다중 서브넷 스포크를 사용하여 3단계 계층 구조 DMVPN 구성

목차

소개

이 문서에서는 다중 서브넷 스포크를 사용하여 3단계 계층 DMVPN(Dynamic Multipoint VPN)을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- DMVPN에 대한 기본 지식
- EIGRP(Enhanced Interior Gateway Routing Protocol)에 대한 기본 지식

참고: 멀티서브넷 스포크가 포함된 계층적 DMVPN의 경우 라우터에 CSCug42027의 버그 수정 사항이 있는지 확인하십시오. 라우터가 CSCug42027의 수정 없이 IOS 버전을 실행하는 경우, 스포크 대 스포크 터널이 서로 다른 서브넷의 스포크 사이에 형성되면 스포크 대 스포크 트래픽이 실패합니다.

CSCug42027은 다음 IOS 및 IOS-XE 버전에서 확인됩니다.

- 15.3(3)S/3.10 이상
- 15.4(3)M 이상
- 15.4(1)T 이상

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- Cisco IOS® 버전 15.5(2)T를 실행하는 Cisco 2911 Integrated Services Router

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

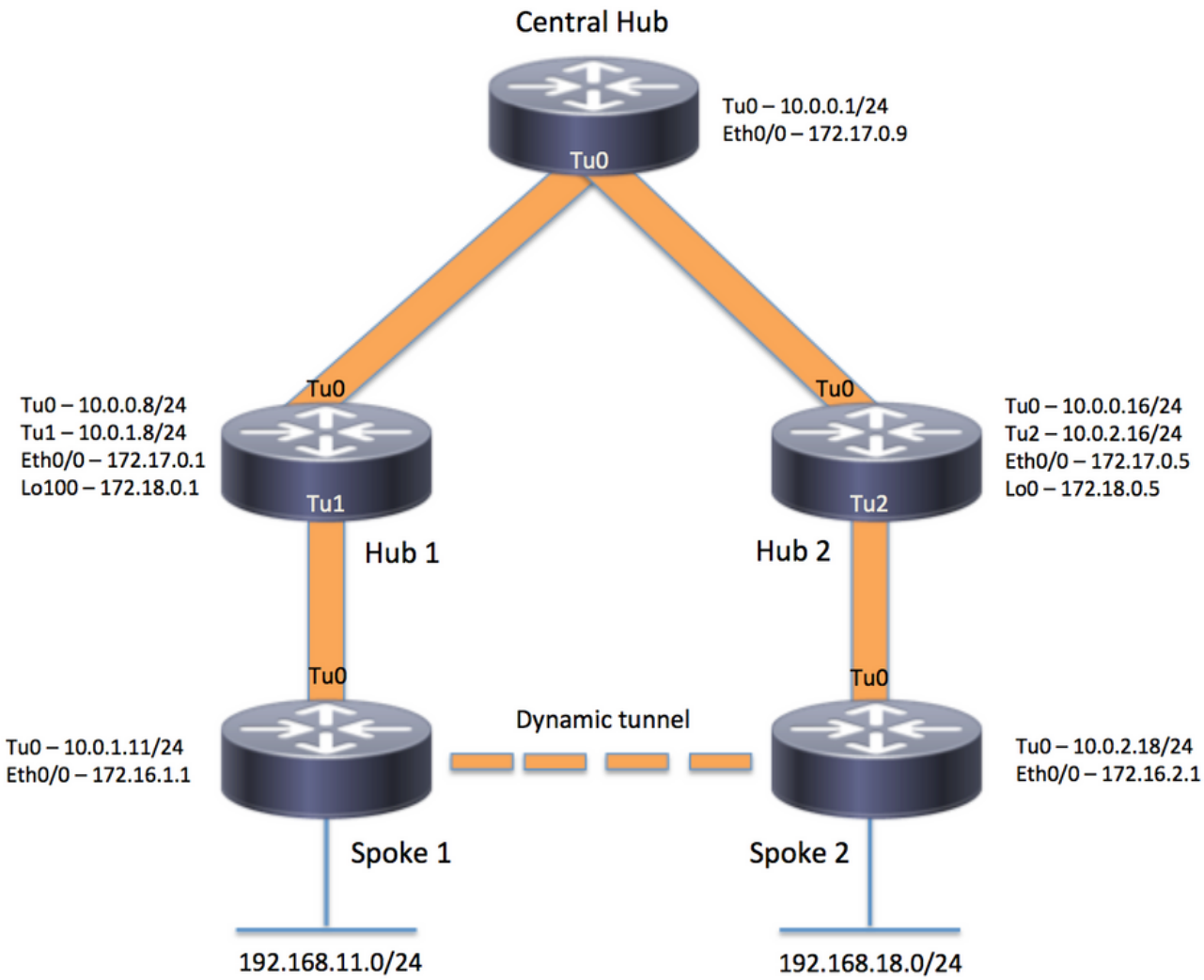
배경 정보

계층적 설정(한 수준 이상)을 통해 더욱 복잡한 트리 기반 DMVPN 네트워크 토폴로지를 구현할 수 있습니다. 트리 기반 토폴로지를 사용하면 중앙 허브의 끝인 지역 허브를 사용하여 DMVPN 네트워크를 구축할 수 있습니다. 이 아키텍처는 지역 허브가 데이터를 처리하고 NHRP(Next Hop Resolution Protocol)가 지역 요인에 대한 트래픽을 제어할 수 있도록 합니다. 그러나 DMVPN 네트워크 내의 스포크 간에 스포크 투 스포크 터널이 동일한 영역에 있든 없든 간에 이 터널은 계속 터널이 구축될 수 있도록 합니다. 또한 이 아키텍처를 통해 DMVPN 네트워크 레이아웃은 지역별 또는 계층적 데이터 흐름 패턴과 더 긴밀하게 일치할 수 있습니다.

구성

이 섹션에서는 이 문서에 설명된 기능을 구성하기 위한 정보를 제공합니다.

네트워크 다이어그램



설정

참고: 이 예에는 컨피그레이션의 관련 섹션만 포함되어 있습니다.

중앙 허브(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
```

지역 1 허브(허브 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
```

지역 2 허브(허브 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
```

지역 1 스포크(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
```

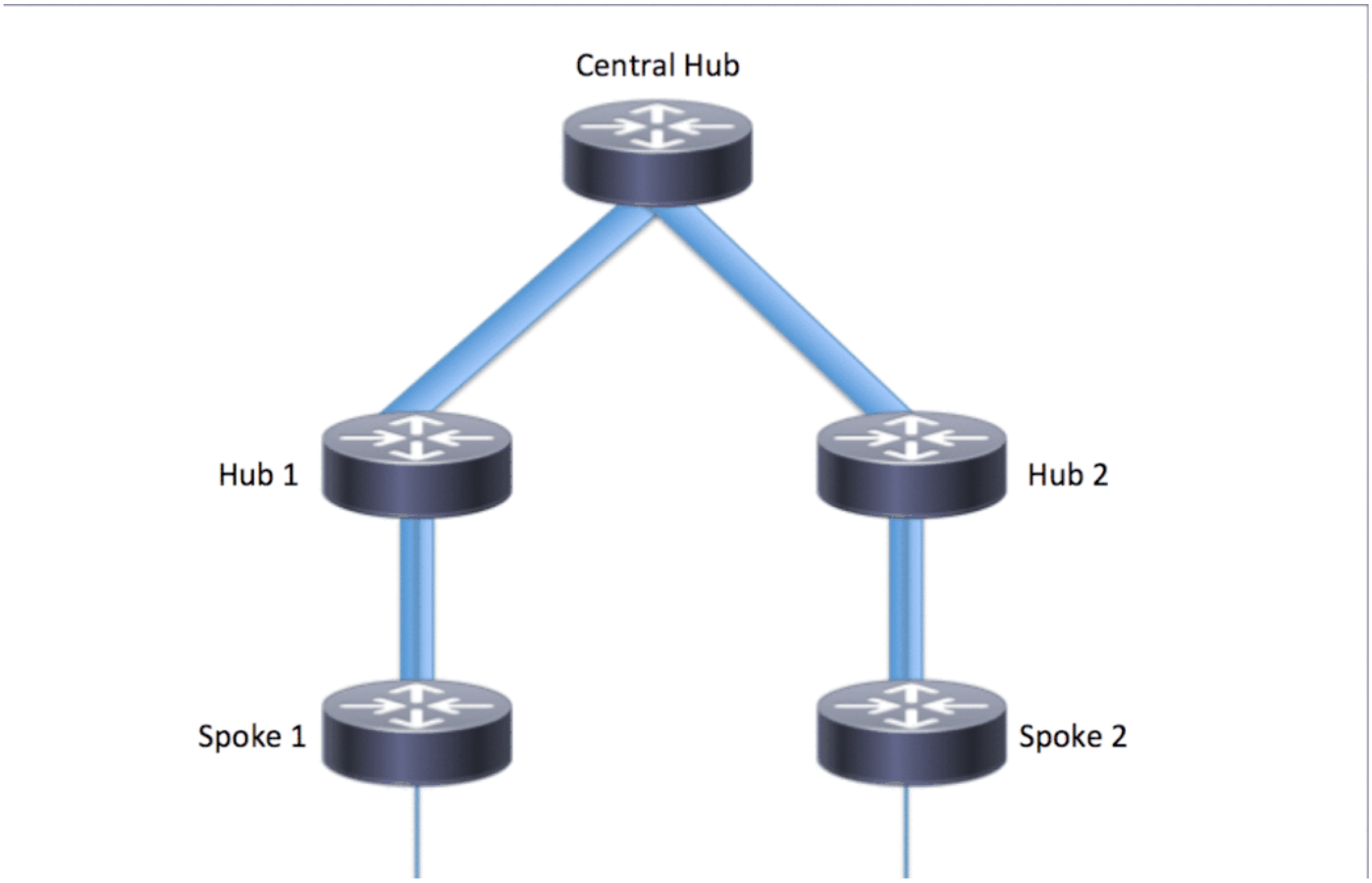
지역 2 스포크(스포크 2)

```
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
```

데이터 및 NHRP 패킷 흐름 이해

이 그림에서는 첫 번째 데이터 패킷 흐름과 NHRP 해결 요청 및 응답 흐름을 보여 줍니다.



첫 번째 데이터 패킷 흐름

1단계. 스포크 1에서 시작된 ICMP ping, 대상 = 192.168.18.10, 소스 = 192.168.11.1

1. 경로 조회는 192.168.18.10에 대해 수행됩니다. 아래에서 볼 수 있듯이 다음 홉은 10.0.1.8(허브 1의 터널 주소)입니다

2. Tunnel0의 대상 192.168.18.10에 대해 NHRP 캐시 조회가 수행되지만 이 단계에서는 항목을 찾을 수 없습니다.
3. NHRP 캐시 조회는 다음 홉(예: Tunnel0의 10.0.1.8)에 대해 수행됩니다. 아래에 표시된 대로 항목이 있고 암호화 세션이 UP입니다.
4. ICMP 에코 요청 패킷은 기존 터널을 통해 다음 홉(예: Hub1)으로 전달됩니다.

<#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
```

2단계. 허브 1에서 수신된 ICMP 패킷

1. 경로 조회는 192.168.18.10에 대해 수행됩니다. 다음 홉은 10.0.0.1(허브 0의 터널 주소)입니다.
2. Hub1은 종료 지점이 아니므로 패킷이 동일한 DMVPN 클라우드 내의 다른 인터페이스로 전달되어야 하므로, Hub1은 NHRP를 Spoke 1로 방향/리디렉션합니다.
3. 동시에 데이터 패킷은 Hub0에 전달됩니다.

<#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
```

3단계. 허브 0에서 수신된 ICMP 패킷

1. 경로 조회는 192.168.18.10에 대해 수행됩니다. 다음 홉은 Tunnel0의 10.0.0.16(Hub2의 터널 주소)입니다
2. 허브 0이 종료 지점이 아니므로 패킷이 동일한 인터페이스를 통해 동일한 DMVPN 클라우드로 다시 전달되어야 하므로 허브 0은 NHRP를 허브 1을 통해 스포크 1로 전송합니다.
3. 데이터 패킷은 허브 2로 전달됩니다.

<#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
```

4단계. 허브 2에서 수신된 ICMP 패킷

1. 경로 조회는 192.168.18.10에 대해 수행됩니다. 다음 홉은 Tunnel2에서 10.0.2.18(Spoke2의 터널 주소)입니다
2. 허브 2는 종료 지점이 아니므로 패킷이 동일한 DMVPN 클라우드 내의 다른 인터페이스로 전달되어야 하므로, 허브 2는 허브 0을 통해 스포크 1로 NHRP를 전송합니다.
3. 데이터 패킷이 스포크 2로 전달됩니다.

<#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
```

5단계. 스포크 2에서 수신된 ICMP 패킷

경로 조회는 192.168.18.10에 대해 수행되며 로컬로 연결된 네트워크입니다. ICMP 요청을 대상으로 전달합니다.

NHRP 해결 요청 흐름

스포크 1

1. 허브 1에서 목적지 192.168.18.10으로 전송한 NHRP 간접 정보를 수신합니다.
2. 192.168.18.10/32에 대한 불완전한 NHRP 캐시 항목이 삽입됩니다.
3. 경로 조회는 192.168.18.10에 대해 수행됩니다. 다음 홉은 Tunnel0의 10.0.1.8(허브 1)입니다
4. Tunnel0의 다음 홉 10.0.1.8에 대해 NHRP 캐시 조회가 수행됩니다. 항목이 발견되고 암호화 소켓도 가동(예: 터널이 있음)
5. 스포크 1은 기존 스포크를 통해 허브 1에 192.168.18.10/32에 대한 NHRP 확인 요청을 지역 hub1 터널로 전송합니다.

<#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
```

허브 1

1. 대상 192.168.18.1/32에 대한 스포크 1의 NHRP 확인 요청이 수신되었습니다.
2. 경로 조회는 192.168.18.1에 대해 수행됩니다. 다음 홉은 Tunnel0의 10.0.0.1(허브 0)입니다
3. 인그레스 및 이그레스에 대한 NHRP 네트워크 ID가 동일하며 로컬 노드가 종료 지점이 아닙니다.
4. NHRP 캐시 조회가 Tunnel0의 다음 홉 10.0.0.1에 대해 수행되며, 항목이 발견되고 암호화 소켓이 가동(터널이 있음)되었습니다.
5. Hub1은 192.168.18.10/32에 대한 NHRP 확인 요청을 기존 터널을 통해 허브 0으로 전달합니다

<#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
```

허브 0

1. NHRP 확인 요청은 목적지 192.168.18.1/32에 대해 수신되며, 허브 1에 의해 전달됩니다.
2. 경로 조회는 192.168.18.1에 대해 수행됩니다. 다음 홉은 Tunnel0의 10.0.0.16(허브 2)입니다
3. 인그레스 및 이그레스에 대한 NHRP 네트워크 ID가 동일하며 로컬 노드가 종료 지점이 아닙니다.

4. NHRP 캐시 조회가 Tunnel0의 다음 홉 10.0.0.16에 대해 수행되며, 항목이 발견되고 암호화 소켓이 가동(터널이 있음)되었습니다.
5. 허브 0은 192.168.18.1/32에 대한 NHRP 확인 요청을 기존 터널을 통해 허브 2로 전달합니다.

<#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
```

허브 2

1. NHRP 확인 요청은 대상 192.168.18.10/32에 대한 스포크 1에서 허브 0에 의해 전달됩니다
2. 경로 조회는 192.168.18.10에 대해 수행되며, 다음 홉은 Tunnel2에서 10.0.2.18(스포크 2)입니다.
3. 인그레스 및 이그레스에 대한 NHRP 네트워크 ID가 동일하며 로컬 노드가 종료 지점이 아닙니다.
4. NHRP 캐시 조회가 Tunnel2에서 다음 홉 10.0.2.18에 대해 수행되며, 항목이 발견되고 암호화 소켓이 작동 중입니다(터널이 있음).
5. 허브 2는 192.168.18.1/32에 대한 NHRP 확인 요청을 기존 터널을 통해 스포크 2로 전달합니다

<#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
```

스포크 2

1. NHRP 확인 요청은 목적지 192.168.18.1/32에 대해 수신되며, 허브 2에 의해 전달됩니다
2. 로컬로 연결된 네트워크인 192.168.18.10에 대해 경로 조회가 수행됩니다.
3. 스포크 2는 종료 지점이며 192.168.18.10, 접두사 /24에 대한 해결 응답을 생성합니다.
4. 스포크 2는 NHRP 해결 요청의 정보를 사용하여 10.0.1.11(스포크 1)에 대한 NHRP 캐시 항목을 삽입합니다.
5. 스포크 2는 원격 엔드포인트 = 스포크 1의 NBMA 주소로 VPN 터널을 시작합니다. 동적 스포크-스포크 터널이 협상됩니다.
6. 그런 다음 스포크 2는 192.168.18.10/24에 대한 NHRP 확인 응답을 방금 빌드된 동적 터널을 통해 스포크 1로 전송합니다.

<#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
```

스포크1

1. NHRP 확인 응답은 동적 터널을 통해 대상 192.168.18.10, 접두사 /24에 대한 스포크 2에서 수신됩니다.
2. 192.168.18.0/24에 대한 NHRP 캐시 항목이 이제 next hop = 10.0.2.18, NBMA = 172.16.2.1로 업데이트됩니다.
3. NHRP 경로가 192.168.18.10 네트워크의 RIB에 추가됩니다. next 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
```

다음을 확인합니다.

참고: Cisco CLI Analyzer(등록된 고객만 해당)는 특정 show 명령을 지원합니다. Cisco CLI Analyzer를 사용하여 show 명령 출력의 분석을 봅니다.

스포크 스포크 터널이 구축되기 전(예: NHRP 바로가기 항목 형성)

<#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#
```

Spoke-Spoke 동적 터널이 형성된 후(예: NHRP 바로가기 항목이 형성된 경우)

<#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:
```

위에서 볼 수 있는 로컬(소켓 없음) NHRP 캐시 항목의 이유

Local Flag(로컬 플래그)는 이 라우터(이 라우터가 서비스)에 로컬인 네트워크에 대한 NHRP 매핑 항목을 나타냅니다. 이 항목은 이 라우터가 이 정보로 NHRP 확인 요청에 응답할 때 생성되며 이 정보를 전송한 다른 모든 NHRP 노드의 터널 IP 주소를 저장하는 데 사용됩니다. 어떤 이유로 이 라우터가 이 로컬 네트워크에 대한 액세스 권한을 상실하면(더 이상 이 네트워크를 서비스할 수 없음) 'local' 항목(ip nhrp 세부 정보 표시)에 나열된 모든 원격 NHRP 노드에 NHRP 제거 메시지를 보내 원격 노드에 NHRP 매핑 테이블에서 이 정보를 지우도록 지시합니다.

암호화를 설정하기 위해 IPsec을 트리거할 필요가 없고 그럴 필요가 없는 NHRP 매핑 엔트리에 대해 소켓이 표시되지 않습니다.

<#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
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

참고: debug 명령을 사용하기 전에 Debug 명령에 대한 중요 정보를 참조하십시오.

DMVPN 트러블슈팅에는 다음 순서로 4개 레이어에서 트러블슈팅이 포함됩니다.

1. 물리적(NBMA 또는 터널 엔드포인트) 라우팅 레이어
2. IPsec 암호화 레이어
3. GRE 캡슐화 레이어
4. 동적 라우팅 프로토콜 레이어

트러블슈팅 전에 다음 명령을 실행하는 것이 좋습니다.

<#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
```

물리적(NBMA 또는 터널 엔드포인트) 라우팅 레이어

허브에서 스포크의 NBMA 주소로, 스포크에서 허브의 NBMA 주소로 ping할 수 있는지 확인합니다 (스포크의 show ip nhrp 출력). 이러한 ping은 DMVPN 터널을 통해서가 아니라 물리적 인터페이스 외부로 직접 전달되어야 합니다. 이 방법이 작동하지 않으면 허브 라우터와 스포크 라우터 간의 라우팅 및 방화벽을 확인해야 합니다.

IPSec 암호화 레이어

다음 명령을 실행하여 허브와 스포크의 NBMA 주소 간에 ISAKMP SA 및 IPsec SA를 확인합니다.

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

이러한 디버그를 활성화하여 IPSec 암호화 레이어 문제를 해결할 수 있습니다.

<#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

스포크는 1/3 NHRP holdtime(스포크 시) 또는 ip nhrp registration timeout <seconds> 값마다 NHRP 등록 요청을 정기적으로 전송합니다. 다음을 실행하여 스포크에서 이를 확인할 수 있습니다 .

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

위 명령을 사용하여 스포크가 NHRP 등록 요청을 전송하고 허브에서 응답을 받는지 확인합니다.

허브에 허브의 NHRP 캐시에 있는 스포크에 대한 NHRP 매핑 항목이 있는지 확인하려면 다음 명령을 실행합니다.

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

NHRP 관련 문제를 트러블슈팅하기 위해 다음 디버그를 사용할 수 있습니다.

<#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
```

동적 라우팅 프로토콜 레이어

사용 중인 동적 라우팅 프로토콜에 따라 다음 문서를 참조하십시오.

- EIGRP 문제 해결
- OSPF 문제 해결
- BGP 문제 해결

관련 정보

- 가장 일반적인 DMVPN 문제 해결 솔루션
- DMVPN 이벤트 추적
- 향상된 NHRP 바로가기 스위칭
- Dynamic Multipoint VPN 2단계에서 3단계로 마이그레이션
- Cisco 기능 내비게이터
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.