Configuración de una interconexión de Data Center vPC de capa 2 en un switch Nexus serie 7000

Contenido

Introducción

Este documento describe cómo configurar una interconexión de Data Center (DCI) de capa 2 (L2) con el uso de un canal de puerto virtual (vPC).

Prerequisites

Se supone que vPC y el protocolo de routing con espera en caliente (HSRP) ya están configurados en los dispositivos que se utilizan en los ejemplos proporcionados en este documento.

Utilice el protocolo de control de agregación de enlaces (LACP) en el enlace vPC, que actúa como DCI.



Consejo: El cifrado de MACSec requiere una licencia de servicios avanzados de LAN en versiones anteriores a la versión 6.1(1) y tiene limitaciones específicas para la tarjeta de línea. Consulte la sección Pautas y limitaciones para Cisco TrustSec de la Guía de configuración de seguridad de NX-OS Nexus de Cisco serie 7000, versión 6.x para obtener información adicional.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- vPC
- HSRP
- Protocolo de árbol de expansión (STP)
- Cifrado MACSec (opcional)

Componentes Utilizados

La información de este documento se basa en un switch Nexus de Cisco serie 7000 que ejecuta la versión de software 6.2(8b).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

El objetivo de un DCI es ampliar VLAN específicas entre diferentes Data Centers, lo que ofrece adyacencia de capa 2 para servidores y dispositivos de almacenamiento conectado a la red (NAS) que están separados por grandes distancias.

vPC presenta la ventaja del aislamiento STP entre los dos sitios (sin unidad de datos de protocolo de puente (BPDU) en vPC de DCI), por lo que cualquier interrupción en un Data Center no se propaga al Data Center remoto porque aún se proporcionan enlaces redundantes entre los Data Centers.

Utilice vPC para interconectar un máximo de dos Data Centers. Si se deben interconectar más de dos Data Centers, utilice Overlay Transport Virtualization (OTV).

Un vPC etherchannel de DCI se configura típicamente con esta información en mente:

- Aislamiento del protocolo de redundancia de primer salto (FHRP): Evite el routing por debajo del nivel óptimo con el uso de un gateway dedicado para cada Data Center. Las configuraciones varían según la ubicación del gateway FHRP.
- Aislamiento de STP: Como se ha mencionado anteriormente, esto evita la propagación de las interrupciones de un Data Center a otro.
- Control de tormentas de difusión: Se utiliza para minimizar la cantidad de tráfico de difusión entre los Data Centers.
- Cifrado MACSec (opcional): Esto cifra el tráfico para evitar la intrusión entre las dos instalaciones.

Configurar

Utilice la información descrita en esta sección para configurar un DCI L2 con el uso de un vPC.

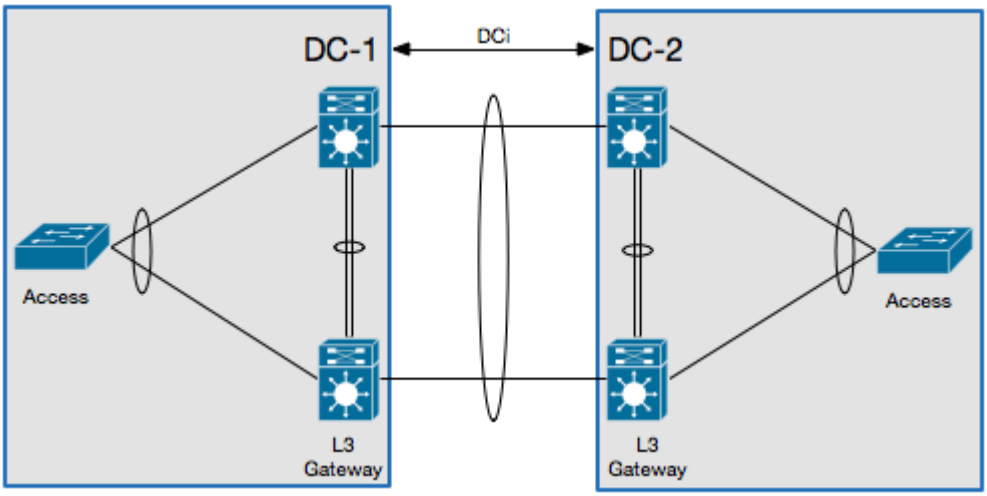
Los clientes registrados pueden utilizar la Command Lookup Tool para obtener más información sobre los comandos que se utilizan aquí.

Aislamiento de FHRP

Esta sección describe dos escenarios para los cuales se puede implementar el aislamiento FHRP.

Interconexión de POD L2/L3 dual

Esta es la topología que se utiliza en este escenario:



En esta situación, la puerta de enlace de capa 3 (L3) se configura en el mismo par vPC y actúa como DCI. Para aislar el HSRP, debe configurar una lista de control de acceso a puertos (PACL) en el canal de puerto DCI y desactivar los protocolos de resolución de direcciones gratuitas (ARP) (GARP) de HSRP en las interfaces virtuales conmutadas (SVI) para las VLAN que se mueven a través del DCI.

Aquí hay un ejemplo de configuración:

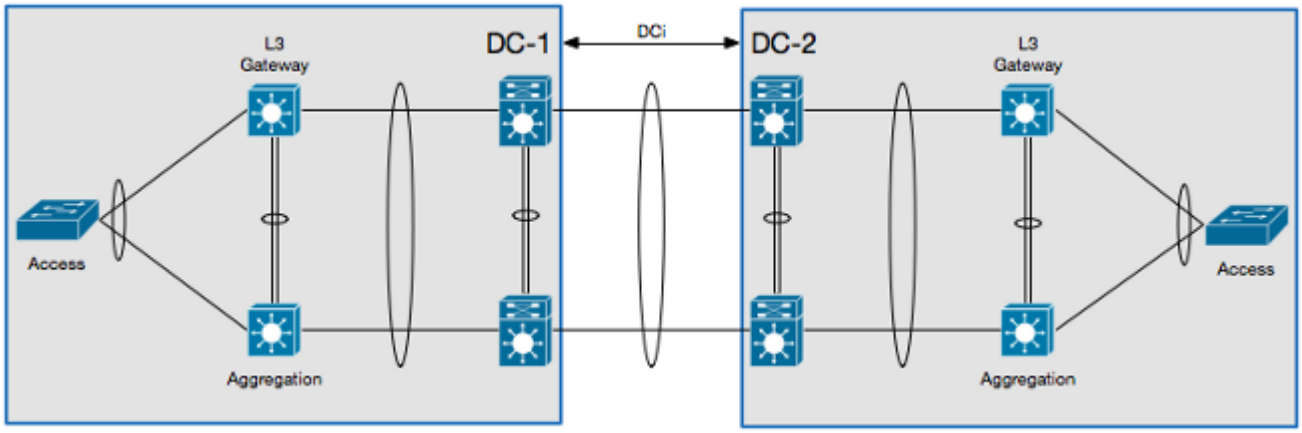
```
ip access-list DENY_HSRP_IP
  10 deny udp any 224.0.0.2/32 eq 1985
  20 deny udp any 224.0.0.102/32 eq 1985
  30 permit ip any any

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

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

vPC multicapa para agregación y DCI

Esta es la topología que se utiliza en este escenario:



En esta situación, el DCI se aísla en su propio contexto de dispositivo virtual (VDC) de capa 2 y el gateway de capa 3 se encuentra en un dispositivo de capa de agregación. Para aislar el HSRP, configure una VLAN Access Control List (VACL) que bloquee el tráfico de control HSRP y un filtro de inspección ARP que bloquee los GARP HSRP en el VDC DCI L2. Ejemplo de configuración:

```
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>
```

Configuración de aislamiento adicional

Esta sección proporciona un ejemplo de configuración que:

- Permite ampliar solo las VLAN necesarias en el Data Center remoto
- Aísla el STP en cada Data Center
- Descarta el tráfico de broadcast que excede el 1% de la velocidad total del link

Ejemplo de configuración:

```
 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
```

El control de tormentas para el tráfico de multidifusión también se puede configurar, pero debe tener el mismo porcentaje que el tráfico de difusión.

Cifrado MACSec

La configuración descrita en esta sección es opcional.

Utilice esta información para configurar el cifrado 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>
```

Desactive la interfaz para que se produzca la autorización de MACSec.

Verificación

Utilice la información que se describe en esta sección para confirmar que la configuración funciona correctamente.

Aislamiento de FHRP

Ingrese el comando show hsrp br en la CLI para verificar que la gateway HSRP esté activa en ambos Data Centers:

<#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)
```

Ingrese este comando en la CLI para verificar el filtro ARP:

<#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
```

Si aparece un resultado similar a este, los GARP entre las dos puertas de enlace activas no se aíslan correctamente.

Aislamiento adicional

Ingrese el comando show spanning-tree root en la CLI para verificar que la raíz STP no apunte hacia el canal de puerto DCI:

<#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
```

Ingrese este comando en la CLI para verificar que el control de tormentas esté configurado correctamente:

<#root>

N7K-A#

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

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

Cifrado MACSec

Ingrese este comando en la CLI para verificar que el cifrado MACSec esté configurado

correctamente:

<#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
...
```

Troubleshoot

Actualmente no hay información específica de troubleshooting disponible para el FHRP o configuraciones de aislamiento adicionales.

Para la configuración de MACSec, si la clave previamente compartida no está acordada en ambos lados del link, verá un resultado similar a este cuando ingrese el comando show interface <DCI-Physical-Port> en la CLI:

<#root>

```
N7K-A#

show interface <DCI-Physical-Port>


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

La clave debe ser la misma en ambos lados de la conexión.

Advertencias

Estas advertencias están relacionadas con el uso de un DCI en el switch Nexus de Cisco serie 7000. No se incluyen advertencias para productos relacionados.

- ID de bug de Cisco CSCur69114 - Filtro HSRP PACL roto - Los paquetes se inundan al dominio de capa 2. Este bug se encuentra solamente en la versión 6.2(10) del software.
- ID de bug de Cisco CSCut75457 - Filtro VACL HSRP roto. Este bug se encuentra solamente en las versiones 6.2(10) y 6.2(12) del software.
- ID de bug de Cisco CSCut43413 - DCi: HSRP MAC virtual inestable a través de PACL de aislamiento FHRP. Este error se debe a una limitación de hardware.

Información Relacionada

- Soluciones de Cisco
- Introducción a la tecnología OTV y consideraciones de implementación
- Consideraciones de diseño de movilidad de cargas de trabajo virtualizadas de Cisco
- Asistencia técnica y documentación

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).