

# Configurar uma interconexão do centro de dados do vPC da camada 2 em um 7000 Series Switch do nexa

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Isolamento FHRP](#)

[Interconexão dupla da VAGEM L2/L3](#)

[VPC Multilayer para a agregação e o DCI](#)

[Configuração adicional do isolamento](#)

[Criptografia de MACSec](#)

[Verificar](#)

[Isolamento FHRP](#)

[Isolamento adicional](#)

[Criptografia de MACSec](#)

[Troubleshooting](#)

[Caveats](#)

[Informações Relacionadas](#)

## Introdução

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

## Pré-requisitos

Supõe-se que o protocolo de roteamento do vPC e do standby recente (HSRP) está configurado já nos dispositivos que são usados nos exemplos fornecidos neste documento.

Nota: O protocolo link aggregation control (LACP) deve ser usado no link do vPC, que atua como o DCI.

Dica: A criptografia de MACSec exige uma licença dos Serviços avançados LAN nas versões antes da versão 6.1(1) e tem limitações placa de linha-específicas. Refira as [diretrizes e as limitações para a](#) seção de [Cisco TrustSec do guia de configuração de segurança do 7000 Series NX-OS do nexo de Cisco](#), liberam 6.x para a informação adicional.

## Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- vPC
- HSRP
- Medida - protocolo de árvore (STP)
- Criptografia de MACSec (opcional)

## Componentes Utilizados

A informação neste documento é baseada em um 7000 Series Switch do nexo de Cisco que execute a versão de software 6.2(8b).

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 VLAN específicos entre centros de dados diferentes, que ofereça a adjacência L2 para os server e os dispositivos do network attached storage (NAS) que são separados por grandes distâncias.

O vPC apresenta o benefício do isolamento STP entre os dois locais (nenhuma unidade de dados de protocolo de bridge (PDU) através do vPC DCI), assim que nenhuma indisponibilidade em um centro de dados não é propagada ao centro de dados remotos porque os enlaces redundantes são fornecidos ainda entre os centros de dados.

Nota: O vPC pode ser usado a fim interconectar um máximo de dois centros de dados. Se mais de dois centros de dados devem ser interconectados, Cisco recomenda que você use a virtualização do transporte da folha de prova (OTV).

Um EtherChannel do vPC DCI é configurado tipicamente com esta informação na mente:

- Primeiro isolamento do protocolo da redundância de salto (FHRP): Impeça o roteamento subótimo com o uso de um gateway dedicado para cada centro de dados. As configurações variam o dependente em cima do lugar do gateway FHRP.
- Isolamento STP: Como mencionado previamente, isto impede a propagação das

indisponibilidade de um centro de dados a outro.

- Controle da tempestade de transmissão: Isto é usado a fim minimizar a quantidade de tráfego de broadcast entre os centros de dados.
- Criptografia de MACSec (opcional): Isto cifra o tráfego a fim impedir a intrusão entre as duas facilidades.

## Configurar

Use a informação que é descrita nesta seção a fim configurar um L2 DCI com o uso de um vPC.

Nota: Use a [Command Lookup Tool](#) ( [somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

### Isolamento FHRP

Esta seção descreve duas encenações para que o isolamento FHRP pode ser executado.

#### Interconexão dupla da VAGEM L2/L3

Esta é a topologia que é usada nesta encenação:

Nesta encenação, o gateway da camada 3 (L3) é configurado nos mesmos pares do vPC e atua como o DCI. A fim isolar o HSRP, você deve configurar um Access Control List da porta (PACL) no canal de porta DCI e desabilitar os protocolos gratuitos de resolução de endereço HSRP (ARP) (GARP) nas interfaces virtuais comutadas (SVI) para os VLAN que se movem através do DCI.

Está aqui 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
```

Nota: A configuração precedente pode igualmente ser usada com 9000 Switch do nexa.

### VPC Multilayer para a agregação e o DCI

Esta é a topologia que é usada nesta encenação:

Nesta encenação, o DCI é isolado em seu próprio contexto do dispositivo virtual L2 (VDC), e o gateway L3 está em um dispositivo da camada da agregação. A fim isolar o HSRP, você deve configurar um VLAN Access Control List (VACL) nesse bloco o tráfego de controle HSRP e um filtro da inspeção ARP que obstrua o HSRP GARP no L2 DCI VDC.

Está aqui um 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 adicional do isolamento

Esta seção fornece um exemplo de configuração disso:

- Permite somente os VLAN que são precisados no centro de dados remotos de ser estendidos.
- Isola o STP em cada centro de dados.
- Deixa cair o tráfego de broadcast que excede 1% da velocidade do enlace total.

Está aqui o 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
```

**Nota:** O controle de tempestade para o tráfego multicast pode igualmente ser configurado, mas deve ter a mesma porcentagem que o tráfego de broadcast.

## Criptografia de MACSec

Nota: A configuração que é descrita nesta seção é opcional.

Use esta informação a fim configurar a criptografia de 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: A relação deve ser batida para que a autorização de MACSec ocorra.

## Verificar

Use a informação que é descrita nesta seção a fim confirmar que sua configuração trabalha corretamente.

## Isolamento FHRP

Incorpore o comando do **Br do hsrp da mostra no CLI** a fim verificar que o gateway HSRP é ativo em ambos os centros de dados:

```
!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)
```

Incorpore este comando no CLI a fim verificar o 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 uma saída similar a esta aparece, a seguir os GARP entre os dois gateways ativo não estão isolados corretamente.

## Isolamento adicional

Incorpore o comando da **raiz de Spanning Tree da mostra no CLI** a fim verificar que a raiz STP não aponta para o canal de porta DCI:

```
N7K-A# show spanning-tree root
```

Vlan	Root ID	Root Cost	Hello Time	Max Age	Fwd Dly	Root Port
VLAN0010	4106 0023.04ee.be01	0	2	20	15	This bridge is root

Incorpore este comando no CLI a fim verificar que o controle de tempestade está configurado corretamente:

```
N7K-A# show interface <DCI-Port-Channel> counters storm-control
```

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

## Criptografia de MACSec

Incorpore este comando no CLI a fim verificar que a criptografia de MACSec está configurada corretamente:

```
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

Não há atualmente nenhuma informação de Troubleshooting específica disponível para o FHRP ou as configurações adicionais do isolamento.

Para a configuração de MACSec, se a chave pré-compartilhada não é concordada em ambos os lados do link, você vê uma saída similar a esta quando você incorpora o comando do **<DCI-Physical-Port> da relação da mostra no CLI**:

```
N7K-A# show interface <DCI-Physical-Port>
Ethernet3/41 is down (Authorization pending)
admin state is up, Dedicated Interface
```

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

## Caveats

Nota: As advertências para os produtos relacionados não são incluídas.

Estas advertências são relacionadas ao uso de um DCI no 7000 Series Switch do nexo de Cisco:

- Identificação de bug Cisco [CSCur69114](#) - *Filtro HSRP PACL quebrado - Os pacotes são inundados ao domínio layer2*. Este erro é encontrado somente na versão de software 6.2(10).
- Identificação de bug Cisco [CSCut75457](#) - *Filtro HSRP VACL quebrado*. Este erro é encontrado somente nas versões de software 6.2(10) e 6.2(12).
- Identificação de bug Cisco [CSCut43413](#) - *DCI: Flapping do MAC virtual de HSRP com o isolamento PACL FHRP*. Este erro é devido a uma limitação do hardware.

## Informações Relacionadas

- [Projetos do centro de dados: Interconexão do centro de dados](#)
- [Introdução de tecnologia e considerações de desenvolvimento OTV](#)
- [Cisco virtualizou considerações de projeto da mobilidade da carga de trabalho](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)