Configurar uma interconexão de data center vPC de camada 2 em um switch Nexus 7000 Series

Contents

Introdução

Este documento descreve como configurar uma interconexão de data center (DCI) da camada 2 (L2) com o uso de um canal de porta virtual (vPC).

Pré-requisitos

Supõe-se que vPC e Hot Standby Routing Protocol (HSRP) já estejam configurados nos dispositivos que são usados nos exemplos fornecidos neste documento.

Use o LACP (Link Aggregation Control Protocol Protocolo de Controle de Agregação de Enlaces) no enlace vPC, que atua como o DCI.



Tip: A criptografia MACSec requer uma licença de serviços avançados de LAN em versões anteriores à versão 6.1(1) e tem limitações específicas de placa de linha. Consulte a seção Diretrizes e limitações do Cisco TrustSec do Guia de configuração de segurança do NX-OS Cisco Nexus 7000 Series, versão 6.x para obter informações adicionais.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- vPC
- HSRP
- Spanning-Tree Protocol (STP)
- Criptografia MACSec (opcional)

Componentes Utilizados

As informações neste documento são baseadas em um switch Cisco Nexus 7000 Series que executa a versão 6.2(8b) do software.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

A finalidade de um DCI é estender VLANs específicas entre data centers diferentes, o que oferece adjacência L2 para servidores e dispositivos NAS (Network-Attached Storage, armazenamento conectado à rede) que estão separados por grandes distâncias.

O vPC apresenta o benefício do isolamento de STP entre os dois locais (sem BPDU (Bridge Protocol Data Unit) através do DCI vPC), de modo que qualquer interrupção em um data center não é propagada para o data center remoto, porque links redundantes ainda são fornecidos entre os data centers.

Use o vPC para interconectar no máximo dois data centers. Se mais de dois data centers precisarem ser interconectados, use a virtualização de transporte de sobreposição (OTV).

Um etherchannel DCI vPC é normalmente configurado com estas informações em mente:

- Isolamento de First Hop Redundancy Protocol (FHRP): Impeça o roteamento abaixo do ideal com o uso de um gateway dedicado para cada data center. As configurações variam de acordo com a localização do gateway de FHRP.
- Isolamento de STP: Como mencionado anteriormente, isso evita a propagação de interrupções de um data center para outro.
- Controle de tempestade de broadcast: Isso é usado para minimizar a quantidade de tráfego de broadcast entre os data centers.
- Criptografia MACSec (opcional): Isso criptografa o tráfego para evitar intrusão entre as duas instalações.

Configurar

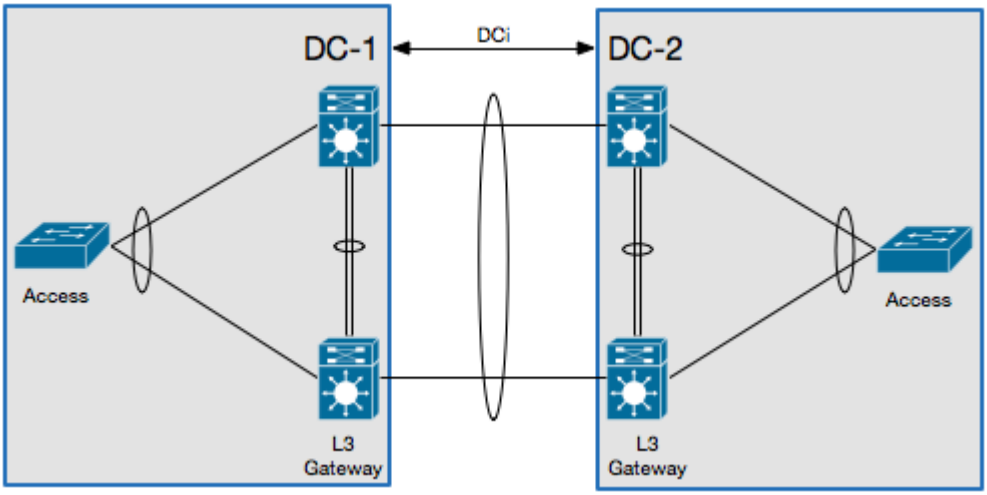
Use as informações descritas nesta seção para configurar um DCI L2 com o uso de um vPC. Os clientes registrados podem usar a Command Lookup Tool para obter mais informações sobre os comandos usados aqui.

Isolamento de FHRP

Esta seção descreve dois cenários para os quais o isolamento de FHRP pode ser implementado.

Interconexão POD L2/L3 dupla

Esta é a topologia usada neste cenário:



Neste cenário, o gateway de Camada 3 (L3) é configurado no mesmo par de vPC e atua como o DCI. Para isolar o HSRP, você deve configurar uma Port Access Control List (PACL) no canal de porta do DCI e desabilitar os Gratuitous Address Resolution Protocols (ARPs) (GARPs) do HSRP nas Switched Virtual Interfaces (SVIs) para as VLANs que se movem pelo DCI.

Aqui está um exemplo de configuração:

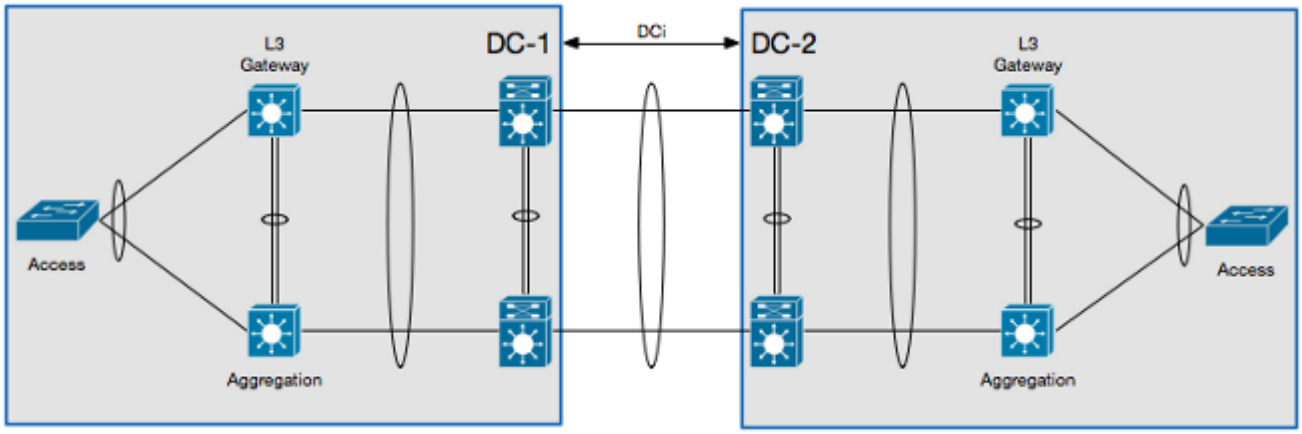
```
ip access-list DENY_HSRP_IP
  10 deny udp any 224.0.0.2/32 eq 1985
  20 deny udp any 224.0.0.102/32 eq 1985
  30 permit ip any any

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

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

vPC multicamada para agregação e DCI

Esta é a topologia usada neste cenário:



Neste cenário, o DCI é isolado em seu próprio Contexto de Dispositivo Virtual (VDC - Virtual Device Context) de L2 e o gateway de L3 está em um dispositivo de camada de agregação. Para isolar o HSRP, configure uma VLAN Access Control List (VACL) que bloqueie o tráfego de controle do HSRP e um filtro de inspeção ARP que bloqueie os HSRP GARPs no VDC de DCI da L2. Exemplo de configuração:

```
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>
```

Configuração de isolamento adicional

Esta seção fornece um exemplo de configuração que:

- Permite que somente as VLANs necessárias no data center remoto sejam estendidas
- Isola o STP em cada data center
- Descarta o tráfego de broadcast que excede 1% da velocidade total do link

Exemplo de configuração:

```
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
```

O controle de storm para tráfego de multicast também pode ser configurado, mas deve ter a mesma porcentagem que o tráfego de broadcast.

Criptografia MACSec

A configuração descrita nesta seção é opcional.

Use estas informações para configurar a criptografia 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>
```

Alterne a interface para que ocorra autorização MACSec.

Verificar

Use as informações descritas nesta seção para confirmar se sua configuração funciona corretamente.

Isolamento de FHRP

Insira o comando show hsrp br na CLI para verificar se o gateway HSRP está ativo em ambos os 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)
```

Digite este comando no CLI para verificar o 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
```

Se uma saída semelhante a essa aparecer, os GARPs entre os dois gateways ativos não serão isolados corretamente.

Isolamento Adicional

Insira o comando show spanning-tree root na CLI para verificar se a raiz do STP não aponta para o canal de porta do 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
```

Digite este comando no CLI para verificar se o storm control está configurado corretamente:

<#root>

N7K-A#

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

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

Criptografia MACSec

Digite este comando no CLI para verificar se a criptografia MACSec está configurada corretamente:

<#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
...
```

Troubleshooting

No momento, não há informações de Troubleshooting específicas disponíveis para o FHRP ou configurações de isolamento adicionais.

Para a configuração do MACSec, se a chave pré-compartilhada não for acordada nos dois lados do link, você verá uma saída semelhante a esta quando inserir o comando show interface <DCI-Physical-Port> na CLI:

<#root>

```
N7K-A#

show interface <DCI-Physical-Port>


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

A chave deve ser a mesma em ambos os lados da conexão.

Caveats

Essas advertências estão relacionadas ao uso de um DCI no switch Cisco Nexus 7000 Series. As advertências para produtos relacionados não estão incluídas.

- ID de bug da Cisco CSCur69114 - Filtro PACL HSRP quebrado - Os pacotes são inundados para o domínio da camada 2. Esse bug é encontrado somente na versão 6.2(10) do software.

- ID de bug Cisco CSCut75457 - Filtro de VACL HSRP quebrado. Esse bug é encontrado somente nas versões 6.2(10) e 6.2(12) do software.
- ID de bug Cisco CSCut43413 - DCi: Flapping de MAC Virtual de HSRP através de PACL de Isolamento de FHRP. Esse bug é devido a uma limitação de hardware.

Informações Relacionadas

- Soluções da Cisco
- Introdução à tecnologia OTV e considerações sobre implantação
- Considerações sobre o projeto de mobilidade de carga de trabalho virtualizada da Cisco
- Suporte técnico e documentação

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.