Configuratie van een Layer 2 vPC Data Center Interconnect op een Nexus 7000 Series switch

Inhoud

Inleiding

Dit document beschrijft hoe u een Layer 2 (L2) Data Center Interconnect (DCI) kunt configureren met het gebruik van een Virtual Port-Channel (vPC).

Voorwaarden

Aangenomen wordt dat vPC en Hot Standby Routing Protocol (HSRP) al zijn ingesteld op de apparaten die worden gebruikt in de voorbeelden die in dit document worden genoemd.

> Opmerking: Link Aggregation Control Protocol (LACP) moet worden gebruikt op de vPC-link, die fungeert als DCI.

> **Tip**: MACSec-encryptie vereist een LAN geavanceerde serviceslicentie in versies voorafgaand aan versie 6.1(1) en heeft lijnspecifieke beperkingen. Raadpleeg de

Richtsnoeren en Beperkingen voor Cisco TrustSec-sectie van de **Cisco Nexus 7000 Series Security Configuration Guide, release 6.x** voor extra informatie.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- vPC
- HSRP
- Spanning-Tree Protocol (STP)
- MACSec-encryptie (optioneel)

Gebruikte componenten

De informatie in dit document is gebaseerd op een Cisco Nexus 7000 Series-switch met softwareversie 6.2(8b).

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

Achtergrondinformatie

Het doel van een DCI is om specifieke VLAN's tussen verschillende datacentra uit te breiden, wat L2-nabijheid biedt voor servers en NAS-apparaten (Network-Attached Storage) die door grote afstanden van elkaar worden gescheiden.

De vPC biedt het voordeel van STP-isolatie tussen de twee sites (geen Bridge Protocol Data Unit (BPDU) over de DCI vPC), zodat elke stroomstoring in een datacenter niet naar het externe datacenter wordt verspreid omdat er nog redundante koppelingen tussen de datacentra worden geleverd.

> Opmerking: De vPC kan worden gebruikt om maximaal twee datacenters onderling te verbinden. Als meer dan twee datacenters moeten worden onderling verbonden, raadt Cisco u aan om Overlay Transport Virtualization (OTV) te gebruiken.

Een DCI vPC Ethernet-kanaal wordt doorgaans geconfigureerd met deze informatie in gedachten:

- First Hopredundantie Protocol (FHRP)-isolatie: Voorkom suboptimale routing met behulp van een speciale gateway voor elk datacenter. De configuraties variëren afhankelijk van de locatie van de FHRP-gateway.

- STP-isolatie: Zoals eerder vermeld, voorkomt dit de verspreiding van stroomstoringen van het ene datacenter naar het andere.

- Controle van de uitzending: Dit wordt gebruikt om de hoeveelheid uitzendverkeer tussen de datacenters te minimaliseren.

- MACSec-encryptie (optioneel): Dit versleutel het verkeer om inbraak tussen de twee faciliteiten te voorkomen.

Configureren

Gebruik de informatie die in deze sectie wordt beschreven om een L2 DCI met het gebruik van een vPC te configureren.

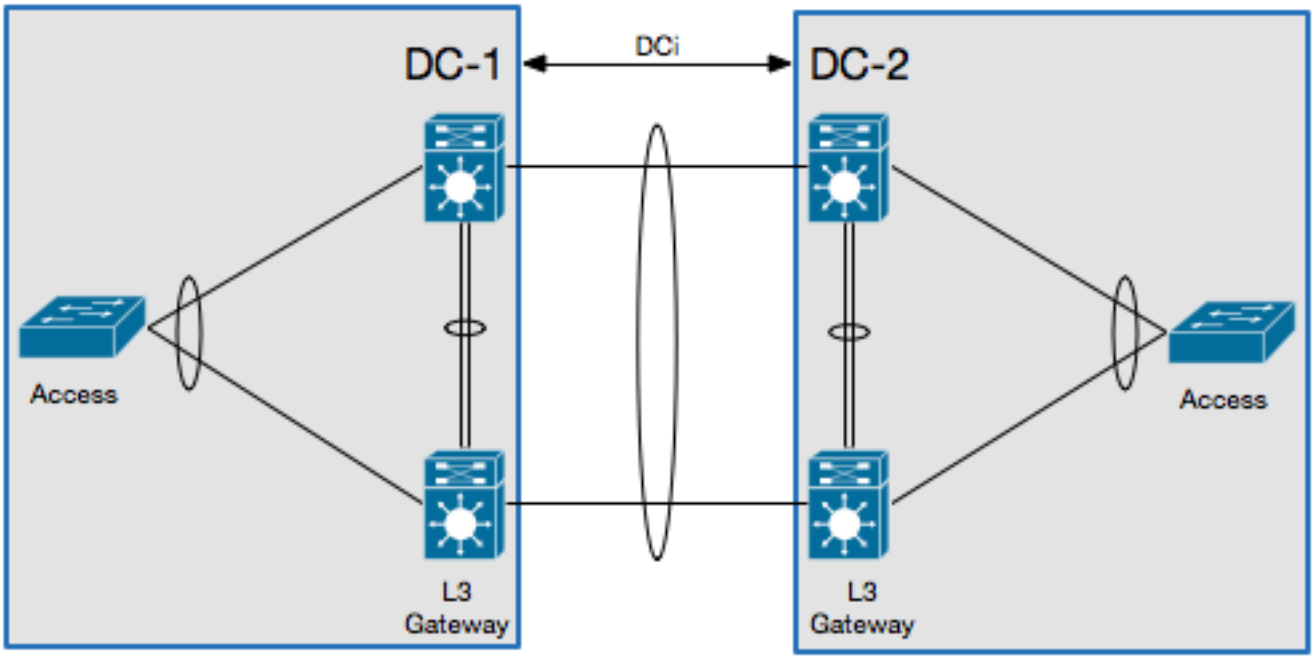
> Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

FHRP-isolatie

In dit deel worden twee scenario's beschreven waarvoor FHRP-isolatie kan worden uitgevoerd.

Dubbele L2/L3 POD-interconnect

Dit is de topologie die in dit scenario wordt gebruikt:



In dit scenario wordt de Layer 3 (L3) poort ingesteld op hetzelfde vPC-paar en werkt deze als de DCI. Om de HSRP te isoleren, moet u een Port Access Control List (PACL) configureren op het DCI-poortkanaal en HSRP gedeelde adresprotocollen (ARP's) uitschakelen op de Switched Virtual Interfaces (SVIs) voor VLAN's die zich over de DCI-indeling verplaatsen.

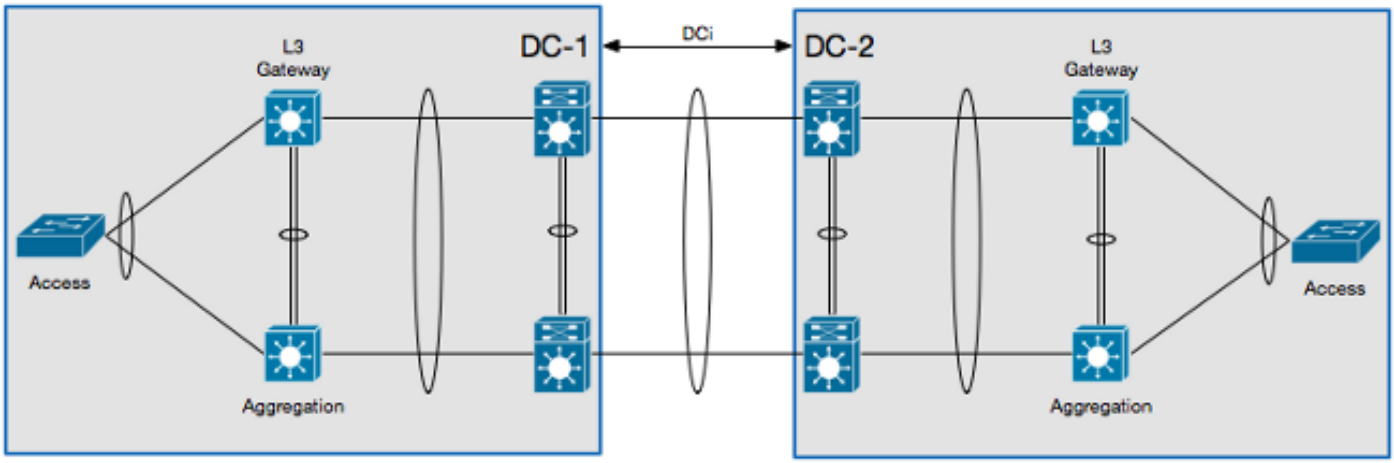
Hier is een voorbeeldconfiguratie:

```
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
```

Opmerking: De vorige configuratie kan ook worden gebruikt met Nexus 9000-switches.

Multilayer vPC voor aggregatie en DCI

Dit is de topologie die in dit scenario wordt gebruikt:



In dit scenario wordt de DCI geïsoleerd op zijn eigen L2 Virtual Devices Context (VDC), en de L3 poort bevindt zich op een aggregatielaag. Om de HSRP te isoleren, moet u een VLAN Access Control List (VACL) configureren die het HSRP-controleverkeer blokkeert en een ARP-inspectiefilter die de HSRP ARP's op de L2 DCI VDC blokkeert.

Hier is een voorbeeldconfiguratie:

```
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>
```

Aanvullende isolatieconfiguratie

Deze sectie verschaft een voorbeeldconfiguratie:

- Hiermee kunnen alleen VLAN's worden uitgebreid die in het externe datacenter nodig zijn.
- Isoleert de STP in elk datacenter.
- Droogt het uitzendverkeer dat 1% van de totale verbindingssnelheid overschrijdt.

Hier is de voorbeeldconfiguratie:

```
 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
```

> Opmerking: Storm control voor multicast verkeer kan ook worden geconfigureerd, maar het moet hetzelfde percentage hebben als het uitzendverkeer.

MACSec-encryptie

> Opmerking: De configuratie die in dit gedeelte wordt beschreven, is optioneel.

Gebruik deze informatie om MACSec-encryptie te configureren:

```
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>
```

> Opmerking: De interface moet worden ingevuld om een MACSec-vergunning te kunnen

verkrijgen.

Verifiëren

Gebruik de informatie die in dit gedeelte wordt beschreven om te bevestigen dat uw configuratie correct werkt.

FHRP-isolatie

Voer de opdracht **show hsrp br** in in de CLI om te verifiëren dat de HSRP poort actief is in beide datacenters:

```
!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)
```

Typ deze opdracht in de CLI om het ARP-filter te controleren:

```
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
```

Als een productie gelijkend op dit verschijnt dan worden de GARPs tussen de twee actieve gateways niet goed geïsoleerd.

Aanvullende isolatie

Voer de opdracht **in van de** show in**-boomwortel** in in de CLI om te verifiëren dat de STP-wortel niet naar het DCI-poortkanaal wijst:

```
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
```

Voer deze opdracht in de CLI om te controleren of de stormcontrole goed is ingesteld:

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

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

MACSec-encryptie

Voer deze opdracht in de CLI om te controleren of MACSec-encryptie correct is geconfigureerd:

```
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
...
```

Problemen oplossen

Er is momenteel geen specifieke informatie over probleemoplossing beschikbaar voor de FHRP of aanvullende isolatieconfiguraties.

Voor MACSec-configuratie, als de vooraf gedeelde toets niet op beide kanten van de link is overeengekomen, ziet u een uitvoer die hierop lijkt wanneer u de opdracht **Show interface <DCI-Physical-Port>** in de CLI invoert:

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

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

> Opmerking: De sleutel moet aan beide zijden van de verbinding hetzelfde zijn.

Caveats

> Opmerking: Voorzorgsmaatregelen voor de verwante producten zijn niet opgenomen.

Deze voorbehouden zijn gerelateerd aan het gebruik van een DCI op de Cisco Nexus 7000 Series-switch:

- Cisco bug-ID CSCur69114 - *Broken van HSRP PACL-filter - Packets worden overstroomd naar Layer 2-domein*. Deze bug zit alleen in softwareversie 6.2(10).
- Cisco bug-ID CSCut75457 - *Verbroken HSRP VACL-filter*. Deze bug zit alleen in softwareversies 6.2(10) en 6.2(12).
- Cisco bug-ID CSCut43413 - *DCi: HSRP virtuele MAC-filtering door middel van FHRP isolatie PACL*. Dit bug is het gevolg van een hardwarebeperking.

Gerelateerde informatie

- Ontwerpen van datacenters: Data Center Interconnect
- Overzichten voor OTV-technologie-introductie en -implementatie
- Cisco gevirtualiseerde overwegingen voor werklastmobiliteit
- Technische ondersteuning en documentatie – Cisco Systems