Configuración de la Redundancia ISP en un Radio DMVPN con la Función VRF-Lite

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Métodos de implementación
Tunelización dividida
Túneles de Spoke a Spoke
Configurar
Diagrama de la red
Configuración del hub
Configuración de Spoke
Verificación
ISP primario y secundario activo
ISP primario inactivo/ISP secundario activo
Restauración del link ISP principal
Troubleshoot
Información Relacionada

Introducción

Este documento describe cómo configurar la redundancia del proveedor de servicios de Internet (ISP) en un spoke de VPN multipunto dinámica (DMVPN) a través de la función Virtual Routing and Forwarding-Lite (VRF-Lite).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de estos temas antes de intentar la configuración que se describe en este documento:

- Conocimiento básico de VRF

- Conocimiento básico del protocolo de routing de gateway interior mejorado (EIGRP)
- Conocimiento básico de DMVPN

Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

El VRF es una tecnología incluida en los routers de red IP que permite que varias instancias de una tabla de ruteo coexistan en un router y funcionen simultáneamente. Esto aumenta la funcionalidad porque permite segmentar las rutas de red sin el uso de varios dispositivos.

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

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

Interfaz	IP Address	VRF	Descripción
Ethernet0/0	172.16.1.1	VRF ISP1	ISP principal
Ethernet0/1	172.16.2.1	VRF ISP2	ISP secundario

Con la función VRF-Lite, se pueden admitir varias instancias de ruteo/reenvío de VPN en el radio DMVPN. La función VRF-Lite obliga al tráfico de varias interfaces de túnel de encapsulación de routing genérico multipunto (mGRE) a utilizar sus respectivas tablas de routing VRF. Por ejemplo, si el ISP primario termina en el VRF ISP1 y el ISP secundario termina en el VRF ISP2, el tráfico que se genera en el VRF ISP2 utiliza la tabla de ruteo *ISP2* VRF, mientras que el tráfico que se genera en el *ISP1* VRF utiliza la tabla de ruteo de VRF.

Una ventaja que viene con el uso de un VRF *de puerta delantera* (fVRF) es principalmente crear una tabla de ruteo independiente de la tabla de ruteo global (donde existen interfaces de túnel). La ventaja con el uso de un VRF *interno* (iVRF) es definir un espacio privado para conservar la DMVPN y la información de red privada. Ambas configuraciones proporcionan seguridad adicional de los ataques en el router desde Internet, donde se separa la información de ruteo.

Estas configuraciones VRF se pueden utilizar tanto en el hub DMVPN como en el spoke. Esto ofrece una gran ventaja sobre un escenario en el que ambos ISP terminan en la tabla de ruteo

global.

Si ambos ISP terminan en el VRF global, comparten la misma tabla de ruteo y ambas interfaces mGRE dependen de la información de ruteo global. En este caso, si falla el ISP primario, es posible que la interfaz ISP primaria no se desactive si el punto de falla está en la red de estructura básica de los ISP y no está conectada directamente. Esto da como resultado un escenario donde ambas interfaces de túnel mGRE todavía utilizan la ruta predeterminada que apunta al ISP primario, lo que hace que la redundancia DMVPN falle.

Aunque hay algunas soluciones alternativas que utilizan los scripts IP Service Level Agreement (IP SLA) o Embedded Event Manager (EEM) para solucionar este problema sin VRF-Lite, es posible que no siempre sean la mejor opción.

Métodos de implementación

Esta sección proporciona descripciones generales breves de túneles divididos y de radio a radio.

Tunelización dividida

Cuando se aprenden subredes específicas o rutas resumidas a través de una interfaz mGRE, se denomina *tunelización dividida*. Si la ruta predeterminada se aprende a través de una interfaz mGRE, entonces se denomina *tunnel-all*.

El ejemplo de configuración que se proporciona en este documento se basa en la tunelización dividida.

Túneles de Spoke a Spoke

El ejemplo de configuración que se proporciona en este documento es un buen diseño para el método de implementación tunnel-all (la ruta predeterminada se aprende a través de la interfaz mGRE).

El uso de dos fVRF separa las tablas de ruteo y asegura que los paquetes encapsulados post-GRE se reenvíen al fVRF respectivo, lo que ayuda a asegurar que el túnel de spoke a spoke aparezca con un ISP activo.

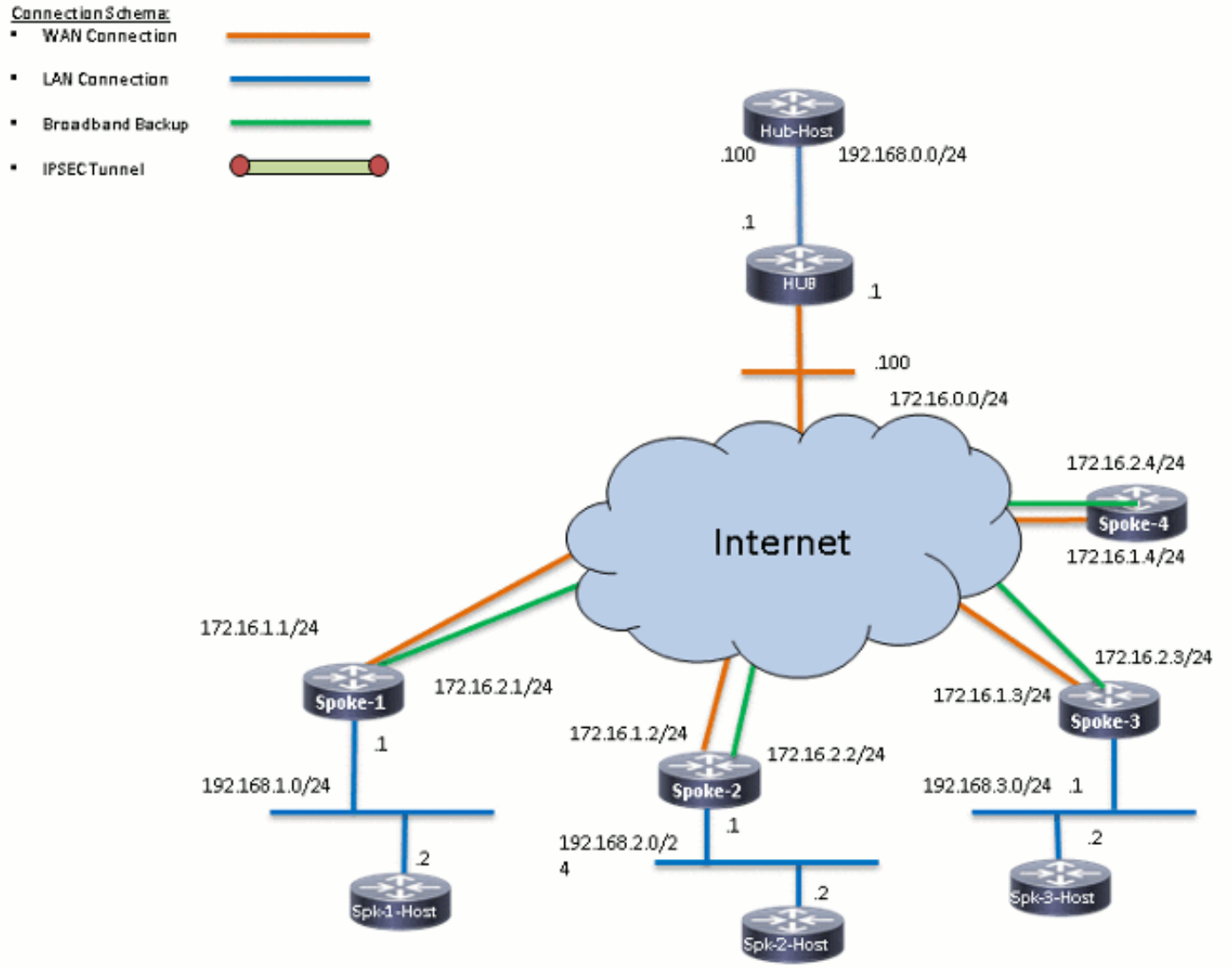
Configurar

Esta sección describe cómo configurar la redundancia ISP en un radio DMVPN a través de la función 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

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



Configuración del hub

A continuación se muestran algunas notas sobre la configuración relevante en el hub:

- Para configurar *Tunnel0* como la interfaz principal en este ejemplo de configuración, se ha cambiado el parámetro *delay*, lo que permite que las rutas aprendidas del *Túnel0* se vuelvan más preferidas.

- La palabra clave **shared** se utiliza con la protección del túnel y se agrega una *clave de túnel* única en todas las interfaces mGRE porque utilizan la misma *fuente de túnel <interface>*. De lo contrario, los paquetes de túnel de encapsulación de routing genérico (GRE) entrantes podrían enviarse a la interfaz de túnel incorrecta después del descifrado.

- Se realiza un resumen de ruta para asegurarse de que todos los radios aprendan la ruta predeterminada a través de los túneles mGRE (**tunnel-all**).

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

```
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 de Spoke

A continuación se muestran algunas notas sobre la configuración relevante en el spoke:

- Para la redundancia de radio, *Tunnel0* y *Tunnel1* tienen *Ethernet0/0* y *Ethernet0/1* como interfaces de origen de túnel, respectivamente. Ethernet0/0 está conectado al ISP primario y Ethernet0/1 está conectado al ISP secundario.
- Para separar los ISP, se utiliza la función VRF. El ISP primario utiliza el VRF *ISP1*. Para el ISP secundario, se configura un VRF denominado *ISP2*.
- El *tunnel vrf ISP1* y el *tunnel vrf ISP2* se configuran en las interfaces Tunnel0 y Tunnel1, respectivamente, para indicar que la búsqueda de reenvío del paquete encapsulado post-GRE se realiza en VRF ISP1 o ISP2.
- Para configurar Tunnel0 como la interfaz principal en este ejemplo de configuración, el parámetro *delay* se ha cambiado, lo que permite que las rutas aprendidas del Tunnel0 se vuelvan más preferidas.

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

```
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 funcione correctamente.

ISP primario y secundario activo

En este escenario de verificación, los ISP primarios y secundarios están activos. A continuación se muestran algunas notas adicionales sobre este escenario:

- La fase 1 y la fase 2 para ambas interfaces mGRE están activas.
- Ambos túneles se activan, pero se prefieren las rutas a través del túnel0 (que se originan a través del ISP primario).

Estos son los comandos **show** relevantes que 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 inactivo/ISP secundario activo

En esta situación, los temporizadores *en espera* EIGRP caducan para la vecindad a través del túnel0 cuando el link ISP1 se desactiva, y las rutas al hub y los otros radios apuntan ahora al túnel1 (originado con Ethernet0/1).

Estos son los comandos **show** relevantes que 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 ISP principal

Cuando se restaura la conectividad a través del ISP primario, la sesión crypto Tunnel0 se activa y se prefieren las rutas aprendidas a través de la interfaz 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
```

Troubleshoot

Para resolver problemas de su configuración, habilite **debug ip eigrp** y **logging dmvpn**.

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

- Soluciones de problemas de DMVPN más comunes
- Guía de solución de problemas de la familia Cisco MDS 9000, versión 2.x, Â resolución de problemas de IPsec
- Soporte Técnico y Documentación - Cisco Systems