Contenu

Introduction

Ce document décrit comment configurer le Protocole EIGPR (Enhanced Interior Gateway Routing Protocol) dans un certain nombre de scénarios commun-rencontrés sur le Cisco IOS®. Afin de recevoir une contiguïté de voisinage EIGRP, le Cisco IOS doit obtenir le paquet HELLO EIGRP d'une adresse IP dans le même sous-réseau. Il est possible de désactiver cette vérification avec la commande d'**ip unnumbered**.

La première partie de l'article présente une panne EIGRP quand elle reçoit un paquet qui n'est pas dans le même sous-réseau.

Un autre exemple explique l'utilisation de la commande d'**ip unnumbered** qui désactive cette vérification, et permet à l'EIGRP pour former une contiguïté entre les pairs qui appartiennent aux différents sous-réseaux.

Cet article présente également un déploiement de hub and spoke de FlexVPN avec une adresse IP envoyée du serveur. Pour ce scénario, la vérification des sous-réseaux est désactivée pour la commande d'**ip address negotiated** et également pour la commande d'**ip unnumbered**. La commande d'**ip unnumbered** est principalement utilisée pour les interfaces point par point de type (de P2P), et ceci fait à FlexVPN une adaptation parfaite puisqu'il est basé sur une architecture de P2P.

Pour finir, un scénario d'IPv6 est présenté avec des différences pour les interfaces de tunnel virtuelles statiques (SVTI) et les interfaces de tunnel virtuelles dynamiques (DVTI). Il y a de légers changements du comportement quand vous comparez l'IPv6 aux scénarios d'ipv4.

Supplémentaire, les modifications entre les versions 15.1 et 15.3 de Cisco IOS sont présentées (ID de bogue Cisco CSCtx45062).

La commande d'**ip unnumbered** est toujours nécessaire pour DVTI. C'est parce que des adresses IP statique-configurées sur une interface de modèle virtuel ne sont jamais copiées à une interface d'accès virtuel. D'ailleurs, une interface sans adresse IP configurée ne peut pas n'établir aucune contiguïté de protocole de routage dynamique. La commande d'**ip unnumbered** n'est pas nécessaire pour SVTI, mais sans ce sous-réseau, la vérification est exécutée quand la contiguïté de protocole de routage dynamique est établie. Également la commande d'**ipv6 unnumbered** n'est pas nécessaire pour des scénarios d'IPV6 en raison des adresses locales à la liaison qui sont utilisées afin d'établir des contiguïtés EIGRP.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration du VPN sur le Cisco IOS
- Configuration de FlexVPN sur le Cisco IOS

Composants utilisés

Les informations dans ce document sont basées sur la version 15.3T de Cisco IOS.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

EIGRP sur un segment d'Ethernets avec des différents sous-réseaux

Topologie : Routeur 1 (R1) (e0/0 : 10.0.0.1/24)-------(e0/1 : 10.0.1.2/24) Router2 (R2)

R1:
```
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0

router eigrp 100
network 10.0.0.1 0.0.0.0
```

R2:
```
interface Ethernet0/0
ip address 10.0.1.2 255.255.255.0

router eigrp 100
network 10.0.1.2 0.0.0.0
```

Expositions 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
```

Le Cisco IOS ne forme pas une contiguïté, qui est prévue. Pour plus d'informations sur ceci, référez-vous au ce qui font le moyen de messages sur sous-réseau commun EIGRP « pas » ? article.

EIGRP sur le segment SVTI avec des différents sous-réseaux

La même situation se produit quand vous utilisez les interfaces de tunnel virtuelles (VTI) (tunnel d'Encapsulation de routage générique (GRE)).

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
```

Expositions 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
```

C'est comportement prévu.

Utilisez la commande d'ip unnumbered

Cet exemple affiche comment utiliser la commande d'**ip unnumbered** qui désactive la vérification et tient compte de l'établissement d'une session EIGRP entre les pairs dans les différents sous-

réseaux.

La topologie est semblable à l'exemple précédent, mais les adresses des tunnels sont maintenant définies par l'intermédiaire de la commande d'**ip unnumbered** ces points aux bouclages :

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
```

Expositions 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
```

R2 est semblable à ceci.

Après que vous changiez la commande d'**ip unnumbered** dans une configuration des adresses IP spécifique, une contiguïté EIGRP ne forme pas.

EIGRP sur SVTI au segment DVTI avec des différents sous-réseaux

Cet exemple utilise également la commande d'ip unnumbered. Les règles mentionnées précédemment s'appliquent à DVTI aussi bien.

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

L'exemple précédent est modifié ici afin d'utiliser DVTI au lieu de SVTI. Supplémentaire, le tunnel protection est ajouté dans cet exemple.

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
```

Tout fonctionne comme prévu :

```
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
```

Quant aux exemples précédents, quand vous essayez de configurer 172.16.0.1 et 172.17.0.2 directement sous les interfaces de tunnel, l'EIGRP échoue avec exactement la même erreur qu'avant.

EIGRP sur IKEv2 le flexible VPN avec des différents sous-réseaux

Voici l'exemple pour la configuration de hub and spoke de FlexVPN. Le serveur envoie l'adresse IP par l'intermédiaire du mode de configuration pour le client.

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

Configuration du 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
```

Configuration en étoile :

```
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
```

Le rai emploie SVTI afin de se connecter au hub qui utilise DVTI pour tous les rais. Puisque l'EIGRP n'est pas aussi flexible que le Protocole OSPF (Open Shortest Path First) et lui n'est pas possible pour le configurer sous l'interface (SVTI ou DVTI), le **réseau 0.0.0.0** est utilisé sur le rai afin de s'assurer que l'EIGRP est activé sur l'interface **Tun0**. Une interface passive est utilisée afin de s'assurer que la contiguïté est formée seulement sur l'interface **Tun0**.

Pour ce déploiement, il est également nécessaire de configurer l'**ip unnumbered** sur le hub. Quand vous configurez manuellement une adresse IP sous l'interface de modèle virtuel, elle n'est pas copiée à l'interface d'accès virtuel. Puis, l'interface d'accès virtuel n'a pas une adresse IP assignée, et la contiguïté EIGRP ne forme pas. C'est pourquoi la commande d'**ip unnumbered** est toujours exigée pour DVTI relie afin de former une contiguïté EIGRP.

Dans cet exemple, une contiguïté EIGRP est établie entre 1.1.1.1 et 192.168.0.9.

Test sur le 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
```

Du point de vue de rai, la commande d'**ip address negotiated** fonctionne les mêmes que la commande **non-numérotée d'IP address**, et la vérification du sous-réseau est désactivée.

Test sur le rai :

```
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
```

Mode de configuration pour l'acheminement

La version 2 (IKEv2) d'échange de clés Internet (IKE) est une autre option. Il est possible d'employer le mode de configuration afin de pousser des artères. Dans ce scénario, l'EIGRP et la commande d'**ip unnumbered** ne sont pas nécessaires.

Vous pouvez modifier l'exemple précédent afin de configurer le hub pour envoyer cette artère par l'intermédiaire du mode de configuration :

```
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
```

Le rai voit 1.1.1.1 en tant que charge statique, pas EIGRP :

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

Les mêmes travaux par processus dans le sens inverse. Le rai envoie une artère au 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
```

Le hub le voit en tant que charge statique (pas EIGRP) :

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

Pour ce scénario, le protocole de routage dynamique et la commande d'**ip unnumbered** ne sont pas nécessaires.

IPV6 EIGRP sur le segment SVTI avec des différents sous-réseaux

Pour l'IPv6, la situation est différente. C'est parce que les adresses locales à la liaison d'IPv6 (FE80::/10) sont utilisées afin d'établir la contiguïté EIGRP ou OSPF. Les adresses locales à la liaison valides appartiennent toujours au même sous-réseau, tellement là n'est aucun besoin d'utiliser la commande d'**ipv6 unnumbered** pour cela.

La topologie ici est identique que pour l'exemple précédent, sauf que toutes les adresses d'ipv4 sont remplacées par des adresses d'IPv6.

Configuration 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
```

Configuration 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
```

Les adresses de tunnel sont dans les différents sous-réseaux (2001:1::1/64 et 2001:2::2/64), mais ce n'est pas importante. Des adresses locales à la liaison sont utilisées afin d'établir la contiguïté. Avec ces adresses, il réussit toujours.

Sur 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
```

Sur 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
```

Le réseau d'IPv6 de pair est installé par le processus EIGRP. Sur R1, le réseau de 2001:2::/64 est installé, et ce réseau est un différent sous-réseau que 2001:1::/64. Le même est vrai sur R2. Par exemple, 2001::1/64 est installé, qui est un sous-réseau pour son adresse IP de pair. Il n'y a aucun besoin de commande d'**ipv6 unnumbered** ici. Supplémentaire, la commande d'**ipv6 addres** n'est pas nécessaire sur l'interface de tunnel afin d'établir la contiguïté EIGRP, parce que des adresses locales à la liaison sont utilisées (et ceux sont générés automatiquement quand vous activez l'IPv6 avec la commande d'**ipv6 enable**).

IPV6 EIGRP sur IKEv2 le flexible VPN avec des différents sous-réseaux

La configuration DVTI pour l'IPv6 est différente que pour l'ipv4 : il n'est pas possible de configurer une adresse IP statique plus.

```
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
```

Ceci est prévu, puisqu'une adresse statique n'est jamais copiée à une interface d'accès virtuel. C'est pourquoi la commande d'**ipv6 unnumbered** est recommandée pour la configuration de hub, et la commande **négociée par ipv6 addres** est recommandée pour la configuration en étoile.

La topologie est identique que l'exemple précédent, sauf que toutes les adresses d'ipv4 sont remplacées par des adresses d'IPv6.

Configuration du 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
```

Configuration du rai (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
```

Vérification :

```
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
```

Pour DVTI, l'IPv6 ne peut pas être configuré manuellement. La commande d'**ipv6 unnumbered** est recommandée pour le hub, et la commande **négociée par ipv6 addres** est recommandée sur le rai.

Ce scénario présente la commande d'**ipv6 unnumbered** pour DVTI. Il est important de noter que, pour l'IPv6 par opposition à l'ipv4, la commande d'**ipv6 unnumbered** sur l'interface de modèle virtuel n'est pas nécessaire. La raison pour ceci est identique que pour le scénario de l'IPv6 SVTI : l'ipv6 addres de lien-gens du pays est utilisé pour la contiguïté de construction. L'interface d'accès virtuel, qui est copiée du virtual-template, hérite de l'adresse locale à la liaison d'IPv6, et de cela est suffisante afin d'établir la contiguïté EIGRP.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Mises en garde connues

ID de bogue Cisco CSCtx45062 FlexVPN : Eigrp ne devrait pas vérifier des sous-réseaux communs si les IP de tunnel sont /32.

Ces bogue et difficulté n'est pas FlexVPN-particularité. Sélectionnez cette commande avant que vous mettiez en application la difficulté (version de logiciel 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
```

Sélectionnez cette commande après la difficulté (logiciel 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 y a réellement deux changements de version de logiciel 15.3 :

- **Le netmask /32** est reçu pour toutes les adresses IP.
- Il n'y a aucune vérification de sous-réseau pour un voisin EIGRP quand vous utilisez l'adresse de **/32**.

Résumé

Le comportement EIGRP est changé par la commande d'**ip unnumbered**. Il désactive vérifie le même sous-réseau tandis qu'il établit une contiguïté EIGRP.

Il est également important de se souvenir que quand vous utilisez l'adresse IP statiquement configurée de DVTIs sur le virtual-template, il n'est pas copié à virtuel-Access. C'est pourquoi la commande d'**ip unnumbered** est nécessaire.

Pour FlexVPN, il n'y a aucun besoin d'utiliser la commande d'**ip unnumbered** quand vous utilisez l'adresse négociée sur le client. Mais, il est important de l'utiliser sur le hub quand vous utilisez l'EIGRP. Quand vous utilisez le mode de configuration pour l'acheminement, l'EIGRP n'est pas nécessaire.

Pour SVTI, l'IPv6 utilise des adresses locales à la liaison pour la contiguïté, et il n'y a aucun besoin d'utiliser la commande d'**ipv6 unnumbered**.

Pour DVTI, l'IPv6 ne peut pas être configuré manuellement. La commande d'**ipv6 unnumbered** est recommandée pour le hub, et la commande **négociée par ipv6 addres** est recommandée sur le rai.

Les informations relatives

- Guide de configuration de FlexVPN du Cisco IOS 15.3
- Cisco IOS 15.3 références de commandes
- Support et documentation techniques - Cisco Systems