Nexus 7000 Series 스위치에서 레이어 2 vPC 데이터 센터 상호 연결 구성

목차

소개

이 문서에서는 vPC(Virtual Port-Channel)를 사용하여 레이어 2(L2) DCI(Data Center Interconnect)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

vPC 및 HSRP(Hot Standby Routing Protocol)가 이 문서에서 제공된 예제에 사용되는 디바이스에 이미 구성되어 있다고 가정합니다.

> **참고:**LACP(Link Aggregation Control Protocol)는 DCI의 역할을 하는 vPC 링크에서 사용해야 합니다.

> **팁**:MACSec 암호화에는 버전 6.1(1) 이전 버전의 LAN 고급 서비스 라이센스가 필요하며 라인 카드별 제한이 있습니다.자세한 내용은 **Cisco Nexus 7000 Series NX-OS 보안 컨피그레이션**

가이드, 릴리스 6.x의 Cisco TrustSec에 대한 지침 및 제한 사항 섹션을 참조하십시오.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- vPC
- HSRP
- STP(Spanning-Tree Protocol)
- MACSec 암호화(선택 사항)

사용되는 구성 요소

이 문서의 정보는 소프트웨어 버전 6.2(8b)를 실행하는 Cisco Nexus 7000 Series 스위치를 기반으로 합니다.

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

배경 정보

DCI의 목적은 서로 다른 데이터 센터 간에 특정 VLAN을 확장하는 것입니다. 이 VLAN은 대규모 거리로 구분된 서버와 NAS(Network-Attached Storage) 디바이스에 L2 인접성을 제공합니다.

vPC는 두 사이트(DCI vPC에서 BPDU(Bridge Protocol Data Unit) 없음) 간 STP 격리의 이점을 제공하므로 데이터 센터 간에 이중화 링크가 계속 제공되므로 데이터 센터의 모든 중단은 원격 데이터 센터로 전파되지 않습니다.

> **참고:**최대 2개의 데이터 센터를 상호 연결하기 위해 vPC를 사용할 수 있습니다.두 개 이상의 데이터 센터를 상호 연결해야 하는 경우 Cisco에서는 OTV(Overlay Transport Virtualization)를 사용하는 것이 좋습니다.

DCI vPC 이더넷 채널은 일반적으로 다음 정보를 염두에 두고 구성됩니다.

- FHRP(First Hop Redundancy Protocol) 격리:각 데이터 센터에 전용 게이트웨이를 사용하여 최적 상태가 아닌 라우팅을 방지합니다.구성은 FHRP 게이트웨이의 위치에 따라 달라집니다.
- STP 격리:앞서 언급했듯이, 이는 한 데이터 센터에서 다른 데이터 센터로 가동 중단이 전파되는 것을 방지합니다.
- 브로드캐스트 스톰 제어:이는 데이터 센터 간 브로드캐스트 트래픽의 양을 최소화하기 위해 사용됩니다.
- MACSec 암호화(선택 사항):이렇게 하면 두 시설 간의 침입을 방지하기 위해 트래픽을 암호화합니다.

구성

vPC를 사용하여 L2 DCI를 구성하려면 이 섹션에 설명된 정보를 사용합니다.

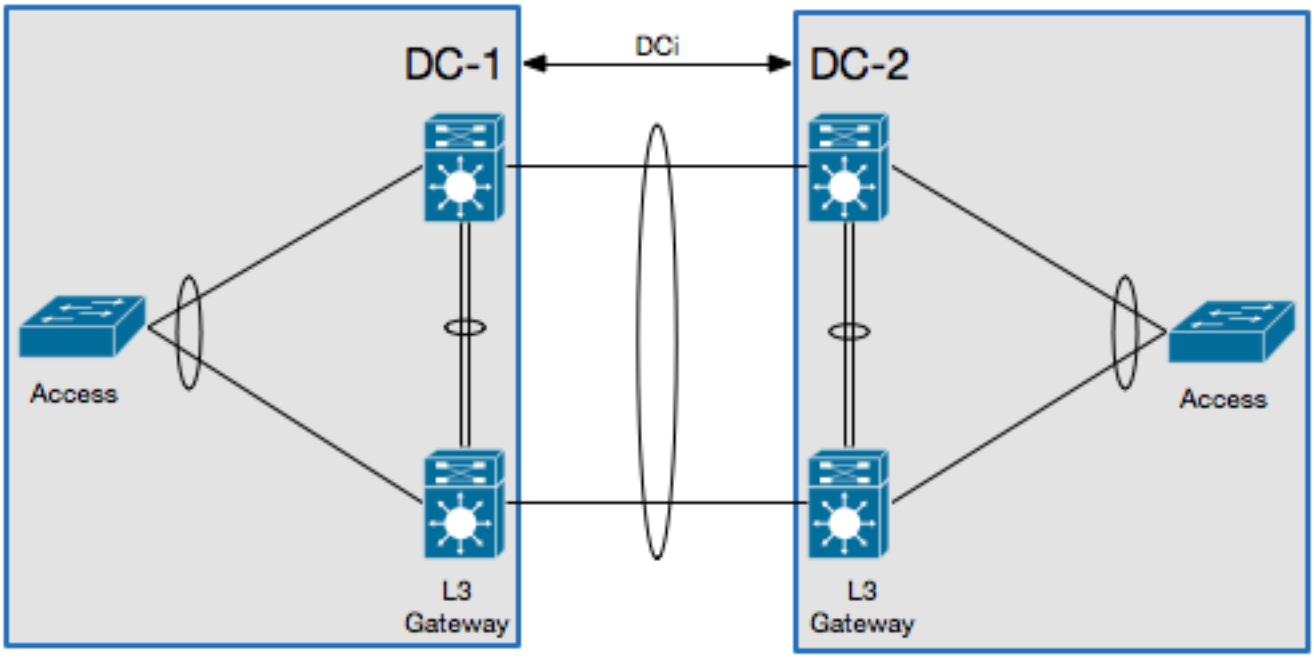
> **참고:**이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

FHRP 격리

이 섹션에서는 FHRP 격리를 구현할 수 있는 두 가지 시나리오에 대해 설명합니다.

듀얼 L2/L3 POD Interconnect

이 시나리오에서 사용되는 토폴로지입니다.



이 시나리오에서는 레이어 3(L3) 게이트웨이가 동일한 vPC 쌍에 구성되어 DCI의 역할을 합니다 .HSRP를 격리하려면 DCI 포트 채널에서 PACL(Port Access Control List)을 구성하고 DCI를 통해 이동하는 VLAN에 대해 SVI(Switched Virtual Interfaces)에서 HSRP ARP(Hardware Address Resolution Protocols)를 비활성화해야 합니다.

다음은 컨피그레이션의 예입니다.

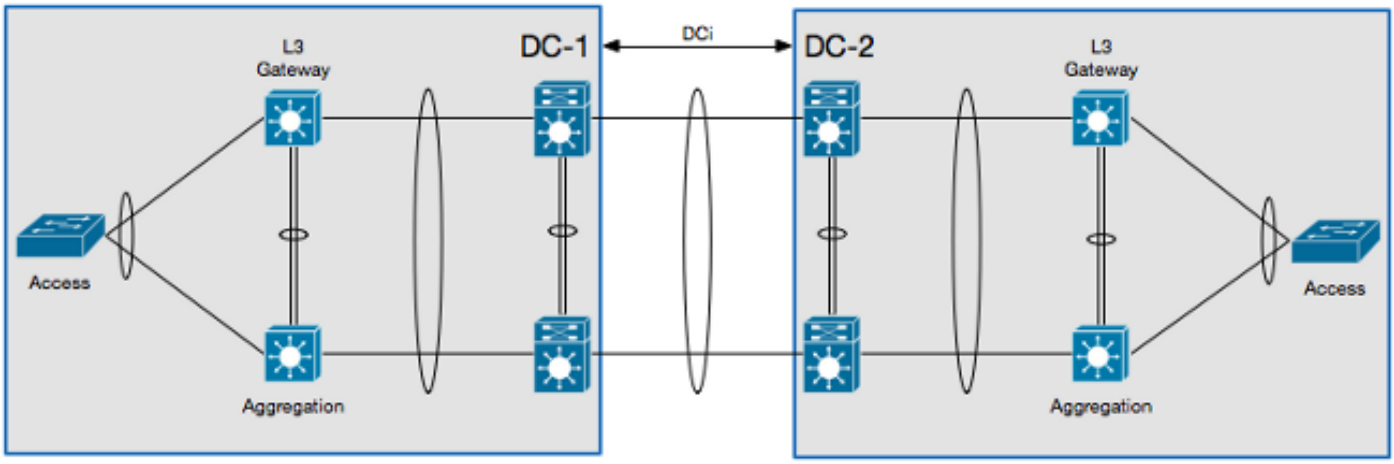
```
ip access-list DENY_HSRP_IP
 10 deny udp any 224.0.0.2/32 eq 1985
 20 deny udp any 224.0.0.102/32 eq 1985
 30 permit ip any any

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

interface Vlan <x>
```

```
 no ip arp gratuitous hsrp duplicate
```

참고:이전 컨피그레이션은 Nexus 9000 스위치에서도 사용할 수 있습니다.

어그리게이션 및 DCI를 위한 멀티레이어 vPC

이 시나리오에서 사용되는 토폴로지입니다.



이 시나리오에서는 DCI가 자체 L2 VDC(Virtual Device Context)에서 격리되고 L3 게이트웨이는 어그리게이션 레이어 디바이스에 있습니다.HSRP를 격리하려면 HSRP 제어 트래픽을 차단하는 VLAN VACL(Access Control List)과 L2 DCI VDC에서 HSRP GARP를 차단하는 ARP 검사 필터를 구성해야 합니다.

다음은 컨피그레이션의 예입니다.

```
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>
```

추가 격리 구성

이 섹션에서는 다음과 같은 구성 예를 제공합니다.

- 원격 데이터 센터에 필요한 VLAN만 확장할 수 있습니다.
- 각 데이터 센터에서 STP를 격리합니다.
- 총 링크 속도의 1%를 초과하는 브로드캐스트 트래픽을 삭제합니다.

다음은 컨피그레이션의 예입니다.

```
 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
```

참고:멀티캐스트 트래픽에 대한 스톰 제어를 구성할 수도 있지만 브로드캐스트 트래픽과 동일한 비율을 가져야 합니다.

MACSec 암호화

참고:이 섹션에서 설명하는 컨피그레이션은 선택 사항입니다.

MACSec 암호화를 구성하려면 다음 정보를 사용합니다.

```
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>
```

참고:MACSec 권한 부여를 수행하려면 인터페이스를 플랩해야 합니다.

다음을 확인합니다.

이 섹션에 설명된 정보를 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

FHRP 격리

CLI에 **show hsrp br** 명령을 입력하여 두 데이터 센터에서 HSRP 게이트웨이가 활성 상태인지 확인합니다.

```
!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)
```

ARP 필터를 확인하려면 CLI에 이 명령을 입력합니다.

```
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
```

이와 유사한 출력이 나타나면 두 활성 게이트웨이 간의 GARP가 제대로 격리되지 않습니다.

추가 격리

STP 루트가 DCI 포트 채널을 가리키지 않는지 확인하려면 CLI에 **show spanning-tree root** 명령을 입력합니다.

```
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
```

스톰 제어가 올바르게 구성되었는지 확인하려면 CLI에 이 명령을 입력합니다.

```
N7K-A# show interface



--------------------------------------------------------------------------------
Port        UcastSupp %     McastSupp %     BcastSupp %     TotalSuppDiscards
--------------------------------------------------------------------------------
```

```
Po103           100.00          100.00          1.00                    0
```

MACSec 암호화

MACSec 암호화가 올바르게 구성되었는지 확인하려면 CLI에 이 명령을 입력합니다.

```
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
...
```

문제 해결

현재 FHRP 또는 추가 격리 컨피그레이션에 사용할 수 있는 구체적인 문제 해결 정보가 없습니다.

MACSec 컨피그레이션의 경우 링크의 양쪽에서 사전 공유 키가 합의되지 않은 경우 CLI에 **show interface <DCI-Physical-Port>** 명령을 입력할 때 다음과 유사한 출력이 표시됩니다.

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

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

참고:키는 연결의 양쪽에서 동일해야 합니다.

주의 사항

참고:관련 제품에 대한 주의 사항은 포함되지 않습니다.

이러한 주의 사항은 Cisco Nexus 7000 Series 스위치에서 DCI를 사용하는 것과 관련이 있습니다.

- Cisco 버그 ID CSCur69114 - *HSRP PACL 필터 끊김 - 패킷이 layer2 도메인으로 플러딩됩니다* .이 버그는 소프트웨어 버전 6.2(10)에서만 찾을 수 있습니다.

- Cisco 버그 ID CSCut75457 - *HSRP VACL 필터가 손상되었습니다*.이 버그는 소프트웨어 버전 6.2(10) 및 6.2(12)에서만 찾을 수 있습니다.

- Cisco 버그 ID CSCut43413 - *DCi:FHRP 격리 PACL을 통한 HSRP 가상 MAC 플래핑*.이 버그는 하드웨어 제한 때문에 발생합니다.

관련 정보

- 데이터 센터 설계:데이터 센터 상호 연결
- OTV 기술 소개 및 구축 고려 사항
- Cisco Virtualized Workload Mobility 설계 고려 사항
- 기술 지원 및 문서 – Cisco Systems