La Redundancia de la configuración ISP en un DMVPN habló con la característica de VRF-Lite

Contenido

Introducción

Este documento describe cómo configurar la Redundancia del Proveedor de servicios de Internet (ISP) en un spoke del Dynamic Multipoint VPN (DMVPN) vía la característica del ruteo virtual y de Expedición-Lite (VRF-Lite).

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de estos temas antes de que usted intente la configuración que se describe en este documento:

- Conocimiento básico del VRF

- Conocimiento básico del Enhanced Interior Gateway Routing Protocol (EIGRP)
- Conocimiento básico del DMVPN

Componentes Utilizados

La información en este documento se basa en la versión 15.4(2)T del ® del Cisco IOS.

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). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

El VRF es una tecnología incluida en el Routers de la red del IP que permite que las instancias múltiples de una tabla de ruteo coexistan en un router y que trabajen simultáneamente. Esto aumenta las funciones porque permite que los trayectos de red sean divididos en segmentos sin el uso de los dispositivos múltiples.

El uso de los ISP duales para la Redundancia se ha convertido en una práctica común. Los administradores utilizan dos links ISP; uno actúa como conexión primaria y el otro actúa como conexión de respaldo.

El mismo concepto se puede implementar para la Redundancia DMVPN en un spoke con el uso de los ISP duales. El objetivo de este documento es demostrar cómo VRF-*Lite* se puede utilizar para segregar la tabla de ruteo cuando un spoke tiene ISP duales. El Dynamic Routing se utiliza para proporcionar la redundancia de trayectos para el tráfico que atraviesa el túnel DMVPN. Los ejemplos de configuración que se describen en este uso del documento este esquema de la configuración:

Interfaz	DIRECCIÓN IP	VRF	Descripción
Ethernet0/0	172.16.1.1	ISP 1 VRF	ISP primario
Ethernet0/1	172.16.2.1	ISP 2 VRF	ISP secundario

Con la característica de VRF-Lite, los VPN Routing/Forwarding Instance múltiples se pueden soportar en el spoke DMVPN. La característica de VRF-Lite fuerza el tráfico de las interfaces del túnel de múltiples puntos múltiples del Generic Routing Encapsulation (mGRE) para utilizar sus tablas de ruteo respectivas VRF. Por ejemplo, si el ISP primario termina en el *ISP1* VRF y el ISP secundario termina en el *ISP2* VRF, el tráfico que se genera en el *ISP2* VRF utiliza la tabla de ruteo *ISP2* VRF, mientras que el tráfico que se genera en el *ISP1* VRF utiliza la tabla de ruteo *ISP1* VRF.

Una ventaja que viene con el uso de una *puerta frontal* VRF (fVRF) es sobre todo tallar una tabla de ruteo separada de la tabla de Global Routing (donde existen las interfaces del túnel). La ventaja con el uso de un VRF *interior* (iVRF) es definir un espacio privado para llevar a cabo la

información DMVPN y de la red privada. Ambas configuraciones proporcionan la Seguridad adicional de los ataques en el router de Internet, en donde se separa la información de ruteo.

Estas configuraciones de VRF se pueden utilizar en ambos el hub and spoke DMVPN. Esto da la gran ventaja sobre un escenario en el cual ambos ISP terminen en la tabla de Global Routing.

Si ambos ISP terminan en el VRF global, comparten la misma tabla de ruteo y ambas interfaces del mGRE confían en la información de ruteo global. En este caso, si el ISP primario falla, la interfaz del ISP primario no pudo ir abajo si la punta del error está en la red de estructura básica de los ISP y conectada no no directamente. Esto da lugar a un escenario donde ambas interfaces de túnel MGRE todavía utilizan la ruta predeterminado que señala al ISP primario, que hace la Redundancia DMVPN fallar.

Aunque hay algunas soluciones alternativas que utilizan los acuerdos llanos del servicio del IP (IP SLA) o los scripts integrados del administrador del evento (EEM) para abordar este problema sin VRF-Lite, puede ser que no sean siempre la mejor opción.

Métodos de implementación

Esta sección proporciona las breves descripciones de los túneles del Túnel dividido y del spoke al spoke.

Tunelización dividida

Cuando las subredes o las rutas resumidas específicas son doctas vía una interfaz del mGRE, después se llama *Túnel dividido*. Si la ruta predeterminado es docta vía una interfaz del mGRE, después se llama túnel-*toda*.

El ejemplo de configuración que se proporciona en este documento se basa en el Túnel dividido.

Túneles del spoke al spoke

El ejemplo de configuración que se proporciona en este documento es un buen diseño para el túnel-todo método de implementación (la ruta predeterminado es docta vía la interfaz del mGRE).

El uso de dos fVRFs segrega las tablas de ruteo y se asegura de que los paquetes encapsulados poste-GRE están remitidos al fVRF respectivo, que ayuda a asegurarse de que el túnel del spoke al spoke sube con un ISP activo.

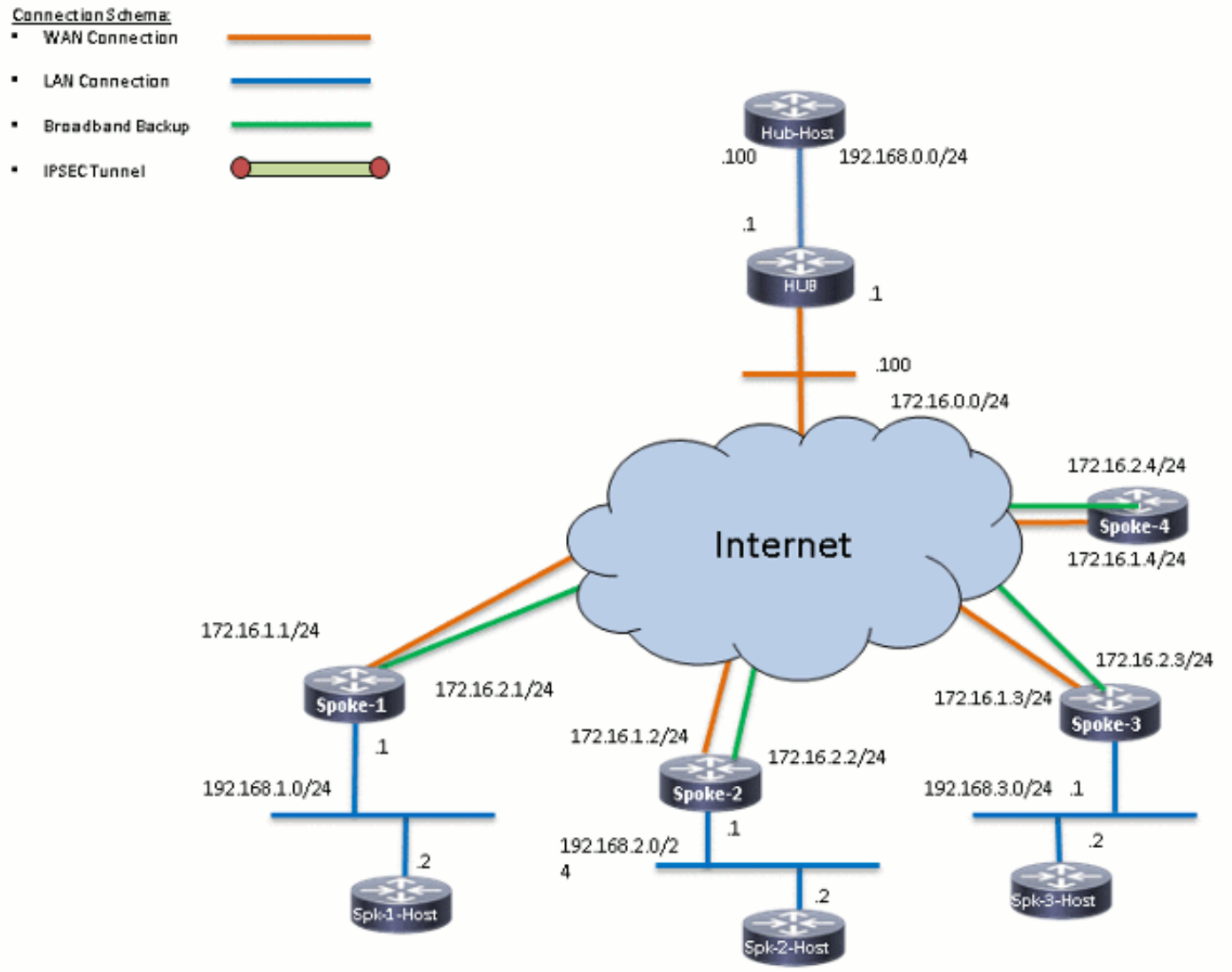
Configurar

Esta sección describe cómo configurar la Redundancia ISP en un spoke DMVPN vía la característica de VRF-Lite.

> Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

Ésta es la topología que se utiliza para los ejemplos dentro de este documento:



Configuración del hub

Aquí están algunas notas sobre la configuración pertinente en el concentrador:

- Para fijar el *tunnel0* como la interfaz primaria en este ejemplo de configuración, se ha cambiado el *parámetro de retraso*, que permite las rutas que son doctas del *tunnel0* preferirse.

- La palabra clave **compartida** se utiliza con la protección del túnel y una *clave del* túnel único se agrega en todas las interfaces del mGRE porque utilizan el mismo *<interface> del origen de túnel*. Si no, los paquetes del túnel entrantes del Generic Routing Encapsulation (GRE) se pudieron llevar en batea a la interfaz del túnel incorrecta después del desciframiento.

- Un resumen de Route se realiza para asegurarse de que todo el spokes aprende la ruta

predeterminado vía los túneles del mGRE (túnel-todos).

Nota: Solamente las secciones pertinentes de la configuración se incluyen en este ejemplo.

```
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HUB1
!
crypto isakmp policy 1
 encr aes 256
 hash sha256
 authentication pre-share
 group 24
crypto isakmp key cisco123 address 0.0.0.0
!
crypto ipsec transform-set transform-dmvpn esp-aes 256 esp-sha256-hmac
 mode transport
!
crypto ipsec profile profile-dmvpn
 set transform-set transform-dmvpn
!
interface Loopback0
 description LAN
 ip address 192.168.0.1 255.255.255.0
!
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 map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 ip nhrp redirect
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile profile-dmvpn shared
!
interface Tunnel1
 bandwidth 1000
 ip address 10.0.1.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 no ip split-horizon eigrp 1
 ip nhrp map multicast dynamic
 ip nhrp network-id 100001
 ip nhrp holdtime 600
 ip nhrp redirect
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0
 ip tcp adjust-mss 1360
 delay 1500
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100001
 tunnel protection ipsec profile profile-dmvpn shared
```

```
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
!
ip route 0.0.0.0 0.0.0.0 172.16.0.100
!
end
```

Configuración radial

Aquí están algunas notas sobre la configuración pertinente en el spoke:

- Para la Redundancia del spoke, el *tunnel0* y *Tunnel1* tienen el *Ethernet0/0* y *Ethernet0/1* como las interfaces del origen de túnel, respectivamente. El Ethernet0/0 está conectado con el ISP primario y Ethernet0/1 está conectado con el ISP secundario.

- Para segregar los ISP, se utiliza la característica VRF. El ISP primario utiliza el *ISP1* VRF. Para el ISP secundario, se configura un VRF *ISP2* nombrado.

- *El vrf ISP1 del túnel* y el *vrf ISP2 del túnel* se configuran en el tunnel0 de las interfaces y Tunnel1, respectivamente, para indicar que la búsqueda de reenvío para el paquete encapsulado poste-GRE está realizada en VRF ISP1 o ISP2.

- Para fijar el tunnel0 como la interfaz primaria en este ejemplo de configuración, se ha cambiado el *parámetro de retraso*, que permite las rutas que son doctas del tunnel0 preferirse.

Nota: Solamente las secciones pertinentes de la configuración se incluyen en este ejemplo.

```
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SPOKE1
!
vrf definition ISP1
 rd 1:1
 !
 address-family ipv4
 exit-address-family
!
vrf definition ISP2
 rd 2:2
 !
 address-family ipv4
 exit-address-family
!
crypto keyring ISP2 vrf ISP2
 pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
crypto keyring ISP1 vrf ISP1
 pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 1
 encr aes 256
```

```
 hash sha256
 authentication pre-share
 group 24
crypto isakmp keepalive 10 periodic
!
crypto ipsec transform-set transform-dmvpn esp-aes 256 esp-sha256-hmac
 mode transport
!
!
crypto ipsec profile profile-dmvpn
 set transform-set transform-dmvpn
!
interface Loopback10
 ip address 192.168.1.1 255.255.255.0
!
interface Tunnel0
 description Primary mGRE interface source as Primary ISP
 bandwidth 1000
 ip address 10.0.0.10 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.0.1 nbma 172.16.0.1 multicast
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel vrf ISP1
 tunnel protection ipsec profile profile-dmvpn
!
interface Tunnel1
 description Secondary mGRE interface source as Secondary ISP
 bandwidth 1000
 ip address 10.0.1.10 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp network-id 100001
 ip nhrp holdtime 360
 ip nhrp nhs 10.0.1.1 nbma 172.16.0.1 multicast
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 delay 1500
 tunnel source Ethernet0/1
 tunnel mode gre multipoint
 tunnel key 100001
 tunnel vrf ISP2
 tunnel protection ipsec profile profile-dmvpn
!
interface Ethernet0/0
 description Primary ISP
 vrf forwarding ISP1
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet0/1
 description Seconday ISP
 vrf forwarding ISP2
 ip address 172.16.2.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
```

```
 network 192.168.0.0 0.0.255.255
!
ip route vrf ISP1 0.0.0.0 0.0.0.0 172.16.1.254
ip route vrf ISP2 0.0.0.0 0.0.0.0 172.16.2.254
!
logging dmvpn
!
end
```

Verificación

Utilice la información que se describe en esta sección para verificar que su configuración trabaja correctamente.

ISP primarios y secundarios activos

En este escenario de la verificación, los ISP primarios y secundarios son activos. Aquí están algunas notas complementarias sobre este escenario:

- La fase 1 y la fase 2 para ambas interfaces del mGRE están para arriba.
- Ambos túneles suben, pero las rutas vía el tunnel0 (originado vía el ISP primario) se prefieren.

Aquí están los **comandos show** relevantes que usted puede utilizar para verificar su configuración en este escenario:

```
SPOKE1#show ip route
<snip>
Gateway of last resort is 10.0.0.1 to network 0.0.0.0

D*    0.0.0.0/0 [90/2944000] via 10.0.0.1, 1w0d, Tunnel0

!--- This is the default route for all of the spoke and hub LAN segments.

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.0/24 is directly connected, Tunnel0
L        10.0.0.10/32 is directly connected, Tunnel0
C        10.0.1.0/24 is directly connected, Tunnel1
L        10.0.1.10/32 is directly connected, Tunnel1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Loopback10
L        192.168.1.1/32 is directly connected, Loopback10

SPOKE1#show ip route vrf ISP1

Routing Table: ISP1
<snip>

Gateway of last resort is 172.16.1.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.1.254
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Ethernet0/0
L        172.16.1.1/32 is directly connected, Ethernet0/0

SPOKE1#show ip route vrf ISP2
```

```
Routing Table: ISP2
<snip>

Gateway of last resort is 172.16.2.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.2.254
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.2.0/24 is directly connected, Ethernet0/1
L        172.16.2.1/32 is directly connected, Ethernet0/1

SPOKE1#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.

 IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.2.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.

 IPSEC FLOW: permit 47 host 172.16.2.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map
```

ISP primario abajo/Active secundario ISP

En este escenario, los temporizadores del *asimiento del* EIGRP expiran para la vecindad con el tunnel0 cuando va el link ISP1 abajo, y las rutas al concentrador y el otro spokes ahora señalan a Tunnel1 (originado con Ethernet0/1).

Aquí están los **comandos show** relevantes que usted puede utilizar para verificar su configuración en este escenario:

```
*Sep  2 14:07:33.374: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is down: holding time expired

SPOKE1#show ip route
<snip>

Gateway of last resort is 10.0.1.1 to network 0.0.0.0

D*    0.0.0.0/0 [90/3072000] via 10.0.1.1, 00:00:20, Tunnel1

!--- This is the default route for all of the spoke and hub LAN segments.

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.0/24 is directly connected, Tunnel0
L        10.0.0.10/32 is directly connected, Tunnel0
C        10.0.1.0/24 is directly connected, Tunnel1
```

```
L        10.0.1.10/32 is directly connected, Tunnel1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Loopback10
L        192.168.1.1/32 is directly connected, Loopback10

SPOKE1#show ip route vrf ISP1

Routing Table: ISP1
<snip>

Gateway of last resort is 172.16.1.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.1.254
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Ethernet0/0
L        172.16.1.1/32 is directly connected, Ethernet0/0

SPOKE1#show ip route vrf ISP2

Routing Table: ISP2
<snip>

Gateway of last resort is 172.16.2.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.2.254
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.2.0/24 is directly connected, Ethernet0/1
L        172.16.2.1/32 is directly connected, Ethernet0/1

SPOKE1#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: DOWN
Peer: 172.16.0.1 port 500
 IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.0.1

!--- Tunnel0 is Inactive and the routes are preferred via Tunnel1.

       Active SAs: 0, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.2.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Inactive and the routes are preferred via Tunnel1.

 IPSEC FLOW: permit 47 host 172.16.2.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map

Interface: Tunnel0
Session status: DOWN-NEGOTIATING
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Inactive

!--- Tunnel0 is Inactive and the routes are preferred via Tunnel1.

 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Inactive
```

Restauración del link del ISP primario

Cuando la Conectividad con el ISP primario se restablece, la sesión de criptografía del tunnel0 hace activa, y se prefieren las rutas que son doctas vía la interfaz del tunnel0.

Aquí tiene un ejemplo:

```
*Sep  2 14:15:59.128: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is up: new adjacency

SPOKE1#show ip route
<snip>

Gateway of last resort is 10.0.0.1 to network 0.0.0.0

D*    0.0.0.0/0 [90/2944000] via 10.0.0.1, 00:00:45, Tunnel0

!--- This is the default route for all of the spoke and hub LAN segments.

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.0/24 is directly connected, Tunnel0
L        10.0.0.10/32 is directly connected, Tunnel0
C        10.0.1.0/24 is directly connected, Tunnel1
L        10.0.1.10/32 is directly connected, Tunnel1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Loopback10
L        192.168.1.1/32 is directly connected, Loopback10

SPOKE1#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.

 IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.2.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.

 IPSEC FLOW: permit 47 host 172.16.2.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map
```

Troubleshooting

Para resolver problemas su configuración, **eigrp del IP del debug del** permiso y **dmvpn del registro**.

Aquí tiene un ejemplo:

```
################## Tunnel0 Failed and Tunnel1 routes installed ###################

*Sep  2 14:07:33.374: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is down: holding time expired
*Sep  2 14:07:33.374: EIGRP-IPv4(1): table(default): route installed for 0.0.0.0/0
(90/3072000) origin(10.0.1.1)
*Sep  2 14:07:33.391: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel1
*Sep  2 14:07:33.399: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel1
*Sep  2 14:07:36.686: %DMVPN-5-CRYPTO_SS:  Tunnel0: local address : 172.16.1.1 remote
address : 172.16.0.1 socket is DOWN
*Sep  2 14:07:36.686: %DMVPN-5-NHRP_NHS_DOWN: Tunnel0: Next Hop Server : (Tunnel:
10.0.0.1 NBMA: 172.16.0.1 ) for (Tunnel: 10.0.0.10 NBMA: 172.16.1.1) is DOWN, Reason:
External(NHRP: no error)

################## Tunnel0 came up and routes via Tunnel0 installed #################

*Sep  2 14:15:55.120: %DMVPN-5-CRYPTO_SS:  Tunnel0: local address : 172.16.1.1 remote
address : 172.16.0.1 socket is UP
*Sep  2 14:15:56.109: %DMVPN-5-NHRP_NHS_UP: Tunnel0: Next Hop Server : (Tunnel:
10.0.0.1 NBMA: 172.16.0.1) for (Tunnel: 10.0.0.10 NBMA: 172.16.1.1) is  UP
*Sep  2 14:15:59.128: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is up: new adjacency
*Sep  2 14:16:01.197: EIGRP-IPv4(1): table(default): route installed for 0.0.0.0/0
(90/3072000) origin(10.0.1.1)
*Sep  2 14:16:01.197: EIGRP-IPv4(1): table(default): route installed for 0.0.0.0/0
(90/2944000) origin(10.0.0.1)
*Sep  2 14:16:01.214: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel0
*Sep  2 14:16:01.214: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel1
```

Información Relacionada

- La mayoría de las soluciones comunes del troubleshooting DMVPN
- Guía de Troubleshooting de la familia del Cisco MDS 9000, IPSec del troubleshooting del del Â del âÂ de la versión 2.x
- Soporte Técnico y Documentación - Cisco Systems