Configurazione di un layer 2 vPC Data Center Interconnect su uno switch Nexus serie 7000

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Configurazione](#)
[Isolamento FHRP](#)
[Doppia interconnessione POD L2/L3](#)
[Multilayer vPC for Aggregation e DCI](#)
[Configurazione aggiuntiva isolamento](#)
[Crittografia MACSec](#)
[Verifica](#)
[Isolamento FHRP](#)
[Isolamento aggiuntivo](#)
[Crittografia MACSec](#)
[Risoluzione dei problemi](#)
[Avvertenze](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare un DCI (Data Center Interconnect) di layer 2 (L2) con l'utilizzo di un vPC (Virtual Port-Channel).

Prerequisiti

Si presume che vPC e Hot Standby Routing Protocol (HSRP) siano già configurati sui dispositivi utilizzati negli esempi riportati in questo documento.

> **Nota:** È consigliabile utilizzare il protocollo LACP (Link Aggregation Control Protocol) sul collegamento vPC, che funge da DCI.

> **Suggerimento**: La crittografia MACSec richiede una licenza LAN Advanced Services nelle versioni precedenti alla 6.1(1) e prevede limitazioni specifiche per la scheda di linea. Per

ulteriori informazioni, consultare la sezione Linee guida e limitazioni per Cisco TrustSec della **guida alla configurazione della sicurezza di Cisco Nexus serie 7000 NX-OS, versione 6.x**.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- vPC
- HSRP
- STP (Spanning-Tree Protocol)
- Crittografia MACSec (opzionale)

Componenti usati

Per la stesura del documento, è stato usato uno switch Cisco Nexus serie 7000 con software versione 6.2(8b).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Lo scopo di un DCI è estendere VLAN specifiche tra centri dati diversi, offrendo l'adiacenza L2 per server e dispositivi NAS (Network-Attached Storage) separati da grandi distanze.

Il vPC presenta il vantaggio dell'isolamento STP tra i due siti (senza BPDU (Bridge Protocol Data Unit) attraverso il vPC DCI), quindi qualsiasi interruzione in un centro dati non viene propagata al centro dati remoto poiché sono ancora forniti collegamenti ridondanti tra i centri dati.

> **Nota:** Il vPC può essere utilizzato per interconnettere un massimo di due centri dati. Se è necessario interconnettere più di due centri dati, Cisco consiglia di utilizzare Overlay Transport Virtualization (OTV).

Un etherchannel vPC DCI è in genere configurato tenendo presenti queste informazioni:

- Isolamento First Hop Redundancy Protocol (FHRP): Evitare il routing non ottimale utilizzando un gateway dedicato per ogni centro dati. Le configurazioni variano a seconda della posizione del gateway FHRP.

- Isolamento STP: Come accennato in precedenza, ciò impedisce la propagazione delle interruzioni da un data center all'altro.

- Controllo broadcast storm: Questa opzione viene utilizzata per ridurre al minimo la quantità di traffico broadcast tra i centri dati.

- Crittografia MACSec (facoltativa): In questo modo il traffico viene criptato per evitare intrusioni tra le due strutture.

Configurazione

Utilizzare le informazioni descritte in questa sezione per configurare un DCI L2 con l'utilizzo di un vPC.

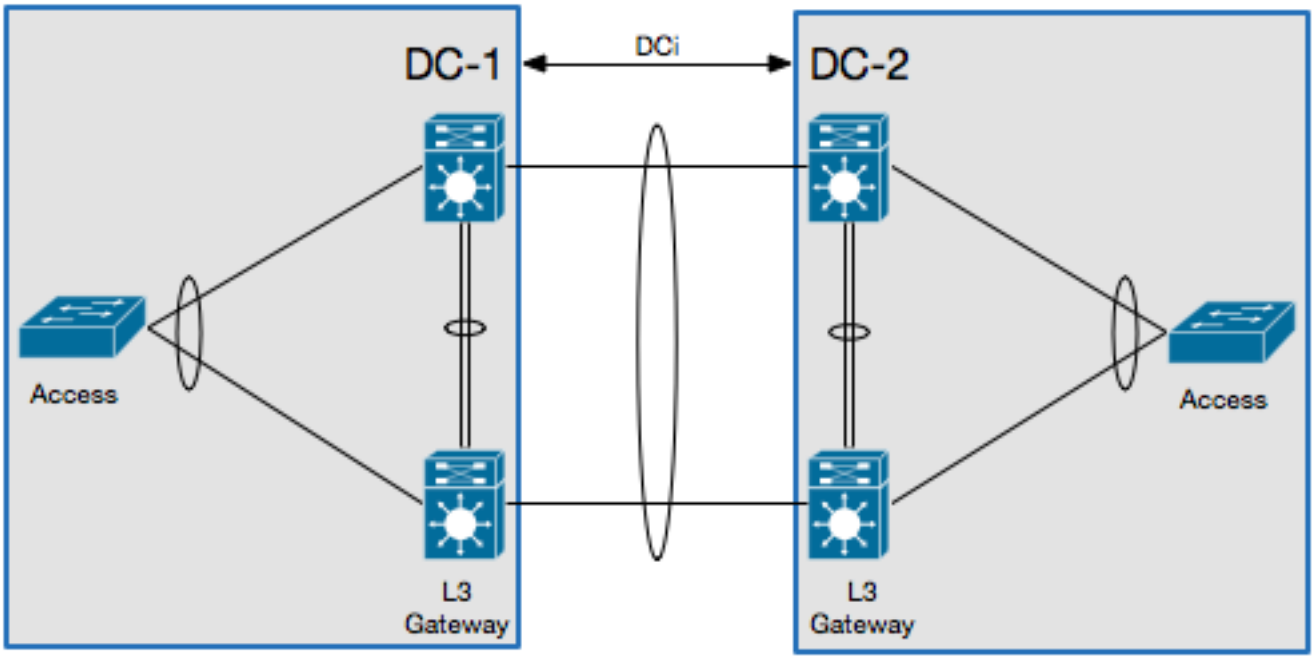
> **Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Isolamento FHRP

In questa sezione vengono descritti due scenari per i quali è possibile implementare l'isolamento FHRP.

Doppia interconnessione POD L2/L3

Questa è la topologia utilizzata in questo scenario:



In questo scenario, il gateway di layer 3 (L3) è configurato sulla stessa coppia vPC e funge da DCI. Per isolare l'HSRP, è necessario configurare un elenco di controllo di accesso (PACL) delle porte sul canale DCI e disabilitare i protocolli ARP (Gratuitous Address Resolution Protocol) (GARP) dell'HSRP sulle interfacce virtuali commutate (SVI) per le VLAN che si spostano attraverso il DCI.

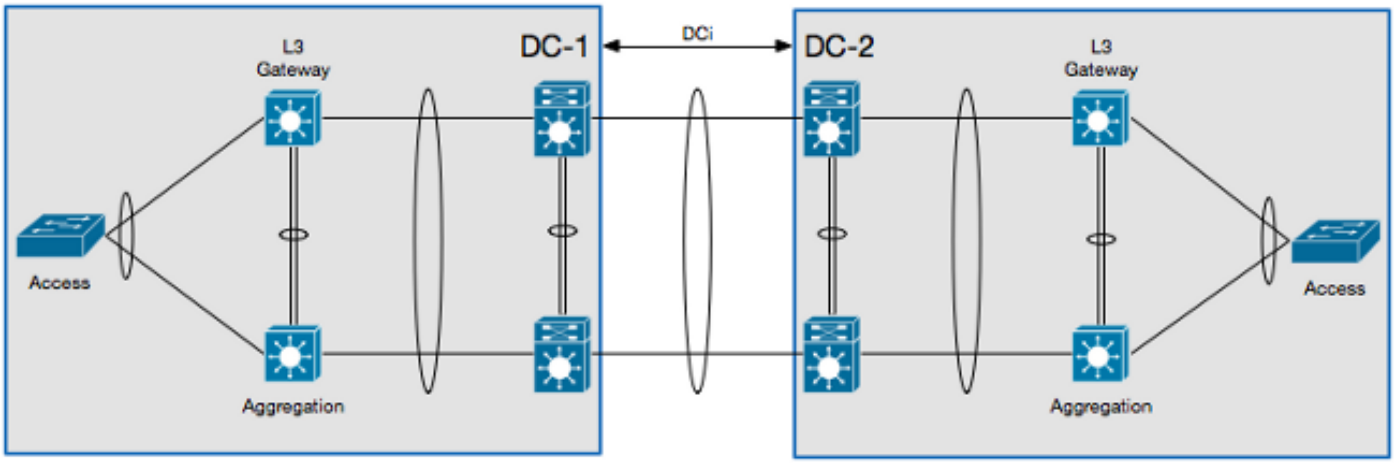
Di seguito è riportato un esempio di configurazione:

```
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
```

Nota: La configurazione precedente può essere utilizzata anche con gli switch Nexus 9000.

Multilayer vPC for Aggregation e DCI

Questa è la topologia utilizzata in questo scenario:



In questo scenario, il DCI viene isolato nel proprio contesto di dispositivo virtuale L2 (VDC) e il gateway L3 si trova su un dispositivo a livello di aggregazione. Per isolare l'HSRP, è necessario configurare un elenco di controllo di accesso VLAN (VACL) che blocchi il traffico di controllo dell'HSRP e un filtro di ispezione ARP che blocchi i GARP HSRP sul VDC L2 DCI.

Di seguito è riportato un esempio di configurazione:

```
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>
```

Configurazione aggiuntiva isolamento

Questa sezione fornisce un esempio di configurazione che:

- Consente di estendere solo le VLAN necessarie nel data center remoto.
- Isolamento dell'STP in ogni centro dati.
- Elimina il traffico di trasmissione che supera l'1% della velocità di collegamento totale.

Di seguito è riportata la configurazione di esempio:

```
 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
```

Nota: È possibile configurare anche il controllo della temporizzazione per il traffico multicast, ma deve avere la stessa percentuale del traffico broadcast.

Crittografia MACSec

Nota: La configurazione descritta in questa sezione è facoltativa.

Utilizzare queste informazioni per configurare la crittografia MACSec:

```
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>
```

Nota: L'interfaccia deve essere interrotta per consentire l'autorizzazione MACSec.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare le informazioni descritte in questa sezione.

Isolamento FHRP

Immettere il comando **show hsrp br** nella CLI per verificare che il gateway HSRP sia attivo in entrambi i data center:

```
!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)
```

Immettere questo comando nella CLI per verificare il filtro ARP:

```
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
```

Se viene visualizzato un output simile a questo, i GARP tra i due gateway attivi non vengono isolati correttamente.

Isolamento aggiuntivo

Immettere il comando **show spanning-tree root** nella CLI per verificare che la radice STP non punti verso il canale della porta DCI:

```
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
```

Immettere questo comando nella CLI per verificare che il controllo temporale sia configurato correttamente:

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

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

Crittografia MACSec

Immettere questo comando nella CLI per verificare che la crittografia MACSec sia configurata correttamente:

```
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
...
```

Risoluzione dei problemi

Attualmente non sono disponibili informazioni specifiche sulla risoluzione dei problemi per FHRP o altre configurazioni di isolamento.

Per la configurazione di MACSec, se la chiave pre-condivisa non è concordata su entrambi i lati del collegamento, viene visualizzato un output simile a questo quando si immette il comando **show interface <DCI-Physical-Port>** nella CLI:

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

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

Nota: La chiave deve essere la stessa su entrambi i lati della connessione.

Avvertenze

> **Nota:** Le avvertenze per i prodotti correlati non sono incluse.

Le seguenti avvertenze sono relative all'uso di un DCI sugli switch Cisco Nexus serie 7000:

- ID bug Cisco CSCur69114 - *Filtro PACL HSRP interrotto - Pacchetti inondati nel dominio di layer 2*. Questo bug si trova solo nella versione software 6.2(10).
- ID bug Cisco CSCut75457 - *Filtro VACL HSRP interrotto*. Questo bug si trova solo nelle versioni software 6.2(10) e 6.2(12).
- ID bug Cisco CSCut43413 - *DCi: Flapping degli indirizzi MAC virtuali HSRP tramite FHRP Isolation PACL*. Questo bug è dovuto a una limitazione hardware.

Informazioni correlate

- Progettazione di data center: Data Center Interconnect
- Introduzione alla tecnologia OTV e considerazioni sull'installazione
- Considerazioni sulla progettazione della mobilità dei carichi di lavoro virtualizzati Cisco
- Documentazione e supporto tecnico – Cisco Systems