

# DHCP op SVTI, DVTI en IKEv2 FlexVPN met het "IP[v6] ongenummerd" Configuratievoorbeeld van opdracht

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[DHCP op één Ethernet-segment met verschillende subnetwerken](#)

[DHCP op SVTI-segment met verschillende subnetten](#)

[Gebruik de opdracht Ongenummerd IP](#)

[DHCP op SVTI-segment met verschillende subnetten](#)

[DHCP op IKEv2 Flex VPN met verschillende subnetwerken](#)

[Configuratie-modus voor routing](#)

[IPv6 wanneer u een SVTI-segmentering met verschillende subnetwerken hebt](#)

[IPv6 DHCP op IKEv2 Flex VPN met verschillende subnetwerken](#)

[Verifiëren](#)

[Problemen oplossen](#)

[gekende Caveats](#)

[Samenvatting](#)

[Verwante informatie](#)

## Inleiding

Dit document beschrijft hoe u het Enhanced Interior Gateway Routing Protocol (DHCP) kunt configureren in een aantal vaak voorkomende scenario's op Cisco IOS<sup>®</sup>. Om een aangrenzende nabijheid te accepteren EBRE moet Cisco IOS het HELLO-pakket EBRE van een IP-adres binnen hetzelfde voorwerp verkrijgen. Het is mogelijk om die verificatie uit te schakelen met de **ip ongenummerde** opdracht.

Het eerste deel van het artikel stelt een mislukking van Ecu voor wanneer het een pakket ontvangt dat niet in zelfde vorm is.

Een ander voorbeeld demonstreert het gebruik van de **ip ongenummerde** opdracht die verificatie blokkeert, en toestaat EIS om een nabijheid tussen gelijken te vormen die tot verschillende subnetten behoren.

Dit artikel presenteert ook een FlexVPN hub en Spoke plaatsing met een IP adres dat van de server wordt verzonden. Voor dit scenario is verificatie van subnetten uitgeschakeld voor de **IP-**

**adresonderhandelde** opdracht en ook voor de **ip ongenummerde** opdracht. De **ip ongenummerde** opdracht wordt voornamelijk gebruikt voor point-to-point (P2P) type interfaces, en dit maakt FlexVPN een perfecte fit omdat deze gebaseerd is op een P2P architectuur.

Ten slotte wordt een IPv6-scenario gepresenteerd samen met verschillen voor zowel Static Virtual Tunnel Interfaces (SVTI) als Dynamic Virtual Tunnel Interfaces (DVTI). Er zijn kleine gedragsveranderingen wanneer u IPv6 met IPv4-scenario's vergelijkt.

Daarnaast worden de wijzigingen tussen Cisco IOS versies 15.1 en 15.3 gepresenteerd ([Cisco bug ID CSCtx45062](#)).

De **ip ongenummerde** opdracht is altijd nodig voor DVTI. Dit komt doordat statisch geconfigureerde IP-adressen op een virtuele-sjabloon-interface nooit naar een virtuele-toegangsinterface zijn gekloond. Bovendien is een interface zonder een IP adres ingesteld niet in staat om dynamische routingprotocol nabijheid tot stand te brengen. De **ip ongenummerde** opdracht is niet nodig voor SVTI, maar zonder dat subtype, wordt verificatie uitgevoerd wanneer dynamische routingprotocol nabijheid wordt vastgesteld. Ook de **ipv6 niet genummerde** opdracht is niet nodig voor IPV6 scenario's wegens de verbinding-lokale adressen die worden gebruikt om nabijheid te bouwen EBRD.

## Voorwaarden

### Vereisten

Cisco raadt u aan basiskennis van deze onderwerpen te hebben:

- VPN-configuratie op Cisco IOS
- FlexVPN-configuratie op Cisco IOS

### Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco IOS versie 15.3T.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## DHCP op één Ethernet-segment met verschillende subnetwerken

**Topologie:** 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 toont:**

```
*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 vormt geen nabijheid, wat wordt verwacht. Raadpleeg voor meer informatie hierover de [betekenis](#) van "[Not on Common Subnet](#)" berichten? artikel.

## DHCP op SVTI-segment met verschillende subnetten

De zelfde situatie komt voor wanneer u Virtual Tunnel Interfaces (VTI) (Generic Routing Encapsulation (GRE) Tunnel) gebruikt.

**Topologie:** 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 toont:**

```
*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
```

Dit wordt verwacht.

## Gebruik de opdracht Ongenummerd IP

Dit voorbeeld toont hoe te om de **ip ongenummerde** opdracht te gebruiken die verificatie schakelt en voor de vestiging van een zitting Ecu tussen gelijken in verschillende subnetten toelaat.

De topologie is gelijk aan het vorige voorbeeld, maar de adressen van de tunnels worden nu gedefinieerd via de **ip ongenummerde** opdracht die op loopbacks wijst:

**Topologie:** 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 toont:

```
*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
```

**(Tunnell) is up: new adjacency**

R1#**show ip eigrp neighbors**

EIGRP-IPv4 Neighbors for AS(100)

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq 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, Tunnell

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
Tunnell	172.16.0.1	YES	TFTP	up	up

R2 is vergelijkbaar.

Nadat u de **ip ongenummerde** opdracht in een specifieke IP adresconfiguratie verandert, vormt een nabijheid Ecu geen vorm.

## DHCP op SVTI-segment met verschillende subnetten

Dit voorbeeld gebruikt ook de ip ongenummerde opdracht. De eerder genoemde regels zijn ook van toepassing op DVTI.

**Topologie:** R1(Tun1): 172.16.0.1/24)—(Virtuele sjabloon: 172.17.0.2/24) R2

Het vorige voorbeeld wordt hier gewijzigd om DVTI in plaats van SVTI te gebruiken. Daarnaast wordt in dit voorbeeld tunnelbescherming toegevoegd.

**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 Tunnell
  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 Tunnell
```

**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
```

Alles werkt zoals verwacht:

**R1#show crypto session**

```
Crypto session current status
Interface: Tunnell
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: Tunnell
  Crypto map tag: Tunnell-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
```

Zoals bij de vorige voorbeelden, wanneer u probeert om 172.16.0.1 en 172.17.0.2 direct onder de tunnelinterfaces te vormen, faalt ER Ecp met precies de zelfde fout zoals voordien.

## DHCP op IKEv2 Flex VPN met verschillende subnetwerken

Hier is het voorbeeld voor de FlexVPN hub en de Spoke-configuratie. De server stuurt het IP-adres via de configuratiemodus voor de client.

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

Configuratie 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

```

## Spelconfiguratie:

```

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

```

De Spoke gebruikt SVTI om verbinding te maken met de hub die DVTI voor alle spaken gebruikt. Omdat DHCP niet zo flexibel is als Open Kortste Pad Eerst (OSPF) en het niet mogelijk is om het onder de interface (SVTI of DVTI) te configureren wordt **netwerk 0.0.0.0** gebruikt op de Spoke om ervoor te zorgen dat DHCP op de **Tun0**-interface is ingeschakeld. Er wordt een passieve interface gebruikt om ervoor te zorgen dat de nabijheid alleen op de **Tun0**-interface wordt gevormd.

Voor deze plaatsing, is het ook noodzakelijk om **ip ongenummerd** op de hub te configureren. Wanneer u handmatig een IP-adres configureren onder de virtuele-sjabloon-interface, wordt het niet gekloond naar de virtuele-toegangsinterface. Vervolgens heeft de virtuele-toegangsinterface geen IP-adres toegewezen, en de nabijheid Eur vormt geen vorm. Dit is waarom de **ip ongenummerde** opdracht altijd voor DVTI interfaces vereist is om een nabijheid te vormen Ecu.

In dit voorbeeld, wordt een nabijheid Eur gebouwd tussen 1.1.1.1 en 192.168.0.9.

Op de hub testen:

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	<b>1.1.1.1</b>	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
```

Vanuit het Spoke-perspectief, werkt het **IP-adres** dat **via onderhandelingen** tot stand is gebracht, hetzelfde als het **IP-adres dat niet is genummerd**, en wordt de verificatie van het subtype uitgeschakeld.

Test op de 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	<b>2.2.2.2</b>	YES	NVRAM	up	up
Tunnel0	<b>192.168.0.9</b>	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
```

## Configuratie-modus voor routing

Internet Key Exchange versie 2 (IKEv2) is een andere optie. Het is mogelijk de configuratie-modus te gebruiken om de routes te duwen. In dit scenario zijn wanneer u een **NU niet genummerde** opdracht gebruikt, u geen EHRM en de **ip niet** nodig.

U kunt het vorige voorbeeld wijzigen om de Hub te configureren om die route via configuratiemodus te verzenden:

```
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
```

Sprake ziet 1.1.1.1 als statisch, niet als een Ecu:

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

Hetzelfde proces werkt in de tegenovergestelde richting. De Spoke stuurt een route naar de 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
```

De hub ziet het als statisch (niet wanneer u een Noord-Europese luchthaven instelt):

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

Voor dit scenario zijn het dynamische routingprotocol en de **ip ongenummerde** opdracht niet nodig.

## IPv6 wanneer u een SVTI-segmentering met verschillende subnetwerken hebt

Voor IPv6 is de situatie anders. Dit is omdat IPv6 link-lokale adressen (FE80::/10) worden gebruikt om Eur of OSPF nabijheid te bouwen. Geldige link-lokale adressen behoren altijd tot het zelfde voorwerp, zodat is er geen behoefte om de **ipv6 ongenummerde** opdracht daarvoor te gebruiken.

De topologie hier is het zelfde als voor het vorige voorbeeld, behalve dat alle IPv4 adressen door IPv6 adressen worden vervangen.

Configuratie R1:

```
interface Tunnell
  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
```

configuratie R2:

```
interface Tunnell
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
```

De tunneladressen zijn in verschillende subnetten (2001:1:1/64 en 2001:2:2/64), maar dat is niet belangrijk. Link-lokale adressen worden gebruikt om nabijheid te bouwen. Met deze adressen slaagt het altijd.

Op 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
Tunnell              [up/up]
```

```
FE80:1::1
2001:1::1
```

```
R1#show ipv6 eigrp neighbors
```

```
EIGRP-IPv6 Neighbors for AS(100)
```

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
0	Link-local address: Tu1		12	00:13:58	821	4926	0	17
	<b>FE80:2::2</b>							

```
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
```

Op 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 (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
0	Link-local address: Tu1		14	00:15:31	21	1470	0	18
	<b>FE80:1::1</b>							

```
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
```

Het peer IPv6 netwerk wordt geïnstalleerd door het EIS proces. Op R1, is het 2001:2:/64 netwerk geïnstalleerd, en dat netwerk is een ander net dan 2001:1:/64. Hetzelfde geldt voor R2. Bijvoorbeeld, 2001::1/64 is geïnstalleerd, wat een net voor zijn peer IP adres is. Het **ongegenummerde ipv6**-commando is niet nodig. Daarnaast is de opdracht **ipv6-adres** niet nodig op de tunnelinterface om nabijheid te maken Ecu, omdat de verbinding-lokale adressen automatisch worden gebruikt (en die worden gegenereerd wanneer u IPv6 met **ipv6 toelaat** bevel).

## IPv6 DHCP op IKEv2 Flex VPN met verschillende subnetwerken

DVTI-configuratie voor IPv6 is anders dan voor IPv4: het is niet mogelijk om een statisch IP-adres meer te configureren.

```
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
```

Dit wordt verwacht, omdat een statisch adres nooit op een virtuele-toegangsinterface wordt gekloond. Dit is waarom de **ipv6 ongenummerde** opdracht wordt aanbevolen voor de hubconfiguratie en de **ipv6**-opdracht **waarover** is onderhandeld, wordt aanbevolen voor de Spoke-configuratie.

De topologie is het zelfde als het vorige voorbeeld, behalve dat alle IPv4 adressen door IPv6 adressen worden vervangen.

### Configuratie 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-Templatel 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
```

## Configuratie 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
```

## Verificatie:

R2#**show ipv6 eigrp neighbors**

EIGRP-IPv6 Neighbors for AS(100)

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
0	Link-local address: Tu0 FE80::A8BB:CCFF:FE00:6500		11 00:12:32	17	1440	0	12

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

Voor DVTI kan IPv6 niet handmatig worden ingesteld. De **ongenummerde** opdracht **ipv6** wordt aanbevolen voor de hub en de opdracht **ipv6 via IP-adres** wordt op de Spoke aanbevolen.

Dit scenario presenteert de **ipv6 ongenummerde** opdracht voor DVTI. Het is belangrijk om op te merken dat, voor IPv6 in plaats van IPv4, de **ipv6 ongenummerde** opdracht op de virtuele-sjabloon interface niet nodig is. De reden hiervoor is dezelfde als voor het IPv6 SVTI-scenario: het link-lokale ipv6-adres wordt gebruikt om nabijheid te bouwen. De virtuele-Access interface, die van het virtueel-sjabloon wordt gekloond, erft het IPv6 link-lokaal adres en dat is genoeg om nabijheid te bouwen Ecu.

## Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.



# Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

## gekende Caveats

[Cisco bug-id CSCtx45062](#) FlexVPN: Eigrp mag geen gemeenschappelijke subnetten controleren als de ip's van de tunnel /32 zijn.

Dit bug en repareren is niet specifiek voor FlexVPN. Voer deze opdracht in voordat u de oplossing implementeert (softwarerelease 15.1):

```
R2(config-if)#do show run int tun1
Building configuration...

Current configuration : 165 bytes

interface Tunnell
 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
```

Typ deze opdracht na de tijdelijke versie (software 15.3):

```
R2(config-if)#do show run int tun1
Building configuration...

Current configuration : 165 bytes

interface Tunnell
 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 (Tunnell) is up: new adjacency
```

Er zijn feitelijk twee veranderingen in softwarerelease 15.3:

- **Netmask /32** wordt voor alle IP adressen geaccepteerd.
- Er is geen Subnet verificatie voor een EcpBuren wanneer u het /32 adres gebruikt.

## Samenvatting

Het gedrag Ecu wordt gewijzigd door de **ip ongenummerde** opdracht. Het schakelt controles voor zelfde net uit terwijl het een nabijheid Ecp vaststelt.

Het is ook belangrijk om eraan te herinneren dat wanneer u DVTIs op het virtueel sjabloon

standaard ingesteld IP-adres gebruikt, het niet op de virtuele toegang is gekloond. Dit is waarom de **ip ongenummerde** opdracht nodig is.

Voor FlexVPN hoeft de **ip ongenummerde** opdracht niet te worden gebruikt wanneer u het overeengekomen adres op de client gebruikt. Maar het is belangrijk om het op de hub te gebruiken wanneer u Ecu gebruikt. Wanneer u de configuratiewijze voor het routing gebruikt, is ER geen nodig.

Voor SVTI gebruikt IPv6 link-lokale adressen voor nabijheid, en er is geen behoefte om de **ipv6 ongenummerde** opdracht te gebruiken.

Voor DVTI kan IPv6 niet handmatig worden ingesteld. De **ongenummerde** opdracht **ipv6** wordt aanbevolen voor de hub en de opdracht **ipv6 via IP-adres** wordt op de Spoke aanbevolen.

## Verwante informatie

- [Cisco IOS 15.3 FlexVPN-configuratiehandleiding](#)
- [Cisco IOS 15.3 Opdrachtreferenties](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)