複数サブネット スポークを使用したフェーズ 3 階層型 DMVPN の設定

内容

はじめに

本書では、複数サブネット スポークを使用したフェーズ 3 階層型 Dynamic Multipoint VPN（DMVPN）を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- DMVPN に関する基礎知識
- Enhanced Interior Gateway Routing Protocol（EIGRP）に関する基礎知識

注：複数サブネットスポークを使用した階層型DMVPNでは、ルータにCSCug42027のバグ修正が適用されていることを確認してください。CSCug42027 の修正が適用されていないバージョンの IOS を実行しているルータでは、異なるサブネットのスポーク間でスポーク間トンネルが形成されると、スポーク間トラフィックが失敗します。

CSCug42027 は次の IOS および IOS XE バージョンで解決されました。

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

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

- Cisco IOS® バージョン 15.5(2)T を実行する Cisco 2911 サービス統合型ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

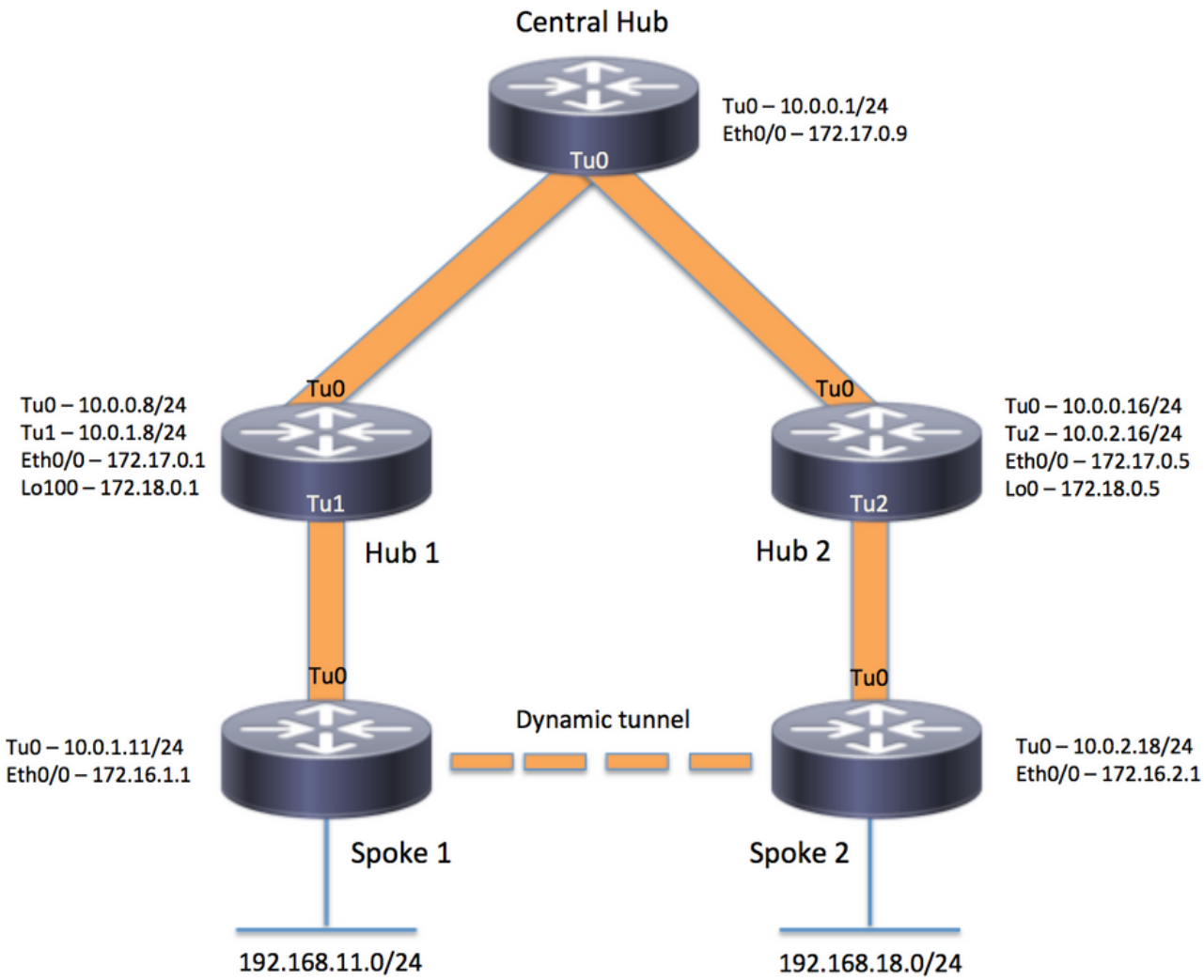
背景説明

（複数レベルからなる）階層型セットアップでは、より複雑なツリーベースの DMVPN ネットワーク トポロジを実現できます。ツリーベースのトポロジを使用すると、中央のハブのスポークであるリージョナル ハブを持つ DMVPN ネットワークを構築できます。このアーキテクチャでは、リージョナル ハブが、そのリージョナル スポークのデータと Next Hop Resolution Protocol（NHRP）制御トラフィックを処理できます。 ただし、スポークが同じリージョンであるかどうかに関わらず、DMVPN ネットワーク内の任意のスポーク間でスポーク間トンネルを作成できます。また、このアーキテクチャでは、リージョナルまたは階層型データ フロー パターンにより近い DMVPN ネットワーク レイアウトを作成できます。

設定

ここでは、このドキュメントで説明する機能を設定するための情報を示します。

ネットワーク図



コンフィギュレーション

注：この例では、設定の関連セクションのみを示しています。

中央ハブ（ハブ 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
```

リージョン 1 ハブ (ハブ 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
```

リージョン 2 ハブ (ハブ 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
```

リージョン 1 スポーク (スポーク 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
```

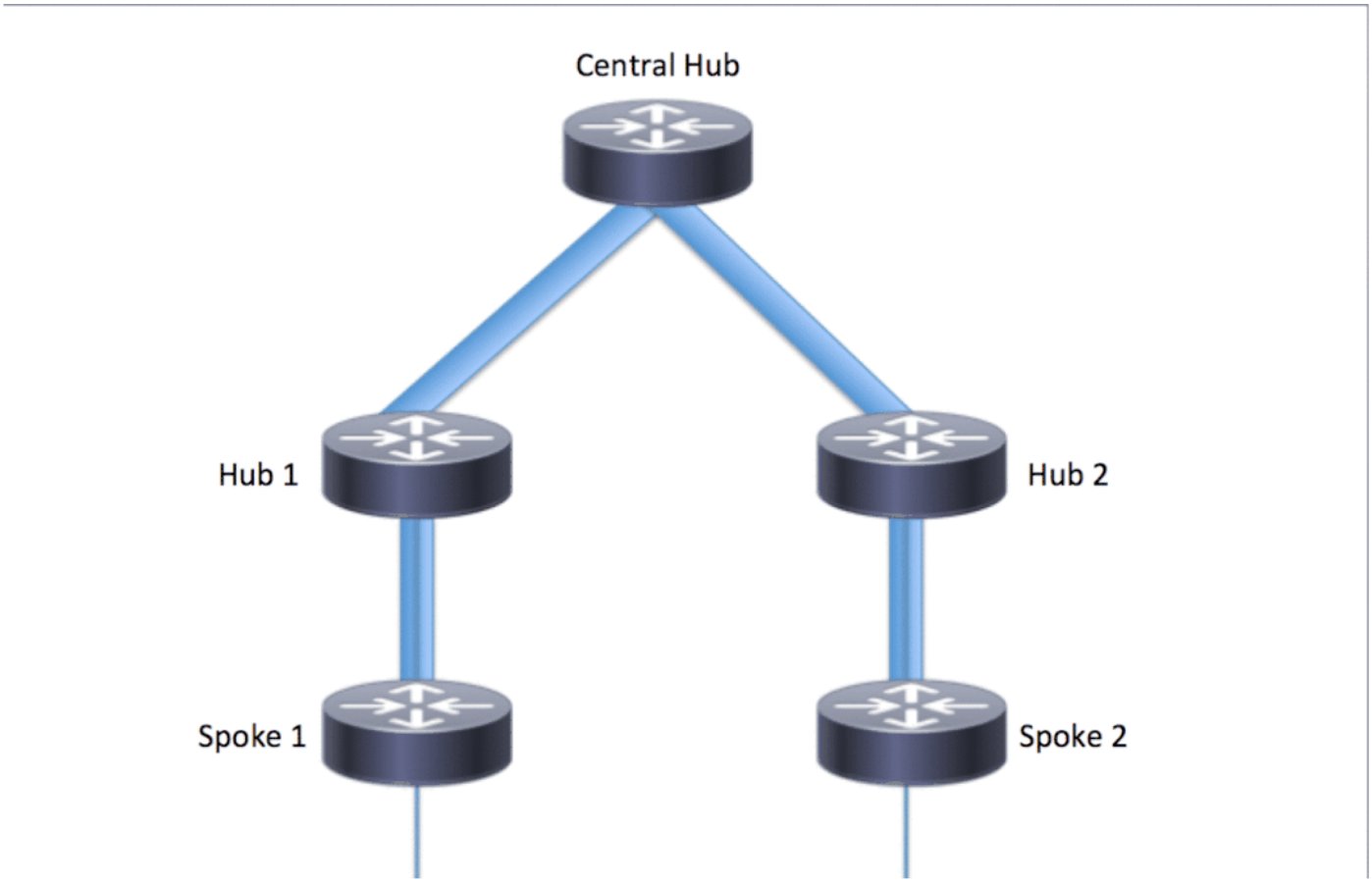
リージョン 2 スポーク (スポーク 2)

```
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
```

データと NHRP パケット フローについて

次の図に最初のデータ パケット フローと、その後に続く NHRP 解決の要求と応答のフローを示します。



最初のデータ パケット フロー

ステップ 1：スポーク1からICMP pingが開始される。宛先= 192.168.18.10、送信元= 192.168.11.1

1. 192.168.18.10 に対するルート ルックアップが行われます。次に示すように、ネクスト ホップは 10.0.1.8 (ハブ 1 のトンネル アドレス) です。
2. トンネル 0 の宛先 192.168.18.10 に対する NHRP キャッシュ ルックアップが行われますが、この段階ではエントリは検出されません。
3. ネクスト ホップ (トンネル 0 の 10.0.1.8) に対する NHRP キャッシュ ルックアップが行われます。次に示すように、該当するエントリが存在し、暗号化セッションが開始されます。
4. ICMP エコー要求パケットが既存のトンネルを経由してネクスト ホップ (ハブ 1) に転送されます。

<#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
```

ステップ 2：ハブ1でICMPパケットを受信

1. 192.168.18.10 に対するルート ルックアップが行われます。ネクスト ホップは 10.0.0.1 (ハブ 0 のトンネル アドレス) です。
2. ハブ 1 は出力点ではなく、パケットを同じ DMVPN クラウド内の別のインターフェイスに転送する必要があるため、ハブ 1 が NHRP 間接参照/リダイレクトをスポーク 1 に送信します。
3. 同時にデータ パケットがハブ 0 に転送されます。

<#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
```

ステップ 3：ハブ0でICMPパケットを受信

1. 192.168.18.10 に対するルート ルックアップが行われます。ネクスト ホップはトンネル 0 の 10.0.0.16 (ハブ 2 のトンネル アドレス) です。
2. ハブ 0 は出力点ではなく、パケットを同じインターフェイス経由で同じ DMVPN クラウドに転送する必要があるため、ハブ 0 は、ハブ 1 を介してスポーク 1 へ NHRP 間接参照を送信します。
3. データ パケットはハブ 2 に転送されます。

<#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
```

ステップ 4：ハブ2でICMPパケットを受信

1. 192.168.18.10 に対するルート ルックアップが行われます。ネクスト ホップはトンネル 2 の 10.0.2.18 (スポーク 2 のトンネル アドレス) です。
2. ハブ 2 は出力点ではなく、パケットを同じ DMVPN クラウド内の別のインターフェイスに転送する必要があるため、ハブ 2 はハブ 0 を介して NHRP 間接参照をスポーク 1 に送信します。
3. データ パケットはスポーク 2 に転送されます。

<#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
```

ステップ 5：スポーク2で受信されたICMPパケット

192.168.18.10 に対するルート ルックアップが行われます。これはローカル接続ネットワークです。ICMP 要求が宛先に転送されます。

NHRP 解決要求フロー

スポーク 1

1. ハブ 1 により宛先 192.168.18.10 に送信された NHRP 間接参照を受信します。
2. 192.168.18.10/32 の不完全な NHRP キャッシュエントリが挿入されます。
3. 192.168.18.10 に対するルート ルックアップが行われます。ネクスト ホップはトンネル 0 の 10.0.1.8 (ハブ 1) です。
4. ネクスト ホップ (トンネル 0 の 10.0.1.8) に対する NHRP キャッシュ ルックアップが行われます。エントリが検出され、暗号化ソケットが稼働しています (トンネルが存在しています) 。
5. スポーク 1 が、リージョナル ハブ 1 トンネルへの既存のスポークを介して、192.168.18.10/32 の NHRP 解決要求をハブ 1 に送信します。

```
<#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
```

ハブ 1

1. スポーク 1 からの宛先 192.168.18.1/32 に対する NHRP 解決要求を受信します。
2. 192.168.18.1 に対するルート ルックアップが行われます。ネクスト ホップはトンネル 0 の 10.0.0.1 (ハブ 0) です。
3. イングレスとイーグレスの NHRP ネットワーク ID は同一であり、ローカル ノードは出力点ではありません。
4. トンネル 0 のネクスト ホップ 10.0.0.1 に対する NHRP キャッシュ ルックアップが行われ、エントリが検出され、暗号化ソケットが稼働しています (トンネルが存在します) 。
5. ハブ 1 は既存のトンネルを介して、192.168.18.10/32 に対する NHRP 解決要求をハブ 0 に転送します。

<#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
```

ハブ 0

1. ハブ 1 により転送された宛先 192.168.18.1/32 に対する NHRP 解決要求を受信します。
2. 192.168.18.1 に対するルート ルックアップが行われます。ネクスト ホップはトンネル 0 の 10.0.0.16 (ハブ 2) です。
3. イングレスとイーグレスの NHRP ネットワーク ID は同一であり、ローカル ノードは出力点ではありません。
4. トンネル 0 のネクスト ホップ 10.0.0.16 に対する NHRP キャッシュ ルックアップが行われ、エントリが検出され、暗号化ソケットが稼働しています (トンネルが存在します) 。
5. ハブ 0 は既存のトンネルを介して、192.168.18.1/32 に対する NHRP 解決要求をハブ 2 に転送します。

<#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
```

ハブ 2

1. ハブ 0 により転送された宛先 192.168.18.10/32 に対する NHRP 解決要求をスポーク 1 から受信します。

2. 192.168.18.10 に対するルート ルックアップが行われます。ネクスト ホップはトンネル 2 の 10.0.2.18 (スポーク 2) です。
3. イングレスとイーグレスの NHRP ネットワーク ID は同一であり、ローカル ノードは出力点ではありません。
4. トンネル 2 のネクスト ホップ 10.0.2.18 に対する NHRP キャッシュ ルックアップが行われ、エントリが検出され、暗号化ソケットが稼働しています (トンネルが存在します) 。
5. ハブ 2 は既存のトンネルを介して、192.168.18.1/32 に対する NHRP 解決要求をスポーク 2 に転送します。

<#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
```

スポーク 2

1. ハブ 2 により転送された宛先 192.168.18.1/32 に対する NHRP 解決要求を受信します。
2. 192.168.18.10 に対するルート ルックアップが行われます。これはローカル接続ネットワークです。
3. スポーク 2 は出力点であり、192.168.18.10、プレフィックス /24 の解決応答を生成します。
4. スポーク 2 は、NHRP 解決要求の情報を使用して、10.0.1.11 (スポーク 1) の NHRP キャッシュ エントリを挿入します。
5. スポーク 2 が VPN トンネルを開始します (リモート エンドポイント = スポーク 1 の NBMA アドレス) 。ダイナミック スポーク間トンネルがネゴシエートされます。

6. 次にスポーク 2 が、作成されたダイナミック トンネルを介して、192.168.18.10/24 の NHRP 解決応答をスポーク 1 に送信します。

<#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
```

スポーク1

1. スポーク 2 からダイナミック トンネルを介して、宛先 192.168.18.10、プレフィックス /24 の NHRP 解決応答を受信します。
2. 192.168.18.0/24 の NHRP キャッシュ エントリがネクスト ホップ = 10.0.2.18、NBMA = 172.16.2.1 に更新されます。
3. NHRP ルートが、192.168.18.10 ネットワーク、ネクスト ホップ = 10.0.2.18 の RIB に追加されます。

<#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
```

確認

> 注:特定のshowコマンドが、Cisco CLI Analyzer(登録ユーザ専用)でサポートされています。show コマンド出力の分析を表示するには、Cisco CLI アナライザを使用します。

スポーク間トンネルの作成前（NHRP ショートカット エントリの作成前）

<#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#
```

スポーク間ダイナミック トンネルの作成後（NHRP ショートカット エントリの作成後）

<#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:
```

上記のローカル（ソケットなし）NHRP キャッシュ エントリの理由

ローカル フラグは、このルータに対してローカルなネットワーク（このルータによりサービスが提供されるネットワーク）の NHRP マッピング エントリを参照します。これらのエントリは、ルータが NHRP 解決要求に対してこの情報で応答し、このルータに、この情報の送信先であるその他のすべての NHRP ノードのトンネル IP アドレスが保存される場合に作成されます。何らかの理由でこのルータがこのローカル ネットワークにアクセスできなくなる場合（このネットワークにサービスを提供できなくなる場合）、ルータは 「local」エントリにリストされているすべてのリモート NHRP ノード（show ip nhrp detail）に対し、NHRP マッピング テーブルからこの情報をクリアするよう指示する NHRP 消去メッセージを送信します。

暗号化を設定するために IPsec をトリガーする必要がない NHRP マッピング エントリのソケットは示されません。

<#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
```

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

注：debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

DMVPN のトラブルシューティングでは、次の 4 つの層で示されている順序でトラブルシューティングを行います。

1. 物理 (NBMA またはトンネル エンドポイント) ルーティング層
2. IPSec 暗号化層
3. GRE カプセル化層
4. ダイナミック ルーティング プロトコル層

トラブルシューティングの前に、次のコマンドを実行することをお勧めします。

<#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 またはトンネル エンドポイント) ルーティング層

ハブからスポークの NBMA アドレス、およびスポークからハブの NBMA アドレス (スポークで実行した show ip nhrp の出力) に対して ping を実行できるかどうかを確認してください。これらの ping は DMVPN トンネルを経由せずに物理インターフェイスから直接発信されます。 機能しない場合は、ハブ ルータとスポーク ルータの間のルーティングとファイアウォールを調べる必要があります。

IPSec 暗号化層

次のコマンドを実行して、ハブとスポークの NBMA アドレス間の ISAKMP SA と IPsec SA を調べます。

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

IPSec 暗号化層の問題をトラブルシューティングするため、次のデバッグを有効にできます。

<#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

スポークから NHRP 登録要求が定期的（1/3 NHRP 保留時間（スポーク）ごとまたは ip nhrp registration timeout <seconds> の値）に送信されます。 スポークでこれを確認するには、次のコマンドを実行します。

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

上記のコマンドを使用して、スポークが NHRP 登録要求を送信し、ハブから応答を受信するかどうかを確認します。

ハブの NHRP キャッシュにスポークの NHRP マッピング エントリが存在しているかどうかを確認するため、次のコマンドを実行します。

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

NHRP 関連の問題のトラブルシューティングを行うには、次の debug を使用できます。

<#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
```

ダイナミック ルーティング プロトコル層

使用するダイナミック ルーティング プロトコルに応じて、次のドキュメントを参照してください。

- EIGRP のトラブルシューティング
- OSPF に関するトラブルシューティング
- BGP のトラブルシューティング

関連情報

- 最も一般的な DMVPN のトラブルシューティング方法
- DMVPN イベント トレース
- 拡張 NHRP ショートカット スイッチング
- ダイナミック マルチポイント VPN フェーズ 2 からフェーズ 3 への移行
- Cisco Feature Navigator
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。