VPN IPSec de multipunto dinámico (Uso de NHRP/GRE multipunto para escalar a VPN IPSec)

Contenido

Introducción

Este documento explica el Ipsec VPN de multipunto dinámico (DMVPN) y porqué una compañía podría querer diseñar o migrar su red para usar esta nueva solución de IPsec VPN en Cisco IOS® Software.

Antecedentes

Es posible que las empresas necesiten interconectar muchos sitios a un sitio principal y quizá también entre sí a través de Internet, a la vez que cifran el tráfico para protegerlo. Por ejemplo, es probable que un grupo de tiendas minoristas que necesitan conectarse con la oficina central de la compañía por cuestiones de inventario y órdenes, también necesite conectarse con otras tiendas de la compañía para verificar la disponibilidad de los productos. En el pasado, la única forma de efectuar la conexión fue mediante una red de capa 2, como por ejemplo: ISDN o Fram Relay para interconectar todo. Configurar y pagar por estos links de cableado directo de tráfico IP interno puede ser lento y costoso. Si todos los sitios (incluso el sitio principal) ya cuentan con acceso a Internet relativamente económico, este acceso puede usarse asimismo para la comunicación interna por IP entre las tiendas y oficinas principales a través de túneles IPsec con el objeto de asegurar la privacidad y la integridad de los datos.

A fin de que las compañías creen extensas redes IPsec que interconecten sus sitios por Internet, debe ser posible ampliar la red IPsec. IPsec encripta el tráfico entre dos puntos finales (pares) y los dos puntos finales realizan el encripción utilizando un “secreto” compartido. Como el secreto es compartido sólo entre estos dos puntos finales, las redes cifradas son intrínsecamente una colección de links punto a punto. Debido a esto, esencialmente, IPsec es una red de túneles punto a punto. El método más factible para escalar una gran red punto a punto es organizarla dentro de una red hub y spoke o de una red de interconexión completa (parcial). En casi todas las redes, la mayoría del tráfico IP se realiza entre los spokes y el hub y sólo una pequeña parte entre los spokes, por lo que el diseño hub y spoke es a menudo la mejor opción. Este diseño también es compatible con las anteriores redes Frame Relay ya que era extremadamente costoso pagar por los links entre todos los sitios en estas redes.

Al utilizar Internet como interconexión entre el hub y los spokes, los spokes también tienen acceso directo entre sí sin costo adicional, pero ha sido muy difícil, si no imposible, configurar y/o administrar una red de malla completa (parcial). A veces se prefieren las redes de interconexión completas o parciales ya que puede haber un ahorro de costos si el tráfico de radio a radio se transmite de manera directa en lugar de a través del concentrador. El tráfico de radio a radio que atraviesa el hub utiliza los recursos del hub y puede generar retrasos adicionales, especialmente cuando se utiliza el cifrado IPsec, ya que el hub necesitará descifrar los paquetes entrantes de los spokes de envío y luego volver a cifrar el tráfico para enviarlo al spoke de recepción. Otro ejemplo en el que el tráfico directo de radio a radio podría resultar útil es el caso en el que dos radios están en la misma ciudad y el eje de conexión se encuentra en otra parte del país.

A medida que se implementaron y crecieron el tamaño de las redes hub y spoke IPsec, se hizo más deseable que enrutaran paquetes IP de la manera más dinámica posible. En las redes radiales más antiguas de Frame Relay, esto se logró ejecutando un protocolo de ruteo dinámico como OSPF o EIGRP sobre los links de Frame Relay. Esto fue útil para anunciar de forma dinámica el alcance de las redes spoke y también para admitir la redundancia en la red de IP Routing. Si la red perdió un router hub, puede tomar el mando un router hub de respaldo en forma automática para retener la conectividad de la red con redes spoke.

Hay un problema fundamental con los túneles IPsec y los protocolos de ruteo dinámico. Los protocolos de ruteo dinámicos dependen del uso de paquetes de difusión o multidifusión IP, pero IPSec no admite el cifrado de paquetes de multidifusión o difusión. El método actual para la resolución de este problema es usar los túneles de encapsulación de ruteo genérica (GRE) junto con el encripción IPSec.

Los túneles GRE admiten el transporte de paquetes de difusión y multidifusión IP al otro extremo

del túnel GRE. El paquete de túnel GRE es un paquete de unidifusión IP, de manera que el paquete GRE puede ser encripción mediante IPsec. En esta situación, GRE realiza el trabajo de tunelización e IPsec realiza la parte de encripción del soporte para la red VPN. Cuando se configuran túneles GRE, las direcciones IP para los puntos finales del túnel (**origen de túnel ...**, **destino de túnel ...**) deben ser conocidas por el otro extremo y deben ser enrutables a través de Internet. Esto significa que el hub y todos los routers radiales en esta red deben tener direcciones IP estáticas no privadas.

Para las conexiones de sitios pequeños a Internet, es habitual que la dirección IP externa de un radio cambie cada vez que se conecta a Internet porque su proveedor de servicios de Internet (ISP) proporciona de forma dinámica la dirección de la interfaz externa (a través del protocolo de configuración dinámica de host (DHCP))) cada vez que el spoke se conecta (línea de suscriptor digital asimétrica (ADSL) y servicios de cable). Esta asignación dinámica de la “dirección externa” del router permite que el ISP suscriba excesivamente el uso de sus espacios de dirección de Internet, ya que no todos los usuarios se conectarán al mismo tiempo. Puede ser mucho más caro abonarle al proveedor para que le asigne una dirección estática al router spoke. La ejecución de un protocolo de ruteo dinámico sobre una VPN IPsec exige el uso de túneles GRE, pero se pierde la opción de tener radios con direcciones de IP asignadas dinámicamente en las interfaces físicas exteriores.

Las restricciones mencionadas y algunas otras se resumen en los cuatro puntos siguientes:

- IPSec utiliza una lista de control de acceso (ACL) para definir qué datos se deben cifrar. Por esto, cada vez que se agrega una nueva (sub)red detrás del router radial o el concentrador, el cliente debe cambiar la ACL en los routers radiales o el concentrador. Si el SP administra el router, el cliente debe notificar al SP a fin de obtener el cambio de la ACL IPsec para que el nuevo tráfico sea encripción.
- Con las grandes redes radiales, el tamaño de la configuración en el router hub puede volverse muy grande, en la medida en que no se pueda utilizar. Por ejemplo, un router de eje de conexión necesitaría hasta 3900 líneas de configuración para soportar 300 routers de radio. Esto es lo suficientemente grande como para que resulte difícil mostrar la configuración y encontrar la sección de la configuración que es pertinente al problema actual que se trata de depurar. Además, esta configuración de tamaño podría ser demasiado extensa para adaptarse a la NVRAM y necesitaría ser almacenada en la memoria flash.
- GRE + IPsec debe conocer la dirección del par de punto final. Las direcciones IP de los radios se conectan directamente a Internet a través de su propio ISP y, con frecuencia, están configuradas de manera que sus direcciones de interfaces externas no sean fijas. Las direcciones IP pueden cambiar cada vez que el sitio se conecta (a través de DHCP).
- Si los radios necesitan comunicarse directamente entre sí a través de la VPN IPsec, entonces la red hub-and-spoke debe convertirse en una malla completa. Dado que no se sabe ya qué radios tendrán que hablar directamente entre sí, se requiere una malla completa, aunque cada radio pueda no tener que hablar directamente con cada otro radio. Además, no es factible configurar IPsec en un router spoke pequeño para que tenga conectividad directa con todos los otros routers spoke en la red; por lo tanto, es posible que los routers radiales necesiten ser routers más potentes.

La solución para DMVPN

La solución DMVPN utiliza Multipunto GRE (mGRE) y Protocolo de resolución de salto siguiente

(NHRP), junto con IPsec y otras mejoras nuevas, para resolver gradualmente los problemas mencionados con anterioridad.

Iniciación automática de encripción de IPsec

Cuando no se utiliza la solución DMVPN, el túnel de cifrado IPsec no se inicia hasta que haya tráfico de datos que requiera el uso de este túnel IPsec. Puede tardar de 1 a 10 segundos en completar el inicio del túnel IPsec y el tráfico de datos se descarta durante este tiempo. Cuando se utiliza GRE con IPsec, la configuración del túnel GRE ya incluye la dirección del par de túnel GRE (**destino de túnel ...**), que también es la dirección del par IPsec. Ambas direcciones están preconfiguradas.

Si utiliza Tunnel Endpoint Discovery (TED) y mapas criptográficos dinámicos en el router hub, puede evitar tener que preconfigurar las direcciones de par IPsec en el hub, pero es necesario enviar y recibir una sonda TED y una respuesta antes de que se pueda iniciar la negociación ISAKMP. Esto no debería ser necesario, ya que al usar GRE las direcciones de los pares de origen y destino se conocen de antemano. Están ya sea en la configuración o resueltos con NHRP (para túneles multipunto GRE).

Con la solución DMVPN, IPSec se activa inmediatamente para los túneles GRE punto a punto y multipunto. Además, no es necesario configurar ninguna ACL de encripción ya que éstas surgirán automáticamente a partir de las direcciones de origen y destino del túnel GRE. Los siguientes comandos se utilizan para definir los parámetros de encripción de IPsec. Observe que no hay ningún **peer configurado ...** o **dirección de coincidencia ...** se requieren porque esta información se deriva directamente del túnel GRE asociado o de las asignaciones NHRP.

```
crypto ipsec profile
```

```
 set transform-set
```

El siguiente comando asocia una interfaz de túnel con el perfil IPsec.

```
interface tunnel
```

```
 ...
 tunnel protection ipsec profile
```

Creación dinámica de túneles para enlaces "Spoke-to-Hub"

No hay información GRE o IPsec sobre un spoke configurada en el router hub en la red DMVPN . El túnel GRE del router radial se configura (mediante comandos NHRP) con información sobre el router hub. Cuando se inicia el router radial, éste inicia el túnel IPSec con el router de eje de conexión de manera automática como se describió anteriormente. Luego utiliza NHRP para informar al concentrador del router de cada dirección IP física actual. Esto es útil por tres motivos:

- Si la dirección IP de la interfaz física del router spoke se asignó en forma dinámica (como sucede, por ejemplo, con ADSL o cablemódem), el router hub no puede configurarse con esta información ya que cada vez que el router spoke se recargue obtendrá una nueva dirección IP de la interfaz física.
- Se acorta y simplifica la configuración del router hub ya que no necesita ninguna información GRE o IPSec acerca de los routers de par. Toda esta información se aprende dinámicamente a través de NHRP.
- Cuando agrega un nuevo router radial a la red DMVPN, no necesita cambiar la configuración en el eje de conexión ni en los routers radiales actuales. El nuevo router spoke se configura con la información del hub y, cuando se inicia, se registra dinámicamente con el router hub. El protocolo de ruteo dinámico propaga la información de ruteo para este spoke al hub. El concentrador distribuye esta nueva información a los otros spokes. También propaga la información de ruteo de los otros radios a este spoke.

Creación dinámica de túneles para el tráfico de radio a radio

Como se dijo antes, actualmente en una red de interconexión, todos los túneles IPsec punto a punto (o IPsec+GRE) deben ser configurados en todos los routers, aún cuando algunos o la mayoría de esos túneles no estén siendo ejecutados o no se los necesite todo el tiempo. Con la solución DMVPN, un router es el hub y todos los demás routers (spokes) se configuran con túneles al hub. Los túneles de radio a eje de conexión están activos continuamente, y los radios no necesitan configurarse para túneles directos a ninguno de los otros radios. En su lugar, cuando un spoke desea transmitir un paquete a otro spoke (como la subred detrás de otro spoke), utiliza NHRP para determinar dinámicamente la dirección de destino requerida del spoke de destino. El router hub actúa como un servidor NHRP y administra este pedido para el spoke fuente. Luego, los dos spokes crean de forma dinámica un túnel IPSec entre ellos (a través de la interfaz mGRE única) y la información se puede transferir directamente. Este túnel dinámico radio a radio será automáticamente desmontado luego de un período de inactividad (configurable).

Soporte de protocolos de ruteo dinámico

La solución DMVPN se basa en túneles GRE que admiten la tunelización de paquetes IP de multidifusión/difusión, por lo que la solución DMVPN también admite protocolos de ruteo dinámicos que se ejecutan en los túneles IPsec+mGRE. Anteriormente, NHRP necesitaba que el usuario configure de manera explícita la correspondencia de difusión/multidifusión para que las direcciones IP de destino del túnel admitan la tunelización GRE de paquetes IP de multidifusión y de difusión. Por ejemplo, en el hub necesitará la línea de configuración **ip nhrp map multicast <spoke-n-addr>** para cada spoke. Con la solución DMVPN, las direcciones radiales no se conocen con anticipación, por lo tanto esta configuración no es posible. En su lugar, NHRP se puede configurar para agregar automáticamente cada radio a la lista de destino multicast en el

hub con el comando **ip nhrp map multicast dynamic**. Con este comando, cuando los routers radiales registran su asignación NHRP de unidifusión con el servidor NHRP (hub), NHRP también creará una asignación de difusión/multidifusión para este spoke. Esto elimina la necesidad de conocer de antemano las direcciones del spoke.

Fast Switching de Cisco Express Forwarding para mGRE

Actualmente, el tráfico en una interfaz mGRE utiliza el modo de switch de proceso, y su rendimiento es pobre. La solución DMVPN agrega la conmutación de Cisco Express Forwarding para el tráfico mGRE, lo cual resulta en un rendimiento superior. No hay comandos de configuración necesarios para activar esta función. Si se permite la conmutación de Cisco Express Forwarding en la interfaz de túnel GRE y las interfaces físicas de salida/entrada, los paquetes de túnel GRE multipunto serán conmutados por Cisco Express Forwarding.

Uso de ruteo dinámico en VPN protegidas IPsec

Esta sección describe el estado actual (solución pre-DMVPN). IPsec se implementa en los routers Cisco a través de un conjunto de comandos que definen el cifrado y luego un comando **crypto map <map-name>** aplicado en la interfaz externa del router. Debido a este diseño y al hecho de que actualmente no existe un estándar para utilizar IPSec para cifrar paquetes de multidifusión/difusión IP, los paquetes de protocolo de ruteo IP no se pueden "reenviar" a través del túnel IPsec y cualquier cambio de ruteo no se puede propagar dinámicamente al otro lado del túnel IPsec.

Nota: Todos los protocolos de ruteo dinámico excepto BGP utilizan paquetes IP de difusión o multidifusión. Los túneles GRE se usan en combinación con IPsec para resolver este problema.

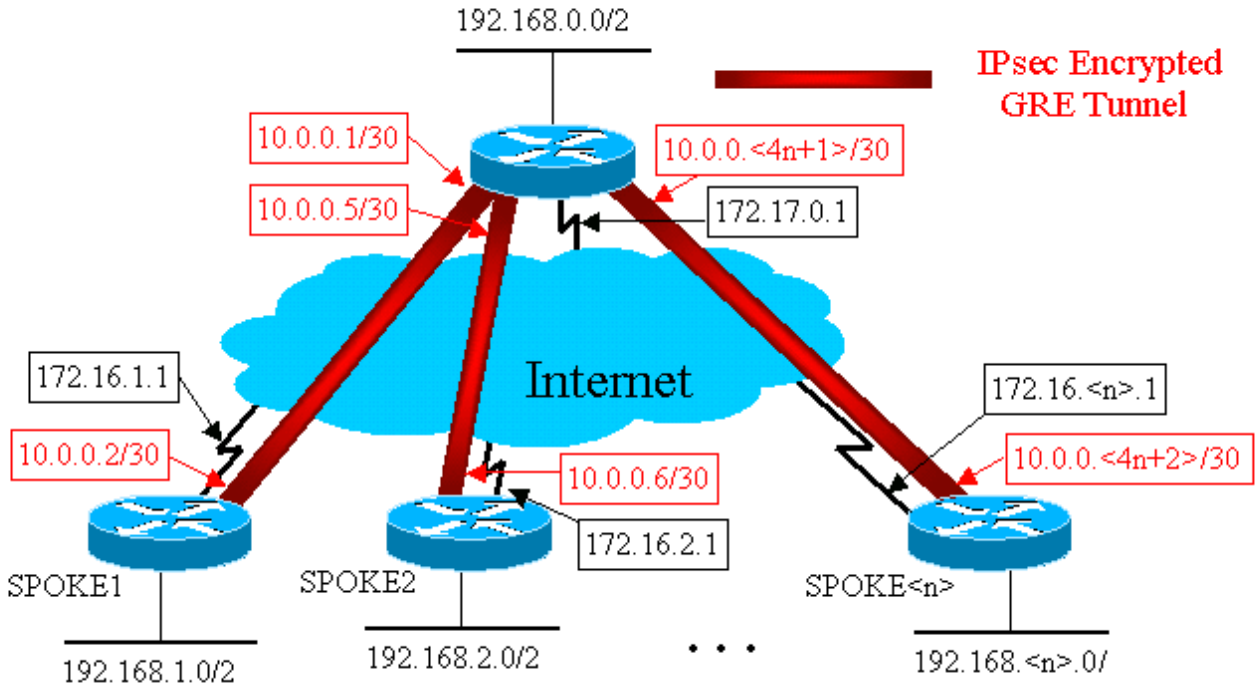
Los túneles GRE se implementan en los routers Cisco mediante una interfaz de túnel virtual (**túnel de interfaz<#>**). El protocolo de tunelización GRE está diseñado para manejar los paquetes de multidifusión/difusión IP de modo que un protocolo de ruteo dinámico pueda ejecutarse sobre un túnel GRE. Los paquetes de túnel GRE son paquetes de unidifusión IP que encapsulan el paquete de multdifusión/unidifusión IP original. Puede usar IPsec para cifrar el paquete de túnel GRE. También puede ejecutar IPsec en modo de transporte y ahorrar 20 bytes, ya que GRE ya ha encapsulado el paquete de datos original y no necesita que IPsec encapsule el paquete IP GRE en otro encabezado de IP.

Cuando se ejecuta IPsec en modo de transporte, hay una restricción que consiste en que las direcciones de origen y destino de IP del paquete que van a cifrarse deben coincidir con las direcciones del par IPsec (el mismo router). En este caso, esto sólo significa que el punto final del túnel GRE y la dirección IPsec del par deben ser las mismas. Esto no es un problema, ya que los mismos routers son puntos finales del túnel tanto de IPsec como de GRE. Combinando túneles GRE con cifrado IPsec, puede utilizar un protocolo de routing IP dinámico para actualizar las tablas de routing en ambos extremos del túnel cifrado. Las entradas de la tabla de IP Routing para las redes aprendidas a través del túnel cifrado tendrán el otro extremo del túnel (dirección IP de la interfaz de túnel GRE) como el siguiente salto IP. Por lo tanto, si las redes cambian a ambos lados del túnel, el otro lado aprenderá dinámicamente del cambio y la conectividad continuará sin ningún cambio de configuración en los routers.

Configuración base

La siguiente es una configuración estándar punto a punto IPsec+GRE. Luego de esto, existe una serie de ejemplos de configuración en los que paso a paso se agregan características específicas de la solución DMVPN para mostrar las diferentes capacidades de DMVPN. Cada ejemplo utiliza al anterior para mostrar cómo utilizar la solución para DMVPN en diseños de red cada vez más complejos. Esta sucesión de ejemplos puede usarse como una plantilla para migrar una VPN IPsec+GRE actual a una DMVPN. Puede detener "la migración" en cualquier momento si ese ejemplo de configuración en particular coincide con los requisitos de diseño de la red.

IPsec + hub y radio GRE (n = 1,2,3,...)



Router del eje de conexión

```
version 12.3
 !
 hostname Hub
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto map vpnmap1 local-address Ethernet0
 crypto map vpnmap1 10 ipsec-isakmp
  set peer 172.16.1.1
  set transform-set trans2
  match address 101
 crypto map vpnmap1 20 ipsec-isakmp
  set peer 172.16.2.1
  set transform-set trans2
  match address 102
 . . .
 crypto map vpnmap1 <10*n> ipsec-isakmp
  set peer 172.16.
```

```
 interface Tunnel1
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.252
  ip mtu 1400
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.16.1.1
 !
 interface Tunnel2
  bandwidth 1000
  ip address 10.0.0.5 255.255.255.252
  ip mtu 1400
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.16.2.1
 !
 . . .
 !
 interface Tunnel




 !
 interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
  crypto map vpnmap1
 !
 interface Ethernet1
  ip address 192.168.0.1 255.255.255.0
 !
 router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
  no auto-summary
 !
 access-list 101 permit gre host 172.17.0.1 host
172.16.1.1
 access-list 102 permit gre host 172.17.0.1 host
172.16.2.1
 ...
 access-list
```

Router Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
```

```
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto map vpnmap1 local-address Ethernet0
 crypto map vpnmap1 10 ipsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.2 255.255.255.252
  ip mtu 1400
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
 !
 interface Ethernet0
  ip address 172.16.1.1 255.255.255.252
  crypto map vpnmap1
 !
 interface Ethernet1
  ip address 192.168.1.1 255.255.255.0
 !
 router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  no auto-summary
 !
 access-list 101 permit gre host 172.16.1.1 host
172.17.0.1
```

Router Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto map vpnmap1 local-address Ethernet0
 crypto map vpnmap1 10 ipsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.6 255.255.255.252
  ip mtu 1400
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
 !
 interface Ethernet0
  ip address 172.16.2.1 255.255.255.252
  crypto map vpnmap1
```

```
 !
 interface Ethernet1
  ip address 192.168.2.1 255.255.255.0
 !
 router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  no auto-summary
 !
 access-list 101 permit gre host 172.16.2.1 host
172.17.0.1
```

Router Spoke<n>

```
version 12.3
 !
 hostname Spoke<n>
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto map vpnmap1 local-address Ethernet0
 crypto map vpnmap1 10 ipsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<4n-2> 255.255.255.252
  ip mtu 1400
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
 !
 interface Ethernet0
  ip address 172.16.<n>.1 255.255.255.252
  crypto map vpnmap1
 !
 interface Ethernet1
  ip address 192.168.<n>.1 255.255.255.0
 !
 router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.
```

En la configuración anterior, las ACL se utilizan para definir qué tráfico se cifrará. En los routers concentradores y los radiales, esta ACL solamente debe coincidir con los paquetes IP del túnel GRE. No importa cómo cambien las redes en ambos extremos, los paquetes de túnel IP GRE no cambiarán, por lo que esta ACL no necesita cambiar.

Nota: Al utilizar las versiones del software Cisco IOS anteriores a 12.2(13)T, debe aplicar el

comando de configuración **crypto map vpnmap1** a las interfaces de túnel GRE (Tunnel<x>) y a la interfaz física (Ethernet0). Con un IOS de Cisco versión 12.2(13)T y superior, sólo se usa el comando de configuración crypto map vpnmap1 en la interfaz física (Ethernet0).

Ejemplos de tablas de ruteo en los routers radiales y de eje de conexión

Tabla de ruteo sobre router de eje de conexión

```
172.17.0.0/24 is subnetted, 1 subnets
 C       172.17.0.0 is directly connected, Ethernet0
      10.0.0.0/30 is subnetted, <n> subnets
 C       10.0.0.0 is directly connected, Tunnel1
 C       10.0.0.4 is directly connected, Tunnel2
 ...
 C       10.0.0.<4n-4> is directly connected, Tunnel<n>
 C    192.168.0.0/24 is directly connected, Ethernet1
 D    192.168.1.0/24 [90/2841600] via 10.0.0.2,
18:28:19, Tunnel1
 D    192.168.2.0/24 [90/2841600] via 10.0.0.6, 2d05h,
Tunnel2
 ...
 D    192.168.<n>.0/24 [90/2841600] via 10.0.0.<4n-2>,
2d05h, Tunnel<n>
```

Tabla de ruteo en el router Radio1

```
172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.1.0 is directly connected, Ethernet0
      10.0.0.0/30 is subnetted, <n> subnets
 C       10.0.0.0 is directly connected, Tunnel1
 D       10.0.0.4 [90/2841600] via 10.0.0.1, 23:00:58,
Tunnel0
 ...
 D      10.0.0.<4n-4> [90/2841600] via 10.0.0.1,
23:00:58, Tunnel0
 D    192.168.0.0/24 [90/2841600] via 10.0.0.1,
23:00:58, Tunnel0
 C    192.168.1.0/24 is directly connected, Loopback0
 D    192.168.2.0/24 [90/3097600] via 10.0.0.1,
23:00:58, Tunnel0
 ...
 D    192.168.<n>.0/24 [90/3097600] via 10.0.0.1,
23:00:58, Tunnel0
```

Tabla de enrutamiento en el router Spoke<n>

```
172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.<n>.0 is directly connected, Ethernet0
      10.0.0.0/30 is subnetted, <n> subnets
 D       10.0.0.0 [90/2841600] via 10.0.0.1, 22:01:21,
Tunnel0
 D       10.0.0.4 [90/2841600] via 10.0.0.1, 22:01:21,
Tunnel0
 ...
 C        10.0.0.<4n-4> is directly connected, Tunnel0
 D    192.168.0.0/24 [90/2841600] via 10.0.0.1,
22:01:21, Tunnel0
 D    192.168.1.0/24 [90/3097600] via 10.0.0.1,
```

```
22:01:21, Tunnel0
 D    192.168.2.0/24 [90/3097600] via 10.0.0.1,
22:01:21, Tunnel0
 ...
 C    192.168.<n>.0/24 is directly connected, Ethernet0
```

Ésta es la configuración básica, y es utilizada como un punto de partida para la comparación con las configuraciones más complejas posibles utilizando la solución DMVPN. El primer cambio reducirá el tamaño de la configuración en el router hub. Esto no es importante si la cantidad de routers radiales es poca, pero es crítico cuando hay más de 50 ó 100.

Reducción del tamaño de la configuración del hub/router

En el siguiente ejemplo, la configuración se modifica mínimamente en el router de eje de conexión de varias interfaces de túnel punto a punto GRE a una única interfaz de túnel multipunto GRE. Este es un primer paso en la solución DMVPN.

Hay un bloque único de líneas de configuración en el router hub para definir las características de mapa crypto para cada router spoke. Esta parte de la configuración define la ACL criptográfica y la interfaz de túnel GRE para ese router spoke. Estas características son mayormente las mismas para todos los radios, excepto para las direcciones IP (**set peer ...**, **tunnel destination ...**).

Si observa la configuración anterior en el router hub, verá que hay al menos 13 líneas de configuración por router spoke; cuatro para el mapa crypto, uno para la ACL crypto y ocho para la interfaz de túnel GRE. El número total de líneas de configuraciones, en caso de que haya 300 routers radiales, es equivalente a 3900 líneas. También necesita 300 subredes (/30) para dirigirse a cada enlace de túnel. Una configuración de este tamaño es muy difícil de administrar y aún más difícil cuando se soluciona el problema de la red VPN. Para reducir este valor, puede utilizar mapas de criptografía dinámicos, lo que reduciría el valor anterior en 1200 línea y dejaría 2700 líneas en una red de 300 radios.

Nota: Cuando se utilizan mapas criptográficos dinámicos, el túnel de cifrado IPsec debe ser iniciado por el router spoke. También puede utilizar **ip unnumbered <interface>** para reducir el número de subredes necesarias para los túneles GRE, pero esto puede dificultar la resolución de problemas más adelante.

Con la solución DMBPN, puede configurar una sola interfaz de túnel GRE multipunto y un solo perfil IPSec en el router de eje de conexión para manejar todos los routers radiales. Esto permite que el tamaño de la configuración en el router de eje de conexión permanezca constante irrespectivamente de la cantidad de routers de eje de conexión que se agreguen a la red VPN.

La solución DMVPN introduce los siguientes comandos nuevos:

```
crypto ipsec profile
```

El comando **crypto ipsec profile <name>** se utiliza como un mapa criptográfico dinámico y está diseñado específicamente para las interfaces de túnel. Este comando se usa para definir los

parámetros para el encripción de IPsec en los túneles VPN de spoke a hub y de spoke a spoke. El único parámetro que se requiere en el perfil es el conjunto de transformación. La dirección de peer IPSec y la **dirección de coincidencia ...** para el proxy IPsec se derivan automáticamente de las asignaciones NHRP para el túnel GRE.

El comando **tunnel protection ipsec profile <name>** se configura en la interfaz de túnel GRE y se utiliza para asociar la interfaz de túnel GRE con el perfil IPsec. Además, el comando **tunnel protection ipsec profile <name>** también se puede utilizar con un túnel GRE punto a punto. En este caso derivará la información del peer IPSec y del proxy del **origen del túnel ...** y **destino del túnel ...** configuración. Esto simplifica la configuración ya que el par IPsec y las ACL criptográficas ya no se necesitan.

Nota: El **comando tunnel protection ...** especifica que el cifrado IPsec se realizará después de que la encapsulación GRE se haya agregado al paquete.

Estos dos primeros comandos nuevos son similares a configurar un mapa crypto y asignar el mapa crypto a una interfaz usando el comando **crypto map <name>**. La gran diferencia es que, con los nuevos comandos, no es necesario especificar la dirección de par IPsec o una ACL para hacer coincidir los paquetes que se van a cifrar. Estos parámetros se determinan de forma automática desde los mapeos NHRP para la interfaz del túnel mGRE.

Nota: Al utilizar el **comando tunnel protection ...** en la interfaz de túnel, un **mapa criptográfico ...** no está configurado en la interfaz física saliente.

El último comando nuevo, **ip nhrp map multicast dynamic**, permite que NHRP agregue automáticamente routers spoke a los mapeos NHRP multicast cuando estos routers spoke inician el túnel mGRE+IPsec y registran sus mapeos NHRP unicast. Esto es necesario para habilitar los protocolos de ruteo dinámico para que funcionen sobre los túneles mGRE+IPsec entre el hub y los radios. Si este comando no estaba disponible, entonces el router hub necesitaría tener una línea de configuración separada para una asignación multicast a cada spoke.

Nota: Con esta configuración, los routers radiales deben iniciar la conexión de túnel mGRE+IPsec, ya que el router hub no está configurado con ninguna información sobre los radios. No obstante, éste no es un problema porque con DMVPN el túnel mGRE+IPsec se inicia automáticamente cuando se inicia el router radial, y se mantiene siempre activo.

Nota: El siguiente ejemplo muestra interfaces de túnel GRE punto a punto en los routers radiales y líneas de configuración NHRP agregadas en los routers radiales y hub para soportar el túnel mGRE en el router hub. Los cambios de configuración son los siguientes.

Router del eje de conexión (anterior)

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.16.1.1
  set transform-set trans2
  match address 101
 crypto map vpnmap1 20 IPsec-isakmp
  set peer 172.16.2.1
  set transform-set trans2
  match address 102
 . . .
 crypto map vpnmap1 <10n> IPsec-isakmp
  set peer 172.16.
```

```
 !
 interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
  crypto map vpnmap1
 !
 access-list 101 permit gre host 172.17.0.1 host
172.16.1.1
 access-list 102 permit gre host 172.17.0.1 host
172.16.2.1
 . . .
 access-list
```

Router de eje de conexión (nuevo)

```
crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  no ip split-horizon eigrp 1
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
```

Router Spoke<n> (antiguo)

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<4n-2> 255.255.255.252
  ip mtu 1400
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
 !
```

```
interface Ethernet0
  ip address 172.16.<n>.1 255.255.255.252
  crypto map vpnmap1
!
 . . .
 !
 access-list 101 permit gre host 172.16.<n>.1 host
172.17.0.1
 !
```

Router Spoke<n> (nuevo)

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.




  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
  tunnel key 100000
 !
interface Ethernet0
  ip address 172.16.<n>.1 255.255.255.252
  crypto map vpnmap1
!
 . . .
 !
 access-list 101 permit gre host 172.16.<n>.1 host
172.17.0.1
 !
```

En los routers radiales, la máscara de subred ha cambiado y los comandos NHRP se han agregado bajo la interfaz de túnel. Los comandos NHRP son necesarios, ya que el router hub ahora utiliza NHRP para asignar la dirección IP de la interfaz de túnel spoke a la dirección IP de la interfaz física spoke.

```
ip address 10.0.0.




      ip mtu 1400
      ip nhrp authentication test
      ip nhrp map 10.0.0.1 172.17.0.1
      ip nhrp network-id 100000
      ip nhrp holdtime 300
      ip nhrp nhs 10.0.0.1
      ...
      tunnel key 100000
```

La subred ahora está /24 en lugar de /30, entonces todos los nodos están en la misma subred en lugar de estar en subredes distintas. Los radios aún envían tráfico de radio a radio a través del hub, ya que utilizan una interfaz de túnel punto a punto GRE. La **autenticación ip nhrp ...**, **ip nhrp network-id ...** y **clave de túnel ...** se utilizan para asignar los paquetes de túnel y los paquetes NHRP a la interfaz de túnel GRE multipunto y a la red NHRP correcta cuando se reciben en el hub. El **mapa ip nhrp ...** e **ip nhrp nhs** ... NHRP utiliza los comandos en spoke para anunciar la asignación NHRP de spokes (10.0.0.<n+1> —> 172.16.<n>.1) al hub. La dirección 10.0.0.<n+1> se recupera de la **dirección ip ...** en la interfaz del túnel y la dirección 172.16.<n>.1 se recupera del **destino del túnel ...** en la interfaz de túnel.

En un caso en el que hay 300 routers radiales, este cambio reduciría el número de líneas de configuración en el hub de 3900 líneas a 16 líneas (una reducción de 3884 líneas). La configuración en cada router spoke aumentaría en 6 líneas.

Soporte de direcciones dinámicas en radios

En un router de Cisco, cada par IPsec debe ser configurado con la dirección IP del otro par IPsec antes de que el túnel IPsec pueda aparecer. Esto ocasiona un problema si el router spoke tiene una dirección dinámica en su interfaz física, lo cual es común en los routers conectados mediante links de DSL o cable.

TED permite que un par IPSec busque a otro par IPSec por medio del envío de un paquete de Protocolos de administración de claves y asociaciones de seguridad de Internet (ISAKMP) a la dirección IP de destino del paquete de datos originales que debían cifrarse. Se supone que este paquete atravesará la red interviniente por el mismo trayecto que el que recorre por el paquete del túnel IPsec. Este paquete será recogido por el par IPSec de otro extremo, que responderá al primer par. Los dos routers entonces negociarán asociaciones de seguridad (SA) IPsec e ISAKMP y encenderán el túnel IPsec. Esto sólo funcionará si los paquetes de datos a cifrar tienen direcciones IP enrutables.

La TED puede utilizarse en combinación con los túneles GRE con la configuración de la sección anterior. Esto se ha probado y funciona, aunque hubo un error en las versiones anteriores del software Cisco IOS donde TED obligó a que se cifrara todo el tráfico IP entre los dos pares IPsec, no sólo los paquetes de túnel GRE. La solución DMVPN proporciona esta y otras capacidades adicionales sin que el host tenga que utilizar direcciones de IP enrutables y sin tener que enviar paquetes de prueba y respuesta. Con una pequeña modificación, la configuración de la última sección puede utilizarse para el soporte de routers radiales con direcciones IP dinámicas en sus interfaces físicas externas.

Router de eje de conexión (sin cambios)

```
crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
```

```
 ip nhrp holdtime 600
 no ip split-horizon eigrp 1
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.0
```

Router Spoke<n> (antiguo)

```
crypto map vpnmap1 10 IPsec-isakmp
 set peer 172.17.0.1
 set transform-set trans2
 match address 101
!
...
!
access-list 101 permit gre host 172.16.
```

Router Spoke<n> (nuevo)

```
crypto map vpnmap1 10 IPsec-isakmp
 set peer 172.17.0.1
 set transform-set trans2
 set security-association level per-host
 match address 101
!
...
!
access-list 101 permit gre any host 172.17.0.1
```

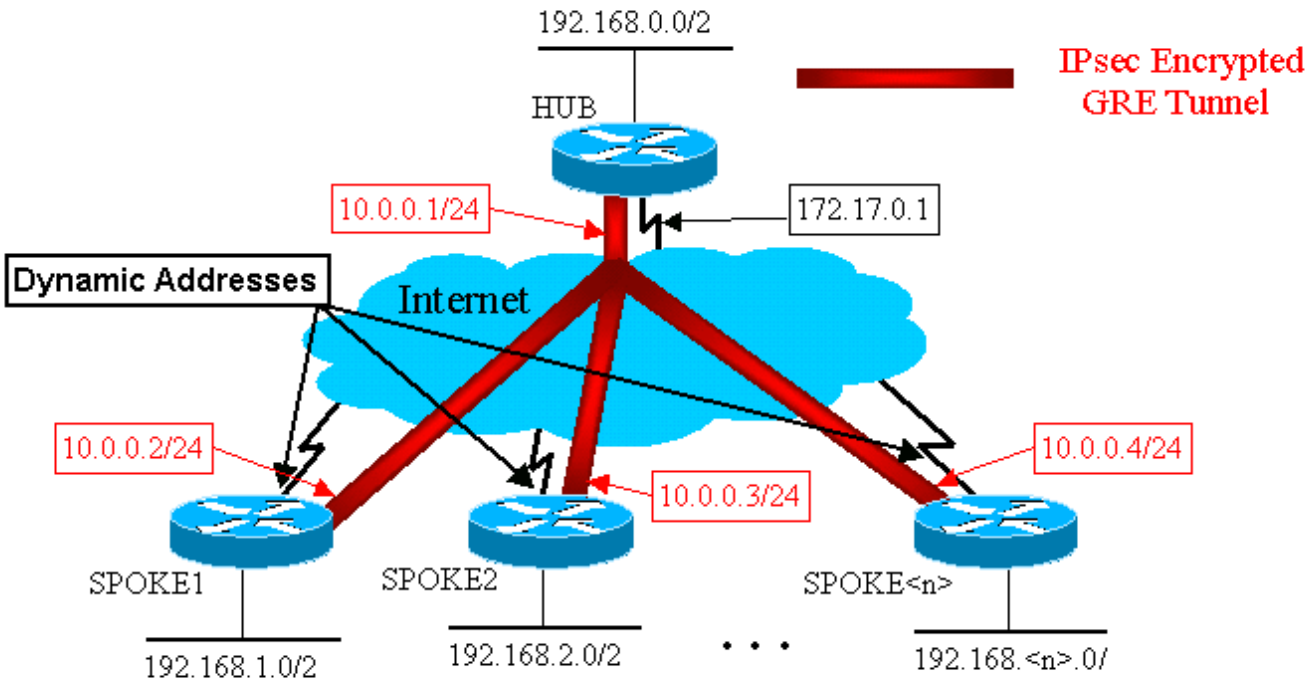
La funcionalidad utilizada en la nueva configuración spoke funciona de la siguiente manera.

- Cuando aparece la interfaz de túnel GRE, comenzará a enviar paquetes de registro NHRP al router concentrador. Estos paquetes de registro NHRP activarán el inicio de IPSec. En el router spoke, se configuran los comandos set peer <peer-address> y **match ip access-list <ACL>**. La ACL especifica GRE como protocolo, cualquiera para el origen y la dirección IP del hub para el destino.**Nota:** Es importante tener en cuenta que se está utilizando alguno como origen en la ACL, y este debe ser el caso, ya que la dirección IP del router spoke es dinámica y, por lo tanto, no se conoce antes de que la interfaz física esté activa. Puede usarse una subred de IP para la fuente en ACL si la dirección spoke de la interfaz dinámica estará restringida a una dirección dentro de esa subred.
- El comando **set security-association level per-host** se utiliza para que el origen IP en el proxy IPsec de spokes sea solamente la dirección de interfaz física actual de spokes (/32), en lugar de la "any" de la ACL. Si se utilizara "any" de la ACL como origen en el proxy IPsec, impediría que cualquier otro router spoke también configure un túnel IPsec+GRE con este hub. Esto se debe a que la IPsec proxy resultante en el hub sería equivalente para permitir gre host 172.17.0.1 any. Esto significaría que a todos los paquetes de túnel GRE destinados a

cualquier spoke se los cifraría y enviaría al primer spoke que estableció un túnel con el concentrador, ya que su proxy IPsec hace coincidir paquetes GRE para cada spoke.

- Una vez establecido el túnel IPsec, un paquete de registro NHRP va desde el router spoke hasta el Servidor de salto siguiente (NHS) configurado. El NHS es el router hub de esta red hub-and-spoke. El paquete de registro NHRP proporciona la información para el router de eje de conexión que permite crear una correspondencia NHRP para este router radial. Con esta correspondencia, el router de eje de conexión puede reenviar paquetes de datos IP de unidifusión a este router de radio por el túnel mGRE+IPsec. Además, el hub agrega el router spoke a su lista de mapeo de multidifusión NHRP. El eje de conexión comienza a enviar paquetes de Dynamic IP Routing Multicast a la radio (en caso de que el Dynamic Routing Protocol esté configurado). El spoke se convertirá entonces en un vecino del protocolo de ruteo del hub e intercambiará actualizaciones de ruteo.

Hub y spoke IPsec + mGRE



Router del eje de conexión

```
version 12.3
 !
 hostname Hub
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
```

```
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  no ip split-horizon eigrp 1
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
 !
 interface Ethernet1
  ip address 192.168.0.1 255.255.255.0
 !
 router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
  no auto-summary
 !
```

En la configuración del eje de conexión anterior, observe que las direcciones IP de los routers radiales no están configuradas. La interfaz física externa del spoke y la asignación a la dirección IP de la interfaz del túnel spoke son aprendidas en forma dinámica por el hub a través del NHRP. Esto permite asignar dinámicamente la dirección IP de la interfaz física externa del spoke.

Router Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto map vpnmap1 local-address Ethernet0
 crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set security-association level per-host
  set transform-set trans2
  match address 101
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.2 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
```

```
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
!
interface Ethernet0
 ip address dhcp hostname Spoke1
 crypto map vpnmap1
!
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
 no auto-summary
!
access-list 101 permit gre 172.16.1.0 0.0.0.255 host
172.17.0.1
```

Router Spoke2

```
version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto map vpnmap1 local-address Ethernet0
crypto map vpnmap1 10 IPsec-isakmp
 set peer 172.17.0.1
 set security-association level per-host
 set transform-set trans2
 match address 101
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.3 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
!
interface Ethernet0
 ip address dhcp hostname Spoke2
 crypto map vpnmap1
!
interface Ethernet1
 ip address 192.168.2.1 255.255.255.0
!
```

```
 router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  no auto-summary
 !
 access-list 101 permit gre 172.16.2.0 0.0.0.255 host
172.17.0.1
```

Lo más importante que debe tener en cuenta acerca de la configuración de spoke es lo siguiente:

- La dirección IP de la interfaz física externa (ethernet0) es dinámica por DHCP.**ip address dhcp hostname Spoke2**
- La ACL crypto (101) especifica una subred como origen del proxy IPsec.**access-list 101 permit gre 172.16.2.0 0.0.0.255 host 172.17.0.1**
- El siguiente comando en el mapa de encripción de IPsec especifica que la asociación de seguridad se hará por host.**set security-association level per-host**
- Todos los túneles forman parte de la misma subred, dado que todos ellos se encuentran conectados a través de la misma interfaz GRE multipunto en el router hub.**ip address 10.0.0.2 255.255.255.0**

La combinación de estos tres comandos hace que sea innecesario configurar la dirección IP de la interfaz física externa del spoke. El proxy IPsec que se utiliza estará basado en host en lugar de en subred.

La configuración en los routers radiales tiene la dirección IP del router de eje de conexión configurada ya que necesita iniciar el túnel IPsec+GRE. Note la similitud entre las configuraciones Spoke 1 y Spoke 2. No sólo son similares estos dos, sino que todas las configuraciones del router spoke serán similares. En la mayoría de los casos, todos los radios simplemente necesitan direcciones IP únicas en sus interfaces, y el resto de sus configuraciones serán las mismas. Esto hace posible una rápida configuración e instrumentación de varios routers spoke.

Los datos NHRP tienen el siguiente aspecto en el eje de conexión y radio.

Router del eje de conexión

```
Hub#show ip nhrp
   10.0.0.2/32 via 10.0.0.2, Tunnel0 created 01:25:18,
expire 00:03:51
     Type: dynamic, Flags: authoritative unique
registered
     NBMA address: 172.16.1.4
   10.0.0.3/32 via 10.0.0.3, Tunnel0 created 00:06:02,
expire 00:04:03
     Type: dynamic, Flags: authoritative unique
registered
     NBMA address: 172.16.2.10
   ...
   10.0.0.<n>/32 via 10.0.0.<n>, Tunnel0 created
00:06:00, expire 00:04:25
     Type: dynamic, Flags: authoritative unique
registered
     NBMA address: 172.16.<n>.41
```

Router Spoke1

```
Spoke1#sho ip nhrp
   10.0.0.1/32 via 10.0.0.1, Tunnel0 created 4d08h,
never expire
     Type: static, Flags: authoritative
     NBMA address: 172.17.0.1
```

Configuración multipunto dinámica de eje de conexión y radio

La configuración en los routers radiales arriba no se basa en funciones de la solución DMVPN, de manera que estos routers radiales pueden ejecutar las versiones del software Cisco IOS anteriores a la 12.2 (13)T. La configuración del router hub depende de las funciones DMVPN, por lo que debe ejecutar la versión 12.2(13)T u otra posterior del IOS de Cisco. Esto le permite cierta flexibilidad a la hora de decidir cuándo necesita actualizar los routers radiales que ya están implementados. Si los routers radiales también están ejecutando Cisco IOS 12.2(13)T o posterior, puede simplificar la configuración radial como se indica a continuación.

Router Spoke<n> (anterior a Cisco IOS 12.2(13)T)

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set security-association level per-host
  set transform-set trans2
  match address 101
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<n+1> 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
  tunnel key 100000
 !
 interface Ethernet0
  ip address dhcp hostname Spoke<n>
  crypto map vpnmap1
 !
 . . .
 !
 access-list 101 permit gre any host 172.17.0.1
```

Router Spoke<n> (después de Cisco IOS 12.2(13)T)

```
crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
```

```
 bandwidth 1000
 ip address 10.0.0.<n+1> 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke<n>
!
```

Tenga en cuenta que hicimos lo siguiente:

1. Eliminamos el comando crypto map vpnmap1 10 ipsec-isakmp y lo reemplazamos por crypto ipsec profile vpnprof.
2. Se quitó el comando **crypto map vpnmap1** de las interfaces Ethernet0 y se puso el comando **tunnel protection ipsec profile vpnprof** en la interfaz Tunnel0.
3. Eliminó la ACL de criptografía, access-list 101 permit gre any host 172.17.0.1.

En este caso, las direcciones de peer IPSec y los proxies se derivan automáticamente del **origen del túnel ...** y **destino del túnel ...** configuración. Los pares y los proxies son los siguientes (como se ve en el resultado del comando **show crypto ipsec sa**):

```
...
local ident (addr/mask/prot/port):    (172.16.1.24/255.255.255.255/47/0)
remote ident (addr/mask/prot/port):   (172.17.0.1/255.255.255.255/47/0)
...
local crypto endpt.: 172.17.1.24, remote crypto endpt.:172.17.0.1
...
```

En resumen, las siguientes configuraciones totales incluyen todos los cambios realizados en este punto desde la [configuración base](#) (eje de conexión y radio IPsec+GRE).

Router del eje de conexión

```
version 12.3
 !
 hostname Hub
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
```

```
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 no ip split-horizon eigrp 1
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
 no auto-summary
!
```

No hay cambios en la configuración del eje de conexión.

Router Spoke1

```
version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.2 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke2
!
```

```
 interface Ethernet1
  ip address 192.168.1.1 255.255.255.0
 !
 router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  no auto-summary
 !
```

Router Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.3 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address dhcp hostname Spoke2
 !
 interface Ethernet1
  ip address 192.168.2.1 255.255.255.0
 !
 router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  no auto-summary
 !
```

Red privada virtual multipunto dinámica con IPsec

Los conceptos y la configuración de esta sección muestran las capacidades completas de DMVPN. NHRP proporciona la capacidad para que los routers radiales aprendan dinámicamente la dirección de interfaz física exterior de los otros routers radiales en la red VPN. Esto significa que el router spoke tendrá suficiente información para construir dinámicamente un túnel IPsec+mGRE directamente hacia otro router spoke. Esto es muy beneficioso ya que, si este

tráfico de datos de radio a radio fuera enviado a través del router concentrador debería ser encripción/desencripción, aumentando al doble el retraso y la carga en el router concentrador. Para utilizar esta función, los routers radiales deben estar conmutados de interfaces de túnel GRE punto a punto (p-pGRE) a GRE multipunto (mGRE). También deben aprender las redes o subredes disponibles detrás de los otros radiales con un salto siguiente de IP de la dirección IP del túnel del otro router radial. Los routers radiales aprenden estas (sub)redes a través del protocolo de ruteo IP dinámico que se ejecuta sobre el túnel IPsec+mGRE con el hub.

El Dynamic IP Routing Protocol que se ejecuta en el router hub puede configurarse para reflejar a todos los spokes las rutas que aprendió un spoke fuera de la misma interfaz pero la IP de próximo salto en estas rutas será generalmente el router hub, no el router spoke del que aprendió esta ruta el hub.

Nota: El protocolo de ruteo dinámico sólo se ejecuta en los links hub y spoke, no se ejecuta en los links dinámicos spoke-to-spoke.

Los protocolos de ruteo dinámico (RIP, OSPF y EIGRP) deben configurarse en un router hub para promocionar las rutas de regreso fuera de la interfaz de túnel mGRE. Además, deben configurarse para establecer el próximo salto de IP al router spoke de origen para aquellas rutas que se conocen por un spoke cuando la ruta se promociona a otros spokes.

A continuación se presentan los requisitos para las configuraciones de los protocolos de ruteo.

RIP

Debe apagar el horizonte dividido en la interfaz de túnel mGRE en el hub; de lo contrario, RIP no anunciará las rutas aprendidas a través de la interfaz mGRE de regreso a esa misma interfaz.

```
no ip split-horizon
```

No se necesitan otros cambios. RIP usará automáticamente el siguiente salto IP original en las rutas que anuncia de regreso a la misma interfaz donde aprendió estas rutas.

EIGRP

Debe apagar el horizonte dividido en la interfaz del túnel mGRE del hub, de lo contrario EIGRP no publicitará las rutas aprendidas a través de la interfaz mGRE de regreso a través de esa misma interfaz.

```
no ip split-horizon eigrp
```

De manera predeterminada, EIGRP establecerá el next-hop de IP como router hub para las rutas que anuncia, aunque anuncie dichas rutas hacia la misma interfaz de la cual las obtuvo. Por consiguiente, en este caso necesita el siguiente comando de configuración para indicar a EIGRP

que utilice el salto siguiente de IP original al anunciar estas rutas.

```
no ip next-hop-self eigrp
```

Nota: El comando **no ip next-hop-self eigrp <as>** estará disponible a partir de la versión 12.3(2) del IOS de Cisco. Para las versiones del IOS de Cisco entre 12.2(13)T y 12.3(2) debe hacer lo siguiente:

- Si no se desean túneles dinámicos de spoke a spoke, no necesita el comando a continuación.
- Si se desean túneles dinámicos de radio a radio, debe utilizar la conmutación de proceso en la interfaz de túnel en los routers radiales.
- De lo contrario, necesitará usar un protocolo de ruteo diferente sobre la DMVPN.

OSPF

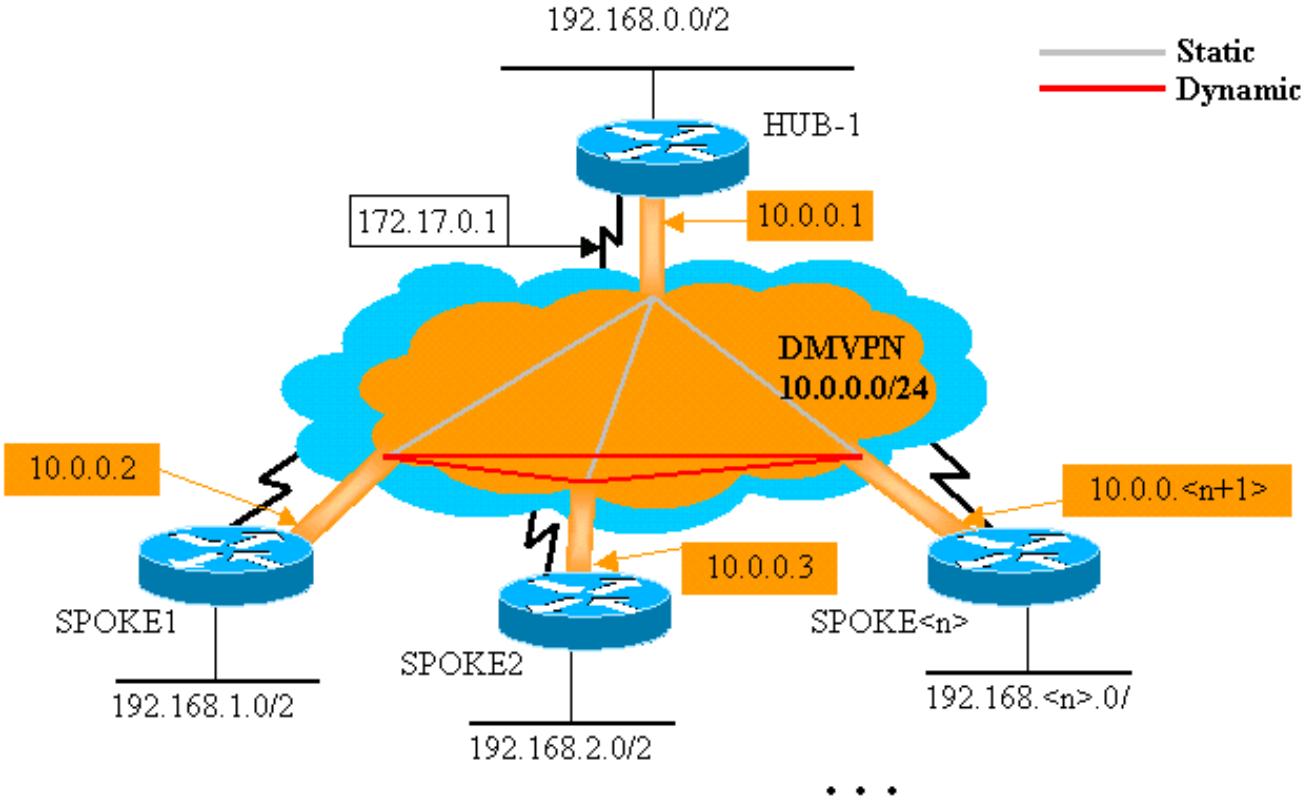
Debido a que OSPF es un protocolo de ruteo de estado de link, no hay problemas de horizonte dividido. Normalmente para las interfaces multipunto debe configurar el tipo de red OSPF para que sea punto-a-multipunto, pero esto haría que el OSPF agregue rutas de host a la tabla de ruteo en los routers spoke. Estas rutas de los hosts harían que los paquetes destinados a las redes detrás de otros routers spoke sean reenviados a través del hub y no reenviados directamente al otro spoke. Para solucionar este problema, configure el tipo de red OSPF para difusión mediante el comando.

```
ip ospf network broadcast
```

También debe asegurarse de que el router hub sea el router designado (DR) para la red IPsec+mGRE. Esto se realiza haciendo que la configuración de la prioridad OSPF sea mayor a 1 en el hub y a 0 en los spokes.

- Hub **ip ospf priority 2**
- Spoke: **ip ospf priority 0**

Hub simple para red DMVPN



Router del eje de conexión

```
version 12.3
 !
 hostname Hub
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  ip ospf network broadcast
  ip ospf priority 2
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
```

```
 ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.0.255 area 0
!
```

El único cambio en la configuración del concentrador es que el OSPF es el protocolo de ruteo en lugar del EIGRP. Observe que el tipo de red OSPF está configurado en broadcast y la prioridad está establecida en 2. Si se configura el tipo de red OSPF para broadcast, OSPF instalará rutas para las redes detrás de los routers radiales con una dirección IP de siguiente salto como dirección de túnel GRE para ese router radial.

Router Spoke1

```
version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.2 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast 172.17.0.1
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 ip ospf network broadcast
 ip ospf priority 0
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke1
!
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
!
```

La configuración de los routers spoke es ahora muy similar a la configuración del hub. Las diferencias son las siguientes:

- La prioridad OSPF se establece en 0. No se puede permitir que los routers radiales se conviertan en DR para la red de acceso múltiple sin difusión (NBMA) mGRE. Sólo el router hub tiene conexiones estáticas directas a todos los routers spoke. El DR debe tener acceso a todos los miembros de la red NBMA.
- Hay correspondencias NHRP unidifusión y multidifusión configuradas para el router de eje de conexión.

  ```
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ```

  En la configuración anterior, el **ip nhrp map multicast ...** no se necesitaba el comando porque el túnel GRE era punto a punto. En ese caso, los paquetes multicast se encapsularán automáticamente a través del túnel hasta el único destino posible. Este comando ahora es necesario porque el túnel GRE de radios ha cambiado a multipunto y hay más de un destino posible.
- Cuando el router radial aparece, debe iniciar la conexión de túnel con el núcleo central, debido a que el router del núcleo central no está configurado con ninguna información referida a los routers radiales y los routers radiales pueden tener direcciones IP asignadas dinámicamente. Los routers radiales también están configurados con el eje de conexión como su NHS NHRP.

  ```
  ip nhrp nhs 10.0.0.1
  ```

  Mediante el comando anterior, el router spoke le envía, en intervalos regulares, paquetes de registro NHRP al router del concetrador a través del túnel mGRE+IPsec. Estos paquetes de registro proporcionan la información de correspondencia NHRP radial que necesita el router de eje de conexión para tunelizar los paquetes a los routers radiales.

Router Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.3 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
```

```
 ip ospf network broadcast
 ip ospf priority 0
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke1
!
interface Ethernet1
 ip address 192.168.3.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
!
```

Router Spoke<n>

```
version 12.3
!
hostname Spoke<n>
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.<n+1> 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast 172.17.0.1
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 ip ospf network broadcast
 ip ospf priority 0
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke<n>
!
interface Ethernet1
 ip address 192.168.<n>.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.
```

```
!
```

Observe que las configuraciones de todos los routers radiales son muy similares. Las únicas diferencias son las direcciones IP en las interfaces locales. Esto ayuda a implementar un gran número de routers radiales. Todos los routers radiales pueden configurarse del mismo modo y sólo es necesario agregar las direcciones de interfaz IP locales.

En este punto, observe las tablas de ruteo y las tablas de mapeo NHRP en los routers Hub, Spoke1 y Spoke2 para ver las condiciones iniciales (justo después de que los routers Spoke1 y Spoke2 se activen) y las condiciones después de que Spoke1 y Spoke2 hayan creado un link dinámico entre ellos.

Condiciones iniciales

Información del router de eje de conexión

```
Hub#show ip route
      172.17.0.0/24 is subnetted, 1 subnets
 C       172.17.0.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 1 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 C    192.168.0.0/24 is directly connected, Ethernet1
 O    192.168.1.0/24 [110/2] via 10.0.0.2, 00:19:53,
Tunnel0
 O    192.168.2.0/24 [110/2] via 10.0.0.3, 00:19:53,
Tunnel0
 Hub#show ip nhrp
 10.0.0.2/32 via 10.0.0.2, Tunnel0 created 00:57:27,
expire    00:04:13
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.1.24
 10.0.0.3/32 via 10.0.0.3, Tunnel0 created 07:11:25,
expire    00:04:33
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.2.75
 Hub#show crypto engine connection active
  ID  Interface   IP-Address    State Algorithm
Encrypt Decrypt
  204 Ethernet0   172.17.0.1     set  HMAC_SHA+DES_56_CB
0       0
  205 Ethernet0   172.17.0.1     set  HMAC_SHA+DES_56_CB
0       0
 2628 Tunnel0     10.0.0.1       set  HMAC_MD5
0     402
 2629 Tunnel0     10.0.0.1       set  HMAC_MD5
357       0
 2630 Tunnel0     10.0.0.1       set  HMAC_MD5
0     427
 2631 Tunnel0     10.0.0.1       set  HMAC_MD5
308       0
```

Información del router Spoke1

```
Spoke1#show ip route
      172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.1.24 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 1 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 O    192.168.0.0/24 [110/2] via 10.0.0.1, 00:31:46,
Tunnel0
 C    192.168.1.0/24 is directly connected, Ethernet1
 O    192.168.2.0/24 [110/2] via 10.0.0.3, 00:31:46,
Tunnel0
 Spoke1#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:42:00,
never expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.1
 Spoke1#show crypto engine connection active
  ID  Interface   IP-Address    State Algorithm
Encrypt Decrypt
    2 Ethernet0   172.16.1.24    set  HMAC_SHA+DES_56_CB
0       0
 2064 Tunnel0     10.0.0.2       set  HMAC_MD5
0     244
 2065 Tunnel0     10.0.0.2       set  HMAC_MD5
276       0
```

Información del router Spoke 2

```
Spoke2#show ip route
      172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.2.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 1 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 O    192.168.0.0/24 [110/2] via 10.0.0.1, 00:38:52,
Tunnel0
 O    192.168.1.0/24 [110/2] via 10.0.0.2, 00:38:52,
Tunnel0
 C    192.168.2.0/24 is directly connected, Ethernet1
 Spoke2#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:32:10,
never expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.1
 Spoke2#show crypto engine connection active
  ID  Interface   IP-Address    State Algorithm
Encrypt Decrypt
   17 Ethernet0   172.16.2.75    set  HMAC_SHA+DES_56_CB
0       0
 2070 Tunnel0     10.0.0.3       set  HMAC_MD5
0     279
 2071 Tunnel0     10.0.0.3       set  HMAC_MD5
316       0
```

En este punto hacemos un ping desde la dirección 192.168.1.2 a la dirección 192.168.2.3. Estas direcciones son para host detrás de los routers Spoke1 y Spoke2 respectivamente. La siguiente secuencia de eventos tiene lugar para generar el túnel mGRE+IPsec de spoke a spoke directo.

1. El router Spoke1 recibe el paquete ping con el destino 192.168.2.3. Busca este destino en la tabla de ruteo y encuentra que necesita reenviar este paquete fuera de la interfaz Tunnel0 a la siguiente dirección IP, 10.0.0.3.
2. El router Radio1 verifica la tabla de correspondencia NHRP para el destino 10.0.0.3 y

encuentra que no hay entrada. El router Spoke1 crea un paquete de solicitud de resolución NHRP y lo envía a su NHS (el router Hub).

3. El router Hub verifica la tabla de mapeo NHRP para el destino 10.0.0.3 y encuentra que corresponde a la dirección 172.16.2.75. El router concentrador crea un paquete de respuesta con resolución NHRP y lo envía al router Spoke1.
4. El router Spoke1 recibe la respuesta de resolución NHRP e ingresa la correspondencia 10.0.0.3 —>172.16.2.75 en su tabla de mapeo NHRP. Cuando se agrega la correlación de NHRP se activa el IPSec para que inicie un túnel IPsec con el par 172.16.2.75.
5. El router Spoke1 inicia ISAKMP con 172.16.2.75 y negocia las SA ISAKMP e IPsec. El proxy IPsec deriva del comando Tunnel0 **tunnel source <address>** y del mapping NHRP.

```
local ident (addr/mask/prot/port): (172.16.1.24/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.2.75/255.255.255.255/47/0)
```

6. Una vez que el túnel IPsec ha terminado de construirse, todos los paquetes de datos adicionales a la subred 192.168.2.0/24 se envían directamente a Spoke2.
7. Después de que un paquete destinado a 192.168.2.3 haya sido reenviado al host, este host enviará un paquete de retorno a 192.168.1.2. Cuando el router Spoke2 recibe este paquete destinado a 192.168.1.2, buscará este destino en la tabla de ruteo y encontrará que necesita reenviar este paquete hacia afuera por la interfaz Tunnel0 al próximo salto de IP, 10.0.0.2.
8. El router Spoke2 verifica la tabla de mapeo NHRP correspondiente al destino 10.0.0.2 y detecta que no hay una entrada. El router Spoke2 crea un paquete de solicitud de resolución NHRP y lo envía a su NHS (el router Hub).
9. El router Hub verifica la tabla de mapeo NHRP para el destino 10.0.0.2 y encuentra que corresponde a la dirección 172.16.1.24. El router concentrador crea un paquete de respuesta con resolución NHRP y lo envía al router Spoke2.
10. El router Spoke2 recibe la respuesta de resolución NHRP e ingresa en la correspondencia 10.0.0.2 —> 172.16.1.24 en su tabla de mapeo NHRP. El agregado del mapeo NHRP hace que IPsec inicie un túnel IPsec con el par 172.16.1.24, pero como ya existe un túnel IP con el par 172.16.1.24, no se necesita hacer nada más.
11. Spoke1 y Spoke2 ahora pueden reenviar paquetes directamente entre sí. Cuando no se ha utilizado el mapeo NHRP para reenviar paquetes para la retención del tiempo, aquélla se borrará. La eliminación de la entrada de mapeo NHRP hará que IPsec elimine las SA de IPsec para este link directo.

Condiciones luego de la creación de un link dinámico entre Spoke1 y Spoke2

Información del router Spoke1

```
Spoke1#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 02:34:16,
never expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.1
 10.0.0.3/32 via 10.0.0.3, Tunnel0 created 00:00:05,
expire 00:03:35
   Type: dynamic, Flags: router unique used
   NBMA address: 172.16.2.75
 Spoke1#show crypto engine connection active
  ID  Interface   IP-Address    State Algorithm
```

```
Encrypt Decrypt
    2 Ethernet0   172.16.1.24    set  HMAC_SHA+DES_56_CB
0       0
    3 Ethernet0   172.16.1.24    set  HMAC_SHA+DES_56_CB
0       0
 2064 Tunnel0     10.0.0.2       set  HMAC_MD5
0     375
 2065 Tunnel0     10.0.0.2       set  HMAC_MD5
426       0
 2066 Tunnel0     10.0.0.2       set  HMAC_MD5
0      20
 2067 Tunnel0     10.0.0.2       set  HMAC_MD5
19        0
```

Información del router Spoke 2

```
Spoke2#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 02:18:25,
never expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.1
 10.0.0.2/32 via 10.0.0.2, Tunnel0 created 00:00:24,
expire 00:04:35
   Type: dynamic, Flags: router unique used
   NBMA address: 172.16.1.24
 Spoke2#show crypto engine connection active
  ID  Interface   IP-Address    State Algorithm
Encrypt Decrypt
   17 Ethernet0   172.16.2.75    set  HMAC_SHA+DES_56_CB
0       0
   18 Ethernet0   172.16.2.75    set  HMAC_SHA+DES_56_CB
0       0
 2070 Tunnel0     10.0.0.3       set  HMAC_MD5
0     407
 2071 Tunnel0     10.0.0.3       set  HMAC_MD5
460       0
 2072 Tunnel0     10.0.0.3       set  HMAC_MD5
0      19
 2073 Tunnel0     10.0.0.3       set  HMAC_MD5
20        0
```

A partir de la salida anterior, puede ver que el Radio 1 y el Radio 2 han recibido asignaciones NHRP para cada uno del router de eje de conexión, y han construido y utilizado un túnel mGRE+Ipsec. Las correspondencias NHRP caducarán transcurridos cinco minutos (el valor actual de retención de tiempo NHRP = 300 segundos). Si las asignaciones NHRP se utilizan en el último minuto antes de caducar, se enviará una solicitud de resolución NHRP y una respuesta para actualizar la entrada antes de eliminarla. De lo contrario, se eliminará el mapeo NHRP y eso hará que IPSec borre los IPSec SA.

IPSec VPN multipunto dinámico con ejes de conexión dobles

Con algunas líneas de configuración adicionales para los routers radiales, puede configurar routers hub duales (o múltiples) para obtener redundancia. Existen dos formas de configurar DMVPN de hub dual.

- Una única red DMVPN con cada radio utilizando una única interfaz de túnel GRE multipunto y apuntando a dos ejes de conexión diferentes como su servidor de próximo salto (NHS).Los

routers hub sólo tendrán una única interfaz de túnel GRE multipunto.

- Redes duales DMVPN con cada una de las radios con dos interfaces de túnel GRE (punto a punto o multipunto) y cada túnel GRE conectado a un router de eje de conexión diferente.Una vez más, los routers hub sólo tendrán una única interfaz de túnel GRE multipunto.

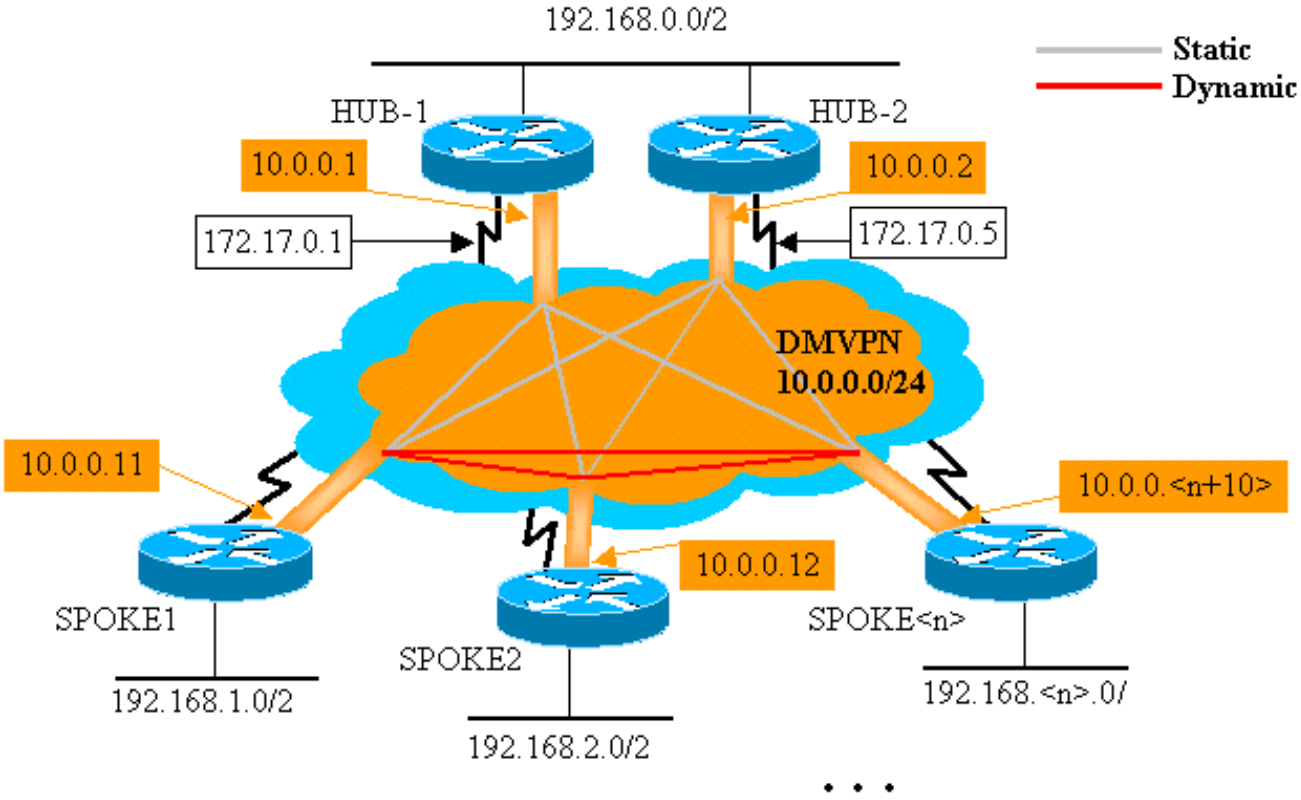
Los siguientes ejemplos se refieren a la configuración de estos dos escenarios diferentes para las DMVPN de hub dual. En ambos casos, las diferencias destacadas están relacionadas con la configuración del hub simple para DMVPN.

Eje de conexión dual – Diseño DMPVN simple

El hub doble con una sola disposición de DMVPN es fácilmente configurable, pero no le permite ejercer tanto control sobre el ruteo a través de la DMVPN como el hub doble con doble disposición de DMVPN. La idea en este caso es tener una única "nube" DMVPN con todos los concentradores (dos en este caso) y todos los radios conectados a esta única subred ("nube"). Los mapeos estáticos NHRP desde los spokes a los hubs definen los links estáticos IPsec+mGRE sobre los cuáles se ejecutarán los protocolos de ruteo dinámico. El protocolo de ruteo dinámico no se ejecutará en los links dinámicos IPsec+mGRE entre spokes. Dado que los routers radiales están ruteando vecinos con los routers hub sobre la misma interfaz de túnel mGRE, no puede utilizar las diferencias de link o interfaces (como métrica, costo, retraso o ancho de banda) para modificar las métricas del protocolo de ruteo dinámico para preferir un hub sobre el otro hub cuando ambos están activos. Si se necesita esta preferencia, se deben usar las técnicas inherentes a la configuración del protocolo de ruteo. Por este motivo, sería mejor que utilice EIGRP o RIP en lugar de OSPF para el protocolo de ruteo dinámico.

Nota: El problema anterior suele ser sólo un problema si los routers hub están ubicados de forma conjunta. Cuando no están ubicados de manera conjunta, el ruteo dinámico probablemente elija el router de hub apropiado, incluso si la red de destino puede alcanzarse a través de cualquier router hub.

Eje de conexión dual – Diseño DMPVN simple



Router del eje de conexión

```
version 12.3
 !
 hostname Hub1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  ip ospf network broadcast
  ip ospf priority 2
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
```

```
 !
 interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
 !
 interface Ethernet1
  ip address 192.168.0.1 255.255.255.0
 !
 router ospf 1
  network 10.0.0.0 0.0.0.255 area 1
  network 192.168.0.0 0.0.0.255 area 0
 !
```

Router del Hub2

```
version 12.3
 !
 hostname Hub2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 900
  ip address 10.0.0.2 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp map  multicast 172.17.0.1
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  ip nhrp nhs 10.0.0.1
  ip ospf network broadcast
  ip ospf priority 1
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address 172.17.0.5 255.255.255.0
 !
 interface Ethernet1
  ip address 192.168.0.2 255.255.255.0
 !
 router ospf 1
  network 10.0.0.0 0.0.0.255 area 1
  network 192.168.0.0 0.0.0.255 area 0
 !
```

El único cambio en la configuración de Hub1 es cambiar OSPF para utilizar dos áreas. El área 0 se utiliza para la red detrás de los dos ejes de conexión y el área 1 se utiliza para la red DMVPN y las redes detrás de los routers radiales. OSPF podría utilizar una sola área, pero aquí se utilizaron

dos áreas para demostrar la configuración para varias áreas OSPF.

La configuración para Hub2 es básicamente la misma que para Hub1 con los correspondientes cambios de dirección IP. La diferencia principal es que Hub2 también es un spoke (o cliente) de Hub1, lo que convierte a Hub1 en el hub principal y Hub2 en el hub secundario. Esto se hace para que Hub2 sea un vecino OSPF con Hub1 sobre el túnel mGRE. Como el Hub1 es el OSPF DR, debe tener una conexión directa con los demás routers OSPF por la interfaz mGRE (red NBMA). Sin el link directo entre Hub1 y Hub2, Hub2 no participaría en el ruteo OSPF cuando Hub1 también está activo. Cuando Hub1 no funcione, Hub2 será el OSPF DR para DMVPN (red NBMA). Cuando el Hub1 vuelva a funcionar, se hará cargo de ser el OSPF DR para la DMVPN.

Los routers detrás del Hub1 y el Hub2 utilizarán el Hub1 para enviar paquetes a las redes spoke porque el ancho de banda para la interfaz de túnel GRE se encuentra configurado para 1000 Kb/seg contra los 900 Kb/seg del Hub2. En contraste, los routers spoke enviarán paquetes para las redes detrás de los routers hub a ambos Hub1 y Hub2, dado que existe una sola interfaz de túnel mGRE en cada router spoke y habrá dos rutas con costos equivalentes. Si se utiliza el equilibrio de carga por paquete, esto puede causar paquetes defectuosos.

Router Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.11 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp map multicast 172.17.0.5
  ip nhrp map 10.0.0.2 172.17.0.5
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  ip nhrp nhs 10.0.0.2
  ip ospf network broadcast
  ip ospf priority 0
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address dhcp hostname Spoke1
 !
```

```
 interface Ethernet1
  ip address 192.168.1.1 255.255.255.0
 !
 router ospf 1
  network 10.0.0.0 0.0.0.255 area 1
  network 192.168.1.0 0.0.0.255 area 1
 !
```

Las diferencias en la configuración de los routers radiales son las siguientes:

- En la nueva configuración, la red radial está configurada con correspondencias NHRP estáticas para Hub2, y Hub2 es agregado como un servidor del salto siguiente.Original:

  ```
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp nhs 10.0.0.1
  ```

  Nuevo:

  ```
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp map multicast 172.17.0.5
  ip nhrp map 10.0.0.2 172.17.0.5
  ip nhrp nhs 10.0.0.1
  ip nhrp nhs 10.0.0.2
  ```

- Las áreas OSPF en los routers radiales se han cambiado al área 1.

Recuerde que al definir el mapeo NHR P estático y NHS en un router spoke para un concentrador, usted ejecutará el protocolo de ruteo dinámico a través de este túnel. Esto define al ruteo hub y spoke o a la red vecina. Tome en cuenta que el Hub2 es un hub para todos los radios y también es un radio para el Hub1. Esto facilita el diseño, la configuración y la modificación de redes radiales multicapa cuando se utiliza la solución DMVPN.

Router Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.12 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp map multicast 172.17.0.5
  ip nhrp map 10.0.0.2 172.17.0.5
```

```
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 ip nhrp nhs 10.0.0.2
 ip ospf network broadcast
 ip ospf priority 0
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke1
!
interface Ethernet1
 ip address 192.168.2.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
!
```

Router Spoke<n>

```
version 12.3
!
hostname Spoke<n>
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.<n+10> 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast 172.17.0.1
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.5
 ip nhrp map 10.0.0.2 172.17.0.5
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 ip nhrp nhs 10.0.0.2
 ip ospf network broadcast
 ip ospf priority 0
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke<x>
```

```
!
interface Ethernet1
 ip address 192.168.<n>.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.




!
```

En este punto, puede echar un vistazo a las tablas de ruteo, las tablas de mapeo NHRP y las conexiones IPsec en los routers Hub1, Hub2, Spoke1 y Spoke2 para ver las condiciones iniciales (justo después de que se activen los routers Spoke1 y Spoke2).

Cambios y condiciones iniciales

Información del router Hub1

```
Hub1#show ip route
      172.17.0.0/24 is subnetted, 1 subnets
 C       172.17.0.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 1 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 C    192.168.0.0/24 is directly connected, Ethernet1
 O    192.168.1.0/24 [110/2] via 10.0.0.11, 00:02:17,
Tunnel0
 O    192.168.2.0/24 [110/2] via 10.0.0.12, 00:02:17,
Tunnel0
 Hub1#show ip nhrp
 10.0.0.2/32 via 10.0.0.2, Tunnel0 created 1w3d, expire
00:03:15
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.17.0.5
 10.0.0.11/32 via 10.0.0.11, Tunnel0 created 1w3d,
expire 00:03:49
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.1.24
 10.0.0.12/32 via 10.0.0.12, Tunnel0 created 1w3d,
expire 00:04:06
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.2.75
 Hub1#show crypto engine connection active
  ID  Interface   IP-Address    State Algorithm
Encrypt Decrypt
    4 Ethernet0   172.17.0.1     set  HMAC_SHA+DES_56_CB
0       0
    5 Ethernet0   172.17.0.1     set  HMAC_SHA+DES_56_CB
0       0
    6 Ethernet0   172.17.0.1     set  HMAC_SHA+DES_56_CB
0       0
 3532 Tunnel0     10.0.0.1       set  HMAC_MD5+DES_56_CB
0     232
 3533 Tunnel0     10.0.0.1       set  HMAC_MD5+DES_56_CB
212       0
 3534 Tunnel0     10.0.0.1       set  HMAC_MD5+DES_56_CB
0      18
```

```
 3535 Tunnel0     10.0.0.1       set  HMAC_MD5+DES_56_CB
17       0
 3536 Tunnel0     10.0.0.1       set  HMAC_MD5+DES_56_CB
0        7
 3537 Tunnel0     10.0.0.1       set  HMAC_MD5+DES_56_CB
7        0
```

Información del router Hub2

```
Hub2#show ip route
      172.17.0.0/24 is subnetted, 1 subnets
 C       172.17.0.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 1 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 C    192.168.0.0/24 is directly connected, Ethernet1
 O    192.168.1.0/24 [110/2] via 10.0.0.11, 00:29:15,
Tunnel0
 O    192.168.2.0/24 [110/2] via 10.0.0.12, 00:29:15,
Tunnel0
 Hub2#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 1w3d, never
expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.1
 10.0.0.11/32 via 10.0.0.11, Tunnel0 created 1w3d,
expire 00:03:15
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.1.24
 10.0.0.12/32 via 10.0.0.12, Tunnel0 created 00:46:17,
expire 00:03:51
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.2.75
 Hub2#show crypto engine connection active
   ID Interface   IP-Address    State Algorithm
Encrypt Decrypt
    4 Ethernet0   171.17.0.5     set  HMAC_SHA+DES_56_CB
0        0
    5 Ethernet0   171.17.0.5     set  HMAC_SHA+DES_56_CB
0        0
    6 Ethernet0   171.17.0.5     set  HMAC_SHA+DES_56_CB
0        0
 3520 Tunnel0     10.0.0.2       set  HMAC_MD5+DES_56_CB
0      351
 3521 Tunnel0     10.0.0.2       set  HMAC_MD5+DES_56_CB
326        0
 3522 Tunnel0     10.0.0.2       set  HMAC_MD5+DES_56_CB
0      311
 3523 Tunnel0     10.0.0.2       set  HMAC_MD5+DES_56_CB
339        0
 3524 Tunnel0     10.0.0.2       set  HMAC_MD5+DES_56_CB
0       25
 3525 Tunnel0     10.0.0.2       set  HMAC_MD5+DES_56_CB
22         0
```

Información del router Spoke1

```
Spoke1#show ip route
      172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.1.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 1 subnets
 C       10.0.0.0 is directly connected, Tunnel0
```

```
 O IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:39:31,
Tunnel0
                     [110/11] via 10.0.0.2, 00:39:31,
Tunnel0
 C    192.168.1.0/24 is directly connected, Ethernet1
 O    192.168.2.0/24 [110/2] via 10.0.0.12, 00:37:58,
Tunnel0
 Spoke1#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 00:56:40,
never expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.1
 10.0.0.2/32 via 10.0.0.2, Tunnel0 created 00:56:40,
never expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.5
 Spoke1#show crypto engine connection active
  ID  Interface   IP-Address    State Algorithm
Encrypt Decrypt
    1 Ethernet0   172.16.1.24    set  HMAC_SHA+DES_56_CB
0       0
    2 Ethernet0   172.16.1.24    set  HMAC_SHA+DES_56_CB
0       0
 2010 Tunnel0     10.0.0.11      set  HMAC_MD5+DES_56_CB
0     171
 2011 Tunnel0     10.0.0.11      set  HMAC_MD5+DES_56_CB
185       0
 2012 Tunnel0     10.0.0.11      set  HMAC_MD5+DES_56_CB
0      12
 2013 Tunnel0     10.0.0.11      set  HMAC_MD5+DES_56_CB
13       0
```

Información del router Spoke 2

```
Spoke2#show ip route
      172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.2.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 1 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 O IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:57:56,
Tunnel0
                     [110/11] via 10.0.0.2, 00:57:56,
Tunnel0
 O    192.168.1.0/24 [110/2] via 10.0.0.11, 00:56:14,
Tunnel0
 C    192.168.2.0/24 is directly connected, Ethernet1
 Spoke2#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 5w6d, never
expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.1
 10.0.0.2/32 via 10.0.0.2, Tunnel0 created 6w6d, never
expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.5
 Spoke2#show crypto engine connection active
  ID  Interface   IP-Address    State Algorithm
Encrypt Decrypt
    2 Ethernet0   172.16.2.75    set  HMAC_SHA+DES_56_CB
0       0
    3 Ethernet0   172.16.2.75    set  HMAC_SHA+DES_56_CB
0       0
```

```
 3712 Tunnel0     10.0.0.12      set  HMAC_MD5+DES_56_CB
0     302
 3713 Tunnel0     10.0.0.12      set  HMAC_MD5+DES_56_CB
331       0
 3716 Tunnel0     10.0.0.12      set  HMAC_MD5+DES_56_CB
0     216
 3717 Tunnel0     10.0.0.12      set  HMAC_MD5+DES_56_CB
236       0
```

Se deben considerar varios temas interesantes con respecto a las tablas de ruteo en Hub1, Hub2, Spoke1 y Spoke2:

- Ambos routers de eje de conexión tienen rutas de costo equivalentes a las redes detrás de los routers radiales.Hub1:
  ```
  O     192.168.1.0/24 [110/2] via 10.0.0.11, 00:02:17, Tunnel0
  O     192.168.2.0/24 [110/2] via 10.0.0.12, 00:02:17, Tunnel0
  ```
  Hub2:
  ```
  O     192.168.1.0/24 [110/2] via 10.0.0.11, 00:29:15, Tunnel0
  O     192.168.2.0/24 [110/2] via 10.0.0.12, 00:29:15, Tunnel0
  ```
  Esto significa que Hub1 y Hub2 promocionarán el mismo costo para las redes detrás de los routers spoke hacia los routers en las redes detrás de los routers hub. Por ejemplo, la tabla de ruteo en un router, R2, que está conectado directamente a la LAN 192.168.0.0/24, sería de la siguiente manera:R2:
  ```
  O     IA 192.168.1.0/24 [110/12] via 192.168.0.1, 00:00:26, Ethernet1/0/3
                          [110/12] via 192.168.0.2, 00:00:27, Ethernet1/0/3O
  O     IA 192.168.2.0/24 [110/12] via 192.168.0.1, 00:00:27, Ethernet1/0/3
                          [110/12] via 192.168.0.2, 00:00:27, Ethernet1/0/3
  ```
- Los routers radiales tienen rutas de costo equivalente por medio de ambos routers hub a la red debajo de los routers hub.Spoke1:
  ```
  O     IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:39:31, Tunnel0
                          [110/11] via 10.0.0.2, 00:39:31, Tunnel0
  ```
  Spoke2
  ```
  O     IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:57:56, Tunnel0
                          [110/11] via 10.0.0.2, 00:57:56, Tunnel0
  ```
  Si los routers spoke realizan un equilibrio de carga por paquete, entonces usted podría obtener paquetes fuera de servicio.

Para evitar hacer un ruteo asimétrico o equilibrio de carga por paquete entre los links de los dos ejes de conexión, debe configurar el protocolo de ruteo con preferencia de un trayecto de radio a eje de conexión en ambas direcciones. Si quiere que el Hub1 sea el principal y el Hub 2 el de respaldo, puede configurar el costo de OSPF en las interfaces del túnel del hub para que sean diferentes.

Hub1:

```
interface tunnel0
...
ip ospf cost 10
...
```

Hub2:

```
interface tunnel0
...
ip ospf cost 20
...
```

Ahora la rutas se ven de la siguiente manera:

Hub1:

```
O     192.168.1.0/24 [110/11] via 10.0.0.11, 00:00:28, Tunnel0
O     192.168.2.0/24 [110/11] via 10.0.0.12, 00:00:28, Tunnel0
```

Hub2:

```
O     192.168.1.0/24 [110/21] via 10.0.0.11, 00:00:52, Tunnel0
O     192.168.2.0/24 [110/21] via 10.0.0.12, 00:00:52, Tunnel0
```

R2:

```
O     IA 192.168.1.0/24 [110/31] via 192.168.0.1, 00:01:06, Ethernet1/0/3
O     IA 192.168.2.0/24 [110/31] via 192.168.0.1, 00:01:06, Ethernet1/0/3
```

Los dos routers hub ahora presentan diferentes costos en las rutas para las redes detrás de los routers spoke. Esto significa que se preferirá Hub1 para reenviar tráfico a los routers radiales, como se puede ver en el router R2. Esto se ocupará del problema de ruteo asimétrico descrito en la primera viñeta anterior.

El ruteo asimétrico en la otra dirección, tal como se describió arriba en la segunda viñeta, aún permanece allá. Cuando utiliza OSPF como protocolo de ruteo dinámico, puede solucionar esto con una solución alternativa usando la **distancia ...** bajo **router ospf 1** en los radios para preferir las rutas aprendidas a través de Hub1 sobre las rutas aprendidas a través de Hub2.

Spoke1:

```
router ospf 1
 distance 111 10.0.0.2 0.0.0.0 1
access-list 1 permit any
```

Spoke2

```
router ospf 1
 distance 111 10.0.0.2 0.0.0.0 1
access-list 1 permit any
```

Ahora la rutas se ven de la siguiente manera:

Spoke1:

```
O     192.168.0.0/24 [110/11] via 10.0.0.1, 00:00:06, Tunnel0
```

Spoke2

```
O     192.168.1.0/24 [110/11] via 10.0.0.1, 00:00:10, Tunnel0
```

La configuración del ruteo anterior brindará protección contra el ruteo asimétrico y, al mismo tiempo, admitirá las fallas a Hub2 si Hub1 deja de funcionar. Significa que cuando los dos ejes de conexión están activos, sólo se utiliza el Hub1. Si desea usar ambos ejes de conexión equilibrando los radios en los ejes de conexión, con protección contra fallas y sin ruteo asimétrico, entonces la configuración de ruteo puede ser compleja, especialmente si se usa OSPF. Por este motivo, la siguiente configuración de eje de conexión dual con DMVPN dual puede ser una mejor

opción.

‘Hub dual – Esquema DMPVN dual’

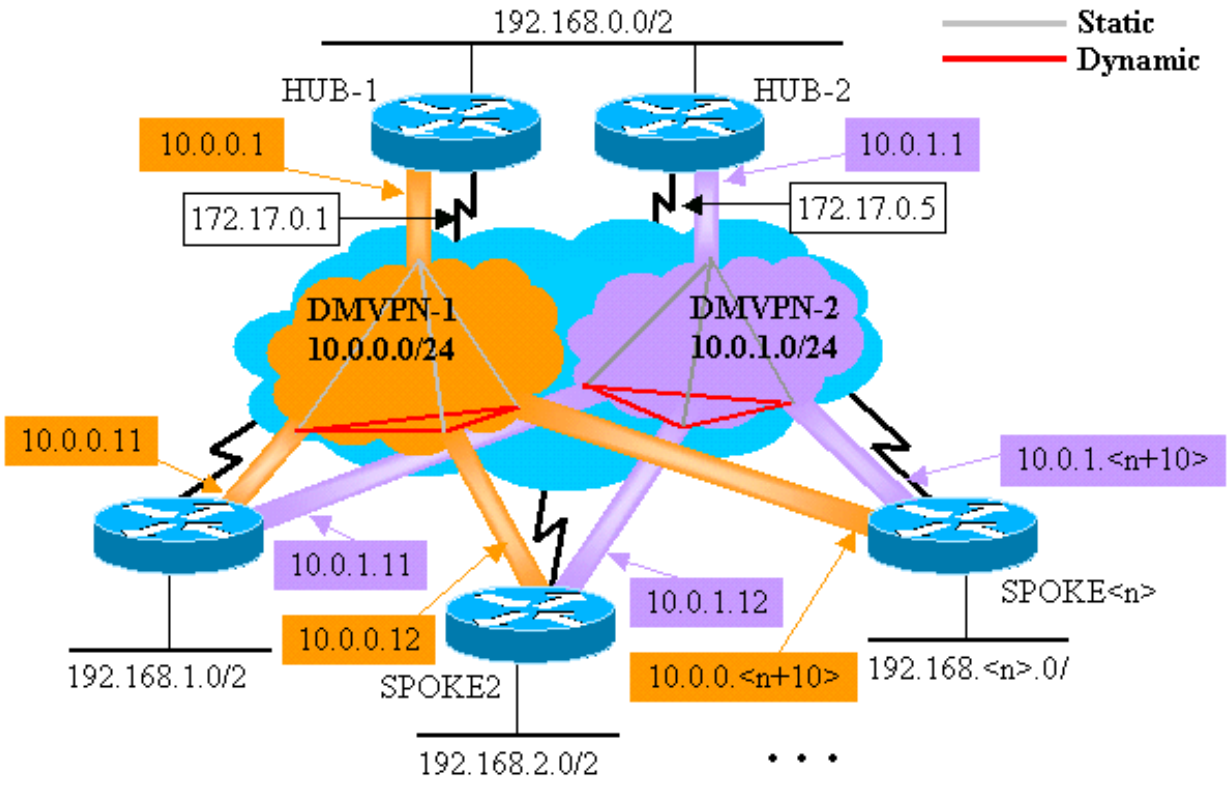
El hub dual con un diseño dual DMVPN es apenas más difícil de configurar, pero le brinda un mejor control del ruteo a través de DMVPN. La idea es tener dos "nubes" DMVPN independientes. Cada eje de conexión (dos en este caso) está conectado a una subred DMVPN (“nube”) y los radios están conectados a ambas subredes (“nubes”). Dado que los routers spoke son vecinos de ruteo de ambos routers hub en las dos interfaces de túnel GRE, puede usar diferencias en la configuración de la interfaz (como ancho de banda, costo y retraso) para modificar las métricas del protocolo de ruteo dinámico de modo que prefiera un hub sobre el otro hub cuando ambos estén activos.

Nota: Por lo general, el problema anterior sólo es relevante si los routers hub están ubicados de forma conjunta. Cuando no están ubicados de manera conjunta, el ruteo dinámico probablemente elija el router de hub apropiado, incluso si la red de destino puede alcanzarse a través de cualquier router hub.

Puede usar las interfaces de túnel p-pGRE o mGRE en los routers radiales. Varias interfaces p-pGRE en un router spoke pueden utilizar el mismo **origen de túnel ...** Dirección IP, pero las interfaces mGRE múltiples en un router spoke deben tener un **origen de túnel** único **...** Dirección IP. Esto es porque cuando se inicia IPsec, el primer paquete es un paquete ISAKMP que necesita asociarse con uno de los túneles mGRE. El paquete ISAKMP sólo tiene la dirección IP de destino (dirección de entidad par IPsec remoto) con la que realiza esta asociación. Esta dirección se compara con el **origen del túnel ...** , pero dado que ambos túneles tienen el mismo **origen de túnel ...** , la primera interfaz de túnel mGRE siempre coincide. Quiere decir que los paquetes de datos entrantes de multidifusión pueden estar asociados con la interfaz mGRE equivocada, lo que rompe el protocolo de ruteo dinámico.

Los paquetes GRE en sí mismos no tienen este problema ya que tienen la **clave de túnel ...** valor para diferenciar entre las dos interfaces mGRE. A partir de Cisco IOS Software Releases 12.3(5) y 12.3(7)T, se introdujo un parámetro adicional para superar esta limitación: **protección de túnel....compartida**. La palabra clave **shared** indica que varias interfaces mGRE utilizarán el cifrado IPSec con la misma dirección IP de origen. Si tiene una versión anterior, puede utilizar túneles p-pGRE en este hub dual con diseño DMVPN dual. En el caso del túnel p-pGRE, tanto el **origen del túnel ...** y el **destino del túnel ...** Las direcciones IP se pueden utilizar para la coincidencia. Para este ejemplo, los túneles p-pGRE se utilizarán en este hub dual con diseño DMVPN dual y no se utilizarán el calificador **compartido**.

‘Hub dual – Esquema DMPVN dual’



Los siguientes cambios resaltados están relacionados con las configuraciones dinámicas multipunto de red radial, ilustradas anteriormente en este documento.

Router Hub1

```
version 12.3
 !
 hostname Hub1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  no ip split-horizon eigrp 1
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
```

```
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.252
!
interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
 no auto-summary
!
```

Router del Hub2

```
version 12.3
!
hostname Hub2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.1.1 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100001
 ip nhrp holdtime 600
 no ip split-horizon eigrp 1
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100001
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 172.17.0.5 255.255.255.252
!
interface Ethernet1
 ip address 192.168.0.2 255.255.255.0
!
router eigrp 1
 network 10.0.1.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
 no auto-summary
!
```

En este caso, las configuraciones de Hub1 y Hub2 son similares. La diferencia principal es que cada uno es el hub de una DMVPN diferente. Cada DMVPN utiliza una diferencia:

- Subred IP (10.0.0.0/24, 10.0.0.1/24)
- Id de la red NHRP (100000, 100001)
- Clave de túnel (100000, 100001)

El protocolo de ruteo dinámico ha sido conmutado de OSPF a EIGRP, porque es más fácil configurar y administrar una red NBMA usando EIGRP, como se describe más adelante en este documento.

Router Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.11 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Tunnel1
  bandwidth 1000
  ip address 10.0.1.11 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.1.1 172.17.0.5
  ip nhrp network-id 100001
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.1.1
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.5
  tunnel key 100001
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address dhcp hostname Spoke1
 !
 interface Ethernet1
  ip address 192.168.1.1 255.255.255.0
 !
 router eigrp 1
```

```
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
 no auto-summary
!
```

Cada uno de los routers spoke está configurado con dos interfaces de túnel p-pGRE, una en cada uno de los dos DMVPN. La **dirección IP ...**, **ip nhrp network-id ...**, **clave de túnel ...** y **destino del túnel ...** se utilizan para diferenciar entre los dos túneles. El protocolo de ruteo dinámico, EIGRP, se ejecuta sobre subredes de túnel p-pGRE y se utiliza para seleccionar una interfaz p-pGRE (DMVPN) sobre la otra.

Router Spoke2

```
version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.12 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Tunnel1
 bandwidth 1000
 ip address 10.0.1.12 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.1.1 172.17.0.5
 ip nhrp network-id 100001
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.1.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.5
 tunnel key 100001
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke2
```

```
 !
 interface Ethernet1
  ip address 192.168.2.1 255.255.255.0
 !
 router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 10.0.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  no auto-summary
 !
```

Router Spoke<n>

```
version 12.3
 !
 hostname Spoke<n>
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.




  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Tunnel1
  bandwidth 1000
  ip address 10.0.1.




  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.1.1 172.17.0.5
  ip nhrp network-id 100001
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.1.1
  delay 1000
  tunnel source Ethernet0
```

```
 tunnel destination 172.17.0.5
 tunnel key 100001
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke<x>
!
interface Ethernet1
 ip address 192.168.<n>.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.<n>.0 0.0.0.255
 no auto-summary
!
```

En este punto, echemos un vistazo a las tablas de ruteo, las tablas de mapeo NHRP y las conexiones IPsec en los routers Hub1, Hub2, Spoke1 y Spoke2 para ver las condiciones iniciales (justo después de que se activen los routers Spoke1 y Spoke2).

Cambios y condiciones iniciales

Información del router Hub1

```
Hub1#show ip route
      172.17.0.0/30 is subnetted, 1 subnets
 C       172.17.0.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 2 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 D       10.0.1.0 [90/2611200] via 192.168.0.2,
00:00:46, Ethernet1
 C    192.168.0.0/24 is directly connected, Ethernet1
 D    192.168.1.0/24 [90/2841600] via 10.0.0.11,
00:00:59, Tunnel0
 D    192.168.2.0/24 [90/2841600] via 10.0.0.12,
00:00:34, Tunnel0
 Hub1#show ip nhrp
 10.0.0.12/32 via 10.0.0.12, Tunnel0 created 23:48:32,
expire 00:03:50
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.2.75
 10.0.0.11/32 via 10.0.0.11, Tunnel0 created 23:16:46,
expire 00:04:45
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.1.24
 Hub1#show crypto engine connection active
   ID Interface   IP-Address    State  Algorithm
Encrypt  Decrypt
   15 Ethernet0   172.17.63.18   set
HMAC_SHA+DES_56_CB      0        0
   16 Ethernet0   10.0.0.1       set
HMAC_SHA+DES_56_CB      0        0
 2038 Tunnel0     10.0.0.1       set
HMAC_MD5+DES_56_CB      0      759
 2039 Tunnel0     10.0.0.1       set
HMAC_MD5+DES_56_CB    726        0
 2040 Tunnel0     10.0.0.1       set
HMAC_MD5+DES_56_CB      0       37
 2041 Tunnel0     10.0.0.1       set
```

```
HMAC_MD5+DES_56_CB     36         0
```

Información del router Hub2

```
Hub2#show ip route
      172.17.0.0/30 is subnetted, 1 subnets
 C       172.17.0.4 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 2 subnets
 D       10.0.0.0 [90/2611200] via 192.168.0.1,
00:12:22, Ethernet1
 C       10.0.1.0 is directly connected, Tunnel0
 C    192.168.0.0/24 is directly connected, Ethernet1
 D    192.168.1.0/24 [90/2841600] via 10.0.1.11,
00:13:24, Tunnel0
 D    192.168.2.0/24 [90/2841600] via 10.0.1.12,
00:12:11, Tunnel0
 Hub2#show ip nhrp
 10.0.1.12/32 via 10.0.1.12, Tunnel3 created 06:03:24,
expire 00:04:39
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.2.75
 10.0.1.11/32 via 10.0.1.11, Tunnel3 created 23:06:47,
expire 00:04:54
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.1.24
 Hub2#show crypto engine connection active
   ID Interface   IP-Address    State  Algorithm
Encrypt  Decrypt
    4 Ethernet0   171.17.0.5     set
HMAC_SHA+DES_56_CB      0         0
    6 Ethernet0   171.17.0.5     set
HMAC_SHA+DES_56_CB      0         0
 2098 Tunnel0     10.0.1.1       set
HMAC_MD5+DES_56_CB      0       722
 2099 Tunnel0     10.0.1.1       set
HMAC_MD5+DES_56_CB    690         0
 2100 Tunnel0     10.0.1.1       set
HMAC_MD5+DES_56_CB      0       268
 2101 Tunnel0     10.0.1.1       set
HMAC_MD5+DES_56_CB    254         0
```

Información del router Spoke1

```
Spoke1#show ip route
      172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.1.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 1 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 C       10.0.1.0 is directly connected, Tunnel1
 D    192.168.0.0/24 [90/2841600] via 10.0.1.1,
00:26:30, Tunnel1
                     [90/2841600] via 10.0.0.1,
00:26:30, Tunnel0
 C    192.168.1.0/24 is directly connected, Ethernet1
 D    192.168.2.0/24 [90/3097600] via 10.0.1.1,
00:26:29, Tunnel1
                     [90/3097600] via 10.0.0.1,
00:26:29, Tunnel0
 Spoke1#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 23:25:46,
never expire
   Type: static, Flags: authoritative
```

```
   NBMA address: 172.17.0.1
 10.0.1.1/32 via 10.0.1.1, Tunnel1 created 23:24:40,
never expire
   Type: static, Flags: authoritative
   NBMA address: 172.17.0.5
 Spoke1#show crypto engine connection active
   ID Interface   IP-Address    State  Algorithm
Encrypt  Decrypt
   16 Ethernet0   172.16.1.24    set
HMAC_SHA+DES_56_CB      0        0
   18 Ethernet0   172.16.1.24    set
HMAC_SHA+DES_56_CB      0        0
 2118 Tunnel0     10.0.0.11      set
HMAC_MD5+DES_56_CB      0      181
 2119 Tunnel0     10.0.0.11      set
HMAC_MD5+DES_56_CB    186        0
 2120 Tunnel1     10.0.1.11      set
HMAC_MD5+DES_56_CB      0      105
 2121 Tunnel1     10.0.1.11      set
HMAC_MD5+DES_56_CB    110        0
```

Información del router Spoke 2

```
Spoke2#show ip route
      172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.2.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 2 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 C       10.0.1.0 is directly connected, Tunnel1
 D    192.168.0.0/24 [90/2841600] via 10.0.1.1,
00:38:04, Tunnel1
                     [90/2841600] via 10.0.0.1,
00:38:04, Tunnel0
 D    192.168.1.0/24 [90/3097600] via 10.0.1.1,
00:38:02, Tunnel1
                     [90/3097600] via 10.0.0.1,
00:38:02, Tunnel0
 C    192.168.2.0/24 is directly connected, Ethernet1
 Spoke2#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 1d02h, never
expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.1
 10.0.1.1/32 via 10.0.1.1, Tunnel1 created 1d02h, never
expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.5
 Spoke2#show crypto engine connection active
   ID Interface   IP-Address    State  Algorithm
Encrypt  Decrypt
    8 Ethernet0   172.16.2.75    set
HMAC_SHA+DES_56_CB      0        0
    9 Ethernet0   172.16.2.75    set
HMAC_SHA+DES_56_CB      0        0
 2036 Tunnel0     10.0.0.12      set
HMAC_MD5+DES_56_CB      0      585
 2037 Tunnel0     10.0.0.12      set
HMAC_MD5+DES_56_CB    614        0
 2038 Tunnel1     10.0.1.12      set
HMAC_MD5+DES_56_CB      0      408
 2039 Tunnel1     10.0.1.12      set
HMAC_MD5+DES_56_CB    424        0
```

De nuevo, hay varios puntos interesantes que deben tenerse en cuenta acerca de las tablas de ruteo en el Hub1, Hub2, Spoke1 y Spoke2:

- Ambos routers de eje de conexión tienen rutas de costo equivalentes a las redes detrás de los routers radiales.Hub1:
  ```
  D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:00:59, Tunnel0
  D    192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:00:34, Tunnel0
  ```
  Hub2:
  ```
  D    192.168.1.0/24 [90/2841600] via 10.0.1.11, 00:13:24, Tunnel0
  D    192.168.2.0/24 [90/2841600] via 10.0.1.12, 00:12:11, Tunnel0
  ```
  Esto significa que Hub1 y Hub2 promocionarán el mismo costo para las redes detrás de los routers spoke hacia los routers en las redes detrás de los routers hub. Por ejemplo, la tabla de ruteo en un router, R2, que está conectado directamente a la LAN 192.168.0.0/24, sería de la siguiente manera:R2:
  ```
  D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:51:51, Ethernet1/0/3
                              [90/2867200] via 192.168.0.2, 00:51:51, Ethernet1/0/3
  D    192.168.2.0/24 [90/2867200] via 192.168.0.2, 00:52:43, Ethernet1/0/3
                      [90/2867200] via 192.168.0.1, 00:52:43, Ethernet1/0/3
  ```
- Los routers radiales tienen rutas de costo equivalente por medio de ambos routers hub a la red debajo de los routers hub.Spoke1:
  ```
  D    192.168.0.0/24 [90/3097600] via 10.0.1.1, 00:26:30, Tunnel1
                              [90/3097600] via 10.0.0.1, 00:26:30, Tunnel0
  ```
  Spoke2
  ```
  D    192.168.0.0/24 [90/3097600] via 10.0.1.1, 00:38:04, Tunnel1
                              [90/3097600] via 10.0.0.1, 00:38:04, Tunnel0
  ```
  Si los routers radiales están haciendo balanceo de carga por paquete, entonces podría obtener paquetes fuera de servicio.

Para evitar hacer un ruteo asimétrico o equilibrio de carga por paquete entre los links de los dos ejes de conexión, debe configurar el protocolo de ruteo con preferencia de un trayecto de radio a eje de conexión en ambas direcciones. Si desea que el Hub1 sea el principal y el Hub2 el de respaldo, puede establecer que el retraso en las interfaces de túnel hub sea diferente.

Hub1:

```
interface tunnel0
...
delay 1000
...
```

Hub2:

```
interface tunnel0
...
delay 1050
...
```

Nota: En este ejemplo, se agregó 50 al retraso en la interfaz de túnel en el Hub2 porque es menor que el retraso en la interfaz Ethernet1 entre los dos hubs (100). Al hacer esto, el Eje de conexión 2 aún reenviará paquetes directamente a los routers radiales, pero anunciará una ruta menos deseable que el Eje de conexión 1 a los routers detrás del Eje de conexión 1 y el Eje de conexión 2. Si el retraso se incrementó en más de 100, el Hub2 reenviaría paquetes para los routers radiales a través del Hub1 a través de la interfaz Ethernet1, aunque los routers detrás del Hub1 y el Hub2 seguirían prefiriendo correctamente el Hub-1 para enviar paquetes a los routers radiales.

Ahora la rutas se ven de la siguiente manera:

Hub1:

```
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:01:11, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:01:11, Tunnel0
```

Hub2:

```
D    192.168.1.0/24 [90/2854400] via 10.0.1.11, 00:00:04, Tunnel0
D    192.168.2.0/24 [90/2854400] via 10.0.1.12, 00:00:04, Tunnel0
```

R2:

```
D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:02:18, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.1, 00:02:18, Ethernet1/0/3
```

Los dos routers de eje de conexión tienen diferentes costos para los routers de la red detrás de los routers radiales; por lo tanto, en este caso, Hub1 será el preferido para reenviar el tráfico a los routers radiales, como se puede observar en R2. Esto se ocupa del problema descrito en la primera viñeta anterior.

El problema descrito en la segunda viñeta anterior sigue presente, pero dado que tiene dos interfaces de túnel p-pGRE, puede establecer el **retardo ...** en las interfaces de túnel por separado para cambiar la métrica EIGRP para las rutas aprendidas del Hub1 frente al Hub2.

Spoke1:

```
interface tunnel0
  delay 1000
interface tunnel1
  delay 1050
```

Spoke2

```
interface tunnel0
  delay 1000
interface tunnel1
  delay 1050
```

Ahora la rutas se ven de la siguiente manera:

Spoke1:

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:15:44, Tunnel0
D    192.168.2.0/24 [90/3097600] via 10.0.0.1, 00:15:44, Tunnel0
```

Spoke2

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:13:54, Tunnel0
D    192.168.1.0/24 [90/3097600] via 10.0.0.1, 00:13:54, Tunnel0
```

La configuración del ruteo anterior brindará protección contra el ruteo asimétrico y, al mismo tiempo, admitirá las fallas a Hub2 si Hub1 deja de funcionar. Significa que cuando los dos ejes de conexión están activos, sólo se utiliza el Hub1.

Si desea utilizar ambos hubs al equilibrar los radios a través de los hubs, con protección contra

fallas y sin ruteo asimétrico, entonces la configuración de ruteo es más compleja, pero puede hacerlo cuando utilice EIGRP. Para lograr esto, establezca el **retardo ...** en las interfaces de túnel de los routers hub de nuevo a ser iguales y luego utilice el comando **offset-list <acl> out <offset> <interface>** en los routers spoke para aumentar la métrica EIGRP para las rutas anunciadas en las interfaces de túnel GRE al hub de respaldo. El **retraso** desigual**...** entre las interfaces Tunnel0 y Tunnel1 en el spoke todavía se utiliza, por lo que el router spoke preferirá su router hub primario. Los cambios en los routers spoke son los siguientes.

Router Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 ...
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.11 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Tunnel1
  bandwidth 1000
  ip address 10.0.1.11 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.1.1 172.17.0.5
  ip nhrp network-id 100001
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.1.1
  delay 1500
  tunnel source Ethernet0
  tunnel destination 172.17.0.5
  tunnel key 100001
  tunnel protection ipsec profile vpnprof
 !
 ...
 !
 router eigrp 1
  offset-list 1 out 12800 Tunnel1
  network 10.0.0.0 0.0.0.255
  network 10.0.1.0 0.0.0.255
  network 192.168.1.0
  distribute-list 1 out
  no auto-summary
 !
 access-list 1 permit 192.168.1.0
 !
```

Router Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 ...
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.12 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1500
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Tunnel1
  bandwidth 1000
  ip address 10.0.1.12 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.1.1 172.17.0.5
  ip nhrp network-id 100001
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.1.1
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.5
  tunnel key 100001
  tunnel protection ipsec profile vpnprof
 !
 ...
 !
 router eigrp 1
  offset-list 1 out 12800 Tunnel1
  network 10.0.0.0 0.0.0.255
  network 10.0.1.0 0.0.0.255
  network 192.168.2.0
  distribute-list 1 out
  no auto-summary
 !
 access-list 1 permit 192.168.2.0
 !
```

Nota: El valor de desplazamiento de 12800 (50*256) se agregó a la métrica EIGRP porque es menor que 25600 (100*256). Este valor (25600) es lo que se le agrega a la métrica EIGRP para rutas aprendidas entre los routers hub. Al utilizar 12800 en el comando **offset-list**, el router hub de respaldo reenviará paquetes directamente a los routers radiales, en lugar de reenviar estos paquetes a través de Ethernet para pasar a través del router hub primario para esos radios. La métrica en las rutas notificadas por los routers de eje de conexión será aún de tal manera que el router de eje de conexión principal correcto la preferirá. Recuerde que la mitad de los radios tienen al Eje 1 como su router principal y la otra mitad al Eje 2 como su router principal.

Nota: Si el valor de desplazamiento se incrementó en más de 25600 (100*256), los hubs reenviarían paquetes para la mitad de los routers radiales a través del otro hub a través de la

interfaz Ethernet1, aunque los routers detrás de los hubs seguirían prefiriendo el hub correcto para enviar paquetes a los routers radiales.

Nota: El comando **distribute-list 1 out** también se agregó, ya que es posible que las rutas aprendidas de un router hub a través de una interfaz de túnel en un spoke puedan ser anunciadas nuevamente al otro hub a través del otro túnel. La **lista de distribución...** garantiza que el router spoke sólo pueda anunciar sus propias rutas.

Nota: Si prefiere controlar los anuncios de ruteo en los routers hub en lugar de en los routers spoke , los comandos **offset-list <acl1> en <value> <interface>** y **distribute-list <acl2> en** se pueden configurar en los routers hub en lugar de en los radios. La <acl2> lista de acceso enumeraría las rutas de detrás de todos los spokes y la <acl1> lista de acceso enumeraría solamente las rutas de detrás de spokes donde otro router hub será el hub principal.

Con estos cambios, las rutas se ven de la siguiente manera:

Hub1:

```
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:12:11, Tunnel2
D    192.168.2.0/24 [90/2854400] via 10.0.0.12, 00:13:24, Tunnel2
```

Hub2:

```
D    192.168.1.0/24 [90/2854400] via 10.0.1.11, 00:09:58, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.10.1.12, 00:11:11, Tunnel0
```

R2:

```
D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:13:13, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.2, 00:14:25, Ethernet1/0/3
```

Spoke1:

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:16:12, Tunnel0
```

Spoke2

```
D    192.168.0.0/24 [90/2841600] via 10.0.1.1, 00:18:54, Tunnel1
```

Conclusión

La solución DMVPN proporciona la siguiente funcionalidad para ampliar mejor las redes VPN IPsec grandes y pequeñas.

- DMVPN permite una mejor escalabilidad en malla completa o en VPN IPsec de malla parcial.Es especialmente útil cuando el tráfico de radio a radio es esporádico (por ejemplo, cada radio no envía constantemente datos a cada otro spoke). Permite a cualquier radio enviar datos directamente a cualquier otro spoke, siempre que haya conectividad IP directa entre los radios.
- DMVPN admite nodos IPsec con direcciones asignadas dinámicamente (como cable, ISDN y DSL).Esto se aplica tanto a hub y spoke como a redes de interconexión. Es posible que DMVPN requiera el link eje de conexión a radio para estar activo constantemente.

- DMVPN simplifica la incorporación de nodos VPN.Cuando agregue un nuevo router radial, sólo tiene que configurar el router radial y conectarlo a la red (aunque, es posible que necesite agregar la información de la autorización ISAKMP para la nueva radio en el eje de conexión). El hub aprenderá dinámicamente sobre el nuevo spoke y el protocolo de ruteo dinámico propagará el ruteo al hub y a todos los demás radios.
- DMVPN reduce el tamaño de la configuración necesaria en todos los routers de la VPN.Este también es el caso para las redes VPN GRE+IPsec hub y spoke solamente.
- DMVPN utiliza GRE y, por lo tanto, admite el tráfico de ruteo dinámico y de multidifusión de IP en la VPN.Esto significa que se puede utilizar un protocolo de ruteo dinámico y que el protocolo puede admitir "concentradores" redundantes. También se admiten las aplicaciones de multidifusión.
- DMVPN admite la tunelización dividida en los radios.

Información Relacionada

- Dynamic Multipoint VPN (DMVPN)
- Página de soporte de IPSec
- Soporte Técnico - Cisco Systems