Configurar DMVPN hierárquica de fase 3 com spokes de várias sub-redes

Contents

Introdução

Este documento fornece informações sobre como configurar uma VPN dinâmica multiponto hierárquica (DMVPN) de fase 3 com spokes de várias sub-redes.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico de DMVPN
- Conhecimento básico do Enhanced Interior Gateway Routing Protocol (EIGRP)

Observação: para DMVPN hierárquica com spokes de várias sub-redes, certifique-se de que os roteadores tenham a correção de bug de CSCug42027. Com os roteadores executando a versão do IOS sem a correção de CSCug42027 , uma vez que o túnel spoke-to-spoke é formado entre os spokes em sub-redes diferentes, o tráfego spoke-to-spoke falha.

O CSCug42027 é resolvido nas seguintes versões do IOS e do IOS-XE:

- 15.3(3)S / 3.10 e posterior.
- 15.4(3)M e posterior.
- 15.4(1)T e posterior.

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware e software:

- Cisco 2911 Integrated Services Routers executando o Cisco IOS® versão 15.5(2)T

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

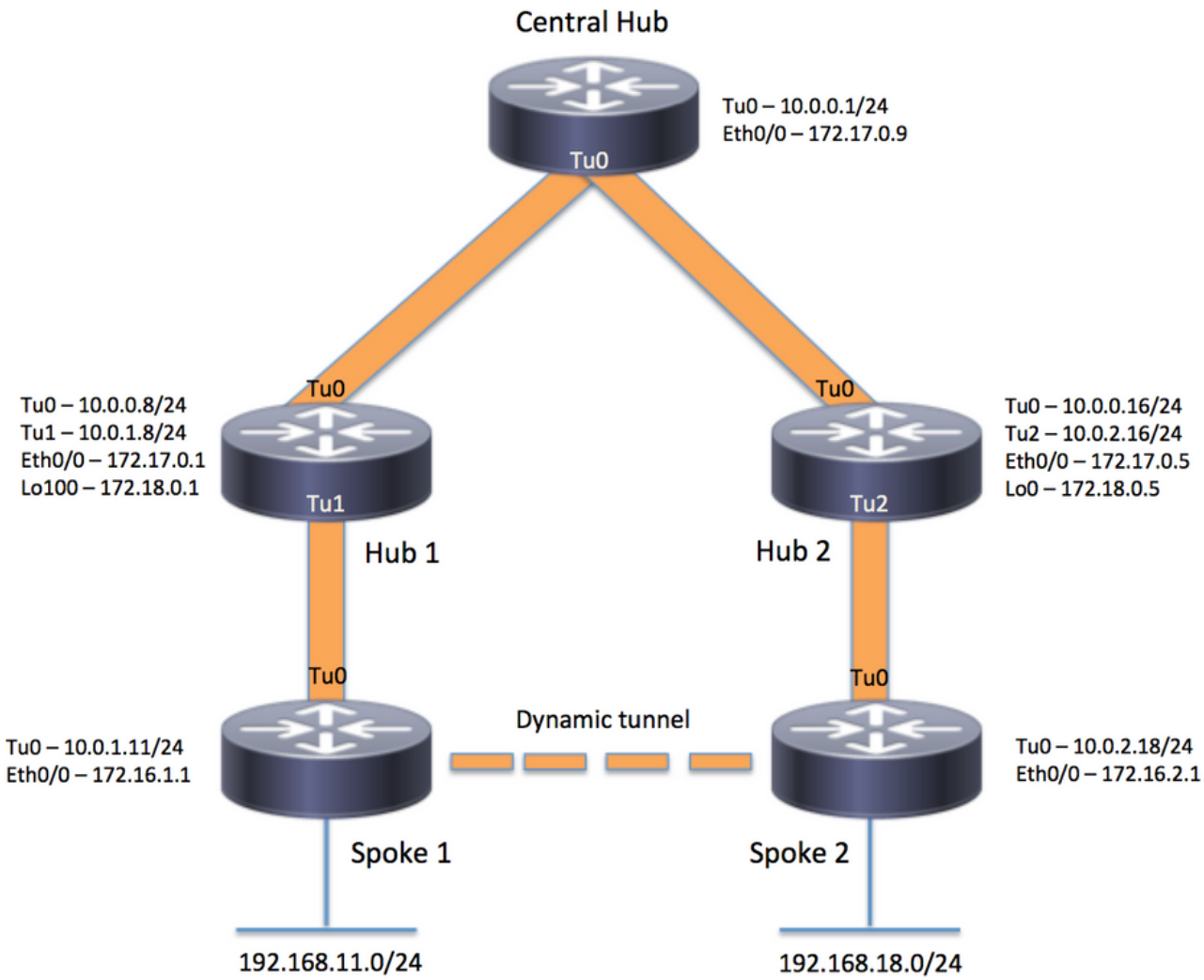
Informações de Apoio

A configuração hierárquica (maior que um nível) permite topologias de rede DMVPN baseadas em árvore mais complexas. As topologias baseadas em árvore permitem a capacidade de criar redes DMVPN com hubs regionais que são spokes de hubs centrais. Essa arquitetura permite que o hub regional manipule os dados e o protocolo NHRP (Next Hop Resolution Protocol) controlem o tráfego para seus spokes regionais. No entanto, ele ainda permite que túneis spoke-to-spoke sejam construídos entre quaisquer spokes dentro da rede DMVPN, estejam eles na mesma região ou não. Essa arquitetura também permite que o layout da rede DMVPN corresponda mais estreitamente aos padrões de fluxo de dados hierárquicos ou regionais.

Configurar

Nesta seção, você verá informações sobre a configuração dos recursos descritos neste documento.

Diagrama de Rede



Configurações

Observação: somente as seções relevantes da configuração são incluídas neste exemplo.

Hub Central (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
```

Hub da região 1 (Hub 1)

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname hub_1
!
crypto isakmp policy 1
  encr aes 256
  hash sha256
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 0.0.0.0
!
```

```
crypto ipsec transform-set transform-dmvpn esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile profile-dmvpn
 set transform-set transform-dmvpn
!
crypto ipsec profile profile-dmvpn-1
 set transform-set transform-dmvpn
!
interface Loopback1
 ip address 192.168.8.1 255.255.255.0
!
interface Loopback100
 ip address 172.18.0.1 255.255.255.252
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.8 255.255.255.0
 no ip redirects
 ip mtu 1400
 no ip split-horizon eigrp 1
 ip nhrp authentication test
 ip nhrp network-id 100000
 ip nhrp nhs 10.0.0.1 nbma 172.17.0.9 multicast
 ip nhrp shortcut
 ip nhrp redirect
 ip summary-address eigrp 1 192.168.8.0 255.255.248.0
 ip tcp adjust-mss 1360
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile profile-dmvpn
!
interface Tunnel1
 bandwidth 1000
 ip address 10.0.1.8 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp redirect
 ip summary-address eigrp 1 192.168.8.0 255.255.248.0
 ip summary-address eigrp 1 192.168.100.0 255.255.252.0
 ip tcp adjust-mss 1360
 tunnel source Loopback100
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile profile-dmvpn-1
!
interface Ethernet0/0
 ip address 172.17.0.1 255.255.255.252
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.8.0
!
ip route 0.0.0.0 0.0.0.0 172.17.0.2
!
end
```

Hub da Região 2 (Hub 2)

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname hub_2
!
crypto isakmp policy 1
  encr aes 256
  hash sha256
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 0.0.0.0
!
crypto ipsec transform-set transform-dmvpn esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile profile-dmvpn
 set transform-set transform-dmvpn
!
crypto ipsec profile profile-dmvpn-1
 set transform-set transform-dmvpn
!
interface Loopback0
 ip address 172.18.0.5 255.255.255.252
!
interface Loopback1
 ip address 192.168.16.1 255.255.255.0
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.16 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp network-id 100000
 ip nhrp holdtime 360
 ip nhrp nhs 10.0.0.1 nbma 172.17.0.9 multicast
 ip nhrp shortcut
 ip nhrp redirect
 ip summary-address eigrp 1 192.168.16.0 255.255.248.0
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile profile-dmvpn
!
interface Tunnel2
 bandwidth 1000
 ip address 10.0.2.16 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 360
 ip nhrp redirect
```

```
 ip summary-address eigrp 1 192.168.16.0 255.255.248.0
 ip summary-address eigrp 1 192.168.100.0 255.255.252.0
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile profile-dmvpn-1
!
interface Ethernet0/0
 ip address 172.17.0.5 255.255.255.252
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 10.0.2.0 0.0.0.255
 network 192.168.16.0
!
ip route 0.0.0.0 0.0.0.0 172.17.0.6
!
end
```

Spoke da região 1 (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
```

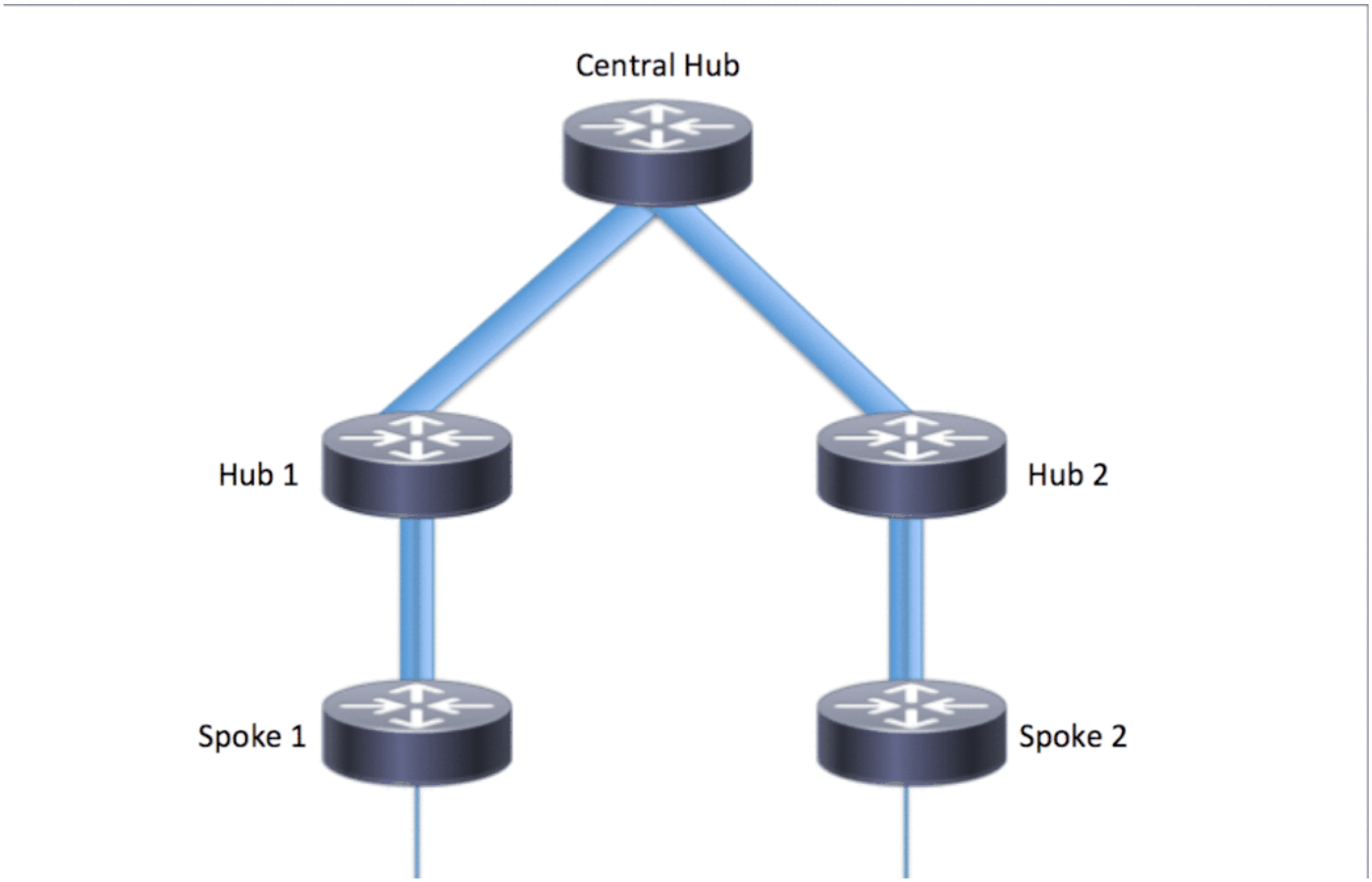
Spoke da região 2 (Spoke 2)

```
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
```

Entendendo o fluxo de pacotes de dados e NHRP

Esta imagem mostra o primeiro fluxo de pacote de dados seguido pelo fluxo de solicitação e resposta de resolução NHRP:



Primeiro fluxo de pacote de dados

Etapa 1. Ping ICMP iniciado do spoke 1, destino = 192.168.18.10, origem = 192.168.11.1

1. A pesquisa de rota é feita para 192.168.18.10. Como visto abaixo, o próximo salto é

10.0.1.8 (endereço de túnel do Hub 1)

2. A pesquisa de cache do NHRP é feita para o destino 192.168.18.10 no Tunnel0, no entanto, nenhuma entrada é encontrada nesse estágio.
3. A pesquisa de cache do NHRP é feita para o próximo salto, ou seja, 10.0.1.8 no Tunnel0. Como visto abaixo, a entrada está presente e a sessão de criptografia está ATIVA.
4. O pacote de solicitação de eco ICMP é encaminhado para o próximo salto, ou seja, Hub1 pelo túnel existente.

<#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
```

Etapa 2. Pacote ICMP recebido no Hub 1

1. A pesquisa de rota é feita para 192.168.18.10. O próximo salto é 10.0.0.1 (endereço de túnel do Hub 0).
2. Como o Hub1 não é o ponto de saída e o pacote precisa ser encaminhado para outra interface dentro da mesma nuvem DMVPN, o Hub 1 envia um redirecionamento/indireção NHRP para Spoke 1.
3. Ao mesmo tempo, o pacote de dados é encaminhado ao 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
```

Etapa 3. Pacote ICMP recebido no Hub 0

1. A pesquisa de rota é feita para 192.168.18.10. O próximo salto é 10.0.0.16 (endereço de túnel do Hub2) no Tunnel0
2. Como o Hub 0 não é o ponto de saída e o pacote precisa ser encaminhado de volta para a mesma nuvem DMVPN através da mesma interface, portanto o Hub 0 envia o NHRP em direção ao Spoke 1 através do Hub 1.
3. O pacote de dados é encaminhado para o Hub 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
```

Etapa 4. Pacote ICMP recebido no Hub 2

1. A pesquisa de rota é feita para 192.168.18.10. O próximo salto é 10.0.2.18 (endereço de túnel de Spoke2) em Tunnel2
2. Como o Hub 2 não é o ponto de saída e o pacote precisa ser encaminhado para outra interface dentro da mesma nuvem DMVPN, o Hub 2 envia o NHRP em direção ao Spoke 1 através do Hub 0.
3. O pacote de dados é encaminhado para 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
```

Etapa 5. Pacote ICMP recebido no Spoke 2

A pesquisa de rota é feita para 192.168.18.10 e é uma rede conectada localmente. Encaminha a solicitação ICMP ao destino.

Fluxo de Solicitação de Resolução NHRP

Spoke 1

1. A indireção de NHRP enviada pelo Hub 1 para o destino 192.168.18.10 é recebida.
2. Uma entrada de cache NHRP incompleta para 192.168.18.10/32 é inserida.
3. A pesquisa de rota é feita para 192.168.18.10. O próximo salto é 10.0.1.8 (Hub 1) no Tunnel0
4. A pesquisa de cache de NHRP é feita para o próximo salto 10.0.1.8 em Tunnel0. Uma entrada é encontrada e o soquete de criptografia também está ativo (ou seja, o túnel existe)
5. O spoke 1 envia a solicitação de resolução de NHRP para 192.168.18.10/32 ao hub 1 pelo spoke existente para o túnel hub1 regional.

<#root>

```
*Apr 13 19:06:07.596: NHRP:

Receive Traffic Indication via Tunnel0

 vrf 0, packet size: 96
*Apr 13 19:06:07.596:  (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Apr 13 19:06:07.596:      shtl: 4(NSAP), sstl: 0(NSAP)
*Apr 13 19:06:07.596:      pktsz: 96 extoff: 68

*Apr 13 19:06:07.596:  (M) traffic code: redirect(0)


*Apr 13 19:06:07.596:      src NBMA: 172.18.0.1
*Apr 13 19:06:07.596:      src protocol: 10.0.1.8, dst protocol: 192.168.11.1
*Apr 13 19:06:07.596:      Contents of nhrp traffic indication packet:
*Apr 13 19:06:07.596:         45 00 00 64 00 01 00 00 FE 01 1E 3C C0 A8 0B 01
*Apr 13 19:06:07.596:         C0 A8 12 0A 08 00 A1 C8 00 01 00
*Apr 13 19:06:07.596: NHRP: Attempting to create instance PDB for (0x0)
```

<#root>

```
*Apr 13 19:06:07.609: NHRP:

 Send Resolution Request via Tunnel0
```

```
 vrf 0, packet size: 84
*Apr 13 19:06:07.609:  src: 10.0.1.11, dst: 192.168.18.10
*Apr 13 19:06:07.609:  (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Apr 13 19:06:07.609:      shtl: 4(NSAP), sstl: 0(NSAP)
*Apr 13 19:06:07.609:      pktsz: 84 extoff: 52
*Apr 13 19:06:07.609:  (M) flags: "router auth src-stable nat ", reqid: 3
*Apr 13 19:06:07.609:      src NBMA: 172.16.1.1
*Apr 13 19:06:07.609:      src protocol: 10.0.1.11, dst protocol: 192.168.18.10
*Apr 13 19:06:07.609:  (C-1) code: no error(0)
*Apr 13 19:06:07.609:        prefix: 32, mtu: 17912, hd_time: 7200
*Apr 13 19:06:07.609:        addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
```

Hub 1

1. A solicitação de resolução NHRP do spoke 1 para o destino 192.168.18.1/32 é recebida.
2. A pesquisa de rota é feita para 192.168.18.1. O próximo salto é 10.0.0.1 (Hub 0) no Tunnel0
3. A ID de rede NHRP para entrada e saída é a mesma e o nó local não é o ponto de saída.
4. A pesquisa de cache do NHRP é feita para o próximo salto 10.0.0.1 no Tunnel0, a entrada é encontrada e o soquete de criptografia está ativo (o túnel existe)
5. O Hub1 encaminha a solicitação de resolução NHRP para 192.168.18.10/32 para o Hub 0 pelo túnel existente

<#root>

```
*Apr 13 19:06:07.610: NHRP:

Receive Resolution Request via Tunnel1

 vrf 0, packet size: 84
*Apr 13 19:06:07.610:  (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Apr 13 19:06:07.610:      shtl: 4(NSAP), sstl: 0(NSAP)
*Apr 13 19:06:07.610:      pktsz: 84 extoff: 52
*Apr 13 19:06:07.610:  (M) flags: "router auth src-stable nat ", reqid: 3
*Apr 13 19:06:07.610:      src NBMA: 172.16.1.1
*Apr 13 19:06:07.610:      src protocol: 10.0.1.11, dst protocol: 192.168.18.10
*Apr 13 19:06:07.610:  (C-1) code: no error(0)
*Apr 13 19:06:07.610:        prefix: 32, mtu: 17912, hd_time: 7200
*Apr 13 19:06:07.610:        addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0

*Apr 13 19:06:07.610: NHRP:

Forwarding Resolution Request via Tunnel0

 vrf 0, packet size: 104
*Apr 13 19:06:07.610:  src: 10.0.0.8, dst: 192.168.18.10
*Apr 13 19:06:07.610:  (F) afn: AF_IP(1), type: IP(800), hop: 254, ver: 1
*Apr 13 19:06:07.610:      shtl: 4(NSAP), sstl: 0(NSAP)
*Apr 13 19:06:07.610:      pktsz: 104 extoff: 52
*Apr 13 19:06:07.610:  (M) flags: "router auth src-stable nat ", reqid: 3
*Apr 13 19:06:07.610:      src NBMA: 172.16.1.1
*Apr 13 19:06:07.610:      src protocol: 10.0.1.11, dst protocol: 192.168.18.10
*Apr 13 19:06:07.610:  (C-1) code: no error(0)
*Apr 13 19:06:07.610:        prefix: 32, mtu: 17912, hd_time: 7200
*Apr 13 19:06:07.610:        addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
```

Hub 0

1. A solicitação de resolução NHRP é recebida para o destino 192.168.18.1/32, encaminhada pelo Hub 1.
2. A pesquisa de rota é feita para 192.168.18.1. O próximo salto é 10.0.0.16 (Hub 2) no Tunnel0
3. A ID de rede NHRP para entrada e saída é a mesma e o nó local não é o ponto de saída.
4. A pesquisa de cache do NHRP é feita para o próximo salto 10.0.0.16 no Tunnel0, a entrada é encontrada e o soquete de criptografia está ativo (o túnel existe)
5. O hub 0 encaminha a solicitação de resolução NHRP para 192.168.18.1/32 para o hub 2 pelo túnel existente.

<#root>

```
*Apr 13 19:06:07.611: NHRP:

Receive Resolution Request via Tunnel0

 vrf 0, packet size: 104
*Apr 13 19:06:07.611:  (F) afn: AF_IP(1), type: IP(800), hop: 254, ver: 1
*Apr 13 19:06:07.611:      shtl: 4(NSAP), sstl: 0(NSAP)
*Apr 13 19:06:07.611:      pktsz: 104 extoff: 52
*Apr 13 19:06:07.611:  (M) flags: "router auth src-stable nat ", reqid: 3
*Apr 13 19:06:07.611:      src NBMA: 172.16.1.1
*Apr 13 19:06:07.611:      src protocol: 10.0.1.11, dst protocol: 192.168.18.10
*Apr 13 19:06:07.611:  (C-1) code: no error(0)
*Apr 13 19:06:07.611:        prefix: 32, mtu: 17912, hd_time: 7200
*Apr 13 19:06:07.611:        addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0

*Apr 13 19:06:07.611: NHRP:

Forwarding Resolution Request via Tunnel0

 vrf 0, packet size: 124
*Apr 13 19:06:07.611:  src: 10.0.0.1, dst: 192.168.18.10
*Apr 13 19:06:07.611:  (F) afn: AF_IP(1), type: IP(800), hop: 253, ver: 1
*Apr 13 19:06:07.611:      shtl: 4(NSAP), sstl: 0(NSAP)
*Apr 13 19:06:07.612:      pktsz: 124 extoff: 52
*Apr 13 19:06:07.612:  (M) flags: "router auth src-stable nat ", reqid: 3
*Apr 13 19:06:07.612:      src NBMA: 172.16.1.1
*Apr 13 19:06:07.612:      src protocol: 10.0.1.11, dst protocol: 192.168.18.10
*Apr 13 19:06:07.612:  (C-1) code: no error(0)
*Apr 13 19:06:07.612:        prefix: 32, mtu: 17912, hd_time: 7200
*Apr 13 19:06:07.612:        addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
```

Hub 2

1. A solicitação de resolução NHRP é recebida do spoke 1 para o destino 192.168.18.10/32, encaminhado pelo hub 0
2. A pesquisa de rota é feita para 192.168.18.10, o próximo salto é 10.0.2.18 (Spoke 2) em Tunnel2
3. A ID de rede NHRP para entrada e saída é a mesma e o nó local não é o ponto de saída.
4. A pesquisa de cache de NHRP é feita para o próximo salto 10.0.2.18 em Tunnel2, a entrada

é encontrada e o soquete de criptografia está ativo (o túnel existe)
5. O hub 2 encaminha a solicitação de resolução de NHRP para 192.168.18.1/32 para Spoke 2 no túnel existente

<#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
```

Spoke 2

1. A solicitação de resolução NHRP é recebida para o destino 192.168.18.1/32, encaminhada pelo Hub 2
2. A pesquisa de rota é feita para 192.168.18.10, que é uma rede conectada localmente.
3. Spoke 2 é o ponto de saída e gera a resposta de resolução para 192.168.18.10, prefixo /24
4. Spoke 2 insere a entrada de cache NHRP para 10.0.1.11 (Spoke 1) usando informações da solicitação de resolução NHRP.
5. Spoke 2 inicia o túnel VPN com o ponto final remoto = endereço NBMA de Spoke 1. O túnel spoke dinâmico é negociado.
6. O spoke 2 envia a resposta de resolução NHRP para 192.168.18.10/24 para o spoke 1 pelo túnel dinâmico que acabou de ser criado.

<#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
```

Spoke1

1. A resposta de resolução NHRP é recebida do spoke 2 para o destino 192.168.18.10, prefixo /24 sobre o túnel dinâmico.
2. A entrada de cache NHRP para 192.168.18.0/24 agora é atualizada com o próximo salto = 10.0.2.18, NBMA = 172.16.2.1
3. Uma rota NHRP é adicionada ao RIB para a rede 192.168.18.10, próximo salto = 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
```

Verificar

> Observação: O Cisco CLI Analyzer (apenas para clientes registrados) suporta determinados comandos show. Use o Cisco CLI Analyzer para visualizar uma análise da saída do comando show.

Antes da construção do túnel spoke-spoke, isto é, a entrada de atalho NHRP é formada

<#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#
```

Depois que o túnel dinâmico spoke-spoke é formado, ou seja, a entrada de atalho NHRP é formada

<#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:
```

Motivo da entrada de cache NHRP local (sem soquete) vista acima

Sinalizador Local refere-se às entradas de mapeamento NHRP que são para redes locais para este roteador (atendidas por este roteador). Essas entradas são criadas quando esse roteador responde a uma solicitação de resolução NHRP com essas informações e são usadas para armazenar o endereço IP do túnel de todos os outros nós NHRP para os quais ele enviou essas informações. Se, por algum motivo, esse roteador perder acesso a essa rede local (ele não pode mais atender a essa rede), ele enviará uma mensagem de limpeza de NHRP a todos os nós NHRP remotos listados na entrada 'local' (show ip nhrp detail) para instruir os nós remotos a apagar essas informações de suas tabelas de mapeamento de NHRP.

Nenhum soquete é visto para entradas de mapeamento NHRP para as quais não precisamos nem queremos disparar o IPsec para configurar a criptografia.

<#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
```

Troubleshooting

Esta seção fornece as informações que você pode usar para solucionar problemas da sua configuração.

> Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

A solução de problemas de DMVPN envolve a solução de problemas em 4 camadas nesta ordem:

1. Camada de roteamento física (NBMA ou ponto final de túnel)
2. camada de Criptografia IPsec
3. Camada de encapsulamento GRE
4. camada de protocolos de roteamento dinâmico

Antes da solução de problemas, é melhor executar estes comandos:

<#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
```

Camada de roteamento física (NBMA ou ponto final de túnel)

Verifique se você pode fazer ping do hub para o endereço NBMA do spoke e do spoke para o endereço NBMA do hub (da saída de show ip nhrp no spoke). Esses pings devem seguir diretamente para fora da interface física e não pelo túnel DMVPN. Se isso não funcionar, você precisará verificar o roteamento e todos os firewalls entre os roteadores hub e spoke.

Camada de criptografia IPSec

Execute os seguintes comandos para verificar as SAs ISAKMP e as SAs IPsec entre os endereços NBMA do hub e do spoke.

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

Essas depurações podem ser ativadas para solucionar problemas da camada de criptografia IPSec:

<#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

O spoke envia solicitações de registro de NHRP regularmente, a cada 1/3 do valor de tempo de espera de NHRP (no spoke) ou do valor de tempo limite de registro de nhRP de ip <segundos>. Você pode verificar isso no spoke executando:

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

Use os comandos acima para verificar se o spoke está enviando solicitações de registro de NHRP e obtendo respostas do hub.

Para verificar se o hub tem a entrada de mapeamento NHRP para o spoke no cache NHRP no hub, execute este comando:

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

Para solucionar problemas relacionados ao NHRP, estas depurações podem ser usadas:

<#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
```

Camada de protocolos de roteamento dinâmico

Consulte estes documentos dependendo do protocolo de roteamento dinâmico que está sendo usado:

- Troubleshooting de EIGRP
- Troubleshooting de OSPF
- Troubleshooting de BGP

Informações Relacionadas

- Soluções de problemas DMVPN mais comuns
- Rastreamento de eventos DMVPN
- Switching de atalho NHRP aprimorado
- Migração da VPN multiponto dinâmica Fase 2 para Fase 3
- Cisco Feature Navigator
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.