使用多子網分支配置第3階段分層DMVPN

目錄

簡介

本文提供如何使用多子網輻條設定第3階段階層式動態多點VPN (DMVPN)的相關資訊。

必要條件

需求

思科建議您瞭解以下主題：

- DMVPN基礎知識
- 增強型內部網關路由協定(EIGRP)基礎知識

> 注意：對於帶有多子網輻條的分層DMVPN，請確保路由器有CSCug42027的錯誤修復。如果路由器運行的IOS版本未修復CSCug42027，則一旦在不同子網的輻射點之間形成了輻射點到輻射點隧道，輻射點到輻射點流量將失敗。

CSCug42027在以下IOS和IOS-XE版本中進行了解析：

- 15.3(3)S / 3.10及更高版本。
- 15.4(3)M以上。
- 15.4(1)T及更高版本。

採用元件

本文件中的資訊是以下列硬體與軟體版本為依據：

- 運行Cisco IOS®版本15.5(2)T的Cisco 2911整合多業務路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

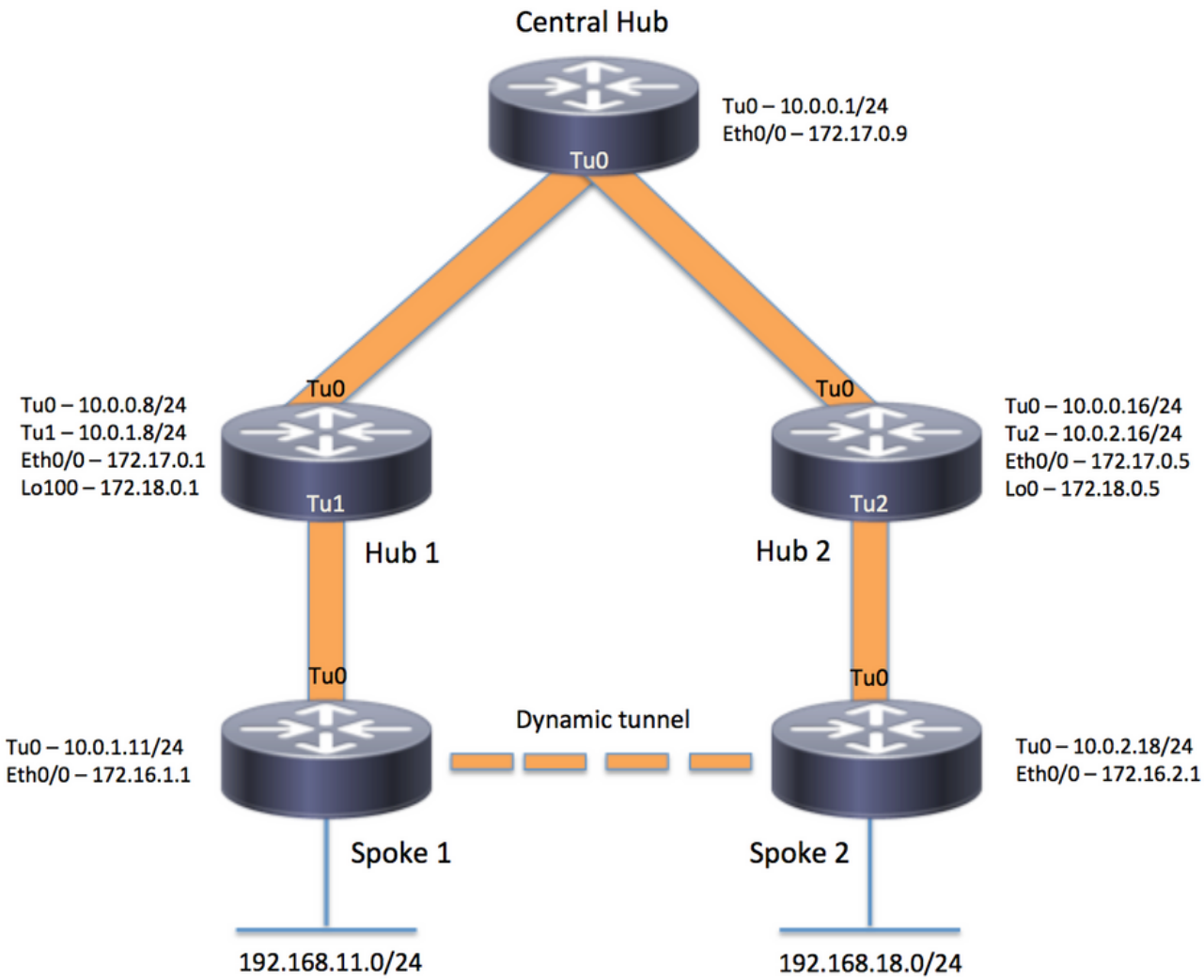
背景資訊

分層設定（大於一個級別）允許使用更複雜的基於樹的DMVPN網路拓撲。基於樹的拓撲允許使用作為中心集線器的分支的區域集線器構建DMVPN網路。此架構允許區域集線器處理其區域輻條的資料和下一跳解析協定(NHRP)控制流量。 但是，它仍然允許在DMVPN網路中的任何分支之間建立分支到分支隧道，無論它們是否位於同一區域。此架構還允許DMVPN網路佈局更加匹配區域或分層資料流模式。

設定

本節提供用於設定本檔案中所述功能的資訊。

網路圖表



組態

注意：本示例中僅包括配置的相關部分。

中央集線器(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
```

區域1中樞（中樞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
```

區域2中樞（中樞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
```

區域1分支（分支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
```

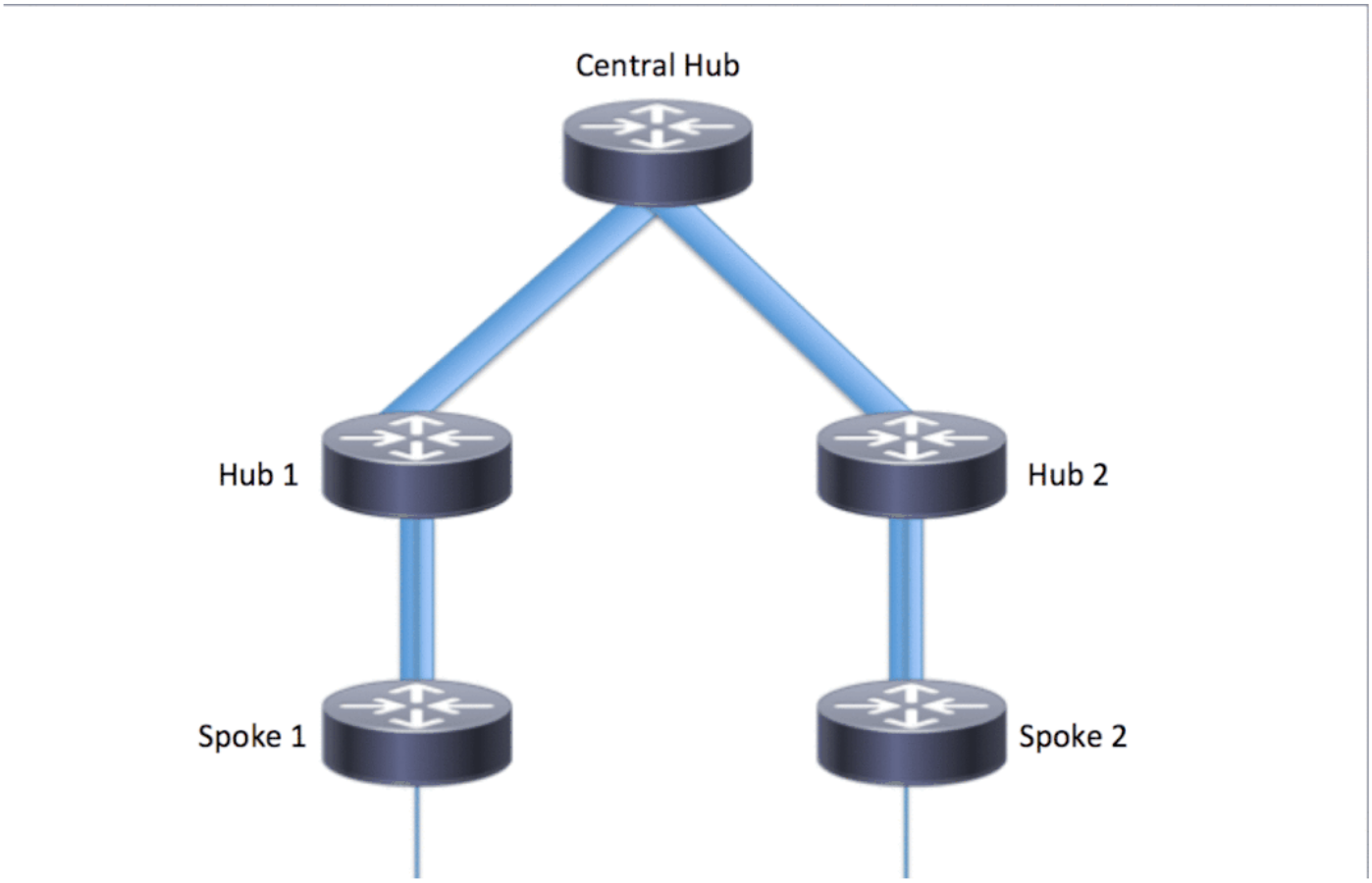
區域2分支（分支2）

```
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
```

瞭解資料和NHRP資料包流

下圖顯示了第一個資料包流，然後是NHRP解析請求和應答流：



第一個資料包流

步驟 1.從分支1發起的ICMP ping，目標= 192.168.18.10，源= 192.168.11.1

1. 對192.168.18.10執行路由查詢。如下圖所示，下一跳是10.0.1.8（集線器1的隧道地址）
2. NHRP快取查詢是在Tunnel0上為目標192.168.18.10完成的，但在此階段找不到任何條目。

3. 對Tunnel0上的下一跳（即10.0.1.8）執行NHRP快取查詢。如下圖所示，條目存在，並且加密會話為UP狀態。
4. ICMP回應請求資料包透過現有隧道轉發到下一跳（即Hub1）。

<#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
```

步驟 2.集線器1上收到的ICMP資料包

1. 對192.168.18.10執行路由查詢。下一跳是10.0.0.1（集線器0的隧道地址）。
2. 由於Hub1不是送出點，並且資料包需要轉發到同一DMVPN雲中的另一個介面，因此Hub 1向Spoke 1傳送NHRP內部方向/重定向。
3. 同時，資料包被轉發到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
```

步驟 3.集線器0上接收的ICMP資料包

1. 對192.168.18.10執行路由查詢。Tunnel0上的下一跳為10.0.0.16（Hub2的隧道地址）
2. 由於中心0不是送出點，並且資料包需要透過同一介面轉發回同一DMVPN雲，因此中心0會透過中心1將NHRP間接傳送至分支1。
3. 資料包被轉發到集線器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
```

步驟 4.集線器2上收到的ICMP資料包

1. 對192.168.18.10執行路由查詢。Tunnel2上的下一跳為10.0.2.18（Spoke2的隧道地址）
2. 由於中心2不是送出點，且資料包需要轉發到同一DMVPN雲中的另一個介面，因此中心2會透過中心0將NHRP單向傳送到分支1。
3. 資料包被轉發到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
```

步驟 5.在Spoke 2上接收的ICMP資料包

路由查詢是針對192.168.18.10完成的，並且是本地連線的網路。將ICMP請求轉發到目的地。

NHRP解決請求流程

分支1

1. 收到集線器1為目的地192.168.18.10傳送的NHRP間接請求。
2. 插入192.168.18.10/32的不完整NHRP快取條目。
3. 對192.168.18.10執行路由查詢。Tunnel0上的下一跳為10.0.1.8（集線器1）
4. NHRP快取查詢針對Tunnel0上的下一跳10.0.1.8完成。找到專案，且加密通訊端也啟動（例如通道存在）
5. 分支1透過現有的分支到區域hub1隧道，將192.168.18.10/32的NHRP解析請求傳送到中心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
```

集線器1

1. 已收到來自分支1的NHRP解析請求，請求目的為192.168.18.1/32。
2. 對192.168.18.1執行路由查詢。Tunnel0上的下一跳為10.0.0.1 (Hub 0)
3. 入口和出口的NHRP網路ID相同，並且本地節點不是出口點。
4. 在Tunnel0上為下一跳10.0.0.1執行NHRP快取查詢，找到條目且加密套接字已啟動（隧道存在）
5. Hub1透過現有隧道將192.168.18.10/32的NHRP解析請求轉發到Hub 0

<#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
```

集線器0

1. 收到目的192.168.18.1/32的NHRP解析請求，由集線器1轉發。
2. 對192.168.18.1執行路由查詢。Tunnel0上的下一跳為10.0.0.16（集線器2）
3. 入口和出口的NHRP網路ID相同，並且本地節點不是出口點。
4. 在Tunnel0上為下一跳10.0.0.16執行NHRP快取查詢，找到條目且加密套接字已啟動（隧道存在）
5. Hub 0透過現有隧道將192.168.18.1/32的NHRP解析請求轉發到Hub 2。

<#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
```

集線器2

1. 從分支1收到目的192.168.18.10/32的NHRP解析請求，由中心0轉發
2. 路由查詢針對192.168.18.10完成，下一跳是Tunnel2上的10.0.2.18（分支2）
3. 入口和出口的NHRP網路ID相同，並且本地節點不是出口點。
4. NHRP快取查詢針對Tunnel2上的下一跳10.0.2.18完成，找到條目且加密套接字為up（隧道存在）
5. 中心2透過現有隧道將192.168.18.1/32的NHRP解析請求轉發到分支2

<#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
```

分支2

1. 收到目的192.168.18.1/32的NHRP解析請求，由集線器2轉發
2. 路由查詢針對192.168.18.10（本地連線的網路）完成。
3. 分支2是退出點，它生成192.168.18.10（字首/24）的解析應答
4. 分支2使用NHRP解析請求的資訊插入10.0.1.11 （分支1）的NHRP快取條目。
5. 分支2起始VPN隧道，遠端端點=分支1的NBMA地址。會協商動態輻射型-輻射型隧道。
6. 然後，Spoke 2透過剛剛構建的動態隧道將192.168.18.10/24的NHRP解析應答傳送到Spoke 1。

<#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
```

分支1

1. NHRP解析應答從分支2透過動態隧道從目標192.168.18.10（字首/24）接收。
2. 192.168.18.0/24的NHRP快取條目現在已更新，下一跳= 10.0.2.18，NBMA = 172.16.2.1
3. NHRP路由增加到192.168.18.10網路的RIB中，下一跳= 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
```

驗證

附註： Cisco CLI Analyzer(僅供已註冊客戶使用)支援某些show指令。使用 Cisco CLI Analyzer 檢視 show 指令輸出的分析。

在構建分支型隧道之前，即形成NHRP捷徑條目

<#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#
```

形成輻條-輻條動態隧道後，即形成NHRP快捷入口

<#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:
```

上述本地（無套接字）NHRP快取條目的原因

本地標誌是指用於此路由器本地網路（由此路由器提供服務）的NHRP對映條目。當此路由器使用此資訊回應NHRP解析請求時，將建立這些條目，並用於儲存已向其傳送此資訊的所有其他NHRP節點的隧道IP地址。如果由於某些原因，此路由器失去對此本地網路的訪問（它無法再服務此網路），它將傳送NHRP清除消息到「local」條目中列出的所有遠端NHRP節點(show ip nhrp detail)，告知遠端節點從其NHRP對映表中清除此資訊。

對於我們不需要也不希望觸發IPsec來設定加密的NHRP對映條目，不會看到套接字。

<#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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

附註：使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

DMVPN故障排除包括按以下順序進行的4層故障排除：

1. 物理（NBMA或隧道終端）路由層
2. IPsec加密層
3. GRE封裝層
4. 動態路由協定層

在疑難排解之前，最好先執行下列指令：

<#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
```

物理（NBMA或隧道終端）路由層

檢查是否可以從中心點ping到分支點的NBMA地址，以及從分支點到Hub的NBMA地址（從分支點上的show ip nhrp的輸出中）。這些ping應該直接從物理介面發出，而不是透過DMVPN隧道。 如果這樣不起作用，您需要檢查路由以及中心路由器和分支路由器之間的任何防火牆。

IPSec加密層

運行以下命令以檢查中心和分支的NBMA地址之間的ISAKMP SA和IPSec SA。

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

啟用以下調試可以對IPSec加密層問題進行故障排除：

<#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

分支定期傳送NHRP註冊請求，每1/3 NHRP保持時間（分支上）或ip nhrp registration timeout <seconds>值傳送一次。 可以透過運行以下命令來檢查分支上的此問題：

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

使用上面的命令可檢查分支是否正在傳送NHRP註冊請求並從中心伺服器獲得回覆。

要檢查中心是否具有中心上NHRP快取中分支的NHRP對映條目，請運行此命令：

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

要排除NHRP相關問題，可以使用以下調試：

<#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
```

動態路由協定層

根據所使用的動態路由協定，請參閱以下文檔：

- 排除EIGRP故障
- OSPF故障排除
- 疑難排解 BGP

相關資訊

- 最常見的DMVPN故障排除解決方案
- DMVPN事件跟蹤
- 增強型NHRP捷徑交換
- 從動態多點VPN第2階段遷移到第3階段
- Cisco Feature Navigator
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。