Configuration et dépannage de FlexVPN Spoke to Spoke via EIGRP

Table des matières

- Introduction
- Conditions préalables
  - Exigences
- Composants utilisés
- Évolutivité
- Informations générales
  - FlexVPN et NHRP
- Processus NHRP
- Configuration de FlexVPN Spoke to Spoke à l'aide du protocole EIGRP
  - Considérations clés pour la topologie basée sur EIGRP
  - Exemple 1 : utilisation de NHO (Next-Hop-Override) pour la communication satellite à satellite
    - Serveur FlexVPN
    - Client FlexVPN 1
    - Client FlexVPN 2
  - Exemple 2 : utilisation des routes installées par le protocole NHRP pour la communication satellite à satellite
    - Serveur FlexVPN
- Vérification et dépannage
  - Exemple 1 : utilisation de NHO (Next-Hop-Override) pour la communication satellite à satellite
    - Spoke 1 (résolution NHRP avant Spoke to Spoke et établissement du tunnel)
    - Spoke 2 (résolution NHRP avant Spoke to Spoke et établissement du tunnel)
    - Spoke 1 (après résolution NHRP Spoke to Spoke et établissement du tunnel)
    - Satellite 2 (après résolution NHRP satellite à satellite et établissement de tunnel)
  - Exemple 2 : utilisation des routes installées par le protocole NHRP pour la communication satellite à satellite
    - Serveur FlexVPN
    - Clients FlexVPN
- Informations connexes

Introduction

Ce document décrit le déploiement et le dépannage de Cisco FlexVPN satellite à satellite à l'aide d'IKEv2 et de NHRP pour les tunnels de cryptage client direct.

Conditions préalables

- Configuration du concentrateur Flex VPN et du client Flex VPN

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- IKEv2
- VPN reposant sur des routes
- Interfaces de tunnel virtuel (VTI)
- NHRP
- IPSEC
- EIGRP
- VRF-Lite

Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Cisco IOS XE 17.9.4a

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Évolutivité

FlexVPN peut facilement s'étendre des petits bureaux aux grands réseaux d'entreprise. Il peut gérer de nombreuses connexions VPN sans nécessiter beaucoup de travail supplémentaire, ce qui est idéal pour les entreprises en pleine croissance ou ayant de nombreux utilisateurs distants.

Caractéristiques principales :

- Configuration dynamique et tunnels à la demande :
  - Interfaces de tunnel virtuel (VTI) : FlexVPN utilise des VTI qui peuvent être créées et supprimées selon les besoins. Cela signifie que les tunnels VPN sont configurés uniquement en cas de trafic et supprimés lorsqu'ils ne sont pas nécessaires, ce qui permet d'économiser des ressources et d'améliorer l'évolutivité.
  - Protocoles de routage dynamique: Il fonctionne avec des protocoles de routage tels que OSPF, EIGRP et BGP sur des tunnels VPN. Les informations de routage sont ainsi mises à jour automatiquement, ce qui est important pour les grands réseaux dynamiques.
- Flexibilité de déploiement :
  - Modèle Hub-and-Spoke : Un concentrateur central se connecte à plusieurs filiales. FlexVPN simplifie la configuration de ces connexions avec une structure unique, ce qui en fait la solution idéale pour les grands réseaux.
  - Topologies à maillage global et à maillage partiel : Tous les sites peuvent communiquer directement sans passer par un concentrateur central, ce qui réduit les délais et améliore les performances.

- Haute disponibilité et redondance :
    - Concentrateurs redondants : Prend en charge plusieurs concentrateurs pour la sauvegarde. Si un concentrateur tombe en panne, les filiales peuvent se connecter à un autre concentrateur, assurant ainsi une connectivité continue.
    - Équilibrage de charge : Répartit les connexions VPN sur plusieurs périphériques pour éviter qu'un seul périphérique ne soit surchargé, ce qui est essentiel pour maintenir les performances dans les grands déploiements.
- Authentification et autorisation évolutives :
    - Intégration AAA : Fonctionne avec des serveurs AAA tels que Cisco ISE ou RADIUS pour une gestion centralisée des informations d'identification et des politiques des utilisateurs, essentielle pour une utilisation à grande échelle.
    - PKI et certificats : Prend en charge l'infrastructure à clé publique (PKI) et les certificats numériques pour une authentification sécurisée, plus évolutive que l'utilisation de clés prépartagées, en particulier dans les environnements de grande taille.

Informations générales

FlexVPN et NHRP

Le serveur FlexVPN fournit la fonctionnalité côté serveur de FlexVPN. Le client FlexVPN établit un tunnel VPN IPsec sécurisé entre un client FlexVPN et un autre serveur FlexVPN.

NHRP est un protocole de type ARP (Address Resolution Protocol) qui atténue les problèmes de réseau NBMA (nonbroadcast multiaccess). Avec le protocole NHRP, les entités NHRP reliées à un réseau NBMA apprennent dynamiquement l'adresse NBMA des autres entités qui font partie de ce réseau, ce qui permet à ces entités de communiquer directement sans que le trafic doive utiliser un saut intermédiaire.

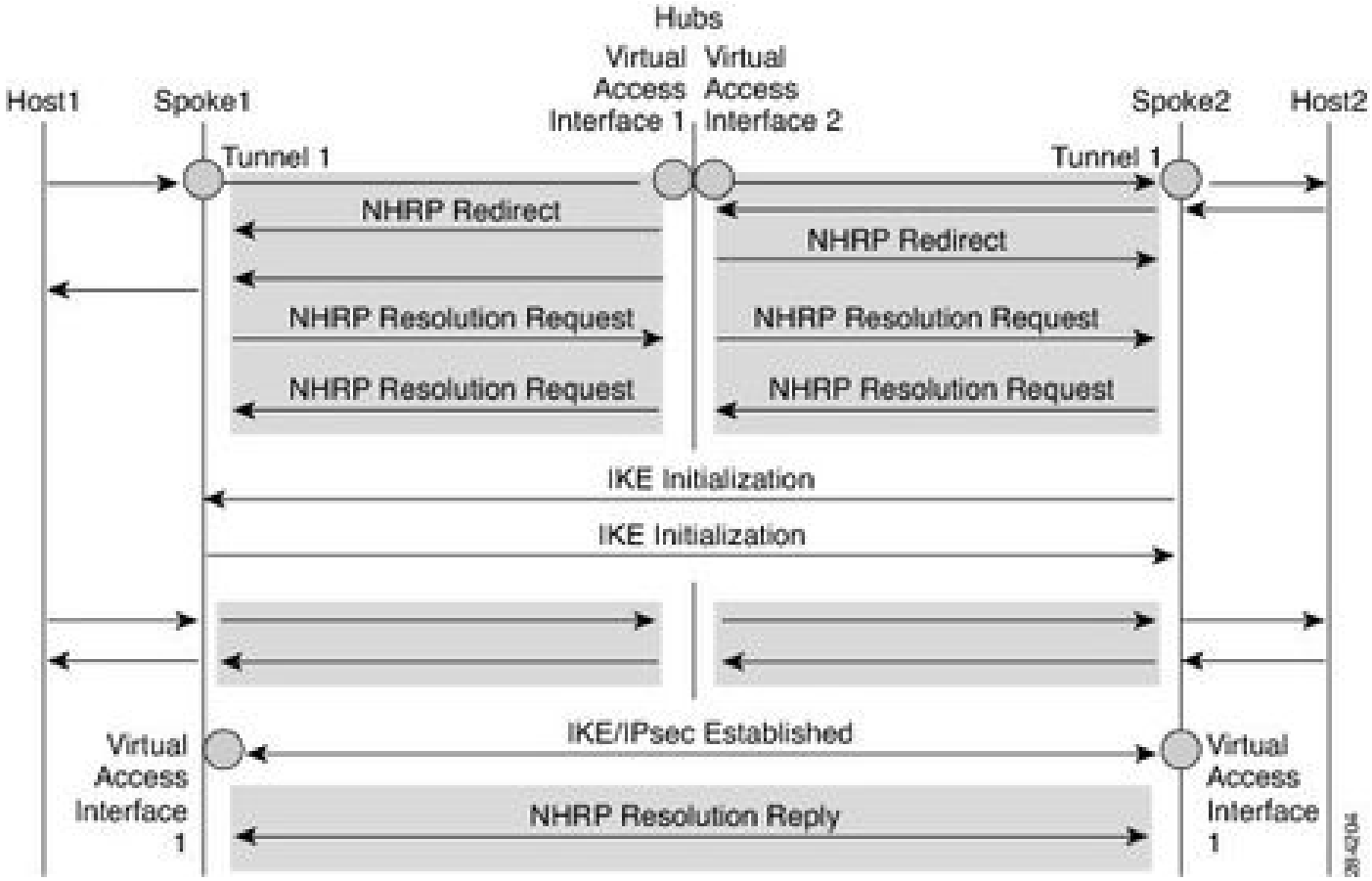
La fonctionnalité Spoke to Spoke de FlexVPN intègre NHRP et le client FlexVPN (spoke) pour établir un canal de chiffrement direct avec un autre client dans un réseau FlexVPN existant. Les connexions sont établies à l'aide des interfaces de tunnel virtuel (VTI), IKEv2 et NHRP, où NHRP est utilisé pour résoudre les clients FlexVPN dans le réseau.

Cisco recommande de s'assurer :

- Les entrées de routage ne sont pas échangées entre les rayons. Une considération clé, expliquée plus loin à mesure que nous progressons dans le dépannage de la topologie basée sur EIGRP.

- Différents profils sont utilisés pour les rayons et la commande config-exchange n'est pas configurée pour les rayons.

Processus NHRP



L'illustration montre le flux de trafic entre Spoke 1 et Spoke 2, avec les réseaux 198.51.100.0/29/24 et 198.51.100.8/29, tous deux annoncés via l'appairage EIGRP directement aux rayons via le concentrateur. Voici à quoi ressemble le flux de trafic lorsque la communication est établie entre Spoke 1 (198.51.100.0/29/24) et Spoke 2 (198.51.100.8/29).

1. L’hôte 1 envoie le trafic destiné à l’hôte 2. La recherche de route sur l’hôte 1 entraîne son transfert vers l’interface du tunnel du concentrateur, car le concentrateur annonce ce réseau via le protocole EIGRP.
2. Lorsque le trafic atteint le concentrateur, la recherche de route d'extrémité du concentrateur confirme que le réseau 198.51.100.8/29 du rayon 2 est appris via l'accès virtuel du rayon 2.
3. Le concentrateur lance la redirection NHRP, car les deux interfaces d'accès virtuel (rayon 1 et rayon 2) font partie du même réseau NHRP ayant le même ID réseau NHRP.
4. À la réception de la redirection, Spoke1 lance une requête de résolution pour le réseau en étoile 2 sur l'interface de tunnel (la même interface sur laquelle il a reçu la redirection). Spoke 2 répète le même processus pour la demande de résolution du réseau Spoke 1.
5. Spoke2 reçoit la demande de résolution sur l'interface du tunnel et récupère le numéro de modèle virtuel tel que défini dans la configuration. Le numéro de modèle virtuel est utilisé pour créer l'interface d'accès virtuelle afin d'établir une session de chiffrement entre deux rayons. Une fois que les SA de chiffrement entre les deux rayons sont actives, les deux rayons installent des routes d'adresse IP de tronçon suivant apprises via IPSEC après l'établissement des interfaces d'accès virtuel.
6. Les deux rayons procèdent ensuite à la vérification de l'accessibilité du tronçon suivant avant d'envoyer la réponse de résolution via la nouvelle interface d'accès virtuel pour la connectivité satellite à satellite.

7. Une fois que le saut suivant est accessible, les deux rayons s'envoient une réponse de résolution.
8. Les deux rayons peuvent désormais remplacer l'adresse IP de tronçon suivant de l'autre réseau de destination pour l'accès virtuel via NHO.
9. Spoke1 installe les entrées de cache nécessaires pour l'adresse IP de tronçon suivant de Spoke2 et son réseau. Spoke1 supprime également l'entrée de cache temporaire pointant vers le concentrateur pour résoudre le réseau sous l'interface de tunnel 1.
10. La même étape est répétée par le rayon 2, il installe également des entrées de cache pour l'IP de tronçon suivant du rayon 1 et son réseau va de l'avant en supprimant l'ancienne entrée de concentrateur via le tunnel.
11. Le protocole NHRP ajoute des routes de raccourci en tant que route de remplacement du tronçon suivant (NHO) ou H (NHRP).

Configuration de FlexVPN Spoke to Spoke à l'aide du protocole EIGRP

Considérations clés pour la topologie basée sur EIGRP

Avant de procéder à la configuration, nous devons comprendre certains concepts clés,

- Pour tout déploiement EIGRP, si les satellites reçoivent une table de routage complète d'autres satellites ou seulement des routes récapitulatives, une liste de préfixes doit être installée côté concentrateur pour les mises à jour de routage sortantes afin de filtrer les adresses IP des satellites à annoncer les unes aux autres.

- Le découpage d'horizon dans EIGRP fonctionne différemment de dans IBGP. Le protocole EIGRP arrête uniquement d'annoncer les réseaux à partir d'une interface d'où ils ont été appris. Par exemple, le concentrateur a deux rayons, l'un connecté via l'accès virtuel 1 et l'autre via les interfaces d'accès virtuel 2. Les routes apprises par le concentrateur via VA 1 à partir du rayon 1 sont annoncées au rayon 2 via VA 2 et vice versa puisque VA 1 et VA 2 sont des interfaces différentes. Dans le cas d'IBGP, il n'annonce aucun réseau appris de son homologue à un autre homologue. Dans un exemple similaire, un concentrateur configuré avec IBGP n'annonce pas les réseaux de retour qu'il a appris de VA 1 à VA 2 et vice versa.

- Ce comportement dans EIGRP crée un conflit dans la contiguïté CEF pour l'adresse IP de tronçon suivant (une adresse IP d'interface d'accès virtuel pour un tunnel de rayon à rayon) car elle est d'abord apprise via EIGRP à l'aide d'une interface de tunnel de concentrateur, puis via IPsec à l'aide d'une interface d'accès virtuel. Cela entraîne un routage asymétrique pour le trafic NHRP et entraîne également une entrée NHRP dupliquée dans la table NHRP et des entrées NHO dupliquées dans la table de routage ainsi que pour les interfaces de tronçon suivant (tunnel via concentrateur) et (accès virtuel via rayon).

- Nous avons suivi ce comportement dans l'ID de bogue Cisco CSCwn54813 et l'ID de bogue Cisco CSCwn54758. Cisco vous conseillerait de respecter la solution de contournement fournie pour le filtrage des adresses de tunnel sur le concentrateur pour les mises à jour sortantes.

- Le modèle virtuel côté concentrateur doit avoir une adresse IP provenant d'un pool différent des interfaces de tunnel en étoile, car nous voulons filtrer les mises à jour EIGRP sortantes pour nous assurer que l'appairage EIGRP en étoile n'est pas affecté.

Voici deux exemples montrant comment configurer FlexVPN spoke to spoke à l'aide du protocole EIGRP sur le serveur FlexVPN et le client FlexVPN. Nous avons suivi les meilleures pratiques pour séparer le trafic sous-jacent et le trafic de superposition en les plaçant tous deux dans des VRF spécifiques. Le VRF A est utilisé pour la couche sous-jacente tandis que le VRF B est utilisé pour la couche de superposition.

Exemple 1 : utilisation de NHO (Next-Hop-Override) pour la communication satellite à satellite

Serveur FlexVPN

```
ip local pool FLEXPOOL 192.0.2.129 192.0.2.254

crypto ikev2 authorization policy CISCO_FLEX
 pool FLEXPOOL
 def-domain cisco.com
 route set interface

crypto ikev2 proposal CISCO_PROP
 encryption aes-gcm-256
 prf sha256
 group 21

crypto ikev2 policy CISCO_POL
 match fvrf A
 proposal CISCO_PROP

crypto ikev2 profile CISCO_IKEV2
 match fvrf A
 match identity remote fqdn domain cisco.com
 identity local fqdn hub.cisco.com
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 aaa authorization group psk list default CISCO_FLEX
 virtual-template 1

crypto ipsec transform-set CISCO_TRANSFORM esp-aes 256 esp-sha256-hmac
 mode transport

crypto ipsec profile CISCO_PROF
 set transform-set CISCO_TRANSFORM
 set pfs group19
 set ikev2-profile CISCO_IKEV2

interface Loopback0
 ip vrf forwarding B
 ip address 192.0.2.1 255.255.255.255

interface GigabitEthernet1
 ip vrf forwarding A
 ip address 203.0.113.2 255.255.255.252
```

```
interface Virtual-Template1 type tunnel
 ip vrf forwarding B
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel vrf A
 tunnel protection ipsec profile CISCO_PROF

ip prefix-list CISCO_PREFIX seq 5 deny 192.0.2.128/25 le 32
ip prefix-list CISCO_PREFIX seq 6 permit 0.0.0.0/0 le 32

router eigrp B
!
address-family ipv4 unicast vrf B autonomous-system 1
!
af-interface default
hello-interval 2
hold-time 10
exit-af-interface
!
topology base
distribute-list prefix CISCO_PREFIX out
exit-af-topology
network 192.0.2.128 0.0.0.127
network 192.0.2.1 0.0.0.0
exit-address-family
```

Client FlexVPN 1

```
ip host vrf A hub.cisco.com 203.0.113.2

crypto ikev2 authorization policy CISCO_FLEX
 route set interface

crypto ikev2 proposal CISCO_PROP
 encryption aes-gcm-256
 prf sha256
 group 21

crypto ikev2 policy CISCO_POL
 match fvrf A
 proposal CISCO_PROP

crypto ikev2 client flexvpn CISCO_CLIENT
 peer 1 fqdn hub.cisco.com dynamic
 client connect Tunnel1

crypto ikev2 profile CISCO_IKEV2
 match fvrf A
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke1.cisco.com
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 aaa authorization group psk list default CISCO_FLEX
 virtual-template 1
```

```
crypto ipsec transform-set CISCO_TRANSFORM esp-aes 256 esp-sha256-hmac
 mode transport

crypto ipsec profile CISCO_PROF
 set transform-set CISCO_TRANSFORM
 set pfs group19
 set ikev2-profile CISCO_IKEV2

interface Tunnel1
 ip vrf forwarding B
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel destination dynamic
 tunnel vrf A
 tunnel protection ipsec profile CISCO_PROF
end

interface GigabitEthernet1
 ip vrf forwarding A
 ip address 203.0.113.6 255.255.255.252

interface Loopback1
 ip vrf forwarding B
 ip address 198.51.100.1 255.255.255.248

interface Virtual-Template1 type tunnel
 ip vrf forwarding B
 ip unnumbered Tunnel1
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel vrf A
 tunnel protection ipsec profile CISCO_PROF

router eigrp B
 address-family ipv4 unicast vrf B autonomous-system 1

 af-interface default
  hello-interval 2
  hold-time 10
  passive-interface
 exit-af-interface

 af-interface Tunnel1
  no passive-interface
 exit-af-interface

  topology base
  exit-af-topology
  network 198.51.100.0 0.0.0.7
  network 192.0.2.128 0.0.0.127
 exit-address-family
```

Client FlexVPN 2

```
ip host vrf A hub.cisco.com 203.0.113.2
```

```
crypto ikev2 authorization policy CISCO_FLEX
 route set interface

crypto ikev2 proposal CISCO_PROP
 encryption aes-gcm-256
 prf sha256
 group 21

crypto ikev2 policy CISCO_POL
 match fvrf A
 proposal CISCO_PROP

crypto ikev2 client flexvpn CISCO_CLIENT
 peer 1 fqdn hub.cisco.com dynamic
 client connect Tunnel1

crypto ikev2 profile CISCO_IKEV2
 match fvrf A
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke2.cisco.com
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 aaa authorization group psk list default CISCO_FLEX
 virtual-template 1

crypto ipsec transform-set CISCO_TRANSFORM esp-aes 256 esp-sha256-hmac
 mode transport

crypto ipsec profile CISCO_PROF
 set transform-set CISCO_TRANSFORM
 set pfs group19
 set ikev2-profile CISCO_IKEV2

interface Tunnel1
 ip vrf forwarding B
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel destination dynamic
 tunnel vrf A
 tunnel protection ipsec profile CISCO_PROF
end

interface GigabitEthernet1
 ip vrf forwarding A
 ip address 203.0.113.10 255.255.255.252

interface Loopback1
 ip vrf forwarding B
 ip address 198.51.100.9 255.255.255.248

interface Virtual-Template1 type tunnel
 ip vrf forwarding B
 ip unnumbered Tunnel1
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel vrf A
 tunnel protection ipsec profile CISCO_PROF

router eigrp B
```

```
 address-family ipv4 unicast vrf B autonomous-system 1

 af-interface default
  hello-interval 2
  hold-time 10
  passive-interface
 exit-af-interface

 af-interface Tunnel1
  no passive-interface
 exit-af-interface

  topology base
  exit-af-topology
  network 198.51.100.8 0.0.0.7
  network 192.0.2.128 0.0.0.127
 exit-address-family
```

Exemple 2 : utilisation des routes installées par le protocole NHRP pour la communication satellite à satellite

Serveur FlexVPN

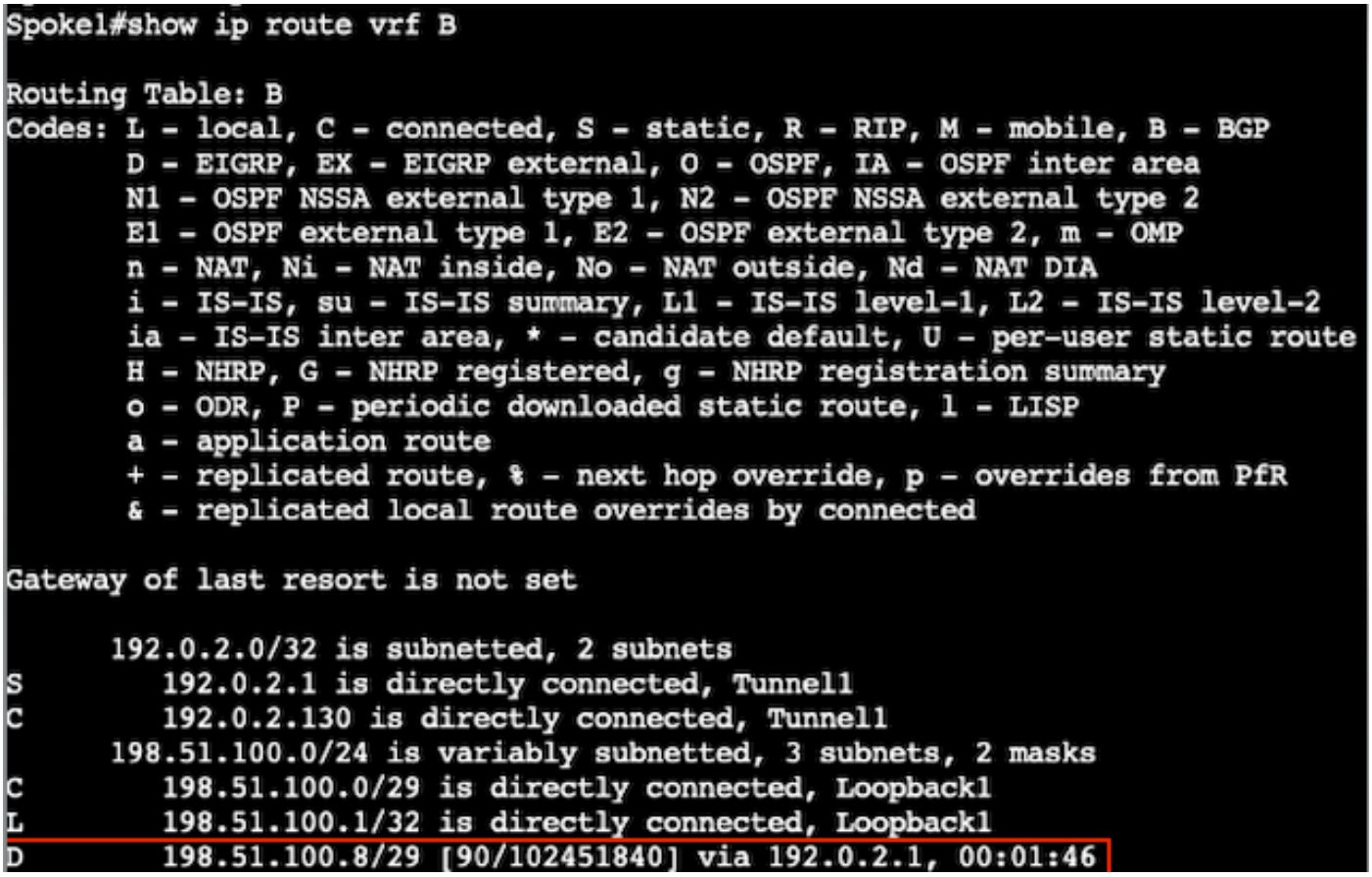
La seule modification apportée à la configuration EIGRP consiste à introduire des routes récapitulatives au lieu d'une table de routage complète sur les rayons. Assurez-vous d'arrêter virtual-template pour insérer la configuration récapitulative dans la topologie EIGRP. Reportez-vous à l'ID de bogue Cisco CSCwn84303.

```
router eigrp B
!
address-family ipv4 unicast vrf B autonomous-system 1
!
af-interface default
hello-interval 2
hold-time 10
exit-af-interface
!
af-interface Virtual-Template1
summary-address 198.51.100.0 255.255.255.0 <<<<<<<<<<< Summary address
exit-af-interface
!
topology base
distribute-list prefix CISCO_PREFIX out
exit-af-topology
network 192.0.2.128 0.0.0.127
network 192.0.2.1 0.0.0.0
exit-address-family
```

Vérification et dépannage

Exemple 1 : utilisation de NHO (Next-Hop-Override) pour la communication satellite à satellite

Spoke 1 (résolution NHRP avant Spoke to Spoke et établissement du tunnel)



Spoke 2 (résolution NHRP avant Spoke to Spoke et établissement du tunnel)

```
Spoke2#show ip route vrf B

Routing Table: B
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      192.0.2.0/32 is subnetted, 2 subnets
S        192.0.2.1 is directly connected, Tunnel1
C        192.0.2.129 is directly connected, Tunnel1
      198.51.100.0/24 is variably subnetted, 3 subnets, 2 masks
D        198.51.100.0/29 [90/102451840] via 192.0.2.1, 00:04:01
C        198.51.100.8/29 is directly connected, Loopback1
L        198.51.100.9/32 is directly connected, Loopback1
Spoke2#
```

Spoke 1 (après résolution NHRP Spoke to Spoke et établissement du tunnel)

Initialisation du protocole ICMP pour déclencher un tunnel de rayon à rayon.

```
Spoke1#ping vrf B 198.51.100.9 source 198.51.100.1 repeat 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 198.51.100.1
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 111/111/111 ms
```

Vérification du raccourci NHRP.

```
Spoke1#show ip nhrp vrf B detail
192.0.2.129/32 via 192.0.2.129
   Virtual-Access1 created 00:00:18, expire 00:09:41
   Type: dynamic, Flags: router nhop rib nho
   NBMA address: 203.0.113.10
   Preference: 255
198.51.100.8/29 via 192.0.2.129
   Virtual-Access1 created 00:00:17, expire 00:09:41
   Type: dynamic, Flags: router rib nho
   NBMA address: 203.0.113.10
   Preference: 255
```

Vérification des routes NHO après la création de raccourcis.

```
Spoke1#show ip route vrf B next-hop-override

Routing Table: B
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      192.0.2.0/32 is subnetted, 3 subnets
S        192.0.2.1 is directly connected, Tunnel1
S   %    192.0.2.129 is directly connected, Virtual-Access1
                     [NHO][1/255] via 192.0.2.129, Virtual-Access1
C        192.0.2.130 is directly connected, Tunnel1
      198.51.100.0/24 is variably subnetted, 3 subnets, 2 masks
C        198.51.100.0/29 is directly connected, Loopback1
L        198.51.100.1/32 is directly connected, Loopback1
D   %    198.51.100.8/29 [90/102451840] via 192.0.2.1, 00:07:13
                         [NHO][90/255] via 192.0.2.129, 00:00:45, Virtual-Access1
```

Vérification des compteurs NHRP.

```
Spoke1#show ip nhrp traffic
Tunnel1: Max-send limit:10000Pkts/10Sec, Usage:0%
   Sent: Total 2
         2 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
   Rcvd: Total 3
         2 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  1 Traffic Indication  0 Redirect Suppress
Virtual-Access1: Max-send limit:10000Pkts/10Sec, Usage:0%
   Sent: Total 3
         0 Resolution Request  1 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         2 Error Indication  0 Traffic Indication  0 Redirect Suppress
   Rcvd: Total 1
         0 Resolution Request  1 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
Virtual-Template1: Max-send limit:10000Pkts/10Sec, Usage:0%
   Sent: Total 0
         0 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
   Rcvd: Total 0
         0 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
```

Satellite 2 (après résolution NHRP satellite à satellite et établissement de tunnel)

Vérification du raccourci NHRP.

```
Spoke2#show ip nhrp vrf B detail
192.0.2.130/32 via 192.0.2.130
   Virtual-Access1 created 00:04:42, expire 00:05:18
   Type: dynamic, Flags: router nhop rib nho
   NBMA address: 203.0.113.6
   Preference: 255
198.51.100.0/29 via 192.0.2.130
   Virtual-Access1 created 00:04:40, expire 00:05:18
   Type: dynamic, Flags: router rib nho
   NBMA address: 203.0.113.6
   Preference: 255
```

Vérification des routes NHO après la création de raccourcis.

```
Spoke2# show ip route vrf B next-hop-override

Routing Table: B
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      192.0.2.0/32 is subnetted, 3 subnets
S        192.0.2.1 is directly connected, Tunnel1
C        192.0.2.129 is directly connected, Tunnel1
S   %    192.0.2.130 is directly connected, Virtual-Access1
                     [NHO][1/255] via 192.0.2.130, Virtual-Access1
      198.51.100.0/24 is variably subnetted, 3 subnets, 2 masks
D   %    198.51.100.0/29 [90/102451840] via 192.0.2.1, 00:11:20
                         [NHO][90/255] via 192.0.2.130, 00:04:52, Virtual-Access1
C        198.51.100.8/29 is directly connected, Loopback1
L        198.51.100.9/32 is directly connected, Loopback1
```

Vérification des compteurs NHRP.



Voici une explication étape par étape de la façon dont un tunnel de rayon à rayon direct est établi à l'aide de débogages à partir de l'un des rayons.

- ICMP initié par Spoke 1.

```
Spoke1#ping vrf B 198.51.100.9 source 198.51.100.1 repeat 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 198.51.100.1
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 111/111/111 ms
```

- Le concentrateur a reçu ICMP et a initié la redirection (indication de trafic) vers les deux rayons.

```
*Feb 3 16:15:35.280: NHRP: Receive Traffic Indication via Tunnel1 vrf: B(0x4), packet size: 104
*Feb 3 16:15:35.280: (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Feb 3 16:15:35.280: shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 3 16:15:35.280: pktsz: 104 extoff: 88
*Feb 3 16:15:35.280: (M) traffic code: redirect(0)
```

```
*Feb 3 16:15:35.280: src NBMA: 203.0.113.2
*Feb 3 16:15:35.280: src protocol: 192.0.2.1, dst protocol: 198.51.100.1
*Feb 3 16:15:35.280: Contents of nhrp traffic indication packet:
*Feb 3 16:15:35.281: 45 00 00 64 00 19 00 00 FE 01 68 0E C6 33 64 01
*Feb 3 16:15:35.281: C6 33 64 09 08 00 F3 F6 00 0D 00 00 00 00 00 00
*Feb 3 16:15:35.281: 3A 53 4F F3 AB CD AB CD AB CD AB CD AB CD AB CD
*Feb 3 16:15:35.281: NHRP-DETAIL: netid_in = 1, to_us = 0
*Feb 3 16:15:35.281: NHRP-DETAIL: NHRP traffic indication for afn 1 received on interface Tunnel1 , for
```

- Les deux rayons ont déclenché une demande de résolution qui a traversé le tunnel1.

```
*Feb 3 16:15:35.295: NHRP: Sending NHRP Resolution Request for dest: 198.51.100.9 to nexthop: 198.51.10
*Feb 3 16:15:35.295: NHRP: Attempting to send packet through interface Tunnel1 via DEST dst 198.51.100.
*Feb 3 16:15:35.295: NHRP-DETAIL: First hop route lookup for 198.51.100.9 yielded 192.0.2.1, Tunnel1
*Feb 3 16:15:35.295: NHRP: Send Resolution Request via Tunnel1 vrf: B(0x4), packet size: 72
*Feb 3 16:15:35.295: src: 192.0.2.130, dst: 198.51.100.9
*Feb 3 16:15:35.295: (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Feb 3 16:15:35.295: shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 3 16:15:35.295: pktsz: 72 extoff: 52
*Feb 3 16:15:35.296: (M) flags: "router auth src-stable nat ", reqid: 10
*Feb 3 16:15:35.296: src NBMA: 203.0.113.6
*Feb 3 16:15:35.296: src protocol: 192.0.2.130, dst protocol: 198.51.100.9
*Feb 3 16:15:35.296: (C-1) code: no error(0), flags: none
*Feb 3 16:15:35.296: prefix: 0, mtu: 9934, hd_time: 600
*Feb 3 16:15:35.296: addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 255
*Feb 3 16:15:35.296: NHRP: 96 bytes out Tunnel1
```

- Les deux rayons ont reçu une demande de résolution via Tunnel1.

```
*Feb 3 16:15:35.392: NHRP: Receive Resolution Request via Tunnel1 vrf: B(0x4), packet size: 92
*Feb 3 16:15:35.392: (F) afn: AF_IP(1), type: IP(800), hop: 254, ver: 1
*Feb 3 16:15:35.392: shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 3 16:15:35.392: pktsz: 92 extoff: 52
*Feb 3 16:15:35.392: (M) flags: "router auth src-stable nat ", reqid: 10
*Feb 3 16:15:35.392: src NBMA: 203.0.113.10
*Feb 3 16:15:35.392: src protocol: 192.0.2.129, dst protocol: 198.51.100.1
*Feb 3 16:15:35.392: (C-1) code: no error(0), flags: none
*Feb 3 16:15:35.392: prefix: 0, mtu: 9934, hd_time: 600
*Feb 3 16:15:35.392: addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 255
*Feb 3 16:15:35.392: NHRP-DETAIL: netid_in = 1, to_us = 0
*Feb 3 16:15:35.392: NHRP-DETAIL: Resolution request for afn 1 received on interface Tunnel1 , for vrf:
```

- Les deux rayons ont effectué une recherche de route pour leurs réseaux locaux 198.51.100.0/29/24 et 198.51.100.8/29.

```
*Feb 3 16:15:35.392: NHRP-DETAIL: Multipath IP route lookup for 198.51.100.1 in vrf: B(0x4) yielded Loo
*Feb 3 16:15:35.392: NHRP: Route lookup for destination 198.51.100.1 in vrf: B(0x4) yielded interface L
*Feb 3 16:15:35.392: NHRP-DETAIL: netid_out 0, netid_in 1
```

```
*Feb 3 16:15:35.392: NHRP-ATTR: smart spoke and attributes are not configured
*Feb 3 16:15:35.392: NHRP: We are egress router. Process the NHRP Resolution Request.
*Feb 3 16:15:35.393: NHRP: Cache radix tree head is not initialized for vrf: B(0x4)
*Feb 3 16:15:35.393: NHRP-DETAIL: Multipath IP route lookup for 198.51.100.1 in vrf: B(0x4) yielded Loo
*Feb 3 16:15:35.393: NHRP: nhrp_rtlookup for 198.51.100.1 in vrf: B(0x4) yielded interface Loopback1, p
*Feb 3 16:15:35.393: NHRP-DETAIL: netid_out 0, netid_in 1
*Feb 3 16:15:35.393: NHRP: We are egress router for target 198.51.100.1, recevied via Tunnel1 vrf: B(0x
```

- La réponse de résolution a été mise en file d'attente et l'établissement d'IPsec a commencé puisque les deux rayons connaissent maintenant leurs adresses NBMA respectives.

```
*Feb 3 16:15:35.393: NHRP: Checking for delayed event 192.0.2.129/198.51.100.1 on list (Tunnel1 vrf: B(
*Feb 3 16:15:35.393: NHRP: No delayed event node found.
*Feb 3 16:15:35.394: NHRP-DETAIL: Updated delayed event with ep src:203.0.113.6 dst:203.0.113.10 ivrf:B
*Feb 3 16:15:35.394: NHRP: Enqueued Delaying resolution request nbma src:203.0.113.6 nbma dst:203.0.113
*Feb 3 16:15:35.394: NHRP: Interface: Tunnel1 configured with FlexVPN. Deferringcache creation for nhop
*Feb 3 16:15:35.406: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to
*Feb 3 16:15:35.456: NHRP: Virtual-Access1: Tunnel mode changed from
'Uninitialized tunnel mode' to 'GRE over point to point IPV4 tunnel mode'
*Feb 3 16:15:35.456: NHRP: Virtual-Access1: NHRP not enabled in delay_if_up
*Feb 3 16:15:35.511: NHRP: Registration with Tunnels Decap Module succeeded
*Feb 3 16:15:35.511: NHRP: Rejecting addr type 1
*Feb 3 16:15:35.511: NHRP: Adding all static maps to cache
*Feb 3 16:15:35.511: NHRP-DETAIL: Adding summary-prefix entry: nhrp router block not configured
*Feb 3 16:15:35.512: NHRP:
*Feb 3 16:15:35.512: Instructing NHRP to create Virtual-Access from Virtual template 1 for interface Vi
*Feb 3 16:15:35.537: %SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as
*Feb 3 16:15:35.539: NHRP-CACHE: Virtual-Access1: Cache add for target 192.0.2.130/32 vrf: B(0x4) label
*Feb 3 16:15:35.540: 203.0.113.6 (flags:0x20)
*Feb 3 16:15:35.540: NHRP-DETAIL: self_cache: Unable to get tableid for swidb:Virtual-Access1 proto:NHR
*Feb 3 16:15:35.540: NHRP-DETAIL: self_cache: Unable to get tableid for swidb:Virtual-Access1 proto:UNK
*Feb 3 16:15:35.548: NHRP: Updating delayed event with destination 203.0.113.10 on interfaceTunnel1 wit
*Feb 3 16:15:35.788: NHRP:
*Feb 3 16:15:35.788: Fetched address from underlying IKEv2 for interfaceVirtual-Access1. Pre-NATed = 20
*Feb 3 16:15:35.788: %DMVPN-5-CRYPTO_SS: Virtual-Access1: local address : 203.0.113.6 remote address :
```

- Lors de l'établissement d'IPSEC et du processus de création de raccourcis NHRP, les deux satellites ont appris et installé mutuellement des adresses IP de tunnel dans leur table de routage en tant que route IPSEC et ont sondé l'accessibilité du saut suivant.

```
*Feb 3 16:15:35.788: NHRP: Processing delayed event on interface Tunnel1 with NBMA 203.0.113.10
*Feb 3 16:15:35.789: NHRP: Could not find instance node for vrf: B(0x4)
*Feb 3 16:15:35.789: NHRP-DETAIL: Cache INIT: NHRP instance root is NULL
*Feb 3 16:15:35.789: NHRP: Inserted instance node for vrf: B(0x4)
*Feb 3 16:15:35.789: NHRP-DETAIL: Initialized remote cache radix head for vrf: B(0x4)
*Feb 3 16:15:35.789: NHRP-DETAIL: Initialized local cache radix head for vrf: B(0x4)
*Feb 3 16:15:35.789: NHRP-RT: Attempting to create instance PDB for vrf: B(0x4)(0x4)
*Feb 3 16:15:35.789: NHRP-CACHE: Virtual-Access1: Cache add for target 192.0.2.129/32 vrf: B(0x4) label
*Feb 3 16:15:35.789: 203.0.113.10 (flags:0x2080)
*Feb 3 16:15:35.789: NHRP-RT: Adding route entry for 192.0.2.129/32 via 192.0.2.129, Virtual-Access1 vr
*Feb 3 16:15:35.791: NHRP-RT: Route addition to RIB Successful
*Feb 3 16:15:35.791: NHRP-EVE: NHP-UP: 192.0.2.129, NBMA: 203.0.113.10
```

```
*Feb 3 16:15:35.791: %DMVPN-5-NHRP_NHP_UP: Virtual-Access1: Next Hop NHP : (Tunnel: 192.0.2.129 NBMA: 2
*Feb 3 16:15:35.791: NHRP-CACHE:
*Feb 3 16:15:35.791: Next-hop not reachable for 192.0.2.129
*Feb 3 16:15:35.791: %NHRP-5-NHOP_UNREACHABLE: Nexthop address 192.0.2.129 for 192.0.2.129/32 is not ro
```

- Jusqu'à la fin de l'installation du raccourci et de la NHO, le satellite A a effectué la recherche du tronçon suivant d'adresses IP d'accès virtuel du satellite B et vice versa, mais la recherche d'espoir suivante a renvoyé « produit N/A » grâce auquel le satellite A a envoyé une indication d'erreur au satellite B confirmant que le tronçon suivant est inaccessible. La recherche particulière peut être appelée recherche par trajets multiples.

```
*Feb 3 16:15:35.791: NHRP-DETAIL: Multipath recursive nexthop lookup(if_in:, netid:1) for 192.0.2.129 i
*Feb 3 16:15:35.791: NHRP: Sending error indication. Reason: 'Cache pak failure' LINE: 13798
*Feb 3 16:15:35.791: NHRP: Attempting to send packet through interface Virtual-Access1 via DEST dst 192
*Feb 3 16:15:35.791: NHRP-DETAIL: Multipath recursive nexthop lookup(if_in:, netid:1) for 192.0.2.129 i
*Feb 3 16:15:35.791: NHRP: Send Error Indication via Virtual-Access1 vrf: B(0x4), packet size: 132
*Feb 3 16:15:35.791: src: 192.0.2.130, dst: 192.0.2.129
*Feb 3 16:15:35.791: (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Feb 3 16:15:35.791: shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 3 16:15:35.791: pktsz: 132 extoff: 0
*Feb 3 16:15:35.791: (M) error code: protocol address unreachable(6), offset: 0
*Feb 3 16:15:35.791: src NBMA: 203.0.113.6
*Feb 3 16:15:35.791: src protocol: 192.0.2.130, dst protocol: 192.0.2.129
*Feb 3 16:15:35.792: Contents of error packet:
*Feb 3 16:15:35.792: 00 01 08 00 00 00 00 00 00 FE 00 5C A2 22 00 34
*Feb 3 16:15:35.792: 01 01 04 00 04 04 C8 02 00 00 00 0A CB 00 71 0A
*Feb 3 16:15:35.792: C0 00 02 81 C6 33 64 01
*Feb 3 16:15:35.792:
```

- Une fois que NHO a lancé le saut suivant et que le raccourci a été créé, les deux rayons ont envoyé à nouveau des demandes de résolution pour le réseau de l'autre.

```
*Feb 3 16:15:35.813: NHRP: No need to delay processing of resolution event nbma src:203.0.113.6 nbma ds
*Feb 3 16:15:35.813: NHRP-CACHE: Virtual-Access1: Cache update for target 192.0.2.129/32 vrf: B(0x4) la
*Feb 3 16:15:35.813: 203.0.113.10 (flags:0x2280)
*Feb 3 16:15:35.813: NHRP-RT: Adding route entry for 192.0.2.129/32 via 192.0.2.129, Virtual-Access1 vr
*Feb 3 16:15:35.814: NHRP-RT: Route addition to RIB Successful
.
*Feb 3 16:15:35.841: NHRP-RT: Route entry 192.0.2.129/32 via 192.0.2.129 (Vi1) clobbered by distance
*Feb 3 16:15:35.847: NHRP-RT: Unable to stop route watch for 192.0.2.129/32 interface Virtual-Access1 .
*Feb 3 16:15:35.847: NHRP-RT: Adding route entry for 192.0.2.129/32 via 192.0.2.129, Virtual-Access1 vr
*Feb 3 16:15:35.847: NHRP-RT: Route addition failed (admin-distance)
*Feb 3 16:15:35.847: NHRP-RT: nexthop-override added to RIB
.
*Feb 3 16:15:37.167: NHRP: Sending NHRP Resolution Request for dest: 198.51.100.9 to nexthop: 198.51.10
*Feb 3 16:15:37.167: NHRP: Attempting to send packet through interface Tunnel1 via DEST dst 198.51.100.
*Feb 3 16:15:37.167: NHRP-DETAIL: First hop route lookup for 198.51.100.9 yielded 192.0.2.1, Tunnel1
*Feb 3 16:15:37.167: NHRP: Send Resolution Request via Tunnel1 vrf: B(0x4), packet size: 72
*Feb 3 16:15:37.167: src: 192.0.2.130, dst: 198.51.100.9
*Feb 3 16:15:37.167: (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Feb 3 16:15:37.167: shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 3 16:15:37.167: pktsz: 72 extoff: 52
```

```
*Feb 3 16:15:37.167: (M) flags: "router auth src-stable nat ", reqid: 10
*Feb 3 16:15:37.167: src NBMA: 203.0.113.6
*Feb 3 16:15:37.167: src protocol: 192.0.2.130, dst protocol: 198.51.100.9
*Feb 3 16:15:37.167: (C-1) code: no error(0), flags: none
*Feb 3 16:15:37.167: prefix: 0, mtu: 9934, hd_time: 600
*Feb 3 16:15:37.167: addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 255
*Feb 3 16:15:37.167: NHRP: 96 bytes out Tunnel1
```

- Une fois que les deux rayons ont reçu des demandes de résolution pour leurs réseaux respectifs, NHO a remplacé la route EIGRP via un tunnel (HUB) par un accès virtuel.

```
*Feb 3 16:30:57.768: NHRP-CACHE: Virtual-Access1: Cache add for target 198.51.100.8/29 vrf: B(0x4) labe
*Feb 3 16:30:57.768: 203.0.113.10 (flags:0x1000)
*Feb 3 16:30:57.768: NHRP-RT: Adding route entry for 198.51.100.8/29 via 192.0.2.129, Virtual-Access1 v
*Feb 3 16:30:57.769: NHRP-RT: Route addition failed (admin-distance)
*Feb 3 16:30:57.769: NHRP-RT: nexthop-override added to RIB
*Feb 3 16:30:57.769: NHRP-EVE: NHP-UP: 192.0.2.129, NBMA: 203.0.113.10
*Feb 3 16:30:57.769: %DMVPN-5-NHRP_NHP_UP: Virtual-Access1: Next Hop NHP : (Tunnel: 192.0.2.129 NBMA: 2
*Feb 3 16:30:57.769: NHRP-CACHE: Deleting incomplete entry for 198.51.100.9/32 interface Tunnel1 vrf: B
*Feb 3 16:30:57.769: NHRP-EVE: NHP-DOWN: 198.51.100.9, NBMA: 198.51.100.9
```

- Ensuite, les deux rayons envoient une réponse de résolution via l'interface d'accès virtuel.

```
*Feb 3 16:30:57.436: NHRP-CACHE: Virtual-Access1: Internal Cache add for target 198.51.100.0/29 vrf: B(
*Feb 3 16:30:57.436: 203.0.113.6 (flags:0x20)
*Feb 3 16:30:57.436: NHRP: Attempting to send packet through interface Virtual-Access1 via DEST dst 192
*Feb 3 16:30:57.436: NHRP-DETAIL: Multipath recursive nexthop lookup(if_in:, netid:1) for 192.0.2.129 i
*Feb 3 16:30:57.436: NHRP: Send Resolution Reply via Virtual-Access1 vrf: B(0x4), packet size: 120
*Feb 3 16:30:57.436: src: 192.0.2.130, dst: 192.0.2.129
*Feb 3 16:30:57.436: (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Feb 3 16:30:57.436: shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 3 16:30:57.436: pktsz: 120 extoff: 60
*Feb 3 16:30:57.437: (M) flags: "router auth dst-stable unique src-stable nat ", reqid: 11
*Feb 3 16:30:57.437: src NBMA: 203.0.113.10
*Feb 3 16:30:57.437: src protocol: 192.0.2.129, dst protocol: 198.51.100.1
*Feb 3 16:30:57.437: (C-1) code: no error(0), flags: none
*Feb 3 16:30:57.437: prefix: 29, mtu: 9976, hd_time: 599
*Feb 3 16:30:57.437: addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 255
*Feb 3 16:30:57.437: client NBMA: 203.0.113.6
*Feb 3 16:30:57.437: client protocol: 192.0.2.130
*Feb 3 16:30:57.437: NHRP: 144 bytes out Virtual-Access1
```

Exemple 2 : utilisation des routes installées par le protocole NHRP pour la communication satellite à satellite

Serveur FlexVPN

Présentation de la vérification de la topologie EIGRP pour la route récapitulative.

```
FLEX-HUB#show ip eigrp vrf B topology 198.51.100.0
EIGRP-IPv4 VR(B) Topology Entry for AS(1)/ID(192.0.0.1)
          Topology(base) TID(0) VRF(B)
EIGRP-IPv4(1): Topology base(0) entry for 198.51.100.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 9837035520, RIB is 76851840
  Descriptor Blocks:
  0.0.0.0 (Null0), from 0.0.0.0, Send flag is 0x0
      Composite metric is (9837035520/0), route is Internal
      Vector metric:
        Minimum bandwidth is 100 Kbit
        Total delay is 50101250000 picoseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1476
        Hop count is 0
        Originating router is 192.0.0.1
```

Clients FlexVPN

Vérification de la présence d'une route récapitulative.

```
Spoke1#show ip route vrf B eigrp

Routing Table: B
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      198.51.100.0/24 is variably subnetted, 4 subnets, 3 masks
D        198.51.100.0/24 [90/102451840] via 192.0.2.1, 00:00:04
```

Essayez d'établir un tunnel de rayon à rayon en initiant le trafic.

```
Spoke1#ping vrf B 198.51.100.9 source 198.51.100.1 repeat 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 198.51.100.1
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 13/13/13 ms
```

Vérification à nouveau.

```
Spoke1#show ip route vrf B next-hop-override

Routing Table: B
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      192.0.2.0/32 is subnetted, 3 subnets
S        192.0.2.1 is directly connected, Tunnel1
H        192.0.2.129 is directly connected, 00:02:18, Virtual-Access1
C        192.0.2.132 is directly connected, Tunnel1
      198.51.100.0/24 is variably subnetted, 4 subnets, 3 masks
D        198.51.100.0/24 [90/102451840] via 192.0.2.1, 00:02:13
C        198.51.100.0/29 is directly connected, Loopback1
L        198.51.100.1/32 is directly connected, Loopback1
H        198.51.100.8/29 [250/255] via 192.0.2.129, 00:02:18, Virtual-Access1
```

Il y a une modification très mineure dans le résultat des débogages pour l'installation du réseau en étoile, où il montre que l'installation de la route a réussi au lieu de l'échec RIB et de l'ajout de NHO.

```
*Feb 3 16:43:38.957: NHRP-CACHE: Virtual-Access1: Cache add for target 198.51.100.8/29 vrf: B(0x4) labe
*Feb 3 16:43:38.957: 203.0.113.10 (flags:0x1000)
*Feb 3 16:43:38.957: NHRP-RT: Adding route entry for 198.51.100.8/29 via 192.0.2.131, Virtual-Access1 v
*Feb 3 16:43:38.957: NHRP-RT: Route addition to RIB Successful
*Feb 3 16:43:38.957: NHRP-EVE: NHP-UP: 192.0.2.131, NBMA: 203.0.113.10
```

Informations connexes

- Configuration de FlexVPN Spoke to Spoke
- Exemple de configuration de configuration de satellite FlexVPN dans une conception de concentrateur redondant avec un bloc client FlexVPN

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.