使用“IP[v6]未编号”命令配置SVTI、DVTI和IKEv2 FlexVPN上的EIGRP示例

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[具有不同子网的一个以太网网段上的EIGRP](#)
[具有不同子网的SVTI网段上的EIGRP](#)
[使用IP未编号命令](#)
[SVTI上的EIGRP到具有不同子网的DVTI网段](#)
[IKEv2 Flex VPN上具有不同子网的EIGRP](#)
[路由配置模式](#)
[SVTI网段上具有不同子网的IPV6 EIGRP](#)
[IKEv2 Flex VPN上具有不同子网的IPV6 EIGRP](#)
[验证](#)
[故障排除](#)
[已知问题说明](#)
[摘要](#)
[相关信息](#)

简介

本文档介绍如何在Cisco IOS®上的许多常见场景中配置增强型内部网关路由协议(EIGRP)。为了接受EIGRP邻居邻接关系，Cisco IOS必须从同一子网内的IP地址获取EIGRP HELLO数据包。可以使用ip unnumbered命令禁用**该验**证。

文章的第一部分在收到不在同一子网中的数据包时显示EIGRP故障。

另一个示例演示如何使用**ip unnumbered**命令来禁用该验证，并允许EIGRP在属于不同子网的对等体之间形成邻接关系。

本文还介绍了FlexVPN中心和分支部署，其中包含从服务器发送的IP地址。对于此场景，会为ip address negotiated命令和**ip unnumbered命**令禁用子网**验证**功能。**ip unnumbered** 命令主要用于点对点(P2P)类型的接口，这使FlexVPN成为一个完美的适合，因为它基于P2P架构。

最后，给出了IPv6方案，以及静态虚拟隧道接口(SVTI)和动态虚拟隧道接口(DVTI)的区别。 在比较IPv6和IPv4场景时，行为略有变化。

此外，还显示了Cisco IOS版本15.1和15.3之间的更改(Cisco bug ID CSCtx45062)。

DVTI始终需**要ip unnumbered**命令。这是因为虚拟模板接口上静态配置的IP地址从未被克隆到虚拟访问接口。此外，未配置IP地址的接口无法建立任何动态路由协议邻接关系。对于SVTI，**ip unnumbered**命令不是必需的，但如果没有该子网，则在建立动态路由协议邻接关系时会执行验证。此外，IPV6场景不需**要ipv6 unnumbered**命令，因为用于构建EIGRP邻接关系的本地链路地址。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- Cisco IOS上的VPN配置
- Cisco IOS上的FlexVPN配置

使用的组件

本文档中的信息基于Cisco IOS版本15.3T。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

具有不同子网的一个以太网网段上的EIGRP

拓扑：路由器1(R1)(e0/0:10.0.0.1/24)—(e0/1:10.0.1.2/24)路由器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
```

R1显示：

```
*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 IOS不会形成邻接关系，这是预期的。有关此的详细信息，请参[阅EIGRP“不在通用子网上”消息的含义。](#)文章。

具有不同子网的SVTI网段上的EIGRP

使用虚拟隧道接口(VTI)(通用路由封装(GRE)隧道)时，也会出现同样的情况。

拓扑：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
```

R1显示：

```
*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
```

这是预料之中的现象。

使用IP未编号命令

本示例显示如何使用**ip unnumbered**命令，该命令禁用验证并允许在不同子网中的对等体之间建立EIGRP会话。

拓扑与上例类似，但隧道的地址现在通过指向环回的**ip unnumbered**命令定义：

拓扑：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
```

R1显示：

```
*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   SRTT   RTO  Q  Seq
                                           (sec)         (ms)       Cnt 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
```

R2类似。

将ip unnumbered命令更**改为**特定IP地址配置后，EIGRP邻接关系不会形成。

SVTI上的EIGRP到具有不同子网的DVTI网段

本示例还使用ip unnumbered命令。上述规则也适用于DVTI。

拓扑：R1(Tun1:172.16.0.1/24)—(虚拟模板：172.17.0.2/24)R2

此处对上一个示例进行了修改，以便使用DVTI而不是SVTI。此外，本示例中还添加了隧道保护。

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-Template1 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-Template1
```

一切都如预期一样运行：

```
R1#show crypto session
Crypto session current status
Interface: Tunnel1
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: Tunnel1
   Crypto map tag: Tunnel1-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, Tunnel1




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
```

至于上述示例，当您尝试直接在隧道接口下配置172.16.0.1和172.17.0.2时，EIGRP会失败，错误与之前完全相同。

IKEv2 Flex VPN上具有不同子网的EIGRP

以下是FlexVPN中心和分支配置的示例。服务器通过客户端的配置模式发送IP地址。

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

集线器(R1)配置：

```
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
```

辐条配置:

```
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
```

辐条使用SVTI以连接到所有辐条使用DVTI的集线器。由于EIGRP不像开放最短路径优先(OSPF)那样灵活，并且无法在接口（SVTI或DVTI）下配置EIGRP，**因此在辐**条上使用网络0.0.0.0来确保在**Tun0接口上启用EIGRP**。使用被动接口来确保仅在Tun0接口上形**成邻**接。

对于此部署，还需要在集线器上**配置**未编号的ip。在虚拟模板接口下手动配置IP地址时，不会将其克隆到虚拟访问接口。然后，虚拟接入接口没有分配IP地址，EIGRP邻接关系也未形成。因此，DVTI接口始终需**要ip unnumbered** 命令才能形成EIGRP邻接关系。

在本例中，在1.1.1.1和192.168.0.9之间建立EIGRP邻接关系。

在集线器上测试：

```
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 Uptime   SRTT   RTO  Q  Seq
                                              (sec)         (ms)       Cnt 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
```

从辐条的角度看，ip address negotiated 命令与ip address unnumbered命令的工作方式相同，并且禁用了子网验证。

在辐条上测试：

```
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
```

路由配置模式

Internet密钥交换版本2(IKEv2)是另一个选项。可以使用配置模式来推送路由。在此场景中，不需要EIGRP和ip unnumbered命令。

您可以修改上一个示例，以便将集线器配置为通过配置模式发送该路由：

```
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
```

分支将1.1.1.1视为静态，而非EIGRP:

```
R2#show ip route
....
     1.0.0.0/24 is subnetted, 1 subnets
S        1.1.1.0 is directly connected, Tunnel0
```

同一过程在相反的方向上工作。分支向中心点发送路由：

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

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

集线器将其视为静态（而非EIGRP）：

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

在此场景中，不需要动态路由协议和**ip unnumbered**命令。

SVTI网段上具有不同子网的IPV6 EIGRP

对于IPv6，情况不同。这是因为IPv6本地链路地址(FE80::/10)用于建立EIGRP或OSPF邻接关系。有效的本地链路地址始终属于同一子网，因此无需为此使用**ipv6 unnumbered**命令。

此处的拓扑与上一个示例相同，不同之处在于所有IPv4地址都替换为IPv6地址。

R1配置：

```
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配置：

```
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
```

隧道地址位于不同的子网（2001:1::1/64和2001:2::2/64）中，但这并不重要。使用本地链路地址建立邻接关系。使用这些地址，它始终会成功。

在 R1 上：

```
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                      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
```

在R2上：

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

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
```

对等IPv6网络由EIGRP进程安装。在R1上，安装了2001:2::/64网络，该网络与2001:1::/64网络不同。R2上也是如此。例如，安装了2001::1/64，这是其对等IP地址的子网。此处不需要**ipv6 unnumbered**命令。此外，隧道接口上不需要**ipv6 address**命令来建立EIGRP邻接关系，因为使用了本地链路地址(当您使用ipv6 enable命令启用IPv6时，这些地址会自**动生成**)。

IKEv2 Flex VPN上具有不同子网的IPV6 EIGRP

IPv6的DVTI配置与IPv4的DVTI配置不同：不能再配置静态IP地址。

```
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
```

这是预期的，因为静态地址从未被克隆到虚拟访问接口。这就是为什么建议**对中心配置使**用ipv6 unnumbered命令，而对分支配置**使用ipv6 address negotiated**命令的原因。

拓扑与上例相同，不同之处在于所有IPv4地址都替换为IPv6地址。

集线器(R1)配置：

```
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
```

分支(R2)配置：

```
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
```

验证：

```
R2#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: Tu0                      11 00:12:32   17  1440  0  12
   FE80::A8BB:CCFF:FE00:6500

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
```

对于DVTI，无法手动配置IPv6。建议**对集线器使用ipv6 unnumbered** 命令，并建议在辐**条上使用ipv6 address negotiated** 命令。

此场景为DVTI**提供ipv6 unnumbered**命令。请注意，对于IPv6而不是IPv4，虚拟模板接口上不需要**ipv6 unnumbered**命令。原因与IPv6 SVTI场景相同：本地链路ipv6地址用于建立邻接关系。从虚拟模板克隆的虚拟访问接口继承IPv6本地链路地址，这足以建立EIGRP邻接关系。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

已知问题说明

Cisco Bug ID CSCtx45062 FlexVPN:如果隧道IP为/32，则EIGRP不应检查公共子网。

此漏洞和修复不特定于FlexVPN。在实施修复（软件版本15.1）之前，输入以下命令：

```
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
```

在修复后输入以下命令（软件15.3）：

```
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
R2(config-if)#
*Jun 14 18:01:12.395: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor
192.168.100.1 (Tunnel1) is up: new adjacency
```

软件版本15.3实际上有两项更改：

- **所有IP地址**都接受子网掩码/32。
- 使用/32地址时，EIGRP邻居没有子网**验证**。

摘要

EIGRP行为通过ip unnumbered**命令**更改。它在建立EIGRP邻接关系时禁用对同一子网的检查。

此外，切记在虚拟模板上使用DVTI静态配置的IP地址时，不会将其克隆到虚拟访问。这就是为什么需**要ip unnumbered**命令的原因。

对于FlexVPN，在客户端上使用协商地址时，无**需使用ip unnumbered**命令。但是，使用EIGRP时，在集线器上使用它非常重要。当您使用配置模式进行路由时，不需要EIGRP。

对于SVTI，IPv6使用本地链路地址进行邻接，无需使用ipv6 **unnumbered命**令。

对于DVTI，无法手动配置IPv6。建议**对集线器使用ipv6 unnumbered** 命令，并建议在辐**条上使用ipv6 address negotiated** 命令。

相关信息

- Cisco IOS 15.3 FlexVPN配置指南
- Cisco IOS 15.3命令参考
- 技术支持和文档 - Cisco Systems