使用「IP[v6]未編號」命令的SVTI、DVTI和IKEv2 FlexVPN上的EIGRP配置示例

目錄

簡介

本檔案介紹如何在Cisco IOS®上常見的多種方案中設定增強型內部閘道路由通訊協定(EIGRP)。為了接受EIGRP鄰居鄰接關係，Cisco IOS必須從同一子網內的IP地址獲取EIGRP HELLO資料包。可以使用**ip unnumbered**命令禁用該驗證。

本文第一部分顯示EIGRP失敗，當它收到不在同一子網中的資料包時。

另一個示例演示了使用**ip unnumbered**命令禁用該驗證，並允許EIGRP在屬於不同子網的對等體之間形成鄰接關係。

本文還提供使用從伺服器傳送的IP地址的FlexVPN中心輻射部署。在此場景中，對於**ip address negotiated**命令以及**ip unnumbered**命令，**將禁用子網驗證。ip unnumbered**命令主要用於點對點(P2P)型別的介面，這使得FlexVPN非常適合，因為它基於P2P架構。

最後，給出了一個IPv6方案，以及靜態虛擬隧道介面(SVTI)和動態虛擬隧道介面(DVTI)的區別。 比較IPv6和IPv4方案時，行為略有變化。

此外，還顯示Cisco IOS版本15.1和15.3之間的更改(思科錯誤ID CSCtx45062)。

DVTI始終需要**ip unnumbered**命令。這是因為虛擬模板介面上靜態配置的IP地址永遠不會克隆到虛擬訪問介面。此外，未配置IP地址的介面無法建立任何動態路由協定鄰接關係。SVTI不需要**ip unnumbered**命令，但是如果沒有該子網，在建立動態路由協定鄰接關係時進行驗證。此外，IPV6方案不需要**ipv6 unnumbered**命令，因為用於建立EIGRP鄰接關係的本地鏈路地址。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

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

採用元件

本檔案中的資訊是根據Cisco IOS版本15.3T。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

一個具有不同子網的乙太網段上的EIGRP

拓撲：路由器1(R1)(e0/0:10.0.0.1/24)-------(e0/1網站：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顯示：

```
*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不會形成預期中的鄰接關係。有關此問題的詳細資訊，請參閱EIGRP 「Not On Common Subnet」消息的含義是什麼？文章。

具有不同子網的SVTI網段上的EIGRP

使用虛擬通道介面(VTI)(通用路由封裝(GRE)通道)時也會發生相同的情況。

拓撲：R1(Tun1:172.16.0.1/24)-------(Tun1網站：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顯示：

```
*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
```

這是預期行為。

使用IP Unnumbered命令

此示例顯示如何使用ip unnumbered命令禁用驗證並允許在不同子網中的對等體之間建立EIGRP會話。

拓撲結構與先前的範例類似，但通道的地址現在是通過指向環回的ip unnumbered命令定義的：

拓撲：R1(Tun1:172.16.0.1/24)-------(Tun1網站：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顯示：

```
*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與此類似。

將ip unnumbered命令更改為特定IP地址配置後，不會形成EIGRP鄰接關係。

具有不同子網的SVTI到DVTI段上的EIGRP

此示例還使用ip unnumbered命令。前面提到的規則也適用於DVTI。

拓撲：R1(Tun1:172.16.0.1/24)-------(Virtual-template網站：172.17.0.2/24)R2

以上示例在此處進行修改，以便使用DVTI而不是SVTI。此外，本範例新增通道保護。

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
```

一切如預期般順利：

```
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
```

與前面示例一樣，當您嘗試在隧道介面下直接配置172.16.0.1和172.17.0.2時，EIGRP會失敗，錯誤與之前完全相同。

具有不同子網的IKEv2 Flex VPN上的EIGRP

以下是FlexVPN集中器和分支配置的示例。伺服器通過客戶端的配置模式傳送IP地址。

拓撲：R1(e0/0:172.16.0.1/24)-------(e0/1網站：172.16.0.2/24)R2

集線器(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
```

分支配置：

```
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
```

輻條使用SVTI連線到對所有輻條使用DVTI的集線器。由於EIGRP不像開放最短路徑優先(OSPF)那樣靈活，並且無法在介面（SVTI或DVTI）下配置它，因此在Spoke上使用**network 0.0.0.0，以確保在Tun0**介面上啟用EIGRP。使用被動介面以確保僅在**Tun**介面上形成**鄰接關**系。

對於此部署，還必須在集線器上配置**ip unnumbered**。在虛擬模板介面下手動配置IP地址時，不會將其克隆到虛擬訪問介面。然後，虛擬訪問介面沒有分配IP地址，並且沒有形成EIGRP鄰接關係。這就是為什麼DVTI介面始終需要**ip unnumbered**命令才能形成EIGRP鄰接關係的原因。

在本示例中，EIGRP鄰接關係在1.1.1.1和192.168.0.9之間建立。

在Hub上測試：

```
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
```

從輻條角度看，ip address negotiated命令的工作方式與ip address unnumbered命令相同，並且已禁用對子網的驗證。

在分支上進行測試：

```
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

Internet金鑰交換版本2(IKEv2)是另一個選項。可以使用配置模式推送路由。在這種情況下，不需要使用EIGRP和ip unnumbered命令。

您可以修改前面的示例，將集線器配置為通過配置模式傳送該路由：

```
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
```

輻射點將1.1.1.1視為靜態，而不是EIGRP:

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

同樣的過程在相反的方向上運行。分支將路由傳送到中心：

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

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

集線器將其視為靜態（而不是EIGRP）：

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

在此案例中，不需要動態路由協定和**ip unnumbered**命令。

具有不同子網的SVTI網段上的IPV6 EIGRP

IPv6的情況則不同。這是因為使用IPv6本地鏈路地址(FE80::/10)建立EIGRP或OSPF鄰接關係。有效的本地鏈路地址始終屬於同一個子網，因此不需要使用**ipv6 unnumbered**命令進行操作。

這裡的拓撲與先前的示例相同，只不過所有IPv4地址都替換為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
```

通道地址位於不同的子網中（2001:1::1/64和2001:2::2/64），但這並不重要。本地鏈路地址用於建立鄰接關係。通過這些地址，它始終成功。

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
```

對等IPv6網路由EIGRP進程安裝。在R1上安裝2001:2::/64網路，該網路是不同於2001:1::/64的子網。在R2上也同樣如此。例如，已安裝2001::1/64，這是其對等IP地址的子網。此處不需要**ipv6 unnumbered**命令。此外，隧道介面上不需要使用**ipv6 address**命令來建立EIGRP鄰接關係，因為使用本地鏈路地址(這些地址在使用**ipv6 enable**命令啟用IPv6時自動生成)。

具有不同子網的IKEv2 Flex VPN上的IPV6 EIGRP

IPv6的DVTI配置與IPv4的DVTI配置不同：不能再配置靜態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
```

這是預期結果，因為靜態地址永遠不會克隆到虛擬訪問介面。因此，建議對集線器配置使用**ipv6 unnumbered**命令，對分支配置使用**ipv6 address negotiated**命令。

除了所有IPv4地址都替換為IPv6地址外，拓撲結構與上一示例相同。

集線器(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
```

驗證：

```
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
```

對於DVTI，無法手動配置IPv6。對於集線器，建議使用**ipv6 unnumbered**命令；對於分支，建議使用**ipv6 address negotiated**命令。

此案例顯示DVTI的**ipv6 unnumbered**命令。必須注意的是，對於IPv6而不是IPv4，虛擬模板介面上不需要使用**ipv6 unnumbered**命令。原因與IPv6 SVTI場景相同：本地鏈路ipv6地址用於建立鄰接關係。從虛擬模板克隆的虛擬訪問介面繼承IPv6本地鏈路地址，這足以建立EIGRP鄰接關係。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

已知警告

思科錯誤ID CSCtx45062 FlexVPN:如果隧道IP為/32，則EIGRP不應檢查公共子網。

此錯誤和修復程式不是FlexVPN特定的。執行修復程式（軟體版本15.1）之前，請輸入以下命令：

```
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
```

修正後輸入以下命令（軟體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
```

在軟體版本15.3中，實際上有兩個變更：

- **所有IP地**址均接受網路掩碼/32。
- 使用/32地址時，沒有針對EIGRP鄰居的**子網驗**證。

摘要

EIGRP行為由**ip unnumbered**命令更改。建立EIGRP鄰接時，它會禁用對同一子網的檢查。

此外，還必須記住，當您在虛擬模板上使用DVTI靜態配置的IP地址時，它不會克隆到虛擬訪問。這就是需要**ip unnumbered**命令的原因。

對於FlexVPN，當您在客戶端上使用協商地址時，無需使用**ip unnumbered**命令。但是，在使用EIGRP時，在集線器上使用它非常重要。使用配置模式進行路由時，不需要EIGRP。

對於SVTI，IPv6使用本地鏈路地址進行鄰接，無需使用**ipv6 unnumbered**命令。

對於DVTI，無法手動配置IPv6。對於集線器，建議使用**ipv6 unnumbered**命令；對於分支，建議使用**ipv6 address negotiated**命令。

相關資訊

- Cisco IOS 15.3 FlexVPN配置指南
- Cisco IOS 15.3命令參考
- 技術支援與文件 - Cisco Systems