Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[EIGRP en un segmento Ethernet con diversas subredes](#)
[EIGRP en el segmento SVTI con diversas subredes](#)
[Utilice el comando IP unnumbered](#)
[EIGRP en SVTI al segmento DVTI con diversas subredes](#)
[EIGRP en IKEv2 la flexión VPN con diversas subredes](#)
[Modo de configuración para rutear](#)
[EIGRP del IPV6 en el segmento SVTI con diversas subredes](#)
[EIGRP del IPV6 en IKEv2 la flexión VPN con diversas subredes](#)
[Verificación](#)
[Troubleshooting](#)
[Advertencias conocidas](#)
[Resumen](#)
[Información relacionada](#)

Introducción

Este documento describe cómo configurar el Enhanced Interior Gateway Routing Protocol (EIGRP) en varios escenarios común-encontrados en el ® del Cisco IOS. Para validar una adyacencia del vecino EIGRP, el Cisco IOS debe obtener el paquete de saludo EIGRP de una dirección IP dentro de la misma subred. Es posible inhabilitar esa verificación con el **comando ip unnumbered**.

La primera parte del artículo presenta un error del EIGRP cuando recibe un paquete que no esté en la misma subred.

Otro ejemplo demuestra el uso del **comando ip unnumbered** que inhabilita esa verificación, y permite que el EIGRP forme una adyacencia entre los pares que pertenecen a diversas subredes.

Este artículo también presenta un despliegue del hub and spoke de FlexVPN con una dirección IP enviada del servidor. Para este escenario, la verificación de las subredes se inhabilita para el **comando ip address negotiated** y también para el **comando ip unnumbered**. Utilizan al **comando ip unnumbered** sobre todo para las interfaces de punto a punto del tipo (P2P), y esto hace FlexVPN un ajuste perfecto puesto que se basa en una arquitectura P2P.

Pasado, un escenario del IPv6 se presenta junto con las diferencias para las interfaces del túnel virtuales estáticas (SVTI) y las interfaces del túnel virtuales dinámicas (DVTI). Hay cambios leves en el comportamiento cuando usted compara el IPv6 a los escenarios del IPv4.

Además, los cambios entre las versiones deL Cisco IOS 15.1 y 15.3 se presentan (Id. de bug

Cisco CSCtx45062).

El comando ip unnumbered es siempre necesario para DVTI. Esto es porque los IP Addresses estático-configurados en una interfaz de plantilla virtual nunca se reproducen a una interfaz de acceso virtual. Por otra parte, una interfaz sin una dirección IP configurada no puede establecer ninguna adyacencia del Dynamic Routing Protocol. **El comando ip unnumbered** no es necesario para SVTI, pero sin esa subred, se realiza la verificación cuando se establece la adyacencia del Dynamic Routing Protocol. También el comando **innumerable del IPv6** no es necesario para los escenarios del IPV6 debido a las direcciones locales del link que se utilizan para construir las adyacencias del EIGRP.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento básico de estos temas:

- Configuración VPN en el Cisco IOS
- Configuración de FlexVPN en el Cisco IOS

Componentes Utilizados

La información en este documento se basa en la versión deL Cisco IOS 15.3T.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

EIGRP en un segmento Ethernet con diversas subredes

Topología: Router1 (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
```

Demostraciones del r1:

```
*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
```

El Cisco IOS no forma una adyacencia, se espera que. ¿Para más información sobre esto, refiera a qué hacen el medio del mensajes “No en subred común” del EIGRP? artículo.

EIGRP en el segmento SVTI con diversas subredes

La misma situación ocurre cuando usted utiliza las interfaces del túnel virtuales (VTI) (túnel del Generic Routing Encapsulation (GRE)).

Topología: 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
```

Demostraciones del r1:

```
*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
```

Debe ocurrir lo siguiente.

Utilice el comando IP unnumbered

Este ejemplo muestra cómo utilizar el **comando ip unnumbered** que inhabilita la verificación y tiene en cuenta el establecimiento de una sesión del EIGRP entre los pares en diversas subredes.

La topología es similar al ejemplo anterior, pero los direccionamientos de los túneles ahora se definen vía el **comando ip unnumbered** que las puntas a los loopback:

Topología: 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
```

Demostraciones del r1:

```
*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
```

El r2 es similar a esto.

Después de que usted cambie el comando ip unnumbered en una configuración de IP Address específica, una adyacencia del EIGRP no forma.

EIGRP en SVTI al segmento DVTI con diversas subredes

Este ejemplo también utiliza el comando ip unnumbered. Las reglas mencionadas previamente se aplican a DVTI también.

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

El ejemplo anterior se modifica aquí para utilizar DVTI en vez de SVTI. Además, la protección del túnel se agrega en este ejemplo.

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
```

Todo trabaja como se esperaba:

```
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
```

En cuanto a los ejemplos anteriores, cuando usted intenta configurar 172.16.0.1 y 172.17.0.2 directamente bajo interfaces del túnel, el EIGRP falla con exactamente el mismo error que antes.

EIGRP en IKEv2 la flexión VPN con diversas subredes

Aquí está el ejemplo para la configuración del hub and spoke de FlexVPN. El servidor envía la dirección IP vía el modo de configuración para el cliente.

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

Configuración del concentrador (r1):

```
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
```

Configuración radial:

```
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
```

Las aplicaciones SVTI del spoke para conectar con el concentrador que utiliza DVTI para todo el spokes. Porque el EIGRP no es tan flexible como el Open Shortest Path First (OSPF) y no es posibles configurarlo bajo interfaz (SVTI o DVTI), la **red 0.0.0.0** se utiliza en el spoke para asegurarse de que el EIGRP está habilitado en la interfaz **Tun0**. Una interfaz pasiva se utiliza para asegurarse de que la adyacencia está formada solamente en la interfaz **Tun0**.

Para este despliegue, es también necesario configurar el **IP innumerable** en el concentrador. Cuando usted configura manualmente una dirección IP bajo interfaz de plantilla virtual, no se reproduce a la interfaz de acceso virtual. Entonces, la interfaz de acceso virtual no tiene una

dirección IP asignada, y la adyacencia del EIGRP no forma. Esta es la razón por la cual requieren al **comando ip unnumbered** siempre para DVTI interconecta para formar una adyacencia del EIGRP.

En este ejemplo, una adyacencia del EIGRP se construye entre 1.1.1.1 y 192.168.0.9.

Prueba en el concentrador:

```
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
```

De la perspectiva del spoke, el **comando ip address negotiated** trabaja lo mismo que el comando **innumerable del IP Address**, y la verificación de la subred se inhabilita.

Prueba en el spoke:

```
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
```

Modo de configuración para rutear

El intercambio de claves de Internet versión 2 (IKEv2) es otra opción. Es posible utilizar al modo de configuración para avanzar las rutas. En este escenario, el EIGRP y el **comando ip unnumbered** no son necesarios.

Usted puede modificar el ejemplo anterior para configurar el concentrador para enviar esa ruta vía el modo de configuración:

```
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
```

El spoke ve 1.1.1.1 como parásitos atmosféricos, no EIGRP:

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

Los mismos procesos funciona en la dirección opuesta. El spoke envía una ruta al concentrador:

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

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

El concentrador lo ve como parásitos atmosféricos (no EIGRP):

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

Para este escenario, el Dynamic Routing Protocol y el **comando ip unnumbered** no son necesarios.

EIGRP del IPV6 en el segmento SVTI con diversas subredes

Para el IPv6, la situación es diferente. Esto es porque utilizan a las direcciones locales del link del IPv6 (FE80::/10) para construir el EIGRP o la adyacencia OSPF. Las direcciones locales del link válidas pertenecen siempre a la misma subred, tan allí no son ninguna necesidad de utilizar el comando **innumerable del IPv6** para ése.

La topología aquí es lo mismo que para el ejemplo anterior, salvo que todos los direccionamientos del IPv4 se substituyen por los direccionamientos del IPv6.

Configuración del r1:

```
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
```

Configuración del r2:

```
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
```

Los direccionamientos del túnel están en diversas subredes (2001:1::1/64 y 2001:2::2/64), pero eso no es importante. Utilizan a las direcciones locales del link para construir la adyacencia. Con estos direccionamientos, tiene éxito siempre.

En el 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                      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
```

En el 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
```

La red del IPv6 del par es instalada por el proceso EIGRP. En el r1, la red de 2001:2::/64 está instalada, y esa red es una diversa subred que 2001:1::/64. Lo mismo es verdad en el r2. Por ejemplo, 2001::1/64 está instalado, que es una subred para su IP Address de Peer. No hay necesidad del comando **innumerable del IPv6** aquí. Además, no necesitan al **comando address**

del IPv6 en la interfaz del túnel para establecer la adyacencia del EIGRP, porque utilizan a las direcciones locales del link (y ésos se generan automáticamente cuando usted habilita el IPv6 con el comando enable del IPv6).

EIGRP del IPV6 en IKEv2 la flexión VPN con diversas subredes

La configuración DVTI para el IPv6 es diferente que para el IPv4: no es posible configurar un IP Address estático más.

```
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
```

Se espera esto, puesto que nunca reproducen a una dirección estática a una interfaz de acceso virtual. Esta es la razón por la cual el comando innumerable del IPv6 se recomienda para la Configuración del hub, y el comando negociado direccionamiento del IPv6 se recomienda para la configuración radial.

La topología es lo mismo que el ejemplo anterior, salvo que todos los direccionamientos del IPv4 se substituyen por los direccionamientos del IPv6.

Configuración del concentrador (r1):

```
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
```

Configuración del spoke (r2):

```
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
```

Verificación:

```
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
```

Para DVTI, el IPv6 no se puede configurar manualmente. El comando **innumerable del IPv6** se recomienda para el concentrador, y el comando **negociado direccionamiento del IPv6** se recomienda en el spoke.

Este escenario presenta a **IPv6 el** comando **innumerable** para DVTI. Es importante notar que, para el IPv6 en comparación con el IPv4, el comando **innumerable del IPv6** en la interfaz de plantilla virtual no es necesario. La razón de esto es lo mismo que para el escenario del IPv6 SVTI: el direccionamiento del IPv6 del local de la conexión se utiliza para la adyacencia constructiva. La interfaz de acceso virtual, que se reproduce de la virtual-plantilla, hereda la dirección local del link del IPv6, y a ésa es suficiente para construir la adyacencia del EIGRP.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Advertencias conocidas

Id. de bug Cisco CSCtx45062 FlexVPN: El eigrp no debe marcar las subredes comunes si los IP del túnel son /32.

Este bug y arreglo no es FlexVPN-específicos. Ingrese este comando antes de que usted implemente el arreglo (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
```

Ingrese este comando después del arreglo (software 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
```

Hay realmente dos cambios en el Software Release 15.3:

- **El netmask /32** se valida para todos los IP Addresses.
- No hay verificación de la subred para un vecino EIGRP cuando usted utiliza el direccionamiento de **/32**.

Resumen

El comportamiento EIGRP es cambiado por el **comando ip unnumbered**. Inhabilita las comprobaciones para la misma subred mientras que establece una adyacencia del EIGRP.

Es también importante recordar que cuando usted utiliza el IP Address configurado de DVTIs estáticamente en la virtual-plantilla, no está reproducido al acceso virtual. Esta es la razón por la cual el **comando ip unnumbered** es necesario.

Para FlexVPN, no hay necesidad de utilizar el **comando ip unnumbered** cuando usted utiliza a la dirección negociada en el cliente. Pero, es importante utilizarla en el concentrador cuando usted utiliza el EIGRP. Cuando usted utiliza al modo de configuración para rutear, el EIGRP no es necesario.

Para SVTI, el IPv6 utiliza a las direcciones locales del link para la adyacencia, y no hay necesidad de utilizar el comando **innumerable del IPv6**.

Para DVTI, el IPv6 no se puede configurar manualmente. El comando **innumerable del IPv6** se recomienda para el concentrador, y el comando **negociado direccionamiento del IPv6** se recomienda en el spoke.

Información relacionada

- Guía de configuración de FlexVPN del Cisco IOS 15.3
- Cisco IOS 15.3 referencias de comandos
- Soporte Técnico y Documentación - Cisco Systems