Configure BGP over DMVPN Phase 3

Contents

Introduction

This document describes the configuration and operation of DMVPN Phase 3 using BGP, including layered troubleshooting for IPsec over DMVPN tunnels.

Prerequisites

For the configuration and debug commands in this document, you need two Cisco routers that run Cisco IOS® Release 15.3(3)M or later. In general, a basic Dynamic Multipoint VPN (DMVPN) Phase 3 requires Cisco IOS Release 12.4(6)T, although the features and debugs seen in this document are not fully supported.

Requirements

Cisco recommends that you have basic knowledge of these topics:

- IKEV1/IKEV2 and IPsec
- DMVPN Components:

- Next Hop Resolution Protocol (NHRP): Creates a distributed (NHRP) mapping database of all the spoke's tunnel to real (public interface) addresses
- Multipoint Generic Routing Encapsulation (mGRE) Tunnel Interface: Single Generic Routing Encapsulation (GRE) interface to support multiple GRE/IPsec tunnels, simplifies size and complexity of configuration, and supports dynamic tunnel creation
- IPsec tunnel protection: Dynamically creates and applies encryption policies

- Routing: Dynamic networks; almost all routing protocols (Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol (RIP), Open Shortest Path First (OSPF), BGP, ODR) are supported

Components Used

The information in this document is based on the Cisco ASR1000 Series Aggregation Services Routers, Version 17.6.5(MD).

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

Background Information

What is DMVPN?

DMVPN is a Cisco IOS software solution for building IPsec+GRE VPNs easily, dynamically, and scalable. It is a solution to build a VPN network with multiple sites without having to configure all devices statically. It is a 'hub and spoke' network where the spokes can communicate with each other directly without having to go through the hub. Encryption is supported through IPsec which makes DMVPN a popular choice for connecting different sites using regular Internet connections.

How DMVPN works?

- Spokes build a dynamic permanent GRE/IPsec tunnel to the hub, but not to other spokes. They register as clients of the NHRP server (hub).
- When a spoke needs to send a packet to a destination (private) subnet behind another spoke, it queries via NHRP for the real (outside) address of the destination spoke.
- Now the originating spoke can initiate a dynamic GRE/IPsec tunnel to the target spoke (because it knows the peer address).
- The dynamic spoke-to-spoke tunnel is built over the mGRE interface.
- When traffic ceases, the spoke-to-spoke tunnel is removed.

What are the different types of DMVPN?

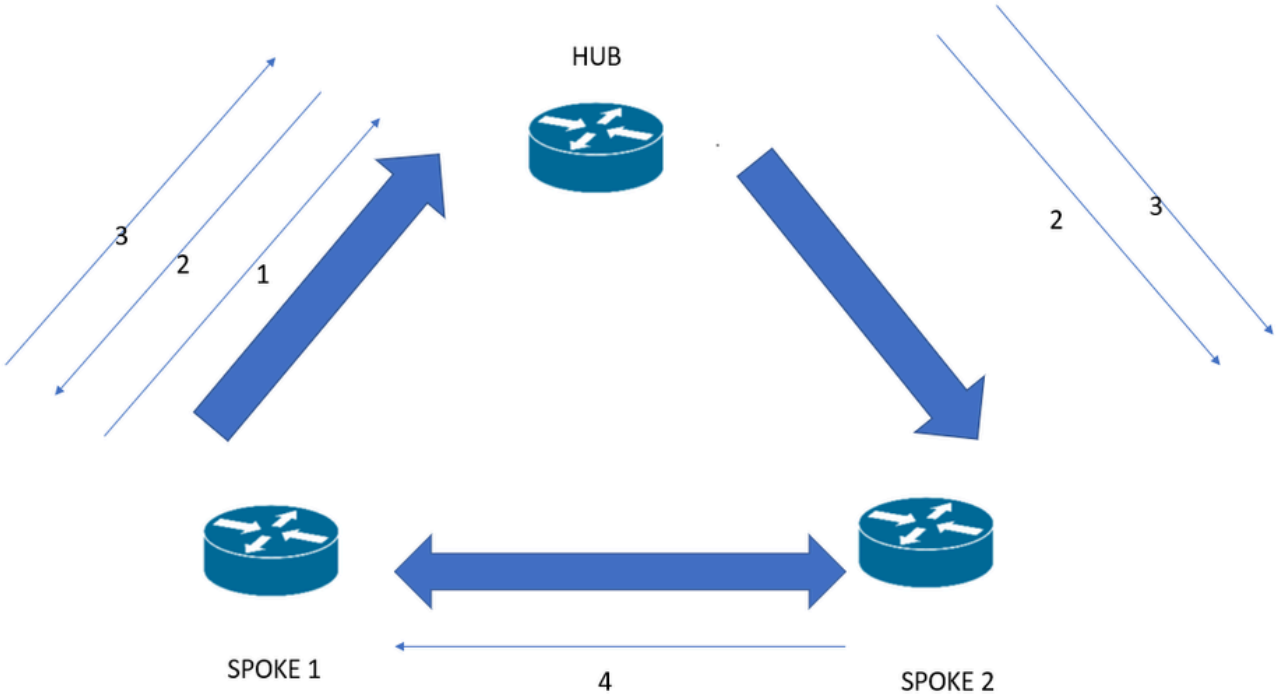
1. DMVPN Phase I: This phase involves a single mGRE interface on the hub, and all the spokes are still static tunnels so you do not get any dynamic spoke-to-spoke connectivity.
2. DMVPN Phase II: This phase involves every site being configured with an mGRE interface so you get your dynamic spoke-to-spoke connectivity.
3. DMVPN Phase III: This phase expands on the scalability of the DMVPN network. This involves summarizing into the DMVPN cloud. Along with configuring NHRP redirects and NHRP shortcut switching. NHRP redirects tell the source to find a better path to the destination it is trying to reach. NHRP shortcuts allow DMVPN to learn about other networks behind other DMVPN routers.

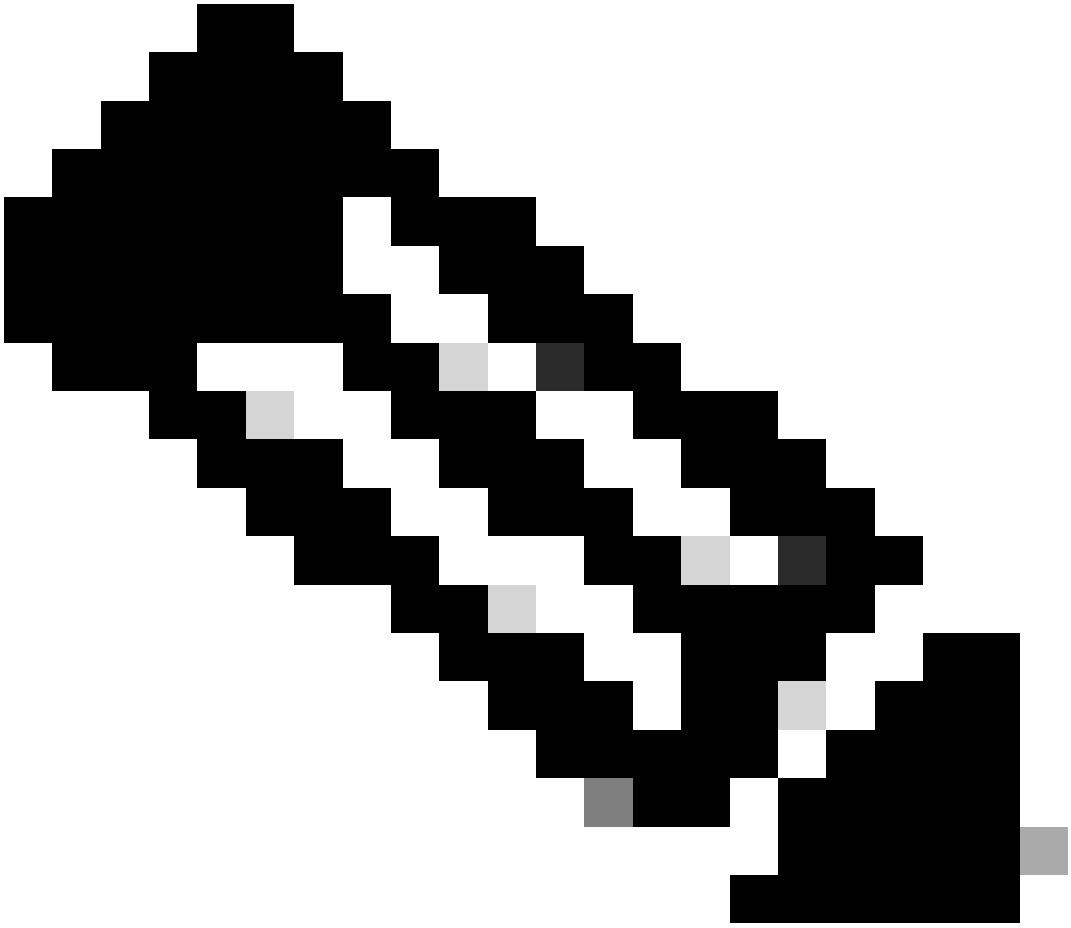
Traffic Flow for DMVPN Phase 3

1. The packet is sent from Spoke’s 1 network to Spoke’s 2 networks via Hub (according to the routing table).
2. Hub routes the packet to Spoke2 but parallelly sends back the NHRP Redirect message to Spoke1 containing information about the suboptimal path to Spoke2 and the tunnel IP of Spoke2.
3. Spoke1 then issues the NHRP Resolution request of Spoke’s 2 Nonbroadcast Multiaccess (NBMA) IP

address to the Next Hop Server (NHS) with the destination IP of Spoke's 2 tunnel. This NHRP Resolution request is sent targeted to **Spoke2 via NHS** (according to the routing table) – it is a normal hop-by-hop NHRP forwarding process.

4. Spoke2 after receiving the resolution request including the NBMA IP of Spoke1 sends the NHRP Resolution reply directly to Spoke1 – **Reply does not traverse the Hub!**
5. Spoke1 after receiving the correct NBMA IP of Spoke2 rewrites the CEF entry for the destination prefix – this procedure is called **NHRP Shortcut**.
6. Spokes do not trigger NHRP by gleaning adjacencies, but NHRP replies update the CEF.



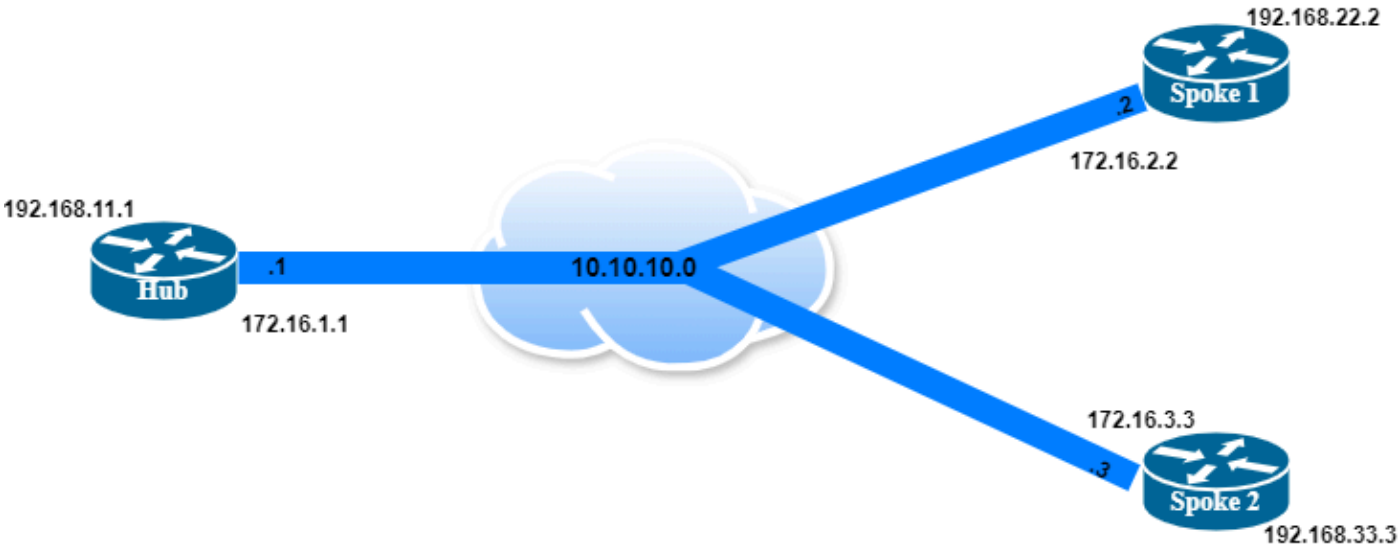


Note:

DMVPN Phase 2: In this phase, the initial spoke-to-spoke packet is indeed process-switched because the CEF adjacency is in the 'glean' state. This means the router does not have enough information to forward the packet using CEF and must use a more resource-intensive process switching to resolve the next hop using NHRP (Next Hop Resolution Protocol).

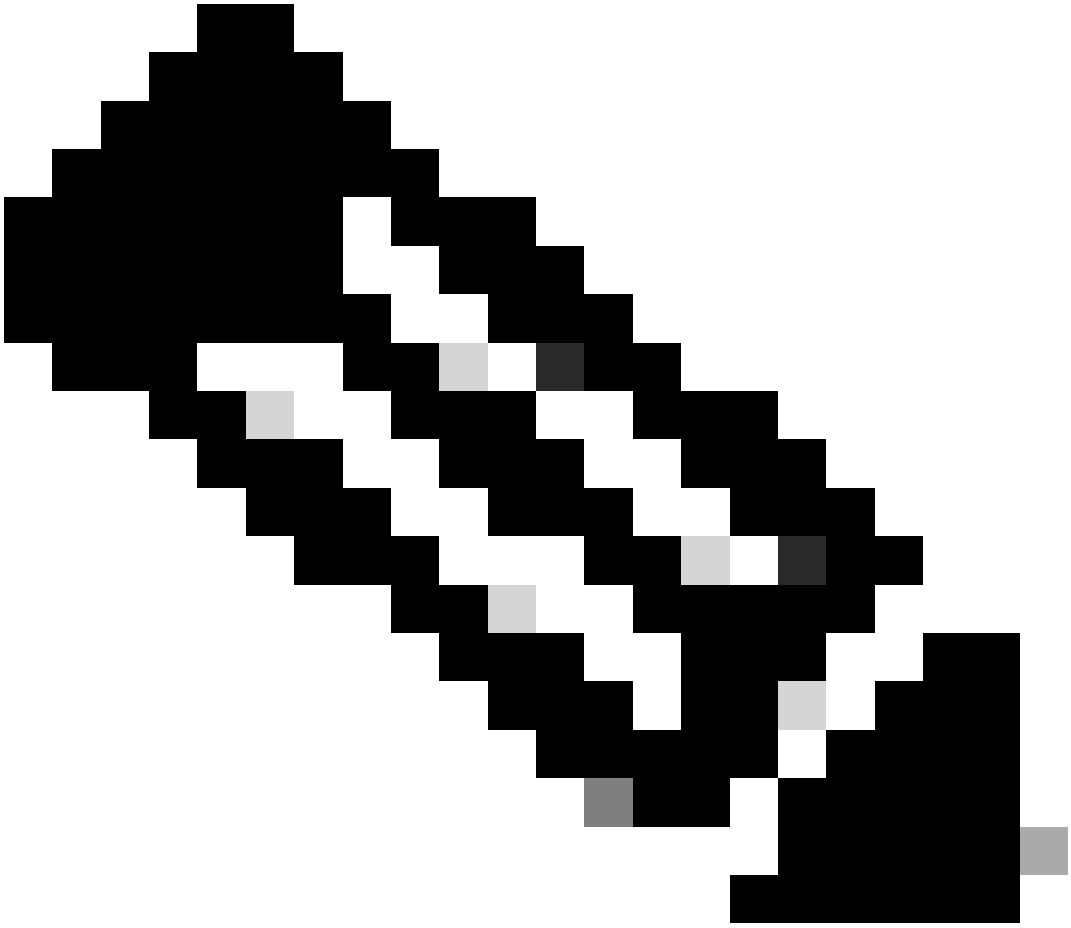
DMVPN Phase 3: This phase improves upon Phase 2 by allowing the initial spoke-to-spoke packet to be switched using CEF from the start. This is achieved through the use of NHRP Redirect and NHRP Shortcut features, which help quickly establish direct spoke-to-spoke tunnels. As a result, CEF is used more consistently, reducing the reliance on process switching.

Network Diagram



Configurations

Crypto Configurations



Note: This is the same on the hub and all the spokes.

1. Configure an Ikev2 proposal and keyring.

```
crypto ikev2 proposal DMVPN
encryption aes-cbc-256
integrity sha256
group 14
crypto ikev2 keyring IKEV2-KEYRING
peer any
address 0.0.0.0 0.0.0.0
pre-shared-key CISCO123
!
```

2. Configure the Ikev2 profile which contains all the connection-related information.

```
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
```

Here is the detail of commands used in the ikev2 profile:

- **match address local interface GigabitEthernet0/0/0**: Local outside interface where VPN terminates, in this case, GigabitEthernet0/0/0
- **match identity remote address 0.0.0.0**: Since remote peer can be multiple, using 0.0.0.0 which indicates any peer
- **authentication local pre-share**: Authentication mode at the local site is pre-shared
- **authentication remote pre-share**: Authentication mode at the local site is pre-shared
- **keyring local IKEV2-KEYRING**: Use the same keyring that you created earlier.

3. Configure IPsec profile.

```
crypto ipsec transform-set T-SET esp-aes 256 esp-sha256-hmac
mode tunnel

crypto ipsec profile IPSEC-IKEV2

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

Create a transform set for the IPsec tunnel negotiation and call the transform set and Ikev2 profile under the IPsec profile.

DMVPN Configuration

1. Configure the outside interface.

```
interface GigabitEthernet0/0/0

ip address 172.16.1.1 255.255.255.0
negotiation auto
cdp enable
```

2. Configure the hub router for mGRE and IPsec integration (that is, associate the tunnel with the IPsec profile configured in the previous procedure)

```
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                    <-------- Mandatory to enable DMVPN Phase 3 on Hub Router
tunnel source GigabitEthernet0/0/0
tunnel mode gre multipoint
tunnel protection ipsec profile IPSEC-IKEV2
!
```

These commands are used in tunnel interface configuration:

- **ip nhrp authentication DMVPN**: In this case, the 'DMVPN' authentication string must have the

same value on all hubs and spokes that are part of the same DMVPN network.
- **ip nhrp map multicast dynamic**: Allows NHRP to add spokes to NHRP multicast mapping dynamically.
- **ip nhrp network-id 1**: 32-bit network identifier which enables NHRP on an interface.
- **ip nhrp redirect**: Enables redirect traffic indication if traffic is forwarded with the NHRP network.
- **tunnel source GigabitEthernet0/0/0**: Sets source address for a tunnel interface, here you are using GigaEthernet 0/0/0 IP address.
- **tunnel mode gre multipoint**: Sets the encapsulation mode to mGRE for this tunnel interface.
- **tunnel protection ipsec profile IPSEC-IKEV2**: Associates a tunnel interface with IPsec Profile which has been already created in crypto configurations.

3. Configure Spoke routers for mGRE and IPsec integration along with an outside interface and Loopback to test Border Gateway Protocol (BGP) connectivity.

SPOKE X: (Similar configuration can be used in all the spokes)

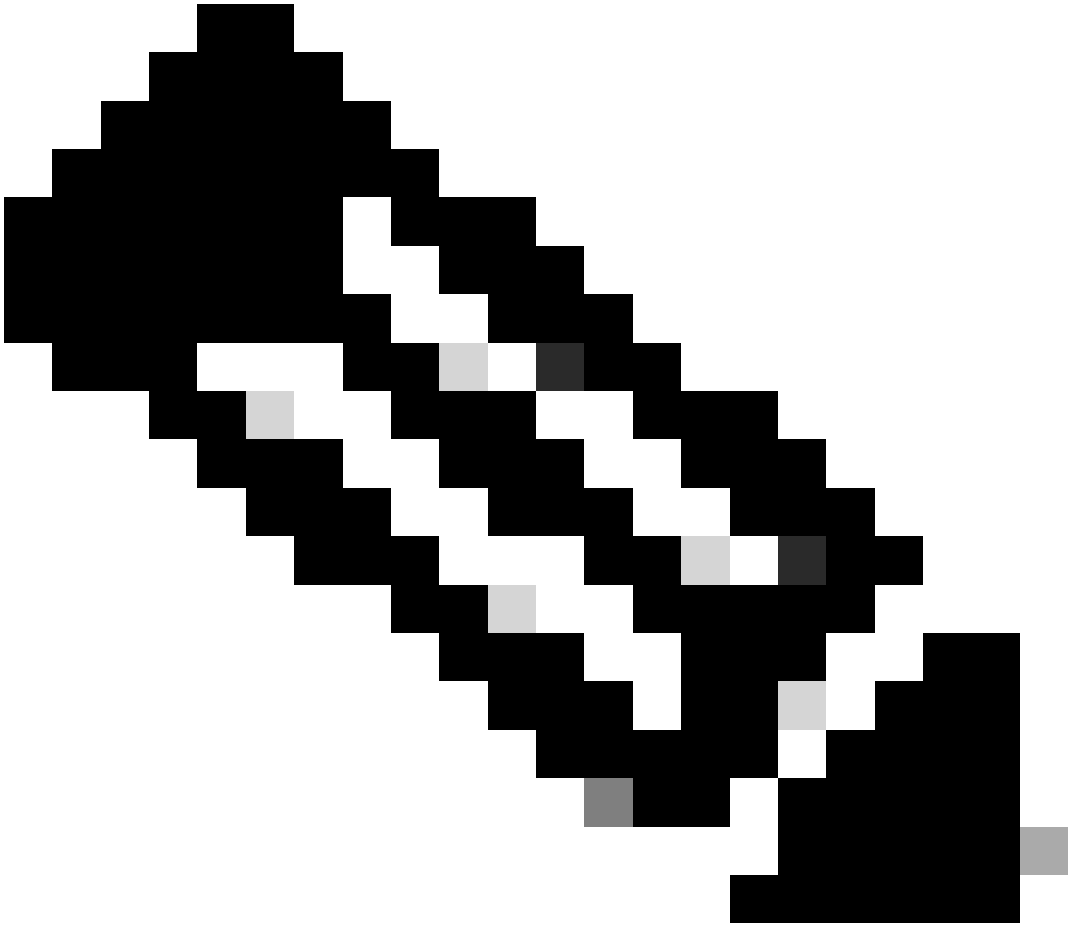
```
interface GigabitEthernet0/0/0
ip address 172.16.3.3 255.255.255.0
speed 1000
no negotiation auto

!

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                    <-------- Mandatory to enable DMVPN Phase 3 on Spoke Router
tunnel source GigabitEthernet0/0/0
tunnel mode gre multipoint
tunnel protection ipsec profile IPSEC-IKEV2
```

These commands are used in tunnel interface configuration:

- **ip nhrp authentication DMVPN**: In this case, the 'DMVPN' authentication string must have the same value on all hubs and spokes that are part of the same DMVPN network.
- **ip nhrp map 10.10.10.1 172.16.1.1**: Manually maps Hub NBMA IP address with tunnel interface IP address.
- **ip nhrp map multicast 172.16.1.1**: Redirects all multicast traffic towards the hub.
- **ip nhrp network-id 1**: 32-bit network identifier which enables NHRP on an interface.
- **ip nhrp nhs 10.10.10.1**: The next hop server which is our hub is configured using this command.
- **ip nhrp shortcut**: Enables NHRP shortcut switching on an interface.
- **tunnel source GigabitEthernet0/0/0**: Sets source address for a tunnel interface, here you are using GigaEthernet 0/0/0 IP address.
- **tunnel mode gre multipoint**: Sets the encapsulation mode to mGRE for this tunnel interface.
- **tunnel protection ipsec profile IPSEC-IKEV2**: Associates a tunnel interface with IPsec Profile which has been already created in crypto configurations.



Note: The **ip nhrp redirect** command sends the message to the Spokes that says “There is a better route to the destination Spoke than via the Hub" and **ip nhrp shortcut** imposes installation of this route in the Forwarding Information Base (FIB) on the Spokes.

BGP Configuration

There are several variations you can choose from:

- eBGP with a different AS number on each spoke
- eBGP with the same AS number on each spoke
- iBGP

Explaining all the three scenarios is out of the scope of this document.

An eBGP with a different AS number on all spokes is configured, so dynamic neighbors cannot be used. Therefore, you must configure the neighbors manually.

eBGP with Different AS on the Spokes

1. BGP configuration on 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

!

These commands are used in the BGP configuration on Hub:

- **router bgp 65010**: Configures a BGP routing process. Use the 'autonomous-system-number' argument that identifies the device to other BGP speakers.
- **network 192.168.11.1 mask 255.255.255.255**: Specifies a network as local to this autonomous system and adds it to the BGP routing table.
- **neighbor 10.10.10.2 remote-as 65011**: Adds the IP address of the neighbor Spoke 1 in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local device.
- **neighbor 10.10.10.3 remote-as 65012**: Adds the IP address of the neighbor Spoke 2 in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local device.

2. BGP configuration on Spoke X:

Spoke2(config)#router bgp 65012

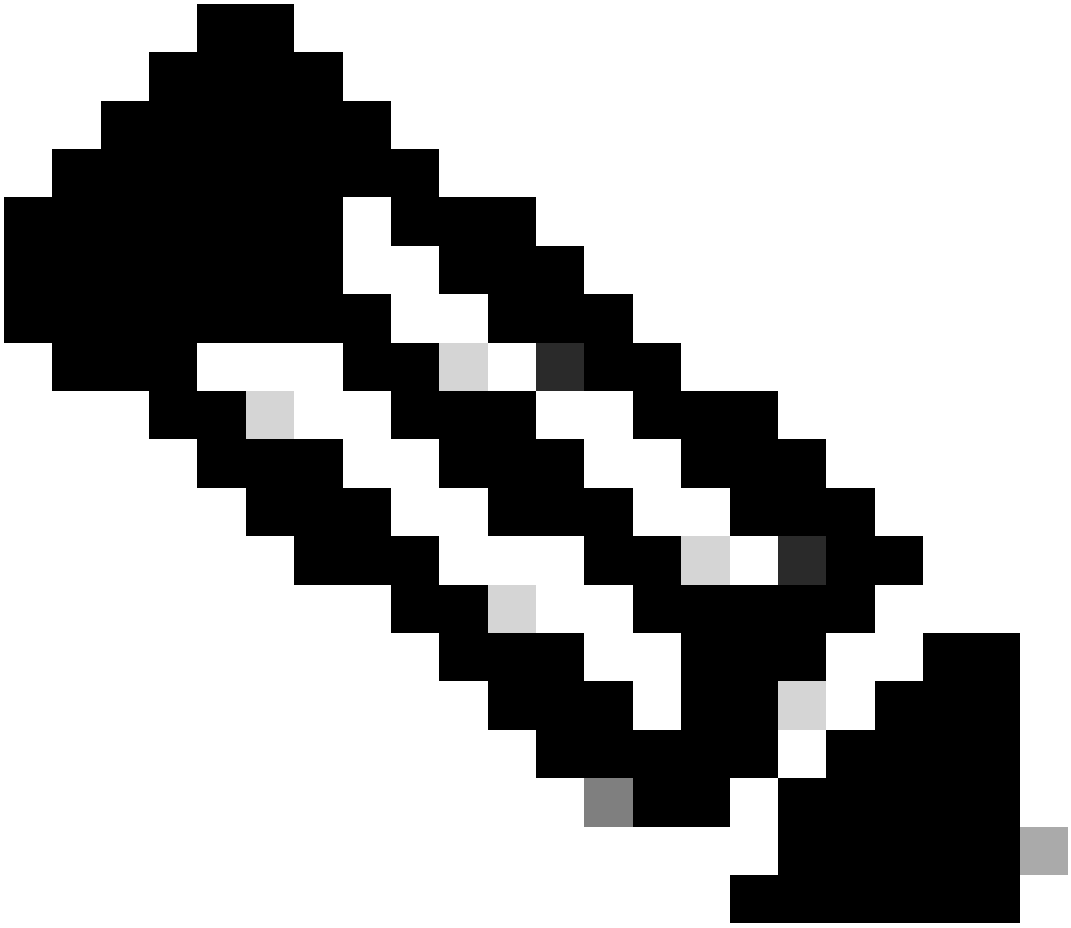
Spoke2(config-router) #bgp log-neighbor-changes

Spoke2(config-router)# network 192.168.33.3 mask 255.255.255.255

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

These commands are used in BGP configuration on Spoke X:

- **router bgp 65012**: Configures a BGP routing process. Use the 'autonomous-system-number' argument that identifies the device to other BGP speakers.
- **network 192.168.33.3 mask 255.255.255.255**: Specifies a network as local to this autonomous system and adds it to the BGP routing table.
- **neighbor 10.10.10.1 remote-as 65010**: Adds the IP address of the Hub in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local device.



Note: A similar configuration must be done on all the spokes in the DMVPN network.

Verify

1. Verification commands on Hub device:

HUB#sh dmvpn

Displays DMVPN-specific session information.

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
T1 - Route Installed, T2 - Nexthop-override
C - CTS Capable
Ent --> Number of NHRP entries with the same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==========

Interface: Tunnel0, IPv4 NHRP Details
Type:Hub, NHRP Peers:2, <<<<<<<<<<<<<<<<<<< **Informs that the device is acting as Hub and 2 NHRP peers are connected to this 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** <<<<<<<<<<<<<<<<<<<<<<<< **Both the peers have dynamically registered with the hub and are in UP state.**
1 172.16.3.3 10.10.10.3 **UP** 01:08:58 **D**

HUB#sh ip nhrp

Shows the NBMA address mapping to tunnel interface IP of all the NHRP peers connected to Hub. Hub maintains the database of all the spokes.

10.10.10.2/32 via 10.10.10.2
Tunnel0 created 01:47:22, expire 01:32:27
Type: dynamic, Flags: unique registered used nhop
NBMA address: 172.16.2.2
10.10.10.3/32 via 10.10.10.3
Tunnel0 created 01:09:11, expire 01:29:58
Type: dynamic, Flags: unique registered used nhop
NBMA address: 172.16.3.3

HUB#sh ip nhrp multicast

Displays NHRP multicast mapping information.

I/F NBMA address
Tunnel0 172.16.2.2 Flags: dynamic (Enabled)
Tunnel0 172.16.3.3 Flags: dynamic (Enabled)

HUB#sh crypto sockets

Number of Crypto Socket connections 2

Tu0 Peers (local/remote): 172.16.1.1/172.16.2.2
Local Ident (addr/mask/port/prot): (172.16.1.1/255.255.255.255/0/47)
Remote Ident (addr/mask/port/prot): (172.16.2.2/255.255.255.255/0/47)
IPSec Profile: "IPSEC-IKEV2"
Socket State: Open
Client: "TUNNEL SEC" (Client State: Active)
Tu0 Peers (local/remote): 172.16.1.1/172.16.3.3
Local Ident (addr/mask/port/prot): (172.16.1.1/255.255.255.255/0/47)
Remote Ident (addr/mask/port/prot): (172.16.3.3/255.255.255.255/0/47)
IPSec Profile: "IPSEC-IKEV2"
Socket State: Open
Client: "TUNNEL SEC" (Client State: Active)
Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "IPSEC-IKEV2" Map-name: "Tunnel0-head-0"

HUB#sh cry ikev2 sa

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.1.1/500 172.16.2.2/500 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/6524 sec

Tunnel-id Local Remote fvrf/ivrf Status
2 172.16.1.1/500 172.16.3.3/500 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/4234 sec

IPv6 Crypto IKEv2 SA

HUB#sh ip bgp summary

Displays the current state of the BGP session/the number of prefixes the router has received from a neighbor or peer group.

BGP router identifier 192.168.11.1 local AS number 65010
The BGP table version is 4, main routing table version is 4.
3 network entries using 432 bytes of memory
3 path entries using 252 bytes of memory
3/3 BGP path/bestpath attribute entries using 480 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1212 total bytes of memory
BGP activity 3/0 prefixes, 3/0 paths, scan interval 60 secs

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

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 172.16.1.2 to network 0.0.0.0

192.168.0.0/16 is variably subnetted, 4 subnets, 2 masks
B 192.168.22.0/24 [20/0] via 10.10.10.2, 00:29:15 <<<<<<<<<<<<<<<<Entry for Spoke 1 advertised routes
B 192.168.33.0/24 [20/0] via 10.10.10.3, 00:18:37 <<<<<<<<<<<<<<<<Entry for Spoke 2 advertised routes

2. Verification commands on Spoke 1:

Spoke1#sh dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
T1 - Route Installed, T2 - Nexthop-override
C - CTS Capable, I2 - Temporary
Ent --> Number of NHRP entries with the same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==========

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers: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 <<<<<<<<<<<<<<<**Hub is showing as S- static since we have configured it as a static entry under tunnel interface**
1 172.16.3.3 10.10.10.3 UP 00:19:34 D <<<<<<<<<<<<<< **Dynamic on-demand Spoke to Spoke tunnel created after sending traffic to Spoke 2**

Spoke1#sh ip bgp summary

BGP router identifier 192.168.22.2, local AS number 65011
The BGP table version is 4, main routing table version is 4.
3 network entries using 744 bytes of memory
3 path entries using 432 bytes of memory
3/3 BGP path/bestpath attribute entries using 864 bytes of memory
2 BGP AS-PATH entries using 64 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2104 total bytes of memory
BGP activity 3/0 prefixes, 3/0 paths, scan interval 60 secs
3 networks peaked at 08:16:54 Jun 2 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** <<<<<<<<<<<<<<<<<<<<<<<< **We have received 2 prefixes from Hub, each for hub loopback and Spoke2 loopback**

Spoke1#sh ip route bgp

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, 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 registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route

+ - replicated route, % - next hop override, p - overrides from PfR

The Gateway of last resort is 172.16.2.10 to network 0.0.0.0

B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:13:16 >>>>>>>>>>>>> Hub network reachable directly via hub

B 192.168.33.0/24 [20/0] via 10.10.10.3, 01:12:46 >>>>>>>>>>>> Spoke network directly reachable via spoke tunnel IP.

Spoke1#sh ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, 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 registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR

The Gateway of last resort is 172.16.2.10 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 172.16.2.10
172.16.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 172.16.2.0/24 is directly connected, GigabitEthernet2
L 172.16.2.2/32 is directly connected, GigabitEthernet2
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.10.10.0/24 is directly connected, Tunnel0
L 10.10.10.2/32 is directly connected, Tunnel0
B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:13:21
192.168.22.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.22.0/24 is directly connected, Loopback10
L 192.168.22.2/32 is directly connected, Loopback10
B 192.168.33.0/24 [20/0] via 10.10.10.3, 01:12:51

Spoke1#sh ip nhrp nhs

Legend: E=Expecting replies, R=Responding, W=Waiting, D=Dynamic
Tunnel0:
10.10.10.1 RE priority = 0 cluster = 0 >>>>>>>>> **Only one Next hop server is configured**

Spoke1#sh ip nhrp traffic

Tunnel0: Max-send limit:10000Pkts/10Sec, Usage:0%
Sent: Total 52
1 Resolution Request 0 Resolution Reply **51 Registration Request** <<<<<<<< **Number of times registration requests were sent to Hub**
0 Registration Reply 0 Purge Request 0 Purge Reply
0 Error Indication 0 Traffic Indication 0 Redirect Suppress
Rcvd: Total 25

0 Resolution Request 1 Resolution Reply 0 Registration Request <<<<<<<<<<< **Number of times we received replies to those registration requests**
24 Registration Reply 0 Purge Request 0 Purge Reply
0 Error Indication 0 Traffic Indication 0 Redirect Suppress

Spoke1#sh ip nhrp multicast

I/F NBMA address
Tunnel0 172.16.1.1 Flags: static (Enabled) <<<<<<<<<<<< **Multicast traffic is configured to be forwarded towards hub NBMA**

Spoke1#sh crypto sockets

Number of Crypto Socket connections **2**

Tu0 Peers (local/remote): 172.16.2.2/172.16.1.1
Local Ident (addr/mask/port/prot): (172.16.2.2/255.255.255.255/0/47)
Remote Ident (addr/mask/port/prot): (172.16.1.1/255.255.255.255/0/47)
IPSec Profile: "IPSEC-IKEV2"
Socket State: Open <<<<<<<<<<<<<<<<<<< **Status of Socket for this particular peer**
Client: "TUNNEL SEC" (Client State: Active)
Tu0 Peers (local/remote): 172.16.2.2/172.16.3.3
Local Ident (addr/mask/port/prot): (172.16.2.2/255.255.255.255/0/47)
Remote Ident (addr/mask/port/prot): (172.16.3.3/255.255.255.255/0/47)
IPSec Profile: "IPSEC-IKEV2"
Socket State: Open
Client: "TUNNEL SEC" (Client State: Active)
Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "IPSEC-IKEV2" Map-name: "Tunnel0-head-0"

Spoke1#sh cry ikev2 sa

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
2 172.16.2.2/500 172.16.3.3/500 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/287 sec

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.2.2/500 172.16.1.1/500 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/4643 sec

IPv6 Crypto IKEv2 SA

Spoke1#traceroute 192.168.33.3 source lo10

Type escape sequence to abort.
Tracing the route to 192.168.33.3

VRF info: (vrf in name/id, vrf out name/id)
1 10.10.10.3 3 msec 4 msec * <<<<<<<<<<<<<< Traffic is directly going to Spoke 2 router without passing through Hub.

Spoke2#sh dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
T1 - Route Installed, T2 - Nexthop-override
C - CTS Capable, I2 - Temporary
Ent --> Number of NHRP entries with the same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==========

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers: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. Verification commands on Spoke 2:

Spoke2#sh ip nhrp

10.10.10.1/32 via 10.10.10.1
Tunnel0 created 01:36:06, never expire
Type: static, Flags:
NBMA address: 172.16.1.1
10.10.10.2/32 via 10.10.10.2
Tunnel0 created 00:08:09, expire 00:01:50
Type: dynamic, Flags: router implicit
NBMA address: 172.16.2.2
10.10.10.3/32 via 10.10.10.3
Tunnel0 created 00:08:09, expire 00:01:50
Type: dynamic, Flags: router unique local
NBMA address: 172.16.3.3
(no-socket)
Spoke2#sh ip nhrp mul
Spoke2#sh ip nhrp multicast
I/F NBMA address
Tunnel0 172.16.1.1 Flags: static (Enabled)
Spoke2#

Spoke2#sh crypto sockets

Number of Crypto Socket connections 2

Tu0 Peers (local/remote): 172.16.3.3/172.16.1.1
Local Ident (addr/mask/port/prot): (172.16.3.3/255.255.255.255/0/47)
Remote Ident (addr/mask/port/prot): (172.16.1.1/255.255.255.255/0/47)
IPSec Profile: "IPSEC-IKEV2"

Socket State: Open <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< **Status of Socket for this particular peer**
Client: "TUNNEL SEC" (Client State: Active)
Tu0 Peers (local/remote): 172.16.3.3/172.16.2.2
Local Ident (addr/mask/port/prot): (172.16.3.3/255.255.255.255/0/47)
Remote Ident (addr/mask/port/prot): (172.16.2.2/255.255.255.255/0/47)
IPSec Profile: "IPSEC-IKEV2"
Socket State: Open
Client: "TUNNEL SEC" (Client State: Active)
Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "IPSEC-IKEV2" Map-name: "Tunnel0-head-0"

Spoke2#sh cry ikev2 sa

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
2 172.16.3.3/500 172.16.2.2/500 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/509 sec

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.3.3/500 172.16.1.1/500 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/4866 sec

IPv6 Crypto IKEv2 SA

Spoke2#sh ip bgp summary

BGP router identifier 192.168.33.3, local AS number 65012
The BGP table version is 4, main routing table version is 4.
3 network entries using 744 bytes of memory
3 path entries using 432 bytes of memory
3/3 BGP path/bestpath attribute entries using 864 bytes of memory
2 BGP AS-PATH entries using 64 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2104 total bytes of memory
BGP activity 3/0 prefixes, 3/0 paths, scan interval 60 secs
3 networks peaked at 08:16:54 Jun 2 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** **>>>>>>>>>>>>>>>>>>>>. We have received 2 prefixes from Hub, each for hub loopback and Spoke2 loopback**

Spoke2#sh ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, 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 registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR

The Gateway of last resort is 172.16.3.10 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 172.16.3.10
172.16.3.0/24/8 is variably subnetted, 2 subnets, 2 masks
C 172.16.3.0/24 is directly connected, GigabitEthernet3
L 172.16.3.3/32 is directly connected, GigabitEthernet3
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.10.10.0/24 is directly connected, Tunnel0
L 10.10.10.3/32 is directly connected, Tunnel0
B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:47:08
B 192.168.22.0/24 [20/0] via 10.10.10.2, 01:46:45
192.168.33.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.33.0/24 is directly connected, Loopback10
L 192.168.33.3/32 is directly connected, Loopback10

Spoke2#sh ip route bgp

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, 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 registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR

The Gateway of last resort is 172.16.3.10 to network 0.0.0.0

B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:21:11 >>>>>>>>>>>>>>>>>**Hub network reachable directly via hub**
B 192.168.22.0/24 [20/0] via 10.10.10.2, 01:20:48 >>>>>>>>>>>> **Spoke network directly reachable via spoke tunnel IP.**

Spoke2#sh ip nhrp nhs

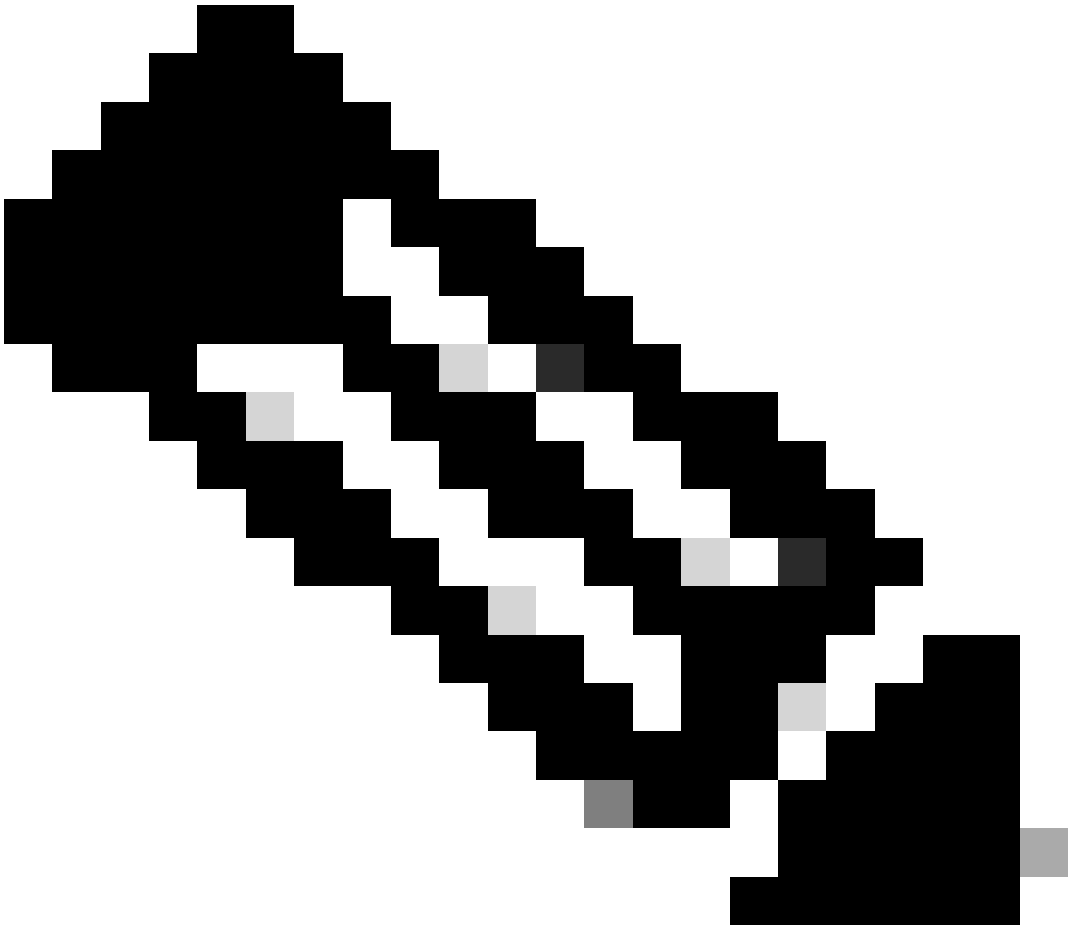
Legend: E=Expecting replies, R=Responding, W=Waiting, D=Dynamic
Tunnel0:
10.10.10.1 RE priority = 0 cluster = 0 >>>>>>>>>>>>>> **Only one Next hop server is configured**

Spoke2#traceroute 192.168.22.2 source loopback 10

Type escape sequence to abort.
Tracing the route to 192.168.22.2

VRF info: (vrf in name/id, vrf out name/id)
1 10.10.10.2 4 msec 4 msec * <<<<<<<<<<<<<< Traffic is directly going to Spoke 1 router without passing through Hub.

Troubleshoot



> **Note**: It is always suggested to use conditional debugs, as running non-conditional debugs can impact the processor and hence the production environment. NBMA address corresponds to the 'outer IP address' (IP address used to source the tunnel interface) and Tunnel IP corresponds to the 'logical IP address, that is, the IP address of the tunnel interface'.

---

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>

In order to troubleshoot DMVPN, you must adopt a layered approach:

debug dmvpn detail all

1. Encryption Layer: After confirming the physical connectivity between two peers, encryption needs to be verified. This Layer encrypts/decrypts GRE packets.

Common Debug commands used to verify the encryption part:

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

OR

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

For a deep-dive understanding of Encryption Layer troubleshooting, refer to the external link:

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

2. GRE/NHRP: Some common issues include NHRP registration fails and dynamic NBMA address changes in spoke leading to inconsistent NHRP mapping in the hub.

Common Debug commands used to verify NHRP mapping:

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

For an understanding of the most common DMVPN troubleshooting solutions, refer to the external link:

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

3. Routing: Routing protocol does not monitor the state of on-demand spoke-spoke tunnels.

IP routing updates and IP multicast data packets only traverse the hub-and-spoke tunnels.

Unicast IP data packets traverse both the hub-and-spoke and on-demand spoke-spoke tunnels.

Debug: Various debug commands depending on the routing protocol.

For the BGP routing deep dive, refer to the external link:

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