Настройте Межсоединение ЦОД vPC Уровня 2 на Коммутаторе Cisco Nexus серии 7000

Содержание

Введение

Этот документ описывает, как настроить Уровень 2 (L2) Межсоединение ЦОД (DCI) с использованием технологии Virtual PortChannel (vPC).

Предварительные условия

Предполагается, что vPC и протокол маршрутизации с горячим резервированием (HSRP) уже настроены на устройствах, которые используются в примерах, предоставленных в этом документе.

> **Примечание:** Протокол управления агрегацией каналов (LACP) должен использоваться на ссылке vPC, которая действует как DCI.

> **Совет:** Шифрование MACSec требует лицензии расширенных сервисов LAN в версиях

до Версии 6.1 (1) и имеет специфичные для линейной платы ограничения. См. Рекомендации и Ограничения для раздела Cisco TrustSec **Cisco Nexus Руководство по конфигурации системы безопасности NX-OS серии 7000, Выпуск 6.x** для дополнительных сведений.

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- VPC
- HSRP
- Протокол STP (Spanning Tree Protocol)
- (Дополнительное) шифрование MACSec

Используемые компоненты

Сведения в этом документе основываются на коммутаторе Cisco Nexus серии 7000, который работает под управлением ПО версии 6.2 (8b).

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Цель DCI состоит в том, чтобы расширить определенные VLAN между другими ЦОД, который предлагает смежность L2 для серверов и устройств Подключенного сетевого накопителя (NAS), которые разделены большими расстояниями.

VPC представляет преимущество изоляции STP между этими двумя узлами (никакой Блок данных протокола моста (BPDU) через vPC DCI), таким образом, любой простой в ЦОД не распространяется к центру удаленных данных, потому что избыточные соединения все еще предоставлены между ЦОД.

> **Примечание:** VPC может использоваться для соединения максимума двух ЦОД. Если больше чем два ЦОД должны быть соединены, Cisco рекомендует использовать Виртуализацию транспорта наложения (OTV).

VPC DCI etherchannel, как правило, настраивается с этой информацией в памяти:

- Изоляция Первого протокола резервирования переходов (FHRP): Предотвратите субоптимальную маршрутизацию с использованием специализированного шлюза для каждого ЦОД. Конфигурации варьируются зависящие от местоположения шлюза FHRP.
- Изоляция STP: Как ранее упомянуто, это предотвращает распространение простоев от одного ЦОД до другого.

- Контроль за широковещательным штормом: Это используется для уменьшения суммы широковещательного трафика между ЦОД.
- (Дополнительное) Шифрование MACSec: Это шифрует трафик для предотвращения проникновения между этими двумя средствами.

Настройка

Используйте информацию, которая описана в этом разделе для настройки L2 DCI с использованием vPC.

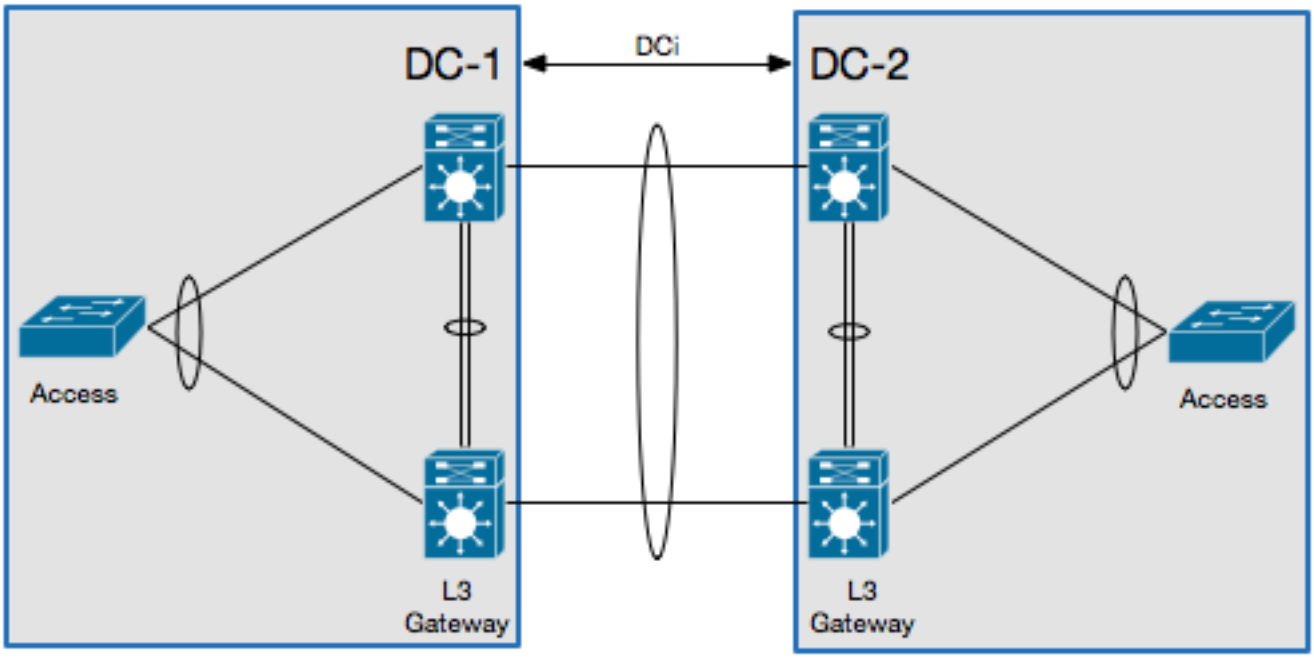
> **Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Изоляция FHRP

В этом разделе описываются два сценария, для которых может быть внедрена изоляция FHRP.

Двойное Межсоединение POD L2/L3

Это - топология, которая используется в этом сценарии:



В этом сценарии Уровень 3 (L3) шлюз настроен на той же паре vPC и действует как DCI. Для изоляции HSRP необходимо настроить Порт список контроля доступа (PACL) на port-channel DCI и отключить Предварительные запросы ARP (протокол разрешения адресов) HSRP (ARPs) (GARP) на Коммутируемых виртуальных интерфейсах (SVI) для VLAN, которые преодолевают DCI.

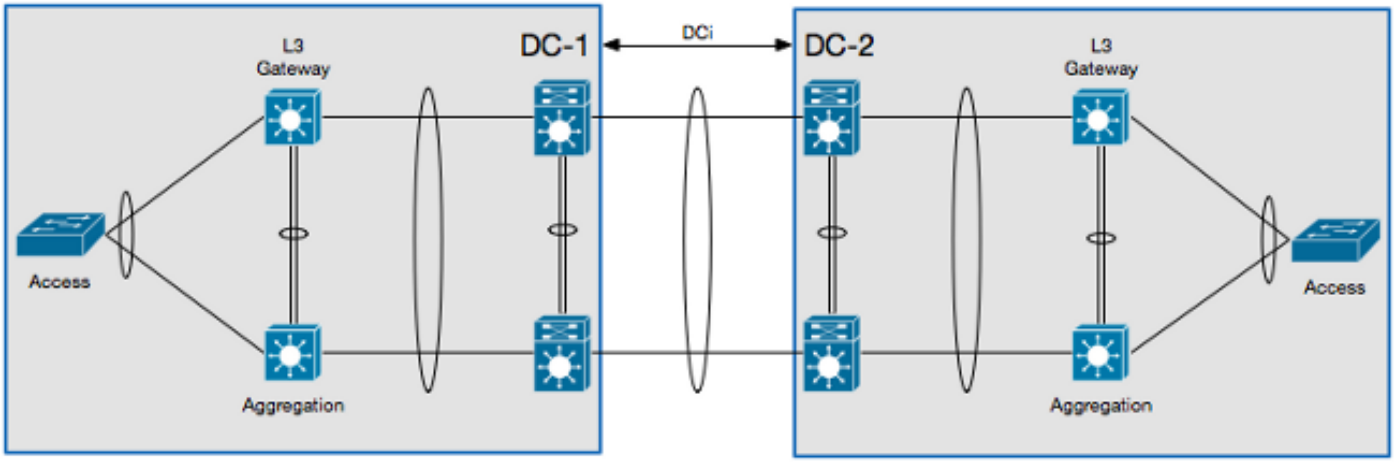
Вот пример конфигурации:

```
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
```

> **Примечание:** Предыдущая конфигурация может также использоваться с коммутаторами Nexus 9000.

Многоуровневый vPC для Агрегации и DCI

Это - топология, которая используется в этом сценарии:



В этом сценарии DCI изолирован самостоятельно контекст виртуального устройства (VDC) L2, и шлюз L3 находится на устройстве уровня агрегации. Для изоляции HSRP необходимо настроить Список контроля доступом VLAN (VACL), который блокирует контрольный трафик HSRP и фильтр проверки ARP, который блокирует GARP HSRP на L2 DCI VDC.

Вот пример конфигурации:

```
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>
```

Дополнительная конфигурация изоляции

Этот раздел предоставляет пример конфигурации что:

- Позволяет только VLAN, которые необходимы в центре удаленных данных, который будет расширен.
- Изолирует STP в каждом ЦОД.
- Отбрасывает широковещательный трафик, который превышает 1% скорости общего размера канала.

Вот пример конфигурации:

```
 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
```

> **Примечание:** Управление штормом для многоадресного трафика может также быть настроено, но это должно иметь тот же процент как широковещательный трафик.

Шифрование MACSec

> **Примечание:** Конфигурация, которая описана в этом разделе, является дополнительной.

Используйте эту информацию для настройки шифрования 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>
```

Примечание: Интерфейсом нужно махать для авторизации MACSec произойти.

Проверка

Используйте информацию, которая описана в этом разделе, чтобы подтвердить, что ваша конфигурация работает должным образом.

Изоляция FHRP

Введите команду **br show hsrp** в CLI, чтобы проверить, что шлюз HSRP активен в обоих ЦОД:

```
!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)
```

Введите эту команду в CLI для проверки фильтра 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
```

Если выходные данные, подобные этому, появляются, то GARP между этими двумя активными шлюзами должным образом не изолированы.

Дополнительная изоляция

Введите **команду show spanning-tree root** в CLI, чтобы проверить, что корень STP не указывает к port-channel 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
```

Введите эту команду в CLI, чтобы проверить, что должным образом настроено управление штормом:

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

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

Шифрование MACSec

Введите эту команду в CLI, чтобы проверить, что должным образом настроено шифрование MACSec:

```
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
...
```

Устранение неполадок

В настоящее время нет никаких определенных сведений об устранении проблем, доступных для FHRP или дополнительных конфигураций изоляции.

Для конфигурации MACSec, если предварительный общий ключ не согласован с обеих сторон ссылки, вы видите выходные данные, подобные этому при вводе команды **<DCI-Physical-Port> show interface** в CLI:

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

> **Примечание:** Ключ должен быть тем же с обеих сторон соединения.

Предупреждения

> **Примечание:** Предупреждения для родственных продуктов не включены.

Эти предупреждения отнесены к использованию DCI на коммутаторе Cisco Nexus серии 7000:

- Идентификатор ошибки Cisco CSCur69114 - *Сломанный Фильтр PACL HSRP - Пакеты лавинно рассылается к layer2 домену*. Этот дефект найден только в версии программного обеспечения 6.2 (10).
- Идентификатор ошибки Cisco CSCut75457 - *Сломанный Фильтр VACL HSRP*. Этот

дефект найден только в версиях программного обеспечения 6.2 (10) и 6.2 (12).

- Идентификатор ошибки Cisco CSCut43413 - *DCi: Виртуальный MAC - адрес HSRP, Колеблющийся через PACL Изоляции FHRP*. Этот дефект происходит из-за аппаратного ограничения.

Дополнительные сведения

- Дизайны ЦОД: межсоединение ЦОД
- Введение в технологию OTV и вопросы развертывания
- Cisco виртуализированные вопросы проектирования мобильности рабочей нагрузки
- Cisco Systems – техническая поддержка и документация