

# FlexVPN: IPv6 в концентраторе и лучевом примере конфигурации при развертывании

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Настройка](#)

[Схема сети](#)

[Транспортная сеть](#)

[Оверлейная сеть](#)

[Конфигурации](#)

[Протоколы маршрутизации](#)

[Конфигурация концентратора](#)

[Конфигурация оконечного устройства](#)

[Проверка](#)

[Сеанс оконечного устройства - концентратора](#)

[Сеанс конечного маршрутизатор - конечного маршрутизатора](#)

[Устранение неполадок](#)

## Введение

Этот документ описывает обычную конфигурацию, которая использует Cisco FlexVPN, которую IOS® говорил и развертывания концентратора в среде IPv6. Это подробно останавливается на понятиях, обсужденных в [FlexVPN: IPv6 Основная LAN к конфигурации LAN](#).

## Предварительные условия

### Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco IOS FlexVPN
- Протоколы маршрутизации

### Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Поколение 2 Cisco ISR (ISR G2)
- Cisco IOS Software Release 15.3 (или Выпуск 15.4Т для динамического конечного маршрутизатор - конечного маршрутизатора туннелирует с IPv6),

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.

## Настройка

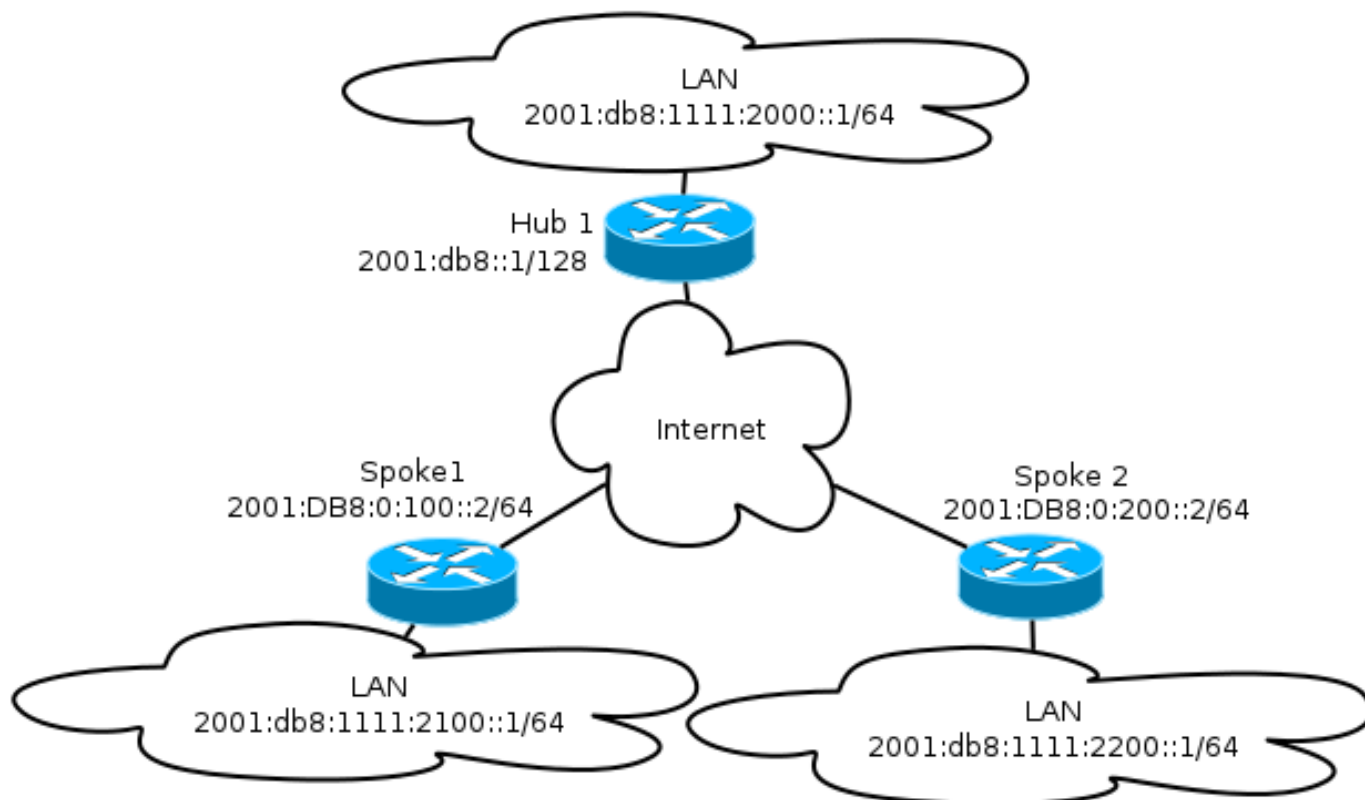
**Примечание:** [Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд \(только для зарегистрированных клиентов\).](#)

В то время как этот пример конфигурации и IPv6 использования схемы сети как транспортная сеть, Универсальная инкапсуляция маршрутизации (GRE), как правило, используется в развертываниях FlexVPN. Использование GRE вместо IPsec позволяет администраторам выполнять IPv4 или IPv6 или обоих по тем же туннелям, независимо от транспортной сети.

## Схема сети

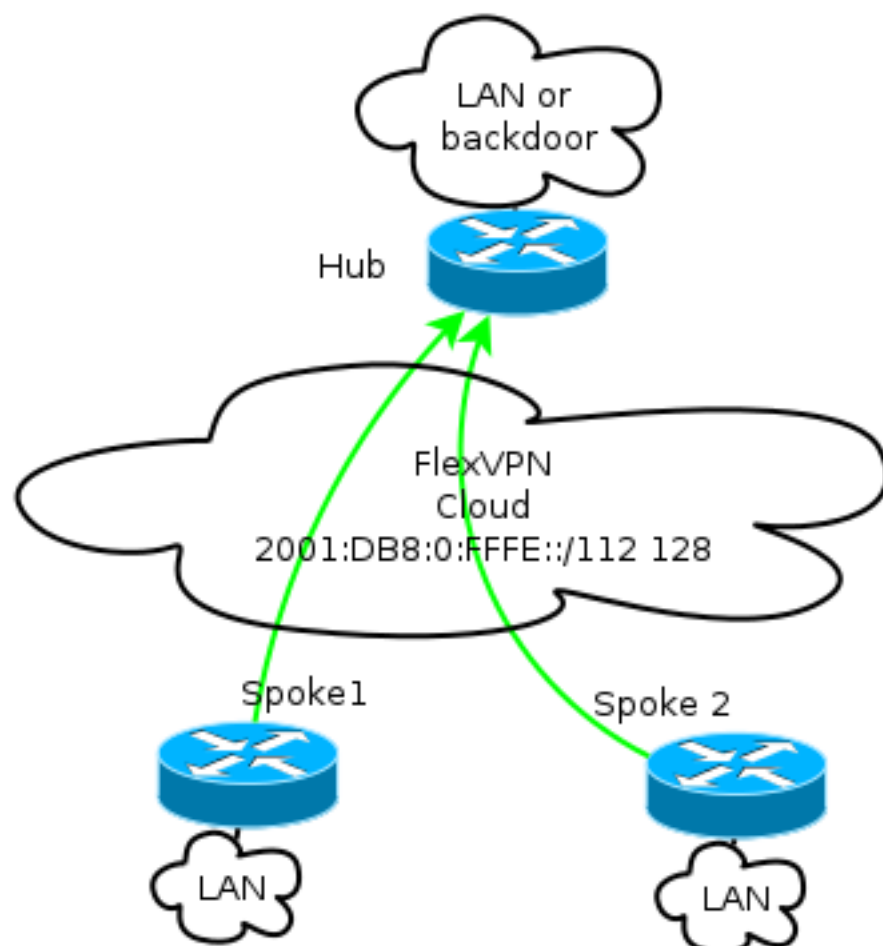
### Транспортная сеть

Это - схема транспортной сети, используемой в данном примере:



### Оверлейная сеть

Это - схема основной топологии оверлейной сети, используемой в данном примере:



Каждый луч назначен от пула адресов/112, но получает адрес/128. Таким образом нотация '/112 128' используется в конфигурации пула IPv6 концентратора.

## Конфигурации

Эта конфигурация показывает IPv4 и наложение IPv6, которое перерабатывает магистраль IPv6.

Когда по сравнению с примерами, которые используют IPv4 в качестве магистрали, обратите внимание, что необходимо использовать команду **tunnel mode**, чтобы к узлу изменяют и принимают транспорт IPv6.

Туннельная функция конечного маршрутизатор - конечного маршрутизатора по IPv6 будет представлена в Cisco IOS Software Release 15.4T, который еще не доступен.

## Протоколы маршрутизации

Cisco рекомендует использовать внутренний протокол граничного шлюза (iBGP) для пиринга между лучом и концентраторами для больших развертываний, потому что iBGP является большей частью протокола масштабируемой маршрутизации.

Протокол BGP слушает, диапазон не поддерживает диапазон IPv6, но это действительно упрощает использование с транспортом IPv4. Несмотря на то, что выполнимо использовать BGP в такой среде, эта конфигурация иллюстрирует базовый пример, таким образом, был выбран Протокол EIGRP.

## Конфигурация концентратора

По сравнению с более старыми примерами эта конфигурация включает использование новых транспортных протоколов.

Для настройки концентратора администратор должен:

- Включите одноадресную маршрутизацию.
- Маршрутизация транспорта условия.
- Настройте новый пул адресов IPv6, которые будут назначены динамично. Пул 2001:DB8:0:FFFE::/112; 16 битов обеспечивают 65,535 устройств, которые будут обращены.
- Включите IPv6 для конфигурации Протокола NHRP для разрешения IPv6 в наложении.
- Учетная запись на адресацию IPv6 в брелоке, а также профиль в крипте - настройке.

В данном примере концентратор объявляет сводку EIGRP ко всем лучам.

Cisco не рекомендует использование сводного адреса на Виртуальном интерфейсе в развертываниях FlexVPN; однако, в Динамической многоточечной VPN (DMVPN), это не только распространено, но и также считается оптимальным методом. Посмотрите [Миграцию FlexVPN: Твердое Перемещение от DMVPN до FlexVPN на Тех же Устройствах: Обновленная конфигурация концентратора](#) для подробных данных.

```

ipv6 unicast-routing
ipv6 cef

ip local pool FlexSpokes 10.1.1.176 10.1.1.254
ipv6 local pool FlexSpokesv6 2001:DB8:0:FFFE::/112 128

crypto ikev2 authorization policy default
  ipv6 pool FlexSpokesv6
pool FlexSpokes
route set interface
crypto ikev2 keyring Flex_key
peer ALL
address ::/0
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile Flex_IKEv2
match identity remote address ::/0
authentication remote pre-share
authentication local pre-share
keyring local Flex_key
aaa authorization group psk list default default
virtual-template 1

crypto ikev2 dpd 30 5 on-demand

interface Virtual-Templatel type tunnel
ip unnumbered Loopback100
ip mtu 1400
ip nhrp network-id 2
ip nhrp redirect
ip tcp adjust-mss 1360
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
  ipv6 unnumbered Loopback100
ipv6 enable
ipv6 eigrp 65001
  ipv6 nhrp network-id 2
  ipv6 nhrp redirect
  tunnel mode gre ipv6
tunnel protection ipsec profile default

interface Ethernet1/0
description LAN subnet
ip address 192.168.0.1 255.255.255.0
ipv6 address 2001:DB8:1111:2000::1/64
ipv6 enable
ipv6 eigrp 65001

interface Loopback0
ip address 172.25.1.1 255.255.255.255
ipv6 address 2001:DB8::1/128
ipv6 enable

ip route 192.168.0.0 255.255.0.0 Null0
ipv6 route 2001:DB8:1111::/48 Null0

ip prefix-list EIGRP_SUMMARY_ONLY seq 5 permit 192.168.0.0/16
ipv6 prefix-list EIGRP_SUMMARY_v6 seq 5 permit 2001:DB8:1111::/48

router eigrp 65001
  distribute-list prefix EIGRP_SUMMARY_ONLY out Virtual-Templatel
  network 10.1.1.0 0.0.0.255
  network 192.168.0.0 0.0.255.255

```

```
redistribute static metric 1500 10 10 1 1500
```

```
ipv6 router eigrp 65001  
  distribute-list prefix-list EIGRP_SUMMARY_v6 out Virtual-Template1  
  redistribute static metric 1500 10 10 1 1500
```

## Конфигурация оконечного устройства

Как в [конфигурации концентратора](#), администратору нужно к адресации условия IPv6, включить маршрутизацию IPv6 и добавьте NHRP и крипто - настройку.

Выполнимо использовать EIGRP и другие протоколы маршрутизации для пиринга конечного маршрутизатор - конечного маршрутизатора. Однако в типичном сценарии, протоколы не необходимы и могли бы повлиять на масштабируемость и устойчивость.

В данном примере настройка маршрутизации поддерживает только смежность EIGRP между лучом и концентратором, и единственный интерфейс, который не пассивен, является интерфейсом Tunnel1:

```
ipv6 unicast-routing  
ipv6 cef  
  
crypto logging session  
  
crypto ikev2 authorization policy default  
route set interface  
crypto ikev2 keyring Flex_key  
peer ALL  
address ::/0  
pre-shared-key local cisco  
pre-shared-key remote cisco  
!  
crypto ikev2 profile Flex_IKEv2  
match identity remote address ::/0  
authentication remote pre-share  
authentication local pre-share  
keyring local Flex_key  
aaa authorization group psk list default default  
virtual-template 1  
  
crypto ikev2 dpd 30 5 on-demand  
  
interface Tunnel1  
description FlexVPN tunnel  
ip address negotiated  
ip mtu 1400  
ip nhrp network-id 2  
ip nhrp shortcut virtual-template 1  
ip nhrp redirect  
ip tcp adjust-mss 1360  
delay 1000  
ipv6 mtu 1400  
ipv6 tcp adjust-mss 1358  
ipv6 address negotiated  
  ipv6 enable  
  ipv6 nhrp network-id 2  
  ipv6 nhrp shortcut virtual-template 1  
  ipv6 nhrp redirect  
tunnel source Ethernet0/0  
  tunnel mode gre ipv6
```

```
tunnel destination 2001:DB8::1
tunnel protection ipsec profile default
```

```
interface Virtual-Templatel type tunnel
ip unnumbered Ethernet1/0
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
delay 1000
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
  ipv6 unnumbered Ethernet1/0
ipv6 enable
  ipv6 nhrp network-id 2
  ipv6 nhrp shortcut virtual-template 1
  ipv6 nhrp redirect
tunnel mode gre ipv6
tunnel protection ipsec profile default
```

Придерживайтесь этих рекомендаций при создании записей протокола маршрутизации на луче:

1. Позвольте протоколу маршрутизации устанавливать отношение через соединение (в этом случае, интерфейс Tunnel1) к концентратору. Обычно не выбираемо установить смежность маршрутизации между лучами, потому что это значительно увеличивает сложность в большинстве случаев.
2. Объявите подсеть (подсети) локальной сети только и включите протокол маршрутизации на IP-адресе, назначенном концентратором. Бойтесь объявлять большую подсеть, потому что она могла бы повлиять на связь конечного маршрутизатор - конечного маршрутизатора.

Данный пример отражает обе рекомендации для EIGRP на Spoke1:

```
ipv6 unicast-routing
ipv6 cef
```

```
crypto logging session
```

```
crypto ikev2 authorization policy default
route set interface
crypto ikev2 keyring Flex_key
peer ALL
address ::/0
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile Flex_IKEv2
match identity remote address ::/0
authentication remote pre-share
authentication local pre-share
keyring local Flex_key
aaa authorization group psk list default default
virtual-template 1
```

```
crypto ikev2 dpd 30 5 on-demand
```

```
interface Tunnel1
description FlexVPN tunnel
```

```
ip address negotiated
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
delay 1000
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
ipv6 address negotiated
  ipv6 enable
  ipv6 nhrp network-id 2
  ipv6 nhrp shortcut virtual-template 1
  ipv6 nhrp redirect
tunnel source Ethernet0/0
  tunnel mode gre ipv6
tunnel destination 2001:DB8::1
tunnel protection ipsec profile default

interface Virtual-Templatel type tunnel
ip unnumbered Ethernet1/0
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
delay 1000
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
  ipv6 unnumbered Ethernet1/0
ipv6 enable
  ipv6 nhrp network-id 2
  ipv6 nhrp shortcut virtual-template 1
  ipv6 nhrp redirect
tunnel mode gre ipv6
tunnel protection ipsec profile default
```

## Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

**Примечание:** [Средство интерпретации выходных данных \(только зарегистрированные клиенты\)](#) поддерживает некоторые команды show. Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.

## Сеанс окончного устройства - концентратора

Должным образом настроенный сеанс между лучом и устройствами концентратора имеет сеанс второй версии протокола Internet Key Exchange (IKEv2), который подключен и имеет протокол маршрутизации, который может установить смежность. В данном примере протокол маршрутизации является EIGRP, таким образом, существует две Команды EIGRP:

- **show crypto ikev2 sa**
- **show ipv6 eigrp 65001 соседний узел**



- **show ip eigrp 65001 соседний узел**

```
Spokel#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA
```

**IPv6 Crypto IKEv2 SA**

```
Tunnel-id   fvrf/ivrf           Status
1           none/none          READY
Local 2001:DB8:0:100::2/500
Remote 2001:DB8::1/500
  Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
  Life/Active Time: 86400/1945 sec
```

```
Spokel#sh ipv6 eigrp 65001 neighbor
EIGRP-IPv6 Neighbors for AS(65001)
```

| H | Address   | Interface | Hold (sec) | Uptime   | SRTT (ms) | RTO  | Q | Seq Cnt | Num |
|---|---|-----------|------------|----------|-----------|------|---|---------|-----|
| 0 | Link-local address:<br><b>FE80::A8BB:CCFF:FE00:6600</b> | Tu1       | 14         | 00:32:29 | 72        | 1470 | 0 | 10      |     |

```
Spokel#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(65001)
```

| H | Address  | Interface | Hold (sec) | Uptime   | SRTT (ms) | RTO  | Q | Seq Cnt | Num |
|---|----------|-----------|------------|----------|-----------|------|---|---------|-----|
| 0 | 10.1.1.1 | Tu1       | 11         | 00:21:05 | 11        | 1398 | 0 | 26      |     |

В IPv4 EIGRP использует назначенный IP - адрес для пиринга; в предыдущем примере это - IP-адрес концентратора 10.1.1.1.

IPv6 использует локальный для канала адрес; в данном примере концентратор является FE80:: A8BB:CCFF:FE00:6600. Используйте команду ping, чтобы проверить, что концентратор может быть достигнут через его локального для канала IP:

```
Spokel#ping FE80::A8BB:CCFF:FE00:6600
Output Interface: tunnell
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::A8BB:CCFF:FE00:6600, timeout is
2 seconds:
Packet sent with a source address of FE80::A8BB:CCFF:FE00:6400%Tunnell
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/5 ms
```

## Сеанс конечного маршрутизатор - конечного маршрутизатора

Сеансы конечного маршрутизатор - конечного маршрутизатора переведены в рабочее состояние динамично по требованию. Используйте команду простой проверки связи с помощью команды ping для инициирования сеанса:

```
Spokel#ping FE80::A8BB:CCFF:FE00:6600
Output Interface: tunnell
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::A8BB:CCFF:FE00:6600, timeout is
2 seconds:
Packet sent with a source address of FE80::A8BB:CCFF:FE00:6400%Tunnell
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/5 ms
```

Для подтверждения прямого подключения конечного маршрутизатор - конечного маршрутизатора администратор должен:

- Проверьте, что динамический сеанс конечного маршрутизатор - конечного маршрутизатора инициирует новый Интерфейс виртуального доступа:

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed
state to up
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP.
Peer 2001:DB8:0:200::2:500      Id: 2001:DB8:0:200::2
```

- Проверьте состояние сеанса IKEv2:

```
Spoke1#show crypto ikev2 sa
  IPv4 Crypto IKEv2 SA
```

```
  IPv6 Crypto IKEv2 SA
```

```
Tunnel-id  fvrf/ivrf          Status
1           none/none        READY
Local 2001:DB8:0:100::2/500
Remote 2001:DB8::1/500
  Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK,
Auth verify: PSK
  Life/Active Time: 86400/3275 sec
```

```
Tunnel-id  fvrf/ivrf          Status
2           none/none        READY
Local 2001:DB8:0:100::2/500
Remote 2001:DB8:0:200::2/500
  Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK,
Auth verify: PSK
  Life/Active Time: 86400/665 sec
```

Обратите внимание на то, что два сеанса доступны: одно оконечное устройство - концентратор и один конечный маршрутизатор - конечный маршрутизатор.

- Проверьте NHRP:

```
Spoke1#show ipv6 nhrp
2001:DB8:0:FFFE::/128 via 2001:DB8:0:FFFE::
Virtual-Access1 created 00:00:10, expire 01:59:49
Type: dynamic, Flags: router nhop rib nho
NBMA address: 2001:DB8:0:200::2
2001:DB8:1111:2200::/64 via 2001:DB8:0:FFFE::
Virtual-Access1 created 00:00:10, expire 01:59:49
Type: dynamic, Flags: router rib nho
```

Выходные данные показывают, что 2001:DB8:1111:2200::/64 (LAN для Spoke2) доступно через 2001:DB8:0:FFFE:: который является согласованным адресом IPv6 на интерфейсе Tunnel1 для Spoke2. Интерфейс Tunnel1 доступен через нешироковещательный множественный доступ (NBMA) адрес 2001:db8:0:200:: 2, который является адресом IPv6, назначенным на Spoke2 статически.

- Проверьте, что трафик проходит через тот интерфейс:

```
Spoke1#sh crypto ipsec sa peer 2001:DB8:0:200::2

interface: Virtual-Access1
  Crypto map tag: Virtual-Access1-head-0, local addr 2001:DB8:0:100::2

protected vrf: (none)
local ident (addr/mask/prot/port): (2001:DB8:0:100::2/128/47/0)
remote ident (addr/mask/prot/port): (2001:DB8:0:200::2/128/47/0)
current_peer 2001:DB8:0:200::2 port 500
```

```
PERMIT, flags={origin_is_acl,}
#pkts encaps: 196, #pkts encrypt: 196, #pkts digest: 196
#pkts decaps: 195, #pkts decrypt: 195, #pkts verify: 195
(...)
```

- Проверьте параметры настройки CEF и путь маршрутизации:

```
Spoke1#show ipv6 route
(...)
D 2001:DB8:1111:2200::/64 [90/27161600]
  via 2001:DB8:0:FFFE::, Virtual-Access1 [Shortcut]
  via FE80::A8BB:CCFF:FE00:6600, Tunnell
(...)
Spoke1#show ipv6 cef 2001:DB8:1111:2200::
2001:DB8:1111:2200::/64
  nexthop 2001:DB8:0:FFFE:: Virtual-Access
```

## Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

**Примечание:** [Прежде чем выполнять какие-либо команды отладки, ознакомьтесь с документом "Важные сведения о командах отладки"](#).

Эти команды отладки помогают вам решать проблемы:

- FlexVPN/IKEv2 и IPsec: **debug crypto ipsecdebug crypto ikev2 [packet|internal]**
- NHRP (конечный маршрутизатор - конечный маршрутизатор):
  - пакет **debug nhrp**
  - **debug nhrp extension**
  - кэш **debug nhrp**
  - маршрут **debug nhrp**

См. [Ведущий Список команд Cisco IOS, Все Версии](#) для получения дополнительной информации об этих командах.