Configuración de BGP sobre DMVPN Fase 3

Contenido

Introducción

Este documento describe la configuración y el funcionamiento de la fase 3 de DMVPN mediante BGP, incluida la resolución de problemas por capas para IPsec sobre túneles DMVPN.

Prerequisites

Para los comandos configuration y debug de este documento, necesita dos routers Cisco que ejecuten Cisco IOS® Release 15.3(3)M o posterior. En general, una VPN dinámica multipunto (DMVPN) básica de fase 3 requiere Cisco IOS versión 12.4(6)T, aunque las funciones y depuraciones que se muestran en este documento no son totalmente compatibles.

Requirements

Cisco recomienda tener conocimientos básicos sobre estos temas:

- IKEV1/IKEV2 e IPsec
- Componentes DMVPN:

- Protocolo de resolución de próximo salto (NHRP): Crea una base de datos de asignación distribuida (NHRP) de todos los túneles del spoke a direcciones reales (de interfaz pública)

- Interfaz de túnel de encapsulación de routing genérico multipunto (mGRE): Interfaz única de encapsulación de routing genérico (GRE) para admitir varios túneles GRE/IPsec, simplifica el tamaño y la complejidad de la configuración y admite la creación dinámica de túneles
- Protección de túnel IPsec: Crea y aplica dinámicamente políticas de cifrado
- Ruteo: Redes dinámicas; se admiten casi todos los protocolos de routing (protocolo de routing de gateway interior mejorado (EIGRP), protocolo de información de routing (RIP), ruta de acceso más corta primero (OSPF), BGP y ODR)

Componentes Utilizados

La información de este documento se basa en los Cisco ASR1000 Series Aggregation Services Routers, versión 17.6.5(MD).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

¿Qué es DMVPN?

DMVPN es una solución de software de Cisco IOS para crear VPN IPsec+GRE de forma sencilla, dinámica y escalable. Se trata de una solución para crear una red VPN con varios sitios sin tener que configurar todos los dispositivos de forma estática. Se trata de una red radial en la que los radios pueden comunicarse entre sí directamente sin tener que pasar por el hub. El cifrado se admite a través de IPsec, lo que convierte a DMVPN en una opción popular para conectar diferentes sitios mediante conexiones de Internet normales.

¿Cómo funciona DMVPN?

- Los radios crean un túnel GRE/IPsec permanente dinámico hacia el hub, pero no hacia otros radios. Se registran como clientes del servidor NHRP (hub).
- Cuando un spoke necesita enviar un paquete a una subred (privada) de destino detrás de otro spoke, consulta a través de NHRP la dirección real (externa) del spoke de destino.
- Ahora, el spoke de origen puede iniciar un túnel GRE/IPsec dinámico al spoke de destino (porque conoce la dirección de peer).
- El túnel dinámico de radio a radio se crea a través de la interfaz mGRE.
- Cuando el tráfico cesa, se elimina el túnel de radio a radio.

¿Cuáles son los diferentes tipos de DMVPN?

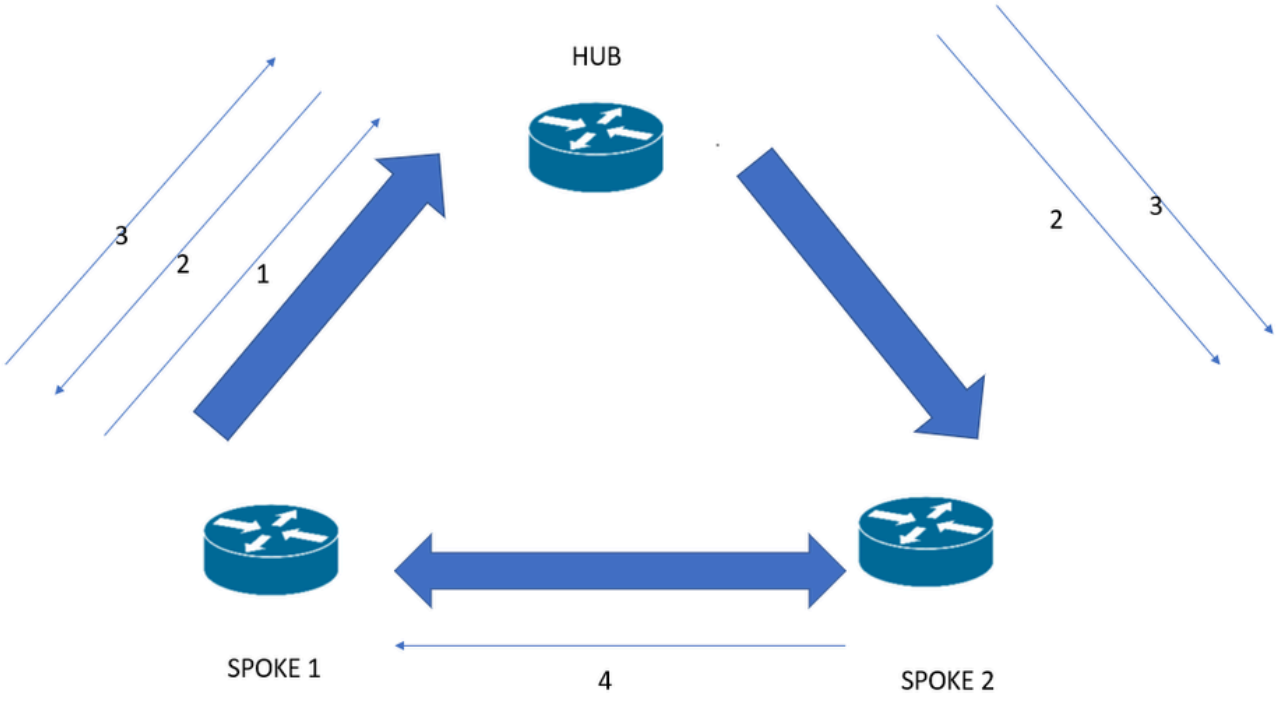
1. Fase I de DMVPN: Esta fase implica una única interfaz mGRE en el hub, y todos los spokes siguen siendo túneles estáticos, por lo que no obtiene ninguna conectividad dinámica de radio a radio.
2. DMVPN Fase II: Esta fase implica que cada sitio se configure con una interfaz mGRE para

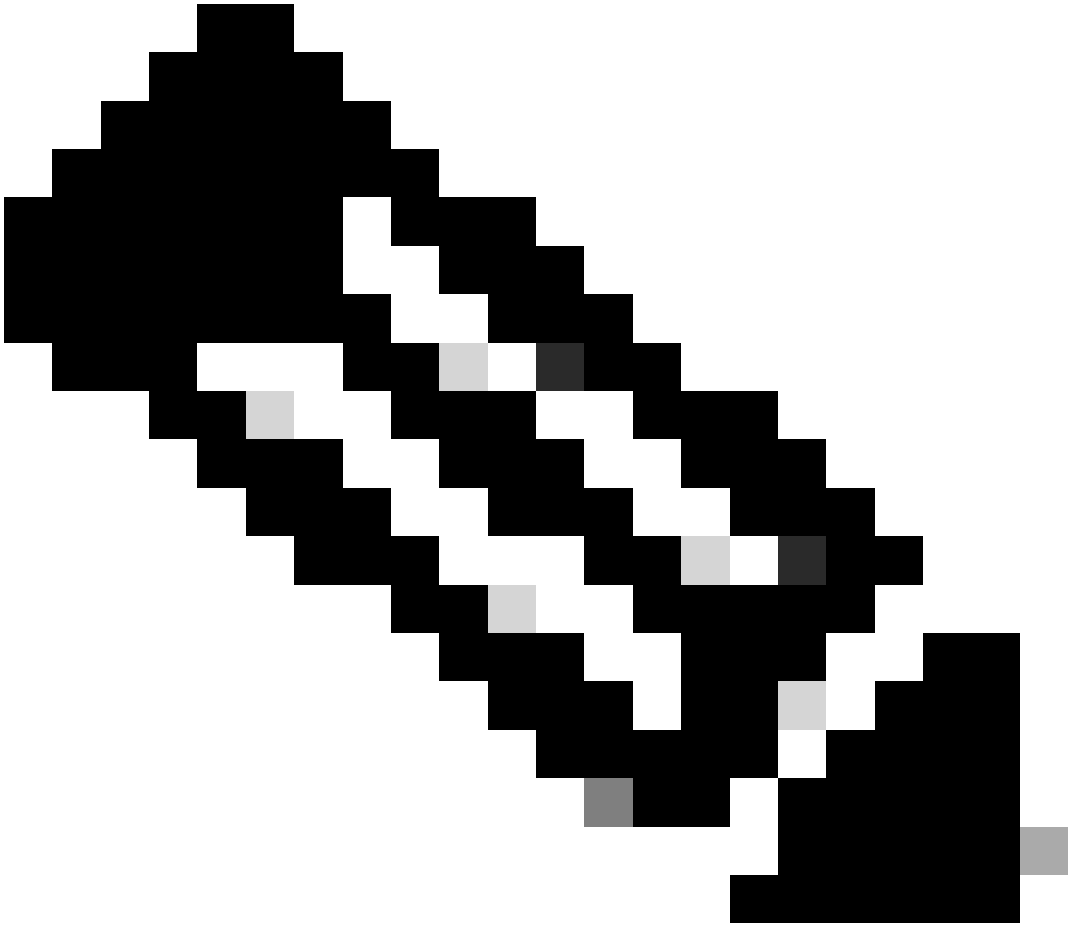
que obtenga su conectividad dinámica de radio a radio.

3. DMVPN Fase III: esta fase amplía la escalabilidad de la red DMVPN. Esto implica resumir en la nube DMVPN. Junto con la configuración de redirecciones NHRP y conmutación de accesos directos NHRP. Los redireccionamientos NHRP indican al origen que busque una mejor trayectoria hacia el destino al que está tratando de llegar. Los accesos directos NHRP permiten que DMVPN conozca otras redes situadas detrás de otros routers DMVPN.

Flujo de tráfico para la fase 3 de DMVPN

1. El paquete se envía desde la red 1 de Spoke a las 2 redes de Spoke a través del concentrador (según la tabla de routing).
2. Hub enruta el paquete a Spoke2 pero envía paralelamente el mensaje de redirección NHRP a Spoke1 que contiene información sobre la trayectoria subóptima a Spoke2 y la IP de túnel de Spoke2.
3. Spoke1 envía la solicitud de resolución NHRP de la dirección IP de acceso múltiple sin difusión (NBMA) 2 de Spoke al servidor de próximo salto (NHS) con la IP de destino del túnel 2 de Spoke. Esta solicitud de resolución NHRP se envía dirigida a Spoke2 a través de NHS (según la tabla de routing): es un proceso de reenvío NHRP salto a salto normal.
4. Spoke2 después de recibir la solicitud de resolución, incluida la IP NBMA de Spoke1, envía la respuesta de resolución NHRP directamente a Spoke1 - Reply no atraviesa el concentrador.
5. Spoke1 después de recibir la IP NBMA correcta de Spoke2 reescribe la entrada CEF para el prefijo de destino - este procedimiento se llama NHRP Shortcut.
6. Los radios no activan el NHRP al detectar adyacencias, pero las respuestas del NHRP actualizan el CEF.



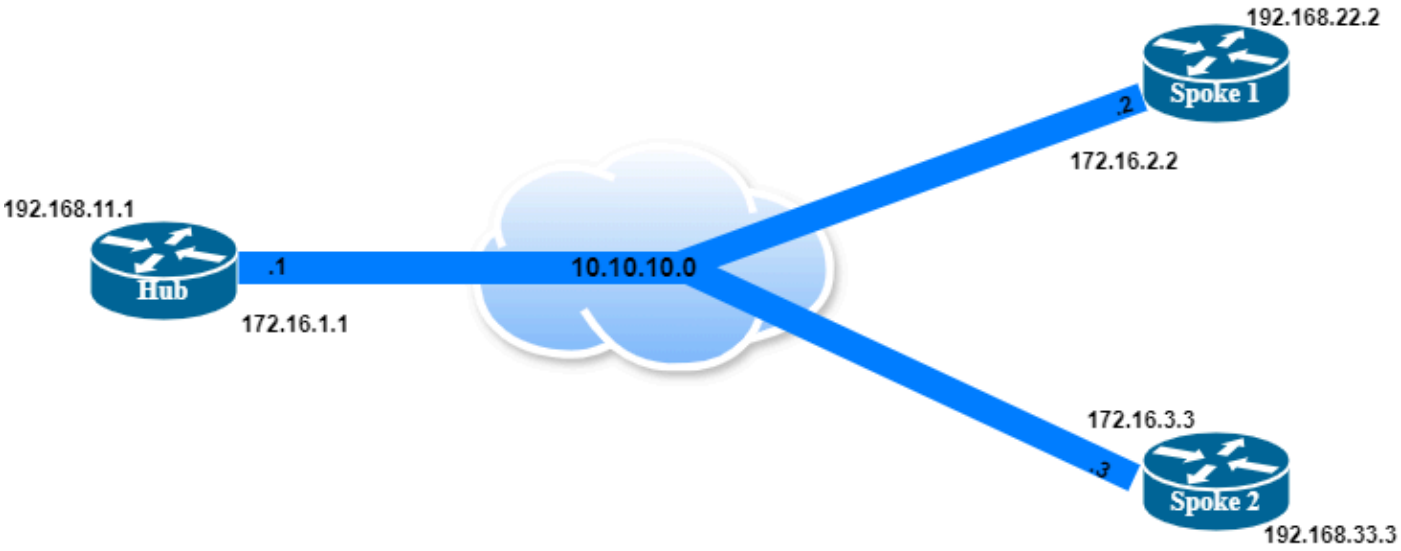


Nota:

Fase 2 de DMVPN: En esta fase, el paquete de radio a radio inicial es conmutado por proceso porque la adyacencia CEF está en el estado 'glean'. Esto significa que el router no tiene suficiente información para reenviar el paquete usando CEF y debe utilizar un proceso de conmutación con más recursos para resolver el salto siguiente usando NHRP (Next Hop Resolution Protocol).

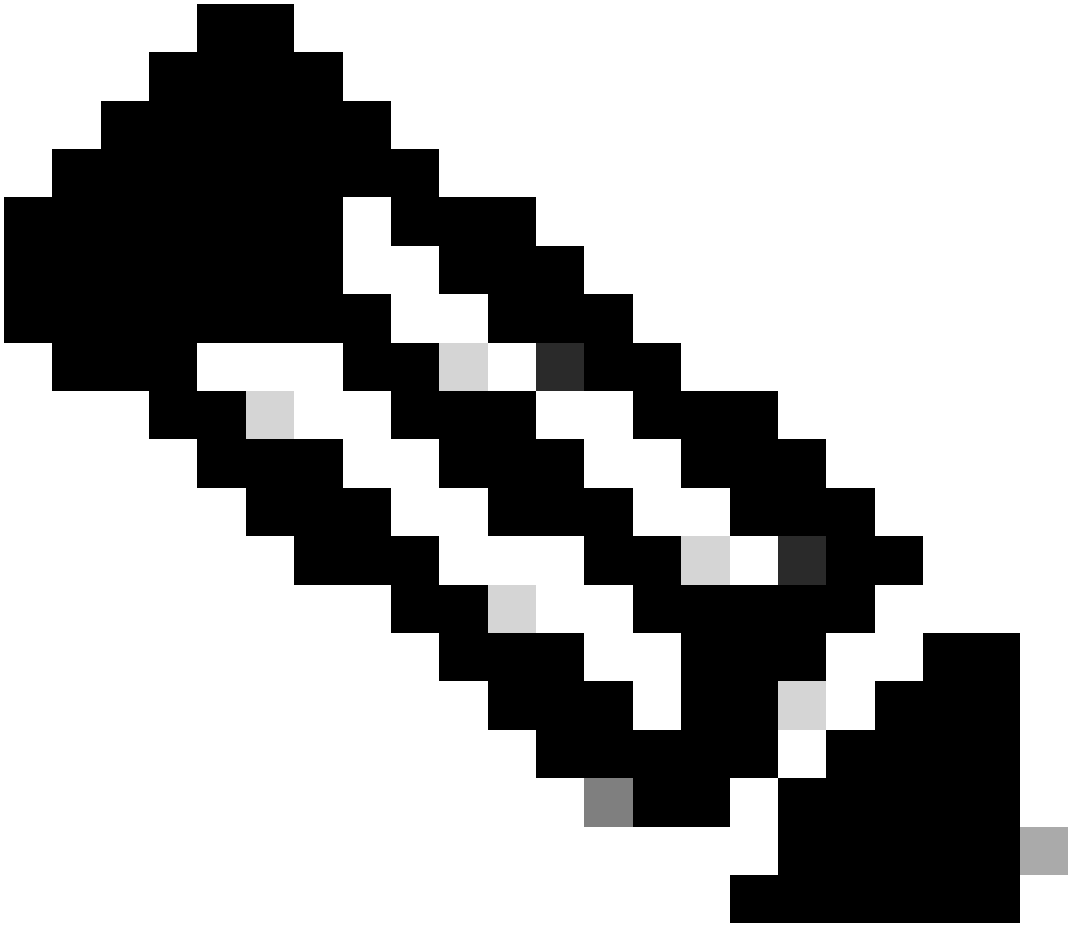
Fase 3 de DMVPN: Esta fase mejora la fase 2 al permitir que el paquete de radio a radio inicial se conmute usando CEF desde el principio. Esto se logra mediante el uso de las funciones NHRP Redirect y NHRP Shortcut, que ayudan a establecer rápidamente túneles directos de radio a radio. Como resultado, CEF se utiliza de manera más consistente, lo que reduce la dependencia de la conmutación de procesos.

Diagrama de la red



Configuraciones

Configuraciones criptográficas



Nota: Esto es lo mismo en el hub y en todos los spokes.

1. Configure una propuesta Ikev2 y un llavero.

```
propuesta crypto ikev2 DMVPN
encryption aes-cbc-256
integridad sha256
grupo 14
crypto ikev2 keyring IKEV2-KEYRING
peer any
address 0.0.0.0 0.0.0.0
pre-shared-key CISCO123
!
```

2. Configure el perfil Ikev2 que contiene toda la información relacionada con la conexión.

```
crypto ikev2 profile IKEV2-PROF
```

```
match address local interface GigabitEthernet0/0/0
match identity remote address 0.0.0.0
authentication local pre-share
authentication remote pre-share
keyring local IKEV2-KEYRING
```

Aquí está el detalle de los comandos usados en el perfil ikev2:

- match address local interface GigabitEthernet0/0/0: Interfaz externa local donde termina la VPN, en este caso, GigabitEthernet0/0/0
- match identity remote address 0.0.0.0: Dado que el peer remoto puede ser múltiple, se utiliza 0.0.0.0 que indica cualquier peer
- authentication local pre-share: El modo de autenticación en el sitio local está previamente compartido
- authentication remote pre-share: El modo de autenticación en el sitio local está previamente compartido
- keyring local IKEV2-KEYRING: Utilice el mismo anillo de claves que creó anteriormente.

3. Configuración del perfil IPsec.

```
crypto ipsec transform-set T-SET esp-aes 256 esp-sha256-hmac
túnel de modo

crypto ipsec profile IPSEC-IKEV2

set transform-set T-SET
set ikev2-profile IKEV2-PROF
```

Cree un conjunto de transformación para la negociación de túnel IPsec y llame al conjunto de transformación y al perfil Ikev2 bajo el perfil IPsec.

Configuración DMVPN

1. Configure la interfaz externa.

```
interface GigabitEthernet0/0/0

IP address 172.16.1.1 255.255.255.0
negotiation auto
cdp enable
```

2. Configure el router hub para la integración de mGRE e IPsec (es decir, asocie el túnel con el perfil IPsec configurado en el procedimiento anterior)

```
interface Tunnel0
IP address 10.10.10.1 255.255.255.0
no ip redirects
ip nhrp authentication DMVPN
```

```
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip nhrp redirect <-------- Obligatorio para activar DMVPN Phase 3 en el router hub
tunnel source GigabitEthernet0/0/0
tunnel mode gre multipoint
tunnel protection ipsec profile IPSEC-IKEV2
!
```

Estos comandos se utilizan en la configuración de la interfaz de túnel:

- ip nhrp authentication DMVPN: En este caso, la cadena de autenticación 'DMVPN' debe tener el mismo valor en todos los hubs y radios que forman parte de la misma red DMVPN.
- ip nhrp map multicast dynamic: Permite a NHRP agregar radios a la asignación de multidifusión NHRP de forma dinámica.
- ip nhrp network-id 1: Identificador de red de 32 bits que habilita NHRP en una interfaz.
- ip nhrp redirect: Habilita la indicación de tráfico de redirección si el tráfico se reenvía con la red NHRP.
- tunnel source GigabitEthernet0/0/0: Establece la dirección de origen para una interfaz de túnel, donde se utiliza la dirección IP GigaEthernet 0/0/0.
- tunnel mode gre multipoint: Establece el modo de encapsulación en mGRE para esta interfaz de túnel.
- tunnel protection ipsec profile IPSEC-IKEV2: Asocia una interfaz de túnel con el perfil IPsec que ya se ha creado en configuraciones criptográficas.

3. Configure los routers de radio para la integración de mGRE e IPsec junto con una interfaz externa y un loopback para probar la conectividad del protocolo de gateway fronterizo (BGP).

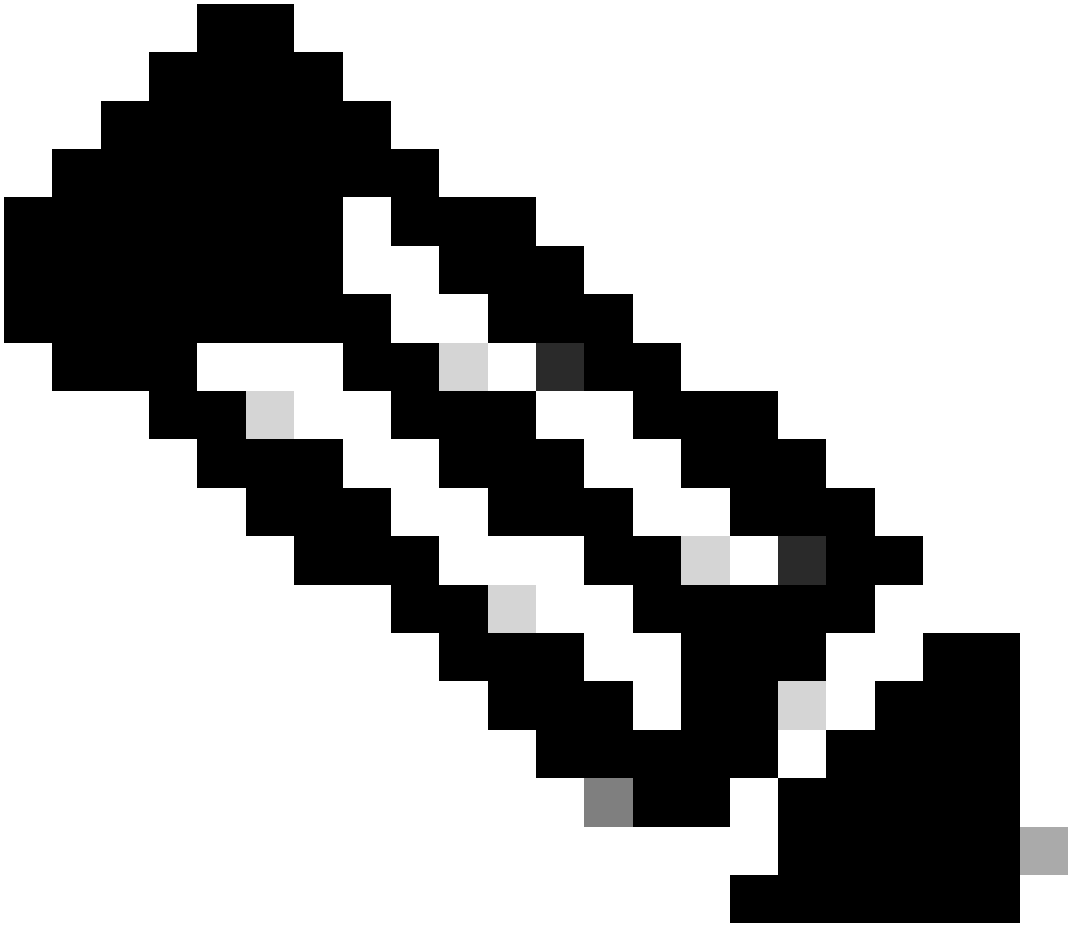
RADIO X: (Se puede utilizar una configuración similar en todos los radios)

```
interface GigabitEthernet0/0/0
IP address 172.16.3.3 255.255.255.0
speed 1000
no negotiation auto

!

interface Loopback10
IP address 192.168.33.3 255.255.255.0
!
interface Tunnel0
IP address 10.10.10.3 255.255.255.0
no ip redirects
ip nhrp authentication DMVPN
ip nhrp map 10.10.10.1 172.16.1.1
ip nhrp map multicast 172.16.1.1
ip nhrp network-id 1
ip nhrp nhs 10.10.10.1
```

ip nhrp shortcut <-------- Obligatorio para activar DMVPN Phase 3 en el router de radio
tunnel source GigabitEthernet0/0/0
tunnel mode gre multipoint
tunnel protection ipsec profile IPSEC-IKEV2

Estos comandos se utilizan en la configuración de la interfaz de túnel:

- ip nhrp authentication DMVPN: En este caso, la cadena de autenticación 'DMVPN' debe tener el mismo valor en todos los hubs y radios que forman parte de la misma red DMVPN.
- ip nhrp map 10.10.10.1 172.16.1.1: Asigna manualmente la dirección IP NBMA del concentrador con la dirección IP de la interfaz de túnel.
- ip nhrp map multicast 172.16.1.1: Redirige todo el tráfico de multidifusión hacia el hub.
- ip nhrp network-id 1: Identificador de red de 32 bits que habilita NHRP en una interfaz.
- ip nhrp nhs 10.10.10.1: El servidor de salto siguiente que es nuestro hub se configura mediante este comando.
- ip nhrp shortcut: Habilita el switching de acceso directo NHRP en una interfaz.
- tunnel source GigabitEthernet0/0/0: Establece la dirección de origen para una interfaz de túnel, donde se utiliza la dirección IP GigaEthernet 0/0/0.
- tunnel mode gre multipoint: Establece el modo de encapsulación en mGRE para esta interfaz de túnel.
- tunnel protection ipsec profile IPSEC-IKEV2: Asocia una interfaz de túnel con el perfil IPsec que ya se ha creado en configuraciones criptográficas.



Nota: El comando ip nhrp redirect envía el mensaje a los Spokes que dice "Hay una mejor ruta al Spoke de destino que a través del Hub" e ip nhrp shortcut impone la instalación de esta ruta en la Base de información de reenvío (FIB) en los Spokes.

Configuración de BGP

Hay varias variaciones entre las que puede elegir:

- eBGP con un número AS diferente en cada radio
- eBGP con el mismo número AS en cada radio
- iBGP

La explicación de los tres escenarios está fuera del alcance de este documento.

Se configura un eBGP con un número AS diferente en todos los spokes, por lo que no se pueden utilizar vecinos dinámicos. Por lo tanto, debe configurar los vecinos manualmente.

eBGP con AS diferente en los radios

1. Configuración de BGP en el HUB:

Hub(config)#router bgp 65010

Hub(config-router)#bgp log-neighbor-changes

Hub(config-router)#network 192.168.11.1 mask 255.255.255.255

Hub(config-router)#neighbor 10.10.10.2 remote-as 65011

Hub(config-router)#neighbor 10.10.10.3 remote-as 65012

!

Estos comandos se utilizan en la configuración de BGP en el Hub:

- router bgp 65010: Configura un proceso de ruteo BGP. Utilice el argumento 'autonomous-system-number' que identifica el dispositivo a otros altavoces BGP.
- network 192.168.11.1 mask 255.255.255.255: Especifica una red como local para este sistema autónomo y la añade a la tabla de ruteo de BGP.
- neighbor 10.10.10.2 remote-as 65011: Agrega la dirección IP del vecino Spoke 1 en el sistema autónomo especificado a la tabla de vecinos BGP multiprotocolo IPv4 del dispositivo local.
- neighbor 10.10.10.3 remote-as 65012: Agrega la dirección IP del vecino Spoke 2 en el sistema autónomo especificado a la tabla de vecinos BGP multiprotocolo IPv4 del dispositivo local.

2. Configuración de BGP en Spoke X:

Spoke2(config)#router bgp 65012

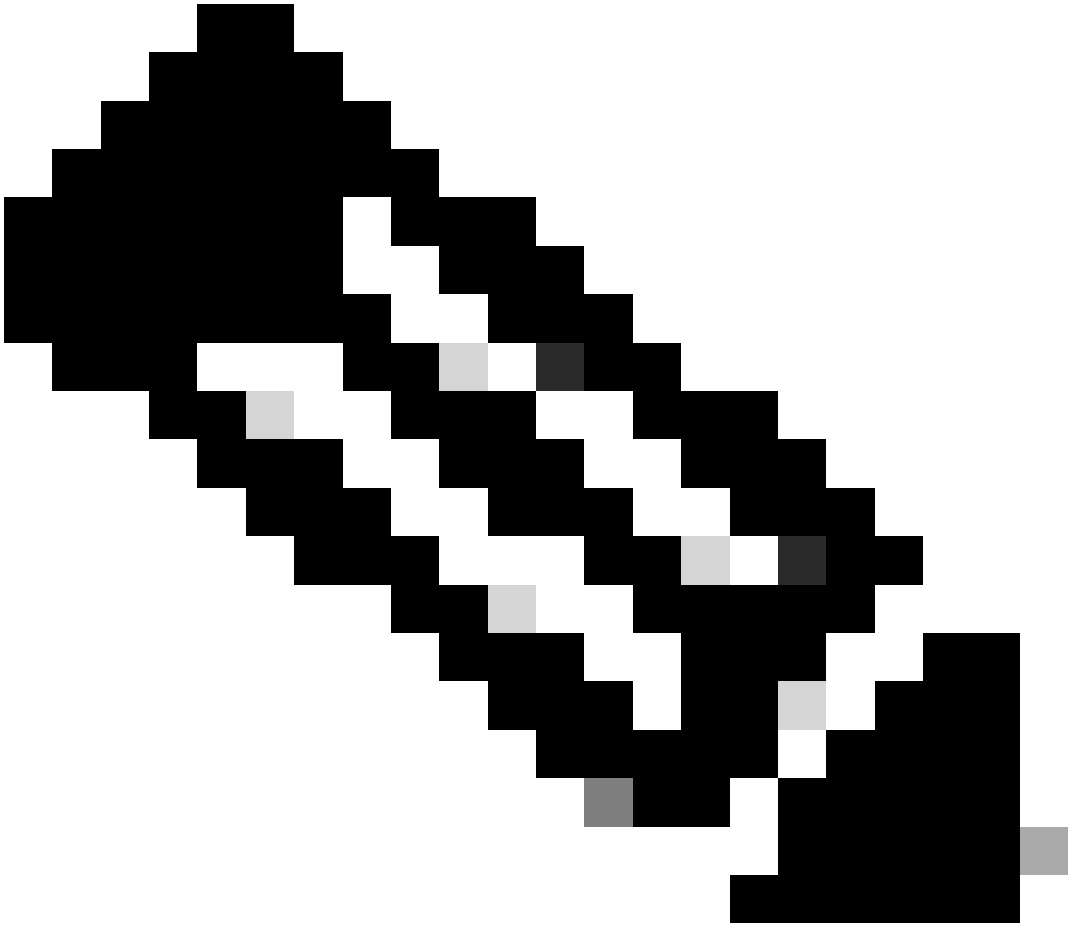
Spoke2(config-router) #bgp log-neighbor-changes

Spoke2(config-router)# network 192.168.33.3 mask 255.255.255.255

Spoke2(config-router)# neighbor 10.10.10.1 remote-as 65010

Estos comandos se utilizan en la configuración BGP en Spoke X:

- router bgp 65012: Configura un proceso de ruteo BGP. Utilice el argumento 'autonomous-system-number' que identifica el dispositivo a otros altavoces BGP.
- network 192.168.33.3 mask 255.255.255.255: Especifica una red como local para este sistema autónomo y la añade a la tabla de ruteo de BGP.
- neighbor 10.10.10.1 remote-as 65010: Agrega la dirección IP del concentrador en el sistema autónomo especificado a la tabla de vecinos BGP multiprotocolo IPv4 del dispositivo local.



Nota: Se debe realizar una configuración similar en todos los radios de la red DMVPN.

Verificación

1. Comandos de verificación en el dispositivo Hub:

HUB#sh dmvpn

Muestra información de sesión específica de DMVPN.

Leyenda: Attrb —> S - Estático, D - Dinámico, I - Incompleto
N - NATed, L - Local, X - Sin socket
T1 - Route Installed, T2 - Nexthop-override
C - Compatible con CTS
Ent —> Número de entradas NHRP con el mismo peer NBMA
Estado de NHS: E —> Esperando respuestas, R —> Respondiendo, W —> Esperando
UpDn Time —> Up or Down Time for a Tunnel

==========

Interfaz: Tunnel0, detalles NHRP IPv4
Tipo:Hub, puntos iguales NHRP:2, <<<<<<<<<<<<<<<<<<<<<<< Indica que el dispositivo actúa como hub y que hay 2 puntos NHRP conectados a este HUB.

Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.2.2 10.10.10.2 UP 01:47:08 D <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
Ambos pares se han registrado dinámicamente en el hub y se encuentran en estado UP.
1 172.16.3.3 10.10.10.3 UP 01:08:58 D

HUB#sh ip nhrp

Muestra la asignación de direcciones NBMA a la IP de interfaz de túnel de todos los pares NHRP conectados al concentrador. Hub mantiene la base de datos de todos los radios.

10.10.10.2/32 vía 10.10.10.2
Tunnel0 creado 01:47:22, caduca 01:32:27
Tipo: dinámico, Indicadores: NHOP usado registrado único
Dirección NBMA: 172.16.2.2
10.10.10.3/32 vía 10.10.10.3
Tunnel0 creado 01:09:11, caduca 01:29:58
Tipo: dinámico, Indicadores: NHOP usado registrado único
Dirección NBMA: 172.16.3.3

HUB#sh ip nhrp multicast

Muestra información de asignación de multidifusión NHRP.

Dirección I/F NBMA
Tunnel0 172.16.2.2 Indicadores: dinámico (activado)
Tunnel0 172.16.3.3 Indicadores: dinámico (activado)

HUB#sh crypto sockets

Número de conexiones de socket criptográfico 2

Tu0 Peers (local/remoto): 172.16.1.1/172.16.2.2
Identificación local (addr/mask/port/port): (172.16.1.1/255.255.255.255/0/47)
Identificación remota (addr/mask/port/port): (172.16.2.2/255.255.255.255/0/47)
Perfil IPSec: "IPSEC-IKEV2"
Estado del socket: Abierto
Cliente: "TUNNEL SEC" (Estado del cliente: Activo)
Tu0 Peers (local/remoto): 172.16.1.1/172.16.3.3
Identificación local (addr/mask/port/port): (172.16.1.1/255.255.255.255/0/47)
Identificación remota (addr/mask/port/port): (172.16.3.3/255.255.255.255/0/47)

Perfil IPSec: "IPSEC-IKEV2"
Estado del socket: Abierto
Cliente: "TUNNEL SEC" (Estado del cliente: Activo)
Sockets criptográficos en estado de escucha:
Cliente: Perfil "TUNNEL SEC": "IPSEC-IKEV2" Map-name: "Tunnel0-head-0"

HUB#sh cry ikev2 sa

SA Crypto IKEv2 IPv4

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.1.1/500 172.16.2.2/500 ninguno/ninguno PREPARADO
Encr: AES-CBC, tamaño de clave: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, signo de autenticación: PSK, verificación de autenticación: PSK
Vida/Tiempo activo: 86400/6524 s

Tunnel-id Local Remote fvrf/ivrf Status
2 172.16.1.1/500 172.16.3.3/500 ninguno/ninguno PREPARADO
Encr: AES-CBC, tamaño de clave: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, signo de autenticación: PSK, verificación de autenticación: PSK
Vida/Tiempo activo: 86400/4234 s

SA Crypto IKEv2 IPv6

HUB#sh ip bgp summary

Muestra el estado actual de la sesión BGP/el número de prefijos que el router ha recibido de un vecino o grupo de peers.

Identificador de router BGP 192.168.11.1 número AS local 65010
La versión de la tabla BGP es 4, la versión de la tabla de ruteo principal es 4.
3 entradas de red que utilizan 432 bytes de memoria
3 entradas de ruta que utilizan 252 bytes de memoria
3/3 entradas de atributo de trayectoria BGP/mejor trayectoria utilizando 480 bytes de memoria
2 entradas BGP AS-PATH que utilizan 48 bytes de memoria
0 entradas de caché de route-map BGP que utilizan 0 bytes de memoria
0 entradas de caché de lista de filtros BGP con 0 bytes de memoria
BGP que utiliza 1212 bytes totales de memoria
Prefijos de actividad BGP 3/0, rutas 3/0, intervalo de análisis de 60 segundos

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.10.2 4 65011 33 33 4 0 0 00:25:35 1
10.10.10.3 4 65012 21 25 4 0 0 00:14:58 1

Hub#sh ip route bgp

Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvil, B - BGP
D - EIGRP, EX - EIGRP externo, O - OSPF, IA - OSPF entre áreas
N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA externo tipo 2

E1 - OSPF tipo externo 1, E2 - OSPF tipo externo 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - ruta estática descargada periódicamente, H - NHRP, l - LISP
a - ruta de aplicación
+ - ruta replicada, % - reemplazo de salto siguiente, p - reemplazos de PfR

El gateway de último recurso es 172.16.1.2 para la red 0.0.0.0

192.168.0.0/16 está dividido en subredes de forma variable, 4 subredes y 2 máscaras
B 192.168.22.0/24 [20/0] vía 10.10.10.2, 00:29:15 <<<<<<<<<<<<<<<<<<< Entrada para las rutas anunciadas Spoke 1
B 192.168.33.0/24 [20/0] vía 10.10.10.3, 00:18:37 <<<<<<<<<<<<<<<<<<< Entrada para las rutas anunciadas Spoke 2

2. Comandos de verificación en Spoke 1:

Spoke1#sh dmvpn

Leyenda: Attrb —> S - Estático, D - Dinámico, I - Incompleto
N - NATed, L - Local, X - Sin socket
T1 - Route Installed, T2 - Nexthop-override
C - Compatible con CTS, I2 - Temporal
Ent —> Número de entradas NHRP con el mismo peer NBMA
Estado de NHS: E —> Esperando respuestas, R —> Respondiendo, W —> Esperando
UpDn Time —> Up or Down Time for a Tunnel
==========

Interfaz: Tunnel0, detalles NHRP IPv4
Tipo:Spoke, Peers NHRP:2,

Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.10.10.1 UP 01:32:09 S <<<<<<<<<<<<<<<<<< El concentrador se muestra como S- estático, ya que lo hemos configurado como entrada estática en la interfaz de túnel
1 172.16.3.3 10.10.10.3 UP 00:19:34 D <<<<<<<<<<<<<<<<<< Túnel dinámico de radio a radio creado después de enviar tráfico a Spoke 2

Spoke1#sh ip bgp summary

Identificador de router BGP 192.168.22.2, número AS local 65011
La versión de la tabla BGP es 4, la versión de la tabla de ruteo principal es 4.
3 entradas de red que utilizan 744 bytes de memoria
3 entradas de ruta con 432 bytes de memoria
3/3 entradas de atributo de trayectoria BGP/mejor trayectoria utilizando 864 bytes de memoria
2 entradas BGP AS-PATH que utilizan 64 bytes de memoria
0 entradas de caché de route-map BGP que utilizan 0 bytes de memoria

0 entradas de caché de lista de filtros BGP con 0 bytes de memoria
BGP que utiliza 2104 bytes totales de memoria
Prefijos de actividad BGP 3/0, rutas 3/0, intervalo de análisis de 60 segundos
3 networks peaked a las 08:16:54 jun 2022 UTC (01:11:51.732 ago)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.10.1 4 65010 85 85 4 0 0 01:12:21 2 <<<<<<<<<<<<<<<<<<<<<<<<<<<< Hemos recibido 2 prefijos de Hub, cada uno para el loopback del hub y el loopback Spoke2

Spoke1#sh ip route bgp

Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvil, B - BGP
D - EIGRP, EX - EIGRP externo, O - OSPF, IA - OSPF entre áreas
N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA externo tipo 2
E1 - OSPF tipo externo 1, E2 - OSPF tipo externo 2, m - OMP
n - NAT, Ni - NAT interna, No - NAT externa, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registrado, g - Resumen de registro NHRP
o - ODR, P - ruta estática descargada periódicamente, l - LISP
a - ruta de aplicación
+ - ruta replicada, % - reemplazo de salto siguiente, p - reemplazos de PfR

El gateway de último recurso es 172.16.2.10 para la red 0.0.0.0

B 192.168.11.0/24 [20/0] mediante 10.10.10.1, 01:13:16 **>>>>>>>>>>>>>>>** Red de concentradores accesible directamente a través del concentrador

B 192.168.33.0/24 [20/0] vía 10.10.10.3, 01:12:46 **>>>>>>>>>>>>>>>** Red de radio directamente accesible vía IP del túnel de radio.

Spoke1#sh ip route

Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvil, B - BGP
D - EIGRP, EX - EIGRP externo, O - OSPF, IA - OSPF entre áreas
N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA externo tipo 2
E1 - OSPF tipo externo 1, E2 - OSPF tipo externo 2, m - OMP
n - NAT, Ni - NAT interna, No - NAT externa, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registrado, g - Resumen de registro NHRP
o - ODR, P - ruta estática descargada periódicamente, l - LISP
a - ruta de aplicación
+ - ruta replicada, % - reemplazo de salto siguiente, p - reemplazos de PfR

El gateway de último recurso es 172.16.2.10 para la red 0.0.0.0

S* 0.0.0.0/0 [1/0] mediante 172.16.2.10
172.16.2.0/24 está dividido en subredes de forma variable, 2 subredes y 2 máscaras
C 172.16.2.0/24 está conectado directamente, GigabitEthernet2
L 172.16.2.2/32 está conectado directamente, GigabitEthernet2
10.0.0.0/8 está dividido en subredes de forma variable, 2 subredes, 2 máscaras
C 10.10.10.0/24 está conectado directamente, Tunnel0
L 10.10.10.2/32 está conectado directamente, Tunnel0
B 192.168.11.0/24 [20/0] vía 10.10.10.1, 01:13:21
192.168.22.0/24 está dividido en subredes de forma variable, 2 subredes y 2 máscaras
C 192.168.22.0/24 está conectado directamente, Loopback10
L 192.168.22.2/32 está conectado directamente, Loopback10
B 192.168.33.0/24 [20/0] vía 10.10.10.3, 01:12:51

Spoke1#sh ip nhrp nhs

Leyenda: E=Esperando respuestas, R=Respondiendo, W=Esperando, D=Dinámico
Túnel0:
10.10.10.1 RE priority = 0 cluster = 0 **>>>>>>>>>>** Sólo se ha configurado un servidor de próximo salto

Spoke1#sh ip nhrp traffic

Túnel0: Límite máximo de envío: 10000 paquetes/10 segundos, uso: 0%
Enviado: Total 52
1 Solicitud de resolución 0 Respuesta de resolución 51 Solicitud de registro **<<<<<<<<<** Número de veces que se enviaron solicitudes de registro al hub
0 Registro Respuesta 0 Solicitud de depuración 0 Respuesta de depuración
0 Indicación de error 0 Indicación de tráfico 0 Redirección Suprimir
Recibido: Total 25
0 Solicitud de resolución 1 Respuesta de resolución 0 Solicitud de registro **<<<<<<<<<<** Número de veces que hemos recibido respuestas a dichas solicitudes de registro
24 Registro Respuesta 0 Solicitud de depuración 0 Respuesta de depuración
0 Indicación de error 0 Indicación de tráfico 0 Redirección Suprimir

Spoke1#sh ip nhrp multicast

Dirección I/F NBMA
Tunnel0 172.16.1.1 Indicadores: static (Enabled) **<<<<<<<<<<**El tráfico multidifusión se configura para reenviarse hacia el hub NBMA

Spoke1#sh crypto sockets

Número de conexiones de socket criptográfico 2

Tu0 Peers (local/remoto): 172.16.2.2/172.16.1.1

Identificación local (addr/mask/port/port): (172.16.2.2/255.255.255.255/0/47)
Identificación remota (addr/mask/port/port): (172.16.1.1/255.255.255.255/0/47)
Perfil IPSec: "IPSEC-IKEV2"
Estado del socket: Abra <<<<<<<<<<<<<<<<<< Estado del socket para este par en particular
Cliente: "TUNNEL SEC" (Estado del cliente: Activo)
Tu0 Peers (local/remoto): 172.16.2.2/172.16.3.3
Identificación local (addr/mask/port/port): (172.16.2.2/255.255.255.255/0/47)
Identificación remota (addr/mask/port/port): (172.16.3.3/255.255.255.255/0/47)
Perfil IPSec: "IPSEC-IKEV2"
Estado del socket: Abierto
Cliente: "TUNNEL SEC" (Estado del cliente: Activo)
Sockets criptográficos en estado de escucha:
Cliente: Perfil "TUNNEL SEC": "IPSEC-IKEV2" Map-name: "Tunnel0-head-0"

Spoke1#sh cry ikev2 sa

SA Crypto IKEv2 IPv4

Tunnel-id Local Remote fvrf/ivrf Status
2 172.16.2.2/500 172.16.3.3/500 ninguno/ninguno PREPARADO
Encr: AES-CBC, tamaño de clave: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, signo de autenticación: PSK, verificación de autenticación: PSK
Vida/Tiempo activo: 86400/287 s

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.2.2/500 172.16.1.1/500 ninguno/ninguno PREPARADO
Encr: AES-CBC, tamaño de clave: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, signo de autenticación: PSK, verificación de autenticación: PSK
Vida/Tiempo activo: 86400/4643 s

SA Crypto IKEv2 IPv6

Spoke1#traceroute 192.168.33.3 source lo10

Ingrese escape sequence para abortar.
Seguimiento de la ruta a 192.168.33.3
Información de VRF: (vrf en nombre/id, vrf en nombre/id)
1 10.10.10.3 3 mseg 4 mseg * <<<<<<<<<<<<<< El tráfico va directamente al router Spoke 2 sin pasar a través del concentrador.

Spoke2#sh dmvpn

Leyenda: Attrb —> S - Estático, D - Dinámico, I - Incompleto
N - NATed, L - Local, X - Sin socket
T1 - Route Installed, T2 - Nexthop-override
C - Compatible con CTS, I2 - Temporal
Ent —> Número de entradas NHRP con el mismo peer NBMA

Estado de NHS: E —> Esperando respuestas, R —> Respondiendo, W —> Esperando
UpDn Time —> Up or Down Time for a Tunnel
==========

Interfaz: Tunnel0, detalles NHRP IPv4
Tipo:Spoke, Peers NHRP:2,

Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- -------------- -------------- ----- -------- -----
1 172.16.1.1 10.10.10.1 UP 01:20:26 S
1 172.16.2.2 10.10.10.2 UP 00:07:51 D

3. Comandos de verificación en Spoke 2:

Spoke2#sh ip nhrp

10.10.10.1/32 vía 10.10.10.1
Tunnel0 creado 01:36:06, nunca caduca
Tipo: static, Flags:
Dirección NBMA: 172.16.1.1
10.10.10.2/32 vía 10.10.10.2
Tunnel0 creado 00:08:09, caduca 00:01:50
Tipo: dinámico, Indicadores: router implícito
Dirección NBMA: 172.16.2.2
10.10.10.3/32 vía 10.10.10.3
Tunnel0 creado 00:08:09, caduca 00:01:50
Tipo: dinámico, Indicadores: router unique local
Dirección NBMA: 172.16.3.3
(sin socket)
Spoke2#sh ip nhrp mul
Spoke2#sh ip nhrp multicast
Dirección I/F NBMA
Tunnel0 172.16.1.1 Indicadores: static (Enabled)
Spoke2#

Spoke2#sh crypto sockets

Número de conexiones de socket criptográfico 2

Tu0 Peers (local/remoto): 172.16.3.3/172.16.1.1
Identificación local (addr/mask/port/port): (172.16.3.3/255.255.255.255/0/47)
Identificación remota (addr/mask/port/port): (172.16.1.1/255.255.255.255/0/47)
Perfil IPSec: "IPSEC-IKEV2"
Estado del socket: Abra <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< Estado del socket para este par en particular
Cliente: "TUNNEL SEC" (Estado del cliente: Activo)
Tu0 Peers (local/remoto): 172.16.3.3/172.16.2.2

Identificación local (addr/mask/port/port): (172.16.3.3/255.255.255.255/0/47)
Identificación remota (addr/mask/port/port): (172.16.2.2/255.255.255.255/0/47)
Perfil IPSec: "IPSEC-IKEV2"
Estado del socket: Abierto
Cliente: "TUNNEL SEC" (Estado del cliente: Activo)
Sockets criptográficos en estado de escucha:
Cliente: Perfil "TUNNEL SEC": "IPSEC-IKEV2" Map-name: "Tunnel0-head-0"

Spoke2#sh cry ikev2 sa

SA Crypto IKEv2 IPv4

Tunnel-id Local Remote fvrf/ivrf Status
2 172.16.3.3/500 172.16.2.2/500 ninguno/ninguno PREPARADO
Encr: AES-CBC, tamaño de clave: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, signo de autenticación: PSK, verificación de autenticación: PSK
Vida/Tiempo activo: 86400/509 s

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.3.3/500 172.16.1.1/500 ninguno/ninguno PREPARADO
Encr: AES-CBC, tamaño de clave: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, signo de autenticación: PSK, verificación de autenticación: PSK
Vida/Tiempo activo: 86400/4866 s

SA Crypto IKEv2 IPv6

Spoke2#sh ip bgp summary

Identificador de router BGP 192.168.33.3, número AS local 65012
La versión de la tabla BGP es 4, la versión de la tabla de ruteo principal es 4.
3 entradas de red que utilizan 744 bytes de memoria
3 entradas de ruta con 432 bytes de memoria
3/3 entradas de atributo de trayectoria BGP/mejor trayectoria utilizando 864 bytes de memoria
2 entradas BGP AS-PATH que utilizan 64 bytes de memoria
0 entradas de caché de route-map BGP que utilizan 0 bytes de memoria
0 entradas de caché de lista de filtros BGP con 0 bytes de memoria
BGP que utiliza 2104 bytes totales de memoria
Prefijos de actividad BGP 3/0, rutas 3/0, intervalo de análisis de 60 segundos
3 networks peaked a las 08:16:54 jun 2022 UTC (01:20:43.775 ago)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.10.1 465010 97 94 4 0 0 01:21:07 2 **>>>>>>>>>>>>>>>>>>>**. Hemos recibido 2 prefijos del hub, cada uno para el loopback del hub y el loopback de Spoke2

Spoke2#sh ip route

Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvil, B - BGP
D - EIGRP, EX - EIGRP externo, O - OSPF, IA - OSPF entre áreas

N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA externo tipo 2
E1 - OSPF tipo externo 1, E2 - OSPF tipo externo 2, m - OMP
n - NAT, Ni - NAT interna, No - NAT externa, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registrado, g - Resumen de registro NHRP
o - ODR, P - ruta estática descargada periódicamente, l - LISP
a - ruta de aplicación
+ - ruta replicada, % - reemplazo de salto siguiente, p - reemplazos de PfR

El gateway de último recurso es 172.16.3.10 para la red 0.0.0.0

S* 0.0.0.0/0 [1/0] mediante 172.16.3.10
172.16.3.0/24/8 está dividido en subredes de forma variable, 2 subredes y 2 máscaras
C 172.16.3.0/24 está conectado directamente, GigabitEthernet3
L 172.16.3.3/32 está conectado directamente, GigabitEthernet3
10.0.0.0/8 está dividido en subredes de forma variable, 2 subredes, 2 máscaras
C 10.10.10.0/24 está conectado directamente, Tunnel0
L 10.10.10.3/32 está conectado directamente, Tunnel0
B 192.168.11.0/24 [20/0] vía 10.10.10.1, 01:47:08
B 192.168.22.0/24 [20/0] vía 10.10.10.2, 01:46:45
192.168.33.0/24 está dividido en subredes de forma variable, 2 subredes y 2 máscaras
C 192.168.33.0/24 está conectado directamente, Loopback10
L 192.168.33.3/32 está conectado directamente, Loopback10

Spoke2#sh ip route bgp

Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvil, B - BGP
D - EIGRP, EX - EIGRP externo, O - OSPF, IA - OSPF entre áreas
N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA externo tipo 2
E1 - OSPF tipo externo 1, E2 - OSPF tipo externo 2, m - OMP
n - NAT, Ni - NAT interna, No - NAT externa, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registrado, g - Resumen de registro NHRP
o - ODR, P - ruta estática descargada periódicamente, l - LISP
a - ruta de aplicación
+ - ruta replicada, % - reemplazo de salto siguiente, p - reemplazos de PfR

El gateway de último recurso es 172.16.3.10 para la red 0.0.0.0

B 192.168.11.0/24 [20/0] mediante 10.10.10.1, 01:21:11 >>>>>>>>>>>>>>>>>>Red de concentradores accesible directamente a través del concentrador
B 192.168.22.0/24 [20/0] vía 10.10.10.2, 01:20:48 >>>>>>>>>>>>>> Red de radio directamente accesible vía IP del túnel de radio.

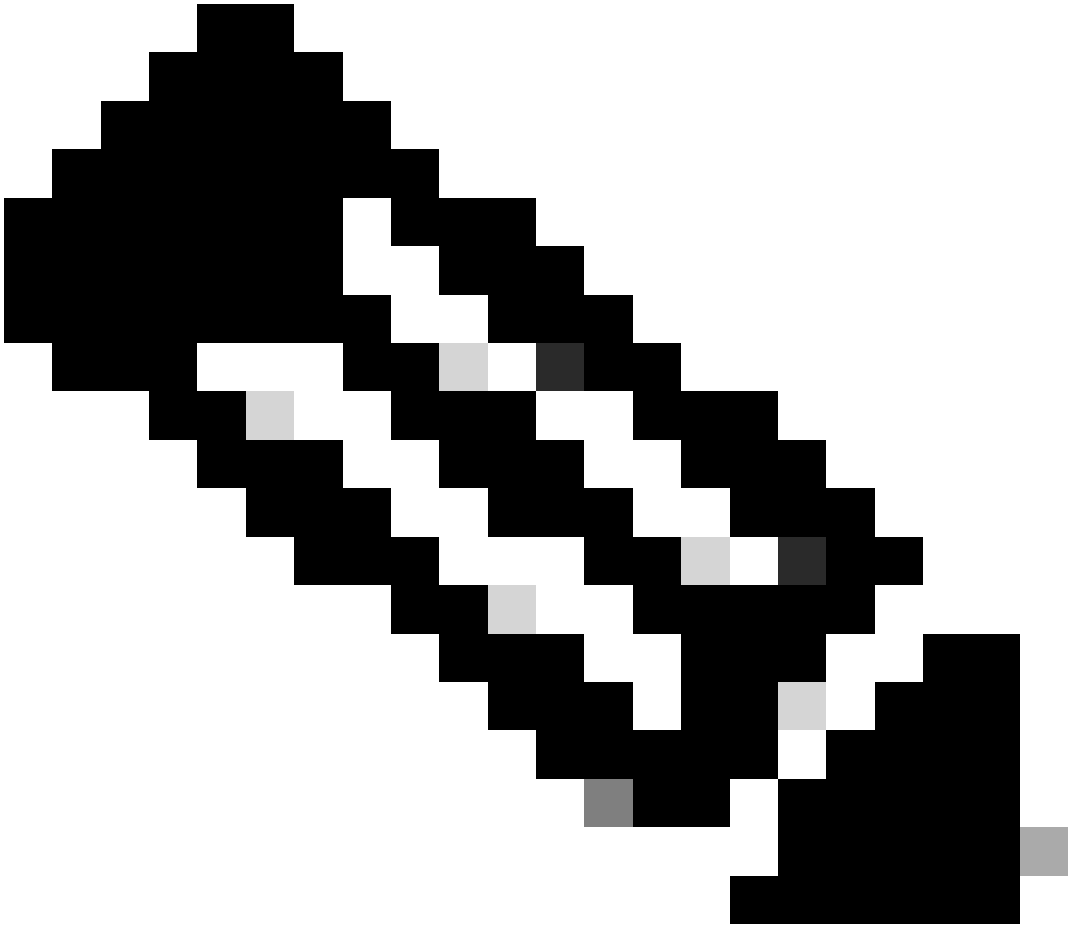
Spoke2#sh ip nhrp nhs

Leyenda: E=Esperando respuestas, R=Respondiendo, W=Esperando, D=Dinámico
Túnel0:
10.10.10.1 RE priority = 0 cluster = 0 **>>>>>>>>>>>>>>>** Sólo se ha configurado un servidor de próximo salto

Spoke2#traceroute 192.168.22.2 source loopback 10

Ingrese escape sequence para abortar.
Seguimiento de la ruta a 192.168.22.2
Información de VRF: (vrf en nombre/id, vrf en nombre/id)
1 10.10.10.2 4 mseg 4 mseg * **<<<<<<<<<<<<<** El tráfico va directamente al router Spoke 1 sin pasar por el concentrador.

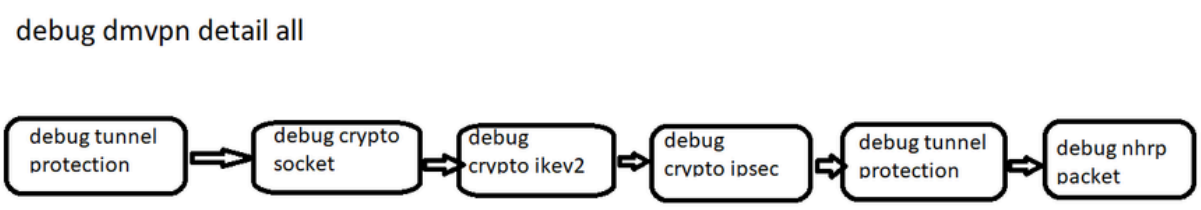
Troubleshoot



Nota: Siempre se sugiere utilizar depuraciones condicionales, ya que la ejecución de depuraciones no condicionales puede afectar al procesador y, por tanto, al entorno de producción. La dirección NBMA corresponde a la 'dirección IP externa' (dirección IP utilizada para originar la interfaz de túnel) y la IP de túnel corresponde a la 'dirección IP lógica, es decir, la dirección IP de la interfaz de túnel'.

debug dmvpn condition peer <nmbma/tunnel> <NMBA IP or Tunnel IP address of peer>
debug crypto condition peer ipv4 <WAN IP of the Peer>
debug nhrp condition peer <nbma/tunnel> <NBMA or Tunnel IP address of Peer>

Para solucionar problemas de DMVPN, debe adoptar un enfoque por capas:



1. Capa de cifrado: Después de confirmar la conectividad física entre dos pares, se debe verificar el cifrado. Esta capa cifra/descifra los paquetes GRE.

Comandos de depuración comunes utilizados para verificar la parte de cifrado:

debug crypto condition peer ipv4 <WAN IP address of Peer>

debug crypto ikev2

debug crypto ikev2 error

debug crypto ikev2 internal

debug crypto ikev2 packet

debug crypto ipsec

debug crypto ipsec error

O

debug dmvpn condition peer <nmbma/tunnel> <NMBA IP or Tunnel IP address of peer>

debug crypto condition peer ipv4 <WAN IP of the Peer>

debug dmvpn detail crypto

Para obtener información detallada sobre la resolución de problemas de la capa de cifrado, consulte el enlace externo:

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html.

2. GRE/NHRP: Algunos problemas comunes incluyen errores de registro NHRP y cambios de dirección NBMA dinámicos en los radios que conducen a una asignación NHRP incoherente en el hub.

Comandos de depuración comunes utilizados para verificar la asignación NHRP:

debug nhrp condition peer <nbma/tunnel> <NBMA or Tunnel IP address of Peer>

debug nhrp cache

debug nhrp packet

debug nhrp detail

debug nhrp error

Para conocer las soluciones de resolución de problemas de DMVPN más comunes, consulte el enlace externo:

https://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976-dmvpn-troubleshoot-00.html.

3. Ruteo: El protocolo de ruteo no monitorea el estado de los túneles spoke-spoke a petición.

Las actualizaciones de routing IP y los paquetes de datos de multidifusión IP sólo atraviesan los túneles radiales.

Los paquetes de datos IP unidifusión atraviesan los túneles de hub y radio y los túneles de radio a petición.

Depurar: Varios comandos debug dependiendo del protocolo de ruteo.

Para la inmersión profunda de ruteo BGP, consulte el link externo:

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html.

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

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

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