Fase-3 hiërarchische DMVPN configureren met multi-subnetspaken

Inhoud

Inleiding

Dit document bevat informatie over het configureren van een fase-3 hiërarchisch dynamisch VPN (DMVPN) met multi-subnetspaken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van DMVPN
- Basiskennis van Enhanced Interior Gateway Routing Protocol (EIGRP)

Opmerking: voor hiërarchische DMVPN met multi-subnetspokes, zorg ervoor dat de routers de bug fix van CSC42027 hebben. Met routers die IOS-versie uitvoeren zonder de oplossing van CSCug42027 , zodra de spraakverbinding tussen de spaken in verschillende subnetten is gevormd, mislukt het spraakverkeer.

CSCug42027 is opgelost in de volgende IOS- en IOS-XE-versies:

- 15.3(3)S / 3.10 en hoger.
- 15.4(3)M en hoger.
- 15.4(1)T en hoger.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende hardware- en softwareversies:

- Cisco 2911 geïntegreerde services routers met Cisco IOS® versie 15.5(2)T

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

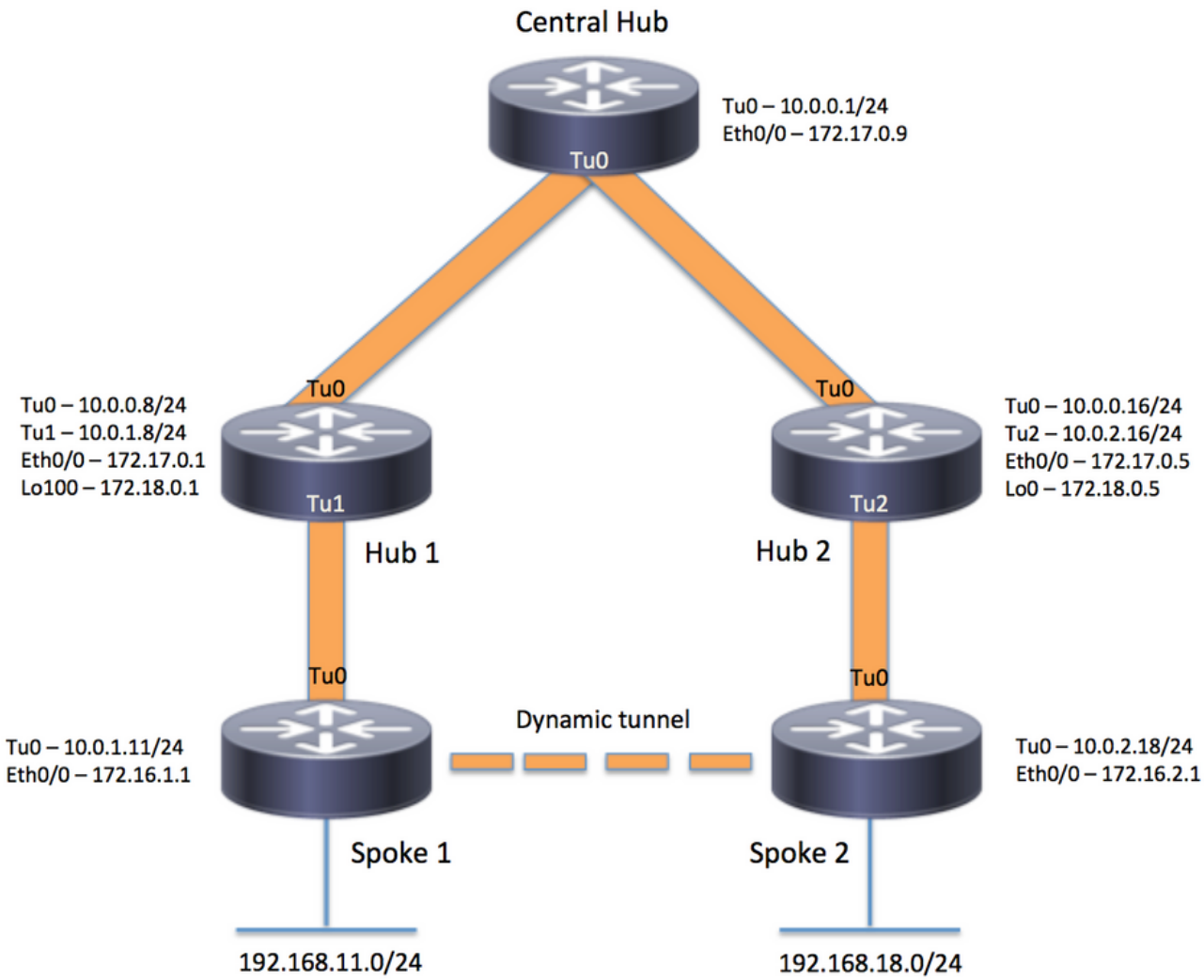
Achtergrondinformatie

De hiërarchische opstelling (groter dan één niveau) staat voor complexere op boom-gebaseerde DMVPN netwerktopologieën toe. Op bomen gebaseerde topologieën maken het mogelijk om DMVPN-netwerken te bouwen met regionale hubs die spaken van centrale hubs zijn. Deze architectuur maakt het mogelijk dat de regionale hub de gegevens verwerkt en het NHRP-controleverkeer (Next Hop Resolution Protocol) voor zijn regionale spokes. Het laat echter nog steeds toe om spraaktunnels te bouwen tussen spaken binnen het DMVPN-netwerk, of ze zich nu in dezelfde regio bevinden of niet. Deze architectuur staat ook de netwerklay-out van DMVPN toe om regionale of hiërarchische patronen van gegevensstroom dichter aan te passen.

Configureren

In deze sectie wordt u met de informatie gepresenteerd om de functies te configureren die in dit document worden beschreven.

Netwerkdiagram



Configuraties

Opmerking: in dit voorbeeld zijn alleen de relevante secties van de configuratie opgenomen.

Centrale hub (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
```

Regio 1 Hub (Hub 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
```

Regio 2 Hub (Hub 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
```

Regio 1 Gesproken (Spoke1)

```
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
```

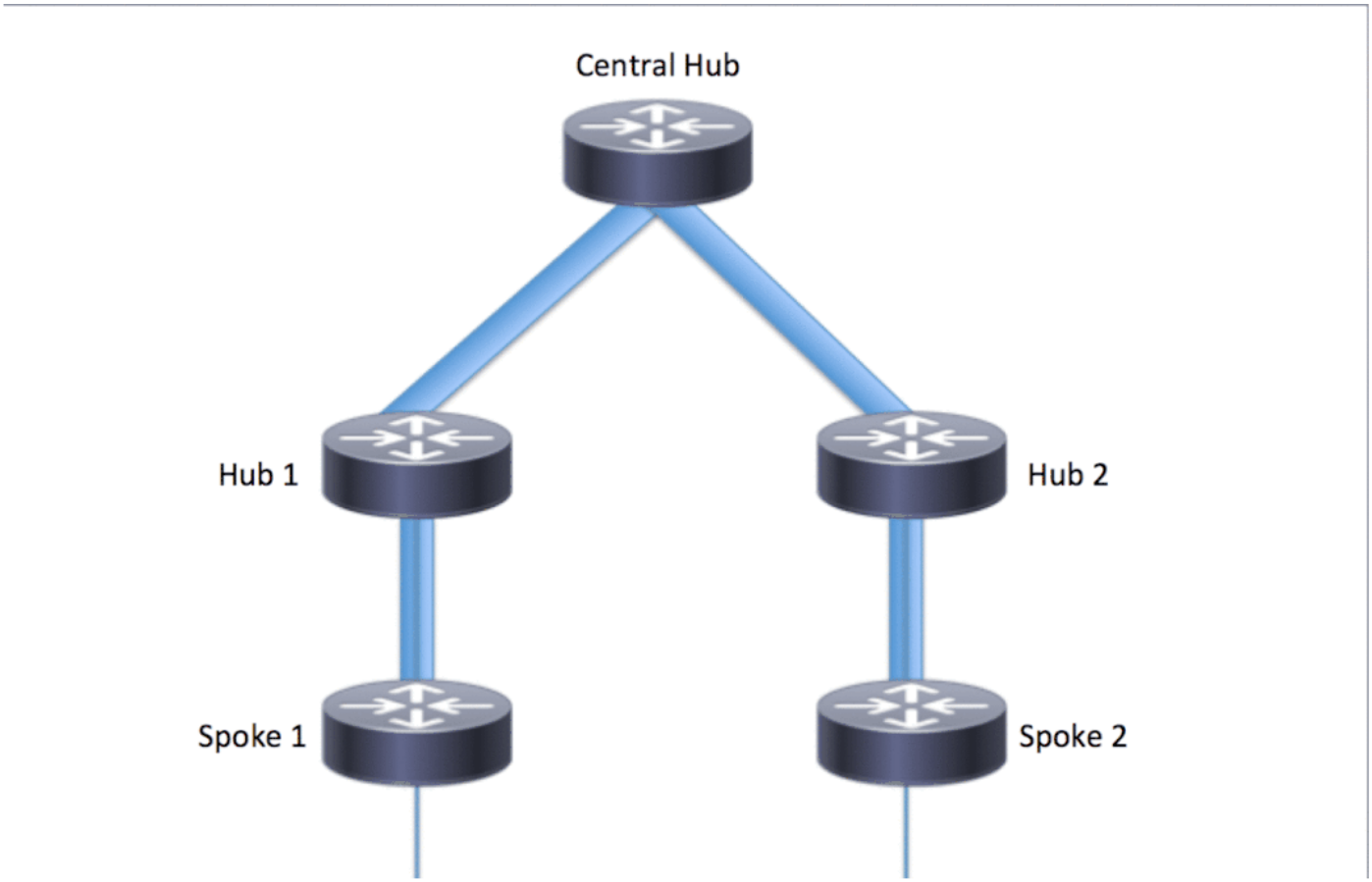
Regio 2 Gesproken (Gesproken 2)

```
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
```

De kennis van de gegevens en NHRP-pakketstroom

Dit beeld toont de eerste gegevenspakketstroom die door het NHRP-resolutieverzoek en de antwoordstroom wordt gevolgd:



First Data Packet Flow

Stap 1. ICMP-ping gestart vanaf spaak 1, bestemming = 192.168.18.10, bron = 192.168.11.1

1. Routeselectie vindt plaats op 192.168.18.10. Zoals hieronder wordt getoond, is de volgende

hop 10.0.1.8 (tunneladres van Hub 1)

2. NHRP cache lookup wordt gedaan voor bestemming 192.168.18.10 op Tunnel0, echter, geen ingang is gevonden in dit stadium.
3. NHRP cache lookup wordt gedaan voor de volgende hop, d.w.z. 10.0.1.8 op Tunnel0. Zoals hieronder wordt getoond, is de ingang aanwezig en is de cryptosessie UP.
4. Het pakket met ICMP-echoverzoeken wordt doorgestuurd naar de volgende hop, bijvoorbeeld Hub1, via de bestaande tunnel.

<#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
```

Stap 2. ICMP-pakket ontvangen op hub 1

1. Routeselectie vindt plaats op 192.168.18.10. De volgende hop is 10.0.0.1 (tunneladres van Hub 0).
2. Aangezien Hub1 niet het uitgangspunt is en het pakket moet worden doorgestuurd naar een andere interface binnen dezelfde DMVPN-cloud, stuurt Hub 1 een NHRP-direct/doorsturen naar Spoke 1.
3. Tegelijkertijd wordt het gegevenspakket doorgestuurd naar 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
```

Stap 3. ICMP-pakket ontvangen op hub 0

1. Routeselectie vindt plaats op 192.168.18.10. De volgende hop is 10.0.0.16 (tunneladres van Hub2) op Tunnel0
2. Omdat Hub 0 niet het exitpunt is en het pakket terug naar dezelfde DMVPN-cloud moet worden doorgestuurd via dezelfde interface, stuurt Hub 0 de NHRP-indirecte naar Spoke 1 via Hub 1.
3. Het gegevenspakket wordt naar Hub 2 doorgestuurd.

<#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
```

Stap 4. ICMP-pakket ontvangen op Hub 2

1. Routeselectie vindt plaats op 192.168.18.10. De volgende hop is 10.0.2.18 (tunneladres van Spoke2) op Tunnel2
2. Omdat Hub 2 niet het exitpunt is en het pakket moet worden doorgestuurd naar een andere interface binnen dezelfde DMVPN-cloud, stuurt Hub 2 de NHRP-indirecte naar Spoke 1 via Hub 0.
3. De gegevens worden doorgestuurd naar Spoke 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
```

Stap 5. ICMP-pakket ontvangen op spraak 2

De raadpleging van de route wordt gedaan voor 192.168.18.10 en het is een plaatselijk verbonden netwerk. Het zendt het ICMP-verzoek naar de bestemming.

Stroom NHRP-oplossingsaanvraag

Gesproken 1

1. De NHRP-indirecte door Hub 1 verzonden voor bestemming 192.168.18.10 wordt ontvangen.
2. Er is een onvolledige NHRP cache ingang voor 192.168.18.10/32 ingevoegd.
3. Routeselectie vindt plaats op 192.168.18.10. De volgende hop is 10.0.1.8 (Hub 1) op Tunnel0
4. NHRP cache lookup wordt gedaan voor volgende hop 10.0.1.8 op Tunnel0. Een ingang wordt gevonden en de crypto contactdoos is ook omhoog (d.w.z. de tunnel bestaat)
5. Spoke 1 stuurt NHRP-resolutie verzoek voor 192.168.18.10/32 naar Hub 1 over de bestaande spoke aan de regionale hub1 tunnel.

<#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
```

Hub 1

1. Het NHRP-resolutieverzoek van Spoke 1 voor bestemming 192.168.18.1/32 wordt ontvangen.
2. Routeselectie vindt plaats op 192.168.18.1. De volgende hop is 10.0.0.1 (Hub 0) op Tunnel0
3. De NHRP netwerk-id voor toegang en uitgang is hetzelfde en de lokale knooppunt is niet het afsluitpunt.
4. NHRP cache lookup wordt gedaan voor volgende hop 10.0.0.1 op Tunnel0, ingang wordt gevonden en de crypto socket is omhoog (tunnel bestaat)
5. Hub1 forwards NHRP resolutie verzoek voor 192.168.18.10/32 naar Hub 0 over de bestaande tunnel

<#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
```

Hub 0

1. Het NHRP-resolutieverzoek wordt ontvangen voor bestemming 192.168.18.1/32, doorgestuurd door Hub 1.
2. Routeselectie vindt plaats op 192.168.18.1. De volgende hop is 10.0.0.16 (Hub 2) op Tunnel0
3. De NHRP netwerk-id voor toegang en uitgang is hetzelfde en de lokale knooppunt is niet het afsluitpunt.
4. NHRP cache lookup wordt gedaan voor volgende hop 10.0.0.16 op Tunnel0, ingang wordt gevonden en de crypto socket is omhoog (tunnel bestaat)
5. Hub 0 stuurt het NHRP-resolutieverzoek voor 192.168.18.1/32 door naar Hub 2 over de bestaande tunnel.

<#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
```

Hub 2

1. Het NHRP-resolutieverzoek wordt ontvangen van Spoke 1 voor bestemming 192.168.18.10/32, doorgestuurd door Hub 0

2. De raadpleging van de route wordt gedaan voor 192.168.18.10, volgende hop is 10.0.2.18 (Spoke 2) op Tunnel2
3. De NHRP netwerk-id voor toegang en uitgang is hetzelfde en de lokale knooppunt is niet het afsluitpunt.
4. NHRP cache lookup wordt gedaan voor volgende hop 10.0.2.18 op Tunnel2, ingang wordt gevonden en crypto socket is omhoog (tunnel bestaat)
5. Hub 2 verstuurt het NHRP resolutie verzoek voor 192.168.18.1/32 om 2 te spreken over de bestaande tunnel

<#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
```

Gesproken 2

1. Het NHRP-resolutieverzoek wordt ontvangen voor bestemming 192.168.18.1/32, doorgestuurd door Hub 2
2. De raadpleging van de route wordt gedaan voor 192.168.18.10, dat een plaatselijk verbonden netwerk is.
3. Spoke 2 is het exit point en het genereert de resolutie antwoord voor 192.168.18.10, prefix /24
4. Spoke 2 voegt de NHRP cache in voor 10.0.1.11 (Spoke 1) met behulp van informatie uit NHRP resolutie verzoek.
5. Spoke 2 initieert de VPN-tunnel met remote endpoint = NBMA-adres van Spoke 1. Er wordt

onderhandeld over de dynamische Spoke-Spoke-tunnel.

6. Spoke 2 stuurt dan het NHRP resolutie antwoord voor 192.168.18.10/24 naar Spoke 1 over de dynamische tunnel die net gebouwd werd.

<#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
```

Gesproken1

1. Het NHRP resolutie antwoord is ontvangen van Spoke 2 voor bestemming 192.168.18.10, prefix /24 over de dynamische tunnel.
2. De NHRP cache ingang voor 192.168.18.0/24 wordt nu bijgewerkt met volgende hop = 10.0.2.18, NBMA = 172.16.2.1
3. In de RIB wordt een NHRP-route toegevoegd voor het 192.168.18.10-netwerk, volgende hop = 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
```

Verifiëren

> Opmerking: De Cisco CLI Analyzer (alleen geregistreerde klanten) ondersteunt bepaalde show-opdrachten. Gebruik de Cisco CLI Analyzer om een analyse van show opdrachtoutput te bekijken.

Voordat Spoke-Spoke Tunnel wordt gebouwd, d.w.z. NHRP Shortcut Entry wordt gevormd

<#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#
```

Nadat Spoke-Spoke Dynamic Tunnel wordt gevormd d.w.z. NHRP wordt de Kortere wegingang gevormd

<#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:
```

Reden voor lokale NHRP cache (zonder socket), zoals hierboven beschreven

Local Flag verwijst naar NHRP-mapping-ingangen die voor lokale netwerken naar deze router zijn (onderhouden door deze router). Deze ingangen worden gecreëerd wanneer deze router een NHRP-resolutieverzoek met deze informatie beantwoordt en wordt gebruikt om het IP-adres van de tunnel op te slaan van alle andere NHRP-knooppunten waarnaar deze informatie is verzonden. Als deze router om de een of andere reden toegang tot dit lokale netwerk verliest (het kan dit netwerk niet meer onderhouden), zal het een NHRP zuiveringsbericht verzenden naar alle afgelegen NHRP-knooppunten die in het 'lokale' item worden vermeld (toon ip nhrp details) om de afgelegen knooppunten te vertellen deze informatie uit hun NHRP-mappingtabellen te wissen.

Er wordt geen socket weergegeven voor NHRP-mapping items waarvoor we geen IPsec voor setup-codering hoeven of willen activeren.

<#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
```

Problemen oplossen

Deze sectie bevat informatie voor het troubleshooten van de configuratie.

> Opmerking: raadpleeg Belangrijke informatie over debug-opdrachten voordat u debug-opdrachten gebruikt.

Probleemoplossing voor DMVPN omvat probleemoplossing op 4 lagen in deze volgorde:

1. Fysieke routinglaag (NBMA of tunneleindpunt)
2. IPsec-encryptielaag
3. GRE-insluitingslaag
4. Dynamische routingprotocollen

Alvorens het probleem op te lossen, is het beter om deze opdrachten uit te voeren:

<#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
```

Fysieke routinglaag (NBMA of tunneleindpunt)

Controleer of u kunt pingen van de hub naar het NBMA-adres van de spaak en van de spaak naar het NBMA-adres van de hub (van de output van show ip nhrp op de spaak). Deze pings zouden direct uit de fysieke interface, niet door de tunnel moeten gaan DMVPN. Als dit niet werkt, moet u de routing en eventuele firewalls tussen de hub en spraakrouters controleren.

IPsec-encryptielaag

Voer de volgende opdrachten uit om de ISAKMP SA's en IPsec SA's te controleren tussen de NBMA-adressen van de hub en de spaak.

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

Deze debugs kunnen worden ingeschakeld om problemen met de IPSec-coderingslaag op te lossen:

<#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

De spaak stuurt NHRP registratieverzoeken op regelmatige basis, elke 1/3 NHRP holdtime (op spaak) of ip NHRP registratie timeout <seconden> waarde. U kunt dit controleren op de spaak door te rennen:

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

Gebruik de bovenstaande commando's om te controleren of de spaak NHRP registratieverzoeken verstuurt en antwoorden krijgt van de hub.

Om te controleren of de hub de NHRP-kaartingvermelding heeft voor de spaak in het NHRP-cachegeheugen op de hub, voert u deze opdracht uit:

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

Om problemen met betrekking tot NHRP op te lossen, kunnen deze debugs worden gebruikt:

<#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
```

Dynamische routingprotocollen

Verwijs deze documenten afhankelijk van het dynamische routeringsprotocol dat wordt gebruikt:

- Probleemoplossing EIGRP
- Probleemoplossing OSPF
- BGP-probleemoplossing

Gerelateerde informatie

- Populairste oplossingen voor DMVPN-probleemoplossing
- DMVPN Event Tracing
- Uitgebreide NHRP Sneltoets Switching
- Migratie van Dynamisch Multipoint VPN-fase 2 naar fase 3
- Cisco Feature Navigator
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.