配置在连结7000系列交换机的Layer2 vPC数据中心互连

目录

简介

本文描述如何配置Layer2 (L2)数据中心互连(DCI)与使用一虚拟Port-Channel (vPC)。

先决条件

假设， vPC和Hot Standby Routing Protocol (HSRP)在本文提供的示例使用的设备已经配置。

> **注意**：在vPC链路应该使用链路汇聚控制协议(LACP)，作为DCI。

> **提示**：MACSec加密在版本要求LAN高级服务准许在版本6.1(1)之前并且有线路卡特定限制。参考指南和限制**Cisco连结7000系列NX-OS安全配置指南的**Cisco TrustSec部分的，**版本6.x**其他信息。

要求

Cisco 建议您了解以下主题：

- vPC
- HSRP
- 生成树协议
- MACSec加密(可选)

使用的组件

本文档中的信息根据运行软件版本6.2(8b)的Cisco连结7000系列交换机。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

DCI的目的将扩大区别数据中心之间的特定VLAN，提供L2服务器和连接网络的存储设备的邻接由大距离分离。

vPC提交STP隔离的好处在两个站点(在DCI vPC间的没有网桥协议数据单元(BPDU)之间的)，因此任何中断在数据中心没有被传播对远程数据数据中心，因为冗余链路仍然提供在数据中心之间。

> **注意**：vPC可以用于为了互联最多两个数据中心。如果超过必须互联两个数据中心，思科建议您使用覆盖传输虚拟化(OTV)。

DCI vPC EtherChannel典型地配置有此信息的念头：

- 第一跳跃冗余协议(FHRP)隔离：防止次优路由与使用每个数据中心的一个专用的网关。配置变化从属在FHRP网关的位置。
- STP隔离：如前所提及，这防止中断的传播一个数据中心到另一个。
- 广播风暴控制：这用于为了最小化在数据中心之间的广播数据流量。
- MACSec加密(可选)：这加密流量为了防止在两设施之间的入侵。

配置

请使用在此部分描述为了配置与使用的L2 DCI vPC的信息。

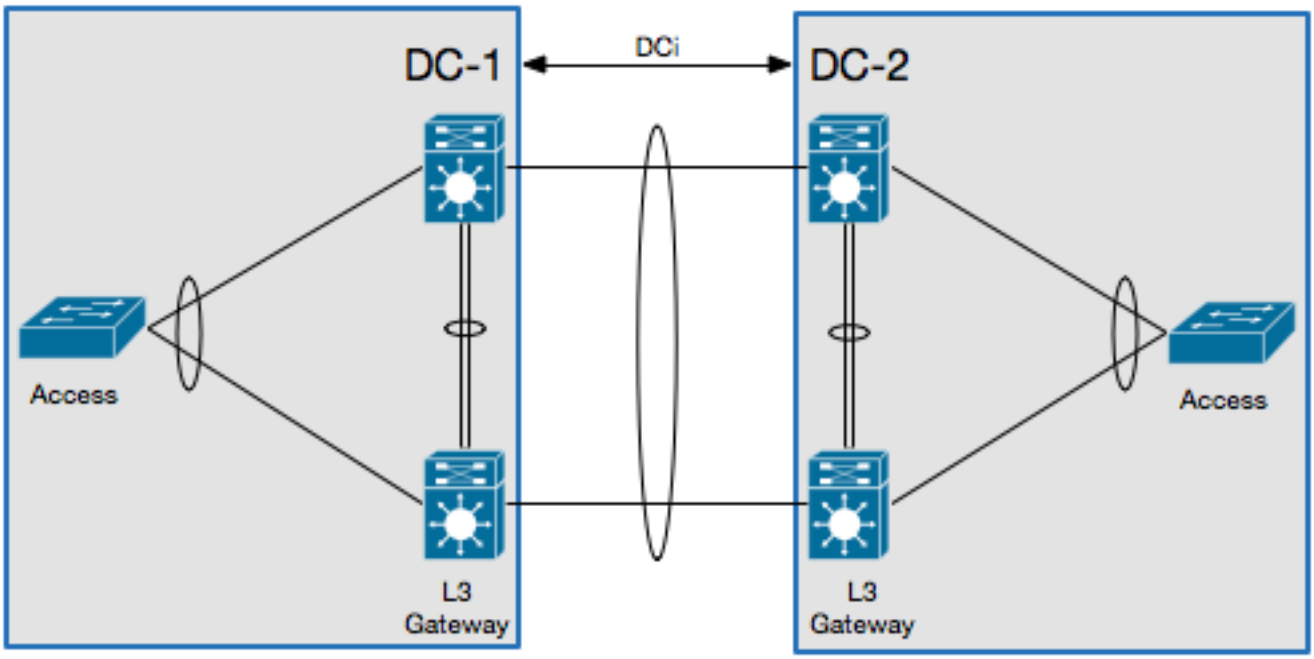
> **注意**：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

FHRP隔离

此部分描述FHRP隔离可以实现的两个方案。

双重L2/L3 Pod互连

这是在此方案使用的拓扑：



在此方案中，第3层(L3)网关在同一个vPC对配置并且作为DCI。为了隔离HSRP，您必须配置端口访问控制表(PACL)在DCI Port-Channel和禁用HSRP无偿地址解析协议(ARPs) (GARPs)在交换虚拟接口(SVIs)在DCI间移动的VLAN的。

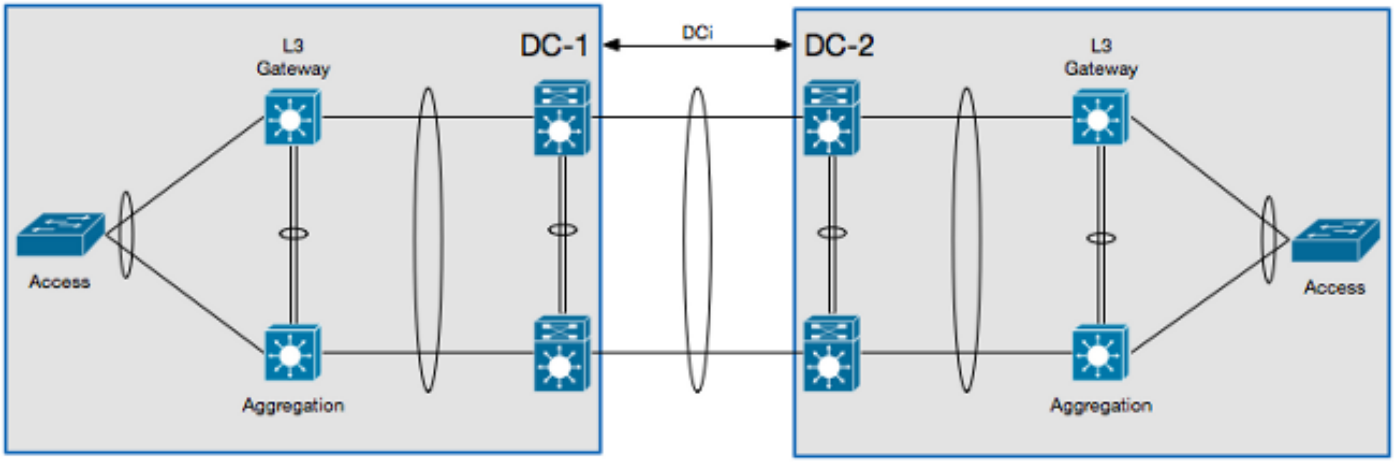
这是配置示例：

```
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
```

注意：先前配置可能也与连结一起使用9000交换机。

聚合和DCI的多层vPC

这是在此方案使用的拓扑：



在此方案中， DCI独自地是隔离的L2虚拟设备上下文(VDC)，并且L3网关在聚合层设备。为了隔离HSRP，阻塞HSRP控制流量和ARP检查过滤器阻塞在L2 DCI VDC的HSRP GARPs的您必须配置VLAN访问控制列表(VACL)。

这是配置示例：

```
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>
```

另外的隔离配置

此部分提供一配置示例那：

- 允许是需要的在将被延伸的远程数据数据中心仅的VLAN。
- 隔离STP在每个数据中心。

- 降低超出1%总链路速度的广播数据流。

这是配置示例：

```
 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
```

注意：组播数据流的风暴控制可能也配置，但是必须有百分比和广播数据流一样。

MACSec加密

注意：在此部分描述的配置可选。

请使用此信息为了配置MACSec加密：

```
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>
```

注意：必须拍动接口为了MACSec授权能发生。

验证

请使用在此部分描述为了确认的信息您的配置适当地工作。

FHRP隔离

输入**show hsrp增殖比**命令到CLI为了验证HSRP网关是活跃的在两个数据中心：

```
!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)
```

输入此命令到CLI为了验证ARP过滤器：

```
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
```

如果输出类似于此出现，则在两激活网关之间的GARPs没有适当地隔离。

另外的隔离

输入**root命令的show spanning-tree**到CLI为了验证STP根不指向往DCI Port-Channel ：

```
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
```

输入此命令到CLI为了验证风暴控制适当地配置：

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

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

MACSec加密

输入此命令到CLI为了验证MACSec加密适当地配置：

```
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
...
```

故障排除

当前没有FHRP或另外的隔离配置的特定故障排除信息联机。

对于MACSec配置，如果预先共享密钥没有同意在链路的两边，您看到输出类似于此，当您输入**show interface <DCI-Physical-Port>**命令到CLI时：

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

注意：密钥必须是相同的在连接的两边。

警告

注意：相关产品的警告没有包括。

这些警告与使用在Cisco连结7000系列交换机的DCI涉及：

- Cisco Bug ID CSCur69114 - *HSRP违反的PACL过滤器-数据包被充斥对layer2域*。此bug在软件版本6.2(10)仅被找到。
- Cisco Bug ID CSCut75457 - *HSRP违反的VACL过滤器*。此bug在软件版本仅被找到6.2(10)和6.2(12)。
- Cisco Bug ID CSCut43413 - *DCi ：通过FHRP隔离PACL拍动的HSRP虚拟MAC*。此bug归结于硬件限制。

相关信息

- **数据中心设计：数据中心互连**
- **OTV技术介绍和部署注意事项**
- **思科虚拟化工作量移动性设计注意事项**
- **技术支持和文档 - Cisco Systems**