Configuración de la DMVPN jerárquica de fase 3 con radios de varias subredes

Contenido

Introducción

Este documento proporciona información sobre cómo configurar una VPN multipunto dinámica jerárquica (DMVPN) de fase 3 con radios de subred múltiple.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de DMVPN
- Conocimientos básicos sobre el protocolo de routing de gateway interior mejorado (EIGRP)

Nota: Para DMVPN jerárquica con radios de subred múltiple, asegúrese de que los routers tengan la corrección de errores de CSCug42027. Con los routers que ejecutan la versión de IOS sin la corrección de CSCug42027 , una vez que el túnel spoke a spoke se forma entre los spokes en diferentes subredes, el tráfico spoke a spoke falla.

CSCug42027 se resuelve en las siguientes versiones de IOS e IOS-XE:

- 15.3(3)S / 3.10 y posteriores.
- 15.4(3)M y posteriores.
- 15.4(1)T y posteriores.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- Routers de servicios integrados Cisco 2911 que ejecutan Cisco IOS® versión 15.5(2)T

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

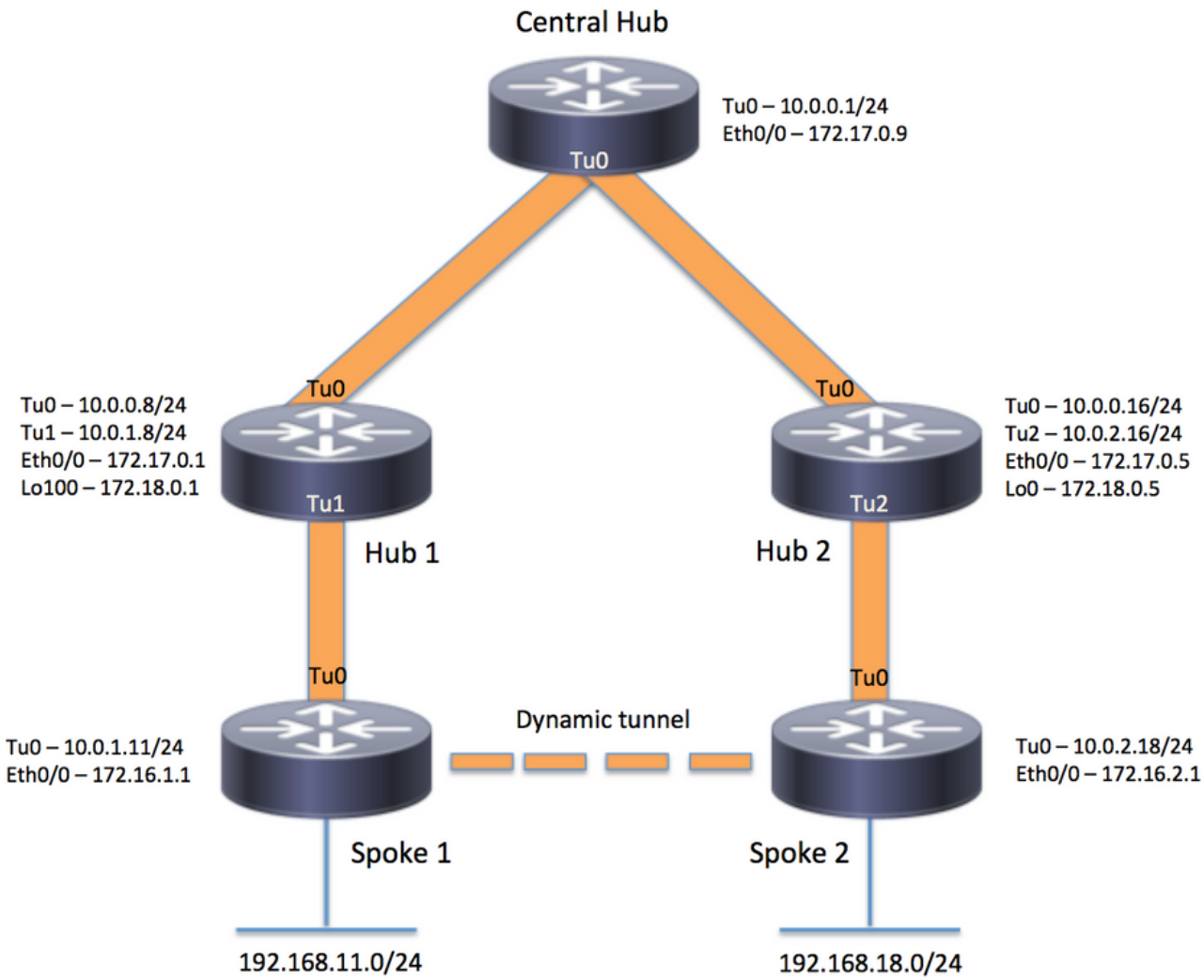
Antecedentes

La configuración jerárquica (de más de un nivel) permite topologías de red DMVPN basadas en árbol más complejas. Las topologías basadas en árbol permiten crear redes DMVPN con hubs regionales que son spokes de hubs centrales. Esta arquitectura permite que el hub regional gestione los datos y el tráfico de control del protocolo de resolución de próximo salto (NHRP) para sus radios regionales. Sin embargo, todavía permite que se construyan túneles de radio a radio entre cualquier radio dentro de la red DMVPN, estén o no en la misma región. Esta arquitectura también permite que el diseño de la red DMVPN coincida más estrechamente con los patrones de flujo de datos regionales o jerárquicos.

Configurar

En esta sección se ofrece información para configurar las funciones descritas en este documento.

Diagrama de la red



Configuraciones

Nota: En este ejemplo sólo se incluyen las secciones relevantes de la configuración.

Concentrador 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 de la región 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
```

Concentrador de la región 2 (Concentrador 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
```

Radio de la región 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
```

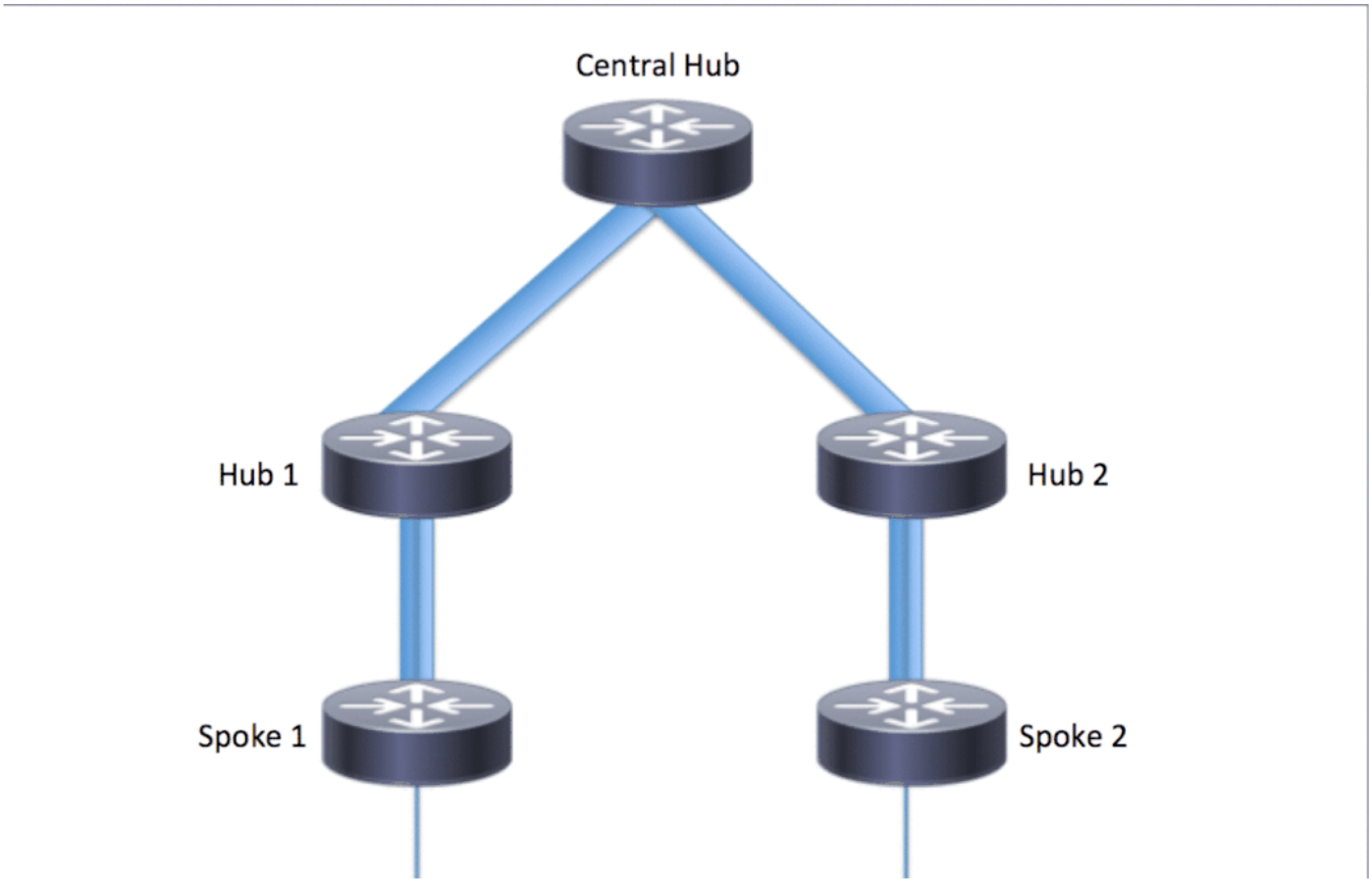
Radio de la región 2 (radio 2)

```
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
```

Introducción al flujo de paquetes de datos y NHRP

Esta imagen muestra el primer flujo de paquetes de datos seguido del flujo de respuesta y solicitud de resolución NHRP:



Primer flujo de paquetes de datos

Paso 1. Ping ICMP iniciado desde spoke 1, destino = 192.168.18.10, origen = 192.168.11.1

1. La búsqueda de rutas se realiza para 192.168.18.10. Como se ve a continuación, el salto

siguiente es 10.0.1.8 (dirección de túnel del Hub 1)

2. La búsqueda de caché NHRP se realiza para el destino 192.168.18.10 en Tunnel0; sin embargo, no se encuentra ninguna entrada en esta etapa.
3. La búsqueda de caché NHRP se realiza para el siguiente salto, es decir, 10.0.1.8 en el túnel0. Como se observa a continuación, la entrada está presente y la sesión de cifrado está ACTIVA.
4. El paquete de solicitud de eco ICMP se reenvía al siguiente salto, es decir, el Hub1 a través del 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
```

Paso 2. Paquete ICMP recibido en el Hub 1

1. La búsqueda de rutas se realiza para 192.168.18.10. El salto siguiente es 10.0.0.1 (dirección de túnel del concentrador 0).
2. Dado que el Hub1 no es el punto de salida y el paquete debe reenviarse a otra interfaz dentro de la misma nube DMVPN, el Hub 1 envía una indirección/redirección NHRP al Spoke 1.
3. Al mismo tiempo, el paquete de datos se reenvía al 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
```

Paso 3. Paquete ICMP recibido en el concentrador 0

1. La búsqueda de rutas se realiza para 192.168.18.10. El siguiente salto es 10.0.0.16 (dirección de túnel del Hub2) en el Túnel0
2. Dado que el concentrador 0 no es el punto de salida y el paquete debe reenviarse de nuevo a la misma nube DMVPN a través de la misma interfaz, por lo tanto, el concentrador 0 envía la indirección NHRP al spoke 1 a través del concentrador 1.
3. El paquete de datos se reenvía al 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
```

Paso 4. Paquete ICMP recibido en el Hub 2

1. La búsqueda de rutas se realiza para 192.168.18.10. El salto siguiente es 10.0.2.18 (dirección de túnel de Spoke2) en el túnel 2
2. Dado que el concentrador 2 no es el punto de salida y el paquete debe reenviarse a otra interfaz dentro de la misma nube DMVPN, el concentrador 2 envía la indirección NHRP al spoke 1 a través del concentrador 0.
3. El paquete de datos se reenvía a 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
```

Paso 5. Paquete ICMP recibido en Spoke 2

La búsqueda de rutas se realiza para 192.168.18.10 y es una red conectada localmente. Reenvía la solicitud ICMP al destino.

Flujo de solicitud de resolución NHRP

Spoke 1

1. Se recibe la indirección NHRP enviada por el Hub 1 para el destino 192.168.18.10.
2. Se inserta una entrada de caché NHRP incompleta para 192.168.18.10/32.
3. La búsqueda de rutas se realiza para 192.168.18.10. El salto siguiente es 10.0.1.8 (Hub 1) en Tunnel0
4. La búsqueda de caché NHRP se realiza para el salto siguiente 10.0.1.8 en el túnel0. Se encuentra una entrada y el socket criptográfico también está activo (es decir, existe un túnel)
5. El spoke 1 envía la solicitud de resolución NHRP para 192.168.18.10/32 al Hub 1 a través del spoke existente al 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. Se recibe la solicitud de resolución NHRP de Spoke 1 para el destino 192.168.18.1/32.
2. La búsqueda de rutas se realiza para 192.168.18.1. El salto siguiente es 10.0.0.1 (Hub 0) en Tunnel0
3. El ID de red NHRP para entrada y salida es el mismo y el nodo local no es el punto de salida.
4. La búsqueda de caché NHRP se realiza para el siguiente salto 10.0.0.1 en el túnel0, se encuentra la entrada y el socket criptográfico está activo (el túnel existe)
5. El Hub1 reenvía la solicitud de resolución NHRP para 192.168.18.10/32 al Hub 0 a través del 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. La solicitud de resolución NHRP se recibe para el destino 192.168.18.1/32, reenviada por el Hub 1.
2. La búsqueda de rutas se realiza para 192.168.18.1. El salto siguiente es 10.0.0.16 (Hub 2) en Tunnel0
3. El ID de red NHRP para entrada y salida es el mismo y el nodo local no es el punto de salida.
4. La búsqueda de caché NHRP se realiza para el salto siguiente 10.0.0.16 en el túnel0, se encuentra la entrada y el socket criptográfico está activo (el túnel existe)
5. El Hub 0 reenvía la solicitud de resolución NHRP para 192.168.18.1/32 al Hub 2 a través del 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. La solicitud de resolución NHRP se recibe desde Spoke 1 para el destino 192.168.18.10/32,

reenviada por Hub 0

2. La búsqueda de ruta se realiza para 192.168.18.10, el salto siguiente es 10.0.2.18 (Spoke 2) en el túnel 2
3. El ID de red NHRP para entrada y salida es el mismo y el nodo local no es el punto de salida.
4. La búsqueda de caché NHRP se realiza para el salto siguiente 10.0.2.18 en el túnel 2, se encuentra la entrada y el socket criptográfico está activo (el túnel existe)
5. El Hub 2 reenvía la solicitud de resolución NHRP para 192.168.18.1/32 al Spoke 2 a través del 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. La solicitud de resolución NHRP se recibe para el destino 192.168.18.1/32, reenviada por el Hub 2
2. La búsqueda de rutas se realiza para 192.168.18.10, que es una red conectada localmente.
3. Spoke 2 es el punto de salida y genera la respuesta de resolución para 192.168.18.10, prefijo /24
4. Spoke 2 inserta la entrada de caché NHRP para 10.0.1.11 (Spoke 1) utilizando la información de la solicitud de resolución NHRP.
5. El Spoke 2 inicia el túnel VPN con el terminal remoto = dirección NBMA del Spoke 1. Se

negocia el túnel de radio-radio dinámico.

6. Luego Spoke 2 envía la respuesta de resolución NHRP para 192.168.18.10/24 al Spoke 1 a través del túnel dinámico que se acaba de construir.

<#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. La respuesta de resolución NHRP se recibe del Spoke 2 para el destino 192.168.18.10, prefijo /24 sobre el túnel dinámico.
2. La entrada de memoria caché NHRP para 192.168.18.0/24 ahora se actualiza con el salto siguiente = 10.0.2.18, NBMA = 172.16.2.1
3. Se agrega una ruta NHRP en el RIB para la red 192.168.18.10, salto siguiente = 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
```

Verificación

> Nota: El Analizador de Cisco CLI (sólo para clientes registrados) admite ciertos comandos show. Utilice el Analizador de Cisco CLI para ver un análisis de los resultados del comando show.

Antes de que se construya el túnel radio-radio, es decir, se forma la entrada de acceso directo NHRP

<#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#
```

Después de la Formación del Túnel Dinámico Spoke-Spoke, es decir, la Formación de la Entrada de Acceso Directo NHRP

<#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 de la entrada de caché NHRP local (sin socket) vista anteriormente

Indicador local hace referencia a entradas de asignación NHRP que son para redes locales a este router (atendidas por este router). Estas entradas se crean cuando este router responde a una solicitud de resolución NHRP con esta información y se utilizan para almacenar la dirección IP de túnel de todos los otros nodos NHRP a los que ha enviado esta información. Si por alguna razón este router pierde el acceso a esta red local (ya no puede dar servicio a esta red) enviará un mensaje de purga NHRP a todos los nodos NHRP remotos enumerados en la entrada 'local' (show ip nhrp detail) para decirle a los nodos remotos que borren esta información de sus tablas de asignación NHRP.

No se ve ningún socket para las entradas de asignación NHRP para las que no necesitamos ni queremos activar IPsec para configurar el cifrado.

<#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
```

Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos debug.

La resolución de problemas de DMVPN implica la resolución de problemas en 4 capas en este orden:

1. Capa de routing físico (NBMA o extremo de túnel)
2. Nivel de cifrado IPsec
3. Capa de encapsulación GRE
4. Capa Dynamic Routing Protocols

Antes de la localización de averías, es mejor ejecutar estos 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
```

Capa de routing físico (NBMA o extremo de túnel)

Verifique si puede hacer ping desde el hub a la dirección NBMA del spoke y desde el spoke a la dirección NBMA del hub (desde la salida de show ip nhrp en el spoke). Estos pings deben ir directamente a la interfaz física, no a través del túnel de DMVPN. Si esto no funciona, debe verificar el ruteo y cualquier firewall entre los routers hub y spoke.

Capa de cifrado IPSec

Ejecute los siguientes comandos para verificar las SA ISAKMP y las SA IPsec entre las direcciones NBMA del hub y el spoke.

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

Estas depuraciones se pueden habilitar para solucionar problemas de la capa de cifrado 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

El spoke envía solicitudes de registro NHRP de manera regular, cada 1/3 de tiempo de espera NHRP (en spoke) o ip nhrp registration timeout **<**seconds**>** valor. Puede comprobar esto en el spoke ejecutando:

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

Utilice los comandos anteriores para verificar si el spoke está enviando solicitudes de registro NHRP y obteniendo respuestas del hub.

Para verificar si el hub tiene la entrada de mapeo NHRP para el spoke en la memoria caché NHRP en el hub, ejecute este comando:

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

Para resolver problemas relacionados con NHRP, se pueden utilizar estos debugs:

<#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
```

Capa de protocolos de routing dinámico

Consulte estos documentos según el protocolo de ruteo dinámico que se utilice:

- Resolución de problemas de EIGRP
- Resolución de problemas de OSPF (Abrir la ruta más corta en primer lugar)
- Troubleshooting de BGP

Información Relacionada

- Soluciones de problemas de DMVPN más comunes
- Seguimiento de eventos DMVPN
- Switching de acceso directo NHRP mejorado
- Migración de Dynamic Multipoint VPN Phase 2 a Phase 3
- Navegador de funciones de Cisco
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).