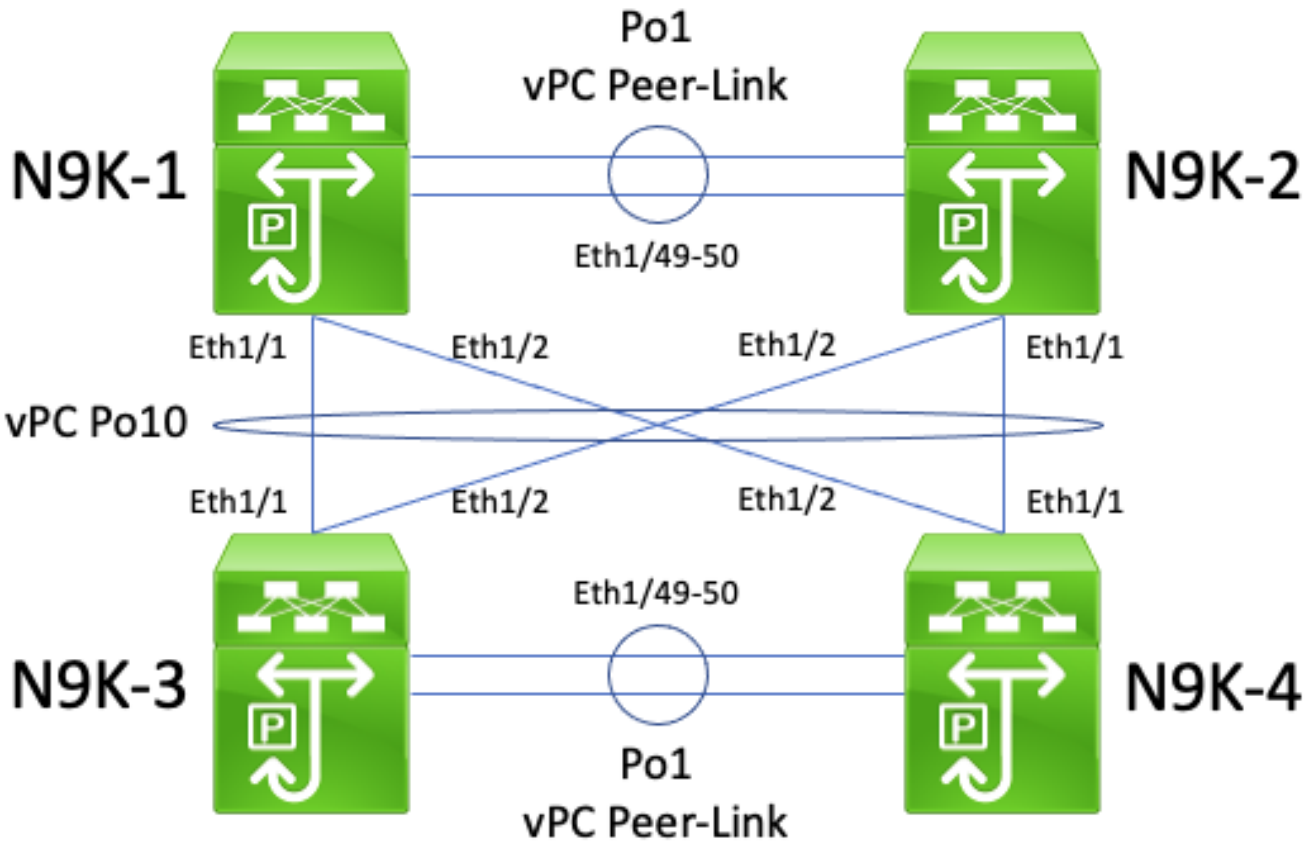
In deze topologie zijn de Nexus-switches N9K-1 en N9K-2 vPC-peers in een vPC-domein waarin de vPC-peergateway is ingeschakeld. De Nexus-switches N9K-3 en N9K-4 zijn vPC-peers in een vPC-domein waarin de vPC-peergateway is ingeschakeld. Beide vPC-domeinen zijn met elkaar verbonden via een back-to-back vPC Po10. Alle vier de switches hebben SVI-interfaces geactiveerd onder een unicast-routeringsprotocol en bevinden zich in hetzelfde uitzendingsdomein.

Aangrenzingen van unicast routingprotocollen via back-to-back vPC's waarvoor de vPC-peergateway is ingeschakeld, worden niet ondersteund omdat de vPC-peergateway kan verhinderen dat er aangrenzingen van unicast routingprotocollen worden gevormd tussen het ene en het andere vPC-domein. In deze topologie kan een routeringsprotocolnabijheid tussen N9K-1 en N9K-3 of N9K-4 (of beide) niet op de verwachte manier tot stand komen. Op dezelfde manier kan de aangrenzing van een routingprotocol tussen N9K-2 en N9K-3 en/of N9K-4 mislukken. Unicast routingprotocolpakketten kunnen namelijk bestemd zijn voor een bepaalde router (bijvoorbeeld N9K-3), maar worden doorgestuurd naar een andere router (bijvoorbeeld N9K-4) op basis van de hashing-beslissing van het Layer 2-poortkanaal van de oorspronkelijke router.

De hoofdoorzaak van dit probleem is dezelfde als de beschreven hoofdoorzaak in de sectie Aangrenzingen van unicast routingprotocollen via een vPC met vPC-peergateway van dit document. U lost dit probleem op door routing/Layer 3 via vPC in te schakelen met de configuratieopdracht **layer 3 peer-router** voor het vPC-domein. Unicast routingprotocolpakketten met een TTL van 1 kunnen dan via de vPC-peerlink worden doorgestuurd zonder de TTL van het pakket te verlagen. Het resultaat is dat zonder problemen aangrenzingen van unicast routingprotocollen kunnen worden gevormd via een back-to-back vPC.

OSPF-aangrenzingen via vPC met vPC-peergateway waarbij het voorvoegsel aanwezig is in de OSPF-LSDB, maar niet in de routingtabel

Bekijk de topologie die hier wordt weergegeven:



In deze topologie zijn de Nexus-switches N9K-1 en N9K-2 vPC-peers in een vPC-domein waarin de vPC-peergateway is ingeschakeld. De Nexus-switches N9K-3 en N9K-4 zijn vPC-peers in een vPC-domein waarin de vPC-peergateway is ingeschakeld. Beide vPC-domeinen zijn met elkaar verbonden via een back-to-back vPC Po10. Alle vier de switches hebben SVI-interfaces geactiveerd onder een unicast-routeringsprotocol en bevinden zich in hetzelfde uitzendingsdomein. N9K-4 is de aangewezen OSPF-router voor het broadcastdomein en N9K-3 is de back-up.

In dit scenario gaat een OSPF-aangrenzing tussen N9K-1 en N9K-3 over in de toestand FULL omdat unicast OSPF-pakketten op beide switches de uitgaande route via Ethernet1/1 volgen. Op dezelfde manier gaat een OSPF-aangrenzing tussen N9K-2 en N9K-3 over in de toestand FULL omdat unicast OSPF-pakketten op beide switches de uitgaande route via Ethernet1/2 volgen.

Een OSPF-aangrenzing tussen N9K-1 en N9K-4 blijft echter de toestand EXSTART of EXCHANGE houden omdat unicast OSPF-pakketten op beide switches de uitgaande route via Ethernet1/1 volgen en door N9K-2 en N9K-4 worden afgewezen, zoals wordt beschreven in de sectie Aangrenzingen van unicast routingprotocollen via back-to-back vPC met vPC-peergateway van dit document. Op dezelfde manier blijft een OSPF-aangrenzing tussen N9K-2 en N9K-4 de toestand EXSTART of EXCHANGE houden omdat unicast OSPF-pakketten op beide switches de uitgaande route via Ethernet1/2 volgen en door N9K-1 en N9K-3 worden afgewezen, zoals wordt beschreven in de sectie Aangrenzingen van unicast routingprotocollen via back-to-back vPC met vPC-peergateway van dit document.

Het resultaat is dat N9K-1 en N9K-2 zich in de toestand FULL bevinden richting de aangewezen back-uprouter (BDR) voor het broadcastdomein, maar zich de toestand EXSTART of EXCHANGE bevinden richting de aangewezen router (DR) voor het broadcastdomein. Zowel de aangewezen router als de back-uprouter van een broadcastdomein behoudt een volledig exemplaar van de OSPF-LSDB (Link State Data Base), maar OSPF DROTHER-routers moeten zich in de toestand FULL bevinden richting de DR voor het broadcastdomein om de installatie van voorvoegsels die

via OSPF zijn geleerd vanuit de DR of de BDR mogelijk te maken. Hierdoor lijken zowel N9K-1 als N9K-2 prefixes te hebben aangeleerd van N9K-3 en N9K-4 aanwezig in de OSPF LSDB, maar deze prefixes zijn niet geïnstalleerd in de unicast-routeringstabel tot N9K-1 en N9K-2 overgang naar een FULL-state met N9K-4 (de DR voor het broadcast-domein).

U lost dit probleem op door routing/Layer 3 via vPC in te schakelen met de configuratieopdracht **layer 3 peer-router** voor het vPC-domein. Unicast routingprotocolpakketten met een TTL van 1 kunnen dan via de vPC-peerlink worden doorgestuurd zonder de TTL van het pakket te verlagen. Het resultaat is dat zonder problemen aangrenzingen van unicast routingprotocollen kunnen worden gevormd via een back-to-back vPC. Hierdoor gaan N9K-1 en N9K-2 over naar een FULL-state met N9K-4 (de DR voor het broadcast-domein) en worden van N9K-3 en N9K-4 geleerde prefixes via OSPF geïnstalleerd in hun respectieve unicast-routingtabellen.

Gerelateerde informatie

- Configuratiehandleiding voor Cisco Nexus 9000 Series NX-OS-interfaces, release 10.1(x)
- Configuratiehandleiding voor Cisco Nexus 9000 Series NX-OS-interfaces, release 9.3(x)
- Configuratiehandleiding voor Cisco Nexus 9000 Series NX-OS-interfaces, release 9.2(x)
- Configuratiehandleiding voor Cisco Nexus 9000 Series NX-OS-interfaces, release 7.x
- Configuratiehandleiding voor Cisco Nexus 7000 Series NX-OS-interfaces 8.x
- Configuratiehandleiding voor Cisco Nexus 7000 Series NX-OS-interfaces 7.x
- Design and Configuration Guide: Best Practices voor Virtual Port Channel (vPC) op Cisco Nexus 7000 Series Switches
- Ondersteunde technologieën voor routing via Virtual Port Channel op Nexus-platforms

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.