Een Layer 2 vPC Data Center Interconnect configureren op een Switch uit de Nexus 7000-reeks

Inhoud

Inleiding

In dit document wordt beschreven hoe u een Layer 2 (L2) Data Center Interconnect (DCI) configureert met behulp van een Virtual Port-Channel (vPC).

Voorwaarden

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

Gebruik het Link Aggregation Control Protocol (LACP) op de vPC-koppeling, die fungeert als het DCI.

Tip: voor MACSec-codering is een LAN Advanced Services-licentie vereist in versies vóór versie 6.1(1) en deze heeft beperkingen die specifiek zijn voor de linecard. Raadpleeg de sectie Richtlijnen en beperkingen voor Cisco TrustSec van de Cisco Nexus 7000 Series NX-OS Security Configuration Guide, versie 6.x voor meer informatie.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op een switch uit de Cisco Nexus 7000-reeks waarop softwareversie 6.2(8b) wordt uitgevoerd.

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 uit te breiden tussen verschillende datacenters, wat L2-aangrenzing biedt voor servers en Network-Attached Storage (NAS)-apparaten die van elkaar worden gescheiden door grote afstanden.

De vPC biedt het voordeel van STP-isolatie tussen de twee locaties (geen Bridge Protocol Data Unit (BPDU) over de DCI vPC), zodat elke storing in een datacenter niet wordt doorgegeven aan het externe datacenter omdat er nog steeds redundante koppelingen tussen de datacenters worden aangeboden.

Gebruik de vPC om maximaal twee datacenters met elkaar te verbinden. Als er meer dan twee datacenters met elkaar verbonden moeten zijn, gebruikt u OTV (Overlay Transport Virtualization).

Een DCI vPC-etherkanaal wordt doorgaans geconfigureerd met deze informatie in het achterhoofd:

- Isolatie van het First Hop Redundancy Protocol (FHRP): voorkom suboptimale routering met behulp van een speciale gateway voor elk datacenter. Configuraties variëren afhankelijk van de locatie van de FHRP-gateway.
- STP-isolatie: Zoals eerder vermeld, voorkomt dit de verspreiding van uitval van het ene datacenter naar het andere.
- Broadcast storm control: Dit wordt gebruikt om de hoeveelheid uitzendverkeer tussen de datacenters te minimaliseren.
- MACSec-codering (optioneel): hiermee wordt het verkeer gecodeerd om inbraak tussen de twee faciliteiten te voorkomen.

Configureren

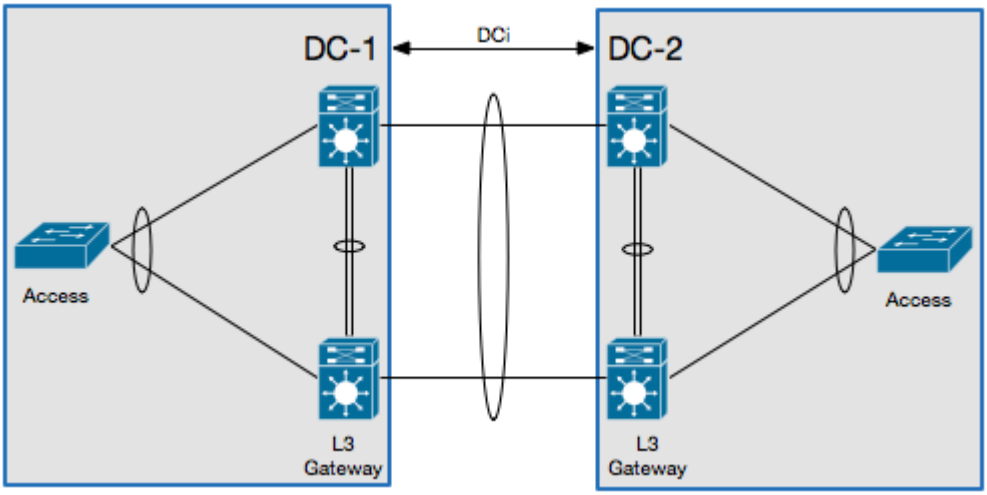
Gebruik de in deze sectie beschreven informatie om een L2 DCI te configureren met behulp van een vPC. Geregistreerde klanten kunnen de Opdrachtopzoektool gebruiken om meer informatie te verkrijgen over de hier gebruikte opdrachten.

FHRP-isolatie

In dit gedeelte worden twee scenario's beschreven waarvoor FHRP-isolatie kan worden geïmplementeerd.

Dubbele L2/L3 POD-verbinding

Dit is de topologie die in dit scenario wordt gebruikt:



In dit scenario is de Layer 3 (L3)-gateway geconfigureerd op hetzelfde vPC-paar en fungeert deze als de DCI. Als u de HSRP wilt isoleren, moet u een Poorttoegangscontrolelijst (PACL) configureren op het DCI-poortkanaal en HSRP Gratuitous Address Resolution Protocols (ARP's) (GARP's) uitschakelen op de switched virtual interfaces (SVI's) voor de VLAN's die zich over de DCI verplaatsen.

Hier is een voorbeeld configuratie:

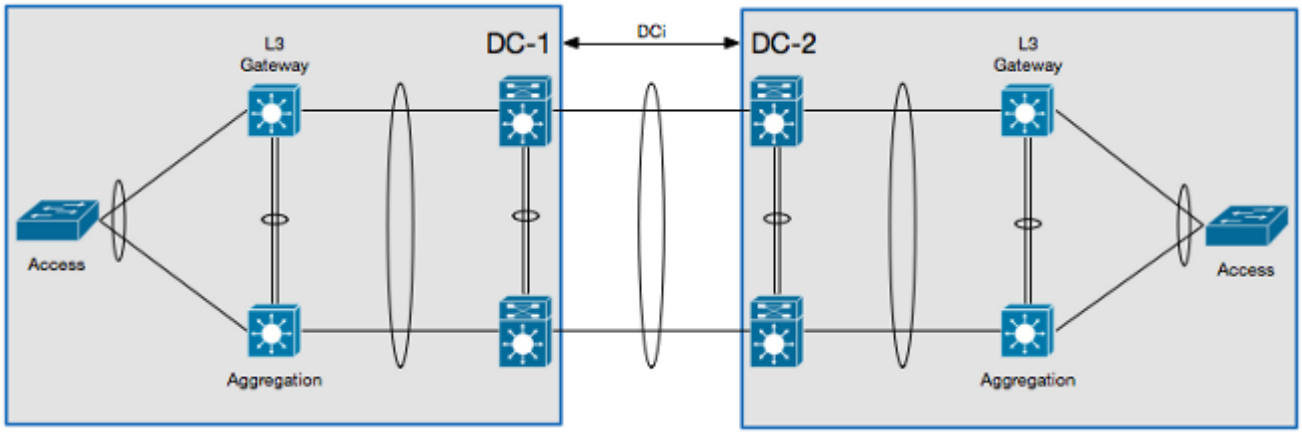
```
ip access-list DENY_HSRP_IP
  10 deny udp any 224.0.0.2/32 eq 1985
  20 deny udp any 224.0.0.102/32 eq 1985
  30 permit ip any any

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

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

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 Device Context (VDC) en de L3-gateway bevindt zich op een aggregatielaagapparaat. Als u de HSRP wilt isoleren, configureert u een VLAN-toegangscontrolelijst (VACL) die het HSRP-controleverkeer blokkeert en een ARP-inspectiefilter dat de HSRP-GARP's op de L2 DCI VDC blokkeert. 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>
```

Extra isolatieconfiguratie

Dit gedeelte bevat een voorbeeldconfiguratie die:

- Hiermee kunnen alleen de VLAN's die nodig zijn in het externe datacenter worden uitgebreid
- Isoleert de STP in elk datacenter
- Hiermee daalt het uitzendverkeer dat meer dan 1% van de totale verbindingssnelheid bedraagt

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
```

Stormbesturing voor multicast-verkeer kan ook worden geconfigureerd, maar het moet hetzelfde percentage hebben als het uitzendverkeer.

MACSec-codering

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

Gebruik deze informatie om MACSec-codering 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>
```

Klap op de interface voor de MACSec-autorisatie.

Verifiëren

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

FHRP-isolatie

Voer de opdracht show hsrp br in de CLI in om te controleren of de HSRP-gateway actief is in beide datacenters:

<#root>

```
!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)
```

Voer deze opdracht in de CLI in om het ARP-filter te verifiëren:

<#root>

```
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 soortgelijke uitgang verschijnt, dan zijn de GARP's tussen de twee actieve gateways niet goed geïsoleerd.

extra isolatie

Voer de opdracht omspanningsboomhoofdmap weergeven in de CLI in om te controleren of de STP-hoofdmap niet naar het DCI-poortkanaal wijst:

<#root>

```
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 in om te controleren of stormbesturing correct is geconfigureerd:

<#root>

```
N7K-A#
```

show interface <DCI-Port-Channel> counters storm-control

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

MACSec-codering

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

```
<#root>

N7K-A#

show cts interface <DCI-Physical-Port>


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 beschikbaar voor het oplossen van problemen met de FHRP of aanvullende isolatieconfiguraties.

Als voor de MACSec-configuratie de vooraf gedeelde sleutel niet is overeengekomen aan beide zijden van de koppeling, ziet u een uitvoer die vergelijkbaar is met deze wanneer u de show-interface <DCI-Physical-Port>-opdracht invoert in de CLI:

```
<#root>

N7K-A#

show interface <DCI-Physical-Port>


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

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

Voorbehouden

Deze waarschuwingen zijn gerelateerd aan het gebruik van een DCI op de Cisco Nexus 7000 Series-switch. Waarschuwingen voor gerelateerde producten zijn niet inbegrepen.

- Cisco bug ID CSCur69114 - HSRP PACL Filter Broken - Pakketten worden overspoeld naar layer2-domein. Deze bug is alleen te vinden in software versie 6.2(10).
- Cisco bug ID CSCut75457 – HSRP VACL-filter kapot. Deze bug is alleen te vinden in softwareversies 6.2(10) en 6.2(12).
- Cisco bug ID CSCut43413 – DCi: HSRP Virtual MAC Flapping through FHRP Isolation PACL. Deze bug is te wijten aan een hardwarebeperking.

Gerelateerde informatie

- Cisco Solutions
- Overwegingen bij introductie en implementatie van OTV-technologie
- Cisco Gevirtualiseerde werkbelasting Mobiliteitsontwerp Overwegingen
- Technische ondersteuning en documentatie

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.