配置带有多子网辐条的第3阶段分层DMVPN

目录

简介

本文档提供有关如何配置带有多子网辐条的第3阶段分层动态多点VPN (DMVPN)的信息。

先决条件

要求

Cisco 建议您了解以下主题：

- DMVPN基础知识
- 增强型内部网关路由协议(EIGRP)基础知识

> 注意：对于带有多子网辐条的分层DMVPN，请确保路由器具有CSCug42027漏洞修复。由于路由器运行的IOS版本不带CSCug42027的修补程序，因此一旦在不同子网的辐射点之间形成了辐射点到辐射点隧道，辐射点到辐射点数据流就会失败。

CSCug42027在以下IOS和IOS-XE版本中进行了解析：

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

使用的组件

本文档中的信息基于下列硬件和软件版本：

- 运行Cisco IOS®版本15.5(2)T的Cisco 2911集成多业务路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

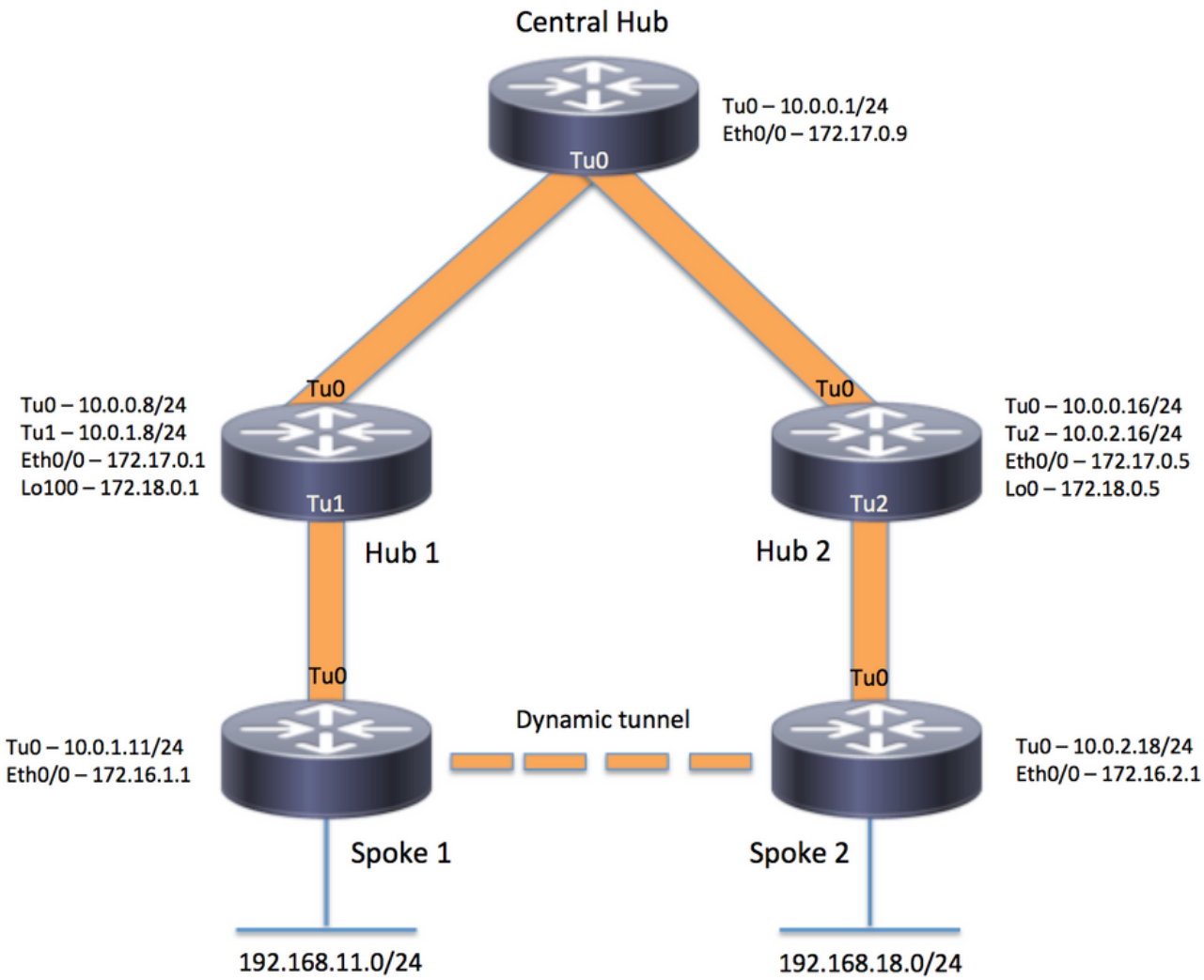
背景信息

分层设置（大于一个级别）允许使用更复杂的基于树的DMVPN网络拓扑。基于树的拓扑允许使用作为中心集线器分支的区域集线器建立DMVPN网络。此架构允许区域网络枢纽处理其区域分支的数据和下一跳解析协议(NHRP)控制流量。 但是，它仍然允许在DMVPN网络内的任何分支之间构建分支到分支隧道，无论它们是否位于同一区域中。此架构还允许DMVPN网络布局与区域或分层数据流模式更加匹配。

配置

本部分提供有关如何配置本文档中所述功能的信息。

网络图



配置

注意：本示例仅包括配置的相关部分。

中央集线器（集线器0）

```
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
```

区域1集线器（集线器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
```

区域2集线器（集线器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
```

区域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
```

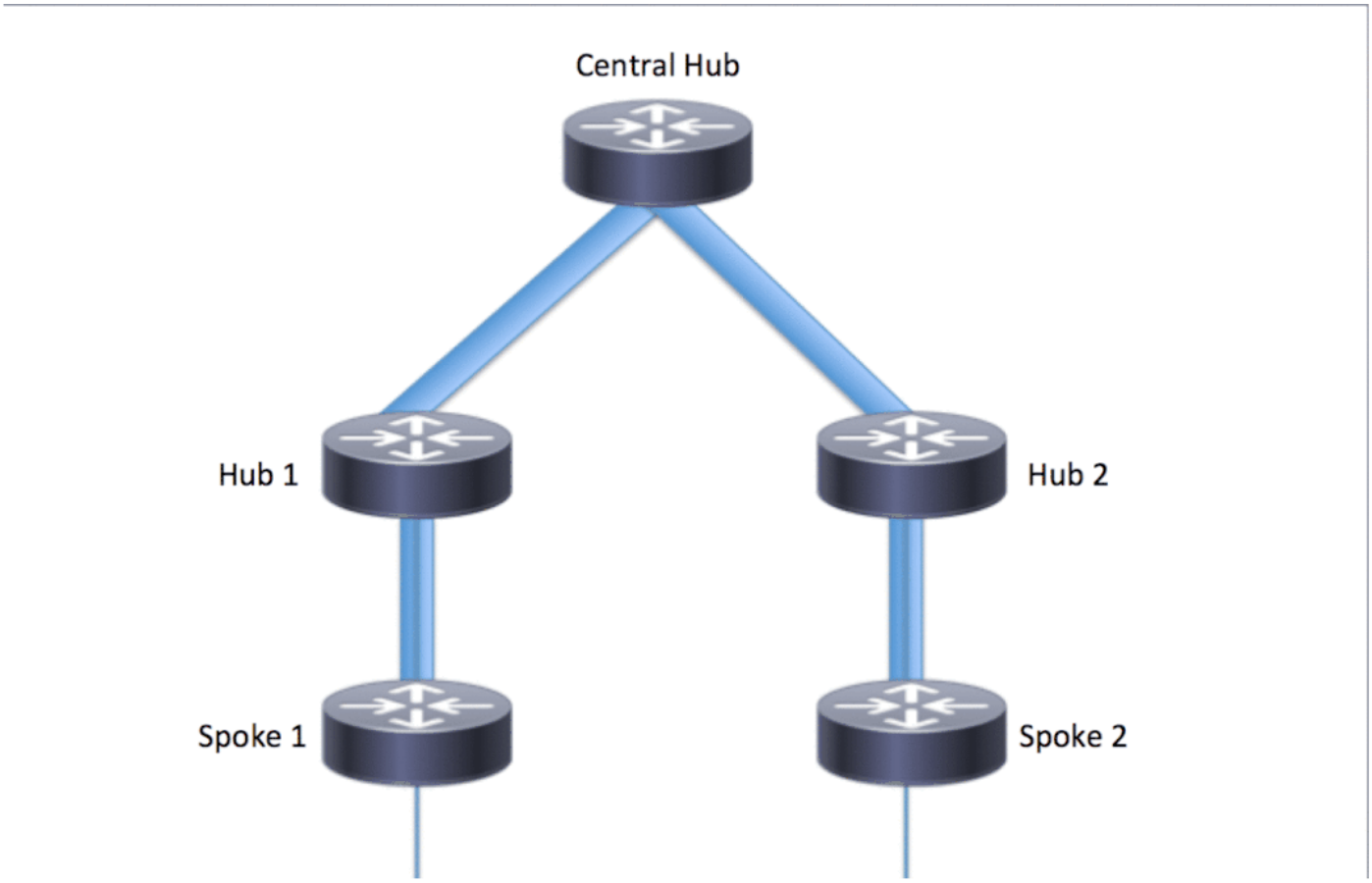
区域2分支（分支2）

```
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
```

了解数据和NHRP数据包流

下图显示了第一个数据包流，后跟NHRP解析请求和应答流：



第一个数据包流

步骤1:ICMP ping从spoke 1发起，目标= 192.168.18.10，源= 192.168.11.1

1. 为192.168.18.10执行路由查找。如下所示，下一跳为10.0.1.8（集线器1的隧道地址）
2. 在Tunnel0上为目标192.168.18.10执行NHRP缓存查找，但在此阶段未找到任何条目。

3. NHRP缓存查找是针对下一跳（即Tunnel0上的10.0.1.8）完成的。如下图所示，条目存在，并且加密会话已启动。
4. ICMP回应请求数据包通过现有隧道转发到下一跳，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
```

第二步：集线器1收到的ICMP数据包

1. 为192.168.18.10执行路由查找。下一跳为10.0.0.1（集线器0的隧道地址）。
2. 由于Hub1不是送出点，并且数据包需要转发到同一DMVPN云中的另一个接口，因此Hub 1会向分支1发送NHRP间接寻址/重定向消息。
3. 同时，会将数据包转发到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
```

第三步：集线器0上收到的ICMP数据包

1. 为192.168.18.10执行路由查找。下一跳是Tunnel0上的10.0.0.16（Hub2的隧道地址）
2. 由于中心0不是送出点，并且数据包需要通过同一接口转发回同一DMVPN云，因此中心0通过中心1将NHRP间接发送给分支1。
3. 数据包将转发到集线器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
```

第四步：集线器2收到的ICMP数据包

1. 为192.168.18.10执行路由查找。下一跳是Tunnel2上的10.0.2.18（Spoke2的隧道地址）
2. 由于中心2不是出口点，并且数据包需要转发到同一DMVPN云中的另一个接口，因此中心2通过中心0将NHRP间接发送到分支1。
3. 数据包被转发到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
```

第五步：在Spoke 2上收到的ICMP数据包

路由查找针对192.168.18.10并且是本地连接的网络。将ICMP请求转发到目的地。

NHRP解析请求流程

分支1

1. 收到集线器1为目的地192.168.18.10发送的NHRP间接通知。
2. 插入192.168.18.10/32的不完整NHRP缓存条目。
3. 为192.168.18.10执行路由查找。下一跳是Tunnel0上的10.0.1.8（集线器1）
4. 对Tunnel0上的下一跳10.0.1.8执行NHRP缓存查找。找到条目并且加密套接字也处于启用状态（即存在隧道）
5. 分支1通过现有分支向区域hub1隧道将192.168.18.10/32的NHRP解析请求发送到中心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
```

集线器1

1. 已收到来自Spoke 1的对目标192.168.18.1/32的NHRP解析请求。
2. 为192.168.18.1执行路由查找。下一跳是Tunnel0上的10.0.0.1（集线器0）
3. 入口和出口的NHRP网络ID相同，并且本地节点不是出口点。
4. 对Tunnel0上的下一跳10.0.0.1执行NHRP缓存查找，找到条目且加密套接字已启动（隧道存在）
5. Hub1将通过现有隧道将192.168.18.10/32的NHRP解析请求转发到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
```

集线器0

1. 接收有关目标192.168.18.1/32的NHRP解析请求，然后由集线器1转发。
2. 为192.168.18.1执行路由查找。下一跳是Tunnel0上的10.0.0.16（集线器2）
3. 入口和出口的NHRP网络ID相同，并且本地节点不是出口点。
4. 在Tunnel0上为下一跳10.0.0.16执行NHRP缓存查找，找到条目且加密套接字已启动（隧道存在）
5. 集线器0通过现有隧道将对192.168.18.1/32的NHRP解析请求转发到集线器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
```

集线器2

1. NHRP解析请求从分支1接收，发往目标192.168.18.10/32，由中心0转发
2. 为192.168.18.10执行路由查找，下一跳为Tunnel2上的10.0.2.18 (Spoke 2)
3. 入口和出口的NHRP网络ID相同，并且本地节点不是出口点。
4. 在Tunnel2上为下一跳10.0.2.18执行NHRP缓存查找，找到条目且加密套接字已启动（隧道存在）
5. 中心2通过现有隧道将192.168.18.1/32的NHRP解析请求转发到Spoke 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. 接收有关目标192.168.18.1/32的NHRP解析请求，然后由集线器2转发
2. 192.168.18.10是本地连接的网络，其路由查找过程将会完成。
3. Spoke 2是退出点，它为192.168.18.10生成解析应答，前缀/24
4. 分支2使用NHRP解析请求中的信息插入10.0.1.11（分支1）的NHRP缓存条目。
5. 分支2启动VPN隧道，远程端点=分支1的NBMA地址。将协商动态分支-分支隧道。
6. 然后，分支2通过刚建立的动态隧道将192.168.18.10/24的NHRP解析应答发送到分支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解析应答从分支2接收，目的地址为192.168.18.10，前缀为/24，通过动态隧道传输。
2. 192.168.18.0/24的NHRP缓存条目现在已更新，下一跳= 10.0.2.18，NBMA = 172.16.2.1
3. NHRP路由添加到192.168.18.10网络的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
```

验证

注意：思科CLI分析器(注册客户)仅支持某些show命令。要查看对 show 命令输出的分析，请使用思科 CLI 分析器。

建立分支-分支隧道之前，即形成NHRP快捷方式条目

<#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#
```

形成分支-分支动态隧道后，即形成NHRP快捷方式条目

<#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:
```

上面显示的本地（无套接字）NHRP缓存条目的原因

本地标志是指用于此路由器本地网络（由此路由器提供服务）的NHRP映射条目。当此路由器响应包含此信息的NHRP解析请求时，将创建这些条目，并用于存储已向其发送此信息的所有其他NHRP节点的隧道IP地址。如果由于某些原因，此路由器无法访问此本地网络（它不再能服务此网络），它将向“local”条目中列出的所有远程NHRP节点(show ip nhrp detail)发送NHRP清除消息，通知远程节点从其NHRP映射表中清除此信息。

对于我们不需要也不希望触发IPsec来设置加密的NHRP映射条目，不会看到套接字。

<#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
```

故障排除

本部分提供可用于对配置进行故障排除的信息。

注意：使用debug命令之前，请参阅有关Debug命令的重要信息。

DMVPN故障排除包括按以下顺序进行4层故障排除：

1. 物理（NBMA或隧道终端）路由层
2. IPsec加密层
3. GRE封装层
4. 动态路由协议层

在排除故障之前，最好运行以下命令：

<#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或隧道终端）路由层

检查是否可从中心ping分支的NBMA地址，以及从分支ping中心的NBMA地址（来自分支上的show ip nhrp输出）。这些 ping 操作应从物理接口发出，无需通过 DMVPN 隧道。 如果此方法不起作用，则需要检查路由以及中心路由器和分支路由器之间的任何防火墙。

IPSec加密层

运行以下命令以检查中心和分支的NBMA地址之间的ISAKMP SA和IPsec SA。

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

可以启用以下调试来解决IPSec加密层问题：

<#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

分支定期发送NHRP注册请求，每1/3 NHRP保持时间（在分支上）或ip nhrp registration timeout <seconds>值。 您可以通过运行以下命令在分支上检查此问题：

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

使用上述命令检查辐射点是否正在发送NHRP注册请求并从中心点获取回复。

要检查中心点上的NHRP缓存中是否有分支点的NHRP映射条目，请运行此命令：

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

要排除NHRP相关问题，可以使用以下调试：

<#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
```

动态路由协议层

根据所使用的动态路由协议，请参阅以下文档：

- EIGRP 故障排除
- OSPF 故障排除
- BGP 故障排除

相关信息

- 最常见的 DMVPN 故障排除解决方案
- DMVPN事件跟踪
- 增强型NHRP快捷方式交换
- 从动态多点VPN第2阶段迁移到第3阶段
- Cisco Feature Navigator
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。