在Nexus 7000系列交換機上配置第2層vPC資料中心互聯

目錄

簡介

本文說明如何使用虛擬連線埠通道(vPC)設定第2層(L2)資料中心互連(DCI)。

必要條件

假設本文所提供的範例中使用的裝置已設定vPC和熱待命路由通訊協定(HSRP)。

> **附註**：應在充當DCI的vPC鏈路上使用鏈路聚合控制協定(LACP)。

> **提示：**MACSec加密在6.1(1)之前的版本中需要LAN高級服務許可證，並具有特定於線路卡的限制。請參閱**Cisco Nexus 7000系列NX-OS安全配置指南6.x**的Cisco TrustSec准則和限制部分瞭解更多資訊。

需求

思科建議您瞭解以下主題：

- vPC
- HSRP
- 生成樹通訊協定(STP)
- MACSec加密（可選）

採用元件

本檔案中的資訊是根據執行軟體版本6.2(8b)的Cisco Nexus 7000系列交換器。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

DCI的用途是擴展不同資料中心之間的特定VLAN，為相距較遠的伺服器和網路連線儲存(NAS)裝置提供L2鄰接關係。

vPC提供了兩個站點之間STP隔離的優勢(DCI vPC上沒有網橋協定資料單元(BPDU))，因此資料中心的任何中斷都不會傳播到遠端資料中心，因為資料中心之間仍提供冗餘鏈路。

> **附註**：vPC可用於最多互聯兩個資料中心。如果兩個以上的資料中心必須互連，思科建議您使用重疊傳輸虛擬化(OTV)。

DCI vPC EtherChannel通常配置時需考慮以下資訊：

- 第一躍點備援通訊協定(FHRP)隔離：使用針對每個資料中心的專用網關，防止出現次優路由。配置取決於FHRP網關的位置。
- STP隔離：如前所述，這可以防止故障從一個資料中心傳播到另一個資料中心。
- 廣播風暴控制：這是為了儘量減少資料中心之間的廣播流量。
- MACSec加密（可選）：這會加密流量，以防止兩個設施之間的入侵。

設定

使用本節中介紹的資訊，以便使用vPC配置L2 DCI。

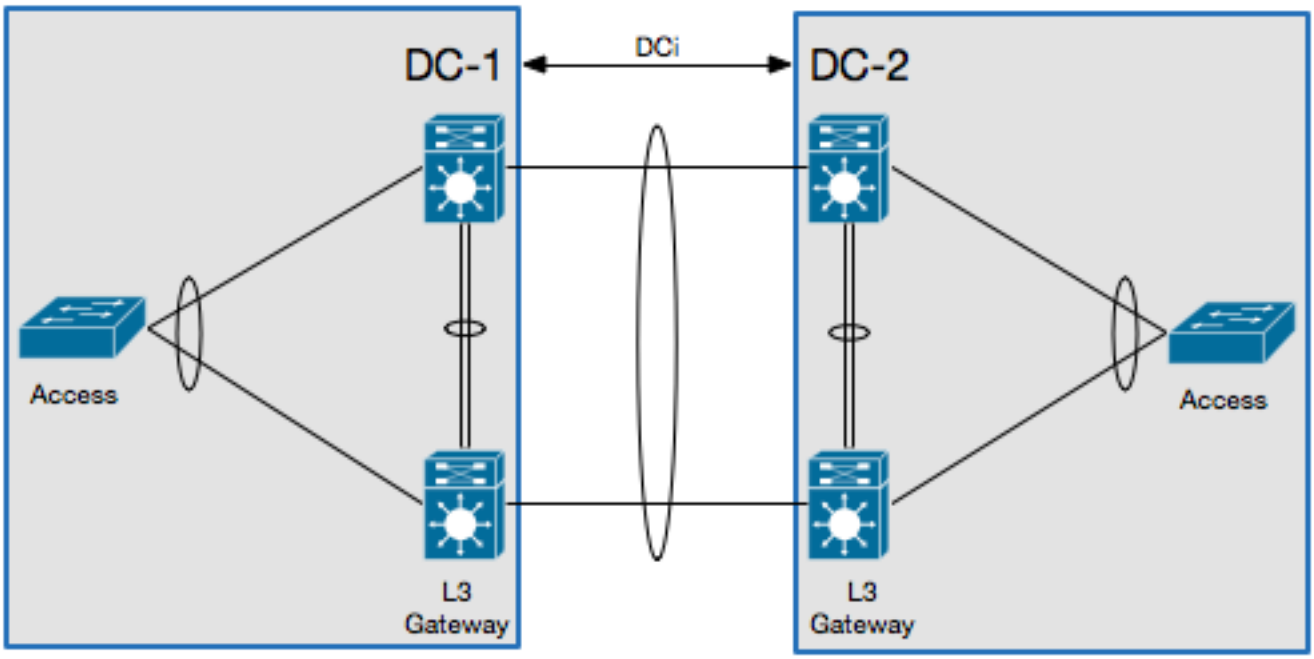
> **附註**：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

FHRP隔離

本節介紹兩種可以實施FHRP隔離的方案。

雙L2/L3 POD互連

以下是在此案例中使用的拓撲：



在此案例中，第3層(L3)閘道設定於同一vPC對上並充當DCI。為了隔離HSRP，您必須在DCI埠通道上配置埠訪問控制清單(PACL)，並為在DCI上移動的VLAN禁用交換虛擬介面(SVI)上的HSRP免費地址解析協定(ARP)(GARP)。

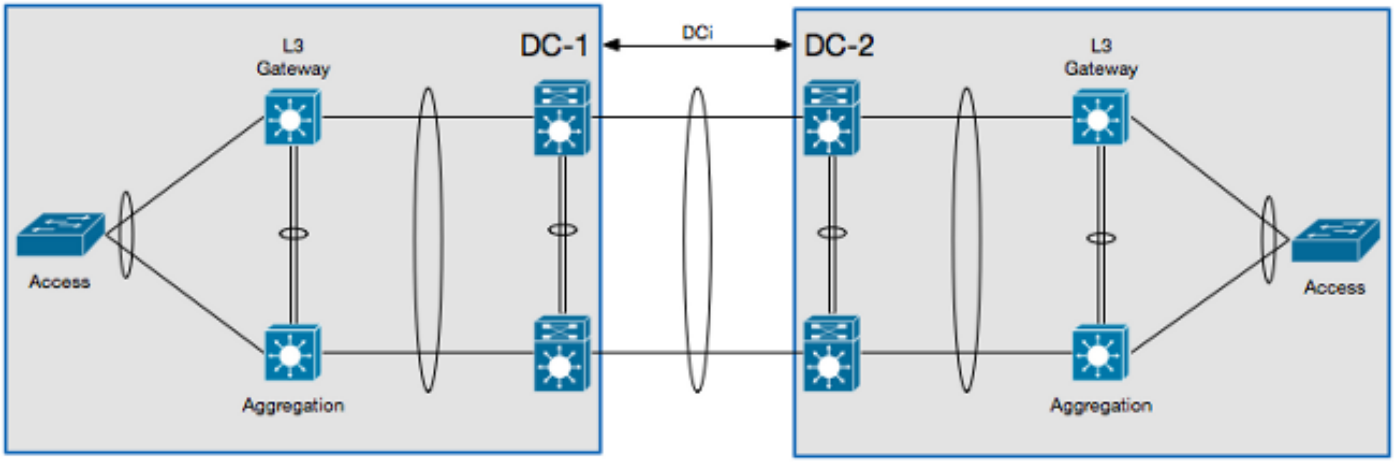
以下是組態範例：

```
ip access-list DENY_HSRP_IP
 10 deny udp any 224.0.0.2/32 eq 1985
 20 deny udp any 224.0.0.102/32 eq 1985
 30 permit ip any any

interface <DCI-Port-Channel>
 ip port access-group DENY_HSRP_IP in

interface Vlan <x>
 no ip arp gratuitous hsrp duplicate
```

附註：先前的配置也可以用於Nexus 9000交換機。

適用於彙總和DCI的多層vPC

以下是在此案例中使用的拓撲：



在此場景中，DCI隔離在它自己的第2層虛擬裝置環境(VDC)上，第3層網關位於匯聚層裝置上。為了隔離HSRP，您必須配置阻止HSRP控制流量的VLAN訪問控制清單(VACL)和阻止第2層DCI VDC上的HSRP GARP的ARP檢查過濾器。

以下是組態範例：

```
ip access-list ALL_IPs
 10 permit ip any any
mac access-list ALL_MACs
 10 permit any any
ip access-list HSRP_IP
 10 permit udp any 224.0.0.2/32 eq 1985
 20 permit udp any 224.0.0.102/32 eq 1985
mac access-list HSRP_VMAC
 10 permit 0000.0c07.ac00 0000.0000.00ff any
 20 permit 0000.0c9f.f000 0000.0000.0fff any
vlan access-map HSRP_Localization 10
       match ip address HSRP_IP
       match mac address HSRP_VMAC
       action drop
       statistics per-entry
vlan access-map HSRP_Localization 20
       match ip address ALL_IPs
       match mac address ALL_MACs
       action forward
       statistics per-entry
vlan filter HSRP_Localization vlan-list <DCI_Extended_VLANs>

feature dhcp

arp access-list HSRP_VMAC_ARP
 10 deny ip any mac 0000.0c07.ac00 ffff.ffff.ff00
 20 deny ip any mac 0000.0c9f.f000 ffff.ffff.f000
 30 permit ip any mac any

ip arp inspection filter HSRP_VMAC_ARP vlan <DCI_Extended_VLANs>
```

其他隔離配置

本節提供的示例配置如下：

- 僅允許擴展遠端資料中心所需的VLAN。

- 隔離每個資料中心的STP。

- 丟棄超過總鏈路速度1%的廣播流量。

以下是組態範例：

```
 interface <DCI-Port-Channel>
 switchport trunk allowed vlan <DCI_Extended_VLANs>
 spanning-tree port type edge trunk
 spanning-tree bpdufilter enable
storm-control broadcast level 1.0
```

附註：也可以配置組播流量的風暴控制，但其百分比必須與廣播流量相同。

MACSec加密

附註：本節所述的設定是選用的。

使用以下資訊配置MACSec加密：

```
feature dot1x
feature cts

! MACSec requires 24 additional bytes for encapsulation.
interface <DCI-Port-Channel>
 mtu 1524

interface <DCI-Physical-Port>
 cts manual
   no propagate-sgt
   sap pmk <Preshared-Key>
```

附註：必須交換介面才能進行MACSec授權。

驗證

使用本節所述的資訊以確認您的組態是否正常運作。

FHRP隔離

在CLI中輸入**show hsrp br** 命令，以驗證HSRP網關在兩個資料中心都處於活動狀態：

```
!DC-1
N7K-A# show hsrp br
*: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   120    Active   local           10.1.1.3        10.1.1.5
    (conf)

!DC-2
N7K-C# show hsrp br
*: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   120    Active   local           10.1.1.3        10.1.1.5
    (conf)
```

在CLI中輸入以下命令以驗證ARP過濾器：

```
N7K-D# show log log | i DUP_VADDR
2015 Apr 10 21:16:45 N7K-A %ARP-3-DUP_VADDR_SRC_IP:  arp [7915]  Source address of
packet received from 0000.0c9f.f00a on Vlan10(port-channel102) is duplicate of local
virtual ip, 10.1.1.5
```

如果出現類似這樣的輸出，則兩個活動網關之間的GARP沒有正確隔離。

其他隔離

在CLI中輸入**show spanning-tree root**命令，以驗證STP根目錄是否未指向DCI埠通道：

```
N7K-A# show spanning-tree root

                                        Root  Hello Max Fwd
Vlan                 Root ID             Cost  Time  Age Dly  Root Port
---------------- -------------------- ------- ----- --- ---  ----------------
VLAN0010          4106 0023.04ee.be01       0    2   20  15  This bridge is root
```

在CLI中輸入以下命令，以驗證是否已正確設定風暴控制：

```
N7K-A# show interface




--------------------------------------------------------------------------------
Port        UcastSupp %     McastSupp %     BcastSupp %     TotalSuppDiscards
--------------------------------------------------------------------------------
Po103            100.00          100.00            1.00                     0
```

MACSec加密

在CLI中輸入以下命令，以驗證MACSec加密是否已正確配置：

```
N7K-A# show cts interface
```

```
CTS Information for Interface Ethernet3/41:
...
   SAP Status:             CTS_SAP_SUCCESS
     Version: 1
     Configured pairwise ciphers: GCM_ENCRYPT
     Replay protection: Enabled
     Replay protection mode: Strict
     Selected cipher: GCM_ENCRYPT
     Current receive SPI: sci:e4c7220b98dc0000 an:0
     Current transmit SPI: sci:e4c7220b98d80000 an:0
...
```

疑難排解

目前，對於FHRP或其他隔離配置，沒有特定的故障排除資訊。

對於MACSec配置，如果鏈路的兩端未協商預共用金鑰，則當您在CLI中輸入**show interface <DCI-Physical-Port>**命令時，會顯示類似以下的輸出：

```
N7K-A# show interface



Ethernet3/41 is down (Authorization pending)
admin state is up, Dedicated Interface
```

> **附註**：連線兩端的金鑰必須相同。

注意事項

> **附註**：不包含相關產品的注意事項。

以下警告與在Cisco Nexus 7000系列交換機上使用DCI有關：

- 思科錯誤ID CSCur69114 - *HSRP PACL過濾器已損壞 — 資料包被泛洪到第2層域*。此錯誤僅在軟體版本6.2(10)中找到。
- 思科錯誤ID CSCut75457 - *HSRP VACL過濾器已損壞*。此錯誤僅在軟體版本6.2(10)和6.2(12)中找到。
- 思科錯誤ID CSCut43413 - *DCi:通過FHRP隔離包的HSRP虛擬MAC擺動*。此錯誤是由於硬體限制所致。

相關資訊

- **資料中心設計：資料中心互連**
- **OTV技術簡介和部署注意事項**

- 思科虛擬化工作負載移動性設計注意事項
- 技術支援與文件 - Cisco Systems