FlexVPN:허브 및 스포크 구축 구성의 IPv6 예

목차

소개

이 문서에서는 IPv6 환경에서 Cisco IOS® FlexVPN 스포크 및 허브 구축을 사용하는 공통 컨피그레이션에 대해 설명합니다.FlexVPN에서 설명하는 개념을 [확장합니다.IPv6 기본 LAN-to-LAN 컨피그레이션](#).

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco IOS FlexVPN
- 라우팅 프로토콜

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISR G2(Integrated Services Routers Generation 2)
- Cisco IOS Software 릴리스 15.3(또는 IPv6을 사용하는 동적 스포크 투 스포크 터널의 경우 릴리스 15.4T)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

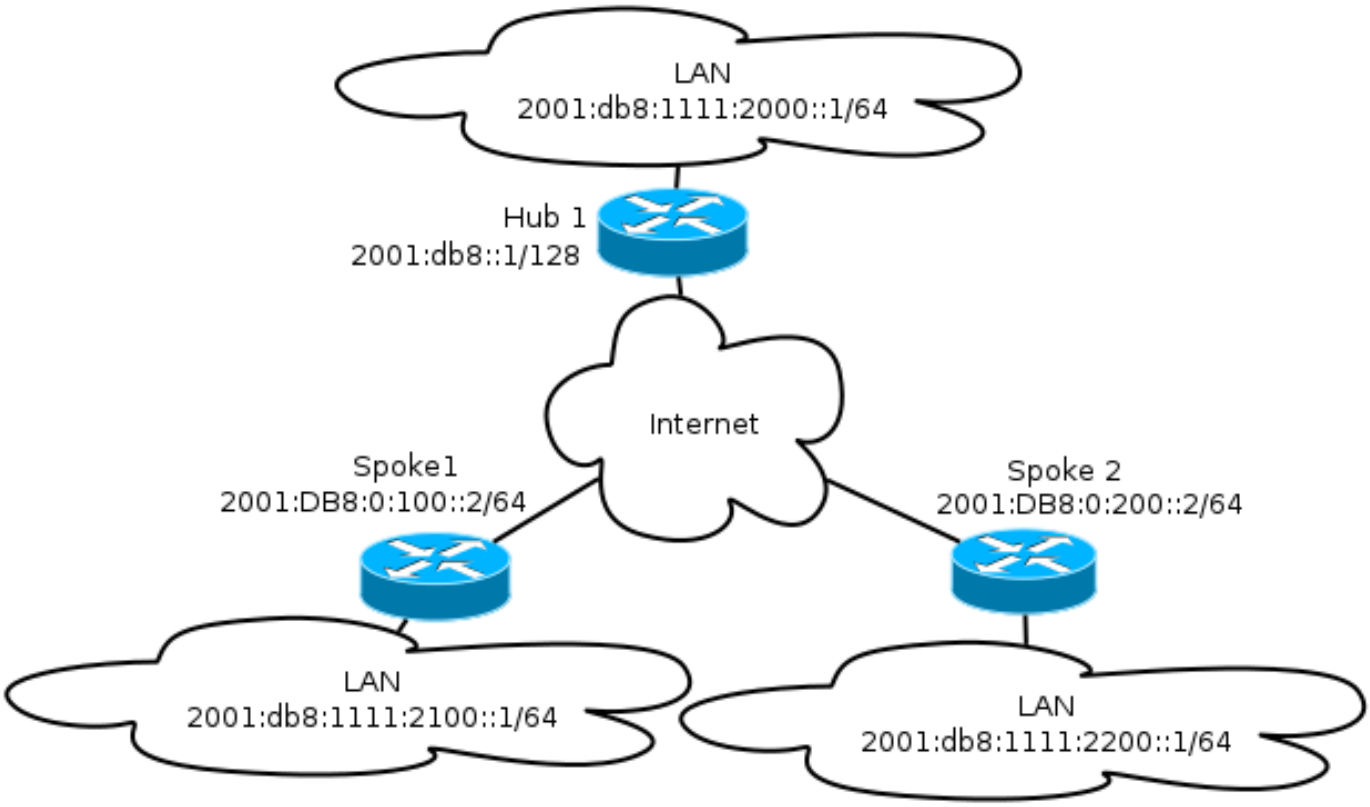
> **참고:**이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

이 컨피그레이션 예와 네트워크 다이어그램은 IPv6을 전송 네트워크로 사용하지만 GRE(Generic Routing Encapsulation)는 일반적으로 FlexVPN 구축에서 사용됩니다.IPsec 대신 GRE를 사용하면 관리자는 전송 네트워크에 관계없이 동일한 터널을 통해 IPv4 또는 IPv6 또는 둘 모두를 실행할 수 있습니다.

네트워크 다이어그램

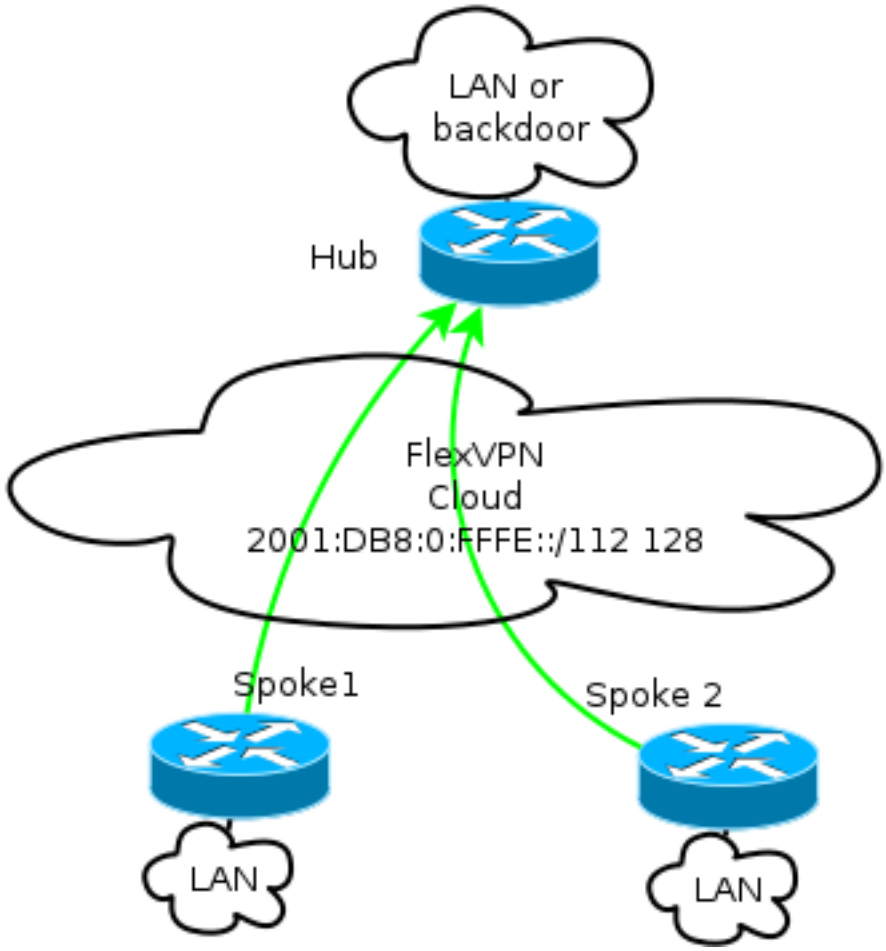
전송 네트워크

이 예에서는 전송 네트워크의 다이어그램입니다.



오버레이 네트워크

이 예에서는 기본 오버레이 네트워크 토폴로지를 나타낸 다이어그램입니다.



모든 스포크는 /112의 주소 풀에서 할당되지만 /128 주소를 수신합니다.따라서 '/112 128' 표기법은 허브의 IPv6 풀 컨피그레이션에 사용됩니다.

구성

이 컨피그레이션에서는 IPv6 백본을 통해 작동하는 IPv4 및 IPv6 오버레이를 보여줍니다.

IPv4를 백본으로 사용하는 예와 비교할 때 노드를 변경하고 IPv6 전송을 수용하려면 **tunnel mode** 명령을 사용해야 합니다.

IPv6를 통한 스포크 투 스포크 터널 기능은 아직 사용할 수 없는 Cisco IOS Software Release 15.4T에 도입됩니다.

라우팅 프로토콜

iBGP는 가장 확장성이 뛰어난 라우팅 프로토콜이므로 대형 구축의 스포크와 허브 간 피어링을 위해 내부 iBGP(Border Gateway Protocol)를 사용하는 것이 좋습니다.

BGP(Border Gateway Protocol) 수신 범위는 IPv6 범위를 지원하지 않지만 IPv4 전송으로 사용을 간소화합니다.이러한 환경에서 BGP를 사용할 수는 있지만 이 컨피그레이션에서는 기본 예를 보여주기 때문에 EIGRP(Enhanced Interior Gateway Routing Protocol)가 선택되었습니다.

허브 구성

이전 예와 달리 이 컨피그레이션에는 새 전송 프로토콜의 사용이 포함됩니다.

허브를 구성하려면 관리자가 다음을 수행해야 합니다.

- 유니캐스트 라우팅을 활성화합니다.
- 전송 라우팅을 프로비저닝합니다.
- 동적으로 할당할 새 IPv6 주소 풀을 프로비저닝합니다.풀은 2001:DB8:0:FFFE::/112;16비트는 65,535개의 장치를 처리할 수 있습니다.
- 오버레이에서 IPv6을 허용하려면 NHRP(Next Hop Resolution Protocol) 컨피그레이션에 IPv6를 활성화합니다.
- 키 링의 IPv6 주소 지정 및 암호화 컨피그레이션의 프로필에 대한 어카운트

이 예에서는 허브가 EIGRP 요약을 모든 스포크에 광고합니다.

Cisco는 FlexVPN 구축에서 가상 템플릿 인터페이스에 요약 주소를 사용하지 않는 것이 좋습니다 .그러나 DMVPN(Dynamic Multipoint VPN)에서는 이 방식이 일반적일 뿐만 아니라 모범 사례로도 간주됩니다.FlexVPN 마이그레이션 참조:동일한 디바이스에서 DMVPN에서 FlexVPN으로 하드 이동:자세한 내용을 위해 허브 구성을 업데이트했습니다.

```
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-Template1 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-Template1
 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
```

스포크 구성

허브 컨피그레이션과 마찬가지로 관리자는 IPv6 주소 지정을 프로비저닝하고 IPv6 라우팅을 활성화하고 NHRP 및 암호화 컨피그레이션을 추가해야 합니다.

EIGRP 및 기타 라우팅 프로토콜을 스포크 투 스포크 피어링에 사용할 수 있습니다.그러나 일반적인 시나리오에서는 프로토콜이 필요하지 않으며 확장성과 안정성에 영향을 줄 수 있습니다.

이 예에서 라우팅 컨피그레이션은 스포크와 허브 사이의 EIGRP 인접성만 유지하며 패시브 인터페이스가 아닌 유일한 인터페이스는 Tunnel1 인터페이스입니다.

```
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-Template1 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
```

스포크에 라우팅 프로토콜 항목을 생성할 때 다음 권장 사항을 따르십시오.

1. 라우팅 프로토콜이 허브에 대한 연결(이 경우 Tunnel1 인터페이스)을 통해 관계를 설정하도록 허용합니다.대부분의 경우 복잡성이 크게 증가하므로 일반적으로 스포크 간 라우팅 인접성을 설정하는 것은 바람직하지 않습니다.

2. 로컬 LAN 서브넷만 알리고, 허브에서 할당한 IP 주소에서 라우팅 프로토콜을 활성화합니다.대형 서브넷은 스포크 투 스포크 통신에 영향을 줄 수 있으므로 광고하지 않도록 주의하십시오.

이 예에서는 Spoke1의 EIGRP에 대한 두 가지 권장 사항을 모두 반영합니다.

```
router eigrp 65001
 network 10.1.1.0 0.0.0.255
 network 192.168.101.0 0.0.0.255
```

```
 passive-interface default
 no passive-interface Tunnel1

ipv6 router eigrp 65001
 passive-interface default
 no passive-interface Tunnel1
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

> **참고:**Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

스포크 투 허브 세션

스포크와 허브 디바이스 간에 올바르게 구성된 세션에는 IKEv2(Internet Key Exchange Version 2) 세션이 있으며 인접성을 설정할 수 있는 라우팅 프로토콜이 있습니다.이 예에서는 라우팅 프로토콜이 EIGRP이므로 두 개의 EIGRP 명령이 있습니다.

- **crypto ikev2 sa 표시**
- **show ipv6 eigrp 65001 neighbor**
- **show ip eigrp 65001 neighbor**

```
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: 86400/1945 sec

Spoke1#sh ipv6 eigrp 65001 neighbor
EIGRP-IPv6 Neighbors for AS(65001)
H   Address                 Interface          Hold Uptime   SRTT   RTO  Q  Seq
                                              (sec)         (ms)       Cnt Num
0   Link-local address:     Tu1                  14 00:32:29   72  1470  0  10
   FE80::A8BB:CCFF:FE00:6600

Spoke1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(65001)
H   Address                 Interface          Hold Uptime   SRTT   RTO  Q  Seq
                                              (sec)         (ms)       Cnt Num
0   10.1.1.1                Tu1                  11 00:21:05   11  1398  0  26
```

IPv4에서 EIGRP는 할당된 IP 주소를 피어에 사용합니다.이전 예에서는 허브 IP 주소가 10.1.1.1입니다.

IPv6는 링크-로컬 주소를 사용합니다.이 예에서 허브는 FE80::A8BB:CCFF:FE00:6600입니다.링크-로컬 IP를 통해 허브에 도달할 수 있는지 확인하려면 ping 명령을 사용합니다.

```
Spoke1#ping FE80::A8BB:CCFF:FE00:6600
Output Interface: tunnel1
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%Tunnel1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/5 ms
```

스포크 투 스포크 세션

Spoke-to-Spoke 세션은 필요에 따라 동적으로 실행됩니다.세션을 트리거하려면 간단한 ping 명령을 사용합니다.

```
Spoke1#ping  2001:DB8:1111:2200::100 source e1/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1111:2200::100, timeout is 2 seconds:
Packet sent with a source address of 2001:DB8:1111:2100::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/8/10 ms
```

직접 스포크 간 연결을 확인하려면 관리자가 다음을 수행해야 합니다.

- 동적 스포크 투 스포크 세션이 새 가상 액세스 인터페이스를 트리거하는지 확인합니다.

```
%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
```

- IKEv2 세션 상태를 확인합니다.

```
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
```

두 개의 세션을 사용할 수 있습니다.스포크 투 허브와 스포크 투 스포크 한 개

- NHRP 확인:

```
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
NBMA address: 2001:DB8:0:200::2
```

출력에 따르면 2001:DB8:1111:2200::/64(Spoke2용 LAN)가 Spoke2의 Tunnel1 인터페이스에서 협상된 IPv6 주소인 2001:DB8:0:FFFE::::::::: Tunnel1 인터페이스는 Non-broadcast multiaccess(NBMA) 주소 2000을 통해 사용할 수 있습니다. 1:db8:0:200::2 - Spoke2에 정적으로 할당된 IPv6 주소입니다.

- 트래픽이 해당 인터페이스를 통해 전달되는지 확인합니다.

```
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
(...)
```

- 라우팅 경로 및 CEF 설정을 확인합니다.

```
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, Tunnel1
(...)
Spoke1#show ipv6 cef 2001:DB8:1111:2200::
2001:DB8:1111:2200::/64
 nexthop 2001:DB8:0:FFFE:: Virtual-Access
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

> **참고:debug** 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

이러한 debug 명령은 문제를 해결하는 데 도움이 됩니다.

- FlexVPN/IKEv2 및 IPsec: **디버그 암호화 ipsecdebug crypto ikev2 [packet|internal]**
- NHRP(스포크 투 스포크):
  - **디버그 nhrp 팩**

- **디버그 nhrp 확장**
- **디버그 nhrp 캐시**
- **디버그 nhrp 경로**

이러한 명령에 대한 자세한 내용은 Cisco IOS Master Command List, All Releases를 참조하십시오
.