

瞭解虛擬連接埠通道 (vPC) 強化

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[適用硬體](#)

[vPC 對等交換器](#)

[概觀](#)

[備援連接非 vPC 橋接器](#)

[vPC 連接橋接器](#)

[注意事項](#)

[vPC 對等間的跨距樹狀目錄優先順序值必須符合](#)

[vPC 對等交換器對於非 vPC VLAN 的影響](#)

[組態](#)

[影響](#)

[備援連接非 vPC 橋接器](#)

[vPC 連接橋接器](#)

[範例故障情況](#)

[備援連接非 vPC 橋接器重新啟動有限狀態機器](#)

[vPC 連接橋接器排清動態學習 MAC 位址](#)

[vPC 對等閘道](#)

[概觀](#)

[注意事項](#)

[vPC 或 vPC VLAN 的單點傳送路由通訊協定鄰接翻動](#)

[自動停用 ICMP 和 ICMPv6 重新導向](#)

[組態](#)

[影響](#)

[vPC 或 vPC VLAN 的單點傳送路由通訊協定鄰接翻動](#)

[自動停用 ICMP 和 ICMPv6 重新導向](#)

[範例故障情況](#)

[具有非標準轉送行為的 vPC 連接主機](#)

[Routing/Layer 3 over vPC \(第 3 層對等路由器 \)](#)

[概觀](#)

[注意事項](#)

[不定期 VPC-2-L3 VPC UNEQUAL WEIGHT 系統日誌](#)

[由於Cisco錯誤ID CSCvs82183和Cisco錯誤ID CSCvw16965，已轉發TTL為1的軟體的資料平面流量](#)

[組態](#)

[影響](#)

[範例故障情況](#)

[未使用 vPC 對等閘道透過 vPC 形成單點傳送路由通訊協定鄰接](#)

[使用 vPC 對等閘道透過 vPC 形成單點傳送路由通訊協定鄰接](#)

[未使用 vPC 對等間道透過 vPC VLAN 形成單點傳送路由通訊協定鄰接](#)

[使用 vPC 對等間道透過 vPC VLAN 形成單點傳送路由通訊協定鄰接](#)

[使用 vPC 對等間道透過連續 vPC 形成單點傳送路由通訊協定鄰接](#)

[使用 vPC 對等間道透過 vPC 形成 OSPF 鄰接，其首碼存在於 OSPF LSDB 中，而非路由表中](#)

相關資訊

簡介

本檔案介紹在 vPC 網域中的 Cisco Nexus 交換器上設定的通用虛擬連線埠通道 (vPC) 增強功能。

必要條件

需求

思科建議您瞭解與使用案例、組態及虛擬連接埠通道 (vPC) 之實作相關的基本資訊。如需有關此功能的詳細資訊，請參閱以下其中一份適用的文件：

- [Cisco Nexus 9000 系列 NX-OS 介面組態指南 \(10.3\(x\) 版 \)](#)
- [Cisco Nexus 9000 系列 NX-OS 介面組態指南 \(10.2\(x\) 版 \)](#)
- [Cisco Nexus 9000 系列 NX-OS 介面組態指南 \(10.1\(x\) 版 \)](#)
- [Cisco Nexus 9000 系列 NX-OS 介面組態指南 \(9.3\(x\) 版 \)](#)
- [Cisco Nexus 9000 系列 NX-OS 介面組態指南 \(9.2\(x\) 版 \)](#)
- [Cisco Nexus 9000 系列 NX-OS 介面組態指南 \(7.x 版 \)](#)
- [Cisco Nexus 7000 系列 NX-OS 介面組態指南 8.x](#)
- [Cisco Nexus 7000 系列 NX-OS 介面組態指南 7.x](#)
- [設計和配置指南：Cisco Nexus 7000 系列交換機上的虛擬埠通道 \(vPC\) 最佳實踐](#)

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

自從 Cisco Nexus 資料中心交換器的 Cisco NX-OS 問世後，虛擬連接埠通道 (vPC) 功能已獲得許多增強功能，其中改善 vPC 連接裝置在故障情況下的可靠性，並最佳化 vPC 對等交換器的轉送行為。瞭解每項增強功能的用途、增強功能引起的行為變化，以及增強功能解決的故障情況，將可協助您瞭解應在 vPC 網域內設定增強功能的原因和時機，以充分滿足業務需求和要求。

適用硬體

本文件涵蓋的程序適用於所有支援 vPC 功能的 Cisco Nexus 資料中心交換器。

vPC 對等交換器

本節將說明 vPC 對等交換器增強功能，此功能須使用 peer-switch vPC 網域組態命令才可啟用。

概觀

在許多環境中，vPC 網域的 Nexus 交換器組為彙總或核心交換器，做為第 2 層交換以太網路網域和第 3 層路由網域間的邊界。兩個交換器皆設定多個 VLAN，並負責安排 VLAN 間東西流量和南北流量的路由。在此類環境中，就跨距樹狀目錄通訊協定角度來看，Nexus 交換器一般也可做為根橋接器。

通常，通過將一個 vPC 對等體的生成樹優先順序設定為較小的值（如 0），將其配置為生成樹的根網橋。另一個 vPC 對等體配置了稍高的生成樹優先順序，如 4096，這允許它在 vPC 對等體作為根橋出現故障時接管生成樹中的根橋角色。透過此組態，做為根橋接器的 vPC 對等體會產生具有橋接器 ID（包含其系統 MAC 位址）的跨距樹狀目錄橋接器通訊協定資料單位（BPDU）。

但是，如果充當根網橋的 vPC 對等體發生故障，導致另一個 vPC 對等體接管作為生成樹根網橋，則另一個 vPC 對等體會使用包含其系統 MAC 地址的網橋 ID 建立生成樹 BPDU，該網橋 ID 不同於原始根網橋的系統 MAC 地址。根據下游網橋的連線方式，此更改的影響會有所不同，將在以下小節中說明。

備援連接非 vPC 橋接器

通過冗餘鏈路連線到兩個 vPC 對等裝置的非 vPC 連線網橋（因此，從生成樹協定角度而言，一個鏈路處於阻塞狀態），它會檢測 BPDU 中的更改（因此，根網橋中的更改），從而觀察根埠的變化。其他指定轉發介面會立即轉換到阻塞狀態，然後遍歷生成樹協定有限狀態機（阻塞、學習和轉發），暫停時間介於所配置的生成樹協定轉發延遲計時器（預設情況下為 15 秒）之間。

根連接埠的變更與後續跨距樹狀目錄通訊協定有限狀態機器的周遊，可能會造成網路大量中斷。vPC 對等交換器增強功能的導入主要用於防止此問題造成的網路中斷（如果其中一個 vPC 對等體離線）。通過 vPC 對等交換機增強功能，非 vPC 連線的網橋仍然有一個處於阻塞狀態的冗餘鏈路，但是如果現有根埠由於鏈路故障而關閉，該介面會立即轉換到轉發狀態。離線 vPC 對等裝置重新聯機時，會發生相同的過程——以最低成本連線到根網橋的介面會搶佔「根埠」角色，冗餘鏈路立即轉換到「阻塞」狀態。觀察到的唯一資料平面影響是 vPC 對等裝置離線時不可避免地丟失正在傳輸的資料包。

vPC 連接橋接器

跨距樹狀目錄網域中與 vPC 連線的網橋會檢測 BPDU 中的更改（從而檢測根網橋中的更改），並刷新本地 MAC 地址表中的動態獲知的 MAC 地址。在不依賴無環拓撲的生成樹協定的 vPC 連線裝置的拓撲中，此行為效率低下，而且沒有必要。從生成樹協定角度看，vPC 被視為單個邏輯介面，與普通埠通道類似，因此 vPC 對等體的丟失與埠通道成員內單個鏈路的丟失類似。在任一情況中，跨距樹狀目錄都不會變更，因此不需要排清跨距樹狀目錄網域（其用途為允許以太網路泛洪和學習行為，在跨距樹狀目錄的新轉送介面中重新學習 MAC 位址）之橋接器的動態學習 MAC 位址。

此外，排清動態學習 MAC 位址可能會造成中斷情況。思考兩個主機具有主要為單向之 UDP 型流量（例如將資料傳送至 TFTP 伺服器的 TFTP 用戶端）的情況。在此流量中，資料大部分會從 TFTP 用戶端流向 TFTP 伺服器（罕見情況為 TFTP 伺服器將封包傳回 TFTP 用戶端）。因此，在生成樹域中動態學習的 MAC 地址刷新後，TFTP 伺服器的 MAC 在一段時間內不會被學習。這表示傳送到

TFTP伺服器的TFTP使用者端資料會在整個VLAN中泛洪，因為流量是未知的單點傳播流量。這可能會造成大量資料流移動至未預期的網路位置，且如果其流向網路的超額訂閱區段，則可能導致效能問題。

vPC 對等交換器增強功能的導入，係用於防止此種效率不彰和不必要的行為發生（如果做為一或多個 VLAN 之跨距樹狀目錄根橋接器的 vPC 對等遭重新載入或關閉）。

要啟用vPC對等交換機增強功能，兩個vPC對等裝置必須具有相同的生成樹協定配置（包括所有vPC VLAN的生成樹優先順序值），並且必須是所有vPC VLAN的根網橋。符合以上先決條件後，必須設定 peer-switch vPC 網域組態命令，才可啟用 vPC 對等交換器增強功能。



註:vPC對等交換機增強功能僅在包含所有VLAN根的vPC域上受支援。

啟用vPC對等交換機增強功能後，兩台vPC對等裝置開始發起相同的生成樹BPDU，其中網橋ID包含兩個vPC對等裝置共用的vPC系統MAC地址。如果重新載入vPC對等體，則由其餘vPC對等體發起的生成樹BPDU不會更改，因此生成樹域中的其他網橋在根網橋中看不到任何更改，也不會對網路中的更改做出次優反應。

注意事項

在生產環境中進行設定前，您應留意 vPC 對等交換器增強功能的一些注意事項。

vPC 對等間的跨距樹狀目錄優先順序值必須符合

啟用 vPC 對等交換器增強功能前，所有 vPC VLAN 的跨距樹狀目錄優先順序組態必須修正，使其在 vPC 對等兩者間皆相同。

考慮下面的配置，其中N9K-1配置為優先順序為0的VLAN 1、10和20的生成樹根網橋。N9K-2是VLAN 1、10和20的輔助生成樹根網橋，優先順序為4096。

```
<#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
```

在啟用vPC對等交換機增強功能之前，您必須修改N9K-2上VLAN 1、10和20的生成樹優先順序配置

, 以匹配N9K-1上相同VLAN的生成樹優先順序配置。此處顯示修改示例。

```
<#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
```

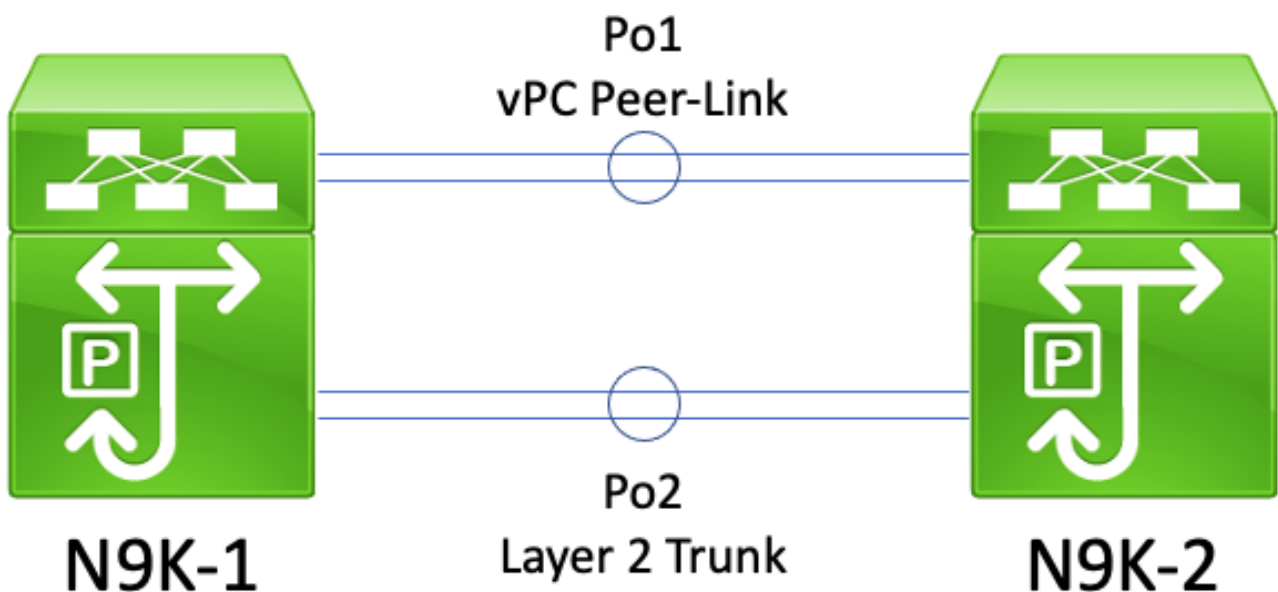
```
spanning-tree vlan 1,10,20 priority 0
```

```
interface port-channel1
```

```
spanning-tree port type network
```

vPC 對等交換器對於非 vPC VLAN 的影響

考量以下拓撲：



在此拓撲中，兩個vPC對等體（N9K-1和N9K-2）之間有兩個第2層中繼——Po1和Po2。Po1是承載vPC VLAN的vPC對等鏈路，而Po2是承載所有非vPC VLAN的第2層中繼。如果N9K-1和N9K-2上通過Po2傳送的非vPC VLAN的生成樹優先順序值相同，則每個vPC對等體都會生成源自vPC系統MAC地址的生成樹BPDU幀，而兩台交換機上的生成樹BPDU幀相同。因此，儘管N9K-2是生成生成樹BPDU的交換機，但N9K-1似乎在Po2上為每個非vPC VLAN接收自己的生成樹BPDU。從生成樹的角度來看，N9K-1將Po2置於所有非vPC VLAN的阻塞狀態。

這是預期行為。為防止出現此行為或因應此問題，兩個vPC對等體皆必須在所有非vPC VLAN中，使用不同的跨距樹狀目錄優先順序值設定。這允許一個vPC對等體成為非vPC VLAN的根網橋，並將vPC對等體之間的第2層中繼轉換到指定轉發狀態。同樣，遠端vPC對等體會將vPC對等體之間的第2層中繼轉換為指定根狀態。這允許非vPC VLAN中的流量透過第2層主幹在兩個vPC對等點間流動。

組態

設定vPC對等交換器功能的方法範例如下所示。

在本例中，N9K-1配置為優先順序為0的VLAN 1、10和20的生成樹根網橋。N9K-2是VLAN 1、10和20的輔助生成樹根網橋，優先順序為4096。

```
<#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
```

首先，N9K-2 的跨距樹狀目錄優先順序組態必須變更為與 N9K-1 的組態相同。為使 vPC 對等交換器功能如預期運作，此變更為必要作業。如果N9K-2的系統MAC地址低於N9K-1的系統MAC地址，則N9K-2會取代生成樹域的根網橋角色，從而導致生成樹域中的其他網橋刷新所有受影響的VLAN的本地MAC地址表。此現象的範例如下所示。

<#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

接著，我們可透過 peer-switch vPC 網域組態命令，啟用 vPC 對等交換器功能。這會更改由兩個 vPC 對等體發起的生成樹 BPDU 中的網橋 ID，這會導致生成樹域中的其他網橋刷新所有受影響 VLAN 的本地 MAC 地址表。

<#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#

```

您可藉由使用 `show spanning-tree summary` 命令，驗證聲稱為 vPC VLAN 之根橋器的兩個 vPC 對等，確認 vPC 對等交換器功能如預期運作。此輸出內容亦應會說明 vPC 對等交換功能現在已經啟用並且正常運作中。

```
<#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

使用 `show spanning-tree vlan {x}` 命令，以檢視特定 VLAN 相關的詳細資訊。擁有主或運行主 vPC 角色的交換機的所有介面都處於指定轉發狀態。具有輔助或操作輔助型 vPC 角色的交換機的所有介面都處於指定轉發狀態，但 vPC 對等鏈路除外，該對等鏈路處於根轉發狀態。請注意，顯示於 `show vpc role` 之輸出內容的 vPC 系統 MAC 位址，會與根橋接器 ID 和各 vPC 對等的橋接器 ID 相同。

<#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

最後，我們可使用各 vPC 對等的 [Ethanalyzer 控制層封包擷取公用程式](#)，確認兩個 vPC 對等正在產生具有橋接器 ID 和根橋接器 ID (包含兩個 vPC 對等間共用的 vPC 系統 MAC 位址) 的跨距樹狀目錄 BPDU。

<#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
```

影響

啟用vPC對等交換機增強功能的影響會有所不同，具體取決於生成樹域中的其他網橋是否通過vPC連線到兩個vPC對等裝置，或者是否冗餘連線到兩個沒有vPC的vPC對等裝置。

備援連接非 vPC 橋接器

如果具有兩個 vPC 對等之備援連結（如此從跨距樹狀目錄通訊協定角度來看，其中一個連結處於「封鎖」狀態）的非 vPC 連接橋接器偵測到跨距樹狀目錄根橋接器中的變更（在跨距樹狀目錄 BPDU 中通告），橋接器的根連接埠可能會在兩個備援介面間變更。相反的，如此可能會造成其他「指定轉送」介面立即轉換至「封鎖」狀態，接著周遊跨距樹狀目錄通訊協定有限狀態機器（封鎖、學習及轉送），其間隔暫停時間相當於設定的跨距樹狀目錄通訊協定轉送延遲計時器時間（依預設為 15 秒）。根連接埠的變更與後續跨距樹狀目錄通訊協定有限狀態機器的周遊，可能會造成網路大量中斷。

值得一提的是，當前作為生成樹域的根網橋的vPC對等體離線時（例如發生電源故障、硬體故障或重新載入時），就會發生此影響。此行為並非專屬於 vPC 對等交換器增強功能 – 從跨距樹狀目錄角度來看，啟用 vPC 對等交換器增強功能僅會造成 vPC 對等離線的類似行為。

vPC 連接橋接器

如果與vPC連線的網橋檢測到在生成樹BPDU中通告的生成樹根網橋發生變化，網橋會從其MAC地址表中刷新動態獲知的MAC地址。配置vPC對等交換機功能時，您可以在以下兩種情況下觀察此行為：

1. 當跨距樹狀目錄優先順序值設定為在兩個 vPC 對等之間比對後，如果先前並非根橋器的 vPC 對等的系統 MAC 位址低於先前為根橋器的 vPC 對等，跨距樹狀目錄根橋接器可能會從一個 vPC 對等變更為其他 vPC 對等。此情況的範例會顯示於[本文件的 vPC 對等交換器組態章節](#)中。
2. 通過peer-switch vPC域配置命令啟用vPC對等交換機功能後，兩個vPC對等交換機開始作為生成樹域的根網橋運行。兩個vPC對等體開始產生相同的生成樹BPDU，它們將自己宣告為生成樹域的根網橋。

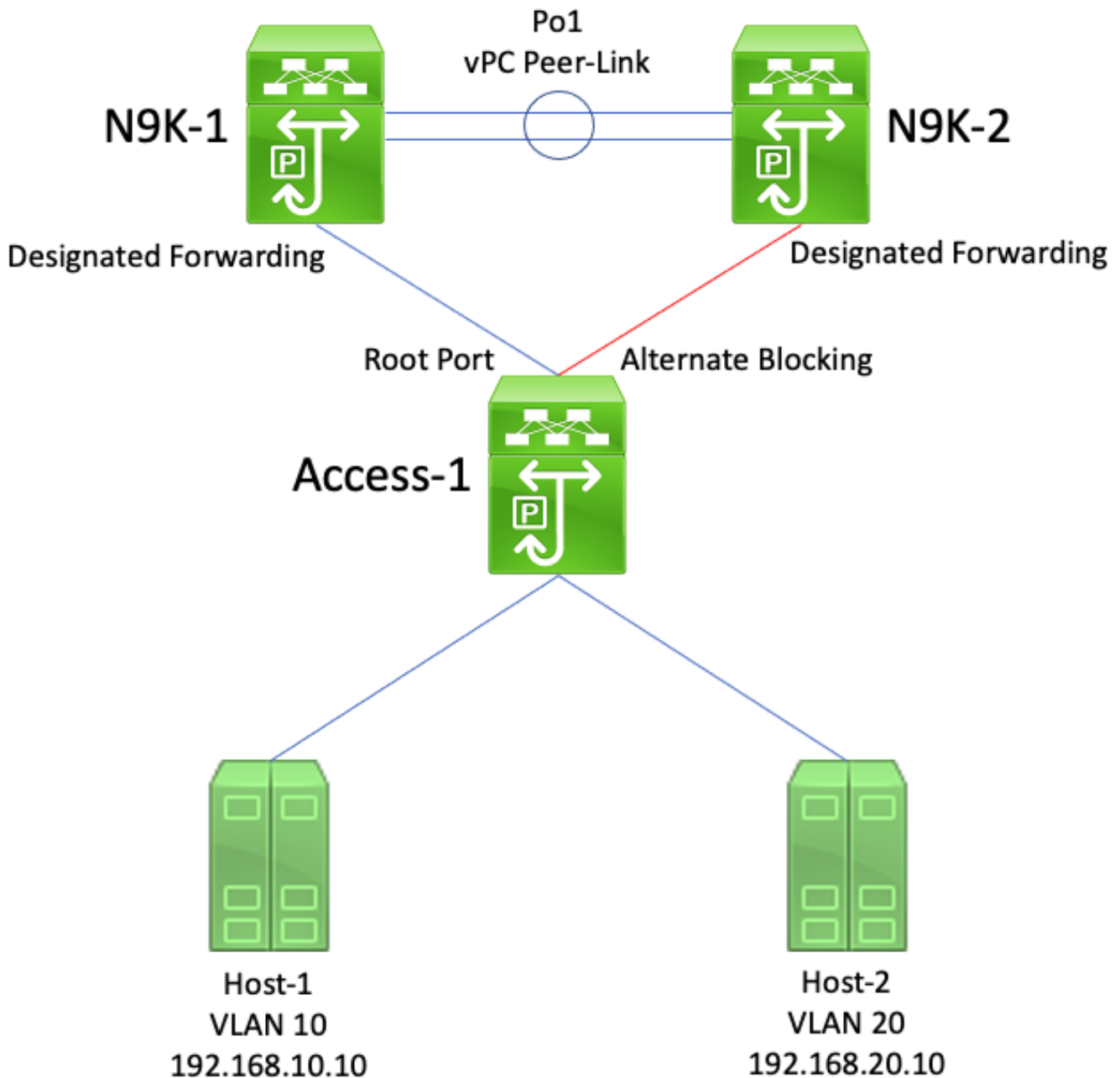
在大多數場景和拓撲中，這兩個場景中的任一個均未觀察到資料平面影響。但是，在很短的一段時間內，由於未知的單點傳播泛洪，資料平面流量在VLAN內泛洪，因為動態學習的MAC地址的直接結果是在任何交換機埠上未獲知幀的目標MAC地址。在部分拓撲中，如果資料層流量泛洪至 VLAN 內之超額訂閱的網路裝置，則此可能會造成短暫的效能問題或封包遺失。這也會導致佔用大量頻寬的單向流量流或靜默主機（主要接收封包且很少傳送封包的主機）出現問題，因為此流量會在一段較長時間內在VLAN中泛洪，而不是像正常情況那樣直接交換到目的地主機。

值得一提的是，此影響與從受影響VLAN內網橋的MAC地址表中動態學習的MAC地址刷新有關。此行為並非專屬於 vPC 對等交換器增強功能或根橋接器中的變更 – 此行為亦可能由拓撲變更通知（變更乃是由於非邊緣連接埠在 VLAN 內出現所產生）所造成。

範例故障情況

備援連接非 vPC 橋接器重新啟動有限狀態機器

考量以下拓撲：



在此拓撲中，N9K-1 和 N9K-2 為 vPC 網域中的 vPC 對等。N9K-1 會設定為適用於所有 VLAN 的跨距樹狀目錄優先順序值 0，使 N9K-1 成為所有 VLAN 的根橋接器。N9K-2 會設定為適用於所有 VLAN 的跨距樹狀目錄優先順序值 4096，使 N9K-2 成為所有 VLAN 的次要根橋接器。Access-1 為透過第 2 層交換器連接埠，同時備援連接至 N9K-1 和 N9K-2 的交換器。此類交換器連接埠並未組合成連接埠通道，因此跨距樹狀目錄通訊協定會將連接放置在處於「指定根」狀態之 N9K-1 的連結，以及連接至處於「替代封鎖」狀態之 N9K-2 的連結。

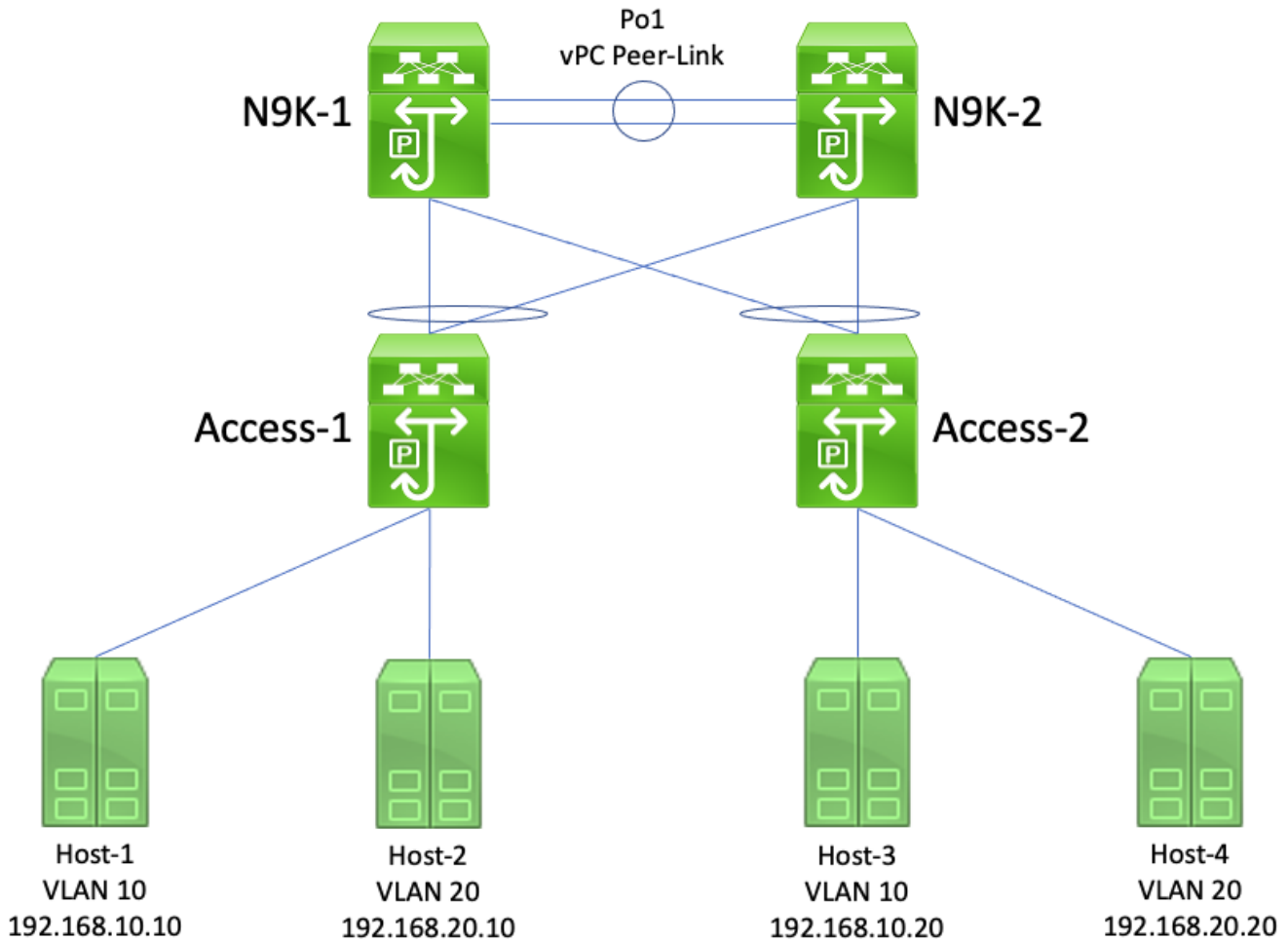
考量 N9K-1 因為交換器硬體故障、斷電或重新載入而離線的故障情況。N9K-2 使用自己的系統 MAC 地址作為網橋 ID 通告生成樹 BPDUs，從而宣告自己是所有 VLAN 的根網橋。Access-1 看到根網橋 ID 發生更改。此外，其「指定根埠」會轉換為「關閉/關閉」狀態，這意味著新的「指定根埠」是指處於「備用阻塞」狀態的鏈路，該狀態面向 N9K-2。

指定根埠的這種更改會導致所有非邊緣生成樹埠逐步通過生成樹協定有限狀態機（阻塞、學習和轉發），暫停時間介於所配置的生成樹協定轉發延遲計時器（預設情況下為 15 秒）之間。此程序可能會對網路造成嚴重中斷。

在啟用vPC對等交換機增強功能的同一故障場景中，N9K-1和N9K-2都使用共用vPC系統MAC地址作為網橋ID傳輸相同的生成樹BPDU。如果N9K-1出現故障，N9K-2將繼續傳輸此相同的生成樹BPDU。因此，Access-1會立即將指向N9K-2的備用阻塞鏈路轉換為指定根狀態，並開始通過鏈路轉發流量。此外，跨距樹狀目錄根橋接器 ID 不會變更的情況，可防止非邊緣連接埠通過跨距樹狀目錄通訊協定有限狀態機器，減少網路中觀察到中斷次數。

vPC 連接橋接器排清動態學習 MAC 位址

考量以下拓撲：



在此拓撲中，N9K-1和N9K-2是vPC域中的vPC對等體，在VLAN 10和VLAN 20之間執行VLAN間路由。N9K-1為VLAN 10和VLAN 20配置了生成樹優先順序值0，使N9K-1成為兩個VLAN的根網橋。N9K-2 會設定為適用於 VLAN 10 和 VLAN 20 的跨距樹狀目錄優先順序值 4096，使 N9K-2 成為兩個 VLAN 的次要根橋接器。Host-1、Host-2、Host-3 及 Host-4 均會持續彼此進行通訊。

考量 N9K-1 因為交換器硬體故障、斷電或重新載入而離線的故障情況。N9K-2使用自己的系統MAC地址作為網橋ID通告生成樹BPDU，從而宣稱自己是VLAN 10和VLAN 20的根網橋。Access-1和Access-2會看到根網橋的ID發生變化，儘管生成樹保持不變（即面向N9K-1和N9K-2的vPC仍為指定根埠），但Access-1和Access-2都會刷新VLAN 10和VLAN 20中所有動態獲知的MAC地址的MAC地址。

在大部分的環境中，排清動態學習的MAC位址會造成的影響微乎其微。沒有任何封包遺失（除在N9K-1故障時傳輸至其中而遺失的封包外），但流量會暫時在各廣播網域內泛洪做為未知的單點傳

送流量，而廣播網域中所有的交換器會重新學習動態 MAC 位址。

在啟用 vPC 對等交換器增強功能的相同故障情況中，N9K-1 和 N9K-2 會使用共用 vPC 系統 MAC 位址做為橋接器 ID 傳輸相同的跨距樹狀目錄 BPDU。如果 N9K-1 出現故障，N9K-2 將繼續傳輸此相同的生成樹 BPDU。因此，Access-1 和 Access-2 不知道生成樹拓撲發生了任何變化 — 從它們的角度來看，根網橋的生成樹 BPDU 完全相同，因此無需刷新相關 VLAN 中動態獲取的 MAC 地址。在此故障情況中，如此可防止每個廣播網域中發生未知單點傳送流量泛洪。

vPC 對等閘道

本節將說明 vPC 對等閘道增強功能，此功能須使用 `peer-gateway vPC` 網域組態命令才可啟用。

概觀

vPC 網域中設定的 Nexus 交換器會依預設執行雙主動第一躍點備援通訊協定 (FHRP) 轉送。這表示如果任一 vPC 對等體收到的封包的目的 MAC 位址屬於交換器上設定的熱待命路由器通訊協定 (HSRP) 或虛擬路由器備援通訊協定 (VRRP) 群組，則交換器會根據其本機路由表路由封包，而不論其 HSRP 或 VRRP 控制平面狀態如何。換句話說，對於處於 HSRP 待命或 VRRP 備份狀態的 vPC 對等，將封包路由傳送至 HSRP 或 VRRP 虛擬 MAC 位址乃是預期的行為。

vPC 對等路由器將資料包路由到 FHRP 虛擬 MAC 地址時，它會使用新的源和目標 MAC 地址重寫該資料包。來源 MAC 位址是封包路由到的 VLAN 中 vPC 對等點的交換虛擬介面 (SVI) 的 MAC 位址。根據 vPC 對等體的本地路由表，目的 MAC 地址是與資料包目的 IP 地址的下一跳 IP 地址關聯的 MAC 地址。在 VLAN 間路由場景中，資料包在重寫後的目的 MAC 地址是資料包最終目的地的主機的 MAC 地址。

部分主機不會跟進標準轉送行為做為最佳化功能。透過此行為，當該主機回覆傳入封包時，不會執行路由表和/或 ARP 快取查詢。但是，主機會翻轉回覆封包之傳入封包的來源和目的地 MAC 位址。換句話說，傳入封包的來源 MAC 位址會成為回覆封包的目的地 MAC 位址，且傳入封包的目的地 MAC 位址會成為回覆封包的來源 MAC 位址。此行為與遵循標準轉送行為的主機不同，可執行本機路由表和/或 ARP 快取查詢，並將回覆封包的目的地 MAC 位址設定為 FHRP 虛擬 MAC 位址。

如果主機產生的回覆封包定址於一個 vPC 對等，但將 vPC 輸出至另一個 vPC 對等，則此非標準主機行為可能違反 vPC 迴圈避免規則。另一台 vPC 對等裝置收到發往其 vPC 對等裝置所擁有的 MAC 地址的資料包，並將資料包從 vPC 對等鏈路轉發到擁有資料包目的 MAC 地址欄位中存在的 MAC 地址的 vPC 對等裝置。擁有 MAC 地址的 vPC 對等裝置嘗試在本地路由資料包。如果資料包需要輸出 vPC，則 vPC 對等體會因為違反 vPC 環路避免規則而丟棄此資料包。因此，您可能會觀察到利用此非標準行為之主機產生的部分流量，或傳送至該主機的部分流量，出現連線問題或封包遺失問題。

vPC 對等閘道增強功能的導入，係用於排除利用此非標準行為之主機所引起的封包遺失問題。藉由讓一個 vPC 對等在本機路由傳送至另一個 vPC 對等之 MAC 位址的封包，即可完成導入，使路由傳送至遠端 vPC 對等的封包不需要輸出 vPC 對等連結即可進行路由傳送。換句話說，vPC 對等閘道增強功能可讓一個 vPC 對等「代表」遠端 vPC 對等來路由傳送封包。vPC 對等閘道增強功能可使用 `peer-gateway vPC` 網域組態命令啟用。

注意事項

vPC 或 vPC VLAN 的單點傳送路由通訊協定鄰接翻動

如果動態單點傳送路由通訊協定鄰接係形成於兩個 vPC 對等，以及 vPC 連接路由器或透過 vPC 孤立連接埠連接的路由器之間，則路由通訊協定鄰接在啟用 vPC 對等閘道增強功能後會開始持續翻動（如果 Routing/Layer 3 over vPC 增強功能後續未立即受到設定）。此類故障情況將會在本文件之[使用 vPC 對等閘道透過 vPC 形成單點傳送路由通訊協定鄰接範例故障情況](#)和[使用 vPC 對等閘道透過 vPC VLAN 形成單點傳送路由通訊協定鄰接](#)的章節中詳細說明。

若要解決此問題，請在使用 peer-gateway vPC 網域組態命令啟用 vPC 對等閘道增強功能後，立即使用 layer3 peer-router vPC 網域組態命令啟用 Routing/Layer 3 over vPC 增強功能。

自動停用 ICMP 和 ICMPv6 重新導向

啟用 vPC 對等網關增強功能後，所有 vPC VLAN SVI（即與通過 vPC 對等鏈路中繼的 VLAN 關聯的任何 SVI）上都會自動禁用 ICMP 和 ICMPv6 重定向資料包的生成。交換器可透過在所有 vPC VLAN SVI 中設定 no ip redirects 和 no ipv6 redirects 達成此目的。如此可避免交換器產生 ICMP 重新導向封包來回覆輸入交換器（但具有交換器 vPC 對等的目的地 MAC 和 IP 位址）的封包。

如果在特定 VLAN 內的環境中需要 ICMP 或 ICMPv6 重定向資料包，則需要使用 peer-gateway exclude-vlan <vlan-id> vPC domain configuration 命令排除此 VLAN，使其無法利用 vPC 對等網關增強功能。

 註:Nexus 9000系列交換機不支援peer-gateway exclude-vlan <vlan-id> vPC域配置命令。

組態

設定 vPC 對等閘道功能的方法範例如下所示。

在此範例中，N9K-1 和 N9K-2 為 vPC 網域中的 vPC 對等。兩個 vPC 對等體都為 VLAN 10 配置了一個 HSRP 組。N9K-1 是優先順序為 150 的 HSRP 活動路由器，而 N9K-2 是預設優先順序為 100 的 HSRP 備用路由器。

```
<#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-1 之 VLAN 10 SVI 的 MAC 位址為 00ee.ab67.db47，而 N9K-2 之 VLAN 10 SVI 的 MAC 位址為 00ee.abd8.747f。VLAN 10 的 HSRP 虛擬 MAC 位址為 0000.0c07.ac0a。在此狀態中，每個交換器的 VLAN 10 SVI MAC 位址和 HSRP 虛擬 MAC 位址會出現在每個交換器的 MAC 位址表中。每台交換機的 VLAN 10 SVI MAC 地址和 HSRP 虛擬 MAC 地址都存在網關(G)標誌，這表示交換機在本地路由發往此 MAC 地址的資料包。

請注意，N9K-1 的 MAC 位址表不會出現 N9K-2 之 VLAN 10 SVI MAC 位址的 Gateway 旗標。同樣的，N9K-2 的 MAC 位址表不會出現 N9K-1 之 VLAN 10 SVI MAC 位址的 Gateway 旗標。

```
<#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)

我們可透過 peer-gateway vPC 網域組態命令啟用 vPC 對等閘道增強功能。這允許交換機本地路由接收的資料包，其目的MAC地址屬於在vPC對等鏈路上獲知的vPC對等裝置的MAC地址。透過在交換器 MAC 位址表內的 VPC 對等 MAC 位址中設定 Gateway 旗標，即可達成此目的。

<#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#
```

您可透過驗證 Gateway 旗標是否出現於 vPC 對等 MAC 的 MAC 位址表中，來確認 vPC 對等閘道增強功能是否如預期運作。

<#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)

影響

啟用vPC對等網關增強功能的影響可能因周圍拓撲和所連線主機的行為而異，具體如下文小節所述。如果以下兩個子部分均不適用於您的環境，則啟用vPC對等網關增強功能不會造成中斷，也不會對您的環境產生影響。

vPC 或 vPC VLAN 的單點傳送路由通訊協定鄰接翻動

如果動態單點傳送路由通訊協定鄰接係形成於兩個 vPC 對等，以及 vPC 連接路由器或透過 vPC 孤立連接埠連接的路由器之間，則路由通訊協定鄰接在啟用 vPC 對等閘道增強功能後會開始持續翻動（如果 Routing/Layer 3 over vPC 增強功能後續未立即受到設定）。此類故障情況將會在本文件之

[使用 vPC 對等閘道透過 vPC 形成單點傳送路由通訊協定鄰接範例故障情況](#)和[使用 vPC 對等閘道透過 vPC VLAN 形成單點傳送路由通訊協定鄰接](#)的章節中詳細說明。

若要解決此問題，請在使用 peer-gateway vPC 網域組態命令啟用 vPC 對等閘道增強功能後，立即使用 layer3 peer-router vPC 網域組態命令啟用 Routing/Layer 3 over vPC 增強功能。

自動停用 ICMP 和 ICMPv6 重新導向

啟用vPC對等網關增強功能後，所有vPC VLAN SVI (即與通過vPC對等鏈路中繼的VLAN關聯的任何SVI) 上都自動禁用ICMP和ICMPv6重定向資料包的生成。交換器可透過在所有 vPC VLAN SVI 中設定 no ip redirects 和 no ipv6 redirects 達成此目的。如此可避免交換器產生 ICMP 重新導向封包來回覆輸入交換器 (但具有交換器 vPC 對等的目的地 MAC 和 IP 位址) 的封包。

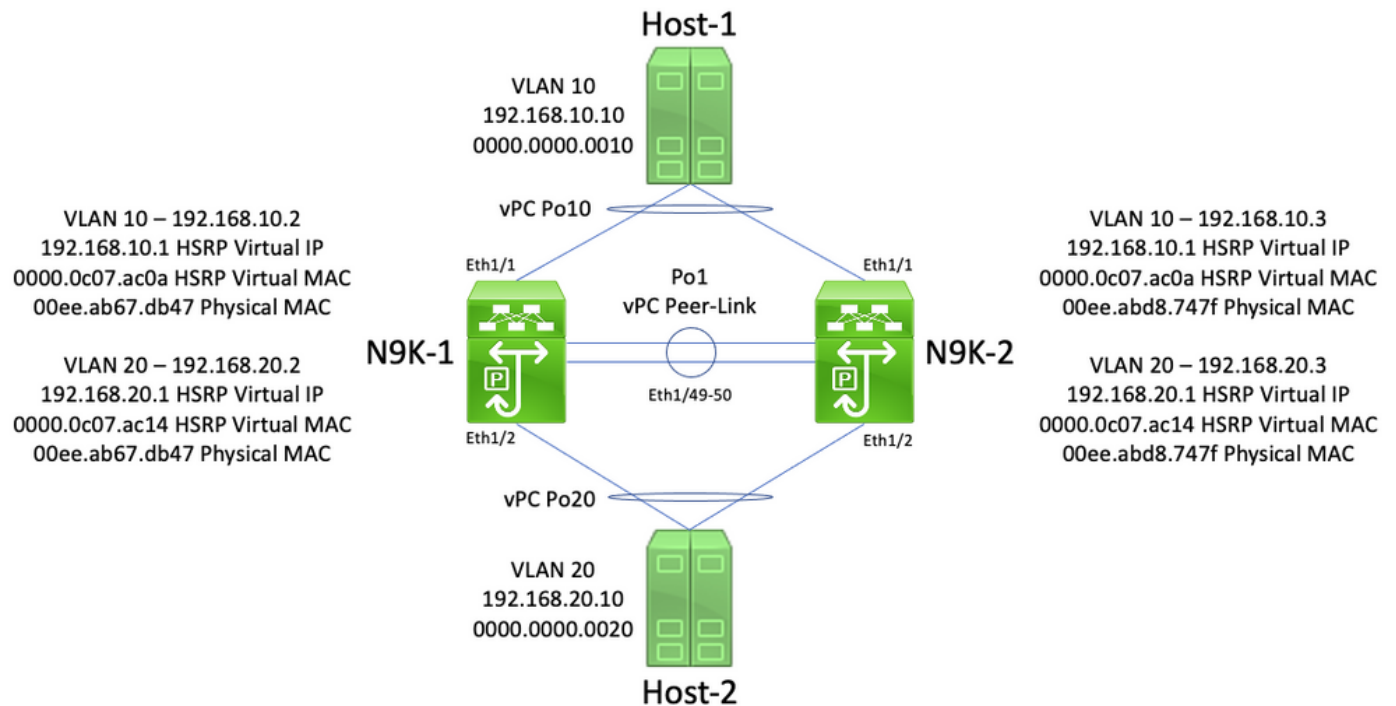
如果在特定VLAN內的環境中需要ICMP或ICMPv6重定向資料包，則需要使用peer-gateway exclude-vlan <vlan-id> vPC domain configuration命令排除此VLAN，使其無法利用vPC對等網關增強功能。

 註:Nexus 9000系列交換機不支援peer-gateway exclude-vlan <vlan-id> vPC域配置命令。

範例故障情況

具有非標準轉送行為的 vPC 連接主機

考量以下拓撲：

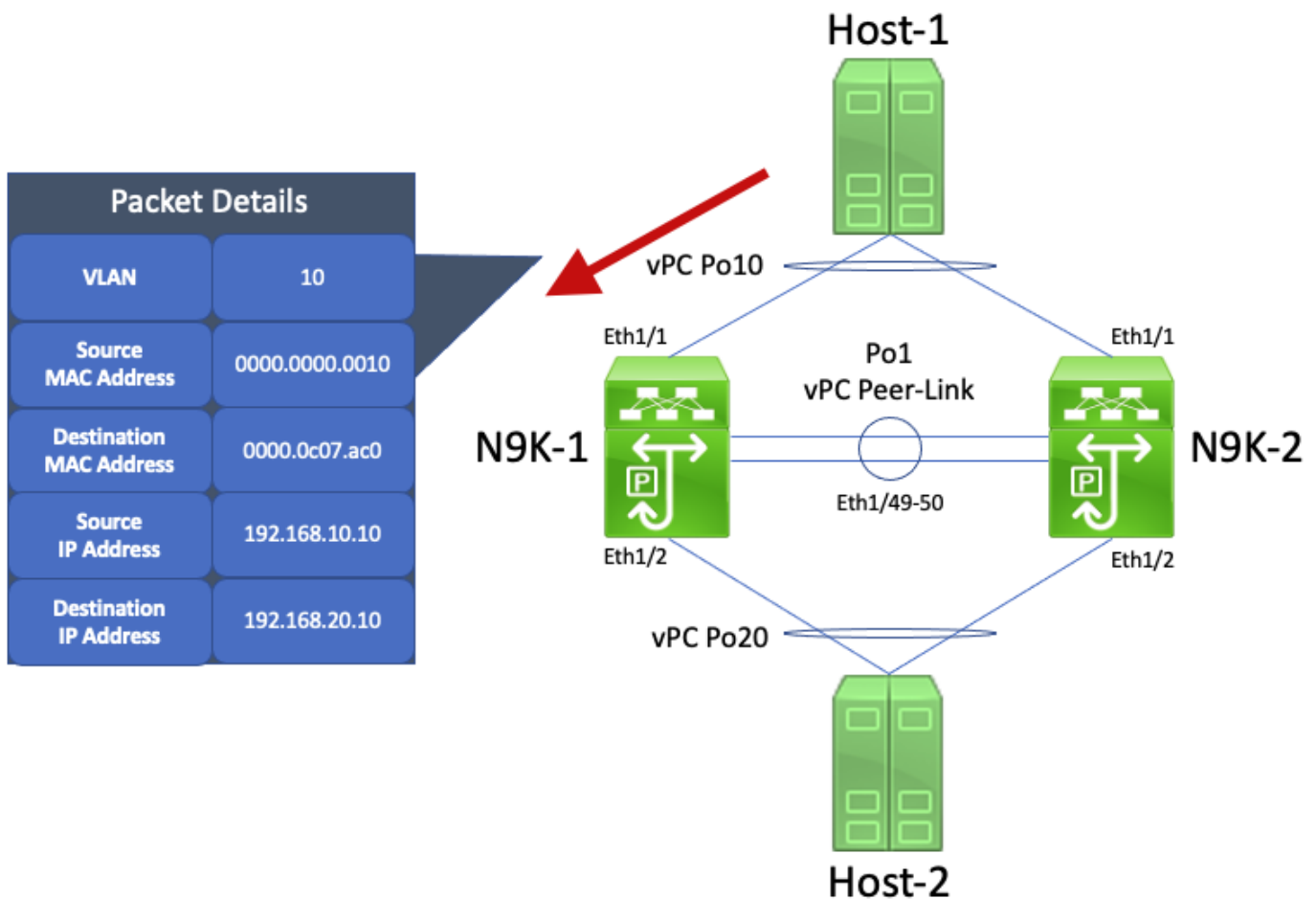


在此拓撲中，N9K-1和N9K-2是vPC域中的vPC對等體，在VLAN 10和VLAN 20之間執行VLAN間路由。介面 Po1 為 vPC 對等連結。名為Host-1的主機通過vPC Po10連線到VLAN 10中的N9K-1和N9K-2。Host-1擁有的IP地址為192.168.10.10,MAC地址為0000.0000.0010。名為Host-2的主機通

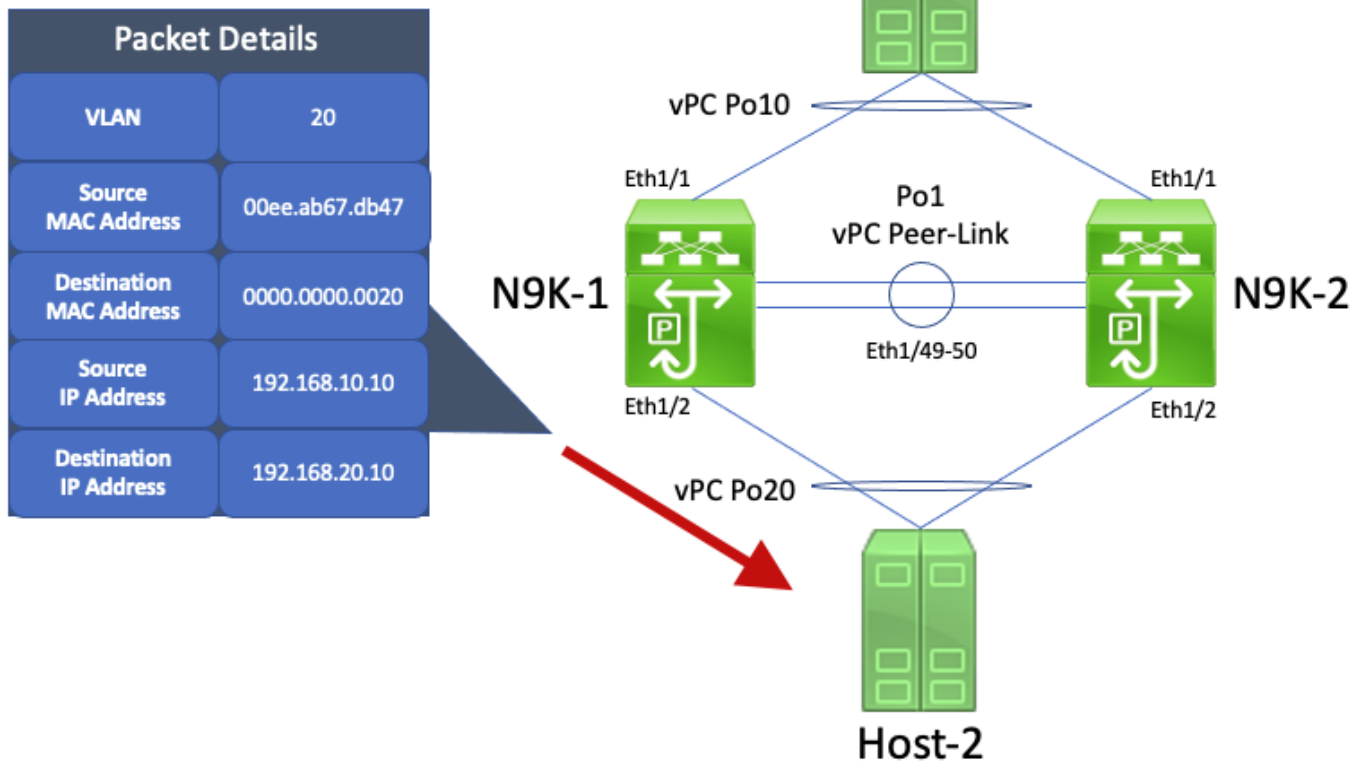
過vPC Po20連線到VLAN 20中的N9K-1和N9K-2。Host-2擁有的IP地址為192.168.20.10,MAC地址為0000.0000.0020。

N9K-1 和 N9K-2 在 VLAN 10 和 VLAN 20 中皆具有 SVI，每個 SVI 下皆已啟用 HSRP。N9K-1的 VLAN 10介面的IP地址為192.168.10.2,N9K-1的VLAN 20介面的IP地址為192.168.20.2。兩個N9K-1的SVI的物理MAC地址均為00ee.ab67.db47。N9K-2的VLAN 10介面的IP地址為192.168.10.3,N9K-2的VLAN 20介面的IP地址為192.168.20.3。兩個N9K-2的SVI的物理MAC地址均為00ee.abd8.747f。VLAN 10 的 HSRP 虛擬 IP 位址為 192.168.10.1，而 HSRP 虛擬 MAC 位址為 0000.0c07.ac0a。VLAN 20 的 HSRP 虛擬 IP 位址為 192.168.20.1，而 HSRP 虛擬 MAC 位址為 0000.0c07.ac14。

考慮以下情況：主機1將ICMP回應請求封包傳送到主機2。在Host-1為其預設網關（HSRP虛擬IP地址）解析ARP後，Host-1按照標準轉發行為生成一個ICMP回應請求資料包，源IP地址為192.168.10.10，目標IP地址為192.168.20.10，源MAC地址為0000.000.0010，目標MAC地址為000.0c07.ac0a。此資料包朝向N9K-1。其視覺範例如下所示。

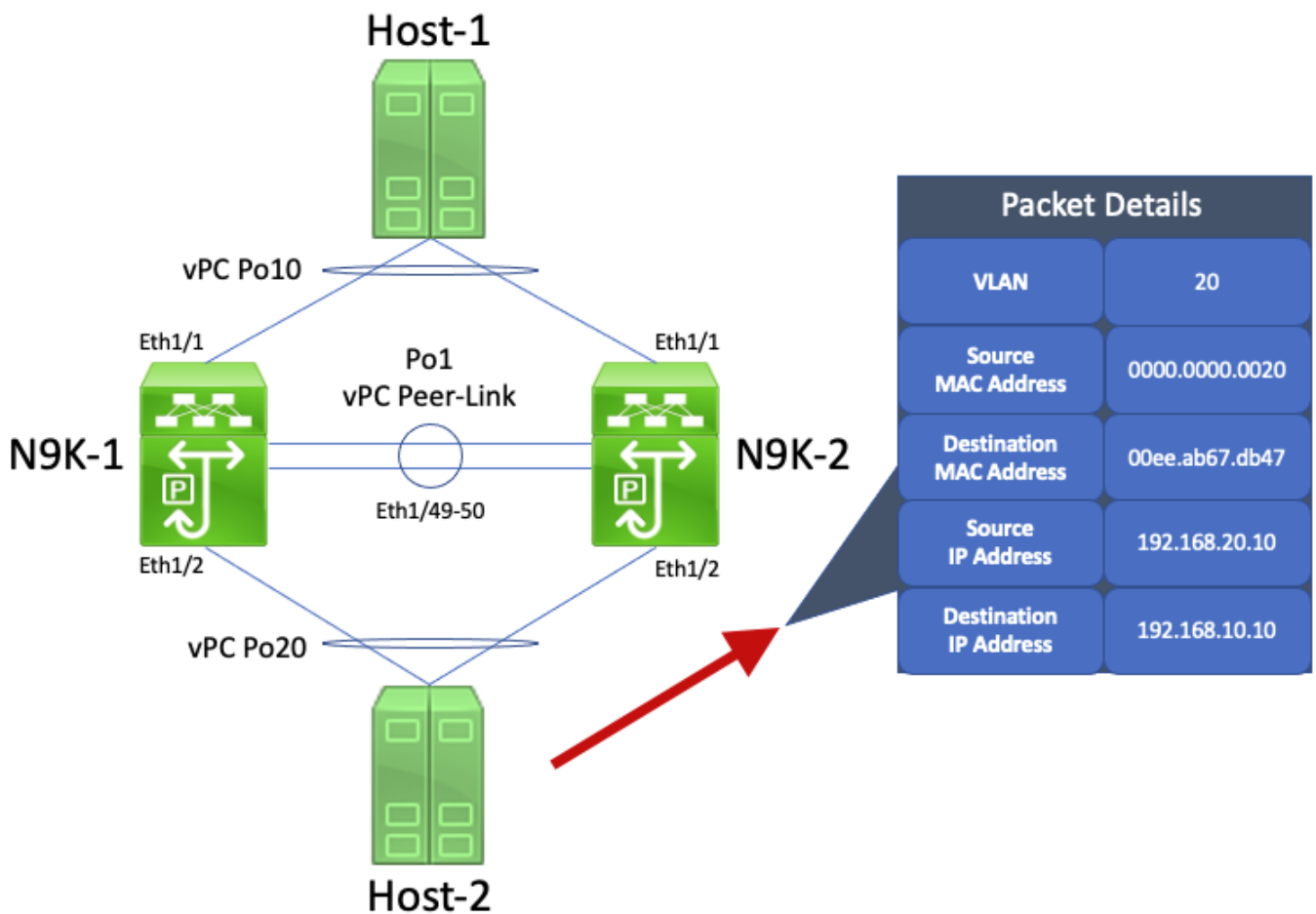


N9K-1 會接收此封包。由於此封包的目的地為 HSRP 虛擬 MAC 位址，因此 N9K-1 可根據其本機路由表路由傳送此封包（不受其 HSRP 控制層狀態影響）。此封包從VLAN 10路由到VLAN 20。作為資料包路由的一部分，N9K-1通過重新定址資料包的源MAC地址和目標MAC地址欄位來執行資料包重寫。資料包的新源MAC地址是與N9K-1的VLAN 20 SVI(00ee.ab67.db47)關聯的物理MAC地址，新的目標MAC地址是與Host-2(0000.0000.0020)關聯的MAC地址。其視覺範例如下所示。

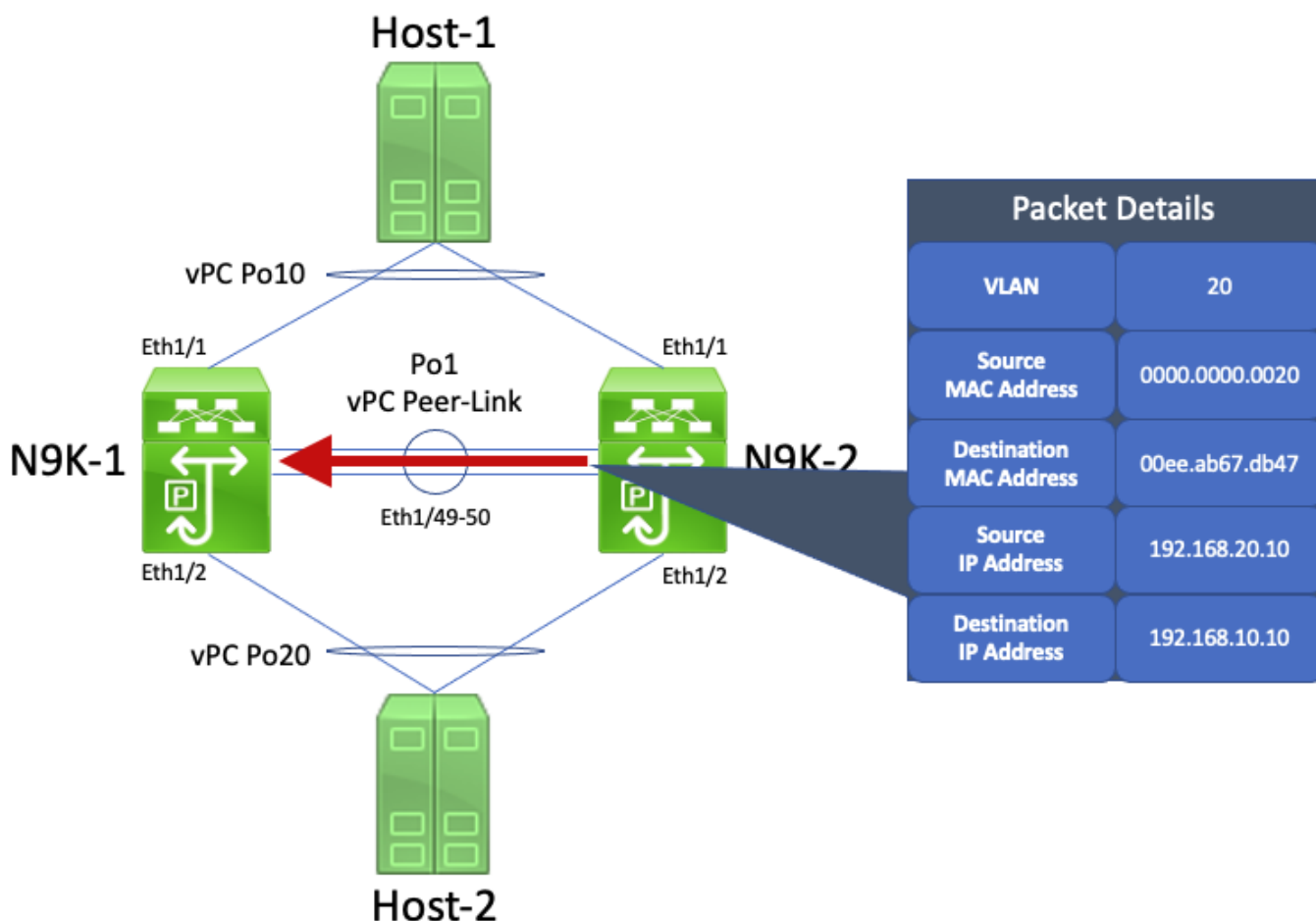


Host 2 會接收此封包，並產生 ICMP 回應回覆封包來回覆 Host-1 的 ICMP 回應要求封包。但是，Host-2 有時並不遵循標準轉送行為。若要最佳化其轉送功能，Host-2 不會執行 Host-1 之 IP 位址 (192.168.10.10) 的路由表或 ARP 快取查詢；反之，Host-2 會反轉其原始接收之 ICMP 回應要求封包的來源 MAC 位址和目的地 MAC 位址欄位。因此，Host-2 生成的 ICMP 回應應答資料包的源 IP 地址為 192.168.20.10，目的 IP 地址為 192.168.10.10，源 MAC 地址為 0000.0000.0020，目的 MAC 地址為 00ee.ab67.db47。

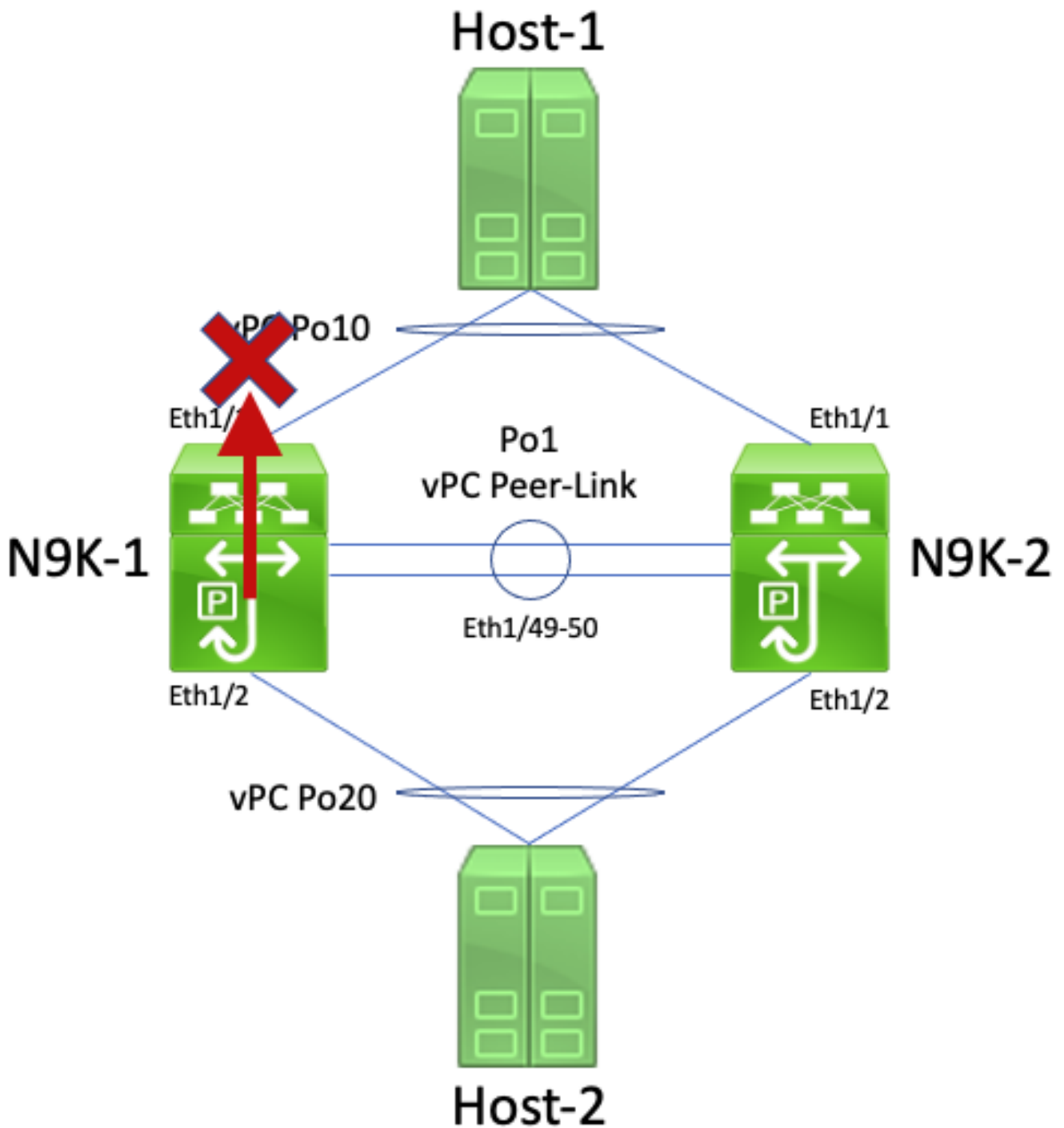
如果此 ICMP 回應應答資料包向 N9K-1 發出，則此資料包將轉發到 Host-1，而不會出現問題。但是，請考量此 ICMP 回應回覆封包輸出至 N9K-2 的情況，如下所示。



N9K-2 會接收此封包。由於此資料包的目的地是N9K-1的VLAN 20 SVI的物理MAC地址，因此N9K-2會通過vPC對等鏈路將該資料包轉發到N9K-1，因為N9K-2無法代表N9K-1路由此資料包。其視覺範例如下所示。




N9K-1 會接收此封包。由於此封包的目的地為 N9K-1 之 VLAN 20 SVI 的實體 MAC 位址，因此 N9K-1 可根據其本機路由表路由傳送此封包（不受其 HSRP 控制層狀態影響）。此封包從 VLAN 20 路由到 VLAN 10。但是，此路由的出口介面解析為 vPC Po10（在 N9K-2 上啟用）。這違反了 vPC 環路避免規則 — 如果 N9K-1 通過 vPC 對等鏈路收到資料包，如果 N9K-2 上相同 vPC 介面已啟動，則 N9K-1 無法將該資料包從 vPC 介面轉發出去。由於此違規，N9K-1 丟棄此資料包。其視覺範例如下所示。



您可透過使用 `peer-gateway vPC` 網域組態命令啟用 vPC 對等閘道增強功能，藉以解決此問題。這允許 N9K-2 代表 N9K-1 路由 ICMP 回應應答資料包（以及其他類似地址的資料包），即使資料包的目的地 MAC 地址屬於 N9K-1 而不是 N9K-2。因此，N9K-2 可以將該資料包從其 vPC Po10 介面轉發出去，而不是通過 vPC 對等鏈路轉發該資料包。

Routing/Layer 3 over vPC (第 3 層對等路由器)

本節將說明 Routing/Layer 3 over vPC 增強功能，此功能須使用 `layer3 peer-router vPC` 網域組態命令才可啟用。

 注意：啟用vPC上的路由/第3層增強功能後，不支援在vPC上形成組播路由協定鄰接（即協定無關組播[PIM]鄰接）。

概觀

在部分環境中，客戶希望透過 vPC 將路由器連接至 Nexus 交換器組，並使用兩個 vPC 對等透過 vPC 形成單點傳送路由通訊協定鄰接。或者，客戶希望透過 vPC VLAN 將路由器連接至單一 vPC 對等，並使用兩個 vPC 對等形成 vPC VLAN 的單點傳送路由通訊協定鄰接。因此，針對透過兩個 Nexus 交換器通告的首碼，vPC 連接路由器會使用等價多重路徑 (ECMP)。相對於在 vPC 連接路由器和兩個 vPC 對等間使用專用路由連結來節省 IP 位址使用率（僅需要 3 個 IP 位址，而非 4 個 IP 位址），或降低組態複雜性（已路由的介面與 SVI，特別是在可能需要使用子介面的 VRF-Lite 環境），此方式可能較為理想。

在過去，Cisco Nexus 平台並不支援透過 vPC 形成單點傳送路由通訊協定鄰接。不過，客戶可能已實作拓撲，其中單點傳送路由通訊協定鄰接毫無問題地會透過 vPC 的（即使不受支援）。在網路發生部分變更後（例如 vPC 連接路由或 vPC 對等本身的軟體升級、防火牆容錯移轉等），透過 vPC 的單點傳送路由通訊協定鄰接會停止運作，導致資料層流量封包遺失，或單點傳送路由通訊協定鄰接無法建立一或兩個 vPC 對等。此類情況故障與不支援之原因背後的技術詳細資料將於[本文件的範例故障情況章節](#)中探討。

導入 Routing/Layer 3 over vPC 增強功能，藉此新增透過 vPC 形成單點傳送路由通訊協定鄰接的支援。藉由讓 TTL 為 1 的單點傳送路由通訊協定封包透過 vPC 對等連結轉送，即可達成此目的，不會使封包的 TTL 遞減。因此，單點傳送通訊協定鄰接可毫無問題地透過 vPC 或 vPC VLAN 形成。使用 peer-gateway vPC 網域組態命令啟用 vPC 對等閘道增強功能後，Routing/Layer 3 over vPC 增強功能可使用 layer3 peer-router vPC 網域組態命令啟用。

針對每個 Cisco Nexus 平台導入 Routing/Layer 3 over vPC 增強功能的支援之 NX-OS 軟體版本，皆記載於在[Nexus 平台上透過虛擬連接埠通道路由的支援拓撲文件](#)內的表 2（「透過 vPC 的路由通訊協定鄰接支援」）。

注意事項

不定期 VPC-2-L3_VPC_UNEQUAL_WEIGHT 系統日誌

啟用 Routing/Layer 3 over vPC 增強功能後，兩個 vPC 對等體都會開始生成類似於以下任一情況的系統日誌：

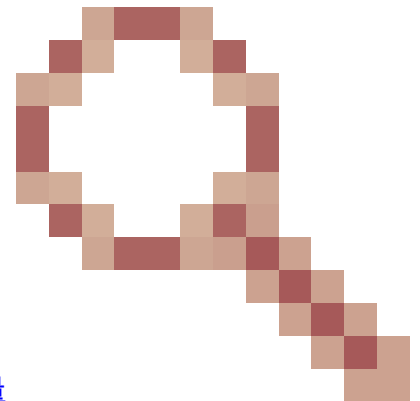
```
2021 May 26 19:13:47.079 switch %VPC-2-L3_VPC_UNEQUAL_WEIGHT: Layer3 peer-router is enabled. Please make
2021 May 26 19:13:47.351 switch %VPC-2-L3_VPC_UNEQUAL_WEIGHT: Unequal weight routing is not supported i
```

以上系統日誌皆不會顯示交換器的問題。啟用 Routing/Layer 3 over vPC 增強功能後，此類系統日誌會對管理員發出警告，表示兩個 vPC 對等的路由組態、成本及加權皆應相同，以確保兩個 vPC 對等皆可以相同方式路由流量。這不一定表示任何一個 vPC 對等出現不符合的路由組態、成本或加權。

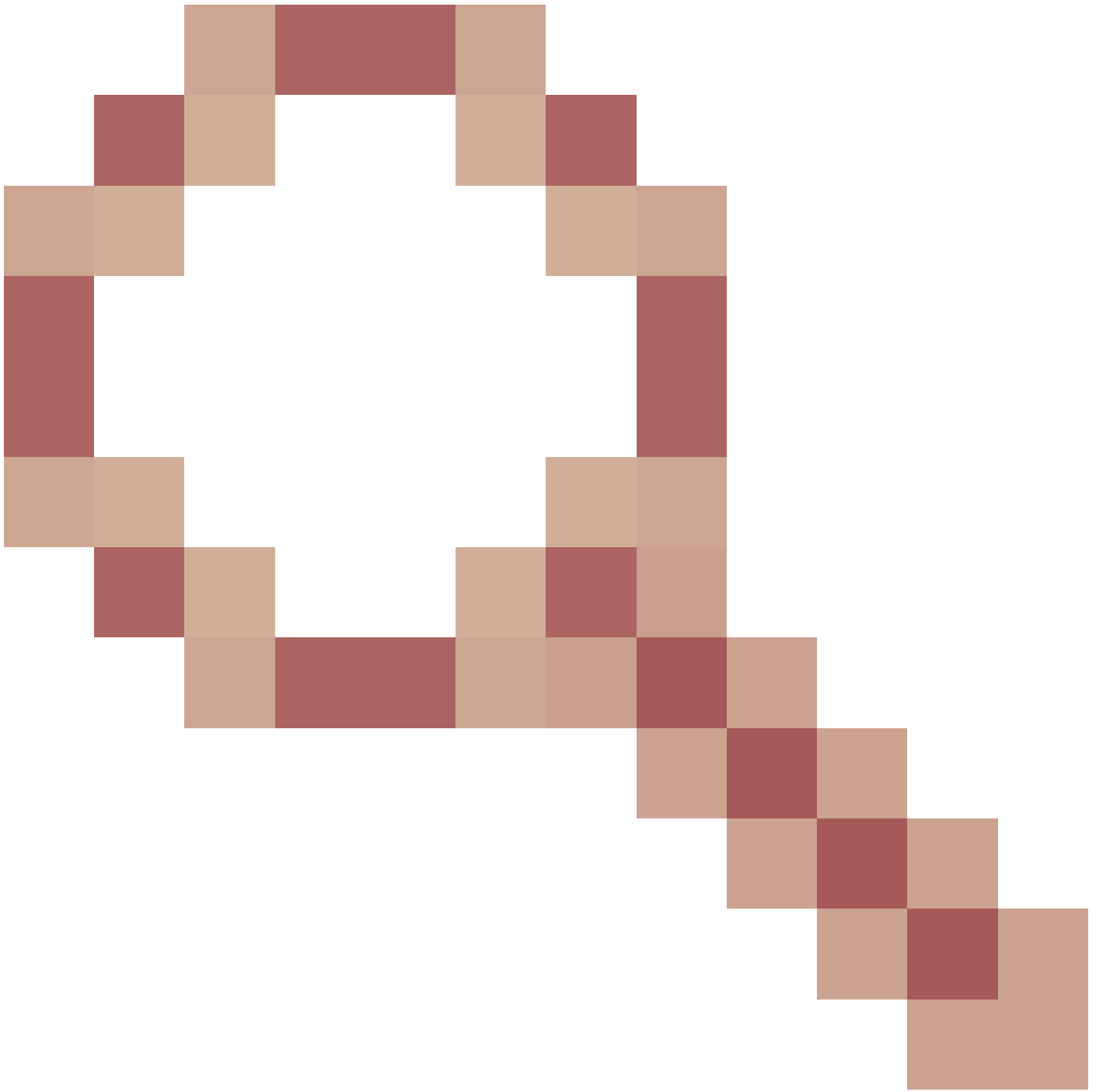
以上系統日誌可透過此處顯示的組態停用。

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

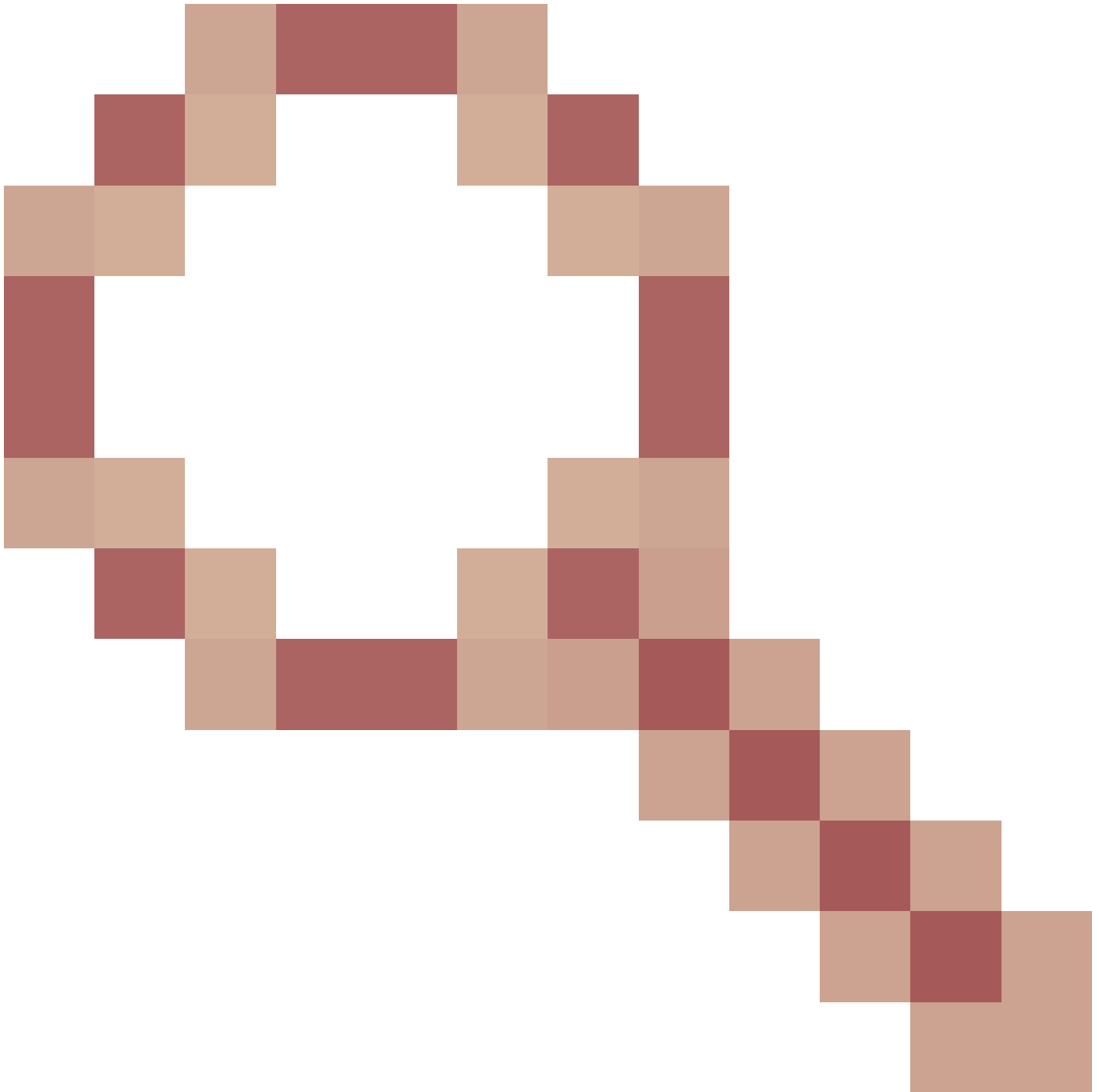
需要在兩個vPC對等體上執行此配置，以禁用兩個vPC對等體上的syslog。



由於Cisco錯誤ID [CSCvs82183](#)，已轉發TTL為1的軟體的資料平面流量
和思科錯誤ID [CSCvw16965](#)



在配備雲擴展ASIC且運行NX-OS軟體版本9.3(6)之前的Nexus 9000系列交換機上啟用vPC上的路由/第3層增強功能時，與TTL為1的單播路由協定不關聯的資料平面流量會被傳送到管理引擎並在軟體中而不是硬體中轉發。根據Nexus交換機是固定機箱（也稱為「架頂式」）交換機還是模組化機箱（也稱為「行尾式」）交換機以及交換機當前的NX-OS軟體版本，此問題的根本原因可能是軟體缺陷Cisco錯誤ID [CSCvs82183](#)



這兩個軟體缺陷只影響配備雲規模ASIC的Nexus 9000系列交換機 — 任何問題都不會影響其他Cisco Nexus硬體平台。如需詳細資料，請參閱個別軟體瑕疵的資訊。

若要避免此類軟體瑕疵，思科建議升級至 NX-OS 軟體 9.3(6) 版或更新版本。做為一般建議，思科通常會建議升級至適用於 Nexus 9000 系列交換器之最新建議的 NX-OS 軟體版本 (請參照[適用於 Cisco Nexus 9000 系列交換器的建議 Cisco NX-OS 版本文件](#)) 。

組態

設定 Routing/Layer 3 over vPC 增強功能的方式範例如下所示。

在此範例中，N9K-1 和 N9K-2 為 vPC 網域中的 vPC 對等。兩個 vPC 對等皆已啟用 vPC 對等閘道增強功能，此功能必須先啟用，才可啟用 Routing/Layer 3 over vPC 增強功能。兩台vPC對等體的VLAN 10中都有一個SVI，該SVI在OSPF進程1下啟用。N9K-1和N9K-3與vPC連線的OSPF路由器

(IP地址和鄰居ID為192.168.10.3) 處於OSPF EXSTART/EXCHANGE狀態。

<#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
```

我們可透過 layer3 peer-router vPC 網域組態命令啟用 Routing/Layer 3 over vPC 增強功能。這可以防止vPC對等體在啟用vPC對等網關增強後降低路由的單播路由協定資料包的TTL。

<#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#

```

您可透過驗證使用 vPC 連接 OSPF 相鄰裝置的 OSPF 鄰接，在啟用 Routing/Layer 3 over vPC 增強功能後，是否立即轉換至 FULL 狀態，確認 Routing/Layer 3 over vPC 增強功能是否如預期運作。

<#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  TOWAY/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  TOWAY/DROTHER          00:12:27 192.168.10.1    Vlan10
192.168.10.3    1  FULL/BDR                00:00:19 192.168.10.3    Vlan10

```

影響

啟用 Routing/Layer 3 over vPC 增強功能本質上不會對 vPC 網域造成任何影響。這表示當您啟用 vPC 上的路由/第3層增強功能時，vPC 對等裝置不會掛起任何 vPC，也不會因啟用此增強功能而受到任何資料平面流量的固有影響。

然而，如果動態路由通訊協定鄰接（曾因未啟用 Routing/Layer 3 over vPC 增強功能而關閉）突然因啟用此增強功能而建立，則根據受影響之路由通訊協定鄰接的角色、透過此類鄰接通告的特定首

碼，以及單點傳送路由表的目前狀態，可能會在啟用 Routing/Layer 3 over vPC 增強功能後觀察到部分中斷情況。

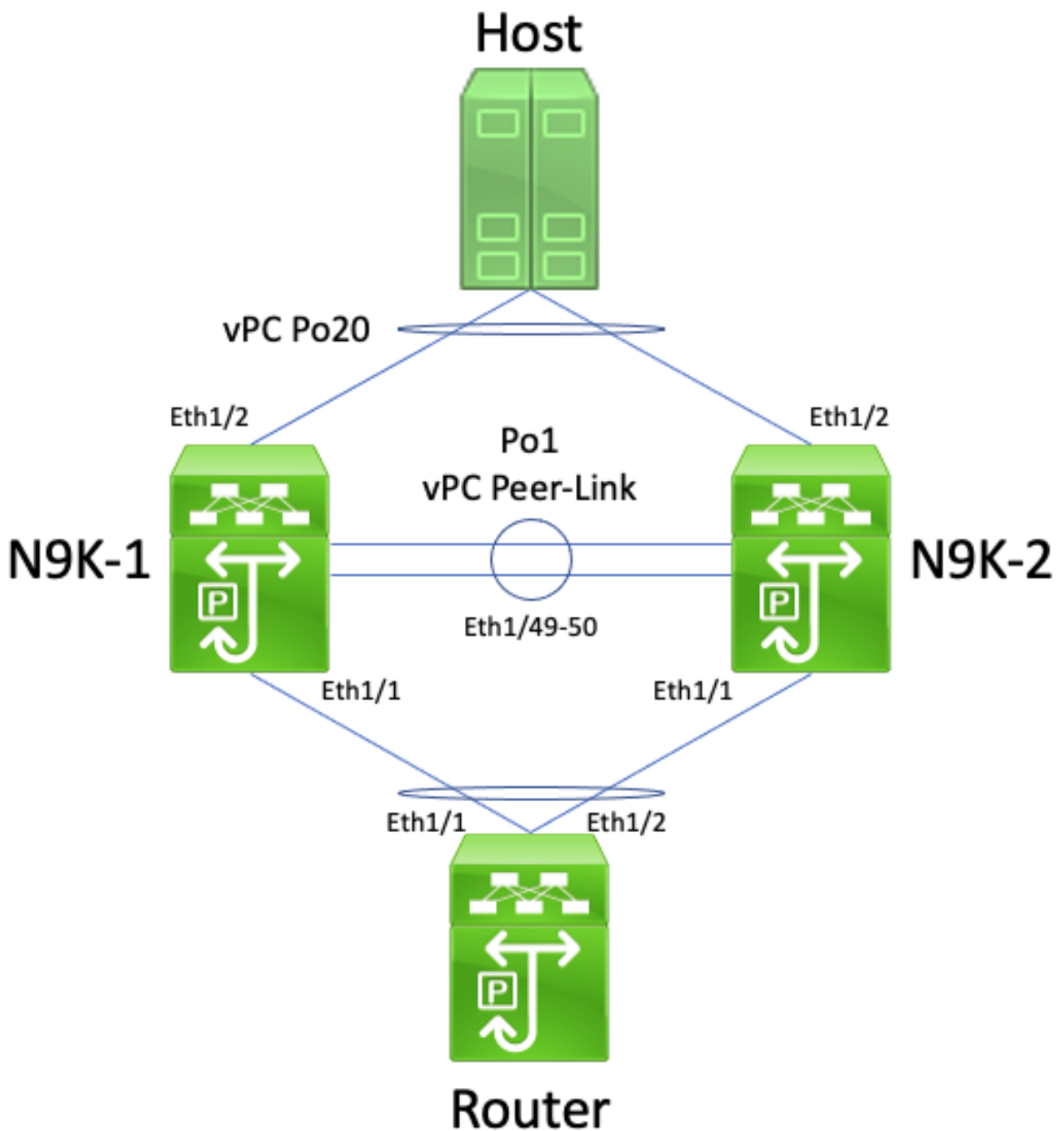
因此，思科建議客戶在維護時段啟用此增強功能，並預期可能會出現控制平面和資料平面中斷，除非客戶非常確信受影響的路由協定鄰接關係不會顯著影響網路運行。

此外，思科也建議仔細檢視[本文件的注意事項章節](#)，瞭解任何影響 NX-OS 軟體版本的軟體瑕疵（可能會造成 TTL 為 1 的自然資料層流量在軟體（而非硬體）中進行處理）。

範例故障情況

未使用 vPC 對等閘道透過 vPC 形成單點傳送路由通訊協定鄰接

考量以下所示的拓撲：



在此拓撲中，Nexus 交換器 N9K-1 和 N9K-2 皆為 vPC 網域內的 vPC 對等，其中的 vPC 對等閘道增強功能尚未啟用。介面 Po1 為 vPC 對等連結。主機名為 Router 的路由器通過 vPC Po10 連線到 N9K-1 和 N9K-2。主機通過 vPC Po20 連線到 N9K-1 和 N9K-2。路由器的 Po10 介面是路由埠通道，在單播路由協定下啟用。N9K-1 和 N9K-2 皆具有遵循相同單點傳送路由通訊協定啟用的 SVI 介面，且皆與 Router 位於相同的廣播網域。

由於 vPC 連接路由器的 ECMP 雜湊決策與其第 2 層連接埠通道雜湊決策可能有所差異，因此不支援透過未啟用 vPC 對等閘道增強功能的 vPC 形成單點傳送路由通訊協定鄰接。在此拓撲中，路由器、N9K-1 和 N9K-2 之間將成功形成路由協定鄰接。考慮路由器和主機之間的流量傳輸。通過 Router 前往 Host 的資料層流量可能會以屬於 N9K-1 之 SVI MAC 位址的目的地 MAC 位址重寫（因為路由器執行的 ECMP 雜湊決策），但會從介面 Ethernet1/2 輸出（因為路由器執行的第 2 層

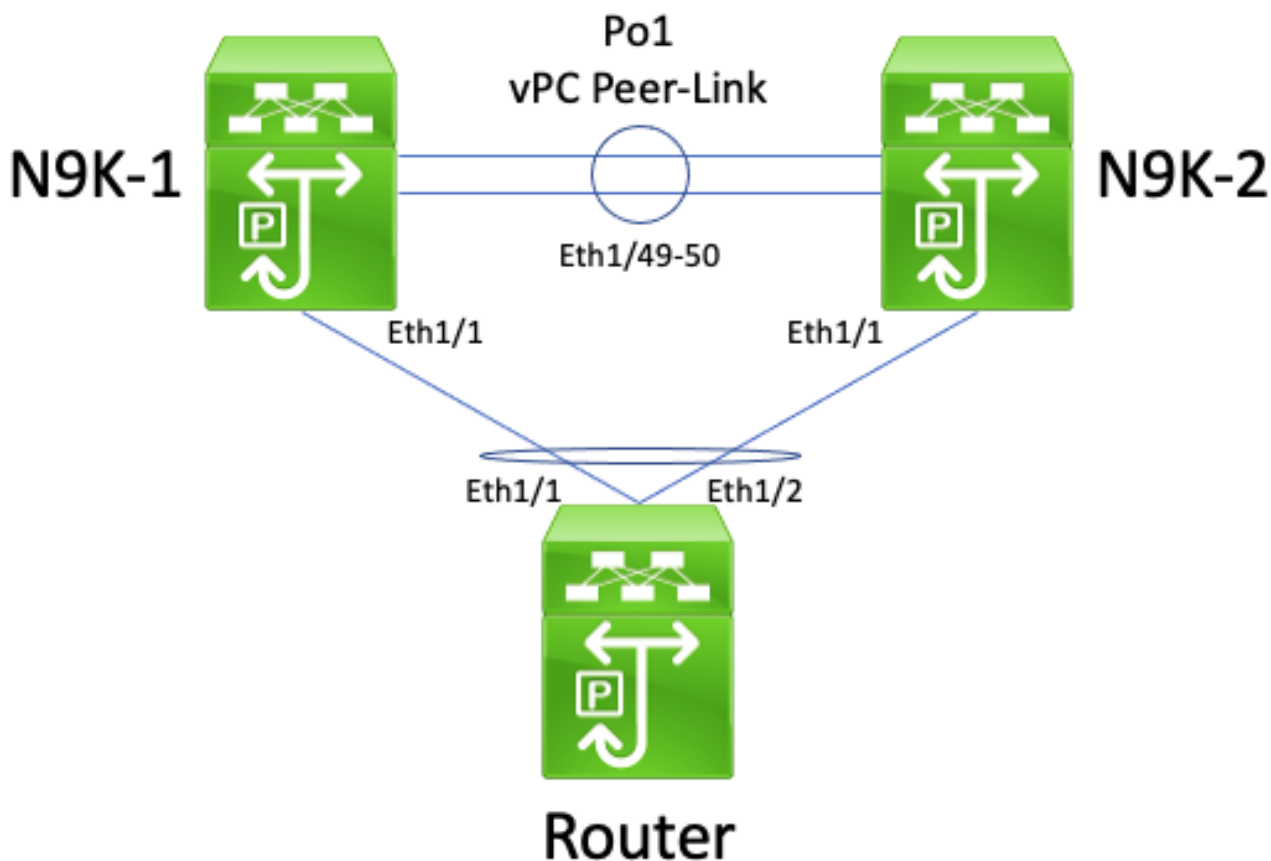
連接埠通道雜湊決策)。

N9K-2收到此資料包，並通過vPC對等鏈路轉發它，因為目標MAC地址屬於N9K-1，並且未啟用vPC對等網關增強功能（允許N9K-2代表N9K-1路由資料包）。N9K-1在vPC對等鏈路上收到此資料包，並發現它需要在vPC Po20中將資料包從其Ethernet1/2轉發出去。這違反了vPC環路避免規則，因此N9K-1丟棄硬體中的資料包。因此，您可能會觀察到部分通過此拓撲之vPC網域的流量發生連線問題或封包遺失問題。

您可透過使用 peer-gateway vPC 網域組態命令啟用 vPC 對等閘道增強功能，再使用 layer3 peer-router vPC 網域組態命令啟用 Routing/Layer 3 over vPC 增強功能來解決此問題。若要有效減少中斷，您應接連不斷地啟用這兩個 vPC 增強功能，如此「使用 vPC 對等閘道透過 vPC 形成單點傳送路由通訊協定鄰接」章節中所述的故障情況將不會再發生。

使用 vPC 對等閘道透過 vPC 形成單點傳送路由通訊協定鄰接

考量以下所示的拓撲：



在此拓撲中，Nexus 交換器 N9K-1 和 N9K-2 皆為 vPC 網域內的 vPC 對等，其中的 vPC 對等閘道增強功能已啟用。介面 Po1 為 vPC 對等連結。主機名為 Router 的路由器通過 vPC Po10 連線到 N9K-1 和 N9K-2。路由器的 Po10 介面是路由埠通道，在單播路由協定下啟用。N9K-1 和 N9K-2 皆具有遵循相同單點傳送路由通訊協定啟用的 SVI 介面，且皆與 Router 位於相同的廣播網域。

由於 vPC 對等閘道增強功能可能會讓單點傳送路由通訊協定鄰接，無法在 vPC 連接路由器和兩個 vPC 對等間形成，因此不支援透過啟用 vPC 對等閘道增強功能的 vPC 形成單點傳送路由通訊協定

鄰接。在此拓撲中，路由器與N9K-1或N9K-2之間的路由協定鄰接關係可能無法按預期啟動，具體取決於路由器發起的單播路由協定資料包如何通過vPC Po10到達N9K-1或N9K-2雜湊。

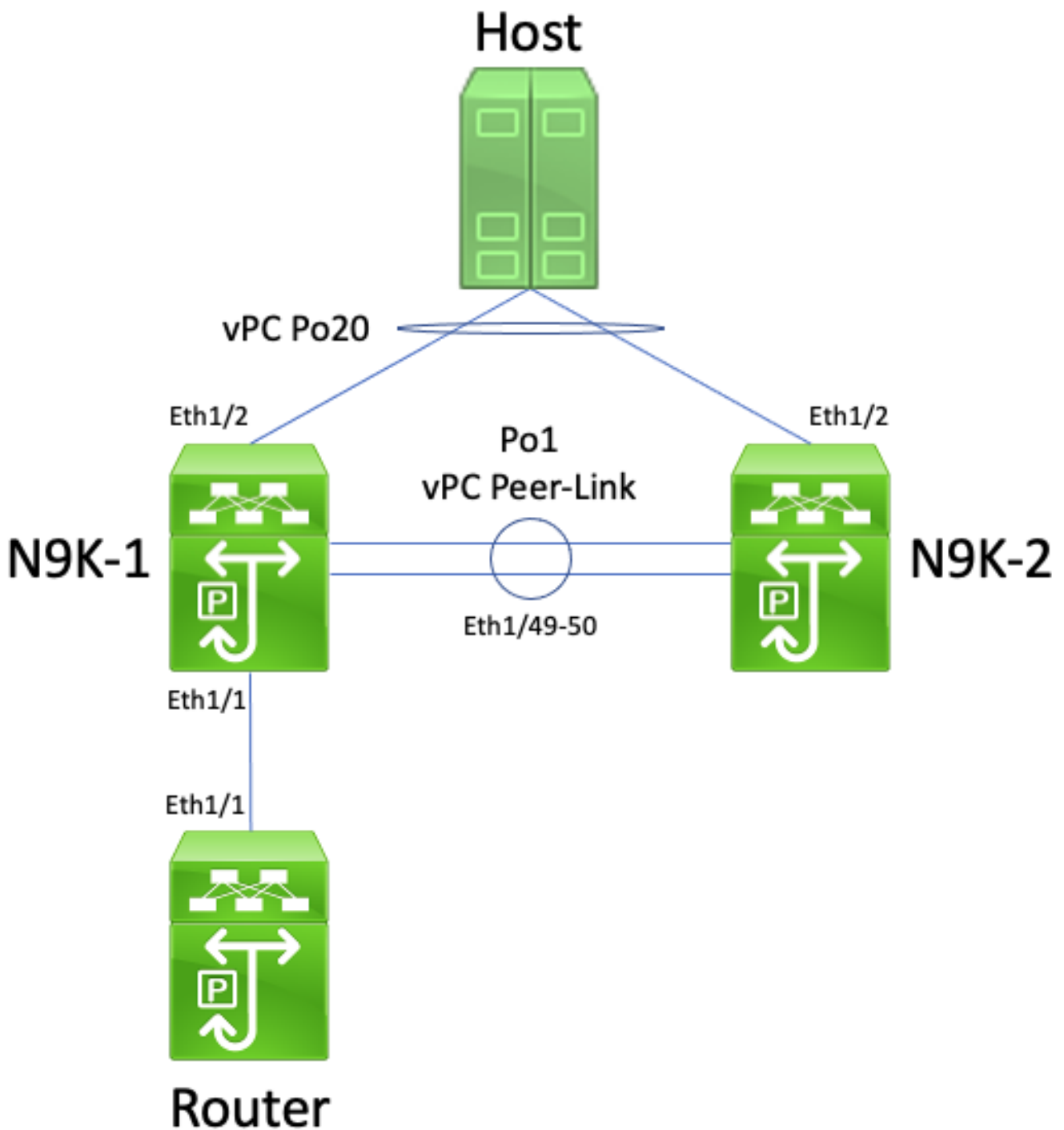
所有路由皆可毫無問題地傳送和接收連結本機的多點傳送路由通訊協定封包（一般稱為「Hello」封包），因為此類封包皆會成功泛洪至 vPC VLAN。但是，請考量從 Router 產生傳送至 N9K-1 的單點傳送路由通訊協定封包，將 Ethernet1/2 輸出至 N9K-2（因為 Router 的第 2 層連接埠通道雜湊決策）的情況。此資料包的目的地是N9K-1的SVI MAC地址，但是入口N9K-2的Ethernet1/1介面。N9K-2發現資料包的目的地是N9K-1的SVI MAC地址，由於啟用了vPC對等網關增強功能，該地址安裝在N9K-2的MAC地址表中，並帶有「G」或「網關」標誌。因此，N9K-2嘗試代表N9K-1對單播路由協定資料包進行本地路由。

但是，通過路由資料包，資料包的生存時間(TTL)會遞減，而大多數單播路由協定資料包的TTL是1。因此，資料包的TTL會遞減到0，然後以N9K-2丟棄。從N9K-1的角度來看，N9K-1正在接收來自路由器的本地鏈路組播路由協定資料包，並且能夠將單播路由協定資料包傳送到路由器，但是沒有接收來自路由器的單播路由協定資料包。因此，N9K-1斷開了路由協定與路由器的鄰接關係，並重新啟動其本地有限狀態機。同樣地，路由器會重新啟動其本地有限狀態機，以用於路由協定。

您可透過 layer 3 peer-router vPC 網域組態命令啟用 Routing/Layer 3 over vPC 增強功能來解決此問題。如此可讓 TTL 為 1 的單點傳送路由通訊協定封包透過 vPC 對等連結轉送，不會使封包的 TTL 遞減。因此，單點傳送通訊協定鄰接可毫無問題地透過 vPC 或 vPC VLAN 形成。

未使用 vPC 對等閘道透過 vPC VLAN 形成單點傳送路由通訊協定鄰接

考量以下所示的拓撲：



在此拓撲中，Nexus 交換器 N9K-1 和 N9K-2 皆為 vPC 網域內的 vPC 對等，其中的 vPC 對等閘道增強功能尚未啟用。介面 Po1 為 vPC 對等連結。主機名為 Router 的路由器通過 Ethernet1/1 連線到 N9K-1 的 Ethernet1/1。路由器的 Ethernet1/1 介面是在單播路由協定下啟用的路由介面。N9K-1 和 N9K-2 皆具有遵循相同單點傳送路由通訊協定啟用的 SVI 介面，且皆與 Router 位於相同的廣播網域。

由於 vPC VLAN 連接路由器的 ECMP 雜湊決策，可能會造成 N9K-2 因為違反 vPC 迴圈避免規則而捨棄資料層流量，因此不支援透過未啟用 vPC 對等閘道增強功能的 vPC VLAN 形成單點傳送路由通訊協定鄰接。在此拓撲中，路由器、N9K-1 和 N9K-2 之間將成功形成路由協定鄰接。考慮路由器和主機之間的流量傳輸。通過 Router 傳送至 Host 的資料層流量可能會以屬於 N9K-2 之 SVI MAC 位址的目的地 MAC 位址重寫（因為路由器執行的 ECMP 雜湊決策），並從介面 Ethernet1/1

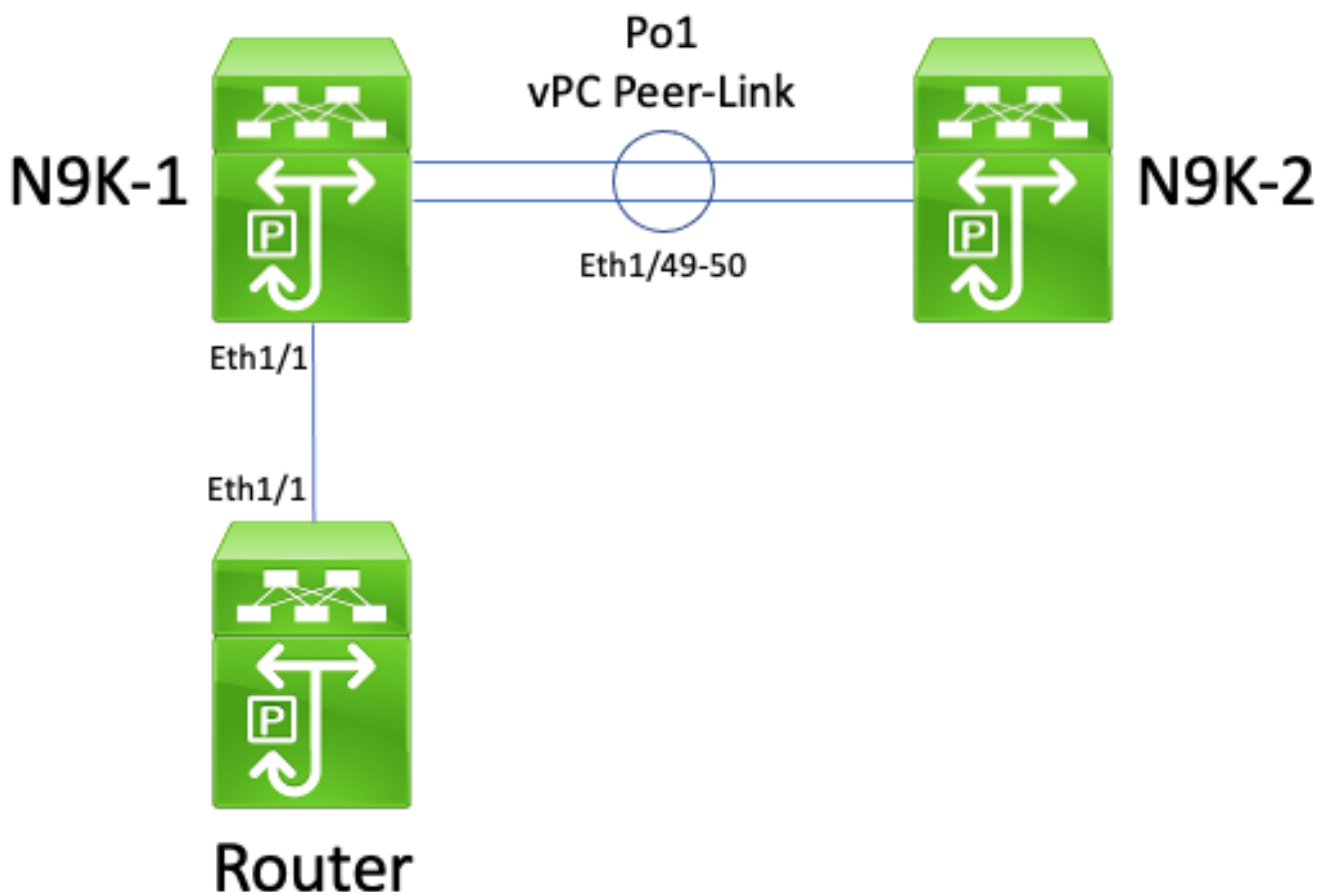
輸出至 N9K-1。

N9K-1收到此資料包，並通過vPC對等鏈路轉發它，因為目標MAC地址屬於N9K-2，並且未啟用vPC對等網關增強功能（允許N9K-1代表N9K-2路由資料包）。N9K-2在vPC對等鏈路上收到此資料包，並發現它需要在vPC Po20中將資料包從其Ethernet1/2轉發出去。這違反了vPC環路避免規則，因此N9K-2丟棄了硬體中的資料包。因此，您可能會觀察到部分通過此拓撲之vPC網域的流量發生連線問題或封包遺失問題。

您可透過使用 peer-gateway vPC 網域組態命令啟用 vPC 對等閘道增強功能，再使用 layer3 peer-router vPC 網域組態命令啟用 Routing/Layer 3 over vPC 增強功能來解決此問題。若要有效減少中斷，您應接連不斷地啟用這兩個 vPC 增強功能，如此「使用 vPC 對等閘道透過 vPC 形成單點傳送路由通訊協定鄰接」章節中所述的故障情況將不會再發生。

使用 vPC 對等閘道透過 vPC VLAN 形成單點傳送路由通訊協定鄰接

考量以下所示的拓撲：



在此拓撲中，Nexus 交換器 N9K-1 和 N9K-2 皆為 vPC 網域內的 vPC 對等，其中的 vPC 對等閘道增強功能已啟用。介面 Po1 為 vPC 對等連結。主機名為Router的路由器通過Ethernet1/1連線到N9K-1的Ethernet1/1。路由器的Ethernet1/1介面是在單播路由協定下啟用的路由介面。N9K-1 和 N9K-2 皆具有遵循相同單點傳送路由通訊協定啟用的 SVI 介面，且皆與 Router 位於相同的廣播網域。

不支援在已啟用vPC對等網關增強功能的vPC VLAN上建立單播路由協定鄰接，因為vPC對等網關增

強功能可防止在連線vPC VLAN的路由器與未直接連線到vPC對等路由器之間形成單播路由協定鄰接。在此拓撲中，由於啟用了vPC對等網關增強功能，N9K-1路由單播路由協定資料包目的地為N9K-2的SVI MAC地址，因此路由器和N9K-2之間的路由協定鄰接無法按預期啟動。因為封包已路由傳送，因此其存留時間 (TTL) 必須遞減。單點傳送路由通訊協定封包的 TTL 一般為 1，而將封包的 TTL 遞減至 0 的路由器必須捨棄該封包。

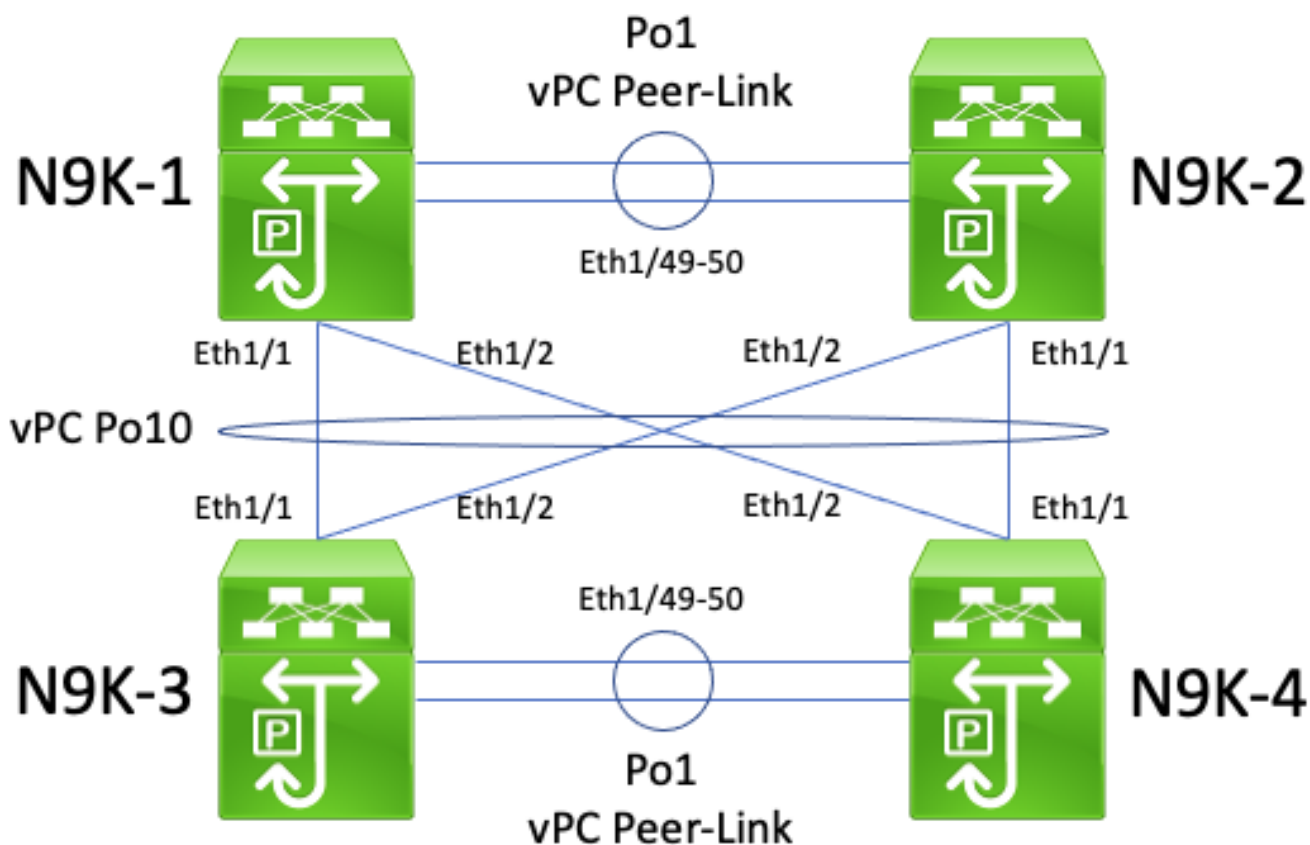
所有路由皆可毫無問題地傳送和接收連結本機的多點傳送路由通訊協定封包（一般稱為「Hello」封包），因為此類封包皆會成功泛洪至 vPC VLAN。但是，請考慮以下情況：來源為發往N9K-2的路由器的單播路由協定資料包從Ethernet1/1發往N9K-1。此資料包的目的地是N9K-2的SVI MAC地址，但是入口N9K-1的Ethernet1/1介面。N9K-1發現資料包的目的地是N9K-2的SVI MAC地址，該地址安裝在N9K-1的MAC地址表中，由於啟用了vPC對等網關增強功能，因此標籤有「G」或「網關」。因此，N9K-1嘗試代表N9K-2對單播路由協定資料包進行本地路由。

但是，通過路由資料包，資料包的TTL會遞減，而大多數單播路由協定資料包的TTL是1。因此，資料包的TTL會遞減到0，然後以N9K-1丟棄。從N9K-2的角度來看，N9K-2正在接收來自路由器的本地鏈路組播路由協定資料包，並且能夠將單播路由協定資料包傳送到路由器，但是沒有接收來自路由器的單播路由協定資料包。因此，N9K-2斷開了路由協定與路由器的鄰接關係，並重新啟動其本地有限狀態機。同樣地，路由器會重新啟動其本地有限狀態機，以用於路由協定。

您可透過 layer 3 peer-router vPC 網域組態命令啟用 Routing/Layer 3 over vPC 增強功能來解決此問題。如此可讓 TTL 為 1 的單點傳送路由通訊協定封包透過 vPC 對等連結轉送，不會使封包的 TTL 遞減。因此，單點傳送通訊協定鄰接可毫無問題地透過 vPC 或 vPC VLAN 形成。

使用 vPC 對等閘道透過連續 vPC 形成單點傳送路由通訊協定鄰接

考量以下所示的拓撲：



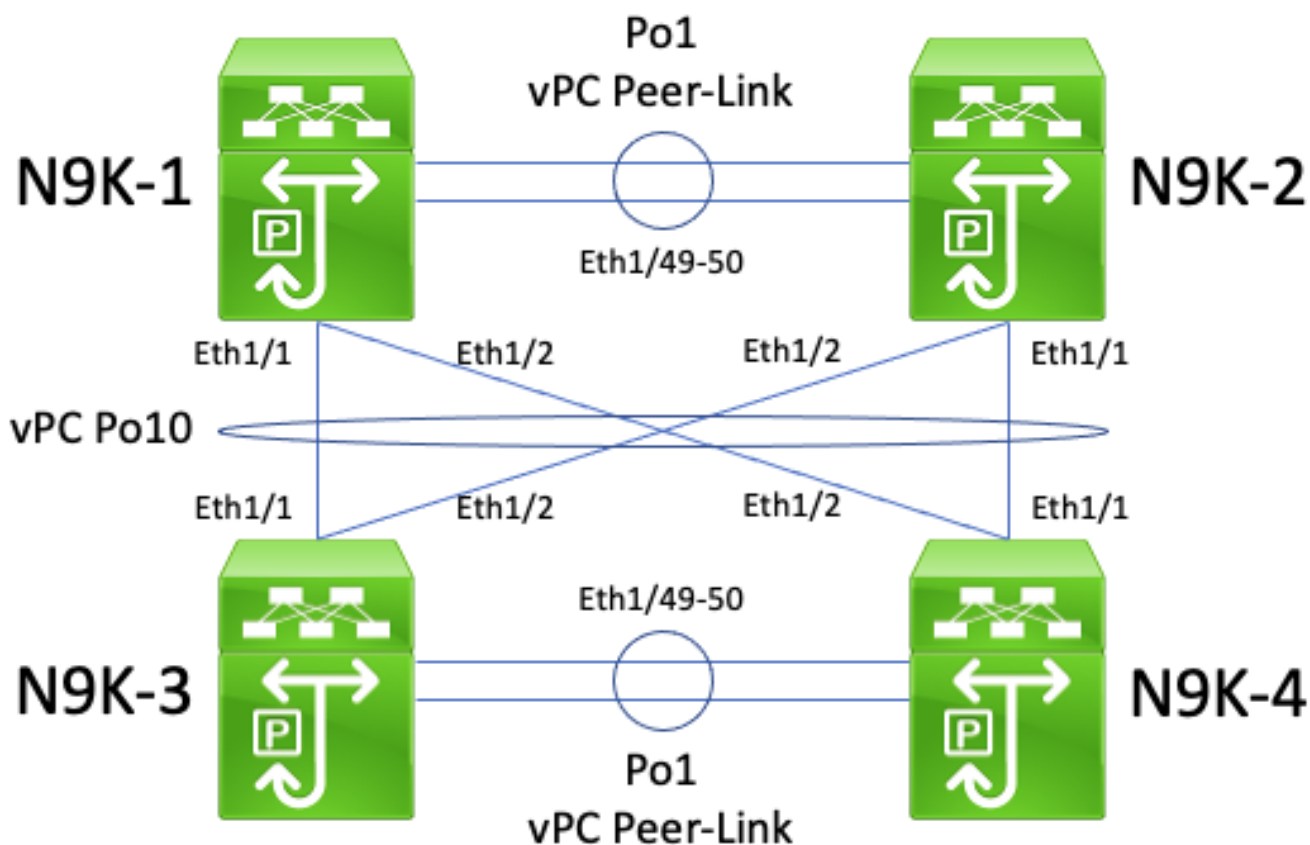
在此拓撲中，Nexus 交換器 N9K-1 和 N9K-2 皆為 vPC 網域內的 vPC 對等，其中的 vPC 對等閘道增強功能已啟用。Nexus 交換器 N9K-3 和 N9K-4 皆為 vPC 網域內的 vPC 對等，其中的 vPC 對等閘道增強功能已啟用。兩個 vPC 域通過背靠背的 vPC Po10 相互連線。所有四台交換機均具有在單播路由協定下啟用的 SVI 介面，並且位於同一個廣播域中。

由於 vPC 對等閘道增強功能可能會讓單點傳送路由通訊協定鄰接，無法在一個 vPC 網域和另一個 vPC 網域間形成，因此不支援透過啟用 vPC 對等閘道增強功能的連續 vPC 形成單點傳送路由通訊協定鄰接。在此拓撲中，在 N9K-1 和 N9K-3 或 N9K-4（或兩者）之間的路由協定鄰接關係可能無法正常運作。同樣地，N9K-2 和 N9K-3 或 N9K-4（或兩者）間的路由通訊協定鄰接可能無法如預期建立。這是因為單點傳送路由通訊協定封包可能會傳送至一個路由器（例如，N9K-3），但會根據起源路由器的第 2 層連接器通道雜湊決策，而轉送至其他路由器（例如，N9K-4）。

此問題的根本原因與[本文件之「使用 vPC 對等閘道透過 vPC 形成單點傳送路由通訊協定鄰接」的章節](#)所述的根本原因相同。您可透過 layer 3 peer-router vPC 網域組態命令啟用 Routing/Layer 3 over vPC 增強功能來解決此問題。如此可讓 TTL 為 1 的單點傳送路由通訊協定封包透過 vPC 對等連結轉送，不會使封包的 TTL 遞減。因此，單點傳送通訊協定鄰接可毫無問題地透過連續 vPC 形成。

使用 vPC 對等閘道透過 vPC 形成 OSPF 鄰接，其首碼存在於 OSPF LSDB 中，而非路由表中

考量以下所示的拓撲：



在此拓撲中，Nexus 交換器 N9K-1 和 N9K-2 皆為 vPC 網域內的 vPC 對等，其中的 vPC 對等閘道增強功能已啟用。Nexus 交換器 N9K-3 和 N9K-4 皆為 vPC 網域內的 vPC 對等，其中的 vPC 對等閘道增強功能已啟用。兩個 vPC 域通過背靠背的 vPC Po10 相互連線。所有四台交換機均具有在單播路由協定下啟用的 SVI 介面，並且位於同一個廣播域中。N9K-4 為廣播網域的 OSPF 指定路由器 (DR)，而 N9K-3 為廣播網域的 OSPF 備份指定路由器 (BDR)。

在此情況中，由於單點傳送 OSPF 封包輸出兩個交換器的 Ethernet1/1，因此 N9K-1 和 N9K-3 間的 OSPF 鄰接會轉換為 FULL 狀態。同樣地，由於單點傳送 OSPF 封包輸出兩個交換器的 Ethernet1/2，因此 N9K-2 和 N9K-3 間的 OSPF 鄰接會轉換為 FULL 狀態。

但是，由於單點傳送 OSPF 封包輸出兩個交換器的 Ethernet1/1，且遭 N9K-2 和 N9K-4 捨棄 (如本文件之「[使用 vPC 對等閘道透過連續 vPC 形成單點傳送路由通訊協定鄰接](#)」的章節所述)，因此 N9K-1 和 N9K-4 間的 OSPF 鄰接會停滯在 EXSTART 或 EXCHANGE 狀態。同樣地，由於單點傳送 OSPF 封包輸出兩個交換器的 Ethernet1/2，且遭 N9K-1 和 N9K-3 捨棄 (如本文件之「[使用 vPC 對等閘道透過連續 vPC 形成單點傳送路由通訊協定鄰接](#)」的章節所述)，因此 N9K-2 和 N9K-4 間的 OSPF 鄰接會停滯在 EXSTART 或 EXCHANGE 狀態。

因此，使用廣播網域之 BDR 的 N9K-1 和 N9K-2 會處於 FULL 狀態，但使用廣播網域的 DR 時會處於 EXSTART 或 EXCHANGE 狀態。廣播網域的 DR 和 BDR 會同時保留 OSPF 連結狀態資料庫 (LSDB) 的完整副本，但使用廣播網域之 DR 的 OSPF DROTHER 路由器必須處於 FULL 狀態，才可安裝透過 DR 或 BDR 的 OSPF 學習的首碼。因此，N9K-1 和 N9K-2 看起來都有從 OSPF LSDB 中存在的 N9K-3 和 N9K-4 獲知的字首，但是在 N9K-1 和 N9K-2 轉換為 N9K-4 的 FULL 狀態 (廣播域的 DR) 之前，這些字首不會安裝到單播路由表中。

您可透過 layer 3 peer-router vPC 網域組態命令啟用 Routing/Layer 3 over vPC 增強功能來解決此

問題。如此可讓 TTL 為 1 的單點傳送路由通訊協定封包透過 vPC 對等連結轉送，不會使封包的 TTL 遞減。因此，單點傳送通訊協定鄰接可毫無問題地透過連續 vPC 形成。因此，N9K-1和N9K-2使用N9K-4 (廣播域的DR) 轉換到FULL狀態，並將通過OSPF從N9K-3和N9K-4獲知的字首成功安裝到各自的單播路由表中。

相關資訊

- [Cisco Nexus 9000 系列 NX-OS 介面組態指南 \(10.3\(x\) 版 \)](#)
- [Cisco Nexus 9000 系列 NX-OS 介面組態指南 \(10.2\(x\) 版 \)](#)
- [Cisco Nexus 9000 系列 NX-OS 介面組態指南 \(10.1\(x\) 版 \)](#)
- [Cisco Nexus 9000 系列 NX-OS 介面組態指南 \(9.3\(x\) 版 \)](#)
- [Cisco Nexus 9000 系列 NX-OS 介面組態指南 \(9.2\(x\) 版 \)](#)
- [Cisco Nexus 9000 系列 NX-OS 介面組態指南 \(7.x 版 \)](#)
- [Cisco Nexus 7000 系列 NX-OS 介面組態指南 8.x](#)
- [Cisco Nexus 7000 系列 NX-OS 介面組態指南 7.x](#)
- [設計和配置指南：Cisco Nexus 7000系列交換機上的虛擬埠通道\(vPC\)最佳實踐](#)
- [在 Nexus 平台上透過虛擬連接埠通道進行路由時所支援的拓撲](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。