vPC(Virtual Port Channel) 개선 사항 이해

목차

소개

이 문서에서는 vPC 도메인의 Cisco Nexus 스위치에 설정된 일반적인 vPC(Virtual Port Channel) 기능 향상에 대해 설명합니다.

사전 요구 사항

요구 사항

시스코에서는 vPC(Virtual Port Channel)의 활용 사례, 설정 및 구현과 관련된 기본 정보를 이해할 것을 권장합니다. 이 기능에 대한 자세한 내용은 해당되는 다음 문서 중 하나를 참조하십시오.

- Cisco Nexus 9000 시리즈 NX-OS 인터페이스 설정 가이드, 릴리스 10.3(x)
- Cisco Nexus 9000 시리즈 NX-OS 인터페이스 설정 가이드, 릴리스 10.2(x)
- Cisco Nexus 9000 시리즈 NX-OS 인터페이스 설정 가이드, 릴리스 10.1(x)
- Cisco Nexus 9000 시리즈 NX-OS 인터페이스 설정 가이드, 릴리스 9.3(x)
- Cisco Nexus 9000 시리즈 NX-OS 인터페이스 설정 가이드, 릴리스 9.2(x)
- Cisco Nexus 9000 시리즈 NX-OS 인터페이스 설정 가이드, 릴리스 7.x
- Cisco Nexus 7000 시리즈 NX-OS 인터페이스 설정 가이드 8.x
- Cisco Nexus 7000 시리즈 NX-OS 인터페이스 설정 가이드 7.x
- 설계 및 설정 가이드: Cisco Nexus 7000 시리즈 스위치의 vPC(Virtual Port Channel) 모범 사례

사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Cisco Nexus 데이터 센터 스위치에 Cisco NX-OS가 도입된 이래로 vPC(Virtual Port Channel) 기능은 실패 시나리오에서 vPC 연결 디바이스의 안정성을 개선하고 두 vPC 피어 스위치의 포워딩 동작을 최적화하는 여러 차례 개선되었습니다. 각 기능 향상의 목적, 기능 향상으로 인해 야기되는 동작의 변화 및 기능 향상으로 해결되는 실패 시나리오를 이해하면 vPC 도메인 내에서 비즈니스 요구 사항을 가장 잘 충족하도록 기능 향상을 설정해야 하는 이유와 그 시기를 파악할 수 있습니다.

적용 가능한 하드웨어

이 문서에서 설명하는 절차는 모든 vPC 지원 Cisco Nexus 데이터 센터 스위치에 적용됩니다.

vPC 피어 스위치

이 섹션에서는 peer-switch vPC 도메인 설정 명령을 통해 활성화되는 vPC 피어 스위치 기능 향상에 대해 설명합니다.

개요

많은 환경에서 vPC 도메인의 Nexus 스위치 쌍은 레이어 2 스위칭 이더넷 도메인과 레이어 3 라우팅 도메인 간의 경계 역할을 하는 어그리게이션 또는 코어 스위치입니다. 두 스위치 모두 여러 VLAN으로 설정되며 VLAN 간 동-서 트래픽과 북-남 트래픽 라우팅을 담당합니다. 이러한 환경에서 Nexus 스위치는 일반적으로 스패닝 트리 프로토콜 관점에서 루트 브리지 역할도 합니다.

일반적으로 하나의 vPC 피어는 스패닝 트리 우선순위를 낮은 값(예: 0)으로 설정하여 스패닝 트리의 루트 브리지로 설정됩니다. 다른 vPC 피어는 다소 높은 스패닝 트리 우선순위(예: 4096)로 설정되며, 이를 통해 루트 브리지 역할을 하는 vPC 피어가 실패할 경우 스패닝 트리 내에서 루트 브리지의 역할을 맡을 수 있습니다. 이 설정을 사용할 때 루트 브리지 역할을 하는 vPC 피어가 시스템 MAC 주소를 포함하는 브리지 ID를 사용하여 스패닝 트리 BPDU(Bridge Protocol Data Unit)가 발생합니다.

하지만 루트 브리지 역할을 하는 vPC 피어가 실패하고 다른 vPC 피어가 스패닝 트리 루트 브리지 역할을 맡는 경우, 다른 vPC 피어는 시스템 MAC 주소가 포함된 브리지 ID를 사용하여 스패닝 트리 BPDU를 발생시킵니다. 여기에서 MAC 주소는 원래 루트 브리지의 시스템 MAC 주소와 다릅니다. 다운스트림 브리지가 연결되는 방식에 따라 이 변경이 미치는 영향은 다양하며 다음 하위 섹션에 설명되어 있습니다.

이중 연결 비 vPC 브리지

BPDU의 변경 사항(그리고 그에 따른 루트 브리지의 변경 사항)을 감지하는 이중화 링크(하나의 링크가 스패닝 트리 프로토콜 관점에서 Blocking 상태에 있음)를 통해 연결된 두 vPC 피어에 연결되는 비 vPC 연결 브리지는 루트 포트의 변경 사항을 확인합니다. 기타 지정된 포워딩 인터페이스는 즉시 Blocking 상태로 전환된 다음 설정된 스패닝 트리 프로토콜 포워딩 지연 타이머(기본적으로 15초)와 같은 간격으로 일시 중지된 상태로 스패닝 트리 프로토콜 유한 상태 머신(Blocking, Learning 및 Forwarding)을 통과합니다.

루트 포트의 변경 사항 및 스패닝 트리 프로토콜 유한 상태 머신의 후속 통과로 인해 네트워크 내에서 상당한 양의 중단이 발생할 수 있습니다. vPC 피어 중 하나가 오프라인 상태가 될 경우 이 문제로 인한 네트워크 중단을 방지하기 위해 vPC 피어 스위치 기능 향상이 주로 도입되었습니다. vPC 피어 스위치 기능 향상을 통해 비 vPC 연결 브리지에는 여전히 단일 이중화 링크가 Blocking 상태에 있지만 링크 실패로 인해 기존 루트 포트가 중단되면 해당 인터페이스가 Forwarding 상태로 즉시 전환됩니다. 오프라인 vPC 피어가 다시 온라인 상태가 되면 동일한 프로세스가 수행됩니다. 루트 브리지에 대한 비용이 가장 낮은 인터페이스는 루트 포트 역할을 점유하며, 이중화 링크는 즉시 Blocking 상태로 전환됩니다. 데이터플레인에서 관찰되는 유일한 영향은 vPC 피어가 오프라인 상태가 되었을 때 vPC 피어를 통과하는 중이었던 패킷의 불가피한 손실입니다.

vPC 연결 브리지

스패닝 트리 도메인의 vPC 연결 브리지는 BPDU의 변경(그리고 그에 따른 루트 브리지의 변경)을 탐지하고 로컬 MAC 주소 테이블에서 동적으로 학습된 MAC 주소를 플러시합니다. 이 동작은 루프 없는 토폴로지에 대해 스패닝 트리 프로토콜에 의존하지 않는 vPC 연결 디바이스가 있는 토폴로지에서는 비효율적이고 불필요합니다. vPC는 일반 포트 채널과 마찬가지로 스패닝 트리 프로토콜 관점에서 단일 논리적 인터페이스로 간주됩니다. 따라서 vPC 피어 손실은 포트 채널 멤버 내의 단일 링크 손실과 유사합니다. 두 시나리오 중 하나에서 스패닝 트리는 변경되지 않으므로, 스패닝 트리 도메인의 브리지에서 동적으로 학습된 MAC 주소를 플러시(플러시의 목적은 이더넷의 플러딩-학습 동작을 통해 MAC 주소를 새로 학습하는 것임)하는 것은 필요하지 않습니다.

또한 동적으로 학습된 MAC 주소의 플러시는 잠재적으로 중단을 일으킬 수 있습니다. 두 호스트가 주로 단방향 UDP 기반 플로우(예: TFTP 클라이언트가 TFTP 서버로 데이터를 송신)를 가지고 있는 시나리오를 가정해 보겠습니다. 이 플로우에서는 데이터가 대부분 TFTP 클라이언트에서 TFTP 서버로 이동하며, 드물게 TFTP 서버가 TFTP 클라이언트로 패킷을 다시 송신하는 경우가 있습니다. 결과적으로 스패닝 트리 도메인에서 동적으로 학습된 MAC 주소를 플러시한 후에는 TFTP 서버의 MAC은 잠시 동안 학습되지 않습니다. 이는 트래픽이 알 수 없는 유니캐스트 트래픽이므로 TFTP 서버로 송신되는 TFTP 클라이언트의 데이터가 VLAN 전체에 플러딩됨을 의미합니다. 이로 인해 대규모 데이터 플로우가 네트워크 내의 의도하지 않은 위치로 이동하게 되며, 네트워크의 초과 서브스크립션 섹션을 통과하는 경우 성능 문제가 발생할 수 있습니다.

하나 이상의 VLAN에 대한 스패닝 트리 루트 브리지 역할을 하는 vPC 피어가 다시 로드되거나 전원이 꺼지는 경우 비효율적이고 불필요한 동작이 발생하지 않도록 vPC 피어 스위치 기능 향상이 도입되었습니다.

vPC 피어 스위치 개선을 활성화하려면 두 vPC 피어가 모두 동일한 스패닝 트리 프로토콜 컨피그레이션(모든 vPC VLAN의 스패닝 트리 우선순위 값 포함)을 가져야 하며 모든 vPC VLAN의 루트 브리지가 되어야 합니다. 이러한 사전 조건이 충족되면 vPC 피어 스위치 기능 향상을 활성화하도록 peer-switch vPC 도메인 설정 명령을 설정해야 합니다.

참고: vPC Peer Switch 개선 사항은 모든 VLAN에 대한 루트가 포함된 vPC 도메인에서만 지원됩니다.

---

vPC 피어 스위치 기능 향상이 활성화되면 두 vPC 피어가 두 vPC 피어 모두에서 공유하는 vPC 시스템 MAC 주소를 포함하는 브리지 ID를 사용하여 동일한 스패닝 트리 BPDU를 발생시키기 시작합니다. vPC 피어가 다시 로드될 경우 나머지 vPC 피어에서 시작된 스패닝 트리 BPDU는 변경되지 않으므로 스패닝 트리 도메인의 다른 브리지는 루트 브리지의 변경 사항을 확인하지 않으며 네트워크의 변경 사항에 차선으로 대응하지 않습니다.

경고

vPC 피어 스위치 기능 향상에는 프로덕션 환경에서 설정하기 전에 유의해야 할 몇 가지 사항이 있습니다.

스패닝 트리 우선순위 값이 vPC 피어 간에 일치해야 함

vPC 피어 스위치 기능 향상을 활성화하기 전에 두 vPC 피어 간에 동일하도록 모든 vPC VLAN에 대한 스패닝 트리 우선순위 설정을 수정해야 합니다.

N9K-1이 우선순위가 0인 VLAN 1, 10, 20의 스패닝 트리 루트 브리지로 설정된다고 가정합니다. N9K-2는 우선순위가 4096인 VLAN 1, 10, 20의 보조 스패닝 트리 루트 브리지입니다.

<#root>

```
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
```

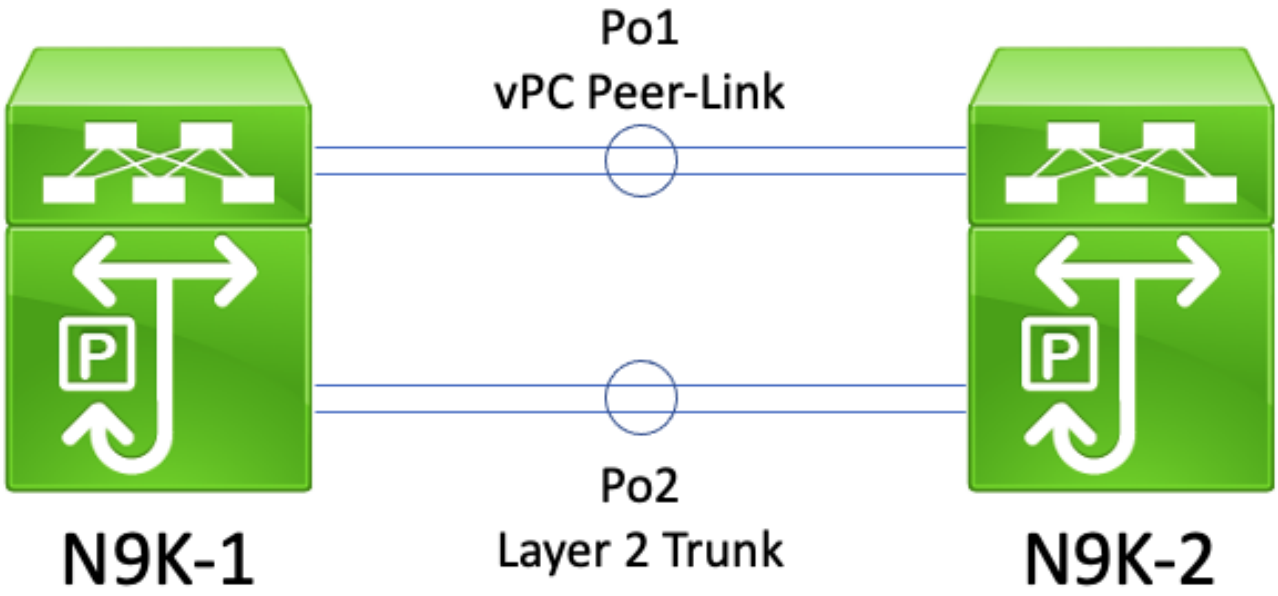
vPC 피어 스위치 기능 향상을 활성화하기 전에 N9K-2의 VLAN 1, 10, 20에 대한 스패닝 트리 우선순위 설정을 수정하여 N9K-1의 동일한 VLAN에 대한 스패닝 트리 우선순위 설정과 일치시켜야 합니다. 이 수정의 예시가 여기에 표시됩니다.

<#root>

```
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
```

vPC 피어 스위치가 비 vPC VLAN에 영향을 미침

여기에 있는 토폴로지를 고려해 보십시오.



이 토폴로지에서는 2개의 vPC 피어(N9K-1 및 N9K-2) 사이에는 Po1과 Po2라는 레이어 2 트렁크 2개가 있습니다. Po1은 vPC VLAN을 전달하는 vPC 피어 링크이고, Po2는 모든 비 vPC VLAN을 전달하는 레이어 2 트렁크입니다. Po2를 통해 전달되는 비 vPC VLAN의 스패닝 트리 우선순위 값이 N9K-1 및 N9K-2에서 동일한 경우, 각 vPC 피어는 vPC 시스템 MAC 주소로부터 비롯된 스패닝 트리 BPDU 프레임을 발생시키며, 이는 두 스위치 모두에서 동일합니다. 따라서 N9K-2가 스패닝 트리 BPDU를 발생시킨 스위치인 경우에도 N9K-1은 각 비 vPC VLAN에 대해 Po2에서 자체 스패닝 트리 BPDU를 수신하는 것처럼 보이게 됩니다. 스패닝 트리 관점에서 볼 때 N9K-1은 모든 비 vPC VLAN에 대해 Po2를 Blocking 상태로 설정합니다.

이는 정상적인 동작입니다. 이 문제가 발생하지 않도록 하거나 이 문제를 해결하려면 모든 비 vPC VLAN에서 두 vPC 피어가 서로 다른 스패닝 트리 우선순위 값으로 설정되어야 합니다. 이렇게 하면 하나의 vPC 피어가 비 vPC VLAN에 대한 루트 브리지가 되고 vPC 피어 간의 레이어 2 트렁크가 Designated Forwarding 상태로 전환됩니다. 마찬가지로 원격 vPC 피어는 vPC 피어 사이의 레이어 2 트렁크를 Designated Root 상태로 전환합니다. 이렇게 하면 비 vPC VLAN의 트래픽이 레이어 2 트렁크를 통해 두 vPC 피어로 이동할 수 있습니다.

설정

vPC 피어 스위치 기능을 설정하는 방법의 예시는 여기에서 확인할 수 있습니다.

이 예시에서 N9K-1이 우선순위가 0인 VLAN 1, 10, 20의 스패닝 트리 루트 브리지로 설정됩니다. N9K-2는 우선순위가 4096인 VLAN 1, 10, 20의 보조 스패닝 트리 루트 브리지입니다.

<#root>

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
```

먼저 N9K-2의 스패닝 트리 우선순위 설정을 N9K-1과 동일하게 변경해야 합니다. 이는 vPC 피어 스위치 기능이 예상대로 작동하기 위한 요구 사항입니다. N9K-2의 시스템 MAC 주소가 N9K-1의 시스템 MAC 주소보다 낮은 경우, N9K-2는 스패닝 트리 도메인에 대한 루트 브리지의 역할을 빼앗고, 이로 인해 스패닝 트리 도메인의 다른 브리지가 영향을 받는 모든 VLAN에 대해 로컬 MAC 주소 테이블을 플러시합니다. 이 현상의 예시가 여기에 나와 있습니다.

<#root>

```
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
```

다음으로 peer-switch vPC 도메인 설정 명령을 통해 vPC 피어 스위치 기능을 활성화할 수 있습니다. 이렇게 하면 두 vPC 피어에서 발생한 스패닝 트리 BPDU 내의 브리지 ID가 변경되어 스패닝 트리 도메인의 다른 브리지가 영향을 받는 모든 VLAN에 대한 로컬 MAC 주소 테이블을 플러시합니다.

```
<#root>
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#
```

show spanning-tree summary 명령을 사용하여 vPC VLAN의 루트 브리지가 되겠다는 두 vPC 피어의 클레임을 검증하여 vPC 피어 스위치 기능이 예상대로 작동하는지 확인할 수 있습니다. 또한 이 출력에는 vPC 피어 스위치 기능이 활성화되어 작동 중임을 나타내야 합니다.

```
<#root>
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
```

특정 VLAN에 대한 자세한 정보를 보려면 show spanning-tree vlan{x} 명령을 사용합니다. 기본 또는 운영 기본 vPC 역할을 보유한 스위치의 모든 인터페이스는 Designated Forwarding 상태입니다. 보조 또는 운영 보조 vPC 역할을 보유한 스위치는 Root Forwarding 상태에 있는 vPC 피어 링크를 제외하고 모든 인터페이스가 Designated Forwarding 상태에 있습니다. show vpc role의 출력에 표시되는 vPC 시스템 MAC 주소는 각 vPC 피어의 루트 브리지 ID 및 브리지 ID와 동일합니다.

<#root>

```
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
```

마지막으로, vPC 피어 중 하나에서 Ethanalyzer 제어플레인 패킷 캡처 유틸리티를 사용하여 두 vPC 피어가 두 vPC 피어 모두 간에 공유되는 vPC 시스템 MAC 주소를 포함하는 브리지 ID 및 루트 브리지 ID를 사용하는 스패닝 트리 BPDU를 발생시키고 있는지 확인합니다.

<#root>

```
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

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
```

영향

vPC 피어 스위치 기능 향상 활성화가 미치는 영향은 스패닝 트리 도메인의 다른 브리지가 vPC를 통해 두 vPC 피어에 연결되었는지 또는 vPC 없이 두 vPC 피어에 이중 연결되어 있는지 여부에 따라 달라집니다.

이중 연결 비 vPC 브리지

두 vPC 피어에 대한 이중 링크(하나의 링크가 스패닝 트리 프로토콜 관점에서 차단 상태임)가 있는 비 vPC 연결 브리지가 스패닝 트리 BPDU에 알려진 스패닝 트리 루트 브리지의 변경을 감지하는 경우 브리지의 루트 포트는 2개의 이중화 인터페이스 사이에서 변경될 수 있습니다. 이에 따라 기타 지정된 포워딩 인터페이스는 즉시 차단 상태로 전환된 다음 설정된 스패닝 트리 프로토콜 포워딩 지연 타이머(기본적으로 15초)와 같은 간격으로 일시 중지된 상태로 스패닝 트리 프로토콜 유한 상태 머신(차단, 학습 및 포워딩)을 통과합니다. 루트 포트의 변경 사항 및 스패닝 트리 프로토콜 유한 상태 머신의 후속 통과로 인해 네트워크 내에서 상당한 양의 중단이 발생할 수 있습니다.

스패닝 트리 도메인에 대한 현재 루트 브리지인 vPC 피어가 오프라인 상태가 될 때마다(예: 정전, 하드웨어 실패 또는 재로드) 이 영향이 발생한다는 점은 언급할 가치가 있습니다. 이 동작은 vPC 피어 스위치 기능 향상과 관련이 없습니다. vPC 피어 스위치 기능 향상을 활성화하면 스패닝 트리 관점에서 vPC 피어가 오프라인이 될 때와 유사한 동작이 발생합니다.

vPC 연결 브리지

vPC 연결 브리지가 스패닝 트리 BPDU에 알려진 스패닝 트리 루트 브리지의 변경을 탐지하면 브리지는 MAC 주소 테이블에서 동적으로 학습된 MAC 주소를 플러시합니다. vPC 피어 스위치 기능을 설정하는 동안 다음 두 가지 시나리오에서 이 동작을 관찰할 수 있습니다.

1. 스패닝 트리 우선순위 값이 두 vPC 피어 간에 일치하도록 설정된 경우, 이전에 루트 브리지가 아니었던 vPC 피어의 시스템 MAC 주소가 이전에 루트 브리지였던 vPC의 시스템 MAC 주소보다 낮으면 스패닝 트리 루트 브리지는 다른 vPC 피어로 변경될 수 있습니다. 이 시나리오의 예시는 이 문서의 vPC 피어 스위치 설정 섹션에 나와 있습니다.
2. peer-switch vPC 도메인 설정 명령을 통해 vPC 피어 스위치 기능이 활성화되면 두 vPC 피어가 모두 스패닝 트리 도메인의 루트 브리지로 작동하기 시작합니다. 두 vPC 피어 모두 스스로를 스패닝 트리 도메인의 루트 브리지로 어설션하는 동일한 스패닝 트리 BPDU를 발생시키기 시작합니다.

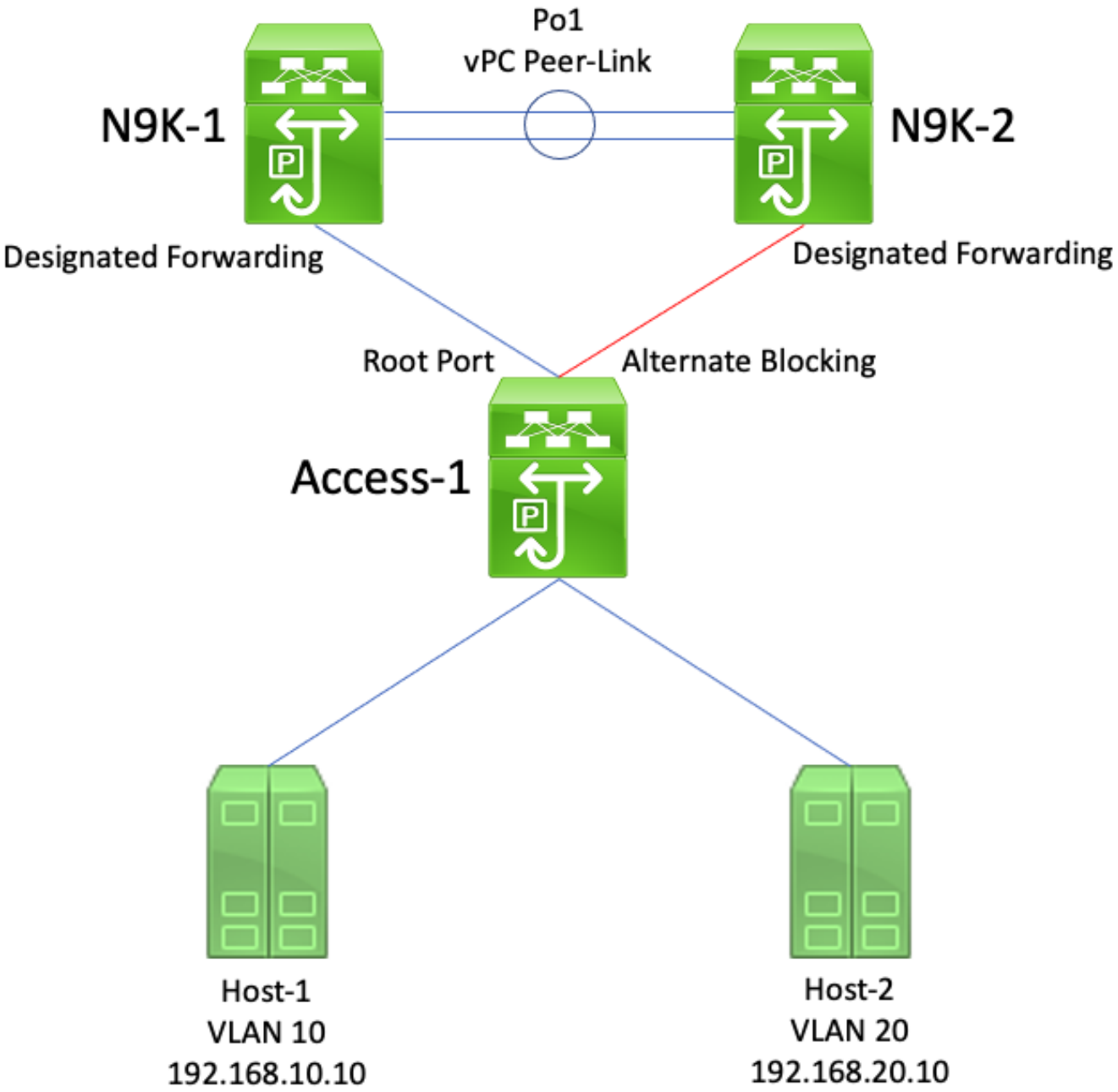
대부분의 시나리오 및 토폴로지에서는 이러한 두 시나리오 중 하나의 결과로 데이터플레인에 미치는 영향이 관찰되지 않습니다. 그러나 짧은 기간 동안 알 수 없는 유니캐스트 플러딩으로 인해 데이터플레인 트래픽이 VLAN 내에서 플러딩되며, 프레임의 대상 MAC 주소는 동적으로 학습된 MAC 주소 플러시의 직접적인 결과에 따라 어떠한 스위치 포트에서도 학습되지 않습니다. 일부 토폴로지에서는 데이터플레인 트래픽이 VLAN 내의 초과 서브스크립션 네트워크 디바이스로 플러딩되는 경우 짧은 기간의 성능 문제 또는 패킷 손실이 발생할 수 있습니다. 이로 인해 대역폭 집약적 단방향 트래픽 플로우 또는 자동 호스트(주로 패킷을 수신하고 거의 송신하지는 않는 호스트) 관련 문제가 발생할 수 있습니다. 이 트래픽이 정상적으로 대상 호스트로 직접 전환되는 대신 장기간 VLAN 내에 플러딩되기 때문입니다.

이러한 영향은 영향을 받는 VLAN 내 브리지의 MAC 주소 테이블에서 동적으로 학습된 MAC 주소의 플러시와 관련이 있습니다. 이 동작은 vPC 피어 스위치 기능 향상 또는 루트 브리지 변경과 관련이 없습니다. VLAN 내에서 비 엣지 포트가 가동되어 생성된 토폴로지 변경 알림으로 인해 발생할 수도 있습니다.

실패 시나리오 예시

유한 상태 머신을 재시작하는 이중 연결 비 vPC 브리지

여기에 있는 토폴로지를 고려해 보십시오.



이 토폴로지에서 N9K-1 및 N9K-2는 vPC 도메인의 vPC 피어입니다. N9K-1은 모든 VLAN에 대해 스패닝 트리 우선순위 값 0으로 설정되어 N9K-1을 모든 VLAN의 루트 브리지로 만듭니다. N9K-2는 모든 VLAN에 대해 스패닝 트리 우선순위 값 4096으로 설정되어 N9K-2를 모든 VLAN의 보조 루트 브리지로 만듭니다. Access-1은 레이어 2 스위치 포트를 통해 N9K-1 및 N9K-2에 이중 연결된 스위치입니다. 이러한 스위치 포트는 포트 채널에 번들링되지 않으므로, 스패닝 트리 프로토콜은 N9K-1에 연결된 링크를 지정된 루트 상태에 두고 N9K-2에 연결된 링크를 대체 차단 상태에 둡니다.

하드웨어 실패, 전원 실패 또는 스위치를 다시 로드하는 것으로 인해 N9K-1이 오프라인 상태가 되는 실패 시나리오를 가정해 보겠습니다. N9K-2는 시스템 MAC 주소를 브리지 ID로 사용하여 스패닝 트리 BPDU를 알림으로써 자신을 모든 VLAN에 대한 루트 브리지로 어설션합니다. Access-1은 루트 브리지의 ID가 변경된 것을 확인합니다. 또한 지정된 루트 포트가 다운/다운 상태로 전환됩니다. 즉, 새 지정된 루트 포트가 N9K-2를 향하는 대체 차단 상태에 있던 링크입니다.

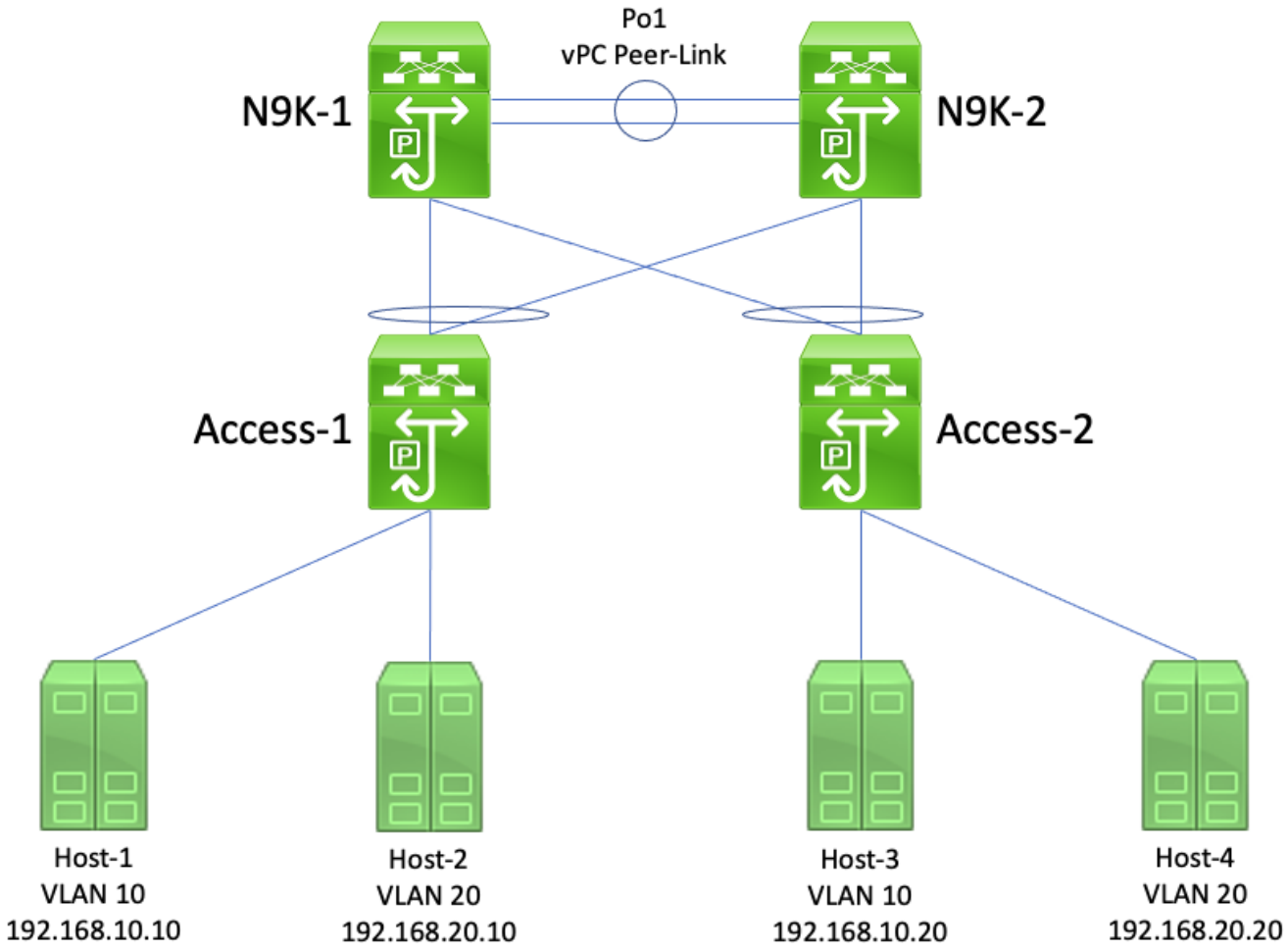
지정된 루트 포트가 변경되면 모든 비 엣지 스패닝 트리 포트가 스패닝 트리 프로토콜 유한 상태 머신(Blocking, Learning 및 Forwarding)을 통과하게 되며, 설정된 스패닝 트리 프로토콜 포워딩 지연

타이머(기본 15초)와 동일하게 일시 중지됩니다. 이 프로세스는 네트워크에 심각한 지장을 줄 수 있습니다.

vPC 피어 스위치 기능 향상이 활성화된 동일한 실패 시나리오에서 N9K-1 및 N9K-2는 모두 공유 vPC 시스템 MAC 주소를 브리지 ID로 사용하여 동일한 스패닝 트리 BPDU를 전송합니다. N9K-1이 실패할 경우 N9K-2는 동일한 스패닝 트리 BPDU를 계속 전송합니다. 따라서 Access-1은 N9K-2로의 대체 차단 링크를 Designated Root 상태로 즉시 전환하고 링크를 통해 트래픽 포워딩을 시작합니다. 또한 스패닝 트리 루트 브리지 ID가 변경되지 않으므로 비 엣지 포트가 스패닝 트리 프로토콜 유한 상태 머신을 통과하지 않으므로 네트워크에서 관찰되는 중단의 규모가 감소합니다.

동적으로 학습된 MAC 주소를 플러시하는 vPC 연결 브리지

여기에 있는 토폴로지를 고려해 보십시오.



이 토폴로지에서 N9K-1 및 N9K-2는 VLAN 10과 VLAN 20 사이에서 VLAN 간 라우팅을 수행하는 vPC 도메인의 vPC 피어입니다. N9K-1은 VLAN 10 및 VLAN 20에 대해 스패닝 트리 우선순위 값 0으로 설정되어 N9K-1을 두 VLAN의 루트 브리지로 만듭니다. N9K-2는 VLAN 10 및 VLAN 20에 대해 스패닝 트리 우선순위 값 4096으로 설정되어 N9K-2를 두 VLAN의 보조 루트 브리지로 만듭니다. Host-1, Host-2, Host-3 및 Host-4는 모두 지속적으로 서로 통신합니다.

하드웨어 실패, 전원 실패 또는 스위치를 다시 로드하는 것으로 인해 N9K-1이 오프라인 상태가 되는 실패 시나리오를 가정해 보겠습니다. N9K-2는 시스템 MAC 주소를 브리지 ID로 사용하여 스패닝 트리 BPDU를 알림으로써 자신을 VLAN 10 및 VLAN 20에 대한 루트 브리지로 어설션합니다.

Access-1 및 Access-2는 루트 브리지 ID의 변경을 확인하고, 스패닝 트리는 그대로 유지되지만(즉, N9K-1 및 N9K-2를 향하는 vPC는 지정된 루트 포트로 유지됨) Access-1 및 Access-2는 VLAN 10 및 VLAN 20의 모든 동적으로 학습된 MAC 주소를 플러시합니다.

대부분의 환경에서 동적으로 학습된 MAC 주소를 플러시하는 것은 최소한의 영향을 미칩니다. (실패한 동안 N9K-1로 전송되어 손실된 패킷을 제외하고) 손실되는 패킷이 없지만 브로드캐스트 도메인의 모든 스위치가 동적 MAC 주소를 다시 학습하는 동안 트래픽은 알 수 없는 유니캐스트 트래픽으로 각 브로드캐스트 도메인 내에서 일시적으로 플러딩됩니다.

vPC 피어 스위치 기능 향상이 활성화된 동일한 실패 시나리오에서 N9K-1 및 N9K-2는 모두 공유 vPC 시스템 MAC 주소를 브리지 ID로 사용하여 동일한 스패닝 트리 BPDU를 전송합니다. N9K-1이 실패할 경우 N9K-2는 동일한 스패닝 트리 BPDU를 계속 전송합니다. 결과적으로 Access-1 및 Access-2는 스패닝 트리 토폴로지의 변경을 알지 못합니다. 이 관점에서 루트 브리지의 스패닝 트리 BPDU는 동일하므로 관련 VLAN으로부터 동적으로 학습된 MAC 주소를 플러시할 필요가 없습니다. 이렇게 하면 이 실패 시나리오에서 각 브로드캐스트 도메인에서 알 수 없는 유니캐스트 트래픽이 플러딩되는 것을 방지할 수 있습니다.

vPC 피어 게이트웨이

이 섹션에서는 peer-gateway vPC 도메인 설정 명령을 통해 활성화되는 vPC 피어 게이트웨이 기능 향상에 대해 설명합니다.

개요

vPC 도메인에 설정된 Nexus 스위치는 기본적으로 듀얼 액티브 FHRP(First Hop Redundancy Protocol) 포워딩을 수행합니다. 즉, vPC 피어가 스위치에 설정된 HSRP(Hot-Standby Router Protocol) 또는 VRRP(Virtual Router Redundancy Protocol) 그룹에 속하는 대상 MAC 주소가 있는 패킷을 수신하면 스위치는 HSRP 또는 VRRP 제어플레인 상태와 무관하게 로컬 라우팅 테이블에 따라 패킷을 라우팅합니다. 다시 말해 HSRP 대기 또는 VRRP 백업 상태의 vPC 피어가 HSRP 또는 VRRP 가상 MAC 주소로 향하는 패킷을 라우팅하는 것은 예상되는 동작입니다.

vPC 피어가 FHRP 가상 MAC 주소로 향하는 패킷을 라우팅하면 새 소스 및 대상 MAC 주소로 패킷을 다시 씁니다. 소스 MAC 주소는 패킷이 라우팅되는 VLAN 내에서 vPC 피어의 SVI(Switched Virtual Interface)의 MAC 주소가 됩니다. 대상 MAC 주소는 vPC 피어의 로컬 라우팅 테이블에 따라 패킷의 대상 IP 주소에 대한 다음 홉 IP 주소와 연결된 MAC 주소가 됩니다. VLAN 간 라우팅 시나리오에서 패킷이 다시 쓰여진 후 패킷의 대상 MAC 주소는 패킷의 최종 목적지가 될 호스트의 MAC 주소가 됩니다.

일부 호스트는 최적화 기능으로 표준 포워딩 동작을 따르지 않습니다. 이 동작을 사용하면 호스트는 수신 패킷에 응답할 때 라우팅 테이블 및/또는 ARP 캐시 조회를 수행하지 않습니다. 대신 호스트는 응답 패킷에 대한 수신 패킷의 소스 및 대상 MAC 주소를 뒤집습니다. 다시 말해 수신 패킷의 소스 MAC 주소는 응답 패킷의 대상 MAC 주소가 되고, 수신 패킷의 대상 MAC 주소는 응답 패킷의 소스 MAC 주소가 됩니다. 이 동작은 로컬 라우팅 테이블 및/또는 ARP 캐시 조회를 수행하고 응답 패킷의 대상 MAC 주소를 FHRP 가상 MAC 주소로 설정하는 표준 포워딩 동작을 따르는 호스트와 다릅니다.

이 비표준 호스트 동작은 호스트에서 생성된 응답 패킷이 하나의 vPC 피어로 전달되지만 vPC를 다

른 vPC 피어로 이그레스하는 경우 vPC 루프 회피 규칙을 위반할 수 있습니다. 다른 vPC 피어는 해당 vPC 피어가 소유한 MAC 주소로 향하는 패킷을 수신하고, 패킷의 대상 MAC 주소 필드에 있는 MAC 주소를 소유한 vPC 피어로 vPC 피어 링크에서 패킷을 전달합니다. MAC 주소를 소유한 vPC 피어는 패킷을 로컬로 라우팅하려고 시도합니다. 패킷이 vPC를 이그레스해야 하는 경우 vPC 피어는 vPC 루프 회피 규칙 위반으로 인해 이 패킷을 삭제합니다. 결과적으로 이 비표준 동작을 사용하여 호스트에서 발생하거나 호스트로 향하는 일부 플로우의 연결 문제 또는 패킷 손실을 관찰할 수 있습니다.

이 비표준 동작을 활용하여 호스트에서 발생하는 패킷 손실을 제거하기 위해 vPC 피어 게이트웨이 기능 향상이 도입되었습니다. 이는 하나의 vPC 피어가 다른 vPC 피어의 MAC 주소로 향하는 패킷을 로컬로 라우팅하여 원격 vPC 피어로 향하는 패킷을 라우팅하기 위해 vPC 피어 링크를 이그레스할 필요가 없도록 하면서 이루어집니다. 다시 말해 vPC 피어 게이트웨이 기능 향상을 통해 하나의 vPC 피어가 원격 vPC 피어를 "대신하여" 패킷을 라우팅할 수 있습니다. peer-gateway vPC 도메인 설정 명령을 통해 vPC 피어 게이트웨이 기능 향상을 활성화할 수 있습니다.

경고

vPC 또는 vPC VLAN을 통한 유니캐스트 라우팅 프로토콜 인접성 플래핑

두 개의 vPC 피어와 vPC 연결 라우터 또는 vPC 고립 포트를 통해 연결된 라우터 간에 동적 유니캐스트 라우팅 프로토콜 인접성이 형성되는 경우, Routing/Layer 3 over vPC 기능 향상이 그 직후에 설정되지 않으면 vPC 피어 게이트웨이 기능 향상 활성화 후 라우팅 프로토콜 인접성이 계속해서 플래핑을 시작할 수 있습니다. 이러한 실패 시나리오는 이 문서의 vPC 피어 게이트웨이가 있는 vPC를 통한 유니캐스트 라우팅 프로토콜 인접성 실패 시나리오 예시 섹션과 vPC 피어 게이트웨이가 있는 vPC를 통한 유니캐스트 라우팅 프로토콜 인접성 섹션에 설명되어 있습니다.

이 문제를 해결하려면 peer-gateway vPC 도메인 설정 명령으로 vPC 피어 게이트웨이 기능 향상을 활성화한 직후 바로 layer3 peer-router vPC 도메인 설정 명령을 사용하여 Routing/Layer 3 over vPC 기능 향상을 활성화합니다.

ICMP 및 ICMPv6 리디렉션 자동 비활성화

vPC 피어 게이트웨이 기능 향상이 활성화되면 ICMP 및 ICMPv6 리디렉션 패킷 생성이 모든 vPC VLAN SVI(즉, vPC 피어 링크를 통해 트렁크된 VLAN과 연결된 모든 SVI)에서 자동으로 비활성화됩니다. 스위치는 모든 vPC VLAN SVI에서 no ip redirects 및 no ipv6 redirects 설정을 통해 이를 수행합니다. 그러면 스위치를 인그레스하지만 스위치 vPC 피어의 대상 MAC 및 IP 주소가 있는 패킷에 대한 응답으로 스위치가 ICMP 리디렉션 패킷을 생성할 수 없습니다.

특정 VLAN 내 환경에서 ICMP 또는 ICMPv6 리디렉션 패킷이 필요한 경우 peer-gateway exclude-vlan<vlan-id> vPC 도메인 설정 명령을 사용하여 vPC 피어 게이트웨이 기능 향상을 활용하는 데 이 VLAN을 제외해야 합니다.

참고: Nexus 9000 시리즈 스위치에서는 peer-gateway exclude-vlan<vlan-id> vPC 도메인 설정 명령이 지원되지 않습니다.

설정

vPC 피어 게이트웨이 기능을 설정하는 방법의 예시는 여기에서 확인할 수 있습니다.

이 예시에서 N9K-1 및 N9K-2는 vPC 도메인의 vPC 피어입니다. 두 vPC 피어 모두 VLAN 10에 대해 설정된 HSRP 그룹을 보유합니다. N9K-1은 우선순위가 150인 HSRP 활성 라우터이고, N9K-2는 기본 우선순위가 100인 HSRP 대기 라우터입니다.

```
<#root>

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)
```

N9K-1의 VLAN 10 SVI MAC 주소는 00ee.ab67.db47이고, N9K-2의 VLAN 10 SVI MAC 주소는 00ee.abd8.747f입니다. VLAN 10의 HSRP 가상 MAC 주소는 0000.0c07.ac0a입니다. 이 상태에서 각 스위치의 VLAN 10 SVI MAC 주소 및 HSRP 가상 MAC 주소는 각 스위치의 MAC 주소 테이블에 있습니다. 각 스위치의 VLAN 10 SVI MAC 주소 및 HSRP 가상 MAC 주소에는 게이트웨이(G) 플래그가 있습니다. 이 플래그는 스위치가 이 MAC 주소로 향하는 패킷을 로컬로 라우팅함을 나타냅니다.

N9K-1의 MAC 주소 테이블에는 N9K-2의 VLAN 10 SVI MAC 주소에 대한 게이트웨이 플래그가 없습니다. 마찬가지로 N9K-2의 MAC 주소 테이블에는 N9K-1의 VLAN 10 SVI MAC 주소에 대한 게이트웨이 플래그가 없습니다.

<#root>

```
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)
```

peer-gateway vPC 도메인 설정 명령을 통해 vPC 피어 게이트웨이 기능 향상을 활성화할 수 있습니다. 이렇게 하면 스위치가 수신된 패킷을 vPC 피어 링크에서 학습된 vPC 피어의 MAC 주소에 속하는 대상 MAC 주소를 사용하여 로컬로 라우팅할 수 있습니다. 이 작업은 스위치의 MAC 주소 테이블 내에 있는 vPC 피어의 MAC 주소에 게이트웨이 플래그를 설정하여 이루어집니다.

```
<#root>

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#
```

vPC 피어의 MAC에 대한 MAC 주소 테이블에 게이트웨이 플래그가 있는지 확인하여 vPC 피어 게이트웨이 기능 향상 정상적으로 작동하는지 확인할 수 있습니다.

```
<#root>

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)
```

영향

vPC 피어 게이트웨이 기능 향상 활성화가 미치는 영향은 아래 하위 섹션에서 설명하는 것과 같이 주변 토폴로지 및 연결된 호스트의 동작에 따라 달라질 수 있습니다. 아래 하위 섹션 중 어느 것도 사용자 환경에 해당되지 않는 경우 vPC 피어 게이트웨이 기능 향상을 활성화해도 중단이 발생하지 않으며 환경에 영향을 미치지 않습니다.

vPC 또는 vPC VLAN을 통한 유니캐스트 라우팅 프로토콜 인접성 플래핑

두 개의 vPC 피어와 vPC 연결 라우터 또는 vPC 고립 포트를 통해 연결된 라우터 간에 동적 유니캐스트 라우팅 프로토콜 인접성이 형성되는 경우, Routing/Layer 3 over vPC 기능 향상이 그 직후에 설정되지 않으면 vPC 피어 게이트웨이 기능 향상 활성화 후 라우팅 프로토콜 인접성이 계속해서 플래핑을 시작할 수 있습니다. 이러한 실패 시나리오는 이 문서의 vPC 피어 게이트웨이가 있는 vPC를 통한 유니캐스트 라우팅 프로토콜 인접성 실패 시나리오 예시 섹션과 vPC 피어 게이트웨이가 있는 vPC를 통한 유니캐스트 라우팅 프로토콜 인접성 섹션에 설명되어 있습니다.

이 문제를 해결하려면 peer-gateway vPC 도메인 설정 명령으로 vPC 피어 게이트웨이 기능 향상을 활성화한 직후 바로 layer3 peer-router vPC 도메인 설정 명령을 사용하여 Routing/Layer 3 over vPC 기능 향상을 활성화합니다.

ICMP 및 ICMPv6 리디렉션 자동 비활성화

vPC 피어 게이트웨이 기능 향상이 활성화되면 ICMP 및 ICMPv6 리디렉션 패킷 생성이 모든 vPC VLAN SVI(즉, vPC 피어 링크를 통해 트렁크된 VLAN과 연결된 모든 SVI)에서 자동으로 비활성화됩니다. 스위치는 모든 vPC VLAN SVI에서 no ip redirects 및 no ipv6 redirects 설정을 통해 이를 수행합니다. 그러면 스위치를 인그레스하지만 스위치 vPC 피어의 대상 MAC 및 IP 주소가 있는 패킷에 대한 응답으로 스위치가 ICMP 리디렉션 패킷을 생성할 수 없습니다.

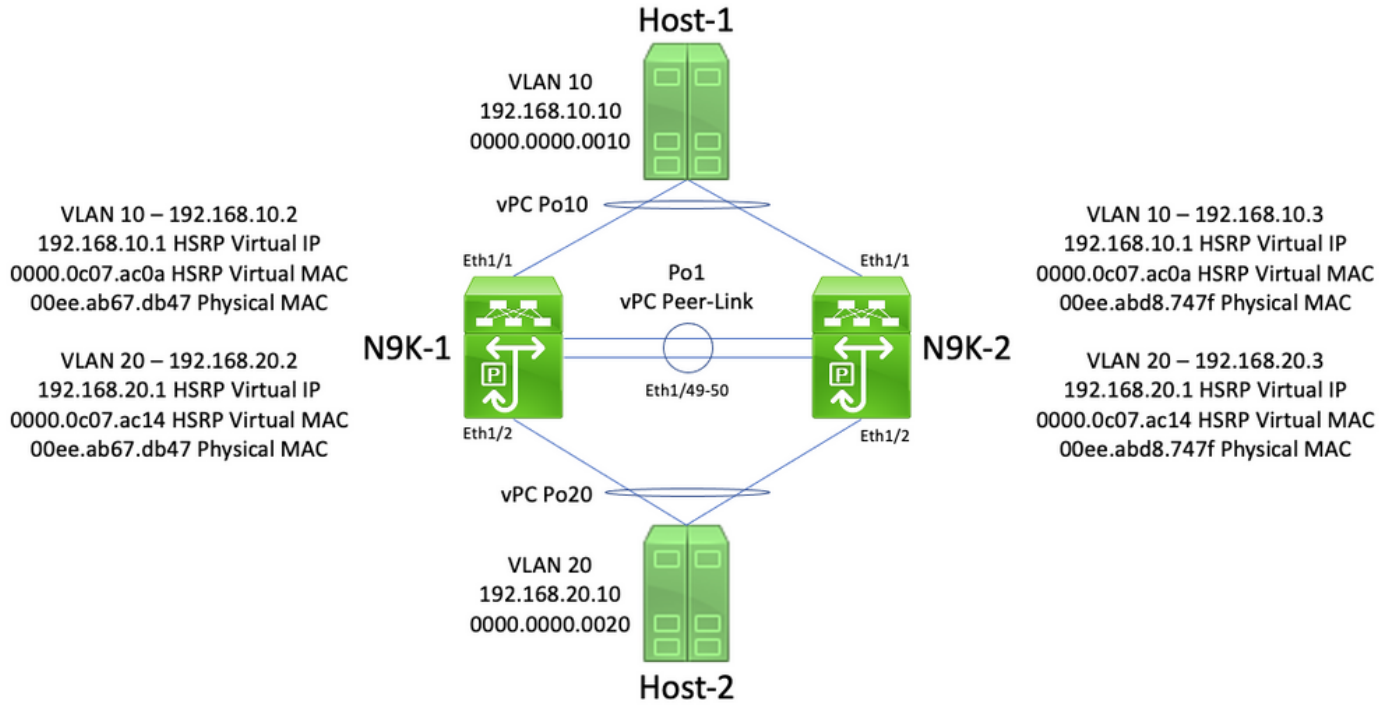
특정 VLAN 내 환경에서 ICMP 또는 ICMPv6 리디렉션 패킷이 필요한 경우 peer-gateway exclude-vlan<vlan-id> vPC 도메인 설정 명령을 사용하여 vPC 피어 게이트웨이 기능 향상을 활용하는 데 이 VLAN을 제외해야 합니다.

참고: Nexus 9000 시리즈 스위치에서는 peer-gateway exclude-vlan<vlan-id> vPC 도메인 설정 명령이 지원되지 않습니다.

실패 시나리오 예시

비표준 포워딩 동작을 사용하는 vPC 연결 호스트

여기에 있는 토폴로지를 고려해 보십시오.

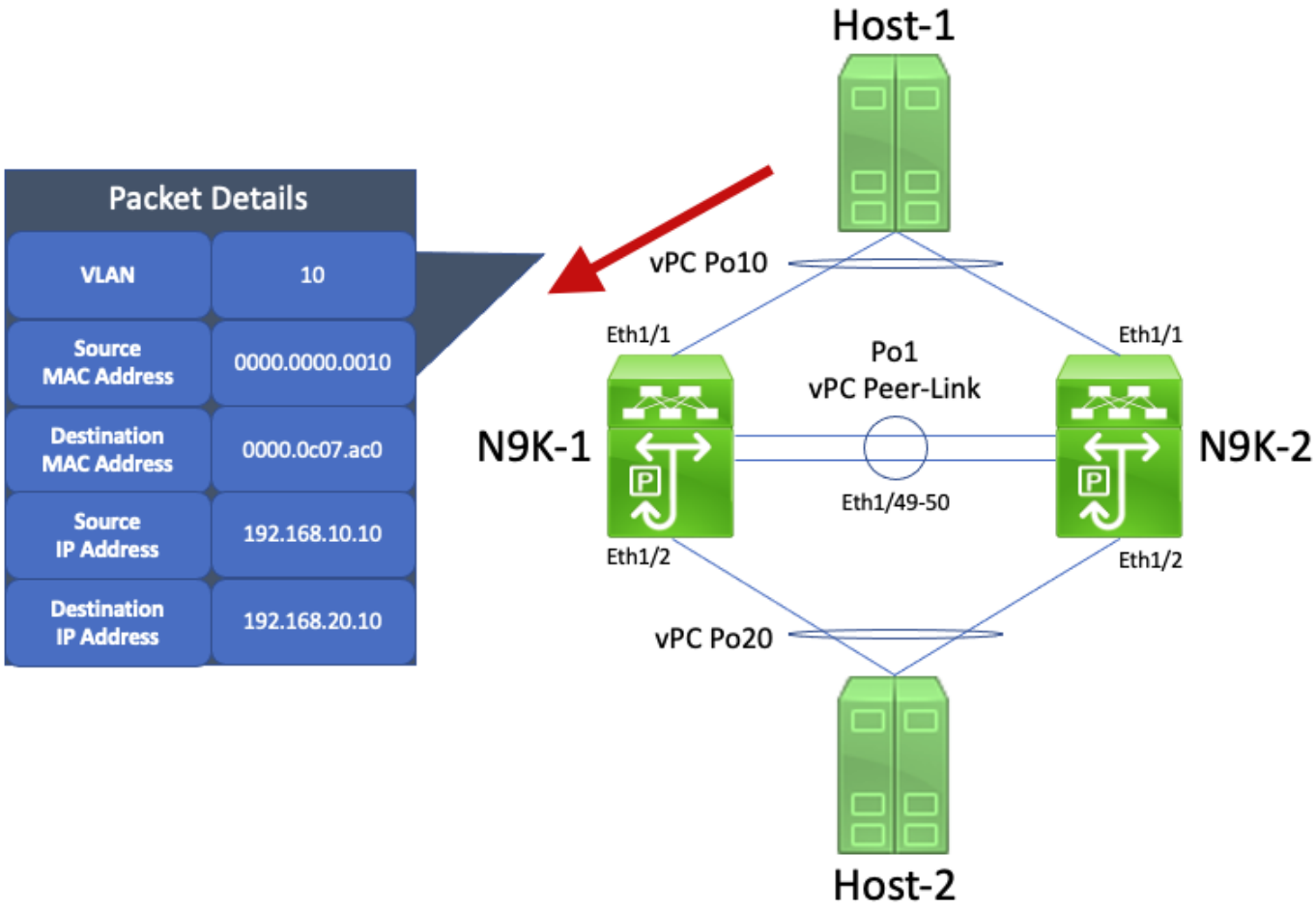


이 토폴로지에서 N9K-1 및 N9K-2는 VLAN 10과 VLAN 20 사이에서 VLAN 간 라우팅을 수행하는 vPC 도메인의 vPC 피어입니다. 인터페이스 Po1은 vPC 피어 링크입니다. 이름이 Host-1인 호스트는 vPC Po10을 통해 VLAN 10의 N9K-1 및 N9K-2에 연결됩니다. Host-1의 IP 주소는 192.168.10.10이며 MAC 주소는 0000.0000.0010입니다. 이름이 Host-2인 호스트는 vPC Po20을 통해 VLAN 20의 N9K-1 및 N9K-2에 연결됩니다. Host-2의 IP 주소는 192.168.20.10이며 MAC 주소는 0000.0000.0020입니다.

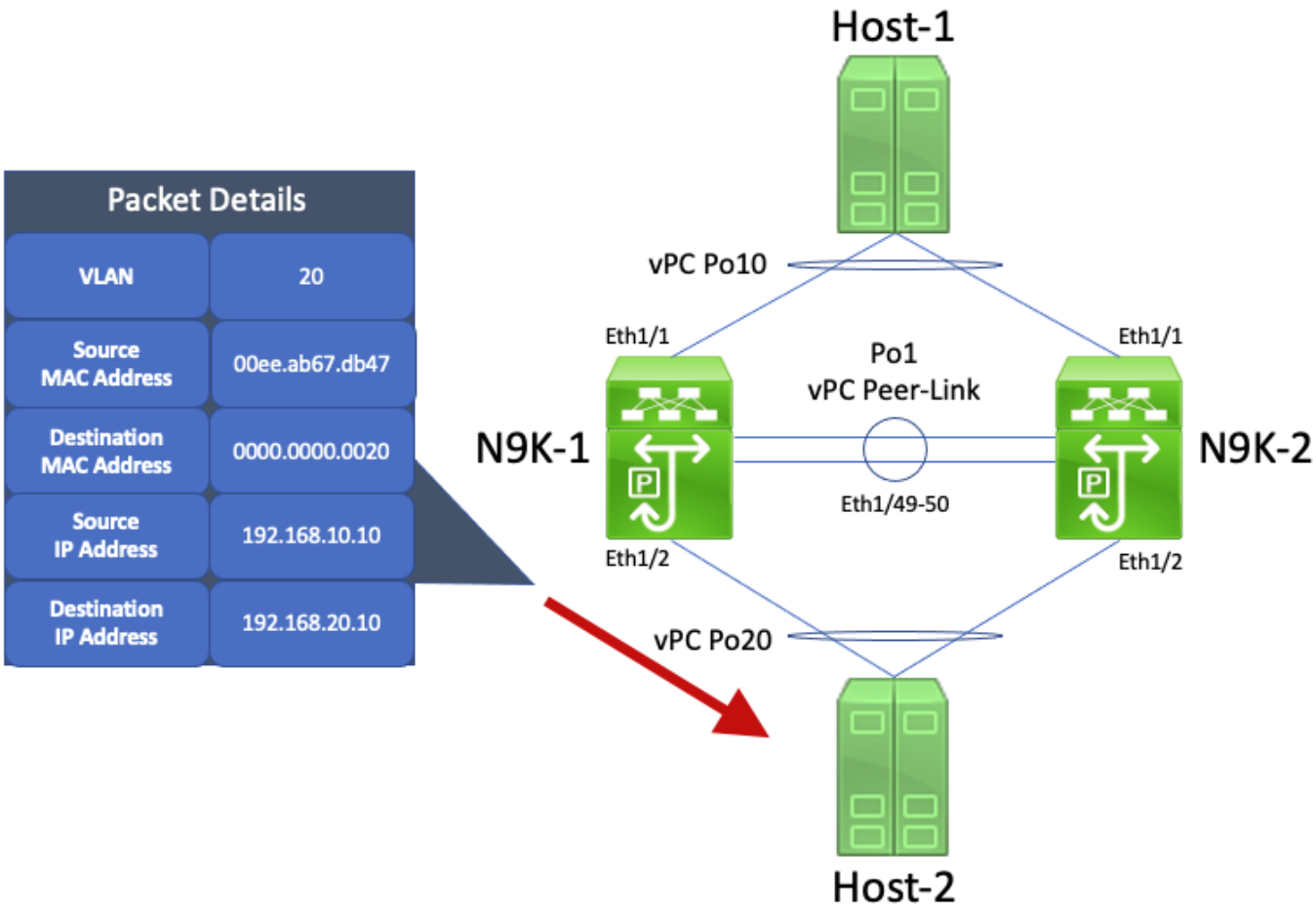
N9K-1 및 N9K-2 모두 VLAN 10 및 VLAN 20에 SVI가 있으며, 각 SVI에서 HSRP가 활성화되어 있습니다. N9K-1의 VLAN 10 인터페이스 IP 주소는 192.168.10.2이고, N9K-1의 VLAN 20 인터페이스 IP 주소는 192.168.20.2입니다. 두 N9K-1의 SVI에는 물리적 MAC 주소 00ee.ab67.db47이 있습니다. N9K-2의 VLAN 10 인터페이스 IP 주소는 1921.68.10.3이고, N9K-2의 VLAN 20 인터페이스 IP 주소는 192.168.20.3입니다. 두 N9K-2의 SVI에는 물리적 MAC 주소 00ee.abd8.747f가 있습니다. VLAN 10의 HSRP 가상 IP 주소는 192.168.10.1이고, HSRP 가상 MAC 주소는 0000.0c07.ac0a입니다. VLAN 20의 HSRP 가상 IP 주소는 192.168.20.1이고, HSRP 가상 MAC 주소는 0000.0c07.ac14입니다.

Host-1이 Host-2에 ICMP 에코 요청 패킷을 보내는 시나리오를 가정 해 보겠습니다. Host-1이 기본 게이트웨이(HSRP 가상 IP 주소)에 대해 ARP를 확인한 후, Host-1은 표준 포워딩 동작을 따르고 소스 IP 주소가 192.168.10.10, 대상 IP 주소가 192.168.20.10, 소스 MAC 주소 0000.0000.0010이고

대상 MAC 주소가 0000.0c07.ac0a인 ICMP 에코 요청 패킷을 생성합니다. 이 패킷은 N9K-1로 이그레스합니다. 이에 대한 시각적 예시가 여기에 나와 있습니다.

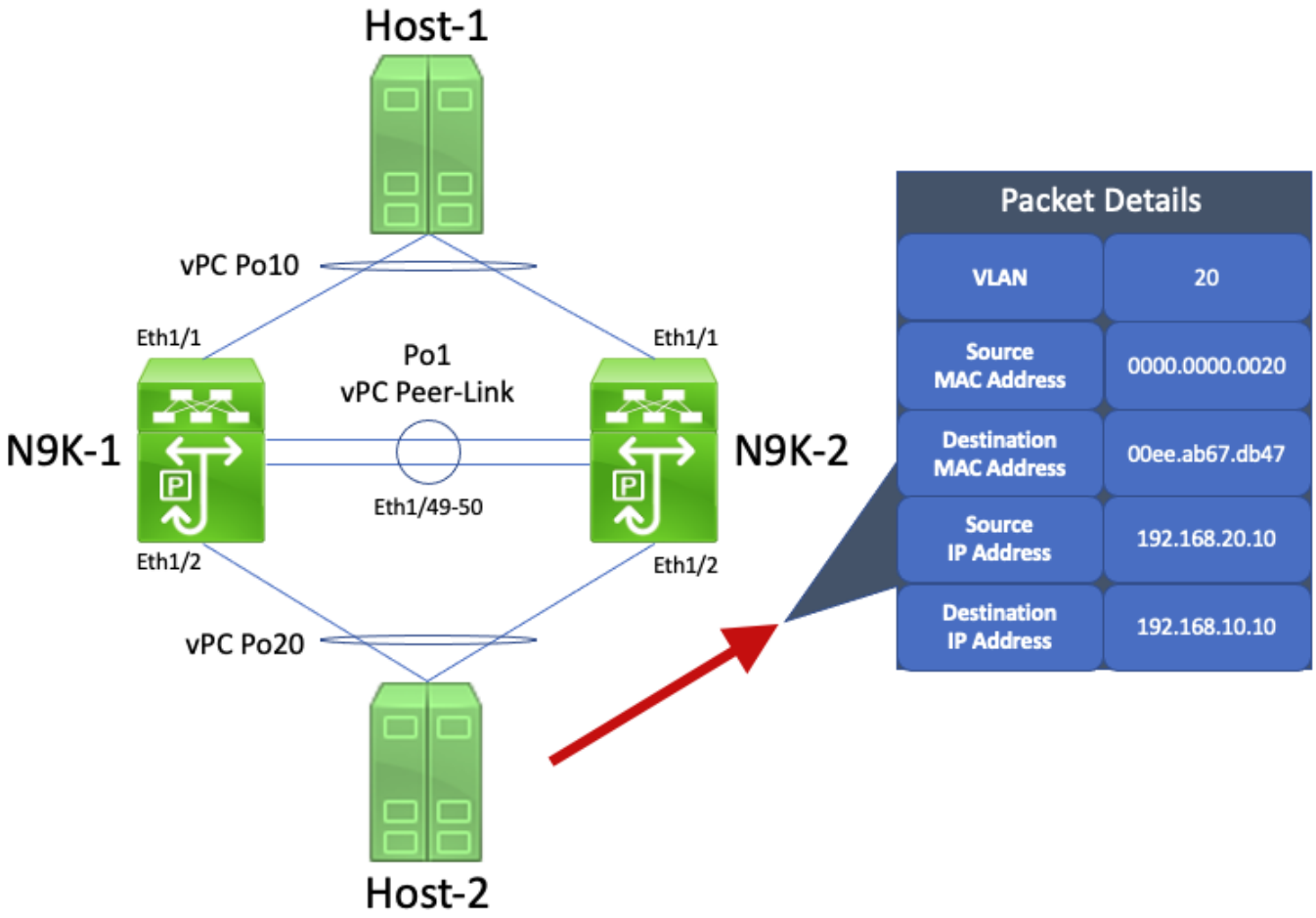


N9K-1이 이 패킷을 수신합니다. 이 패킷은 HSRP 가상 MAC 주소로 향하므로 N9K-1은 HSRP 제어 플레인 상태와 무관하게 로컬 라우팅 테이블에 따라 이 패킷을 라우팅할 수 있습니다. 이 패킷은 VLAN 10에서 VLAN 20으로 라우팅됩니다. 패킷 라우팅의 일부로 N9K-1은 패킷의 소스 및 대상 MAC 주소 필드를 다시 주소 지정하여 패킷 다시 쓰기를 수행합니다. 패킷의 새 소스 MAC 주소는 N9K-1의 VLAN 20 SVI와 연결된 물리적 MAC 주소(00ee.ab67.db47)가 되고, 새 대상 MAC 주소는 Host-2와 연결된 MAC 주소(0000.0000.0020)가 됩니다. 이에 대한 시각적 예시가 여기에 나와 있습니다.

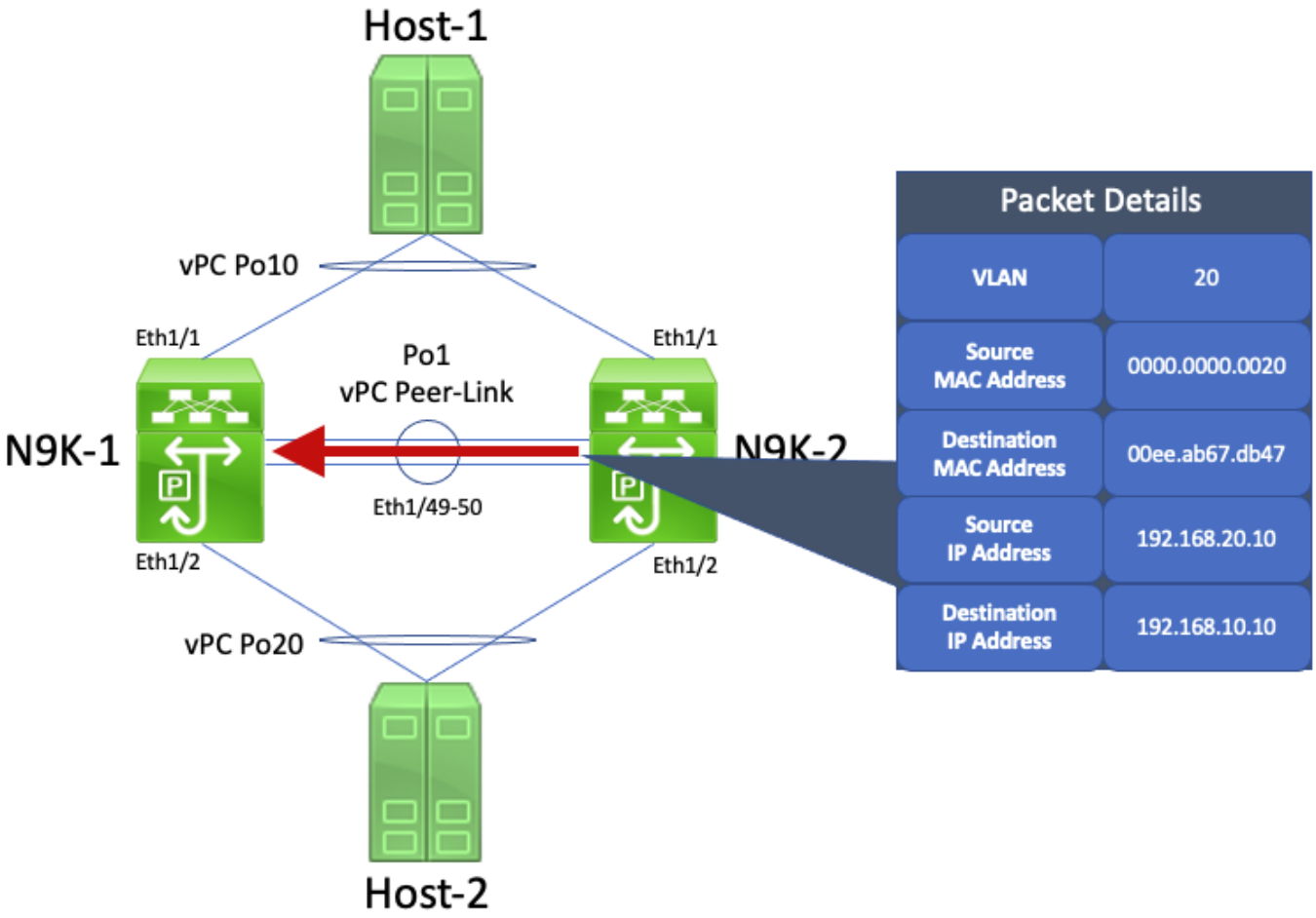


Host-2는 이 패킷을 수신하고 Host-1의 ICMP 에코 요청 패킷에 대한 응답으로 ICMP 에코 응답 패킷을 생성합니다. 하지만 Host-2가 표준 포워딩 동작을 따르지 않는 경우. 포워딩 최적화를 위해 Host-2는 Host-1의 IP 주소(192.168.10.10)에 대한 라우팅 테이블 또는 ARP 캐시 조회를 수행하지 않습니다. 대신 Host-2에서 원래 수신했던 ICMP 에코 요청 패킷 호스트의 소스 MAC 주소 및 대상 MAC 주소 필드를 반전시킵니다. 따라서 Host-2에서 생성된 ICMP 에코 응답 패킷의 소스 IP 주소는 192.168.20.10, 대상 IP 주소는 192.168.10.10, 소스 MAC 주소는 0000.0000.0020, 대상 MAC 주소는 00ee.ab67.db47입니다.

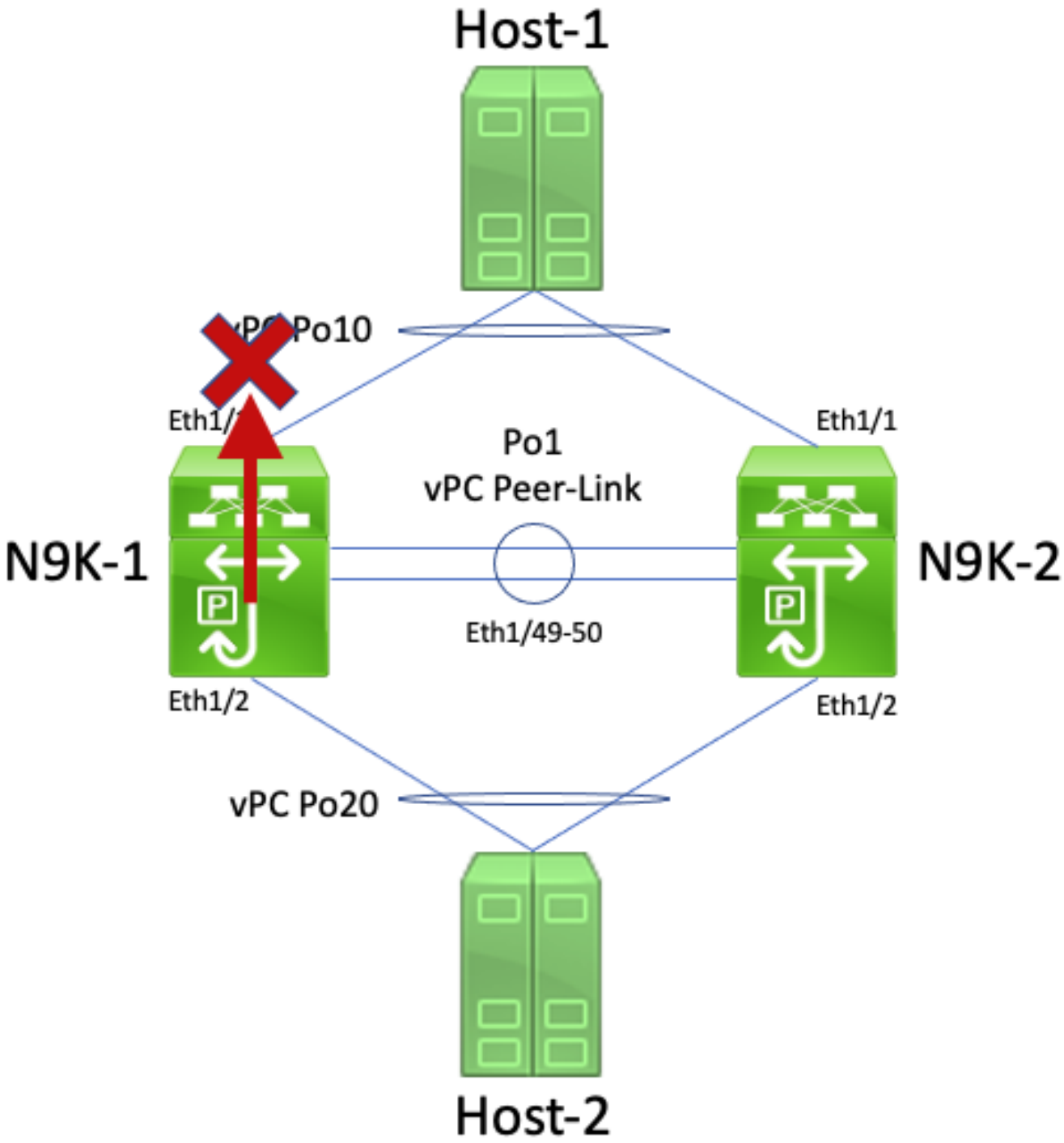
이 ICMP 에코 응답 패킷이 N9K-1로 이그레스되는 경우 이 패킷은 문제 없이 Host-1로 포워딩됩니다. 하지만 여기에 나와 있는 것처럼 이 ICMP 에코 응답 패킷이 N9K-2로 이그레스되는 시나리오를 고려해 보십시오.



N9K-2가 이 패킷을 수신합니다. 이 패킷은 N9K-1 VLAN 20 SVI의 물리적 MAC 주소로 향하므로, N9K-2는 N9K-1을 대신하여 이 패킷을 라우팅할 수 없기에 vPC 피어 링크를 통해 N9K-1로 이 패킷을 포워딩합니다. 이에 대한 시각적 예시가 여기에 나와 있습니다.



N9K-1이 이 패킷을 수신합니다. 이 패킷은 N9K-1 VLAN 20 SVI의 물리적 MAC 주소로 향하므로 N9K-1은 HSRP 제어플레인 상태와 무관하게 로컬 라우팅 테이블에 따라 이 패킷을 라우팅할 수 있습니다. 이 패킷은 VLAN 20에서 VLAN 10으로 라우팅됩니다. 하지만 이 경로의 이그레스 인터페이스는 N9K-2에 있는 vPC Po10으로 확인됩니다. 이는 vPC 루프 회피 규칙을 위반하는 것입니다. N9K-1이 vPC 피어 링크를 통해 패킷을 수신하는 경우, N9K-1은 동일한 vPC 인터페이스가 N9K-2에서 작동하면 vPC 인터페이스에서 해당 패킷을 포워딩할 수 없습니다. N9K-1은 이 위반의 결과에 따라 이 패킷을 삭제합니다. 이에 대한 시각적 예시가 여기에 나와 있습니다.



peer-gateway vPC 도메인 설정 명령으로 vPC 피어 게이트웨이 기능 향상을 활성화하여 이 문제를 해결할 수 있습니다. 이렇게 하면 패킷의 대상 MAC 주소를 N9K-2가 아닌 N9K-1이 소유하더라도 N9K-2가 N9K-1을 대신하여 ICMP 에코 응답 패킷(및 유사하게 주소가 지정된 기타 패킷)을 라우팅할 수 있습니다. 그 결과, N9K-2는 vPC 피어 링크를 통해 포워딩하는 대신 vPC Po10 인터페이스에서 이 패킷을 포워딩할 수 있습니다.

Routing/Layer 3 over vPC(Layer3 Peer-Router)

이 섹션에서는 layer3 peer-router vPC 도메인 설정 명령을 통해 활성화되는 Routing/Layer 3 over

vPC 기능 향상에 대해 설명합니다.

참고: vPC를 통한 멀티캐스트 라우팅 프로토콜 인접성(즉, PIM(Protocol Independent Multicast) 인접성)을 형성하는 것은 Routing/Layer 3 over vPC 기능 향상이 활성화된 상태에서 지원되지 않습니다.

개요

일부 환경에서는 고객이 vPC를 통해 라우터를 Nexus 스위치 쌍에 연결하고 두 vPC 피어 모두에서 vPC를 통해 유니캐스트 라우팅 프로토콜 인접성을 형성하려고 합니다. 또는 고객이 vPC VLAN을 통해 라우터를 단일 vPC 피어에 연결하고 vPC VLAN을 통해 두 vPC 피어와 유니캐스트 라우팅 프로토콜 인접성을 형성하고자 할 수 있습니다. 그에 따라 vPC 연결 라우터는 두 Nexus 스위치에 의해 알려진 접두사에 대해 ECMP(Equal-Cost Multi-Path)를 갖게 됩니다. vPC 연결 라우터와 두 vPC 피어 간에 전용 라우팅 링크를 사용하여 IP 주소 사용률(4개의 IP 주소 대신 3개의 IP 주소가 필요함)을 유지하거나 설정 복잡성(특히 하위 인터페이스가 필요한 VRF-Lite 환경에서 SVI와 함께 라우팅되는 인터페이스)를 줄이는 것보다 선호됩니다.

이전에는 Cisco Nexus 플랫폼에서 vPC를 통해 유니캐스트 라우팅 프로토콜 인접성을 형성하는 것이 지원되지 않았습니다. 하지만 고객은 지원되지 않더라도 유니캐스트 라우팅 프로토콜 인접성이 vPC를 통해 문제 없이 형성되는 토폴로지를 구현했을 수 있습니다. vPC 연결 라우터 또는 vPC 피어 자체의 소프트웨어 업그레이드, 방화벽 페일오버 등과 같은 네트워크 변경이 발생한 후 vPC를 통한 유니캐스트 라우팅 프로토콜 인접성 작동이 중단되어 데이터플레인 트래픽의 패킷 손실이 발생하거나 vPC 유니캐스트 라우팅 프로토콜 인접성이 1개 또는 2개의 vPC 피어에서 발생하지 않게 됩니다. 이러한 시나리오가 실패하고 지원되지 않는 이유에 대한 기술적 세부 정보는 이 문서의 실패 시나리오 예시 섹션에서 설명합니다.

vPC를 통한 유니캐스트 라우팅 프로토콜 인접성 형성 지원을 추가하기 위해 Routing/Layer 3 over vPC 기능 향상이 도입되었습니다. 이는 TTL이 1인 유니캐스트 라우팅 프로토콜 패킷을 패킷의 TTL을 줄이지 않고 vPC 피어 링크를 통해 포워딩되도록 허용함으로써 이루어집니다. 이로 인해 vPC 또는 vPC VLAN을 통해 문제 없이 유니캐스트 라우팅 프로토콜 인접성을 형성할 수 있습니다. peer-gateway vPC 도메인 설정 명령으로 vPC 피어 게이트웨이 기능 향상을 활성화한 이후 바로 layer3 peer-router vPC 도메인 설정 명령을 사용하여 Routing/Layer 3 over vPC 기능 향상을 활성화할 수 있습니다.

각 Cisco Nexus 플랫폼에 대한 Routing/Layer 3 over vPC 기능 향상 지원이 도입된 NX-OS 소프트웨어 릴리스는 Nexus 플랫폼 문서의 가상 포트 채널을 통한 라우팅에 대해 지원되는 토폴로지 내에 있는 표 2("vPC VLAN을 통한 라우팅 프로토콜 인접성 지원")에서 설명되어 있습니다.

경고

간헐적 VPC-2-L3_VPC_UNEQUAL_WEIGHT 시스템 로그

Routing/Layer 3 over vPC 기능 향상이 활성화된 이후 두 vPC 피어 모두 1시간마다 다음 중 하나와 유사한 시스템 로그 생성을 시작합니다.

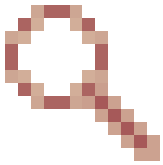
```
2021 May 26 19:13:47.079 switch %VPC-2-L3_VPC_UNEQUAL_WEIGHT: Layer3 peer-router is enabled. Please mak
2021 May 26 19:13:47.351 switch %VPC-2-L3_VPC_UNEQUAL_WEIGHT: Unequal weight routing is not supported i
```

이러한 시스템 로그가 스위치의 문제를 나타내는 것은 아닙니다. 이러한 시스템 로그는 두 vPC 피어가 모두 트래픽을 동일하게 라우팅할 수 있도록 Routing/Layer 3 over vPC 기능 향상이 활성화된 경우 라우팅 설정, 비용 및 가중치가 두 vPC 피어 간에 동일해야 함을 관리자에게 경고합니다. 하지만 반드시 vPC 피어 간에 라우팅 설정, 비용 또는 가중치 불일치가 있음을 나타내지는 않습니다.

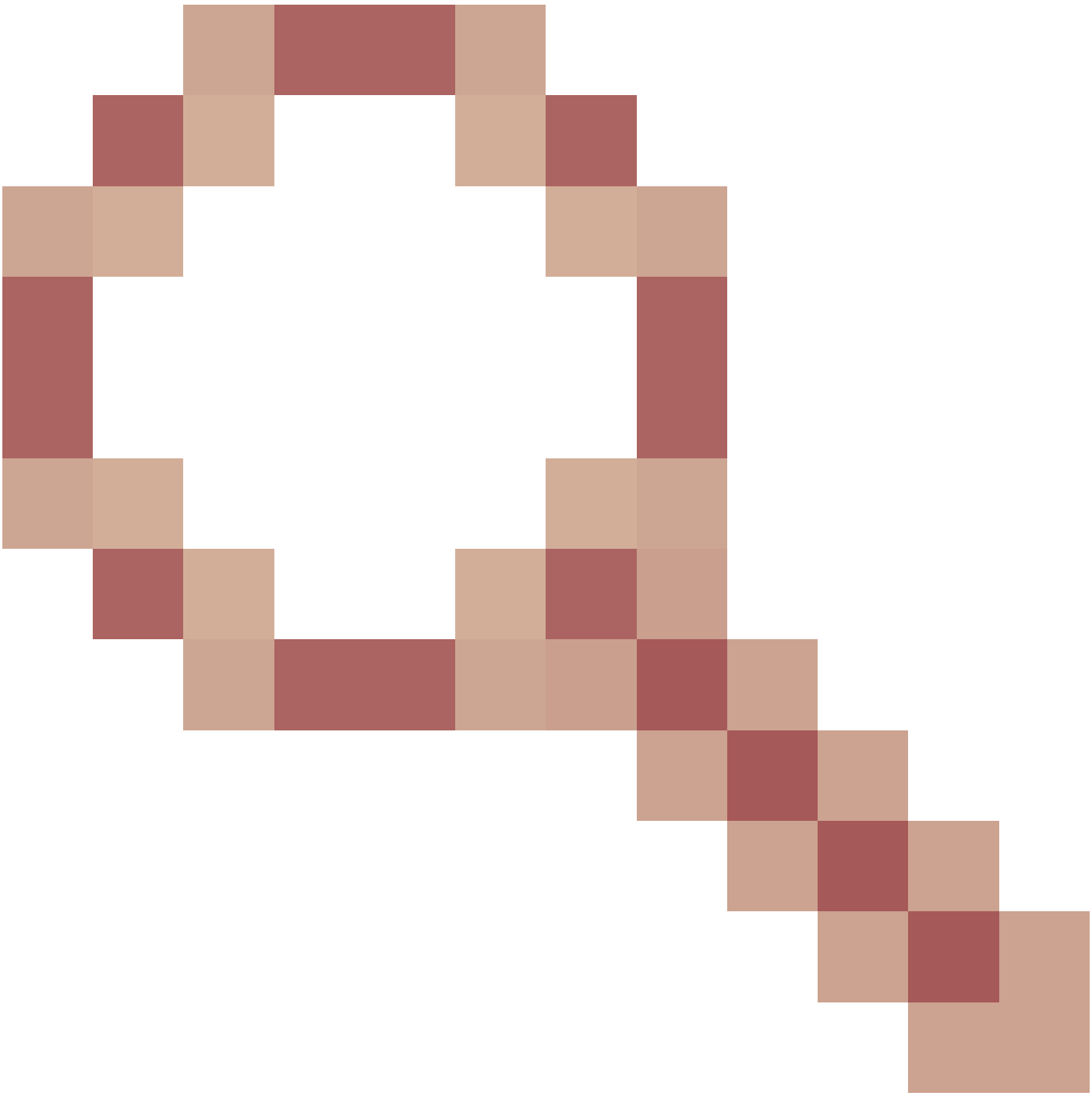
이러한 시스템 로그는 여기에 표시된 설정을 통해 비활성화할 수 있습니다.

```
<#root>

switch#

configure terminal

switch(config)#

vpc domain 1

switch(config-vpc-domain)#

no layer3 peer-router syslog

switch(config-vpc-domain)#

end

switch#
```

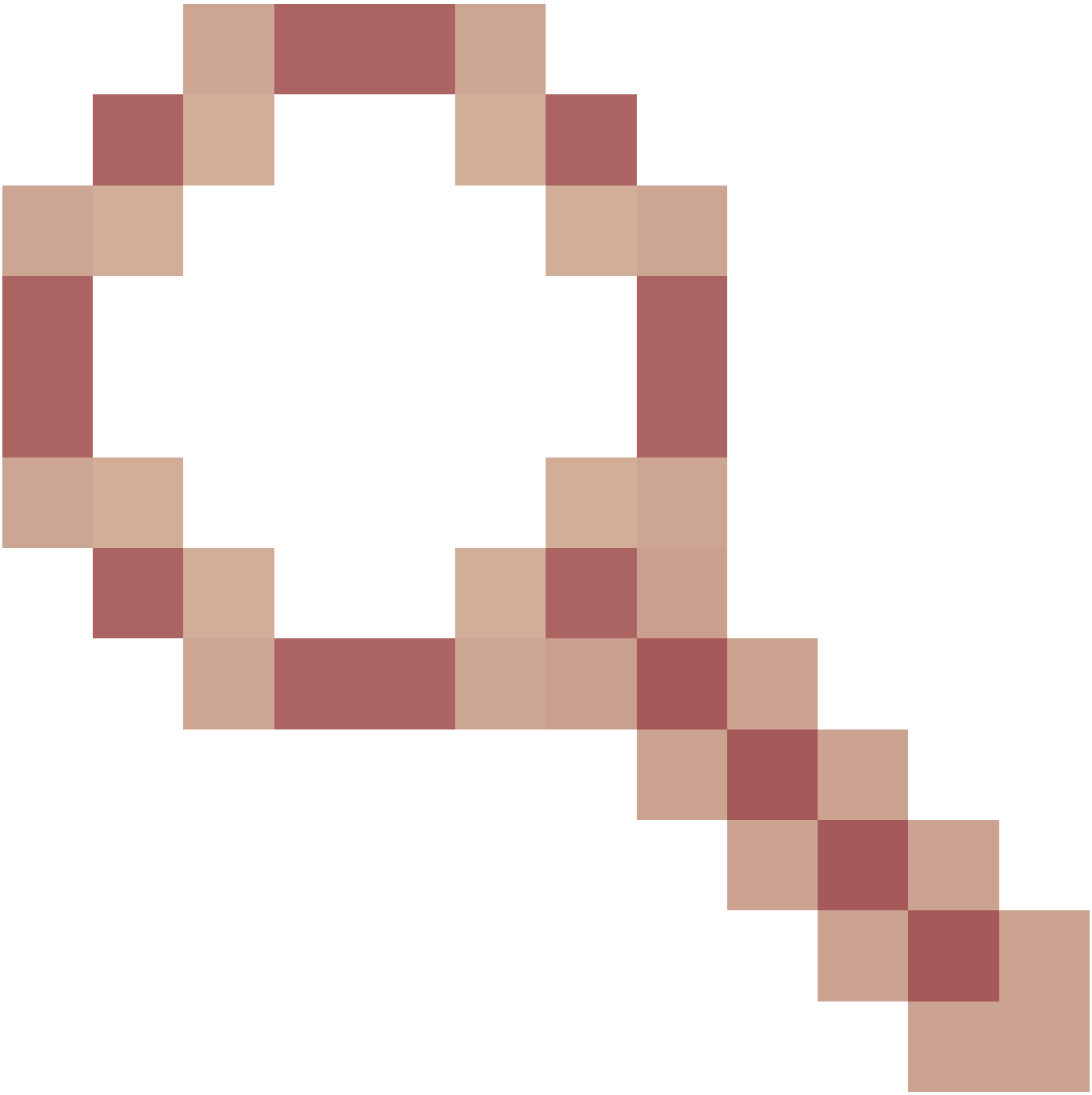
두 vPC 피어에서 시스템 로그를 비활성화하려면 이 설정을 두 vPC 피어에서 모두 수행해야 합니다
.



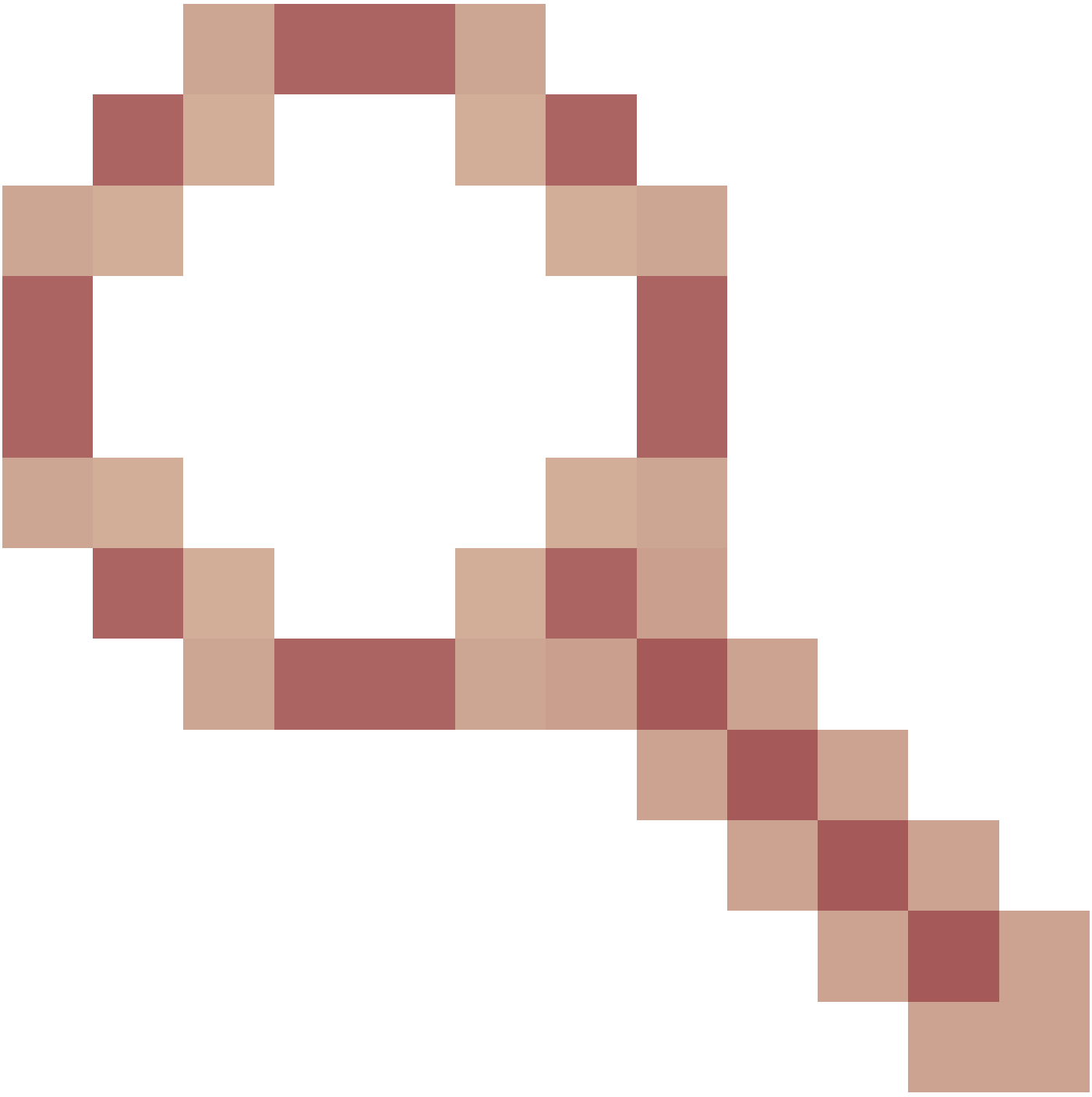
TTL이 1인 데이터 플레인 트래픽이 Cisco 버그 ID CSCvs로 인해 전달되었습니다82183 및 Cisco 버그 ID CSCvw16965



NX-OS 소프트웨어 릴리스 9.3(6) 이전의 NX-OS 소프트웨어 릴리스를 실행하는 Cloud Scale ASIC가 장착된 Nexus 9000 시리즈 스위치에서 Routing/Layer 3 over vPC 기능 향상이 활성화된 경우 TTL이 1인 유니캐스트 라우팅 프로토콜에 연결되지 않은 데이터플레인 트래픽은 수퍼바이저로 펀트되고 하드웨어 대신 소프트웨어로 포워딩됩니다. Nexus 스위치가 고정 섀시("Top of Rack"이라고도 함) 스위치인지 모듈형 섀시("End of Row"라고도 함) 스위치인지, 스위치의 현재 NX-OS 소프트웨어 릴리스인지에 따라 이 문제의 근본 원인은 소프트웨어 결함 Cisco 버그 ID CSCvs로 인한 것일 수 [있습니다82183]



또는 소프트웨어 결함 Cisco 버그 ID CSCvw16965



. 두 소프트웨어 결함 모두 Cloud Scale ASIC가 장착된 Nexus 9000 시리즈 스위치에만 영향을 미칩니다. 다른 Cisco Nexus 하드웨어 플랫폼은 이러한 문제의 영향을 받지 않습니다. 자세한 내용은 각 개별 소프트웨어 결함 내의 정보를 참조하십시오.

이러한 소프트웨어 결함을 방지하려면 NX-OS 소프트웨어 릴리스 9.3(6) 이상으로 업그레이드하는 것이 좋습니다. 일반적인 권장 사항으로 Cisco Nexus 9000 시리즈 스위치 권장 Cisco NX-OS 릴리스 문서에서 설명하는 Nexus 9000 시리즈 스위치의 현재 권장 NX-OS 소프트웨어 릴리스로 정기적으로 업그레이드하는 것이 좋습니다.

설정

Routing/Layer 3 over vPC 기능 향상을 설정하는 방법의 예시는 여기에서 확인할 수 있습니다.

이 예시에서 N9K-1 및 N9K-2는 vPC 도메인의 vPC 피어입니다. 두 vPC 피어 모두 이미 vPC 피어

게이트웨이 기능 향상 활성화되어 있습니다. 이는 Routing/Layer 3 over vPC 기능 향상 활성화에 필요합니다. 두 vPC 피어 모두 VLAN 10에 SVI가 있으며, 이는 OSPF 프로세스 1에서 활성화됩니다. N9K-1 및 N9K-3은 IP 주소 및 인접 ID가 192.168.10.3인 vPC 연결 OSPF 라우터에서 OSPF EXSTART/EXCHANGE 상태에서 응답이 없습니다.

<#root>

```
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
```

layer3 peer-router vPC 도메인 설정 명령을 통해 Routing/Layer 3 over vPC 기능 향상을 활성화할 수 있습니다. 이렇게 하면 vPC 피어 게이트웨이 기능 향상이 활성화된 결과로 라우팅되는 유니캐스트 라우팅 프로토콜 패킷의 TTL을 vPC 피어가 줄일 수 없게 됩니다.

<#root>

```
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#
```

Routing/Layer 3 over vPC 기능 향상을 활성화한 직후 vPC 연결 OSPF 네이버가 있는 OSPF 인접성이 FULL 상태로 전환되는지 확인하여 Routing/Layer 3 over vPC 기능 향상이 정상적으로 작동하는지 확인할 수 있습니다.

<#root>

```
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
```

영향

Routing/Layer 3 over vPC 기능 향상을 활성화해도 vPC 도메인에 영향을 미치지 않습니다. 따라서 Routing/Layer 3 over vPC 기능 향상을 활성화할 때 어떠한 vPC 피어도 vPC를 일시 중단하지 않으

며, 이 기능 향상을 활성화해도 데이터플레인 트래픽에 영향을 미치지 않습니다.

하지만 Routing/Layer 3 over vPC 기능 향상을 활성화하지 않아 이전에 중단되었던 동적 라우팅 프로토콜 인접성이 이 기능 향상을 활성화하면서 갑자기 작동하는 경우, 영향을 받는 라우팅 프로토콜 인접성의 역할, 이러한 인접성을 통해 알려진 특정 접두사, 그리고 유니캐스트 라우팅 테이블의 현재 상태에 따라 Routing/Layer 3 over vPC 기능 향상 활성화 시 약간의 중단이 관찰될 수 있습니다.

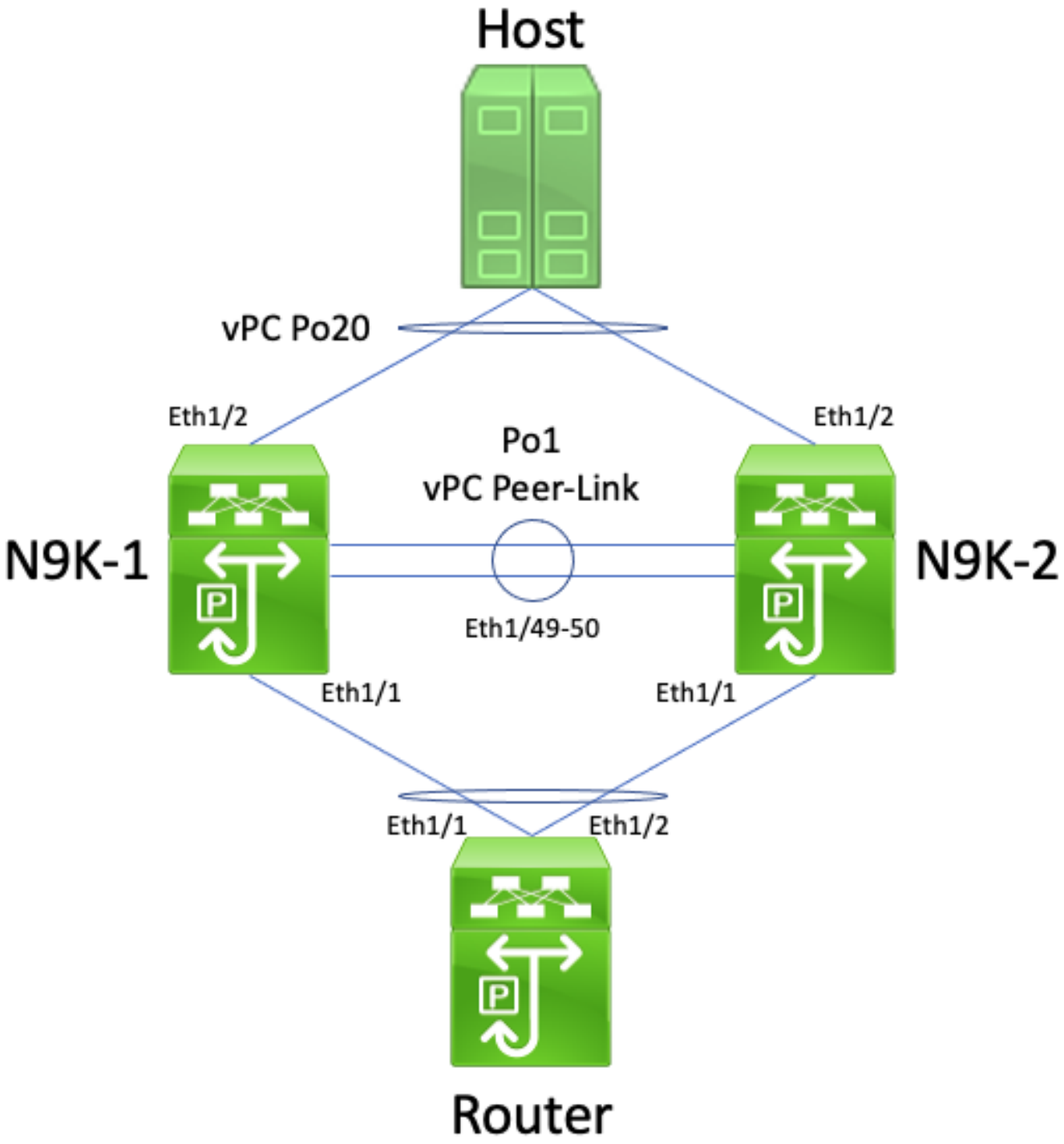
이러한 이유로 Cisco에서는 고객에게 영향을 받는 라우팅 프로토콜 인접성이 네트워크의 작동에 크게 영향을 미치지 않을 것이라 확신하지 않는 한, 유지 관리 기간 동안 제어플레인 및 데이터플레인 중단이 발생할 수 있음을 감안하고 기능 향상을 활성화할 것을 조언합니다.

또한 NX-OS 소프트웨어 릴리스에 영향을 미쳐 시스코에서는 TTL이 1인 자연 데이터플레인 트래픽이 하드웨어 대신 소프트웨어에서 처리될 수 있도록 하는 모든 소프트웨어 결함에 대해 이 문서의 경고 섹션을 면밀하게 검토할 것을 권장합니다.

실패 시나리오 예시

vPC 피어 게이트웨이가 없는 vPC를 통한 유니캐스트 라우팅 프로토콜 인접성

여기에 표시된 토폴로지를 고려해 보십시오.



이 토폴로지에서 Nexus 스위치 N9K-1 및 N9K-2는 vPC 피어 게이트웨이 기능 향상이 활성화되지 않은 vPC 도메인 내의 vPC 피어입니다. 인터페이스 Po1은 vPC 피어 링크입니다. 호스트 이름이 Router인 라우터는 vPC Po10을 통해 N9K-1 및 N9K-2에 연결됩니다. 호스트는 vPC Po20을 통해 N9K-1 및 N9K-2에 연결됩니다. 라우터의 Po10 인터페이스는 유니캐스트 라우팅 프로토콜에서 활성화되는 라우팅된 포트 채널입니다. N9K-1 및 N9K-2 모두 동일한 유니캐스트 라우팅 프로토콜에서 SVI 인터페이스가 활성화되어 있으며, Router와 동일한 브로드캐스트 도메인에 있습니다.

vPC 연결 라우터의 ECMP 해싱 결정과 해당 레이어 2 포트 채널 해싱 결정이 다를 수 있으므로 vPC 피어 게이트웨이 기능 향상이 활성화되지 않은 vPC를 통한 유니캐스트 라우팅 프로토콜 인접성은 지원되지 않습니다. 이 토폴로지에서 Router, N9K-1 및 N9K-2 간에 라우팅 프로토콜 인접성이 형성됩니다. Router와 Host 간의 트래픽 플로우를 고려하십시오. Router를 통과하여 Host로 향하는

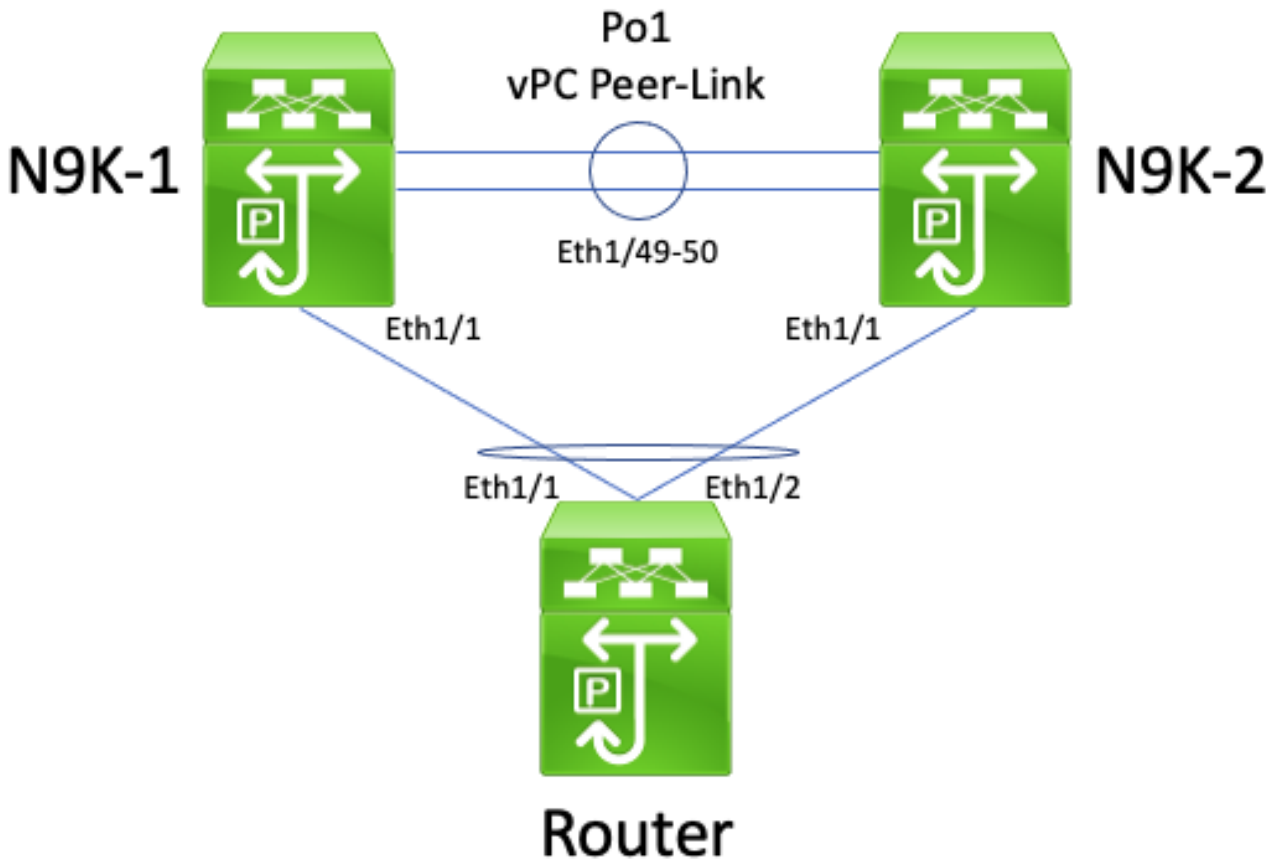
데이터플레인 트래픽은 (라우터의 ECMP 해싱 결정으로 인해) N9K-1의 SVI MAC 주소에 속하는 대상 MAC 주소로 다시 작성될 수 있지만 (라우터의 Layer 2 포트 채널 해싱 결정으로 인해) 인터페이스 Ethernet1/2에서 이그레스됩니다.

대상 MAC 주소가 N9K-1에 속하고 vPC 피어 게이트웨이 기능 향상(N9K-2가 N9K-1 대신 패킷을 라우팅하도록 허용)이 활성화되지 않았으므로 N9K-2는 이 패킷을 수신하여 vPC 피어 링크를 통해 포워딩합니다. N9K-1은 vPC 피어 링크에서 이 패킷을 수신하고 vPC Po20의 Ethernet1/2에서 패킷을 포워딩해야 함을 인식합니다. 이는 vPC 루프 회피 규칙을 위반하므로 N9K-1은 하드웨어에서 패킷을 삭제합니다. 따라서 이 토폴로지의 vPC 도메인을 통과하는 일부 플로우에서 연결 문제 또는 패킷 손실이 관찰될 수 있습니다.

peer-gateway vPC 도메인 설정 명령으로 vPC 피어 게이트웨이 기능 향상을 활성화한 다음 layer3 peer-router vPC 도메인 설정 명령을 사용하여 Routing/Layer 3 over vPC 기능 향상을 활성화하여 이 문제를 해결할 수 있습니다. 중단을 최소화하려면 vPC 피어 게이트웨이가 있는 vPC를 통한 유니캐스트 라우팅 프로토콜 인접성에 설명된 실패 시나리오에서 시간이 걸리지 않도록 두 vPC 모두의 기능 향상을 빠르게 연속으로 활성화해야 합니다.

vPC 피어 게이트웨이가 있는 vPC를 통한 유니캐스트 라우팅 프로토콜 인접성

여기에 표시된 토폴로지를 고려해 보십시오.



이 토폴로지에서 Nexus 스위치 N9K-1 및 N9K-2는 vPC 피어 게이트웨이 기능 향상이 활성화된 vPC 도메인 내의 vPC 피어입니다. 인터페이스 Po1은 vPC 피어 링크입니다. 호스트 이름이 Router인 라우터는 vPC Po10을 통해 N9K-1 및 N9K-2에 연결됩니다. 라우터의 Po10 인터페이스는

유니캐스트 라우팅 프로토콜에서 활성화되는 라우팅된 포트 채널입니다. N9K-1 및 N9K-2 모두 동일한 유니캐스트 라우팅 프로토콜에서 SVI 인터페이스가 활성화되어 있으며, Router와 동일한 브로드캐스트 도메인에 있습니다.

vPC 피어 게이트웨이 기능 향상으로 인해 유니캐스트 라우팅 프로토콜 인접성이 vPC 연결 라우터 및 두 vPC 피어 간에 형성되지 않을 수 있으므로 vPC 피어 게이트웨이 기능 향상이 활성화된 vPC를 통한 유니캐스트 라우팅 프로토콜 인접성은 지원되지 않습니다. 이 토폴로지에서 Router와 N9K-1 또는 N9K-2 간의 라우팅 프로토콜 인접성은 Router에서 vPC Po10을 통해 N9K-1 또는 N9K-2 해시로 유니캐스트 라우팅 프로토콜 패킷이 발생하는 방식에 따라 예상대로 작동하지 않을 수 있습니다.

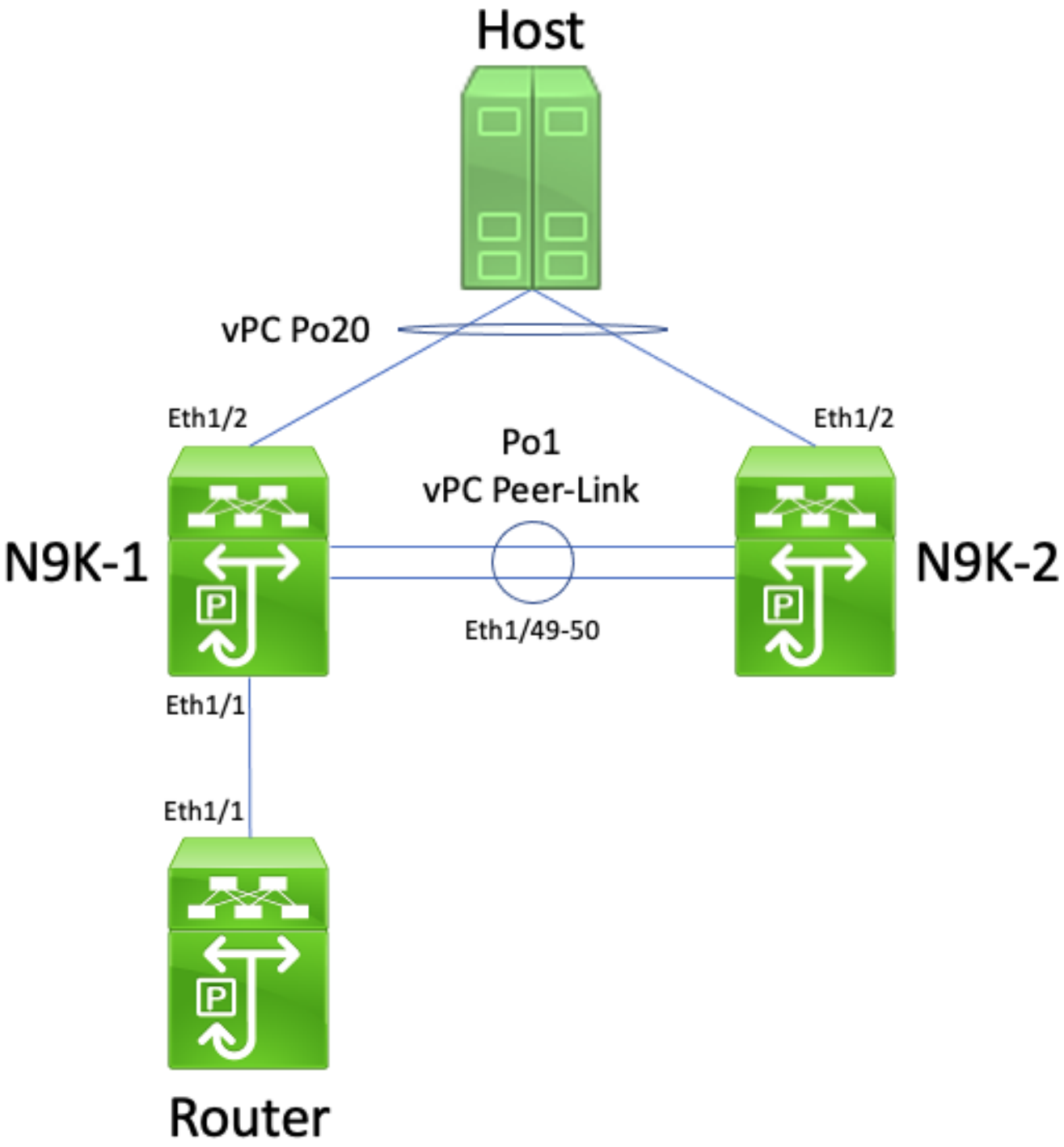
모든 링크-로컬 멀티캐스트 라우팅 프로토콜 패킷(일반적으로 "Hello" 패킷이라고 함)은 vPC VLAN으로 플러딩되므로 모든 라우터에서 이러한 패킷을 송신 및 수신할 수 있습니다. 하지만 Router의 레이어 2 포트 채널 해싱 결정으로 인해 Router에서 N9K-1로 향하는 유니캐스트 라우팅 프로토콜 패킷이 Ethernet1/2을 N9K-2로 이그레스하는 시나리오를 고려해 보십시오. 이 패킷은 N9K-1의 SVI MAC 주소로 향하지만 N9K-2의 Ethernet1/1 인터페이스를 인그레스합니다. N9K-2는 패킷이 N9K-1의 SVI MAC 주소로 향하는 것을 확인합니다.이 주소는 vPC 피어 게이트웨이 기능 향상이 활성화되어 있으므로 "G" 또는 "Gateway" 플래그와 함께 N9K-2의 MAC 주소 테이블에 설치됩니다. 그 결과 N9K-2는 N9K-1을 대신하여 유니캐스트 라우팅 프로토콜 패킷을 로컬로 라우팅하려고 시도합니다.

하지만 패킷을 라우팅하면 패킷의 TTL(Time to Live)이 감소하며, 대부분의 유니캐스트 라우팅 프로토콜 패킷의 TTL은 1입니다. 결과적으로 패킷의 TTL은 0으로 감소하고 N9K-2에 의해 삭제됩니다. N9K-1의 관점에서 N9K-1은 Router에서 링크-로컬 멀티캐스트 라우팅 프로토콜 패킷을 수신하고 있으며 유니캐스트 라우팅 프로토콜 패킷을 Router로 송신할 수는 있지만, Router에서 유니캐스트 라우팅 프로토콜 패킷을 수신하지 않습니다. 그 결과 N9K-1은 Router와의 라우팅 프로토콜 인접성을 해제하고 라우팅 프로토콜에 대한 로컬 유한 상태 머신을 재시작합니다. 마찬가지로 라우터는 라우팅 프로토콜에 대한 로컬 유한 상태 머신을 재시작합니다.

layer 3 peer-router vPC 도메인 설정 명령으로 layer 3 peer-router vPC 3 기능 향상을 활성화하여 이 문제를 해결할 수 있습니다. 이렇게 하면 TTL이 1인 유니캐스트 라우팅 프로토콜 패킷을 패킷의 TTL을 줄이지 않고 vPC 피어 링크를 통해 포워딩되도록 할 수 있습니다. 이로 인해 vPC 또는 vPC VLAN을 통해 문제 없이 유니캐스트 라우팅 프로토콜 인접성을 형성할 수 있습니다.

vPC VLAN 피어 게이트웨이가 없는 vPC를 통한 유니캐스트 라우팅 프로토콜 인접성

여기에 표시된 토폴로지를 고려해 보십시오.



이 토폴로지에서 Nexus 스위치 N9K-1 및 N9K-2는 vPC 피어 게이트웨이 기능 향상이 활성화되지 않은 vPC 도메인 내의 vPC 피어입니다. 인터페이스 Po1은 vPC 피어 링크입니다. 호스트 이름이 Router인 라우터는 Ethernet1/1을 통해 N9K-1의 Ethernet1/1에 연결됩니다. Router의 Ethernet1/1 인터페이스는 유니캐스트 라우팅 프로토콜에서 활성화되는 라우팅된 인터페이스입니다. N9K-1 및 N9K-2 모두 동일한 유니캐스트 라우팅 프로토콜에서 SVI 인터페이스가 활성화되어 있으며, Router와 동일한 브로드캐스트 도메인에 있습니다.

vPC 피어 게이트웨이 기능 향상이 활성화되지 않은 vPC VLAN을 통한 유니캐스트 라우팅 프로토콜 인접성은 지원되지 않습니다. vPC VLAN 연결 라우터의 ECMP 해싱 결정으로 인해 N9K-2가 vPC 루프 회피 규칙을 위반하는 데이터플레인 트래픽을 삭제할 수 있기 때문입니다. 이 토폴로지에서 Router, N9K-1 및 N9K-2 간에 라우팅 프로토콜 인접성이 형성됩니다. Router와 Host 간의 트래

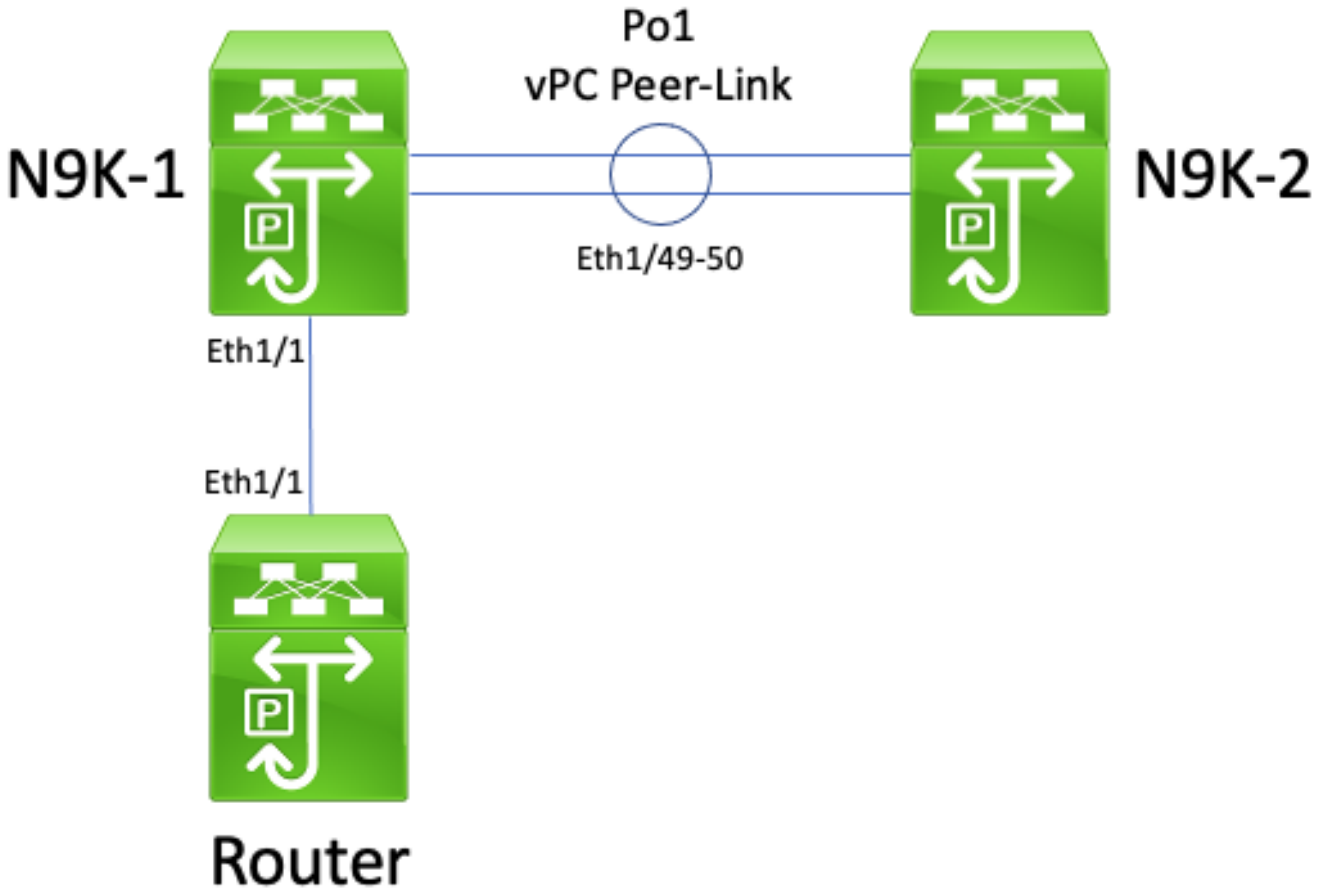
픽 플로우를 고려하십시오. Router를 통과하여 Host로 향하는 데이터플레인 트래픽은 (라우터의 ECMP 해싱 결정으로 인해) N9K-2의 SVI MAC 주소에 속하는 대상 MAC 주소로 다시 작성될 수 있고 인터페이스 Ethernet1/1에서 N9K-1로 이그레스됩니다.

대상 MAC 주소가 N9K-2에 속하고 vPC 피어 게이트웨이 기능 향상(N9K-1이 N9K-2 대신 패킷을 라우팅하도록 허용)이 활성화되지 않았으므로 N9K-1은 이 패킷을 수신하여 vPC 피어 링크를 통해 포워딩합니다. N9K-2는 vPC 피어 링크에서 이 패킷을 수신하고 vPC Po20의 Ethernet1/2에서 패킷을 포워딩해야 함을 인식합니다. 이는 vPC 루프 회피 규칙을 위반하므로 N9K-2는 하드웨어에서 패킷을 삭제합니다. 따라서 이 토폴로지의 vPC 도메인을 통과하는 일부 플로우에서 연결 문제 또는 패킷 손실이 관찰될 수 있습니다.

peer-gateway vPC 도메인 설정 명령으로 vPC 피어 게이트웨이 기능 향상을 활성화한 다음 layer3 peer-router vPC 도메인 설정 명령을 사용하여 Routing/Layer 3 over vPC 기능 향상을 활성화하여 이 문제를 해결할 수 있습니다. 중단을 최소화하려면 vPC 피어 게이트웨이가 있는 vPC를 통한 유니캐스트 라우팅 프로토콜 인접성에 설명된 실패 시나리오에서 시간이 걸리지 않도록 두 vPC 모두의 기능 향상을 빠르게 연속으로 활성화해야 합니다.

vPC VLAN 피어 게이트웨이가 있는 vPC를 통한 유니캐스트 라우팅 프로토콜 인접성

여기에 표시된 토폴로지를 고려해 보십시오.



이 토폴로지에서 Nexus 스위치 N9K-1 및 N9K-2는 vPC 피어 게이트웨이 기능 향상이 활성화된 vPC 도메인 내의 vPC 피어입니다. 인터페이스 Po1은 vPC 피어 링크입니다. 호스트 이름이

Router인 라우터는 Ethernet1/1을 통해 N9K-1의 Ethernet1/1에 연결됩니다. Router의 Ethernet1/1 인터페이스는 유니캐스트 라우팅 프로토콜에서 활성화되는 라우팅된 인터페이스입니다. N9K-1 및 N9K-2 모두 동일한 유니캐스트 라우팅 프로토콜에서 SVI 인터페이스가 활성화되어 있으며, Router와 동일한 브로드캐스트 도메인에 있습니다.

vPC 피어 게이트웨이 기능 향상으로 인해 유니캐스트 라우팅 프로토콜 인접성이 vPC VLAN 연결 라우터 및 vPC VLAN 연결 라우터가 직접 연결되지 않은 vPC 피어 간에 형성되지 않을 수 있으므로 vPC 피어 게이트웨이 기능 향상이 활성화된 vPC VLAN을 통한 유니캐스트 라우팅 프로토콜 인접성은 지원되지 않습니다. 이 토폴로지에서 vPC 피어 게이트웨이 기능 향상이 활성화되면서 N9K-2의 SVI MAC 주소로 향하는 N9K-1 라우팅 유니캐스트 라우팅 프로토콜 패킷의 결과로 Router와 N9K-2 간의 라우팅 프로토콜 인접성이 작동하지 않습니다. 패킷이 라우팅되므로 패킷의 TTL(Time To Live)을 줄여야 합니다. 유니캐스트 라우팅 프로토콜 패킷은 일반적으로 TTL이 1이며, 패킷의 TTL을 0으로 줄이는 라우터는 해당 패킷을 삭제해야 합니다.

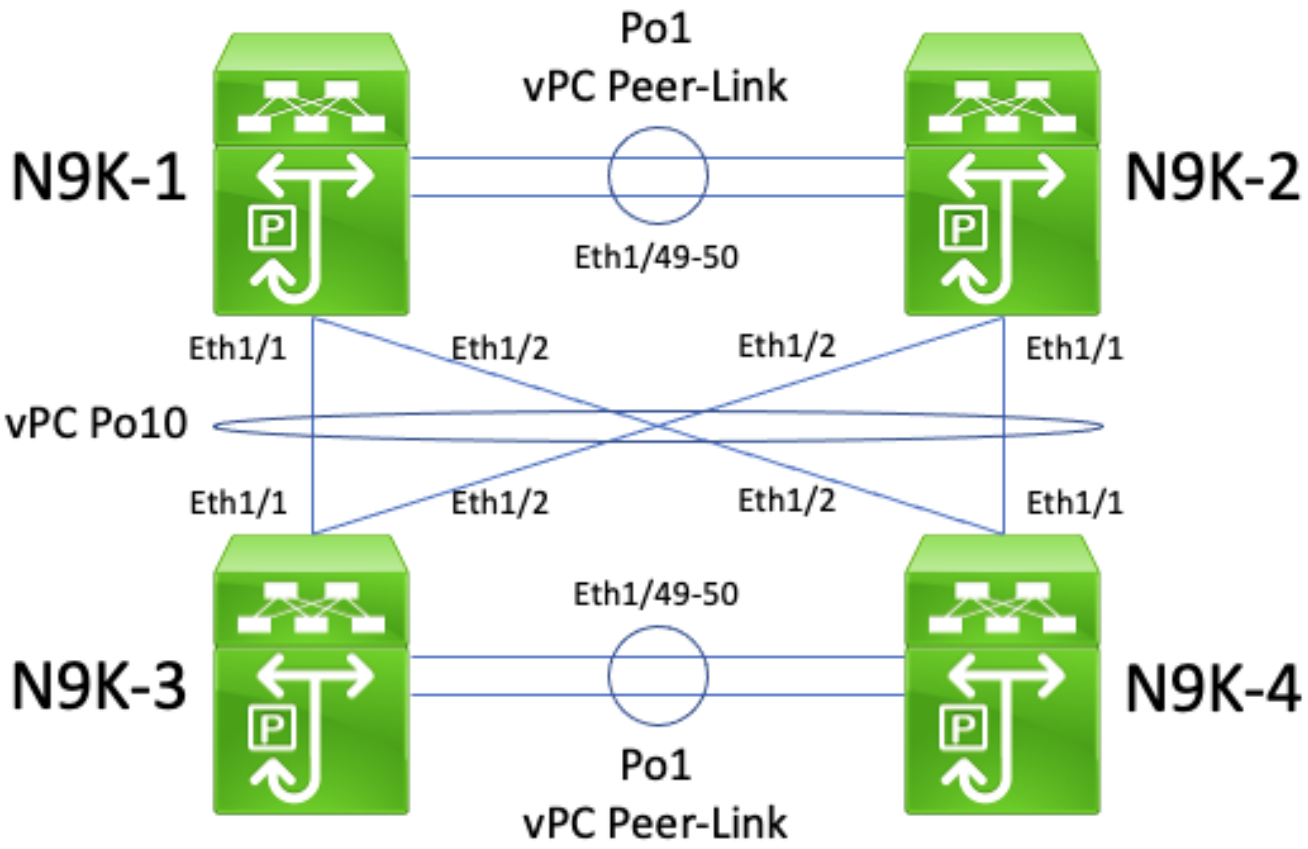
모든 링크-로컬 멀티캐스트 라우팅 프로토콜 패킷(일반적으로 "Hello" 패킷이라고 함)은 vPC VLAN으로 플러딩되므로 모든 라우터에서 이러한 패킷을 송신 및 수신할 수 있습니다. 하지만 Router에서 N9K-2로 향하는 유니캐스트 라우팅 프로토콜이 Ethernet1/1을 N9K-1로 이그레스하는 시나리오를 고려해 보십시오. 이 패킷은 N9K-2의 SVI MAC 주소로 향하지만 N9K-1의 Ethernet1/1 인터페이스를 인그레스합니다. N9K-1은 패킷이 N9K-2의 SVI MAC 주소로 향하는 것을 확인합니다. 이 주소는 vPC 피어 게이트웨이 기능 향상이 활성화되어 있으므로 "G" 또는 "Gateway" 플래그와 함께 N9K-1의 MAC 주소 테이블에 설치됩니다. 그 결과 N9K-1은 N9K-2를 대신하여 유니캐스트 라우팅 프로토콜 패킷을 로컬로 라우팅하려고 시도합니다.

하지만 패킷을 라우팅하면 패킷의 TTL이 감소하며, 대부분의 유니캐스트 라우팅 프로토콜 패킷의 TTL은 1입니다. 결과적으로 패킷의 TTL은 0으로 감소하고 N9K-1에 의해 삭제됩니다. N9K-2의 관점에서 N9K-2는 Router에서 링크-로컬 멀티캐스트 라우팅 프로토콜 패킷을 수신하고 있으며 유니캐스트 라우팅 프로토콜 패킷을 Router로 송신할 수는 있지만, Router에서 유니캐스트 라우팅 프로토콜 패킷을 수신하지 않습니다. 그 결과 N9K-2는 Router와의 라우팅 프로토콜 인접성을 해제하고 라우팅 프로토콜에 대한 로컬 유한 상태 머신을 재시작합니다. 마찬가지로 라우터는 라우팅 프로토콜에 대한 로컬 유한 상태 머신을 재시작합니다.

layer 3 peer-router vPC 도메인 설정 명령으로 layer 3 peer-router vPC 3 기능 향상을 활성화하여 이 문제를 해결할 수 있습니다. 이렇게 하면 TTL이 1인 유니캐스트 라우팅 프로토콜 패킷을 패킷의 TTL을 줄이지 않고 vPC 피어 링크를 통해 포워딩되도록 할 수 있습니다. 이로 인해 vPC 또는 vPC VLAN을 통해 문제 없이 유니캐스트 라우팅 프로토콜 인접성을 형성할 수 있습니다.

vPC 피어 게이트웨이가 있는 Back-to-Back vPC를 통한 유니캐스트 라우팅 프로토콜 인접성

여기에 표시된 토폴로지를 고려해 보십시오.



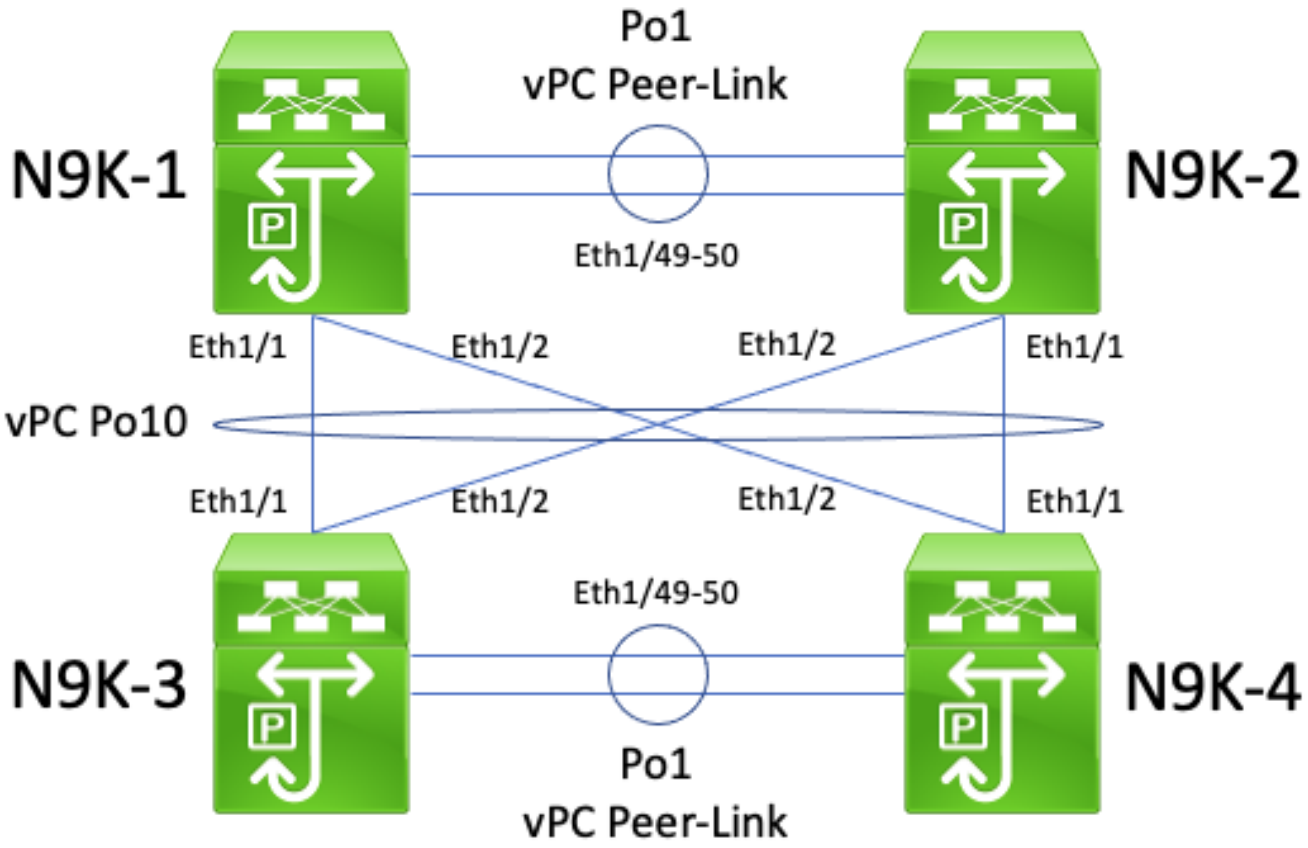
이 토폴로지에서 Nexus 스위치 N9K-1 및 N9K-2는 vPC 피어 게이트웨이 기능 향상이 활성화된 vPC 도메인 내의 vPC 피어입니다. Nexus 스위치 N9K-3 및 N9K-4는 vPC 피어 게이트웨이 기능 향상이 활성화된 vPC 도메인 내의 vPC 피어입니다. 두 vPC 도메인은 Back-to-Back vPC Po10을 통해 서로 연결됩니다. 4개 스위치 모두 유니캐스트 라우팅 프로토콜에서 SVI 인터페이스가 활성화되어 있으며, 동일한 브로드캐스트 도메인에 있습니다.

vPC 피어 게이트웨이 기능 향상으로 인해 유니캐스트 라우팅 프로토콜 인접성이 하나의 vPC 도메인과 다른 vPC 도메인 간에 형성되지 않을 수 있으므로 vPC 피어 게이트웨이 기능 향상이 활성화된 Back-to-Back vPC를 통한 유니캐스트 라우팅 프로토콜 인접성은 지원되지 않습니다. 이 토폴로지에서 N9K-1과 N9K-3 또는 N9K-4(또는 둘 다) 간의 라우팅 프로토콜 인접성이 예상대로 작동하지 않을 수 있습니다. 마찬가지로 N9K-2와 N9K-3 또는 N9K-4(또는 둘 다) 간의 라우팅 프로토콜 인접성이 예상대로 작동하지 않을 수 있습니다. 이는 유니캐스트 라우팅 프로토콜 패킷이 하나의 라우터(예: N9K-3)로 향하지만 발생하는 라우터의 레이어 2 포트 채널 해싱 결정에 따라 다른 라우터(예: N9K-4)로 포워딩될 수 있기 때문입니다.

이 문제의 근본 원인은 이 문서의 vPC 피어 게이트웨이가 있는 vPC를 통한 유니캐스트 라우팅 프로토콜 인접성에서 설명하는 근본 원인과 동일합니다. layer 3 peer-router vPC 도메인 설정 명령으로 layer 3 peer-router vPC 3 기능 향상을 활성화하여 이 문제를 해결할 수 있습니다. 이렇게 하면 TTL이 1인 유니캐스트 라우팅 프로토콜 패킷을 패킷의 TTL을 줄이지 않고 vPC 피어 링크를 통해 포워딩되도록 할 수 있습니다. 이로 인해 Back-to-Back vPC를 통해 문제 없이 유니캐스트 라우팅 프로토콜 인접성을 형성할 수 있습니다.

접두사가 OSPF LSDB에는 있지만 라우팅 테이블에는 없는 vPC 피어 게이트웨이가 있는 vPC를 통한 OSPF 인접성

여기에 표시된 토폴로지를 고려해 보십시오.



이 토폴로지에서 Nexus 스위치 N9K-1 및 N9K-2는 vPC 피어 게이트웨이 기능 향상이 활성화된 vPC 도메인 내의 vPC 피어입니다. Nexus 스위치 N9K-3 및 N9K-4는 vPC 피어 게이트웨이 기능 향상이 활성화된 vPC 도메인 내의 vPC 피어입니다. 두 vPC 도메인은 Back-to-Back vPC Po10을 통해 서로 연결됩니다. 4개 스위치 모두 유니캐스트 라우팅 프로토콜에서 SVI 인터페이스가 활성화되어 있으며, 동일한 브로드캐스트 도메인에 있습니다. N9K-4는 브로드캐스트 도메인의 OSPF DR(Designated Router)이며, N9K-3은 브로드캐스트 도메인의 OSPF BDR(Backup Designated Router)입니다.

이 시나리오에서 N9K-1과 N9K-3 간의 OSPF 인접성은 두 스위치의 Ethernet1/1을 이그레스하는 유니캐스트 OSPF 패킷으로 인해 FULL 상태로 전환됩니다. 마찬가지로 N9K-2와 N9K-3 간의 OSPF 인접성은 두 스위치의 Ethernet1/2를 이그레스하는 유니캐스트 OSPF 패킷으로 인해 FULL 상태로 전환됩니다.

하지만 N9K-1과 N9K-4 사이의 OSPF 인접성은 유니캐스트 OSPF 패킷이 두 스위치의 Ethernet1/1을 이그레스하고 N9K-2 및 N9K-4에 의해 삭제되므로 EXSTART 또는 EXCHANGE 상태로 응답하지 않습니다. 이는 이 문서의 vPC 피어 게이트웨이가 있는 Back-to-Back vPC를 통한 프로토콜 인접성 섹션에서 설명합니다. 마찬가지로 N9K-2와 N9K-4 사이의 OSPF 인접성은 유니캐스트 OSPF 패킷이 두 스위치의 Ethernet1/2를 이그레스하고 N9K-1 및 N9K-3에 의해 삭제되므로 EXSTART 또는 EXCHANGE 상태로 응답하지 않습니다. 이는 이 문서의 vPC 피어 게이트웨이가 있는 Back-to-Back vPC를 통한 프로토콜 인접성 섹션에서 설명합니다.

그 결과 N9K-1 및 N9K-2는 브로드캐스트 도메인에 대한 BDR과 함께 FULL 상태이지만, 브로드캐스트 도메인에 대한 DR과 함께 EXSTART 또는 EXCHANGE 상태에 있게 됩니다. 브로드캐스트 도

메인의 DR 및 BDR은 모두 OSPF LSDB(Link State Data Base)의 전체 복사본을 유지하지만 OSPF DROTHER 라우터는 DR 또는 BDR에서 OSPF를 통해 학습된 접두사를 설치하기 위해 브로드캐스트 도메인에 대한 DR과 함께 FULL 상태여야 합니다. 그에 따라 N9K-1 및 N9K-2는 모두 OSPF LSDB에 있는 N9K-3 및 N9K-4로부터 학습된 접두사가 있는 것으로 보이지만, 이러한 접두사는 N9K-1 및 N9K-2가 N9K-4(브로드캐스트 도메인의 DR)와 함께 FULL 상태로 전환될 때까지 유니캐스트 라우팅 테이블에 설치되지 않습니다.

layer 3 peer-router vPC 도메인 설정 명령으로 layer 3 peer-router vPC 3 기능 향상을 활성화하여 이 문제를 해결할 수 있습니다. 이렇게 하면 TTL이 1인 유니캐스트 라우팅 프로토콜 패킷을 패킷의 TTL을 줄이지 않고 vPC 피어 링크를 통해 포워딩되도록 할 수 있습니다. 이로 인해 Back-to-Back vPC를 통해 문제 없이 유니캐스트 라우팅 프로토콜 인접성을 형성할 수 있습니다. 결과적으로 N9K-1 및 N9K-2는 N9K-4(브로드캐스트 도메인의 DR)와 함께 FULL 상태로 전환되며, OSPF를 통해 N9K-3 및 N9K-4에서 학습된 접두사를 각 유니캐스트 라우팅 테이블에 설치하게 됩니다.

관련 정보

- Cisco Nexus 9000 시리즈 NX-OS 인터페이스 설정 가이드, 릴리스 10.3(x)
- Cisco Nexus 9000 시리즈 NX-OS 인터페이스 설정 가이드, 릴리스 10.2(x)
- Cisco Nexus 9000 시리즈 NX-OS 인터페이스 설정 가이드, 릴리스 10.1(x)
- Cisco Nexus 9000 시리즈 NX-OS 인터페이스 설정 가이드, 릴리스 9.3(x)
- Cisco Nexus 9000 시리즈 NX-OS 인터페이스 설정 가이드, 릴리스 9.2(x)
- Cisco Nexus 9000 시리즈 NX-OS 인터페이스 설정 가이드, 릴리스 7.x
- Cisco Nexus 7000 시리즈 NX-OS 인터페이스 설정 가이드 8.x
- Cisco Nexus 7000 시리즈 NX-OS 인터페이스 설정 가이드 7.x
- 설계 및 설정 가이드: Cisco Nexus 7000 시리즈 스위치의 vPC(Virtual Port Channel) 모범 사례
- Nexus 플랫폼에서 가상 포트 채널을 통한 라우팅에 대해 지원되는 토폴로지

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.