目录

简介

本文描述如何配置在一定数量的普通遇到的方案的增强的内部网关路由选择协议(EIGRP)在Cisco IOS。为了接受EIGRP邻居邻接， Cisco IOS必须从在相同子网内的一个IP地址得到EIGRP Hello信息包。禁用该验证用**ip unnumbered命令**是可能的。

条款的第一部分提交一EIGRP失败，当收到不在相同子网的数据包时。

另一示例展示使用**ip unnumbered命令**禁用该验证，并且允许EIGRP形成在属于不同的子网的对等体之间的一邻接。

此条款也提交FlexVPN星型网部署用从服务器发送的IP地址。对于此方案，子网的验证禁用为**ip address negotiated命令**并且为**ip unnumbered命令**。**ip unnumbered命令**主要使用点到点(P2P)类型接口，并且这做FlexVPN完善的适应，因为根据P2P体系结构。

最后， IPv6方案与静态虚拟隧道接口(SVTI)和动态虚拟隧道接口的(DVTI)差异一起被提交。当您比较IPv6对IPv4方案，有在行为上的轻微的变化。

另外，提交在Cisco IOS版本15.1和15.3之间的更改([Cisco Bug ID CSCtx45062](#))。

ip unnumbered命令为DVTI总是需要的。这是因为在虚拟模板接口的静态配置的IP地址从未被克隆对虚拟访问接口。而且，没有配置的IP地址的一个接口不能设立任何动态路由协议邻接。**ip unnumbered命令**为SVTI不是必要的，但是没有该子网，验证进行，当动态路由协议邻接设立时。并且**IPv6未编号的**命令为IPV6方案不是需要的由于使用为了构建EIGRP邻接的链路本地地址。

Cisco 建议您具有以下主题的基础知识：

- 在Cisco IOS的VPN配置
- 在Cisco IOS的FlexVPN配置

使用的组件

本文档中的信息根据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。

在一个以太网段的EIGRP用不同的子网

拓扑：路由器1 (R1) (e0/0 ：10.0.0.1/24)-------(e0/1 ：10.0.1.2/24) Router2 (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不形成邻接，预计。关于此的更多信息，参考什么执行EIGRP " Not on Common Subnet " Messages平均值？条款。

在SVTI分段的EIGRP用不同的子网

同一个情况发生，当您使用虚拟隧道接口(VTI) (通用路由封装(GRE)隧道)。

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。

请使用IP unnumbered命令

此示例显示如何使用**ip unnumbered命令**功能失效验证并且允许一EIGRP会话的建立在对等体之间的用不同的子网。

拓扑类似于前一个示例，但是通道的地址通过**ip unnumbered命令**当前定义对环回的点：

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类似于此。

在您更改ip unnumbered命令到一个特定IP地址配置后，EIGRP邻接不形成。

在SVTI的EIGRP对用不同的子网的DVTI分段

此示例也使用ip unnumbered命令。以前被提及的规则适用对DVTI。

拓扑：R1(Tun1 ：172.16.0.1/24) (Virtual模板：172.17.0.2/24) R2

修改前一个示例此处为了使用DVTI而不是SVTI。另外，通道保护在本例中被添加。

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
```
一切运作正如所料：

```
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
```

关于前面的示例，当您设法配置172.16.0.1和172.17.0.2直接地在隧道接口下时，EIGRP失效与同

一个错误象以前。

在IKEv2弹性用不同的子网的VPN的EIGRP

这是FlexVPN星型网配置的示例。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
```

分支用途SVTI为了连接到使用DVTI所有spoke的集线器。由于EIGRP不一样灵活，象开放最短路径优先(OSPF)和不是可能配置它在接口下(SVTI或DVTI)，**网络0.0.0.0**在分支用于为了保证EIGRP在**Tun0**接口启用。无源接口用于为了保证邻接在**Tun0**接口仅形成。

对于此部署，配置在集线器的**ip unnumbered**也是必要的。当您手工配置IP地址在虚拟模板接口下时，没有被克隆对虚拟访问接口。然后，虚拟访问接口没有分配的一个IP地址，并且EIGRP邻接不形成。这就是为什么**ip unnumbered命令**为DVTI接口总是要求为了形成EIGRP邻接。

在本例中，EIGRP邻接被构建在1.1.1.1和192.168.0.9之间。

测试在集线器：

```
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
```

从分支方面，**ip address negotiated命令**工作同**IP地址未编号的**命令一样，并且子网的验证禁用。

测试在分支：

```
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
```


路由的配置模式

互联网密钥交换版本2 (IKEv2)是另一个选项。使用配置模式为了推送路由是可能的。在此方案中，
EIGRP和**ip unnumbered命令**不是需要的。

您能修改前一个示例为了配置集线器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
```

分支看到1.1.1.1作为静态，不是EIGRP：

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

在相反的方向的同样处理工作。分支发送路由到集线器：

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

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

集线器看到它作为静态(不是EIGRP)：

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

对于此方案，动态路由协议和ip unnumbered命令不是需要的。

在SVTI分段的IPV6 EIGRP用不同的子网

对于IPv6，情况不同的。这是因为IPv6链路本地地址(FE80::/10)用于为了构件EIGRP或OSPF邻接。有效链路本地地址总是属于相同子网，那么那里是没有需要使用IPv6未编号的命令那。

此处拓扑是相同的象为前一个示例，除了所有IPv4地址置换与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
```
通道地址用不同的子网(2001:1::1/64和2001:2::2/64)，但是那不是重要。链路本地地址用于为了构建邻接。使用这些地址，它总是成功。

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：

```
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
```

对等体IPv6网络由EIGRP进程安装。在R1，2001:2::/64网络安装，并且该网络比2001:1::/64是一不同的子网。同样是真的在R2。例如，2001::1/64安装，是其对端IP地址的一子网。没有对**IPv6未编号的**命令的需要在这里。另外，**address命令的IPv6**在隧道接口没有必要为了设立EIGRP邻接，因为使用链路本地地址(和那些自动地生成，当您启用与**enable命令的IPv6的**IPv6)时。

在IKEv2弹性用不同的子网的VPN的IPV6 EIGRP

IPv6的DVTI配置为IPv4不同跟：再配置静态IP地址是不可能的。

```
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
```

因为一个静态地址从未被克隆对虚拟访问接口，这预计。这就是为什么**IPv6未编号的**命令为集线器上配置推荐，并且**IPv6地址协商的**命令为辐条配置推荐。

拓扑是相同的象前一个示例，除了所有IPv4地址置换与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， IPv6不可能手工配置。**IPv6未编号的**命令为集线器推荐，并且**IPv6地址协商的**命令在分支推荐。

此方案展示**IPv6** DVTI的**未编号的**命令。注意是重要的，对于与IPv4相对的IPv6， **IPv6未编号的** on命令虚拟模板接口不是需要的。对此的原因是相同的象为IPv6 SVTI方案：链路本地IPv6地址使用构建邻接。虚拟访问接口，从虚拟模板被克隆，继承IPv6链路本地地址和那是满足为了构建EIGRP邻接。

[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 ：如果通道ip's是/32， Eigrp不应该检查普通的子网。

此bug和修正不是FlexVPN特定。请输入此命令，在您实现修正前(软件版本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
```
在修正(软件15.3)以后输入此命令：

```
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
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
```
实际上有在软件版本15.3上的两个变化：

- **网络屏蔽/32**为所有IP地址接受。
- 当您使用**/32**地址时，没有EIGRP邻居的子网验证。

摘要

EIGRP行为由**ip unnumbered命令**更改。当设立一EIGRP邻接时，它禁用检查相同子网。

应该记住的是，当您静态使用在虚拟模板时的DVTIs配置的IP地址，它没有被克隆对虚拟访问。这就是为什么**ip unnumbered命令**是需要的。

对于FlexVPN，当您使用在客户端时的协商得到的地址没有需要使用**ip unnumbered命令**。当您使用EIGRP时，但是，使用它在集线器是重要的。当您使用配置模式路由时，EIGRP不是需要的。

对于SVTI，IPv6使用链路本地地址邻接，并且没有需要使用**IPv6未编号的**命令。

对于DVTI，IPv6不可能手工配置。**IPv6未编号的**命令为集线器推荐，并且**IPv6地址协商的**命令在分支推荐。

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](#)