Configuration d'un DMVPN hiérarchique de phase 3 avec des rayons multisous-réseau

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Diagramme du réseau
  - Configurations
    - Concentrateur central (Hub0)
    - Concentrateur de la région 1 (concentrateur 1)
    - Concentrateur de la région 2 (concentrateur 2)
    - Région 1 satellite (satellite 1)
    - Région 2 satellite (satellite 2)
- Présentation du flux de paquets NHRP et de données
  - Premier flux de paquets de données
  - Flux des demandes de résolution NHRP
- Vérifier
  - Avant la création du tunnel satellite, c'est-à-dire la formation d'une entrée de raccourci NHRP
  - Après la formation du tunnel dynamique Spoke-Spoke, c'est-à-dire la formation d'une entrée de raccourci NHRP
- Dépannage
  - Couche de routage physique (NBMA ou point d'extrémité de tunnel)
  - Couche de cryptage IPSec
  - NHRP
  - Couche Protocoles de routage dynamique
- Informations connexes

Introduction

Ce document fournit des informations sur la façon de configurer un DMVPN (Hierarchical Dynamic Multipoint VPN) de phase 3 avec des rayons multisous-réseau.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base de DMVPN
- Connaissances de base du protocole EIGRP (Enhanced Interior Gateway Routing Protocol)

Remarque : pour un DMVPN hiérarchique avec des rayons à plusieurs sous-réseaux, assurez-vous que les routeurs ont le correctif de bogue CSCug42027. Avec les routeurs exécutant la version IOS sans le correctif de CSCug42027 , une fois que le tunnel de rayon à rayon est formé entre les rayons dans différents sous-réseaux, le trafic de rayon à rayon échoue.

CSCug42027 est résolu dans les versions IOS et IOS-XE suivantes :

- 15.3(3)S / 3.10 et versions ultérieures.
- 15.4(3)M et versions ultérieures.
- 15.4(1)T et versions ultérieures.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeurs à services intégrés Cisco 2911 exécutant Cisco IOS® Version 15.5(2)T

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. If your network is live, make sure that you understand the potential impact of any command.

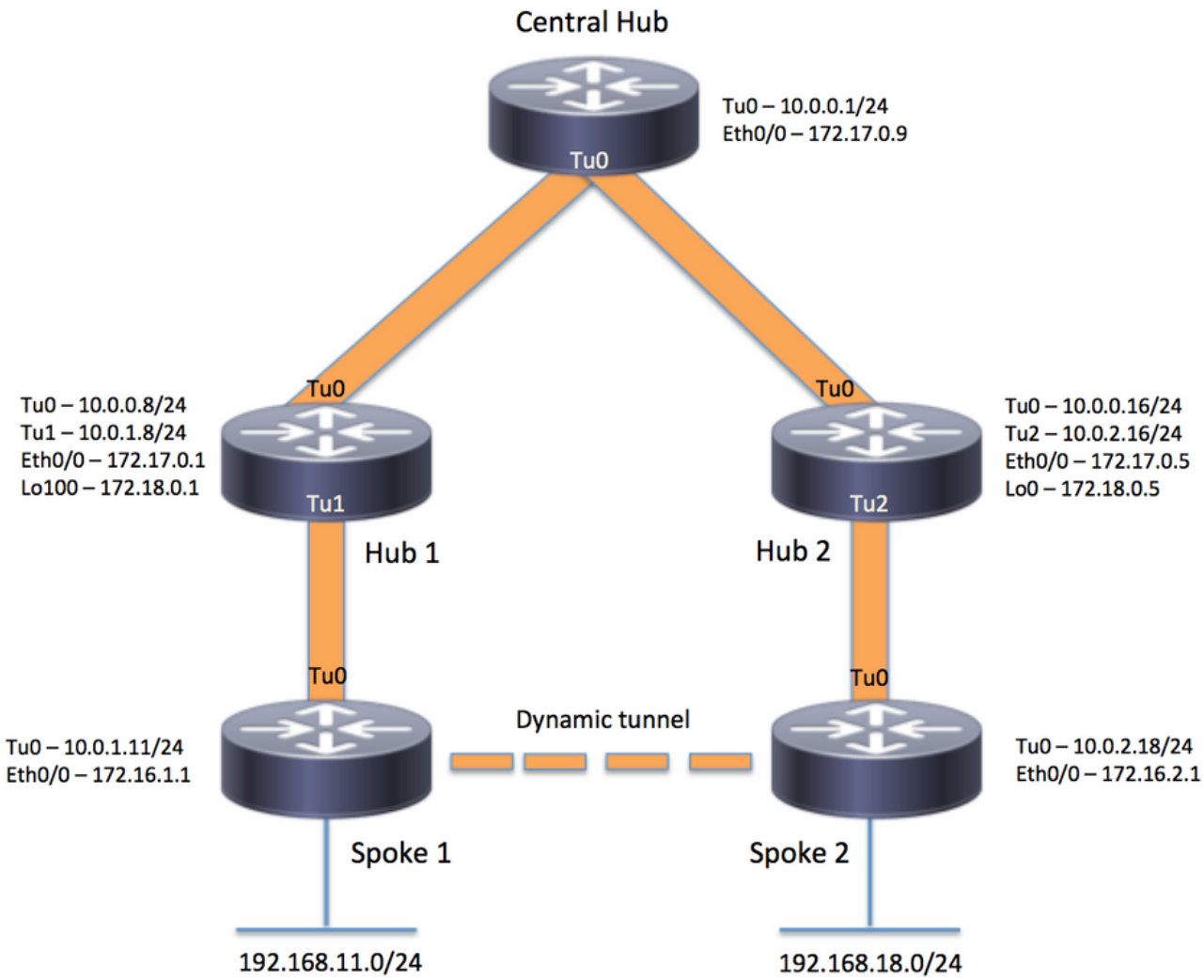
Informations générales

La configuration hiérarchique (supérieure à un niveau) permet des topologies réseau DMVPN arborescentes plus complexes. Les topologies arborescentes permettent de créer des réseaux DMVPN avec des concentrateurs régionaux qui sont des rayons de concentrateurs centraux. Cette architecture permet au concentrateur régional de gérer le trafic de contrôle des données et du protocole NHRP (Next Hop Resolution Protocol) pour ses rayons régionaux. Cependant, il permet toujours de construire des tunnels de rayon à rayon entre tous les rayons du réseau DMVPN, qu'ils se trouvent dans la même région ou non. Cette architecture permet également à la disposition du réseau DMVPN de correspondre plus étroitement aux modèles de flux de données régionaux ou hiérarchiques.

Configurer

Cette section vous fournit des informations utilisées pour configurer les fonctionnalités décrites dans ce document.

Diagramme du réseau



Configurations

> Remarque : seules les sections pertinentes de la configuration sont incluses dans cet exemple.

Concentrateur central (Hub0)

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname central_hub
!
crypto isakmp policy 1
  encr aes 256
  hash sha256
  authentication pre-share
  group 2
```

```
crypto isakmp key cisco123 address 0.0.0.0
!
crypto ipsec transform-set transform-dmvpn esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile profile-dmvpn
 set transform-set transform-dmvpn
!
interface Loopback1
 ip address 192.168.1.1 255.255.255.0
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 no ip split-horizon eigrp 1
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp shortcut
 ip nhrp redirect
 ip summary-address eigrp 1 192.168.0.0 255.255.192.0
 ip tcp adjust-mss 1360
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile profile-dmvpn
!
interface Ethernet0/0
 ip address 172.17.0.9 255.255.255.252
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.1.0
!
ip route 0.0.0.0 0.0.0.0 172.17.0.10
!
end
```

Concentrateur de la région 1 (concentrateur 1)

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname hub_1
!
crypto isakmp policy 1
  encr aes 256
  hash sha256
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 0.0.0.0
```

```
!
crypto ipsec transform-set transform-dmvpn esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile profile-dmvpn
 set transform-set transform-dmvpn
!
crypto ipsec profile profile-dmvpn-1
 set transform-set transform-dmvpn
!
interface Loopback1
 ip address 192.168.8.1 255.255.255.0
!
interface Loopback100
 ip address 172.18.0.1 255.255.255.252
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.8 255.255.255.0
 no ip redirects
 ip mtu 1400
 no ip split-horizon eigrp 1
 ip nhrp authentication test
 ip nhrp network-id 100000
 ip nhrp nhs 10.0.0.1 nbma 172.17.0.9 multicast
 ip nhrp shortcut
 ip nhrp redirect
 ip summary-address eigrp 1 192.168.8.0 255.255.248.0
 ip tcp adjust-mss 1360
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile profile-dmvpn
!
interface Tunnel1
 bandwidth 1000
 ip address 10.0.1.8 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp redirect
 ip summary-address eigrp 1 192.168.8.0 255.255.248.0
 ip summary-address eigrp 1 192.168.100.0 255.255.252.0
 ip tcp adjust-mss 1360
 tunnel source Loopback100
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile profile-dmvpn-1
!
interface Ethernet0/0
 ip address 172.17.0.1 255.255.255.252
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.8.0
!
ip route 0.0.0.0 0.0.0.0 172.17.0.2
!
end
```

Concentrateur de la région 2 (concentrateur 2)

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname hub_2
!
crypto isakmp policy 1
  encr aes 256
  hash sha256
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 0.0.0.0
!
crypto ipsec transform-set transform-dmvpn esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile profile-dmvpn
 set transform-set transform-dmvpn
!
crypto ipsec profile profile-dmvpn-1
 set transform-set transform-dmvpn
!
interface Loopback0
 ip address 172.18.0.5 255.255.255.252
!
interface Loopback1
 ip address 192.168.16.1 255.255.255.0
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.16 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp network-id 100000
 ip nhrp holdtime 360
 ip nhrp nhs 10.0.0.1 nbma 172.17.0.9 multicast
 ip nhrp shortcut
 ip nhrp redirect
 ip summary-address eigrp 1 192.168.16.0 255.255.248.0
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile profile-dmvpn
!
interface Tunnel2
 bandwidth 1000
 ip address 10.0.2.16 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 360
```

```
 ip nhrp redirect
 ip summary-address eigrp 1 192.168.16.0 255.255.248.0
 ip summary-address eigrp 1 192.168.100.0 255.255.252.0
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile profile-dmvpn-1
!
interface Ethernet0/0
 ip address 172.17.0.5 255.255.255.252
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 10.0.2.0 0.0.0.255
 network 192.168.16.0
!
ip route 0.0.0.0 0.0.0.0 172.17.0.6
!
end
```

Région 1 satellite (satellite 1)

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname spoke_1
!
crypto isakmp policy 1
  encr aes 256
  hash sha256
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 0.0.0.0
crypto isakmp keepalive 10
!
crypto ipsec transform-set transform-dmvpn esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile profile-dmvpn
 set transform-set transform-dmvpn
!
interface Loopback1
 ip address 192.168.11.1 255.255.255.0
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.1.11 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp network-id 100000
 ip nhrp nhs 10.0.1.8 nbma 172.18.0.1 multicast
 ip nhrp shortcut
 ip tcp adjust-mss 1360
```

```
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile profile-dmvpn
!
interface Ethernet0/0
 ip address 172.16.1.1 255.255.255.252
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.11.0
!
ip route 0.0.0.0 0.0.0.0 172.16.1.2
!
end
```

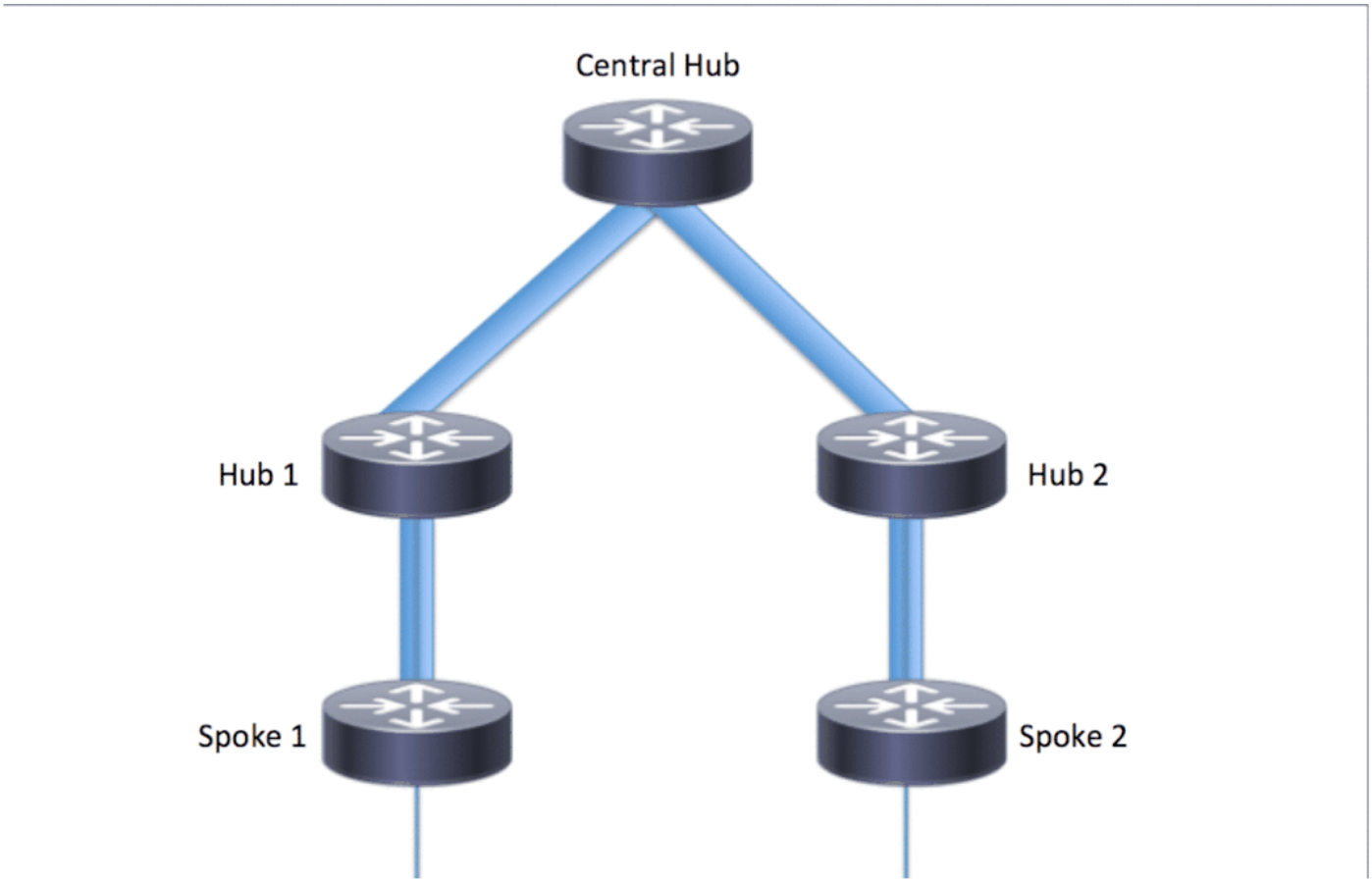
Région 2 satellite (satellite 2)

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname spoke_2
!
crypto isakmp policy 1
  encr aes 256
  hash sha256
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 0.0.0.0
crypto isakmp keepalive 10
!
crypto ipsec transform-set transform-dmvpn esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile profile-dmvpn
 set transform-set transform-dmvpn
!
interface Loopback1
 ip address 192.168.18.1 255.255.255.0
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.2.18 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp network-id 100000
 ip nhrp nhs 10.0.2.16 nbma 172.18.0.5 multicast
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
```

```
 tunnel protection ipsec profile profile-dmvpn
!
interface Ethernet0/0
 ip address 172.16.2.1 255.255.255.252
!
router eigrp 1
 network 10.0.2.0 0.0.0.255
 network 192.168.18.0
!
ip route 0.0.0.0 0.0.0.0 172.16.2.2
!
end
```

Présentation du flux de paquets NHRP et de données

Cette image montre le premier flux de paquets de données suivi du flux de requête et de réponse de résolution NHRP :



Premier flux de paquets de données

Étape 1. Ping ICMP initié à partir du rayon 1, destination = 192.168.18.10, source = 192.168.11.1

1. La recherche de route est effectuée pour 192.168.18.10. Comme indiqué ci-dessous, le saut suivant est 10.0.1.8 (adresse de tunnel du concentrateur 1)
2. La recherche dans le cache NHRP est effectuée pour la destination 192.168.18.10 sur Tunnel0, cependant, aucune entrée n'est trouvée à ce stade.
3. La recherche dans le cache NHRP est effectuée pour le saut suivant, c'est-à-dire 10.0.1.8 sur Tunnel0. Comme indiqué ci-dessous, l'entrée est présente et la session de chiffrement est UP.
4. Le paquet de requête d'écho ICMP est transmis au tronçon suivant, c'est-à-dire au concentrateur 1 via le tunnel existant.

<#root>

```
spoke_1#show ip route 192.168.18.10


Routing entry for 192.168.0.0/18, supernet
  Known via "eigrp 1", distance 90, metric 5248000, type internal
  Redistributing via eigrp 1
  Last update from 10.0.1.8 on Tunnel0, 02:30:37 ago
  Routing Descriptor Blocks:
  * 10.0.1.8, from 10.0.1.8, 02:30:37 ago, via Tunnel0
      Route metric is 5248000, traffic share count is 1
      Total delay is 105000 microseconds, minimum bandwidth is 1000 Kbit
      Reliability 255/255, minimum MTU 1400 bytes
      Loading 1/255, Hops 2

spoke_1#show ip nhrp
10.0.1.8/32 via 10.0.1.8
   Tunnel0 created 02:31:32, never expire
   Type: static, Flags: used
   NBMA address: 172.18.0.1
```

Étape 2. Paquet ICMP reçu sur le concentrateur 1

1. La recherche de route est effectuée pour 192.168.18.10. Le saut suivant est 10.0.0.1 (adresse de tunnel du concentrateur 0).
2. Puisque le concentrateur 1 n'est pas le point de sortie et que le paquet doit être transféré vers une autre interface dans le même nuage DMVPN, le concentrateur 1 envoie une indirection/redirection NHRP au satellite 1.
3. En même temps, le paquet de données est transmis à Hub0.

<#root>

```
*Apr 13 19:06:07.592: NHRP: Send Traffic Indication via Tunnel1 vrf 0, packet size: 96


*Apr 13 19:06:07.592:  src: 10.0.1.8, dst: 192.168.11.1
*Apr 13 19:06:07.592:  (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Apr 13 19:06:07.592:      shtl: 4(NSAP), sstl: 0(NSAP)
*Apr 13 19:06:07.592:      pktsz: 96 extoff: 68

*Apr 13 19:06:07.592:  (M) traffic code: redirect(0)
```

```
*Apr 13 19:06:07.592:      src NBMA: 172.18.0.1
*Apr 13 19:06:07.592:      src protocol: 10.0.1.8, dst protocol: 192.168.11.1
*Apr 13 19:06:07.592:      Contents of nhrp traffic indication packet:
*Apr 13 19:06:07.592:         45 00 00 64 00 01 00 00 FE 01 1E 3C C0 A8 0B 01
*Apr 13 19:06:07.592:         C0 A8 12 0A 08 00 A1 C8 00 01 00
```

Étape 3. Paquet ICMP reçu sur le concentrateur 0

1. La recherche de route est effectuée pour 192.168.18.10. Le saut suivant est 10.0.0.16 (adresse de tunnel de Hub2) sur Tunnel0
2. Puisque le concentrateur 0 n'est pas le point de sortie et que le paquet doit être réacheminé sur le même nuage DMVPN via la même interface, le concentrateur 0 envoie donc l'indirection NHRP au satellite 1 via le concentrateur 1.
3. Le paquet de données est transmis au concentrateur 2.

<#root>

```
*Apr 13 19:06:07.591: NHRP: Send Traffic Indication via Tunnel0 vrf 0, packet size: 96


*Apr 13 19:06:07.591:  src: 10.0.0.1, dst: 192.168.11.1
*Apr 13 19:06:07.591:  (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Apr 13 19:06:07.591:      shtl: 4(NSAP), sstl: 0(NSAP)
*Apr 13 19:06:07.591:      pktsz: 96 extoff: 68

*Apr 13 19:06:07.591:  (M) traffic code: redirect(0)


*Apr 13 19:06:07.591:      src NBMA: 172.17.0.9
*Apr 13 19:06:07.591:      src protocol: 10.0.0.1, dst protocol: 192.168.11.1
*Apr 13 19:06:07.592:      Contents of nhrp traffic indication packet:
*Apr 13 19:06:07.592:         45 00 00 64 00 01 00 00 FD 01 1F 3C C0 A8 0B 01
*Apr 13 19:06:07.592:         C0 A8 12 0A 08 00 A1 C8 00 01 00
```

Étape 4. Paquet ICMP reçu sur le concentrateur 2

1. La recherche de route est effectuée pour 192.168.18.10. Le saut suivant est 10.0.2.18 (adresse de tunnel de Spoke2) sur Tunnel2
2. Puisque le concentrateur 2 n'est pas le point de sortie et que le paquet doit être transféré à une autre interface dans le même nuage DMVPN, le concentrateur 2 envoie l'indirection NHRP à Spoke 1 via le concentrateur 0.
3. Le paquet de données est transmis au satellite 2.

<#root>

```
*Apr 13 19:06:07.592: NHRP: Send Traffic Indication via Tunnel0 vrf 0, packet size: 96


*Apr 13 19:06:07.593:  src: 10.0.0.16, dst: 192.168.11.1
*Apr 13 19:06:07.593:  (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Apr 13 19:06:07.593:      shtl: 4(NSAP), sstl: 0(NSAP)
```

```
*Apr 13 19:06:07.593:      pktsz: 96 extoff: 68

*Apr 13 19:06:07.593:  (M) traffic code: redirect(0)


*Apr 13 19:06:07.593:      src NBMA: 172.17.0.5
*Apr 13 19:06:07.593:      src protocol: 10.0.0.16, dst protocol: 192.168.11.1
*Apr 13 19:06:07.593:      Contents of nhrp traffic indication packet:
*Apr 13 19:06:07.593:         45 00 00 64 00 01 00 00 FC 01 20 3C C0 A8 0B 01
*Apr 13 19:06:07.593:         C0 A8 12 0A 08 00 A1 C8 00 01 00
```

Étape 5. Paquet ICMP reçu sur le satellite 2

La recherche de route est effectuée pour 192.168.18.10 et il s'agit d'un réseau connecté localement. Il transfère la requête ICMP à la destination.

Flux des demandes de résolution NHRP

Rayon 1

1. L'indirection NHRP envoyée par le concentrateur 1 pour la destination 192.168.18.10 est reçue.
2. Une entrée de cache NHRP incomplète pour 192.168.18.10/32 est insérée.
3. La recherche de route est effectuée pour 192.168.18.10. Le saut suivant est 10.0.1.8 (concentrateur 1) sur Tunnel0
4. La recherche dans le cache NHRP est effectuée pour le tronçon suivant 10.0.1.8 sur Tunnel0. Une entrée est trouvée et le socket de chiffrement est également activé (c'est-à-dire qu'un tunnel existe)
5. Le satellite 1 envoie une demande de résolution NHRP pour 192.168.18.10/32 au concentrateur 1 sur le satellite existant vers le tunnel régional du concentrateur 1.

<#root>

```
*Apr 13 19:06:07.596: NHRP:

Receive Traffic Indication via Tunnel0

 vrf 0, packet size: 96
*Apr 13 19:06:07.596:  (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Apr 13 19:06:07.596:      shtl: 4(NSAP), sstl: 0(NSAP)
*Apr 13 19:06:07.596:      pktsz: 96 extoff: 68

*Apr 13 19:06:07.596:  (M) traffic code: redirect(0)


*Apr 13 19:06:07.596:      src NBMA: 172.18.0.1
*Apr 13 19:06:07.596:      src protocol: 10.0.1.8, dst protocol: 192.168.11.1
*Apr 13 19:06:07.596:      Contents of nhrp traffic indication packet:
*Apr 13 19:06:07.596:         45 00 00 64 00 01 00 00 FE 01 1E 3C C0 A8 0B 01
*Apr 13 19:06:07.596:         C0 A8 12 0A 08 00 A1 C8 00 01 00
*Apr 13 19:06:07.596: NHRP: Attempting to create instance PDB for (0x0)
```

<#root>

```
*Apr 13 19:06:07.609: NHRP:

 Send Resolution Request via Tunnel0

 vrf 0, packet size: 84
*Apr 13 19:06:07.609:  src: 10.0.1.11, dst: 192.168.18.10
*Apr 13 19:06:07.609:  (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Apr 13 19:06:07.609:      shtl: 4(NSAP), sstl: 0(NSAP)
*Apr 13 19:06:07.609:      pktsz: 84 extoff: 52
*Apr 13 19:06:07.609:  (M) flags: "router auth src-stable nat ", reqid: 3
*Apr 13 19:06:07.609:      src NBMA: 172.16.1.1
*Apr 13 19:06:07.609:      src protocol: 10.0.1.11, dst protocol: 192.168.18.10
*Apr 13 19:06:07.609:  (C-1) code: no error(0)
*Apr 13 19:06:07.609:        prefix: 32, mtu: 17912, hd_time: 7200
*Apr 13 19:06:07.609:        addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
```

Concentrateur 1

1. La demande de résolution NHRP de Spoke 1 pour la destination 192.168.18.1/32 est reçue.
2. La recherche de route est effectuée pour 192.168.18.1. Le saut suivant est 10.0.0.1 (concentrateur 0) sur Tunnel0
3. L'ID réseau NHRP pour l'entrée et la sortie est identique et le noeud local n'est pas le point de sortie.
4. La recherche dans le cache NHRP est effectuée pour le tronçon suivant 10.0.0.1 sur Tunnel0, l'entrée est trouvée et le socket de chiffrement est activé (le tunnel existe)
5. Le concentrateur 1 transmet la demande de résolution NHRP pour 192.168.18.10/32 au concentrateur 0 sur le tunnel existant

<#root>

```
*Apr 13 19:06:07.610: NHRP:

Receive Resolution Request via Tunnel1

 vrf 0, packet size: 84
*Apr 13 19:06:07.610:  (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Apr 13 19:06:07.610:      shtl: 4(NSAP), sstl: 0(NSAP)
*Apr 13 19:06:07.610:      pktsz: 84 extoff: 52
*Apr 13 19:06:07.610:  (M) flags: "router auth src-stable nat ", reqid: 3
*Apr 13 19:06:07.610:      src NBMA: 172.16.1.1
*Apr 13 19:06:07.610:      src protocol: 10.0.1.11, dst protocol: 192.168.18.10
*Apr 13 19:06:07.610:  (C-1) code: no error(0)
*Apr 13 19:06:07.610:        prefix: 32, mtu: 17912, hd_time: 7200
*Apr 13 19:06:07.610:        addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0

*Apr 13 19:06:07.610: NHRP:

Forwarding Resolution Request via Tunnel0

 vrf 0, packet size: 104
*Apr 13 19:06:07.610:  src: 10.0.0.8, dst: 192.168.18.10
*Apr 13 19:06:07.610:  (F) afn: AF_IP(1), type: IP(800), hop: 254, ver: 1
*Apr 13 19:06:07.610:      shtl: 4(NSAP), sstl: 0(NSAP)
*Apr 13 19:06:07.610:      pktsz: 104 extoff: 52
*Apr 13 19:06:07.610:  (M) flags: "router auth src-stable nat ", reqid: 3
*Apr 13 19:06:07.610:      src NBMA: 172.16.1.1
*Apr 13 19:06:07.610:      src protocol: 10.0.1.11, dst protocol: 192.168.18.10
```

```
*Apr 13 19:06:07.610:  (C-1) code: no error(0)
*Apr 13 19:06:07.610:        prefix: 32, mtu: 17912, hd_time: 7200
*Apr 13 19:06:07.610:        addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
```

Concentrateur 0

1. La demande de résolution NHRP est reçue pour la destination 192.168.18.1/32, transmise par le concentrateur 1.
2. La recherche de route est effectuée pour 192.168.18.1. Le saut suivant est 10.0.0.16 (concentrateur 2) sur Tunnel0
3. L'ID réseau NHRP pour l'entrée et la sortie est identique et le noeud local n'est pas le point de sortie.
4. La recherche dans le cache NHRP est effectuée pour le tronçon suivant 10.0.0.16 sur Tunnel0, l'entrée est trouvée et le socket de chiffrement est activé (le tunnel existe)
5. Le concentrateur 0 transmet la demande de résolution NHRP pour 192.168.18.1/32 au concentrateur 2 via le tunnel existant.

<#root>

```
*Apr 13 19:06:07.611: NHRP:

Receive Resolution Request via Tunnel0

 vrf 0, packet size: 104
*Apr 13 19:06:07.611:  (F) afn: AF_IP(1), type: IP(800), hop: 254, ver: 1
*Apr 13 19:06:07.611:      shtl: 4(NSAP), sstl: 0(NSAP)
*Apr 13 19:06:07.611:      pktsz: 104 extoff: 52
*Apr 13 19:06:07.611:  (M) flags: "router auth src-stable nat ", reqid: 3
*Apr 13 19:06:07.611:      src NBMA: 172.16.1.1
*Apr 13 19:06:07.611:      src protocol: 10.0.1.11, dst protocol: 192.168.18.10
*Apr 13 19:06:07.611:  (C-1) code: no error(0)
*Apr 13 19:06:07.611:        prefix: 32, mtu: 17912, hd_time: 7200
*Apr 13 19:06:07.611:        addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0

*Apr 13 19:06:07.611: NHRP:

Forwarding Resolution Request via Tunnel0

 vrf 0, packet size: 124
*Apr 13 19:06:07.611:  src: 10.0.0.1, dst: 192.168.18.10
*Apr 13 19:06:07.611:  (F) afn: AF_IP(1), type: IP(800), hop: 253, ver: 1
*Apr 13 19:06:07.611:      shtl: 4(NSAP), sstl: 0(NSAP)
*Apr 13 19:06:07.612:      pktsz: 124 extoff: 52
*Apr 13 19:06:07.612:  (M) flags: "router auth src-stable nat ", reqid: 3
*Apr 13 19:06:07.612:      src NBMA: 172.16.1.1
*Apr 13 19:06:07.612:      src protocol: 10.0.1.11, dst protocol: 192.168.18.10
*Apr 13 19:06:07.612:  (C-1) code: no error(0)
*Apr 13 19:06:07.612:        prefix: 32, mtu: 17912, hd_time: 7200
*Apr 13 19:06:07.612:        addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
```

Concentrateur 2

1. La demande de résolution NHRP est reçue du satellite 1 pour la destination

192.168.18.10/32, transmise par le concentrateur 0
2. La recherche de route est effectuée pour 192.168.18.10, le tronçon suivant est 10.0.2.18 (satellite 2) sur le tunnel 2
3. L'ID réseau NHRP pour l'entrée et la sortie est identique et le noeud local n'est pas le point de sortie.
4. La recherche dans le cache NHRP est effectuée pour le tronçon suivant 10.0.2.18 sur Tunnel2, l'entrée est trouvée et le socket de chiffrement est activé (le tunnel existe)
5. Le concentrateur 2 transmet la demande de résolution NHRP pour 192.168.18.1/32 à Spoke 2 via le tunnel existant

<#root>

```
*Apr 13 19:06:07.613: NHRP:

 Receive Resolution Request via Tunnel0

 vrf 0, packet size: 124
*Apr 13 19:06:07.613:  (F) afn: AF_IP(1), type: IP(800), hop: 253, ver: 1
*Apr 13 19:06:07.613:      shtl: 4(NSAP), sstl: 0(NSAP)
*Apr 13 19:06:07.613:      pktsz: 124 extoff: 52
*Apr 13 19:06:07.613:  (M) flags: "router auth src-stable nat ", reqid: 3
*Apr 13 19:06:07.613:      src NBMA: 172.16.1.1
*Apr 13 19:06:07.613:      src protocol: 10.0.1.11, dst protocol: 192.168.18.10
*Apr 13 19:06:07.613:  (C-1) code: no error(0)
*Apr 13 19:06:07.613:        prefix: 32, mtu: 17912, hd_time: 7200
*Apr 13 19:06:07.613:        addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0

*Apr 13 19:06:07.613: NHRP:

Forwarding Resolution Request via Tunnel2

 vrf 0, packet size: 144
*Apr 13 19:06:07.613:  src: 10.0.2.16, dst: 192.168.18.10
*Apr 13 19:06:07.613:  (F) afn: AF_IP(1), type: IP(800), hop: 252, ver: 1
*Apr 13 19:06:07.613:      shtl: 4(NSAP), sstl: 0(NSAP)
*Apr 13 19:06:07.613:      pktsz: 144 extoff: 52
*Apr 13 19:06:07.613:  (M) flags: "router auth src-stable nat ", reqid: 3
*Apr 13 19:06:07.613:      src NBMA: 172.16.1.1
*Apr 13 19:06:07.613:      src protocol: 10.0.1.11, dst protocol: 192.168.18.10
*Apr 13 19:06:07.613:  (C-1) code: no error(0)
*Apr 13 19:06:07.613:        prefix: 32, mtu: 17912, hd_time: 7200
*Apr 13 19:06:07.613:        addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
```

Rayon 2

1. La demande de résolution NHRP est reçue pour la destination 192.168.18.1/32, transmise par le concentrateur 2
2. La recherche de route est effectuée pour 192.168.18.10, qui est un réseau connecté localement.
3. Spoke 2 est le point de sortie et génère la réponse de résolution pour 192.168.18.10, préfixe /24
4. Spoke 2 insère l'entrée de cache NHRP pour 10.0.1.11 (Spoke 1) en utilisant les informations de la demande de résolution NHRP.

5. Spoke 2 lance le tunnel VPN avec le point d'extrémité distant = adresse NBMA de Spoke 1. Le tunnel satellite dynamique est négocié.
6. Ensuite, Spoke 2 envoie la réponse de résolution NHRP pour 192.168.18.10/24 à Spoke 1 via le tunnel dynamique qui vient d'être construit.

<#root>

```
*Apr 13 19:06:07.613: NHRP: Receive Resolution Request via Tunnel0 vrf 0, packet size: 144


*Apr 13 19:06:07.613:  (F) afn: AF_IP(1), type: IP(800), hop: 252, ver: 1
*Apr 13 19:06:07.613:      shtl: 4(NSAP), sstl: 0(NSAP)
*Apr 13 19:06:07.613:      pktsz: 144 extoff: 52
*Apr 13 19:06:07.613:  (M) flags: "router auth src-stable nat ", reqid: 3
*Apr 13 19:06:07.613:      src NBMA: 172.16.1.1
*Apr 13 19:06:07.613:      src protocol: 10.0.1.11, dst protocol: 192.168.18.10
*Apr 13 19:06:07.614:  (C-1) code: no error(0)
*Apr 13 19:06:07.614:        prefix: 32, mtu: 17912, hd_time: 7200
*Apr 13 19:06:07.614:        addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0



*Apr 13 19:06:07.672: NHRP: Send Resolution Reply via Tunnel0 vrf 0, packet size: 172


*Apr 13 19:06:07.672:  src: 10.0.2.18, dst: 10.0.1.11
*Apr 13 19:06:07.672:  (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Apr 13 19:06:07.672:      shtl: 4(NSAP), sstl: 0(NSAP)
*Apr 13 19:06:07.672:      pktsz: 172 extoff: 60
*Apr 13 19:06:07.672:  (M) flags: "router auth dst-stable unique src-stable nat ", reqid: 3
*Apr 13 19:06:07.672:      src NBMA: 172.16.1.1
*Apr 13 19:06:07.672:      src protocol: 10.0.1.11, dst protocol: 192.168.18.10
*Apr 13 19:06:07.672:  (C-1) code: no error(0)
*Apr 13 19:06:07.672:        prefix: 24, mtu: 17912, hd_time: 7200
*Apr 13 19:06:07.672:        addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0
*Apr 13 19:06:07.672:        client NBMA: 172.16.2.1
*Apr 13 19:06:07.672:        client protocol: 10.0.2.18
```

Rayon1

1. La réponse de résolution NHRP est reçue de Spoke 2 pour la destination 192.168.18.10, préfixe /24 sur le tunnel dynamique.
2. L'entrée de cache NHRP pour 192.168.18.0/24 est maintenant mise à jour avec le saut suivant = 10.0.2.18, NBMA = 172.16.2.1
3. Une route NHRP est ajoutée dans le RIB pour le réseau 192.168.18.10, tronçon suivant = 10.0.2.18.

<#root>

```
*Apr 13 19:06:07.675: NHRP: Receive Resolution Reply via Tunnel0 vrf 0, packet size: 232


*Apr 13 19:06:07.675:  (F) afn: AF_IP(1), type: IP(800), hop: 252, ver: 1
*Apr 13 19:06:07.675:      shtl: 4(NSAP), sstl: 0(NSAP)
```

```
*Apr 13 19:06:07.675:      pktsz: 232 extoff: 60
*Apr 13 19:06:07.675:  (M) flags: "router auth dst-stable unique src-stable nat ", reqid: 3
*Apr 13 19:06:07.675:      src NBMA: 172.16.1.1
*Apr 13 19:06:07.675:      src protocol: 10.0.1.11, dst protocol: 192.168.18.10
*Apr 13 19:06:07.675:  (C-1) code: no error(0)
*Apr 13 19:06:07.675:        prefix: 24, mtu: 17912, hd_time: 7200
*Apr 13 19:06:07.675:        addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0
*Apr 13 19:06:07.675:        client NBMA: 172.16.2.1
*Apr 13 19:06:07.675:        client protocol: 10.0.2.18

*Apr 13 19:06:07.676: NHRP: Adding route entry for 192.168.18.0/24 () to RIB


*Apr 13 19:06:07.676: NHRP: Route addition to RIB Successful


*Apr 13 19:06:07.676: NHRP: Route watch started for 192.168.18.0/23

*Apr 13 19:06:07.676: NHRP: Adding route entry for 10.0.2.18/32 (Tunnel0) to RIB


*Apr 13 19:06:07.676: NHRP: Route addition to RIB Successful .
```

<#root>

```
spoke_1#show ip route 192.168.18.10
Routing entry for 192.168.18.0/24


Known via "nhrp"

, distance 250, metric 1
  Last update from 10.0.2.18 00:09:46 ago
  Routing Descriptor Blocks:
  *

10.0.2.18

, from 10.0.2.18, 00:09:46 ago
      Route metric is 1, traffic share count is 1
      MPLS label: none
```

Vérifier

> Remarque : l'analyseur CLI Cisco (pour les clients enregistrés uniquement) prend en charge certaines commandes show. Utilisez cet outil pour obtenir une analyse des rapports produits par ces commandes.

Avant la création du tunnel satellite, c'est-à-dire la formation d'une entrée de raccourci NHRP

<#root>

```
spoke_1#show ip nhrp
10.0.1.8/32 via 10.0.1.8
   Tunnel0 created 02:19:32, never expire
   Type: static, Flags: used
   NBMA address: 172.18.0.1
spoke_1#

spoke_1#show ip route next-hop-override
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
       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
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.1.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.1.2
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
D        10.0.0.0/24 [90/5120000] via 10.0.1.8, 02:20:14, Tunnel0
C        10.0.1.0/24 is directly connected, Tunnel0
L        10.0.1.11/32 is directly connected, Tunnel0
D        10.0.2.0/24 [90/6681600] via 10.0.1.8, 02:20:03, Tunnel0
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/30 is directly connected, Ethernet0/0
L        172.16.1.1/32 is directly connected, Ethernet0/0
      172.25.0.0/32 is subnetted, 1 subnets
C        172.25.179.254 is directly connected, Loopback0

D     192.168.0.0/18 [90/5248000] via 10.0.1.8, 02:20:03, Tunnel0  <<<< Summary route received from hub1


D     192.168.8.0/21 [90/3968000] via 10.0.1.8, 02:20:14, Tunnel0
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.11.0/24 is directly connected, Loopback1
L        192.168.11.1/32 is directly connected, Loopback1
spoke_1#


spoke_1#show dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==============================================================================

Interface Tunnel0 is up/up, Addr. is 10.0.1.11, VRF ""
   Tunnel Src./Dest. addr: 172.16.1.1/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "profile-dmvpn"
   Interface State Control: Disabled
   nhrp event-publisher : Disabled

IPv4 NHS:
10.0.1.8  RE NBMA Address: 172.18.0.1 priority = 0 cluster = 0
```

```
Type:Spoke, Total NBMA Peers (v4/v6): 1

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1 172.18.0.1             10.0.1.8    UP 00:02:31     S        10.0.1.8/32
```

<<<< Tunnel to the regional hub 1

```
Crypto Session Details:
--------------------------------------------------------------------------------

Interface: Tunnel0
Session: [0xF5F94CC8]
  Session ID: 0
  IKEv1 SA: local 172.16.1.1/500 remote 172.18.0.1/500 Active
```

<<<<< Crypto session to the regional hub 1

```
          Capabilities:D connid:1019 lifetime:23:57:28
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 172.18.0.1
  IPSEC FLOW: permit 47 host 172.16.1.1 host 172.18.0.1
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 35 drop 0 life (KB/Sec) 4153195/3448
        Outbound: #pkts enc'ed 35 drop 0 life (KB/Sec) 4153195/3448
   Outbound SPI : 0xACACB658, transform : esp-256-aes esp-sha-hmac
    Socket State: Open

Pending DMVPN Sessions:

spoke_1#
```

Après la formation du tunnel dynamique Spoke-Spoke, c'est-à-dire la formation d'une entrée de raccourci NHRP

<#root>

```
spoke_1#show ip nhrp
10.0.1.8/32 via 10.0.1.8
   Tunnel0 created 02:24:04, never expire
   Type: static, Flags: used
   NBMA address: 172.18.0.1
```

10.0.2.18/32 via 10.0.2.18

<<<<<<<<<< The new NHRP cache entry for spoke 2 that was learnt

Tunnel0 created 00:01:41, expire 01:58:18

Type: dynamic, Flags: router used nhop rib

NBMA address: 172.16.2.1

192.168.11.0/24 via 10.0.1.11
Tunnel0 created 00:01:26, expire 01:58:33
Type: dynamic, Flags: router unique local
NBMA address: 172.16.1.1
(no-socket)

192.168.18.0/24 via 10.0.2.18 <<<<<<<<<<<<< New NHRP cache entry formed for the remote subnet behind sp

Tunnel0 created 00:01:41, expire 01:58:18

Type: dynamic, Flags: router rib

NBMA address: 172.16.2.1

spoke_1#

spoke_1#sh ip route next-hop-override
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
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
o - ODR, P - periodic downloaded static route,

H - NHRP

, l - LISP
a - application route
+ - replicated route, % - next hop override

Gateway of last resort is 172.16.1.2 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 172.16.1.2
10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
D 10.0.0.0/24 [90/5120000] via 10.0.1.8, 02:23:57, Tunnel0
C 10.0.1.0/24 is directly connected, Tunnel0
L 10.0.1.11/32 is directly connected, Tunnel0
D 10.0.2.0/24 [90/6681600] via 10.0.1.8, 02:23:46, Tunnel0

H 10.0.2.18/32 is directly connected, 00:01:48, Tunnel0

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.1.0/30 is directly connected, Ethernet0/0
L 172.16.1.1/32 is directly connected, Ethernet0/0
172.25.0.0/32 is subnetted, 1 subnets
C 172.25.179.254 is directly connected, Loopback0
D 192.168.0.0/18 [90/5248000] via 10.0.1.8, 02:23:46, Tunnel0
D 192.168.8.0/21 [90/3968000] via 10.0.1.8, 02:23:57, Tunnel0
192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks

```
C        192.168.11.0/24 is directly connected, Loopback1
L        192.168.11.1/32 is directly connected, Loopback1

H     192.168.18.0/24 [250/1] via 10.0.2.18, 00:01:48


spoke_1#

spoke_1#sh dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==============================================================================

Interface Tunnel0 is up/up, Addr. is 10.0.1.11, VRF ""
   Tunnel Src./Dest. addr: 172.16.1.1/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "profile-dmvpn"
   Interface State Control: Disabled
   nhrp event-publisher : Disabled

IPv4 NHS:
10.0.1.8  RE NBMA Address: 172.18.0.1 priority = 0 cluster = 0
Type:Spoke, Total NBMA Peers (v4/v6): 3

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1 172.18.0.1             10.0.1.8    UP 00:05:44     S        10.0.1.8/32
    2 172.16.2.1            10.0.2.18    UP 00:01:51   DT1       10.0.2.18/32

<<<< Entry for spoke2's tunnel


      172.16.2.1            10.0.2.18    UP 00:01:51   DT1    192.168.18.0/24

<<<< Entry for the subnet behind spoke2 that was learnt


    1 172.16.1.1            10.0.1.11    UP 00:01:37   DLX    192.168.11.0/24

<<<< Entry formed for the local subnet



Crypto Session Details:
--------------------------------------------------------------------------------

Interface: Tunnel0
Session: [0xF5F94DC0]
  Session ID: 0
  IKEv1 SA: local 172.16.1.1/500 remote 172.18.0.1/500 Active
          Capabilities:D connid:1019 lifetime:23:54:15
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 172.18.0.1
  IPSEC FLOW: permit 47 host 172.16.1.1 host 172.18.0.1
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 8 drop 0 life (KB/Sec) 4153188/3255
        Outbound: #pkts enc'ed 9 drop 0 life (KB/Sec) 4153188/3255
   Outbound SPI : 0xACACB658, transform : esp-256-aes esp-sha-hmac
    Socket State: Open
```

```
Interface: Tunnel0
Session: [0xF5F94CC8]
  Session ID: 0
  IKEv1 SA: local 172.16.1.1/500 remote 172.16.2.1/500 Active
          Capabilities:D connid:1020 lifetime:23:58:08
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 172.16.2.1
  IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.2.1
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 10 drop 0 life (KB/Sec) 4185320/3488
        Outbound: #pkts enc'ed 10 drop 0 life (KB/Sec) 4185318/3488
   Outbound SPI : 0xCAD04C8B, transform : esp-256-aes esp-sha-hmac
    Socket State: Open

Pending DMVPN Sessions:
```

Raison de l'entrée de cache NHRP locale (sans socket) vue ci-dessus

L'indicateur local fait référence aux entrées de mappage NHRP qui sont destinées aux réseaux locaux de ce routeur (desservis par ce routeur). Ces entrées sont créées lorsque ce routeur répond à une demande de résolution NHRP avec ces informations et est utilisé pour stocker l'adresse IP du tunnel de tous les autres noeuds NHRP auxquels il a envoyé ces informations. Si, pour une raison quelconque, ce routeur perd l'accès à ce réseau local (il ne peut plus desservir ce réseau), il envoie un message de purge NHRP à tous les noeuds NHRP distants répertoriés dans l'entrée « local » (show ip nhrp detail) pour demander aux noeuds distants d'effacer ces informations de leurs tables de mappage NHRP.

Aucun socket n'est visible pour les entrées de mappage NHRP pour lesquelles nous n'avons pas besoin ni ne voulons déclencher IPsec pour configurer le chiffrement.

<#root>

```
spoke_1#sh ip nhrp 192.168.11.0 detail
192.168.11.0/24 via 10.0.1.11
   Tunnel0 created 00:01:01, expire 01:58:58
   Type: dynamic, Flags: router unique
```

local

```
   NBMA address: 172.16.1.1
```

(no-socket)

Requester: 10.0.2.18

```
 Request ID: 2
```

Dépannage

Cette section fournit les informations que vous pouvez utiliser afin de dépanner votre configuration.

> Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de débogage.

Le dépannage DMVPN implique un dépannage sur 4 couches dans l'ordre suivant :

1. Couche de routage physique (NBMA ou point d'extrémité de tunnel)
2. Couche de chiffrement IPsec
3. Couche d'encapsulation GRE
4. Couche Protocoles de routage dynamique

Avant le dépannage, il est préférable d'exécuter les commandes suivantes :

<#root>

```
!! Enable msec debug and log timestamps


service timestamps debug datetime msec
service timestamps log datetime msec


!! To help correlate the debug output with the show command outputs


terminal exec prompt timestamp
```

Couche de routage physique (NBMA ou point d'extrémité de tunnel)

Vérifiez si vous pouvez envoyer une requête ping à partir du concentrateur vers l'adresse NBMA du rayon et à partir du rayon vers l'adresse NBMA du concentrateur (à partir du résultat de la commande show ip nhrp on the spoke). Ces pings doivent être émis directement de l'interface physique plutôt que par le tunnel DMVPN. Si cela ne fonctionne pas, vous devez vérifier le routage et les éventuels pare-feu entre les routeurs hub et spoke.

Couche de cryptage IPSec

Exécutez les commandes suivantes pour vérifier les associations de sécurité ISAKMP et IPsec entre les adresses NBMA du concentrateur et du rayon.

```
show crypto isakmp sa detail
show crypto ipsec sa peer <NBMA-address-peer>
```

Ces débogages peuvent être activés pour résoudre les problèmes de couche de chiffrement IPSec :

<#root>

!! Use the conditional debugs to restrict the debug output for a specific peer.

```
debug crypto condition peer ipv4 <NBMA address of the peer>
debug crypto isakmp
debug crypto ipsec
```

NHRP

Le rayon envoie régulièrement des demandes d'enregistrement NHRP, chaque valeur de 1/3 de délai de conservation NHRP (sur le rayon) ou de délai d'attente d'enregistrement ip nhrp <secondes>. Vous pouvez vérifier ceci sur le rayon en exécutant :

```
show ip nhrp nhs detail
show ip nhrp traffic
```

Utilisez les commandes ci-dessus pour vérifier si le rayon envoie des demandes d'enregistrement NHRP et reçoit des réponses du concentrateur.

Pour vérifier si le concentrateur a l'entrée de mappage NHRP pour le rayon dans le cache NHRP sur le concentrateur, exécutez cette commande :

```
show ip nhrp <spoke-tunnel-ip-address>
```

Pour résoudre les problèmes liés au protocole NHRP, ces débogages peuvent être utilisés :

<#root>

!! Enable conditional NHRP debugs

```
debug nhrp condition peer tunnel <tunnel address of the peer>

OR

debug nhrp condition peer nbma <nbma address of the peer>

debug nhrp
debug nhrp packet
```

Couche Protocoles de routage dynamique

Référez-vous à ces documents en fonction du protocole de routage dynamique utilisé :

- Dépannage EIGRP
- Dépannage OSPF
- Dépannage de BGP

Informations connexes

- Solutions de dépannage DMVPN les plus fréquentes
- Suivi des événements DMVPN
- Commutation de raccourcis NHRP améliorée
- Migration d'un VPN multipoint dynamique phase 2 à phase 3
- Navigateur de fonctionnalités Cisco
- Assistance et documentation techniques - Cisco Systems

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.