

"IP[v6] 번호가 지정되지 않은" 명령 컨피그레이션의 SVTI, DVTI 및 IKEv2 FlexVPN의 EIGRP 예

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[서브넷이 다른 단일 이더넷 세그먼트의 EIGRP](#)

[다른 서브넷이 있는 SVTI 세그먼트의 EIGRP](#)

[IP 번호가 지정되지 않은 명령 사용](#)

[서로 다른 서브넷이 있는 DVTI 세그먼트에 대한 SVTI의 EIGRP](#)

[다른 서브넷을 사용하는 IKEv2 Flex VPN의 EIGRP](#)

[라우팅을 위한 구성 모드](#)

[서로 다른 서브넷이 있는 SVTI 세그먼트의 IPV6 EIGRP](#)

[다른 서브넷을 사용하는 IKEv2 Flex VPN의 IPV6 EIGRP](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[알려진 주의 사항](#)

[요약](#)

[관련 정보](#)

소개

이 문서에서는 Cisco IOS®에서 자주 발생하는 여러 시나리오에서 EIGRP(Enhanced Interior Gateway Routing Protocol)를 구성하는 방법에 대해 설명합니다. EIGRP 네이버 인접성을 수락하려면 Cisco IOS는 동일한 서브넷 내의 IP 주소에서 EIGRP HELLO 패킷을 받아야 합니다. ip unnumbered 명령을 사용하여 해당 확인을 비활성화할 수 있습니다.

문서의 첫 번째 부분에서는 동일한 서브넷에 없는 패킷을 수신할 때 EIGRP 오류를 표시합니다.

또 다른 예는 해당 확인을 비활성화하고 EIGRP가 다른 서브넷에 속하는 피어 간에 인접성을 형성하도록 허용하는 ip unnumbered 명령을 사용하는 것을 보여줍니다.

또한 서버에서 IP 주소를 전송한 FlexVPN 허브 및 스포크 구축도 소개합니다. 이 시나리오에서는 ip address negotiated 명령과 ip unnumbered 명령에 대해 서브넷 확인이 비활성화됩니다. ip unnumbered 명령은 주로 P2P(Point-to-Point) 유형 인터페이스에 사용되며, FlexVPN은 P2P 아키텍처를 기반으로 하기 때문에 최적의 성능을 제공합니다.

마지막으로 IPv6 시나리오는 SVTI(Static Virtual Tunnel Interface) 및 DVTI(Dynamic Virtual Tunnel Interfaces)의 차이점과 함께 제시됩니다. IPv6과 IPv4 시나리오를 비교할 때 약간 변경된 동작이 있

습니다.

또한 Cisco IOS 버전 15.1과 15.3 간의 변경 사항이 표시됩니다([Cisco 버그 ID CSCtx45062](#)).

DVTI에 **ip unnumbered** 명령이 항상 필요합니다. 가상 템플릿 인터페이스에서 정적으로 구성된 IP 주소는 가상 액세스 인터페이스에 복제되지 않기 때문입니다. 또한 IP 주소가 구성되지 않은 인터페이스는 동적 라우팅 프로토콜 인접성을 설정할 수 없습니다. SVTI에 **ip unnumbered** 명령은 필요하지 않지만, 해당 서브넷이 없으면 동적 라우팅 프로토콜 인접성이 설정될 때 확인이 수행됩니다. 또한 EIGRP 인접성을 구축하기 위해 사용되는 링크-로컬 주소 때문에 IPv6 unnumbered 명령이 필요하지 않습니다.

사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대한 기본적인 지식을 얻을 것을 권장합니다.

- Cisco IOS의 VPN 구성
- Cisco IOS의 FlexVPN 컨피그레이션

사용되는 구성 요소

이 문서의 정보는 Cisco IOS 버전 15.3T를 기반으로 합니다.

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.

서브넷이 다른 단일 이더넷 세그먼트의 EIGRP

토폴로지: 라우터 1(R1)(e0/0:10.0.0.1/24)—(e0/1:10.0.1.2/24) 라우터 2(R2)

```
R1:
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0

router eigrp 100
network 10.0.0.1 0.0.0.0
```

```
R2:
interface Ethernet0/0
 ip address 10.0.1.2 255.255.255.0

router eigrp 100
network 10.0.1.2 0.0.0.0
```

R1에는 다음이 표시됩니다.

```
*Mar 3 16:39:34.873: EIGRP: Received HELLO on Ethernet0/0 nbr 10.0.1.2
*Mar 3 16:39:34.873: AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0
*Mar 3 16:39:34.873: EIGRP-IPv4(100): Neighbor 10.0.1.2 not on common subnet
for Ethernet0/0
```

Cisco IOS는 인접성을 형성하지 않으며, 이는 예상됩니다. 이에 대한 자세한 내용은 [What Do EIGRP "Not On Common Subnet" Messages Mean을 참조하십시오.](#)을(를) 참조하십시오.

다른 서브넷이 있는 SVTI 세그먼트의 EIGRP

VTI(Virtual Tunnel Interfaces)(GRE(Generic Routing Encapsulation) 터널)를 사용할 때도 동일한 상황이 발생합니다.

토폴로지:R1(Tun1:172.16.0.1/24)—(Tun1:172.17.0.2/24) R2

```
R1:
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0

interface Tunnel1
 ip address 172.16.0.1 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.2

router eigrp 100
 network 172.16.0.1 0.0.0.0
 passive-interface default
 no passive-interface Tunnel1
```

```
R2:
interface Ethernet0/0
 ip address 10.0.0.2 255.255.255.0

interface Tunnel1
 ip address 172.17.0.2 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.1

router eigrp 100
 network 172.17.0.2 0.0.0.0
 passive-interface default
 no passive-interface Tunnel1
```

R1에는 다음이 표시됩니다.

```
*Mar 3 16:41:52.167: EIGRP: Received HELLO on Tunnel1 nbr 172.17.0.2
*Mar 3 16:41:52.167: AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0
*Mar 3 16:41:52.167: EIGRP-IPv4(100): Neighbor 172.17.0.2 not on common subnet
for Tunnel1
```

이는 예상 동작입니다.

IP 번호가 지정되지 않은 명령 사용

이 예에서는 확인을 비활성화하고 다른 서브넷의 피어 간에 EIGRP 세션을 설정하는 `ip unnumbered` 명령을 사용하는 방법을 보여 줍니다.

토폴로지는 이전 예와 유사하지만 이제 루프백을 가리키는 `ip unnumbered` 명령을 통해 터널의 주소가 정의됩니다.

토폴로지:R1(Tun1:172.16.0.1/24)—(Tun1:172.17.0.2/24) R2

R1:

```
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0

interface Loopback0
 ip address 172.16.0.1 255.255.255.0

interface Tunnel1
 ip unnumbered Loopback0
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.2

router eigrp 100
 network 172.16.0.1 0.0.0.0
 passive-interface default
 no passive-interface Tunnel1
```

R2:

```
interface Ethernet0/0
 ip address 10.0.0.2 255.255.255.0

interface Loopback0
 ip address 172.17.0.2 255.255.255.0

interface Tunnel1
 ip unnumbered Loopback0
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.1

router eigrp 100
 network 172.17.0.2 0.0.0.0
 passive-interface default
 no passive-interface Tunnel1
```

R1에는 다음이 표시됩니다.

```
*Mar  3 16:50:39.046: EIGRP: Received HELLO on Tunnel1 nbr 172.17.0.2
*Mar  3 16:50:39.046:   AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0
*Mar  3 16:50:39.046: EIGRP: New peer 172.17.0.2
*Mar  3 16:50:39.046: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 172.17.0.2
(Tunnel1) is up: new adjacency
```

R1#show ip eigrp neighbors

EIGRP-IPv4 Neighbors for AS(100)

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
0	172.17.0.2	Tu1	12 00:00:07	7	1434	0	13

R1#show ip route eigrp

```
172.17.0.0/24 is subnetted, 1 subnets
D      172.17.0.0 [90/27008000] via 172.17.0.2, 00:00:05, Tunnel1
```

R1#show ip int brief

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	10.0.0.1	YES	manual	up	up
Loopback0	172.16.0.1	YES	manual	up	up
Tunnel1	172.16.0.1	YES	TFTP	up	up

R2는 이와 유사합니다.

ip unnumbered 명령을 특정 IP 주소 컨피그레이션으로 변경하면 EIGRP 인접성이 형성되지 않습니다.

서로 다른 서브넷이 있는 DVTI 세그먼트에 대한 SVTI의 EIGRP

이 예에서는 ip unnumbered 명령도 사용합니다. 앞서 언급한 규칙은 DVTI에도 적용됩니다.

토폴로지:R1(Tun1:172.16.0.1/24)—(가상 템플릿:172.17.0.2/24) R2

이전 예는 SVTI 대신 DVTI를 사용하기 위해 여기에서 수정됩니다. 또한 이 예에서는 터널 보호가 추가됩니다.

R1:

```
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set TS esp-des esp-md5-hmac
!
crypto ipsec profile prof
  set transform-set TS
!
interface Loopback0
  ip address 172.16.0.1 255.255.255.0
!
interface Tunnel1
  ip unnumbered Loopback0
  tunnel source Ethernet0/0
  tunnel mode ipsec ipv4
  tunnel destination 10.0.0.2
  tunnel protection ipsec profile prof
!
router eigrp 100
  network 172.16.0.1 0.0.0.0
  passive-interface default
  no passive-interface Tunnel1
```

R2:

```
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
crypto isakmp profile profLAN
  keyring default
  match identity address 10.0.0.1 255.255.255.255
  virtual-template 1
!
```

```

crypto ipsec transform-set TS esp-des esp-md5-hmac
!
crypto ipsec profile profLAN
 set transform-set TS
 set isakmp-profile profLAN

interface Loopback0
 ip address 172.17.0.2 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.0.2 255.255.255.0
!
interface Virtual-Templatel type tunnel
 ip unnumbered Loopback0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile profLAN
!
!
router eigrp 100
 network 172.17.0.2 0.0.0.0
 passive-interface default
 no passive-interface Virtual-Templatel

```

모든 것이 예상대로 작동합니다.

R1#**show crypto session**

```

Crypto session current status
Interface: Tunnell
Session status: UP-ACTIVE
Peer: 10.0.0.2 port 500
IKEv1 SA: local 10.0.0.1/500 remote 10.0.0.2/500 Active
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 2, origin: crypto map

```

R1#**show crypto ipsec sa**

```

interface: Tunnell
Crypto map tag: Tunnell-head-0, local addr 10.0.0.1
protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 10.0.0.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 89, #pkts encrypt: 89, #pkts digest: 89
#pkts decaps: 91, #pkts decrypt: 91, #pkts verify: 91

```

R1#**show ip eigrp neighbors**

```

EIGRP-IPv4 Neighbors for AS(100)
H Address Interface Hold Uptime SRTT RTO Q Seq
0 172.17.0.2 Tu1 13 00:06:31 7 1434 0 19

```

R1#**show ip route eigrp**

```

172.17.0.0/24 is subnetted, 1 subnets
D 172.17.0.0 [90/27008000] via 172.17.0.2, 00:06:35, Tunnell

```

R2#**show crypto session**

```

Crypto session current status
Interface: Virtual-Access1

```

```
Profile: profLAN
Session status: UP-ACTIVE
Peer: 10.0.0.1 port 500
IKEv1 SA: local 10.0.0.2/500 remote 10.0.0.1/500 Active
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 2, origin: crypto map
```

```
R2#show crypto ipsec sa
interface: Virtual-Access1
```

```
  Crypto map tag: Virtual-Access1-head-0, local addr 10.0.0.2
  protected vrf: (none)
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 10.0.0.1 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 107, #pkts encrypt: 107, #pkts digest: 107
    #pkts decaps: 105, #pkts decrypt: 105, #pkts verify: 105
```

```
R2#show ip eigrp neighbors
```

```
EIGRP-IPv4 Neighbors for AS(100)
```

H	Address	Interface	Hold	Uptime	SRTT	RTO	Q	Seq
0	172.16.0.1	Vi1	13	00:07:41	11	200	0	16

```
R2#show ip route eigrp
```

```
  172.16.0.0/24 is subnetted, 1 subnets
  D       172.16.0.0 [90/1433600] via 172.16.0.1, 00:07:44, Virtual-Access1
```

이전 예와 마찬가지로 터널 인터페이스 아래에서 직접 172.16.0.1 및 172.17.0.2을 구성하려고 하면 이전과 동일한 오류가 발생하여 EIGRP가 실패합니다.

다른 서브넷을 사용하는 IKEv2 Flex VPN의 EIGRP

다음은 FlexVPN 허브 및 스포크 컨피그레이션의 예입니다. 서버는 클라이언트의 컨피그레이션 모드를 통해 IP 주소를 전송합니다.

토폴로지:R1(e0/0:172.16.0.1/24)—(e0/1:172.16.0.2/24) R2

허브(R1) 구성:

```
aaa new-model
aaa authorization network LOCALIKEv2 local

crypto ikev2 authorization policy AUTHOR-POLICY
 pool POOL
!
crypto ikev2 keyring KEYRING
 peer R2
 address 172.16.0.2
 pre-shared-key CISCO
!

crypto ikev2 profile default
 match identity remote key-id FLEX
```

```

authentication remote pre-share
authentication local pre-share
keyring local KEYRING
aaa authorization group psk list LOCALIKEv2 AUTHOR-POLICY
virtual-template 1

interface Loopback0
  ip address 1.1.1.1 255.255.255.0
!
interface Ethernet0/0
  ip address 172.16.0.1 255.255.255.0

interface Virtual-Template1 type tunnel
  ip unnumbered Loopback0
  tunnel source Ethernet0/0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile default
!
!
router eigrp 1
  network 1.1.1.1 0.0.0.0
  passive-interface default
  no passive-interface Virtual-Template1
!
ip local pool POOL 192.168.0.1 192.168.0.10

```

스포크 구성:

```

aaa new-model
aaa authorization network FLEX local

crypto ikev2 authorization policy FLEX
  route set interface
!
!
!
crypto ikev2 keyring KEYRING
  peer R1
  address 172.16.0.1
  pre-shared-key CISCO
!
!
!
crypto ikev2 profile default
  match identity remote address 172.16.0.1 255.255.255.255
  identity local key-id FLEX
  authentication remote pre-share
  authentication local pre-share
  keyring local KEYRING
  aaa authorization group psk list FLEX FLEX

interface Loopback0
  ip address 2.2.2.2 255.255.255.0
!
interface Ethernet0/0
  ip address 172.16.0.2 255.255.255.0

interface Tunnel0
  ip address negotiated
  tunnel source Ethernet0/0
  tunnel mode ipsec ipv4

```

```
tunnel destination 172.16.0.1
tunnel protection ipsec profile default
```

```
router eigrp 1
network 0.0.0.0
passive-interface default
no passive-interface Tunnel0
```

스포크는 모든 스포크에 DVTI를 사용하는 허브에 연결하기 위해 SVTI를 사용합니다. EIGRP는 OSPF(Open Shortest Path First)만큼 유연하지 않으며 인터페이스(SVTI 또는 DVTI)에서 구성할 수 없으므로 **Spoke0** 인터페이스에서 EIGRP가 활성화되도록 하기 위해 스포크에서 **네트워크 0.0.0**을 사용합니다. 패시브 인터페이스는 인접성이 **Tun0** 인터페이스에서만 형성되도록 하기 위해 사용됩니다.

이 구축의 경우 Hub에서 **IP 번호**가 지정되지 않도록 구성해야 합니다. 가상 템플릿 인터페이스에서 IP 주소를 수동으로 구성할 경우 가상 액세스 인터페이스에 클론되지 않습니다. 그러면 가상 액세스 인터페이스에 IP 주소가 할당되지 않고 EIGRP 인접성이 형성되지 않습니다. 따라서 EIGRP 인접성을 **형성**하기 위해 DVTI 인터페이스에 ip unnumbered 명령이 항상 필요한 것입니다.

이 예에서는 EIGRP 인접성이 1.1.1.1~192.168.0.9 사이에 구축됩니다.

허브에서 테스트:

```
R1#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	172.16.0.1	YES	NVRAM	up	up
Ethernet0/1	unassigned	YES	NVRAM	administratively down	down
Ethernet0/2	unassigned	YES	NVRAM	administratively down	down
Ethernet0/3	unassigned	YES	NVRAM	administratively down	down
Loopback0	1.1.1.1	YES	manual	up	up
Virtual-Access1	1.1.1.1	YES	unset	up	up
Virtual-Template1	1.1.1.1	YES	manual	up	down

```
R1#show crypto session
```

```
Crypto session current status
```

```
Interface: Virtual-Access1
```

```
Session status: UP-ACTIVE
```

```
Peer: 172.16.0.2 port 500
```

```
IKEv2 SA: local 172.16.0.1/500 remote 172.16.0.2/500 Active
```

```
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
```

```
Active SAs: 2, origin: crypto map
```

```
R1#show ip eigrp neighbors
```

```
EIGRP-IPv4 Neighbors for AS(1)
```

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
0	192.168.0.9	Vi1	10	01:28:49	12	1494	0	13

```
R1#show ip route eigrp
```

```
....
```

```
Gateway of last resort is not set
```

```
2.0.0.0/24 is subnetted, 1 subnets
```

```
D 2.2.2.0 [90/27008000] via 192.168.0.9, 01:28:52, Virtual-Access1
```

Spoke(스포크) 관점에서 ip address negotiated 명령은 ip address unnumbered 명령과 동일하게 작

동하며 서브넷을 확인할 수 없습니다.

스포크 테스트:

```
R2#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	172.16.0.2	YES	NVRAM	up	up
Ethernet0/1	unassigned	YES	NVRAM	administratively down	down
Ethernet0/2	unassigned	YES	NVRAM	administratively down	down
Ethernet0/3	unassigned	YES	NVRAM	administratively down	down
Loopback0	2.2.2.2	YES	NVRAM	up	up
Tunnel0	192.168.0.9	YES	NVRAM	up	up

```
R2#show crypto session
```

```
Crypto session current status
```

```
Interface: Tunnel0
```

```
Session status: UP-ACTIVE
```

```
Peer: 172.16.0.1 port 500
```

```
IKEv2 SA: local 172.16.0.2/500 remote 172.16.0.1/500 Active
```

```
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
```

```
Active SAs: 2, origin: crypto map
```

```
R2#show ip eigrp neighbors
```

```
EIGRP-IPv4 Neighbors for AS(1)
```

H	Address	Interface	Hold Uptime	SRTT	RTO	Q	Seq
			(sec)	(ms)		Cnt	Num
0	1.1.1.1	Tu0	14 01:30:18	15	1434	0	14

```
R2#show ip route eigrp
```

```
....
```

```
1.0.0.0/24 is subnetted, 1 subnets
```

```
D 1.1.1.0 [90/27008000] via 1.1.1.1, 01:30:21
```

라우팅을 위한 구성 모드

IKEv2(Internet Key Exchange version 2)도 다른 옵션입니다. 경로를 푸시하기 위해 컨피그레이션 모드를 사용할 수 있습니다. 이 시나리오에서는 EIGRP 및 **ip unnumbered** 명령이 필요하지 않습니다.

컨피그레이션 모드를 통해 해당 경로를 전송하도록 허브를 구성하려면 이전 예를 수정할 수 있습니다.

```
crypto ikev2 authorization policy AUTHOR-POLICY
```

```
pool POOL
```

```
route set access-list SPLIT
```

```
ip access-list standard SPLIT
```

```
permit 1.1.1.0 0.0.0.255
```

스포크는 1.1.1.1을 EIGRP가 아닌 정적으로 간주합니다.

```
R2#show ip route
```

```
....
```

```
1.0.0.0/24 is subnetted, 1 subnets
S      1.1.1.0 is directly connected, Tunnel0
```

동일한 프로세스가 반대 방향으로 작동합니다. Spoke는 Hub로 경로를 전송합니다.

```
crypto ikev2 authorization policy FLEX
  route set access-list SPLIT
```

```
ip access-list standard SPLIT
  permit 2.2.2.0 0.0.0.255
```

허브는 이를 고정(EIGRP 아님)으로 간주합니다.

```
R1#show ip route
....
2.0.0.0/24 is subnetted, 1 subnets
S      2.2.2.0 is directly connected, Virtual-Access1
```

이 시나리오에서는 동적 라우팅 프로토콜 및 `ip unnumbered` 명령이 필요하지 않습니다.

서로 다른 서브넷이 있는 SVTI 세그먼트의 IPV6 EIGRP

IPv6에서는 상황이 다릅니다. 이는 EIGRP 또는 OSPF 인접성을 구축하기 위해 IPv6 링크-로컬 주소 (FE80::/10)가 사용되기 때문입니다. 유효한 링크-로컬 주소는 항상 동일한 서브넷에 속하므로 `ipv6 unnumbered` 명령을 사용할 필요가 없습니다.

모든 IPv4 주소가 IPv6 주소로 대체된다는 점을 제외하면 이 토폴로지는 이전 예와 동일합니다.

R1 구성:

```
interface Tunnel1
  no ip address
  ipv6 address FE80:1::1 link-local
  ipv6 address 2001:1::1/64
  ipv6 enable
  ipv6 eigrp 100
  tunnel source Ethernet0/0
  tunnel mode gre ipv6
  tunnel destination 2001::2
```

```
interface Loopback0
  description Simulate LAN
  no ip address
  ipv6 address 2001:100::1/64
  ipv6 enable
  ipv6 eigrp 100
```

```
interface Ethernet0/0
  no ip address
  ipv6 address 2001::1/64
  ipv6 enable
```

```
ipv6 router eigrp 100
```

R2 구성:

```

interface Tunnel1
no ip address
ipv6 address FE80:2::2 link-local
ipv6 address 2001:2::2/64
ipv6 enable
ipv6 eigrp 100
tunnel source Ethernet0/0
tunnel mode gre ipv6
tunnel destination 2001::1

```

```

interface Loopback0
description Simulate LAN
no ip address
ipv6 address 2001:200::1/64
ipv6 enable
ipv6 eigrp 100

```

```

interface Ethernet0/0
no ip address
ipv6 address 2001::2/64
ipv6 enable

```

```

ipv6 router eigrp 100

```

터널 주소는 서로 다른 서브넷(2001:1::1/64 및 2001:2::2/64)에 있지만 중요하지 않습니다. 링크-로컬 주소는 인접성을 구축하기 위해 사용됩니다. 이러한 주소를 사용하면 항상 성공합니다.

R1:

```

R1#show ipv6 int brief

```

```

Ethernet0/0          [up/up]
  FE80::A8BB:CCFF:FE00:6400
  2001::1
Loopback0           [up/up]
  FE80::A8BB:CCFF:FE00:6400
  2001:100::1
Tunnel1             [up/up]
  FE80:1::1
  2001:1::1

```

```

R1#show ipv6 eigrp neighbors

```

```

EIGRP-IPv6 Neighbors for AS(100)
H   Address                Interface          Hold Uptime    SRTT    RTO  Q  Seq
                               (sec)          (ms)          Cnt  Num
0   Link-local address: Tu1   Tu1                12 00:13:58    821   4926  0  17
    FE80:2::2

```

```

R1#show ipv6 route eigrp

```

```

...
D   2001:2::/64 [90/28160000]
    via FE80:2::2, Tunnel1
D   2001:200::/64 [90/27008000]
    via FE80:2::2, Tunnel1

```

R2:

```

R2#show ipv6 int brief

```

```

Ethernet0/0          [up/up]
  FE80::A8BB:CCFF:FE00:6500
  2001::2

```

```

Loopback0          [up/up]
  FE80::A8BB:CCFF:FE00:6500
  2001:200::1
Tunnel1            [up/up]
  FE80:2::2
  2001:2::2

```

```
R2#show ipv6 eigrp neighbors
```

```
EIGRP-IPv6 Neighbors for AS(100)
```

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
0	Link-local address: Tu1 FE80:1::1		14 00:15:31	21	1470	0	18

```
R2#show ipv6 route eigrp
```

```

...
D 2001:1::/64 [90/28160000]
  via FE80:1::1, Tunnel1
D 2001:100::/64 [90/27008000]
  via FE80:1::1, Tunnel1

```

피어 IPv6 네트워크는 EIGRP 프로세스에 의해 설치됩니다. R1에서 2001:2::/64 네트워크가 설치되고 해당 네트워크가 2001:1::/64와 다른 서브넷입니다. R2에서도 마찬가지입니다. 예를 들어 2001::1/64가 설치되고 피어 IP 주소의 서브넷입니다. 여기서 **ipv6 unnumbered** 명령은 필요하지 않습니다. 또한 링크-로컬 주소가 사용되므로 EIGRP 인접성을 설정하기 위해 터널 인터페이스에 **ipv6 address** 명령이 필요하지 않습니다. 또한 **ipv6 enable** 명령을 사용하여 IPv6을 활성화할 때 이러한 주소가 자동으로 생성되기 때문입니다.

다른 서브넷을 사용하는 IKEv2 Flex VPN의 IPV6 EIGRP

IPv6에 대한 DVTI 컨피그레이션이 IPv4와 다릅니다. 더 이상 고정 IP 주소를 구성할 수 없습니다.

```

R1(config)#interface Virtual-Template2 type tunnel
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address ?
  autoconfig  Obtain address using autoconfiguration
  dhcp        Obtain a ipv6 address using dhcp
  negotiated   IPv6 Address negotiated via IKEv2 Modeconfig

```

```
R1(config-if)#ipv6 address
```

고정 주소는 가상 액세스 인터페이스에 복제되지 않으므로 이 작업이 필요합니다. 따라서 허브 컨피그레이션에 **ipv6 unnumbered** 명령이 권장되고 스포크 컨피그레이션에 **ipv6 address negotiated** 명령이 권장됩니다.

모든 IPv4 주소가 IPv6 주소로 대체된다는 점을 제외하면 토폴로지는 이전 예와 동일합니다.

허브(R1) 구성:

```

aaa authorization network LOCALIKEv2 local

crypto ikev2 authorization policy AUTHOR-POLICY
  ipv6 pool POOL

crypto ikev2 keyring KEYRING

```

```
peer R2
address 2001::2/64
pre-shared-key CISCO

crypto ikev2 profile default
match identity remote key-id FLEX
authentication remote pre-share
authentication local pre-share
keyring local KEYRING
aaa authorization group psk list LOCALIKEv2 AUTHOR-POLICY
virtual-template 1
```

interface Loopback0

```
no ip address
ipv6 address 2001:100::1/64
ipv6 enable
ipv6 eigrp 100
```

```
interface Ethernet0/0
no ip address
ipv6 address 2001::1/64
ipv6 enable
```

```
interface Virtual-Template1 type tunnel
no ip address
ipv6 unnumbered Loopback0
ipv6 enable
ipv6 eigrp 100
tunnel source Ethernet0/0
tunnel mode ipsec ipv6
tunnel protection ipsec profile default
```

```
ipv6 local pool POOL 2001:10::/64 64
ipv6 router eigrp 100
eigrp router-id 1.1.1.1
```

스포크(R2) 구성:

```
aaa authorization network FLEX local

crypto ikev2 authorization policy FLEX
route set interface

crypto ikev2 keyring KEYRING
peer R1
address 2001::1/64
pre-shared-key CISCO

crypto ikev2 profile default
match identity remote address 2001::1/64
identity local key-id FLEX
authentication remote pre-share
authentication local pre-share
keyring local KEYRING
aaa authorization group psk list FLEX FLEX

interface Tunnel0
no ip address
ipv6 address negotiated
ipv6 enable
ipv6 eigrp 100
```

```
tunnel source Ethernet0/0
tunnel mode ipsec ipv6
tunnel destination 2001::1
tunnel protection ipsec profile default
!
interface Ethernet0/0
no ip address
ipv6 address 2001::2/64
ipv6 enable
```

```
ipv6 router eigrp 100
eigrp router-id 2.2.2.2
```

확인:

R2#show ipv6 eigrp neighbors

EIGRP-IPv6 Neighbors for AS(100)

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
0	Link-local address: Tu0 FE80::A8BB:CCFF:FE00:6500		11	00:12:32	17	1440	0	12

R2#show ipv6 route eigrp

```
....
D 2001:100::/64 [90/27008000]
via FE80::A8BB:CCFF:FE00:6500, Tunnel0
```

R2#show crypto session detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

```
Interface: Tunnel0
Uptime: 00:13:17
Session status: UP-ACTIVE
Peer: 2001::1 port 500 fvrf: (none) ivrf: (none)
Phase1_id: 2001::1
Desc: (none)
IKEv2 SA: local 2001::2/500
remote 2001::1/500 Active
Capabilities:(none) connid:1 lifetime:23:46:43
IPSEC FLOW: permit ipv6 ::/0 ::/0
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 190 drop 0 life (KB/Sec) 4271090/2803
Outbound: #pkts enc'ed 194 drop 0 life (KB/Sec) 4271096/2803
```

R2#ping 2001:100::1 repeat 100

```
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 2001:100::1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/4/5 ms
```

R2#show crypto session detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel0

```
Uptime: 00:13:27
Session status: UP-ACTIVE
Peer: 2001::1 port 500 fvrf: (none) ivrf: (none)
  Phase1_id: 2001::1
  Desc: (none)
IKEv2 SA: local 2001::2/500
  remote 2001::1/500 Active
  Capabilities:(none) connid:1 lifetime:23:46:33
IPSEC FLOW: permit ipv6 ::/0 ::/0
  Active SAs: 2, origin: crypto map
  Inbound:  #pkts dec'ed 292 drop 0 life (KB/Sec) 4271071/2792
  Outbound: #pkts enc'ed 296 drop 0 life (KB/Sec) 4271082/2792
```

DVTI의 경우 IPv6을 수동으로 구성할 수 없습니다. 허브에 **ipv6 unnumbered** 명령을 사용하는 것이 좋습니다. 스포크에서는 **ipv6 address negotiated** 명령을 사용하는 것이 좋습니다.

이 시나리오에서는 DVTI에 대한 **ipv6 unnumbered** 명령을 제공합니다. IPv4가 아닌 IPv6의 경우 가상 템플릿 인터페이스에서 **ipv6 unnumbered** 명령이 필요하지 않습니다. 그 이유는 IPv6 SVTI 시나리오와 동일합니다. link-local ipv6 주소는 인접성을 구축하는 데 사용됩니다. 가상 템플릿에서 복제된 가상 액세스 인터페이스는 IPv6 링크-로컬 주소를 상속하며 EIGRP 인접성을 구축하기에 충분합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

알려진 주의 사항

[Cisco 버그 ID CSCtx45062](#) FlexVPN:터널 ip가 /32인 경우 EIGRP는 공통 서브넷을 확인할 수 없습니다.

이 버그 및 픽스는 FlexVPN에 한정되지 않습니다. 픽스를 구현하기 전에 다음 명령을 입력합니다 (Software Release 15.1).

```
R2(config-if)#do show run int tun1
Building configuration...

Current configuration : 165 bytes

interface Tunnel1
 tunnel source Ethernet0/0
 tunnel destination 192.168.0.1
 tunnel protection ipsec profile prof1

R2(config-if)#ip address 192.168.200.1 255.255.255.255
```

Bad mask /32 for address 192.168.200.1

수정(소프트웨어 15.3) 후 다음 명령을 입력합니다.

```
R2(config-if)#do show run int tun1
Building configuration...
```

Current configuration : 165 bytes

```
interface Tunnell
 tunnel source Ethernet0/0
 tunnel destination 192.168.0.1
 tunnel protection ipsec profile prof1
```

```
R2(config-if)#ip address 192.168.200.1 255.255.255.255
```

```
R2(config-if)#
```

```
*Jun 14 18:01:12.395: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor
192.168.100.1 (Tunnell) is up: new adjacency
```

Software Release 15.3에는 실제로 두 가지 변경 사항이 있습니다.

- **넷마스크 /32**는 모든 IP 주소에 허용됩니다.
- **/32** 주소를 사용할 때 EIGRP 인접 디바이스에 대한 서브넷 확인은 없습니다.

요약

EIGRP 동작은 ip unnumbered 명령에 의해 **변경됩니다**.EIGRP 인접성을 설정하는 동안 동일한 서브넷에 대한 검사를 비활성화합니다.

또한 가상 템플릿에서 정적으로 구성된 IP 주소를 사용할 때 가상 액세스에 복제되지 않는다는 점을 기억해야 합니다.따라서 ip unnumbered 명령이 필요합니다.

FlexVPN의 경우 클라이언트에서 협상된 주소를 사용할 때 ip unnumbered 명령을 사용할 필요가 없습니다.그러나 EIGRP를 사용할 때는 허브에서 사용하는 것이 중요합니다.라우팅에 컨피그레이션 모드를 사용하는 경우 EIGRP가 필요하지 않습니다.

SVTI의 경우 IPv6는 인접성을 위해 링크-로컬 주소를 사용하며 ipv6 unnumbered 명령을 사용할 필요가 없습니다.

DVTI의 경우 IPv6을 수동으로 구성할 수 없습니다.허브에 ipv6 unnumbered 명령을 사용하는 것이 좋습니다. 스포크에서는 ipv6 address negotiated 명령을 사용하는 것이 좋습니다.

관련 정보

- [Cisco IOS 15.3 FlexVPN 컨피그레이션 가이드](#)
- [Cisco IOS 15.3 명령 참조](#)
- [기술 지원 및 문서 - Cisco Systems](#)