Настройте резервирование интернет-провайдера на луче DMVPN с облегченной VRF функцией

Содержание

Введение

Этот документ описывает, как настроить резервирование интернет-провайдера (ISP) на луче Динамической многоточечной VPN (DMVPN) через Виртуальную маршрутизацию и Облегченную Передачей (Облегченную VRF) функцию.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с этими темами перед попыткой конфигурации, которая описана в этом документе:

- Базовые знания о VRF
- Базовые знания о Протоколе EIGRP
- Базовые знания о DMVPN

Используемые компоненты

Сведения в этом документе основываются на Cisco IOS® Version 15.4 (2) T.

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

VRF является технологией, включенной в маршрутизаторы IP - сети, который позволяет множественным случаям таблицы маршрутизации сосуществовать в маршрутизаторе и работать одновременно. Это увеличивает функциональность, потому что она позволяет сетевым путям быть сегментированными без использования составных устройств.

Использование двойных интернет-провайдеров для резервирования стало общей практикой. Администраторы используют два канала поставщика; каждый действует как первичное соединение и другие действия как резервное подключение.

То же понятие может быть внедрено для резервирования DMVPN на луче с использованием двойных интернет-провайдеров. Цель этого документа состоит в том, чтобы продемонстрировать, как *Облегченный VRF* может использоваться для разделения таблицы маршрутизации, когда луч имеет двойных интернет-провайдеров. Динамическая маршрутизация используется для обеспечения избыточности путей для трафика, который пересекает туннель DMVPN. Примеры конфигурации, которые описаны в этом документе, используют эту схему конфигурации:

Interface	IP-адрес	VRF	Описание
Ethernet 0/0	172.16.1.1	ISP 1 VRF	Основной поставщик услуг Интернет
Ethernet 0/1	172.16.2.1	ISP 2 VRF	Вторичный интернет-провайдер

С Облегченной VRF функцией множественная Маршрутизация VPN / экземпляры VRF может поддерживаться на луче DMVPN. Облегченная VRF функция вынуждает трафик от множественной Многоточечной Универсальной инкапсуляции маршрутизации (mGRE) туннельные интерфейсы использовать их соответствующие таблицы маршрутизации VRF. Например, если основной поставщик услуг Интернет завершается в *ISP1 VRF*, и вторичный

интернет-провайдер завершается в *ISP2 VRF*, трафик, который генерируется в *ISP2 VRF*, использует таблицу маршрутизации VRF *ISP2*, в то время как трафик, который генерируется в *ISP1 VRF*, использует таблицу маршрутизации VRF *ISP1*.

Преимущество, которое идет с использованием *наружного* VRF (FVRF), должно прежде всего вырезать таблицу отдельной маршрутизации от таблицы глобальной маршрутизации (где туннельные интерфейсы существуют). Преимущество с использованием *внутреннего* VRF (iVRF) должно определить личное пространство для удержания информации о частной сети и DMVPN. Обе из этих конфигураций предоставляют дополнительную безопасность от атак на маршрутизатор из Интернета, где разделены сведения о маршрутизации.

Эти конфигурации VRF могут использоваться на обоих концентратор DMVPN и луч. Это дает большое преимущество перед сценарием, в котором оба из интернет-провайдеров завершаются в таблице глобальной маршрутизации.

Если оба из интернет-провайдеров завершаются в глобальном VRF, они совместно используют ту же таблицу маршрутизации, и оба из интерфейсов mGRE полагаются на глобальные сведения о маршрутизации. В этом случае, если основной поставщик услуг Интернет отказывает, интерфейс основного поставщика услуг Интернет не мог бы выключиться, если место ошибки находится в магистральной сети интернет-провайдеров и не непосредственно связано. Это приводит к сценарию, где оба из туннельных интерфейсов MGRE все еще используют маршрут по умолчанию, который указывает к основному поставщику услуг Интернет, который заставляет резервирование DMVPN отказывать.

Хотя существуют некоторые обходные пути, которые используют соглашения об Уровне IP-сервиса (IP SLA) или сценарии встроенного диспетчера событий (EEM) для решения этой проблемы без Облегченного VRF, они не могли бы всегда быть лучшим выбором.

Методы развертываний

Этот раздел предоставляет краткие обзоры туннелей конечного маршрутизатор - конечного маршрутизатора и разделенного туннелирования.

Раздельное туннелирование

Когда определенные подсети или итоговые маршруты изучены через интерфейс mGRE, тогда это называют *разделенным туннелированием*. Если маршрут по умолчанию изучен через интерфейс mGRE, то это называют *туннелем - все*.

Пример конфигурации, который предоставлен в этом документе, основывается на разделенном туннелировании.

Туннели конечного маршрутизатор - конечного маршрутизатора

Пример конфигурации, который предоставлен в этом документе, является хорошим дизайном для туннеля - весь метод развертываний (маршрут по умолчанию изучен через интерфейс mGRE).

Использование двух FVRF выделяет таблицы маршрутизации и гарантирует, что

инкапсулированные пакеты пост-GRE переданы соответствующему FVRF, который помогает гарантировать, что туннель конечного маршрутизатор - конечного маршрутизатора придумывает активного интернет-провайдера.

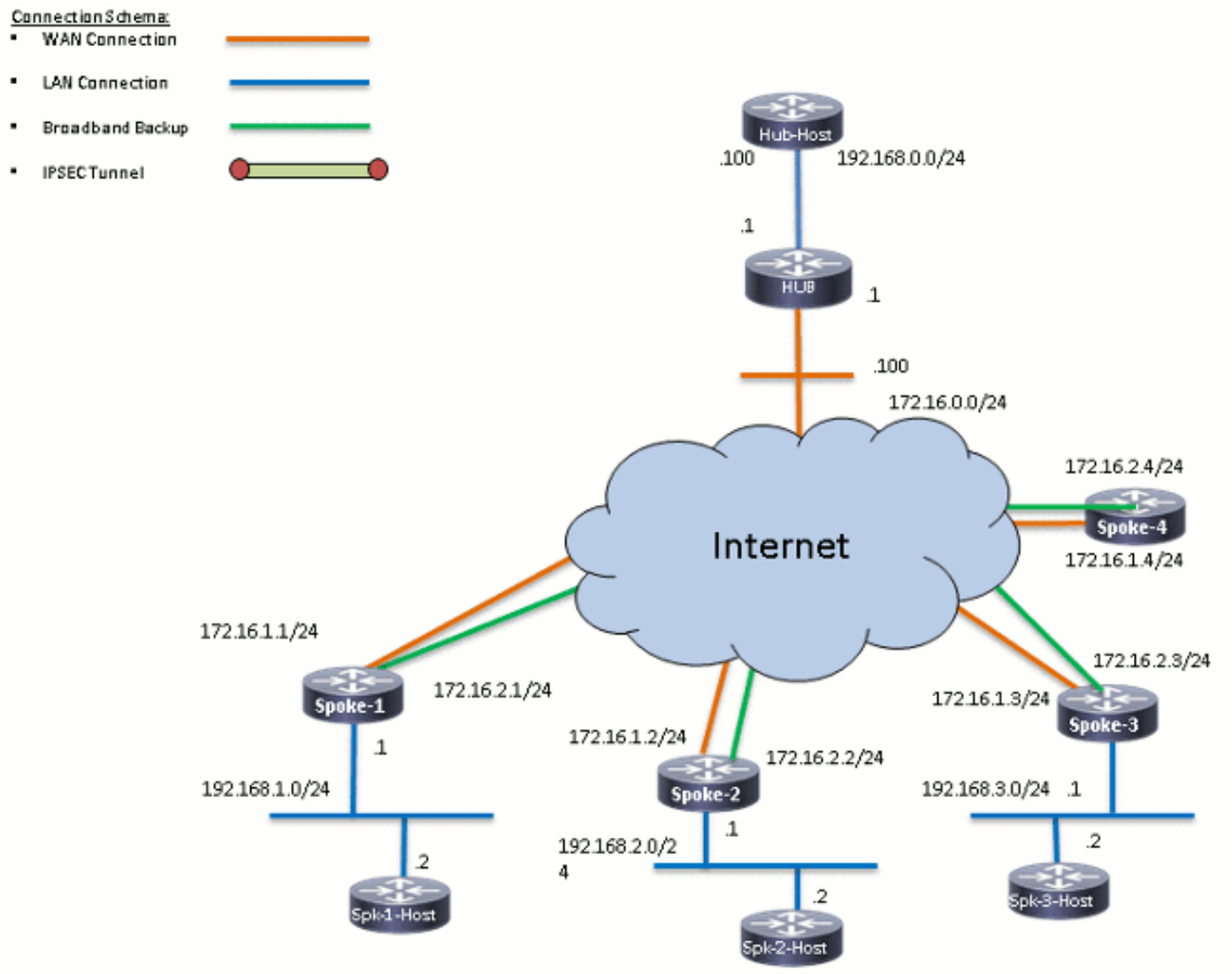
Настройка

В этом разделе описывается настроить резервирование интернет-провайдера на луче DMVPN через Облегченную VRF функцию.

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

Схема сети

Это - топология, которая используется для примеров в этом документе:



Конфигурация концентратора

Вот некоторые примечания о соответствующей конфигурации на концентраторе:

- Для установки *Tunnel0* как основного интерфейса в этом примере конфигурации *параметр задержки* был изменен, который позволяет маршруты, которые изучены из *Tunnel0* для становления более предпочтительными.

- **Совместно используемое** ключевое слово используется с tunnel protection, и *ключ уникального туннеля* добавлен на всех интерфейсах mGRE, потому что они используют тот же *<interface> точки начала туннеля*. В противном случае входящие пакеты Туннеля универсальной инкапсуляции маршрутизации (GRE) могли бы плыться на плоскодонке к неправильному туннельному интерфейсу после расшифровки.

- Объединение маршрутов выполнено, чтобы гарантировать, что все лучи изучают маршрут по умолчанию через туннели mGRE (**туннель - все**).

  Примечание: Только соответствующие разделы конфигурации включены в данный пример.

```
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HUB1
!
crypto isakmp policy 1
 encr aes 256
 hash sha256
 authentication pre-share
 group 24
crypto isakmp key cisco123 address 0.0.0.0
!
crypto ipsec transform-set transform-dmvpn esp-aes 256 esp-sha256-hmac
 mode transport
!
crypto ipsec profile profile-dmvpn
 set transform-set transform-dmvpn
!
interface Loopback0
 description LAN
 ip address 192.168.0.1 255.255.255.0
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 no ip split-horizon eigrp 1
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 ip nhrp redirect
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile profile-dmvpn shared
```

```
!
interface Tunnel1
 bandwidth 1000
 ip address 10.0.1.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 no ip split-horizon eigrp 1
 ip nhrp map multicast dynamic
 ip nhrp network-id 100001
 ip nhrp holdtime 600
 ip nhrp redirect
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0
 ip tcp adjust-mss 1360
 delay 1500
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100001
 tunnel protection ipsec profile profile-dmvpn shared
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
!
ip route 0.0.0.0 0.0.0.0 172.16.0.100
!
end
```

Конфигурация оконечного устройства

Вот некоторые примечания о соответствующей конфигурации на луче:

- Для лучевого резервирования *Tunnel0* и *Tunnel1* имеют *Ethernet0/0* и *Ethernet0/1*, поскольку точка начала туннеля взаимодействует, соответственно. Ethernet0/0 связан с основным поставщиком услуг Интернет, и Ethernet0/1 связан со вторичным интернет-провайдером.

- Для разделения интернет-провайдеров функция VRF использована. Основной поставщик услуг Интернет использует *ISP1 VRF*. Для вторичного интернет-провайдера настроен VRF под названием *ISP2*.

- *ISP1 tunnel vrf* и *tunnel vrf, ISP2* настроены на Tunnel0 интерфейсов и Tunnel1, соответственно, чтобы указать, что поиск пересылки для инкапсулированного пакета пост-GRE выполнен или в VRF ISP1 или в ISP2.

- Для установки Tunnel0 как основного интерфейса в этом примере конфигурации *параметр задержки* был изменен, который позволяет маршруты, которые изучены из Tunnel0 для становления более предпочтительными.

  Примечание: Только соответствующие разделы конфигурации включены в данный пример.

```
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
!
hostname SPOKE1
!
vrf definition ISP1
 rd 1:1
 !
 address-family ipv4
 exit-address-family
!
vrf definition ISP2
 rd 2:2
 !
 address-family ipv4
 exit-address-family
!
crypto keyring ISP2 vrf ISP2
 pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
crypto keyring ISP1 vrf ISP1
 pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 1
 encr aes 256
 hash sha256
 authentication pre-share
 group 24
crypto isakmp keepalive 10 periodic
!
crypto ipsec transform-set transform-dmvpn esp-aes 256 esp-sha256-hmac
 mode transport
!
!
crypto ipsec profile profile-dmvpn
 set transform-set transform-dmvpn
!
interface Loopback10
 ip address 192.168.1.1 255.255.255.0
!
interface Tunnel0
 description Primary mGRE interface source as Primary ISP
 bandwidth 1000
 ip address 10.0.0.10 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.0.1 nbma 172.16.0.1 multicast
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel vrf ISP1
 tunnel protection ipsec profile profile-dmvpn
!
interface Tunnel1
 description Secondary mGRE interface source as Secondary ISP
 bandwidth 1000
 ip address 10.0.1.10 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp network-id 100001
 ip nhrp holdtime 360
 ip nhrp nhs 10.0.1.1 nbma 172.16.0.1 multicast
```

```
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 delay 1500
 tunnel source Ethernet0/1
 tunnel mode gre multipoint
 tunnel key 100001
 tunnel vrf ISP2
 tunnel protection ipsec profile profile-dmvpn
!
interface Ethernet0/0
 description Primary ISP
 vrf forwarding ISP1
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet0/1
 description Seconday ISP
 vrf forwarding ISP2
 ip address 172.16.2.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
!
ip route vrf ISP1 0.0.0.0 0.0.0.0 172.16.1.254
ip route vrf ISP2 0.0.0.0 0.0.0.0 172.16.2.254
!
logging dmvpn
!
end
```

Проверка

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

Основные и вторичные активные интернет-провайдеры

В этом сценарии проверки и основные и вторичные интернет-провайдеры активны. Вот некоторые дополнительные примечания об этом сценарии:

- Фаза 1 и фаза 2 для обоих из интерфейсов mGRE подключены.
- Оба из туннелей подходят, но предпочтены маршруты через Tunnel0 (полученный через основного поставщика услуг Интернет).

Вот соответствующие **команды показа**, которые можно использовать для проверки конфигурации в этом сценарии:

```
SPOKE1#show ip route
<snip>
Gateway of last resort is 10.0.0.1 to network 0.0.0.0

D*   0.0.0.0/0 [90/2944000] via 10.0.0.1, 1w0d, Tunnel0

!--- This is the default route for all of the spoke and hub LAN segments.

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
```

```
C       10.0.0.0/24 is directly connected, Tunnel0
L       10.0.0.10/32 is directly connected, Tunnel0
C       10.0.1.0/24 is directly connected, Tunnel1
L       10.0.1.10/32 is directly connected, Tunnel1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Loopback10
L       192.168.1.1/32 is directly connected, Loopback10

SPOKE1#show ip route vrf ISP1

Routing Table: ISP1
<snip>

Gateway of last resort is 172.16.1.254 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 172.16.1.254
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.0/24 is directly connected, Ethernet0/0
L       172.16.1.1/32 is directly connected, Ethernet0/0

SPOKE1#show ip route vrf ISP2

Routing Table: ISP2
<snip>

Gateway of last resort is 172.16.2.254 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 172.16.2.254
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.2.0/24 is directly connected, Ethernet0/1
L       172.16.2.1/32 is directly connected, Ethernet0/1

SPOKE1#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.

 IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.2.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.

 IPSEC FLOW: permit 47 host 172.16.2.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map
```

Основной поставщик услуг Интернет Выключенный/Вторичный Активный интернет-провайдер

В этом сценарии *Таймеры ожидания* EIGRP истекают для соседства через Tunnel0, когда ссылка ISP1 выключается, и маршруты к концентратору и другим лучам теперь указывают к

Tunnel1 (полученный с Ethernet0/1).

Вот соответствующие **команды показа**, которые можно использовать для проверки конфигурации в этом сценарии:

```
*Sep 2 14:07:33.374: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is down: holding time expired

SPOKE1#show ip route
<snip>

Gateway of last resort is 10.0.1.1 to network 0.0.0.0

D*   0.0.0.0/0 [90/3072000] via 10.0.1.1, 00:00:20, Tunnel1

!--- This is the default route for all of the spoke and hub LAN segments.

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.0.0.0/24 is directly connected, Tunnel0
L       10.0.0.10/32 is directly connected, Tunnel0
C       10.0.1.0/24 is directly connected, Tunnel1
L       10.0.1.10/32 is directly connected, Tunnel1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Loopback10
L       192.168.1.1/32 is directly connected, Loopback10

SPOKE1#show ip route vrf ISP1

Routing Table: ISP1
<snip>

Gateway of last resort is 172.16.1.254 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 172.16.1.254
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.0/24 is directly connected, Ethernet0/0
L       172.16.1.1/32 is directly connected, Ethernet0/0

SPOKE1#show ip route vrf ISP2

Routing Table: ISP2
<snip>

Gateway of last resort is 172.16.2.254 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 172.16.2.254
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.2.0/24 is directly connected, Ethernet0/1
L       172.16.2.1/32 is directly connected, Ethernet0/1

SPOKE1#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: DOWN
Peer: 172.16.0.1 port 500
 IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.0.1

!--- Tunnel0 is Inactive and the routes are preferred via Tunnel1.

       Active SAs: 0, origin: crypto map

Interface: Tunnel1
```

```
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.2.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Inactive and the routes are preferred via Tunnel1.

 IPSEC FLOW: permit 47 host 172.16.2.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map

Interface: Tunnel0
Session status: DOWN-NEGOTIATING
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Inactive

!--- Tunnel0 is Inactive and the routes are preferred via Tunnel1.

 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Inactive
```

Восстановление ссылки основного поставщика услуг Интернет

Когда подключение через основного поставщика услуг Интернет восстановлено, сеанс шифрования Tunnel0 становится активным, и маршруты, которые изучены через интерфейс Tunnel0, предпочтены.

Например:

```
*Sep 2 14:15:59.128: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is up: new adjacency

SPOKE1#show ip route
<snip>

Gateway of last resort is 10.0.0.1 to network 0.0.0.0

D*   0.0.0.0/0 [90/2944000] via 10.0.0.1, 00:00:45, Tunnel0

!--- This is the default route for all of the spoke and hub LAN segments.

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.0.0.0/24 is directly connected, Tunnel0
L       10.0.0.10/32 is directly connected, Tunnel0
C       10.0.1.0/24 is directly connected, Tunnel1
L       10.0.1.10/32 is directly connected, Tunnel1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Loopback10
L       192.168.1.1/32 is directly connected, Loopback10

SPOKE1#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.
```

```
 IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.2.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.

 IPSEC FLOW: permit 47 host 172.16.2.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map
```

Устранение неполадок

Для устранения проблем конфигурации включите **eigrp ip отладки** и **logging dmvpn**.

Например:

```
################## Tunnel0 Failed and Tunnel1 routes installed ####################

*Sep 2 14:07:33.374: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is down: holding time expired
*Sep 2 14:07:33.374: EIGRP-IPv4(1): table(default): route installed for 0.0.0.0/0
(90/3072000) origin(10.0.1.1)
*Sep 2 14:07:33.391: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel1
*Sep 2 14:07:33.399: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel1
*Sep 2 14:07:36.686: %DMVPN-5-CRYPTO_SS: Tunnel0: local address : 172.16.1.1 remote
address : 172.16.0.1 socket is DOWN
*Sep 2 14:07:36.686: %DMVPN-5-NHRP_NHS_DOWN: Tunnel0: Next Hop Server : (Tunnel:
10.0.0.1 NBMA: 172.16.0.1 ) for (Tunnel: 10.0.0.10 NBMA: 172.16.1.1) is DOWN, Reason:
External(NHRP: no error)

################## Tunnel0 came up and routes via Tunnel0 installed #################

*Sep 2 14:15:55.120: %DMVPN-5-CRYPTO_SS: Tunnel0: local address : 172.16.1.1 remote
address : 172.16.0.1 socket is UP
*Sep 2 14:15:56.109: %DMVPN-5-NHRP_NHS_UP: Tunnel0: Next Hop Server : (Tunnel:
10.0.0.1 NBMA: 172.16.0.1) for (Tunnel: 10.0.0.10 NBMA: 172.16.1.1) is UP
*Sep 2 14:15:59.128: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is up: new adjacency
*Sep 2 14:16:01.197: EIGRP-IPv4(1): table(default): route installed for 0.0.0.0/0
(90/3072000) origin(10.0.1.1)
*Sep 2 14:16:01.197: EIGRP-IPv4(1): table(default): route installed for 0.0.0.0/0
(90/2944000) origin(10.0.0.1)
*Sep 2 14:16:01.214: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel0
*Sep 2 14:16:01.214: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel1
```

Дополнительные сведения

- Наиболее распространенные решения для устранения проблем DMVPN
- Руководство по поиску и устранению проблем Семейства Cisco MDS 9000, IPsec

Устранения проблем выпуска 2.x Г¦

- Cisco Systems – техническая поддержка и документация