Konfigurieren eines Layer-2-vPC-Rechenzentrums-Interconnects auf einem Switch der Serie Nexus 7000

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie eine Layer 2 (L2) Data Center Interconnect (DCI) mit einem Virtual Port Channel (vPC) konfiguriert wird.

Voraussetzungen

Es wird davon ausgegangen, dass vPC und Hot Standby Routing Protocol (HSRP) bereits auf den Geräten konfiguriert sind, die in den in diesem Dokument beschriebenen Beispielen verwendet werden.

> **Hinweis**: Link Aggregation Control Protocol (LACP) sollte für die vPC-Verbindung verwendet werden, die als DCI fungiert.

Tipp: Für die MACSec-Verschlüsselung ist eine LAN Advanced Services-Lizenz in Versionen vor Version 6.1(1) erforderlich, und es gelten Line Card-spezifische Einschränkungen. Weitere Informationen finden Sie im Abschnitt Richtlinien und Einschränkungen für Cisco TrustSec im **Nexus NX-OS Security Configuration Guide der Cisco Nexus 7000-Serie, Version 6.x**.

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- vPC
- HSRP
- Spanning Tree Protocol (STP)
- MACSec-Verschlüsselung (optional)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einem Cisco Nexus Switch der Serie 7000, auf dem die Software Version 6.2(8b) ausgeführt wird.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Der Zweck eines DCI besteht in der Erweiterung spezieller VLANs zwischen verschiedenen Rechenzentren, die L2-Adjacency für Server und Network-Attached Storage (NAS)-Geräte bieten, die durch große Entfernungen voneinander getrennt sind.

Der vPC bietet den Vorteil der STP-Isolierung zwischen den beiden Standorten (keine Bridge Protocol Data Unit (BPDU) über den DCI vPC), sodass Ausfälle in einem Rechenzentrum nicht an das Remote-Rechenzentrum weitergeleitet werden, da zwischen den Rechenzentren noch redundante Verbindungen bereitgestellt werden.

Hinweis: Der vPC kann verwendet werden, um maximal zwei Rechenzentren miteinander zu verbinden. Wenn mehr als zwei Rechenzentren miteinander verbunden werden müssen, empfiehlt Cisco die Verwendung von Overlay Transport Virtualization (OTV).

Ein DCI-vPC-EtherChannel wird in der Regel mit folgenden Informationen konfiguriert:

- First Hop Redundancy Protocol (FHRP)-Isolierung: Vermeiden Sie suboptimales Routing durch die Verwendung eines dedizierten Gateways für jedes Rechenzentrum. Die Konfigurationen variieren je nach Standort des FHRP-Gateways.

- STP-Isolierung: Wie bereits erwähnt verhindert dies die Ausbreitung von Ausfällen von einem

Rechenzentrum in ein anderes.

- Broadcast-Sturmkontrolle: Diese Funktion dient dazu, die Menge an Broadcast-Datenverkehr zwischen den Rechenzentren zu minimieren.
- MACSec-Verschlüsselung (optional): Dadurch wird der Datenverkehr verschlüsselt, um ein Eindringen zwischen den beiden Einrichtungen zu verhindern.

Konfigurieren

Verwenden Sie die in diesem Abschnitt beschriebenen Informationen, um ein L2-DCI mit der Verwendung eines vPC zu konfigurieren.

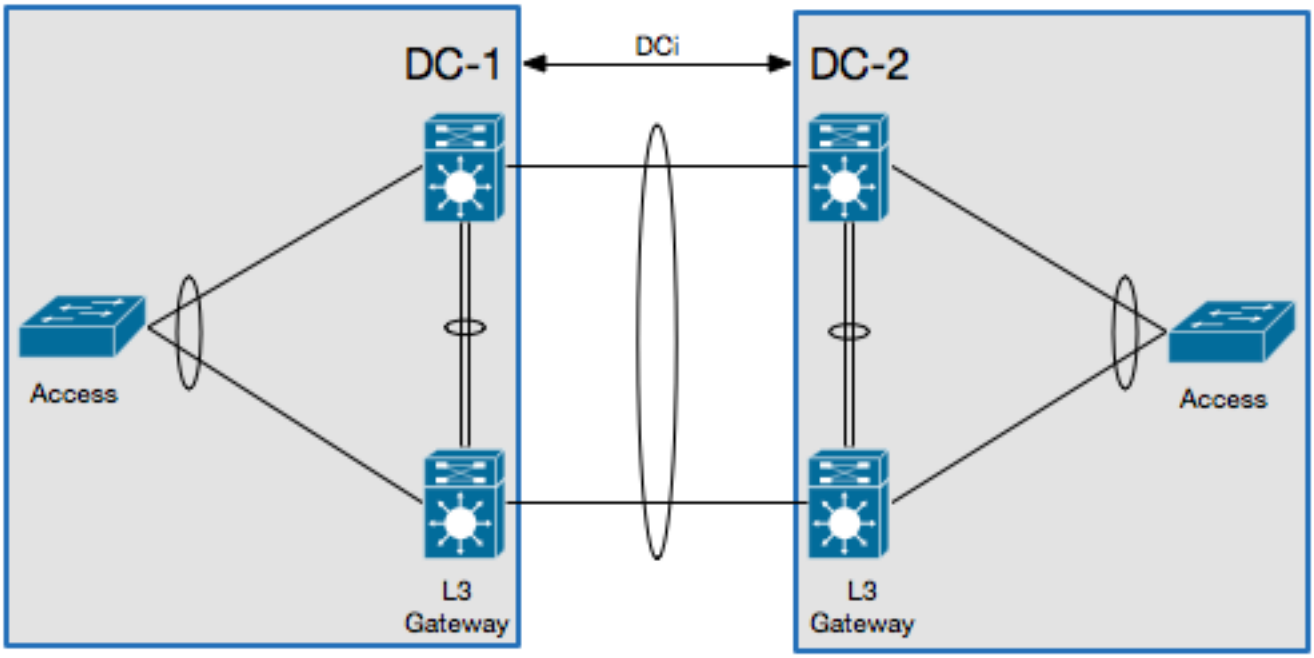
> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

FHRP-Isolierung

In diesem Abschnitt werden zwei Szenarien beschrieben, für die die FHRP-Isolierung implementiert werden kann.

Dual-L2/L3-POD-Interconnect

Dies ist die Topologie, die in diesem Szenario verwendet wird:



In diesem Szenario wird das Layer 3 (L3)-Gateway auf demselben vPC-Paar konfiguriert und fungiert als DCI. Um das HSRP zu isolieren, müssen Sie eine Port Access Control List (PACL) für den DCI-Port-Channel konfigurieren und HSRP Gratuitous Address Resolution Protocols (ARPs) (GARPs) auf den Switched Virtual Interfaces (SVIs) für die VLANs deaktivieren, die sich über das

DCI bewegen.

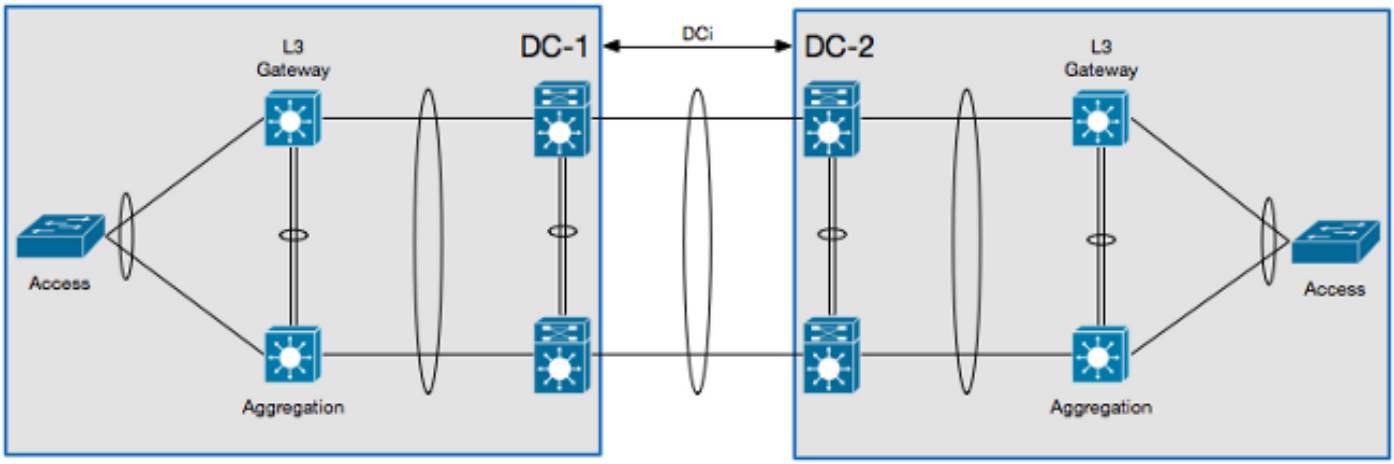
Hier ein Beispiel für eine Konfiguration:

```
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
```

> **Hinweis**: Die vorherige Konfiguration kann auch mit Nexus 9000-Switches verwendet werden.

Multilayer-vPC für Aggregation und DCI

Dies ist die Topologie, die in diesem Szenario verwendet wird:



In diesem Szenario ist das DCI auf seinem eigenen L2 Virtual Device Context (VDC) isoliert, und das L3-Gateway befindet sich auf einem Aggregation Layer-Gerät. Um das HSRP zu isolieren, müssen Sie eine VLAN Access Control List (VACL) konfigurieren, die den HSRP-Steuerungsdatenverkehr blockiert, und einen ARP-Inspektionsfilter, der die HSRP GARPs im L2 DCI-VDC blockiert.

Hier ein Beispiel für eine Konfiguration:

```
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>
```

Zusätzliche Isolationskonfiguration

Dieser Abschnitt enthält eine Beispielkonfiguration mit folgenden Merkmalen:

- Ermöglicht nur die Erweiterung der VLANs, die im Remote-Rechenzentrum benötigt werden.
- Isoliert das STP in jedem Rechenzentrum.
- Löscht den Broadcast-Datenverkehr, der mehr als 1 % der gesamten Verbindungsgeschwindigkeit beträgt.

Die Beispielkonfiguration ist wie folgt:

```
 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
```

> **Hinweis**: Die Sturmkontrolle für Multicast-Datenverkehr kann ebenfalls konfiguriert werden, muss jedoch denselben Prozentsatz wie der Broadcast-Datenverkehr aufweisen.

MACSec-Verschlüsselung

> **Hinweis**: Die in diesem Abschnitt beschriebene Konfiguration ist optional.

Verwenden Sie diese Informationen, um die MACSec-Verschlüsselung zu konfigurieren:

```
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>
```

Hinweis: Die Schnittstelle muss markiert werden, damit die MACSec-Autorisierung erfolgt.

Überprüfen

Verwenden Sie die in diesem Abschnitt beschriebenen Informationen, um sicherzustellen, dass Ihre Konfiguration ordnungsgemäß funktioniert.

FHRP-Isolierung

Geben Sie den Befehl **show hsrp br** in die CLI ein, um zu überprüfen, ob das HSRP-Gateway in beiden Rechenzentren aktiv ist:

```
!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)
```

Geben Sie diesen Befehl in die CLI ein, um den ARP-Filter zu überprüfen:

```
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
```

Wenn eine ähnliche Ausgabe angezeigt wird, sind die GARPs zwischen den beiden aktiven Gateways nicht ausreichend isoliert.

Zusätzliche Isolierung

Geben Sie den Befehl **show spanning-tree root** in die CLI ein, um zu überprüfen, ob der STP-Root nicht auf den DCI-Port-Channel zeigt:

```
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
```

Geben Sie diesen Befehl in die CLI ein, um zu überprüfen, ob die Sturmkontrolle ordnungsgemäß konfiguriert ist:

```
N7K-A# show interface




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

MACSec-Verschlüsselung

Geben Sie diesen Befehl in die CLI ein, um zu überprüfen, ob die MACSec-Verschlüsselung ordnungsgemäß konfiguriert ist:

```
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
...
```

Fehlerbehebung

Derzeit sind keine spezifischen Informationen zur Fehlerbehebung für das FHRP oder zusätzliche Isolationskonfigurationen verfügbar.

Wenn für die MACSec-Konfiguration auf beiden Seiten der Verbindung kein Pre-Shared Key vereinbart wurde, wird eine ähnliche Ausgabe angezeigt, wenn Sie den Befehl **show interface <DCI-Physical-Port>** in die CLI eingeben:

```
N7K-A# show interface


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

Hinweis: Der Schlüssel muss auf beiden Seiten der Verbindung identisch sein.

Einsprüche

Hinweis: Hinweise zu den verwandten Produkten sind nicht enthalten.

Diese Vorbehalte beziehen sich auf die Verwendung eines DCI auf dem Cisco Nexus Switch der Serie 7000:

- Cisco Bug ID CSCur69114 - *HSRP PACL Filter Broken - Pakete werden in Layer 2-Domäne geflutet*. Dieser Fehler wurde nur in der Softwareversion 6.2(10) gefunden.
- Cisco Bug ID CSCut75457 - *HSRP VACL Filter Broken*. Dieser Fehler wird nur in Softwareversionen 6.2(10) und 6.2(12) gefunden.
- Cisco Bug-ID CSCut43413 - *DCi: HSRP Virtual MAC Flapping durch FHRP Isolation PACL*. Dieser Fehler ist auf eine Hardware-Einschränkung zurückzuführen.

Zugehörige Informationen

- Rechenzentrums-Designs: Data Center Interconnect
- Überlegungen zur Einführung und Bereitstellung der OTV-Technologie
- Designüberlegungen für Cisco Virtualized Workload Mobility
- Technischer Support und Dokumentation - Cisco Systems