# Esempio di configurazione di EIGRP su SVTI, DVTI e IKEv2 FlexVPN con il comando "IP[v6] Unnumber"

## Sommario



## Introduzione

Questo documento descrive come configurare Enhanced Interior Gateway Routing Protocol (EIGRP) in una serie di scenari comuni su Cisco IOS®. Per accettare un router adiacente EIGRP, Cisco IOS deve ottenere il pacchetto EIGRP HELLO da un indirizzo IP nella stessa subnet. È possibile disabilitare questa verifica con il comando **ip unnumber**.

La prima parte dell'articolo presenta un errore EIGRP quando riceve un pacchetto che non si trova nella stessa subnet.

Un altro esempio mostra l'uso del comando **ip unnumber** che disabilita questa verifica e permette a EIGRP di formare un'adiacenza tra peer che appartengono a subnet diverse.

In questo articolo viene inoltre presentata una distribuzione Hub e Spoke FlexVPN con un indirizzo IP inviato dal server. In questo scenario, la verifica delle subnet è disabilitata per il comando **ip address negotiation** e anche per il comando **ip senza numero**. Il comando **ip senza numero** viene utilizzato principalmente per le interfacce Point-to-Point (P2P) e questo rende

FlexVPN una soluzione ideale poiché è basato su un'architettura P2P.

Infine, viene presentato uno scenario IPv6 con le differenze sia per le interfacce SVTI (Static Virtual Tunnel Interfaces) che per le interfacce DVTI (Dynamic Virtual Tunnel Interfaces). Quando si confrontano gli scenari IPv6 con IPv4, il comportamento cambia leggermente.

Inoltre, vengono presentate le modifiche tra le versioni 15.1 e 15.3 di Cisco IOS (ID bug Cisco CSCtx45062).

il comando **ip senza numero** è sempre necessario per DVTI. Questo perché gli indirizzi IP configurati staticamente su un'interfaccia di modello virtuale non vengono mai duplicati su un'interfaccia di accesso virtuale. Inoltre, un'interfaccia senza un indirizzo IP configurato non è in grado di stabilire alcuna adiacenza del protocollo di routing dinamico. il comando **ip senza numero** non è necessario per SVTI, ma senza tale subnet, la verifica viene eseguita quando viene stabilita l'adiacenza del protocollo di routing dinamico. Inoltre, il comando **ipv6 senza numero** non è necessario per gli scenari IPV6 a causa degli indirizzi locali del collegamento utilizzati per compilare le adiacenze EIGRP.

# Prerequisiti

## Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Configurazione VPN su Cisco IOS
- Configurazione FlexVPN su Cisco IOS

## Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco IOS versione 15.3T.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# EIGRP su un segmento Ethernet con subnet diverse

**Topologia:** Router 1 (R1) (e0/0: 10.0.0.1/24)-------(e0/1: 10.0.1.2/24) Router 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 mostra:

```
*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 non forma un'adiacenza, come invece è previsto. Per ulteriori informazioni su questo argomento, consultare il documento What Do EIGRP "Not On Common Subnet" Messages? (Cosa significano i messaggi EIGRP "non nella subnet comune") articolo.

# EIGRP su segmento SVTI con subnet diverse

La stessa situazione si verifica quando si utilizzano le interfacce del tunnel virtuale (VTI, Generic Routing Encapsulation) (tunnel GRE).

**Topologia:** 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 mostra:

```
*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
```

Si tratta di un comportamento normale.

## Utilizzare il comando IP senza numero

Nell'esempio viene mostrato come usare il comando **ip unnumber** che disabilita la verifica e consente di stabilire una sessione EIGRP tra peer di subnet diverse.

La topologia è simile a quella dell'esempio precedente, ma gli indirizzi dei tunnel sono ora definiti con il comando **ip senza numero** che punta ai loopback:

**Topologia:** 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 mostra:

```
*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 è simile a questo.

Dopo aver modificato il comando **ip senza numero** in una configurazione di indirizzo IP specifica, non viene creata alcuna adiacenza EIGRP.

# EIGRP su segmento SVTI-DVTI con subnet diverse

In questo esempio viene inoltre utilizzato il comando ip unnumber. Le regole citate in precedenza si applicano anche a DVTI.

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

L'esempio precedente viene modificato in questo punto in modo da utilizzare DVTI anziché SVTI. Inoltre, nell'esempio viene aggiunta la protezione del tunnel.

**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
```

Tutto funziona come previsto:

```
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
```

Come negli esempi precedenti, quando si cerca di configurare 172.16.0.1 e 172.17.0.2 direttamente nelle interfacce del tunnel, il protocollo EIGRP ha esito negativo con lo stesso errore di prima.

# EIGRP su VPN Flex IKEv2 con subnet diverse

Di seguito è riportato l'esempio della configurazione FlexVPN Hub and Spoke. Il server invia l'indirizzo IP tramite la modalità di configurazione del client.

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

Configurazione hub (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
```

## Configurazione spoke:

```
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
```

Il raggio utilizza SVTI per collegarsi all'hub che utilizza DVTI per tutti i raggi. Poiché EIGRP non è flessibile come Open Shortest Path First (OSPF) e non è possibile configurarlo tramite l'interfaccia (SVTI o DVTI), sullo spoke viene utilizzata la **rete 0.0.0.0** per garantire che EIGRP sia abilitato sull'interfaccia **Tun0**. Per verificare che l'adiacenza si formi solo sull'interfaccia **Tun0,** viene usata un'interfaccia passiva.

Per questa distribuzione, è anche necessario configurare **ip senza numero** sull'hub. L'indirizzo IP configurato manualmente nell'interfaccia del modello virtuale non viene duplicato nell'interfaccia di accesso virtuale. Quindi, all'interfaccia di accesso virtuale non è assegnato un indirizzo IP e l'adiacenza EIGRP non si forma. Per questo motivo, per formare un'adiacenza EIGRP le interfacce DVTI devono sempre usare il comando **ip unnumber**.

Nell'esempio, viene creata un'adiacenza EIGRP compresa tra 1.1.1.1 e 192.168.0.9.

Test sull'hub:

```
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
```

Dal punto di vista Spoke, il comando **ip address negotiation** funziona come il comando **ip address unnumber** e la verifica della subnet è disabilitata.

Test sul raggio:

```
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
```

## Modalità di configurazione per il routing

IKEv2 (Internet Key Exchange versione 2) è un'altra opzione. È possibile usare la modalità di configurazione per eseguire il push dei percorsi. in questo scenario, non è necessario usare il comando **EIGRP** e il comando **ip unnumber**.

Èpossibile modificare l'esempio precedente per configurare l'hub in modo che invii il percorso tramite la modalità di configurazione:

```
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
```

Per il spoke 1.1.1.1 è statico, non EIGRP:

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

Lo stesso processo funziona nella direzione opposta. Spoke invia un percorso all'hub:

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

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

L'hub lo considera statico (non EIGRP):

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

in questo scenario, non è necessario usare il protocollo di routing dinamico e il comando **ip senza numero**.

# IPV6 EIGRP su segmento SVTI con subnet diverse

Per l'IPv6 la situazione è diversa. Ciò è dovuto al fatto che gli indirizzi locali del collegamento IPv6 (FE80::/10) vengono utilizzati per creare l'adiacenza EIGRP o OSPF. Gli indirizzi locali del collegamento validi appartengono sempre alla stessa subnet, pertanto non è necessario utilizzare il comando **ipv6 senza numero**.

La topologia è la stessa dell'esempio precedente, con la differenza che tutti gli indirizzi IPv4 vengono sostituiti con indirizzi IPv6.

Configurazione 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
```

Configurazione 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
```

Gli indirizzi del tunnel sono in subnet diverse (2001:1:1/64 e 2001:2:2/64), ma questo non è importante. Gli indirizzi locali del collegamento vengono utilizzati per creare l'adiacenza. Con questi indirizzi ha sempre esito positivo.

In 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
```

In 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 rete IPv6 peer viene installata dal processo EIGRP. In R1 è installata la rete 2001:2::/64, che è una subnet diversa da 2001:1::/64. Lo stesso vale per R2. Ad esempio, è installata la rete 2001::1/64, che è una subnet per il relativo indirizzo IP peer. Non è necessario utilizzare il comando **ipv6 senza numero**. Inoltre, il comando **ipv6 address** non è necessario sull'interfaccia del tunnel per stabilire l'adiacenza EIGRP, in quanto vengono utilizzati indirizzi locali del collegamento, che vengono generati automaticamente quando si abilita IPv6 con il comando **ipv6 enable**.

# IPV6 EIGRP su VPN Flex IKEv2 con subnet diverse

La configurazione DVTI per IPv6 è diversa da quella per IPv4: non è più possibile configurare un indirizzo IP statico.

```
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
```

Ciò è previsto, poiché un indirizzo statico non viene mai duplicato in un'interfaccia di accesso virtuale. Per questo motivo, il comando **ipv6 senza numero** è consigliato per la configurazione Hub e il comando **ipv6 address negotiation** è consigliato per la configurazione Spoke.

La topologia è la stessa dell'esempio precedente, con la differenza che tutti gli indirizzi IPv4 vengono sostituiti con indirizzi IPv6.

Configurazione hub (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
```

Configurazione raggio (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
```

## Verifica:

```
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
```

Per DVTI, IPv6 non può essere configurato manualmente. Il comando **ipv6 senza numero** è consigliato per l'hub e il comando **ipv6 address negotiation** è consigliato per il spoke.

In questo scenario viene illustrato il comando **ipv6 unnumber** per DVTI. È importante notare che per IPv6 anziché per IPv4, non è necessario il comando **ipv6 senza numero** sull'interfaccia del modello virtuale. Il motivo è lo stesso dello scenario SVTI IPv6: l'indirizzo ipv6 locale del collegamento viene utilizzato per la compilazione dell'adiacenza. L'interfaccia di accesso virtuale, duplicata dal modello virtuale, eredita l'indirizzo locale del collegamento IPv6 e ciò è sufficiente per creare l'adiacenza EIGRP.

# Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

# Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa

configurazione.

## Avvertenze note

ID bug Cisco CSCtx45062 FlexVPN: Eigrp non deve controllare le subnet comuni se gli ip del tunnel sono /32.

Questo bug e questa correzione non sono specifici di FlexVPN. Immettere questo comando prima di implementare la correzione (software versione 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
```

Immettere questo comando dopo la correzione (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
```

Il software versione 15.3 è stato modificato in due modi:

- **Netmask /32** è accettato per tutti gli indirizzi IP.
- Quando si utilizza l'indirizzo **/32** non è disponibile alcuna verifica della subnet per un router adiacente EIGRP.

## Riepilogo

Il comportamento EIGRP viene modificato dal comando **ip unnumber**. Disabilita i controlli per la stessa subnet mentre stabilisce un'adiacenza EIGRP.

Èinoltre importante ricordare che quando si utilizzano i servizi di virtualizzazione virtuale con indirizzi IP configurati staticamente nel modello virtuale, questi non vengono duplicati nell'accesso virtuale. Per questo motivo, è necessario usare il comando **ip senza numero**.

Per FlexVPN, non è necessario usare il comando **ip unnumber** quando si usa l'indirizzo negoziato sul client. Tuttavia, è importante utilizzarlo sull'hub quando si utilizza EIGRP. Quando si utilizza la modalità di configurazione per il routing, il protocollo EIGRP non è necessario.

Per SVTI, IPv6 utilizza indirizzi locali del collegamento per le adiacenze e non è necessario utilizzare il comando **ipv6 senza numero**.

Per DVTI, IPv6 non può essere configurato manualmente. Il comando **ipv6 senza numero** è consigliato per l'hub e il comando **ipv6 address negotiation** è consigliato per il spoke.

## Informazioni correlate

- Guida alla configurazione di Cisco IOS 15.3 FlexVPN
- Riferimenti per i comandi di Cisco IOS 15.3
- Documentazione e supporto tecnico – Cisco Systems