Our DMVPN Labs Topology
This is the main topology we will during our labs (Cbtme company had 1 hub(HQ) and two spokes(Branches), each one of them had internet connection.

Internet
int f0/0
ip add 110.110.110.2 255.255.255.0
no sh
int f0/1
ip add 120.120.120.2 255.255.255.0
no sh
int f1/0
ip add 130.130.130.2 255.255.255.0
no sh

Cbtme-Hub
int f0/0
ip add 110.110.110.1 255.255.255.0
no sh
int loop 0
ip add 1.1.1.1 255.255.255.0
int loop 1
ip add 11.11.11.11 255.255.255.0

ip route 120.120.120.0 255.255.255.0 110.110.110.2
ip route 130.130.130.0 255.255.255.0 110.110.110.2
Cbtme-Spoke 1
int f0/0
ip add 120.120.120.1 255.255.255.0
no sh
int loop 0
ip add 2.2.2.2 255.255.255.0
int loop 1
ip add 22.22.22.22 255.255.255.0

ip route 110.110.110.0 255.255.255.0 120.120.120.2
ip route 130.123.130.0 255.255.255.0 120.120.120.2

Cbtme-Spoke 2
int f0/0
ip add 130.130.130.1 255.255.255.0
no sh
int loop 0
ip add 3.3.3.3 255.255.255.0
int loop 1
ip add 33.33.33.33 255.255.255.0

ip route 110.110.110.0 255.255.255.0 130.130.130.2
ip route 120.120.120.0 255.255.255.0 130.130.130.2

To test your Internet connectivity we can use this tiny tclsh script on hub & spokes:

cbtme-Hub#tclsh
cbtme-Hub(tcl)#foreach address {
+>110.110.110.1
+>120.120.120.1
+>130.130.130.1
+>} { ping $address
+>}


DMVPN Configuration Tips

Type of IP address we use:
- Hub & Spokes Public IP address = infrastructure addressing space = Outside Address = Service
  Provide address = NBMA ip address
In our example it will be 110.110.110.1, 120.120.120.1, 130.130.130.1
- Hub & Spokes Private IP address = tunnel ip address = enterprise addressing space = Inside address
In our example it will be 192.168.100.1, 192.,168.100.2, 192.168.100.3

Commands we regularly use:
- ip nhrp map tunnel add nmba add
- ip nhrp nhs tunnel add
- ip nhrp multicast nmba add

Common used terms:
GRE tunnel
- use “tunnel destination” command
- use “tunnel mode gre multipoint” command

mGRE tunnel
- NOT use “tunnel destination” command
- use “tunnel mode gre multipoint” command

Static Mapping
-use “ip nhrp map private ip add public ip add” command

Dynamic Mapping
- NOT -use “ip nhrp map private ip add public ip add” command

DMVPN Phase 1
- Hub use mGRE tunnel
- Spokes use GRE tunnel
- Multicast & Unicast between Hub & Spokes only (spokes talk to each other through hub)
- no need for ip nhrp map multicast dynamic or ip nhrp map multicast x.x.x.x command if no routing protocol used in phase 1

DMVPN Phase 2
- Hub use mGRE tunnel
- Spokes use mGRE tunnel
- Spokes talk to each other directly

DMVPN Phase 3
Same as Phase 2 but instead of using “no next-hop eigrp command“ we use
- ip nhrp redirect in hub
- ip nhrp shortcut in spokes
Lab 1 Phase 1 Static Mapping

Hub
int tunnel 1
ip add 192.168.100.1 255.255.255.0
tunnel source 110.110.110.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.2 120.120.120.1
ip nhrp map 192.168.100.3 130.130.130.1

Spoke 1
int tunnel 1
ip add 192.168.100.2 255.255.255.0
tunnel source 120.120.120.1
tunnel destination 110.110.110.1
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1

Spoke 2
int tunnel 1
ip add 192.168.100.3 255.255.255.0
tunnel source 130.130.130.1
tunnel destination 110.110.110.1
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
**cbtme-Hub#sh dmvpn**

Legend: Attrb --> S - Static, D - Dynamic, I - Incompletea
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer

Tunnel1, Type:Spoke, NHRP Peers:2,
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
----- --------------- ----- ------- ------ ------ ------ -------
1  120.120.120.1  192.168.100.2  NHRP    never S
1  130.130.130.1  192.168.100.3  NHRP    never S

Above you see that R1 is the hub router and that is has two peers. There’s a couple of interesting items that we can find here:

- **Ent** stands for the number of entries in the NHRP database for this spoke router. Normally you will only see 1 entry here.
- **Peer NBMA Addr** is the IP address on the outside interface of the spoke router, in our example 120.120.120.1 and 130.130.10.3
- **Peer Tunnel Add** is the IP address on the tunnel interface of the spoke router.
- **State** shows if your tunnel is up or down.
- **UpDn Tm** is the up or down time of the current state (up or down). You will see the time here once we are using the tunnels.
- **Attrb** means attributes. You can see them at top of the show command. The D stands for **dynamic** which you will normally see for spoke routers.

**cbtme-Spoke1#sh dmvpn**

Legend: Attrb --> S - Static, D - Dynamic, I - Incompletea
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer

Tunnel1, Type:Spoke, NHRP Peers:1,
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
----- --------------- ----- ------- ------ ------ ------- ------ -------
1  110.110.110.1  192.168.100.1  NHRP    never S

**cbtme-Spoke2#sh dmvpn**

Legend: Attrb --> S - Static, D - Dynamic, I - Incompletea
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer

Tunnel1, Type:Spoke, NHRP Peers:1,
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
----- --------------- ----- ------- ------ ------ ------- ------ -------
1  110.110.110.1  192.168.100.3  NHRP    never S
cbtme-Spoke1#ping 192.168.100.3
!!!!!!

cbtme-Hub#sh ip nhrp
192.168.100.2/32 via 192.168.100.2, Tunnel1 created 00:03:00, never expire
   Type: static, Flags:
   NBMA address: 120.120.120.1
192.168.100.3/32 via 192.168.100.3, Tunnel1 created 00:02:59, never expire
   Type: static, Flags: used
   NBMA address: 130.130.130.1

cbtme-Hub#sh ip nhrp br
   Target          Via          NBMA         Mode  Intfc  Claimed
192.168.100.2/32  192.168.100.2  120.120.120.1 static Tu1  < >
192.168.100.3/32  192.168.100.3  130.130.130.1 static Tu1  < >
Lab 2 Phase 1 Dynamic Mapping

Hub
int tunnel 1
ip add 192.168.100.1 255.255.255.0
tunnel source 110.110.110.1
tunnel mode gre multipoint
ip nhrp network 111

(Notice in Hub no ip nhrp map command, since mapping will be dynamic)

Spoke 1
int tunnel 1
ip add 192.168.100.2 255.255.255.0
tunnel source 120.120.120.1
tunnel destination 110.110.110.1
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1

(ip nhrp nhs command send registration request to hub, tells our spoke router who the Next Hop Server (NHS) is)

Spoke 2
int tunnel 1
ip add 192.168.100.3 255.255.255.0
tunnel source 130.130.130.1
tunnel destination 110.110.110.1
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1
cbtme-Hub#sh ip nhrp
192.168.100.2/32 via 192.168.100.2, Tunnel1 created 00:00:30, expire 01:59:29
  Type: dynamic, Flags: unique registered
  NBMA address: 120.120.120.1
192.168.100.3/32 via 192.168.100.3, Tunnel1 created 00:00:21, expire 01:59:38
  Type: dynamic, Flags: unique registered
  NBMA address: 130.130.130.1

cbtme-Spoke1#sh ip nhrp nhs
Legend: E=Expecting replies, R=Responding
Tunnel1: 192.168.100.1 RE

cbtme-Spoke2#sh dm
Legend: Attrb -- S - Static, D - Dynamic, I - Incomplete
  N - NATed, L - Local, X - No Socket
  # Ent --> Number of NHRP entries with same NBMA peer
  NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
  UpDn Time --> Up or Down Time for a Tunnel
===================================
Interface: Tunnel1, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

<table>
<thead>
<tr>
<th># Ent</th>
<th>Peer NBMA Addr</th>
<th>Peer Tunnel Add</th>
<th>State</th>
<th>UpDn Tm</th>
<th>Attrb</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>110.110.110.1</td>
<td>192.168.100.1</td>
<td>UP</td>
<td>00:00:17</td>
<td>S</td>
</tr>
</tbody>
</table>

cbtme-Spoke2#ping 192.168.100.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/373/1056 ms
cbtme-Spoke2#sh dm
Legend: Attrb -- S - Static, D - Dynamic, I - Incomplete
  N - NATed, L - Local, X - No Socket
  # Ent --> Number of NHRP entries with same NBMA peer
  NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
  UpDn Time --> Up or Down Time for a Tunnel
===================================
Interface: Tunnel1, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,

<table>
<thead>
<tr>
<th># Ent</th>
<th>Peer NBMA Addr</th>
<th>Peer Tunnel Add</th>
<th>State</th>
<th>UpDn Tm</th>
<th>Attrb</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>110.110.110.1</td>
<td>192.168.100.1</td>
<td>UP</td>
<td>00:00:29</td>
<td>S</td>
</tr>
<tr>
<td>1</td>
<td>120.120.120.1</td>
<td>192.168.100.2</td>
<td>UP</td>
<td>00:00:01</td>
<td>D</td>
</tr>
</tbody>
</table>
cbtme-Hub#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
===================================================================
Interface: Tunnel1, IPv4 NHRP Details
Type:Hub, NHRP Peers:2,

<table>
<thead>
<tr>
<th># Ent</th>
<th>Peer</th>
<th>NBMA Addr</th>
<th>Peer Tunnel</th>
<th>Add</th>
<th>State</th>
<th>UpDn Tm</th>
<th>Attrb</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>120.120.120.1</td>
<td>192.168.100.2</td>
<td>UP 00:00:13</td>
<td>D</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>130.130.130.1</td>
<td>192.168.100.3</td>
<td>UP 00:00:49</td>
<td>D</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Lab 3 Phase 2 Static Mapping

Hub
int tunnel 1
ip add 192.168.100.1 255.255.255.0
tunnel source 110.110.110.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.2 120.120.120.1
ip nhrp map 192.168.100.3 130.130.130.1

Spoke 1
int tunnel 1
ip add 192.168.100.2 255.255.255.0
tunnel source 120.120.120.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp map 192.168.100.2 120.120.120.1
ip nhrp map 192.168.100.3 130.130.130.1

(notice in phase 2 in spokes we do not used tunnel destination, we use tunnel mode gre multi, we use
ip nhrp map command for hub & other spokes)

Spoke 2
int tunnel 1
ip add 192.168.100.3 255.255.255.0
tunnel source 130.130.130.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp map 192.168.100.2 120.120.120.1
ip nhrp map 192.168.100.3 130.130.130.1
Lab 4 Phase 2 Dynamic Mapping

Hub
int tunnel 1
ip add 192.168.100.1 255.255.255.0
tunnel source 110.110.110.1
tunnel mode gre multipoint
ip nhrp network 111

Spoke 1
int tunnel 1
ip add 192.168.100.2 255.255.255.0
tunnel source 120.120.120.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1

Spoke 2
int tunnel 1
ip add 192.168.100.3 255.255.255.0
tunnel source 130.130.130.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1

cbtme-Spoke2#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
      N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==========================================================================
Interface: Tunnel1, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- -------------- ------ ----- ------- ------
   1 110.110.110.1 192.168.100.1 UP 00:00:09 S

cbtme-Spoke2#ping 192.168.100.2
!!!!!
**cbtme-Spoke2**

```
# sh dmvpn
```

Legend:
- Attrb --> S - Static, D - Dynamic, I - Incomplete
- N - NATed, L - Local, X - No Socket
- # Ent --> Number of NHRP entries with same NBMA peer
- NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
- UpDn Time --> Up or Down Time for a Tunnel

==========================================================================

**Interface: Tunnel1, IPv4 NHRP Details**

**Type:** Spoke, NHRP Peers: 2,

<table>
<thead>
<tr>
<th># Ent</th>
<th>Peer NBMA Addr</th>
<th>Peer Tunnel Add</th>
<th>State</th>
<th>UpDn Tm</th>
<th>Attrb</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>110.110.110.1</td>
<td>192.168.100.1</td>
<td>UP</td>
<td>00:00:30</td>
<td>S</td>
</tr>
<tr>
<td>1</td>
<td>120.120.120.1</td>
<td>192.168.100.2</td>
<td>UP</td>
<td>00:00:03</td>
<td>D</td>
</tr>
</tbody>
</table>

**cbtme-Spoke1**

```
# traceroute 192.168.100.3
```

1 192.168.100.3 48 msec 88 msec 52 msec

```
# sh ip nhrp summ
```

IP NHRP cache 3 entries, 1104 bytes
- 1 static 2 dynamic 0 incomplete

```
# sh ip nhrp traffic
```

Tunnel1: Max-send limit: 100Pkts/10Sec, Usage: 0%

Sent: Total 3
- 1 Resolution Request 1 Resolution Reply 1 Registration Request
- 0 Registration Reply 0 Purge Request 0 Purge Reply
- 0 Error Indication 0 Traffic Indication 0 Redirect Suppress

Rcvd: Total 3
- 1 Resolution Request 1 Resolution Reply 0 Registration Request
- 1 Registration Reply 0 Purge Request 0 Purge Reply
- 0 Error Indication 0 Traffic Indication 0 Redirect Suppress
IGP / EGP over DMVPN

EIGRP over Phase 1
Hub
int tunnel 1
no ip split-horizon eigrp 100
exit
router eigrp 100
no au
exit

EIGRP over Phase 2
Hub
int tunnel 1
no ip split-horizon eigrp 100
no ip next-hop-self eigrp 100
exit
router eigrp 100
no au
exit

OSPF over DMVPN Phase 1
Hub
int tunnel 1
ip ospf pri 10
ip ospf network point-to-multipoint

Spokes
int tunnel 1
ip ospf network point-to-multipoint

OSPF over DMVPN Phase 2
Hub
int tunnel 1
ip ospf pri 10
ip ospf network broadcast

Spokes
int tunnel 1
ip ospf network broadcast

It's good practice to add 'ip ospf pri 0' under spokes tunnel interface

BGP over DMVPN
just need ebgp-multihop in spokes
**Running Multicast before running IGP/EGP**
To run routing protocols we need to make sure multicast is running:

**Phase 1**
_hub (ONLY)_
int tunnel 1
ip nhrp map multicast 192.168.100.2
ip nhrp map multicast 192.168.100.3

or
ip nhrp map multicast dynamic

**Phase 2**
_hub_
int tunnel 1
ip nhrp map multicast dynamic

_spokes_
int tunnel
ip nhrp map multicast 192.168.100.1

**Next few labs our objective is making loops interfaces reachable in hub & spokes**
Lab 5 Phase 1 Dynamic Mapping with EIGRP

Hub
int tunnel 1
ip add 192.168.100.1 255.255.255.0
tunnel source 110.110.110.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map multicast dynamic

Spoke 1
int tunnel 1
ip add 192.168.100.2 255.255.255.0
tunnel source 120.120.120.1
tunnel destination 110.110.110.1
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1

Spoke 2
int tunnel 1
ip add 192.168.100.3 255.255.255.0
tunnel source 130.130.130.1
tunnel destination 110.110.110.1
ip nhrp network 111
ip nhrp map 192.168.100.3 110.110.110.1
ip nhrp nhs 192.168.100.1

Hub
Router eigrp 100
No au
Net 192.168.100.1 0.0.0.0
Net 1.1.1.1 0.0.0.0
Net 11.11.11.11 0.0.0.0
int tunnel 1
no ip split-horizon eigrp 100

Spoke 1
Router eigrp 100
No au
Net 192.168.100.2 0.0.0.0
Net 2.2.2.2 0.0.0.0
Net 22.22.22.22 0.0.0.0

Spoke 2
Router eigrp 100
No au
Net 192.168.100.3 0.0.0.0
Net 3.3.3.3 0.0.0.0
Net 33.33.33.33 0.0.0.0
cbtme-Hub#sh ip route
1.0.0.0/24 is subnetted, 1 subnets
C   1.1.1.0 is directly connected, Loopback0
2.0.0.0/24 is subnetted, 1 subnets
D   2.2.2.0 [90/297372416] via 192.168.100.2, 00:07:38, Tunnel1
33.0.0.0/24 is subnetted, 1 subnets
D   33.33.33.0 [90/297372416] via 192.168.100.3, 00:10:05, Tunnel1
3.0.0.0/24 is subnetted, 1 subnets
D   3.3.3.0 [90/297372416] via 192.168.100.3, 00:10:05, Tunnel1
22.0.0.0/24 is subnetted, 1 subnets
D   22.22.22.0 [90/297372416] via 192.168.100.2, 00:07:40, Tunnel1
110.0.0.0/24 is subnetted, 1 subnets
C   110.110.110.0 is directly connected, FastEthernet0/0
130.130.0.0/24 is subnetted, 1 subnets
S   130.130.130.0 [1/0] via 110.110.110.2
11.0.0.0/24 is subnetted, 1 subnets
C   11.11.11.0 is directly connected, Loopback1
C   192.168.100.0/24 is directly connected, Tunnel1
120.0.0.0/24 is subnetted, 1 subnets
S   120.120.120.0 [1/0] via 110.110.110.2

cbtme-Spoke2#sh ip route
1.0.0.0/24 is subnetted, 1 subnets
D   1.1.1.0 [90/297372416] via 192.168.100.1, 00:10:14, Tunnel1
2.0.0.0/24 is subnetted, 1 subnets
D   2.2.2.0 [90/310172416] via 192.168.100.1, 00:07:47, Tunnel1
33.0.0.0/24 is subnetted, 1 subnets
C   33.33.33.0 is directly connected, Loopback1
3.0.0.0/24 is subnetted, 1 subnets
C   3.3.3.0 is directly connected, Loopback0
22.0.0.0/24 is subnetted, 1 subnets
D   22.22.22.0 [90/310172416] via 192.168.100.1, 00:07:47, Tunnel1
110.0.0.0/24 is subnetted, 1 subnets
S   110.110.110.0 [1/0] via 130.130.130.2
130.130.0.0/24 is subnetted, 1 subnets
C   130.130.130.0 is directly connected, FastEthernet0/0
11.0.0.0/24 is subnetted, 1 subnets
D   11.11.11.0 [90/297372416] via 192.168.100.1, 00:10:17, Tunnel1
C   192.168.100.0/24 is directly connected, Tunnel1
120.0.0.0/24 is subnetted, 1 subnets
S   120.120.120.0 [1/0] via 130.130.130.2
Lab 6 Phase 2 Dynamic Mapping with EIGRP

Hub
int tunnel 1
ip add 192.168.100.1 255.255.255.0
tunnel source 110.110.110.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map multicast dynamic

Spoke 1
int tunnel 1
ip add 192.168.100.2 255.255.255.0
tunnel source 120.120.120.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1
ip nhrp map multicast 110.110.110.1

Spoke 2
int tunnel 1
ip add 192.168.100.3 255.255.255.0
tunnel source 130.130.130.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1
ip nhrp map multicast 110.110.110.1

Hub
Router eigrp 100
No au
Net 192.168.100.1 0.0.0.0
Net 1.1.1.1 0.0.0.0
Net 11.11.11.11 0.0.0.0
int tunnel 1
no ip split-horizon eigrp 100
no ip next-hop-self eigrp 100

Spoke 1
Router eigrp 100
No au
Net 192.168.100.2 0.0.0.0
Net 2.2.2.2 0.0.0.0
Net 22.22.22.22 0.0.0.0
**Spoke 2**

Router eigrp 100
No au
Net 192.168.100.3 0.0.0.0
Net 3.3.3.3 0.0.0.0
Net 33.33.33.33 0.0.0.0

cbtme-Spoke2#sh ip route
   1.0.0.0/24 is subnetted, 1 subnets
   D  1.1.1.0 [90/297372416] via 192.168.100.1, 00:00:30, Tunnel1
   2.0.0.0/24 is subnetted, 1 subnets
   D  2.2.2.0 [90/310172416] via 192.168.100.2, 00:00:29, Tunnel1
   33.0.0.0/24 is subnetted, 1 subnets
   C  33.33.33.0 is directly connected, Loopback1
   3.0.0.0/24 is subnetted, 1 subnets
   C  3.3.3.0 is directly connected, Loopback0
   22.0.0.0/24 is subnetted, 1 subnets
   D  22.22.2.0 [90/310172416] via 192.168.100.2, 00:00:29, Tunnel1
   110.0.0.0/24 is subnetted, 1 subnets
   S   110.110.110.0 [1/0] via 130.130.130.2
   130.130.0.0/24 is subnetted, 1 subnets
   C   130.130.130.0 is directly connected, FastEthernet0/0
   11.0.0.0/24 is subnetted, 1 subnets
   D   11.11.1.0 [90/297372416] via 192.168.100.1, 00:00:33, Tunnel1
   C   192.168.100.0/24 is directly connected, Tunnel1
   120.0.0.0/24 is subnetted, 1 subnets
   S   120.120.120.0 [1/0] via 130.130.130.2

cbtme-Hub#show ip nhrp multicast
   I/F     NBMA address
   Tunnel1  130.130.130.1  Flags: dynamic
   Tunnel1  120.120.120.1  Flags: dynamic

cbtme-Spoke1#show ip nhrp multicast
   I/F     NBMA address
   Tunnel1  110.110.110.1  Flags: static
Lab 7 Phase 1 Dynamic Mapping with OSPF

Hub
int tunnel 1
ip add 192.168.100.1 255.255.255.0
tunnel source 110.110.110.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map multicast dynamic

Spoke 1
int tunnel 1
ip add 192.168.100.2 255.255.255.0
tunnel source 120.120.120.1
tunnel destination 110.110.110.1
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1
ip nhrp map multicast 110.110.110.1

Spoke 2
int tunnel 1
ip add 192.168.100.3 255.255.255.0
tunnel source 130.130.130.1
tunnel destination 110.110.110.1
ip nhrp network 111
ip nhrp map 192.168.100.3 110.110.110.1
ip nhrp nhs 192.168.100.1
ip nhrp map multicast 110.110.110.1

Hub
router ospf 100
network 1.1.1.1 0.0.0.0 area 0
network 11.11.11.11 0.0.0.0 area 0
network 192.168.100.1 0.0.0.0 area 0

int tunnel 1
ip ospf pri 10
ip ospf network point-to-multipoint

Spoke 1
router ospf 100
network 2.2.2.2 0.0.0.0 area 0
network 22.22.22.22 0.0.0.0 area 0
network 192.168.100.2 0.0.0.0 area 0

int tunnel 1
ip ospf network point-to-multipoint
**Spoke 2**

router ospf 100
network 3.3.3.3 0.0.0.0 area 0
network 33.33.33.33 0.0.0.0 area 0
network 192.168.100.3 0.0.0.0 area 0

int tunnel 1
ip ospf network point-to-multipoint

cbtme-Spoke2#sh ip route
    1.0.0.0/32 is subnetted, 1 subnets
O    1.1.1.1 [110/11112] via 192.168.100.1, 00:00:11, Tunnel1
2.0.0.0/32 is subnetted, 1 subnets
O    2.2.2.2 [110/22223] via 192.168.100.1, 00:00:11, Tunnel1
33.0.0.0/24 is subnetted, 1 subnets
C    33.33.33.0 is directly connected, Loopback1
3.0.0.0/24 is subnetted, 1 subnets
C    3.3.3.0 is directly connected, Loopback0
22.0.0.0/32 is subnetted, 1 subnets
O    22.22.22.22 [110/22223] via 192.168.100.1, 00:00:11, Tunnel1
130.130.0.0/24 is subnetted, 1 subnets
C    130.130.130.0 is directly connected, FastEthernet0/0
11.0.0.0/24 is subnetted, 1 subnets
O    11.11.11.11 [110/11112] via 192.168.100.1, 00:00:14, Tunnel1
192.168.100.0/24 is variably subnetted, 3 subnets, 2 masks
C    192.168.100.0/24 is directly connected, Tunnel1
O    192.168.100.1/32 [110/11111] via 192.168.100.1, 00:00:14, Tunnel1
O    192.168.100.2/32 [110/22222] via 192.168.100.1, 00:00:14, Tunnel1
S*   0.0.0.0/0 [1/0] via 130.130.130.2
Lab 8 Phase 2 Dynamic Mapping with OSPF

Hub
int tunnel 1
ip add 192.168.100.1 255.255.255.0
tunnel source 110.110.110.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map multicast dynamic

Spoke 1
int tunnel 1
ip add 192.168.100.2 255.255.255.0
tunnel source 120.120.120.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1
ip nhrp map multicast 110.110.110.1

Spoke 2
int tunnel 1
ip add 192.168.100.3 255.255.255.0
tunnel source 130.130.130.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1
ip nhrp map multicast 110.110.110.1

Hub
router ospf 100
network 1.1.1.1 0.0.0.0 area 0
network 11.11.11.11 0.0.0.0 area 0
network 192.168.100.1 0.0.0.0 area 0
int tunnel 1
ip ospf pri 0
ip ospf network broadcast

Spoke1
router ospf 100
network 2.2.2.2 0.0.0.0 area 0
network 22.22.22.22 0.0.0.0 area 0
network 192.168.100.2 0.0.0.0 area 0
int tunnel 1
ip ospf pri 0 (best practice to add pri0)
ip ospf network broadcast
Spoke 2
router ospf 100
network 3.3.3.3 0.0.0.0 area 0
network 33.33.33.33 0.0.0.0 area 0
network 192.168.100.3 0.0.0.0 area 0
int tunnel 1
ip ospf pri 0  (best practice to add pri0)
ip ospf network broadcast

cbtme-Spoke2#sh ip route
   1.0.0.0/32 is subnetted, 1 subnets
 O  1.1.1.1 [110/11112] via 192.168.100.1, 00:00:30, Tunnel1
   2.0.0.0/32 is subnetted, 1 subnets
 O  2.2.2.2 [110/11112] via 192.168.100.2, 00:00:20, Tunnel1
   33.0.0.0/24 is subnetted, 1 subnets
 C   33.33.33.0 is directly connected, Loopback1
 C   3.0.0.0/24 is subnetted, 1 subnets
 C   3.3.3.0 is directly connected, Loopback0
 O   22.0.0.0/32 is subnetted, 1 subnets
 O   22.22.22.22 [110/11112] via 192.168.100.2, 00:00:20, Tunnel1
   110.0.0.0/24 is subnetted, 1 subnets
 S   110.110.110.0 [1/0] via 130.130.130.2
   130.130.0.0/24 is subnetted, 1 subnets
 C   130.130.130.0 is directly connected, FastEthernet0/0
   11.0.0.0/32 is subnetted, 1 subnets
 O   11.11.11.11 [110/11112] via 192.168.100.1, 00:00:33, Tunnel1
 C   192.168.100.0/24 is directly connected, Tunnel1
   120.0.0.0/24 is subnetted, 1 subnets
 S   120.120.120.0 [1/0] via 130.130.130.2
cbtme-Spoke2#
Lab 9 Phase 3 Dynamic Mapping with EIGRP

Hub
int tunnel 1
ip add 192.168.100.1 255.255.255.0
tunnel source 110.110.110.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map multicast dynamic

Spoke 1
int tunnel 1
ip add 192.168.100.2 255.255.255.0
tunnel source 120.120.120.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1
ip nhrp map multicast 110.110.110.1

Spoke 2
int tunnel 1
ip add 192.168.100.3 255.255.255.0
tunnel source 130.130.130.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1
ip nhrp map multicast 110.110.110.1

Hub
Router eigrp 100
No au
Net 192.168.100.1 0.0.0.0
Net 1.1.1.1 0.0.0.0
Net 11.11.11.11 0.0.0.0
int tunnel 1
no ip split-horizon eigrp 100
ip nhrp redirect

Spoke 1
Router eigrp 100
No au
Net 192.168.100.2 0.0.0.0
Net 2.2.2.2 0.0.0.0
Net 22.22.22.22 0.0.0.0
Int tunnel 1
ip nhrp shortcut
Spoke 2
Router eigrp 100
No au
Net 192.168.100.3 0.0.0.0
Net 3.3.3.3 0.0.0.0
Net 33.33.33.33 0.0.0.0
Int tunnel 1
ip nhrp shortcut

(With EIGRP in Phase 3 we remove ‘no ip next-hop-self eigrp 100’ and we use instead ip nhrp redirect under hub tunnel interface, ip nhrp shortcut under spokes tunnel interface)
Lab 10  Phase 3 Dynamic Mapping with OSPF

Hub
int tunnel 1
ip add 192.168.100.1 255.255.255.0
tunnel source 110.110.110.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map multicast dynamic

Spoke 1
int tunnel 1
ip add 192.168.100.2 255.255.255.0
tunnel source 120.120.120.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1
ip nhrp map multicast 110.110.110.1

Spoke 2
int tunnel 1
ip add 192.168.100.3 255.255.255.0
tunnel source 130.130.130.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1
ip nhrp map multicast 110.110.110.1

Hub
router ospf 100
network 1.1.1.1 0.0.0.0 area 0
network 11.11.11.11 0.0.0.0 area 0
network 192.168.100.1 0.0.0.0 area 0

int tunnel 1
ip nhrp redirect
ip ospf network point-to-multipoint

Spoke 1
router ospf 100
network 2.2.2.2 0.0.0.0 area 0
network 22.22.22.22 0.0.0.0 area 0
network 192.168.100.2 0.0.0.0 area 0
int tunnel 1
ip nhrp shortcut
ip ospf network point-to-multipoint
Spoke 2
router ospf 100
network 3.3.3.3 0.0.0.0 area 0
network 33.33.33.33 0.0.0.0 area 0
network 192.168.100.3 0.0.0.0 area 0
int tunnel 1
ip nhrp shortcut
ip ospf network point-to-multipoint

(In DMVPN phase 3 with OSPF, we use ip nhrp redirect & shortcut BUT we also remove ip ospf pri on hub & spokes, and we change ip ospf net broadcast back to ip ospf network point-to-multipoint)
Lab 11  Phase 2, 3 Dynamic  Mapping with RIP

Hub
int tunnel 1
ip add 192.168.100.1 255.255.255.0
tunnel source 110.110.110.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map multicast dynamic

Spoke 1
int tunnel 1
ip add 192.168.100.2 255.255.255.0
tunnel source 120.120.120.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1
ip nhrp map multicast 110.110.110.1

Spoke 2
int tunnel 1
ip add 192.168.100.3 255.255.255.0
tunnel source 130.130.130.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1
ip nhrp map multicast 110.110.110.1

Hub
router rip
ver 2
no au
net 1.1.1.1
net 11.11.11.11
net 192.168.100.1

in tunnel 1
no ip split-horizon
Spoke 1
router rip
ver 2
no au
net 2.2.2.2
net 22.22.22.22
net 192.168.100.2

Spoke 2
router rip
ver 2
no au
net 3.3.3.3
net 33.33.33.33
net 192.168.100.3

cbtme-Spoke2#sh ip route
  1.0.0.0/24 is subnetted, 1 subnets
   R  1.1.1.0 [120/1] via 192.168.100.1, 00:00:13, Tunnel1
   2.0.0.0/24 is subnetted, 1 subnets
   R  2.2.2.0 [120/2] via 192.168.100.2, 00:00:13, Tunnel1
  33.0.0.0/24 is subnetted, 1 subnets
   C  33.33.33.0 is directly connected, Loopback1
   3.0.0.0/24 is subnetted, 1 subnets
   C  3.3.3.0 is directly connected, Loopback0
   22.0.0.0/24 is subnetted, 1 subnets
   R  22.22.22.0 [120/2] via 192.168.100.2, 00:00:13, Tunnel1
   110.0.0.0/24 is subnetted, 1 subnets
    S  110.110.110.0 [1/0] via 130.130.130.2
    130.130.0.0/24 is subnetted, 1 subnets
   C  130.130.130.0 is directly connected, FastEthernet0/0
    11.0.0.0/24 is subnetted, 1 subnets
    R  11.11.11.0 [120/1] via 192.168.100.1, 00:00:16, Tunnel1
   C  192.168.100.0/24 is directly connected, Tunnel1
    120.0.0.0/24 is subnetted, 1 subnets
    S  120.120.120.0 [1/0] via 130.130.130.2
cbtme-Spoke2#
Lab 12  Phase 1, 2, 3 Dynamic Mapping with BGP

Hub
int tunnel 1
ip add 192.168.100.1 255.255.255.0
tunnel source 110.110.110.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map multicast dynamic

Spoke 1
int tunnel 1
ip add 192.168.100.2 255.255.255.0
tunnel source 120.120.120.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1
ip nhrp map multicast 110.110.110.1

Spoke 2
int tunnel 1
ip add 192.168.100.3 255.255.255.0
tunnel source 130.130.130.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1
ip nhrp map multicast 110.110.110.1
Hub will belong to AS 101
Spoke1 will belong to AS 102
Spoke2 will belong to AS 103
Each device connected to other devices using EBGP

Hub
router bgp 101
net 1.1.1.0 mask 255.255.255.0
net 11.11.11.0 mask 255.255.255.0
nei 192.168.100.2 remote-as 102
nei 192.168.100.3 remote-as 103

Spoke 1
router bgp 102
net 2.2.2.0 mask 255.255.255.0
net 22.22.22.0 mask 255.255.255.0
nei 192.168.100.1 remote-as 101
nei 192.168.100.3 remote-as 103
nei 192.168.100.3 ebpg-multihop 2

Spoke 2
router bgp 103
net 3.3.3.0 mask 255.255.255.0
net 33.33.33.0 mask 255.255.255.0
nei 192.168.100.1 remote-as 101
nei 192.168.100.2 remote-as 102
nei 192.168.100.2 ebpg-multihop 2
cibtme-Hub#sh ip bgp summ
Neighbor  V  AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down  State/PfxRcd
192.168.100.2 4  102 7 7 7 0 0 00:01:48 4
192.168.100.3 4  103 7 7 7 0 0 00:01:48 4

cibtme-Hub#sh ip bgp

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 1.1.1.0/24</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>i</td>
<td></td>
</tr>
<tr>
<td>* 2.2.2.0/24</td>
<td>192.168.100.2</td>
<td>0</td>
<td>103</td>
<td>102 i</td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>192.168.100.2</td>
<td>0</td>
<td>102 i</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 3.3.3.0/24</td>
<td>192.168.100.3</td>
<td>0</td>
<td>102</td>
<td>103 i</td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>192.168.100.3</td>
<td>0</td>
<td>103 i</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 11.11.11.0/24</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>i</td>
<td></td>
</tr>
<tr>
<td>* 22.22.22.0/24</td>
<td>192.168.100.2</td>
<td>0</td>
<td>103</td>
<td>102 i</td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>192.168.100.2</td>
<td>0</td>
<td>102 i</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 33.33.33.0/24</td>
<td>192.168.100.3</td>
<td>0</td>
<td>102</td>
<td>103 i</td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>192.168.100.3</td>
<td>0</td>
<td>103 i</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

cbtme-Spoke2#sh ip bgp summ
Neighbor  V  AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down  State/PfxRcd
192.168.100.1 4  101 8 8 7 0 00:02:15 4
192.168.100.2 4  102 7 7 7 0 00:01:54 4

cbtme-Spoke2#sh ip bgp

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 1.1.1.0/24</td>
<td>192.168.100.1</td>
<td>0</td>
<td>102</td>
<td>101 i</td>
<td></td>
</tr>
<tr>
<td>&gt;</td>
<td>192.168.100.1</td>
<td>0</td>
<td>101 i</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 2.2.2.0/24</td>
<td>192.168.100.2</td>
<td>0</td>
<td>101</td>
<td>102 i</td>
<td></td>
</tr>
<tr>
<td>&gt;</td>
<td>192.168.100.2</td>
<td>0</td>
<td>102 i</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 3.3.3.0/24</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>i</td>
<td></td>
</tr>
<tr>
<td>&gt;</td>
<td>192.168.100.1</td>
<td>0</td>
<td>102</td>
<td>101 i</td>
<td></td>
</tr>
<tr>
<td>* 11.11.11.0/24</td>
<td>192.168.100.1</td>
<td>0</td>
<td>101</td>
<td>i</td>
<td></td>
</tr>
<tr>
<td>&gt;</td>
<td>192.168.100.1</td>
<td>0</td>
<td>101 i</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 22.22.22.0/24</td>
<td>192.168.100.2</td>
<td>0</td>
<td>101</td>
<td>102 i</td>
<td></td>
</tr>
<tr>
<td>&gt;</td>
<td>192.168.100.2</td>
<td>0</td>
<td>102 i</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 33.33.33.0/24</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>i</td>
<td></td>
</tr>
</tbody>
</table>

cbtme-Spoke2#
Lab 13 Protect DMVPN with IPsec

Let’s practice it on Phase 2 Dynamic Mapping with RIP lab 9 we already done before.

**Hub**

int tunnel 1
ip add 192.168.100.1 255.255.255.0
tunnel source 110.110.110.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map multicast dynamic

router rip
ver 2
no au
net 1.1.1.1
net 11.11.11.11
net 192.168.100.1
in tunnel 1
no ip split-horizon

**Spoke 1**

int tunnel 1
ip add 192.168.100.2 255.255.255.0
tunnel source 120.120.120.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1
ip nhrp map multicast 110.110.110.1

router rip
ver 2
no au
net 2.2.2.2
net 22.22.22.22
net 192.168.100.2

**Spoke 2**

int tunnel 1
ip add 192.168.100.3 255.255.255.0
tunnel source 130.130.130.1
tunnel mode gre multipoint
ip nhrp network 111
ip nhrp map 192.168.100.1 110.110.110.1
ip nhrp nhs 192.168.100.1
ip nhrp map multicast 110.110.110.1
router rip
ver 2
no au
net 3.3.3.3
net 33.33.33.33
net 192.168.100.3

**Hub**

crypto isakmp policy 1
encri 3des
hash md5
authentication pre-share
group 2
lifetime 86400
!
crypto isakmp key alya-yasser address 0.0.0.0
< (isakmp key is just my daughter name ;))
crypto ipsec transform-set TS esp-3des esp-md5-hmac
!
crypto ipsec profile protect-gre
set security-association lifetime seconds 86400
set transform-set TS
!
interface Tunnel 1
tunnel protection ipsec profile protect-gre

**Spokes 1 & 2**

crypto isakmp policy 1
encri 3des
hash md5
authentication pre-share
group 2
lifetime 86400
!
crypto isakmp key alya-yasser address 0.0.0.0 0.0.0.0

crypto ipsec transform-set TS esp-3des esp-md5-hmac
!
crypto ipsec profile protect-gre
set security-association lifetime seconds 86400
set transform-set TS
!
interface Tunnel 1
tunnel protection ipsec profile protect-gre
cbtme-Hub#sh crypto session
Crypto session current status

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 120.120.120.1 port 500
  IKE SA: local 110.110.110.1/500 remote 120.120.120.1/500 Active
  IPSEC FLOW: permit 47 host 110.110.110.1 host 120.120.120.1
    Active SAs: 2, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 130.130.130.1 port 500
  IKE SA: local 110.110.110.1/500 remote 130.130.130.1/500 Active
  IPSEC FLOW: permit 47 host 110.110.110.1 host 130.130.130.1
    Active SAs: 2, origin: crypto map

cbtme-Hub#ping 2.2.2.2
!!!!!
cbtme-Hub#ping 33.33.33.33
!!!!!

cbtme-Hub#sh crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
    K - Keepalives, N - NAT-traversal
    X - IKE Extended Authentication
    psk - Preshared key, rsig - RSA signature
    renc - RSA encryption
IPv4 Crypto ISAKMP SA

<table>
<thead>
<tr>
<th>C-id</th>
<th>Local</th>
<th>Remote</th>
<th>I-VRF</th>
<th>Status</th>
<th>Encr</th>
<th>Hash</th>
<th>Auth</th>
<th>DH</th>
<th>Lifetime</th>
<th>Cap.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1002</td>
<td>110.110.110.1</td>
<td>130.130.130.1</td>
<td></td>
<td>ACTIVE</td>
<td>3des</td>
<td>md5</td>
<td>psk</td>
<td>2</td>
<td>23:55:53</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Engine-id:Conn-id = SW:2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1001</td>
<td>110.110.110.1</td>
<td>120.120.120.1</td>
<td></td>
<td>ACTIVE</td>
<td>3des</td>
<td>md5</td>
<td>psk</td>
<td>2</td>
<td>23:55:48</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Engine-id:Conn-id = SW:1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IPv6 Crypto ISAKMP SA
cbtme-Hub#show crypto sockets

Number of Crypto Socket connections 2

Tu1 Peers (local/remote): 110.110.110.1/130.130.130.1
  Local Ident (addr/mask/port/prot): (110.110.110.1/255.255.255.255/0/47)
  Remote Ident (addr/mask/port/prot): (130.130.130.1/255.255.255.255/0/47)
  IPSec Profile: "protect-gre"
  Socket State: Open
  Client: "TUNNEL SEC" (Client State: Active)
Tu1 Peers (local/remote): 110.110.110.1/120.120.120.1
  Local Ident (addr/mask/port/prot): (110.110.110.1/255.255.255.255/0/47)
  Remote Ident (addr/mask/port/prot): (120.120.120.1/255.255.255.255/0/47)
  IPSec Profile: "protect-gre"
  Socket State: Open
  Client: "TUNNEL SEC" (Client State: Active)

Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "protect-gre" Map-name: "Tunnel1-head-0"

cbtme-Spoke2#sh crypto session
Crypto session current status

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 110.110.110.1 port 500
  IKE SA: local 130.130.130.1/500 remote 110.110.110.1/500 Active
  IPSEC FLOW: permit 47 host 130.130.130.1 host 110.110.110.1
  Active SAs: 2, origin: crypto map

cbtme-Spoke2#
Lab14 DMVPN QoS (Per Tunnel QoS, pre classify)

QoS Pre Classify:

- VPN will encrypt the packet and add (encapsulate) VPN header to it.
- QoS Pre Classify is an IOS feature that allows us to classify packets before encryption and encapsulation, and will move internal TOS to VPN header.
- Remember classification must happen before encryption.
- QoS Pre Classify can be applied under physical interfaces, when using GRE it will be applied under tunnel interface and we cannot apply under crypto-map for IPsec tunnel.

```
Int s0/0
Qos pre-classify
or
Int tunnel 1
Qos pre-classify
or
Crypto-map Yasser
Qos pre-classify
```

Per-Tunnel QoS (Hierarchical policy with nhrp Group):

- When apply MQC we can create a parent policy that will apply to all spokes and inside it we have child policies for each spoke.
- The main point here is telling the tunnels about these policies and this can be done as the following:

```
Hub
Int tunnel 1
ip nhrp map group group name service-policy output parent policy name
```

```
Spoke
Int tunnel 1
ip nhrp group group name
```

- Spokes can share the same group name or belong to different groups.
- If you practice it with GNS3 use 7200 IOS, since it supports ip nhrp map group command.
Hub
class-map http
match protocol http

policy-map child-speoke1
class http
priority 512

policy-map child-speoke2
class http
priority 256

policy-map parent-speoke1
class class-default
shape average 2000000
service-policy child-speoke1

policy-map parent-speoke2
class class-default
shape average 1000000
service-policy child-speoke2

int tunnel 1
ip nhrp map group SPOKE-1-GROUP service-policy output parent-speoke1
ip nhrp map group SPOKE-2-GROUP service-policy output parent-speoke2
qos pre-classify

spoke1
int tunnel1
ip nhrp group SPOKE-1-GROUP

spoke 2
int tunnel 1
ip nhrp group SPOKE-2-GROUP
**cbtme-Hub#sh dmvpn detail**

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete  
N - NATed, L - Local, X - No Socket  
# Ent --> Number of NHRP entries with same NBMA peer  
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting  
UpDn Time --> Up or Down Time for a Tunnel

---

Interface Tunnel1 is up/up, Addr. is 192.168.100.1, VRF ""
Tunnel Src./Dest. addr: 110.110.110.1/MGRE, Tunnel VRF ""
Protocol/Transport: "multi-GRE/IP", Protect ""
Interface State Control: Disabled  
nhrp event-publisher : Disabled  
Type:Hub, Total NBMA Peers (v4/v6): 2

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network  
----- -------- -------- -------- -------- ------ -------
1 120.120.120.1 192.168.100.2 UP 00:03:57 D 192.168.100.2/32

**NHRP group: SPOKE-1-GROUP**  
Output QoS service-policy applied: parent-spoke1  
1 130.130.130.1 192.168.100.3 UP 00:03:42 D 192.168.100.3/32

**NHRP group: SPOKE-2-GROUP**  
Output QoS service-policy applied: parent-spoke2

---

Crypto Session Details:

---

Pending DMVPN Sessions:

**cbtme-Hub#sh ip nhrp group-map**

Interface: Tunnel1  
NHRP group: SPOKE-1-GROUP  
QoS policy: parent-spoke1  
Tunnels using the QoS policy:
Tunnel destination overlay/transport address  
192.168.100.2/120.120.120.1

NHRP group: SPOKE-2-GROUP  
QoS policy: parent-spoke2  
Tunnels using the QoS policy:
Tunnel destination overlay/transport address  
192.168.100.3/130.130.130.1

---

To check that the policy is in effect:
**cbtme-Hub#show policy-map multipoint**
**DMVPN Tuning**

- We can tune GRE / m GRE tunnel interface, to avoid problems with fragmentation of user packets in GRE Tunnels, set the IP MTU side with the ip mtu command and set the TCP MSS value using the ip tcp adjust-mss interface command.

```
int tunnel 1
ip mtu 1400
ip tcp adjust-mss 1360
```

- We can make interface source in spokes (tunnel source fo/0) if its DHCP client and getting Dynamic Public Ip address in f0/0 from Internet SP.

- Configuring an authentication string ensures that only routers configured with the same string can communicate using NHRP. So to have authentication under hub & spokes we add:

```
int tunnel 1
ip nhrp authentication cbtme
```

- Changing the Length of Time NBMA Addresses Are Advertised as Valid
  The default length of time is 7200 seconds (2 hours).
  This controls how long a spoke-to-spoke shortcut path will stay up after it is no longer used or how often the spoke-to-spoke short-cut path mapping entry will be refreshed if it is still being used. We recommend that a value from 300 to 600 seconds be used.

```
ip nhrp holdtime 600  < NHRP NBMA addresses are advertised as valid in positive NHRP responses for 10 minutes.

ip nhrp registration timeout 100 < NHRP registration requests are now sent every 100 seconds (default value is one third NHRP holdtime value).
```

**Configuring NHRP Server-Only Mode**

You can configure an interface so that it cannot initiate NHRP resolution requests to establish NHRP shortcut SVCs but can respond only to NHRP resolution requests. Configure NHRP server-only mode on routers you do not want placing NHRP resolution requests.

If an interface is placed in NHRP server-only mode, you have the option to specify the ip nhrp server-only[non-caching] command keyword. In this case, NHRP does not store mapping information in the NHRP cach, such as NHRP responses that go through the router. To save memory and block building of NHRP shortcuts, the non-caching option is generally used on a router located between two other NHRP routers (NHRP hubs).

```
ip nhrp server-only non-caching
```
Controlling the Triggering of NHRP

There are two ways to control when NHRP is triggered on any platform. These methods are:

- Triggering NHRP on a per-Destination Basis
  ```
  access-list 110 permit ip any any
  int tunnel 1
  ip nhrp interset 110
  ```

- Triggering NHRP on a Packet Count Basis
  ```
  int tunnel 1
  ip nhrp use 5
  ```

  In this example, if in the first minute five packets are sent to the first destination and five packets are sent to a second destination, then a single NHRP request is generated for the second destination. If in the second minute the same traffic is generated and no NHRP responses have been received, then the system resends its request for the second destination.

Controlling the NHRP Packet Rate

There is the maximum value for the number of NHRP messages that the local NHRP process can handle within a set period of time. This limit protects the router against things like a runaway NHRP process sending NHRP requests or an application (worm) that is doing an IP address scan that is triggering many spoke-to-spoke tunnels. The larger the Max-send-interval the more NHRP packets the system can process and send.

```
int tunnel 1
ip nhrp max-send 10 every 10
```

Clearing the NHRP Cache

The NHRP cache can contain entries of statically configured NHRP mappings and dynamic entries caused by the Cisco IOS software learning addresses from NHRP packets. To clear statically configured entries, use the `no ip nhrp map` command in interface configuration mode.

```
clear ip nhrp
```

Verification commands for all phases

```
sh ip nhrp
sh ip nhrp detail
show ip nhrp nhs
debug nhrp packet
sh dmvpn
show ip nhrp multicast
```
DMVPN troubleshooting

1-
DMVPN misconfiguration will lead you to see the word “negative”

```
cbtme-Hub#sh ip nhrp
192.168.100.2/32, Tunnel1 created 00:00:26, expire 00:02:38
 Type: incomplete, Flags: negative
 Cache hits: 5
192.168.100.3/32, Tunnel1 created 00:00:39, expire 00:02:25
 Type: incomplete, Flags: negative
 Cache hits: 6
```

Check ip nhrp map & ip nhrp nhs in the spokes, fix anything misconfigured then type "clear ip nhrp" in your hub

```
cbtme-Hub#sh ip nhrp
192.168.100.2/32 via 192.168.100.2, Tunnel1 created 00:01:05, expire 01:59:15
 Type: dynamic, Flags: unique registered
 NBMA address: 120.120.120.1
192.168.100.3/32 via 192.168.100.3, Tunnel1 created 00:01:37, expire 01:58:22
 Type: dynamic, Flags: unique registered
 NBMA address: 130.130.130.1
```

2-
One of the useful command during troubleshooting is:

```
cbtme-Hub#show tunnel endpoint tunnel1
Tunnel1 running in multi-GRE/IP mode
 Endpoint transport 120.120.120.1 Refcount 2 Base 0x67053940
 overlay 192.168.100.2 Refcount 2 Parent 0x67053940
 Endpoint transport 130.130.130.1 Refcount 2 Base 0x67053880
 overlay 192.168.100.3 Refcount 2 Parent 0x67053880
```

3-
be careful from this command when you see it in Hub:
ip nhrp server-only NON-caching

spokes will talk to each others but hub tunnel ip will not be reachable for them and also sh dmvpn , sh ip nhrp in hub will not show anything

4-
ip nhrp interest command controls which packets cause NHRP address resolution to take place; the ip nhrp use command controls how readily the system attempts such address resolution.
In the following example, any TCP traffic (classified by ACL 101) can cause NHRP requests to be sent, but no other IP packets will cause NHRP requests:

```
ip nhrp interest 101
```
5-
Tunnel key number: This is another mechanism to keep your DMVPN network clean of any unwanted members, this is actually built into the GRE encapsulation itself, only GRE’s tunnels with the same tunnel key can communicate. So if the hub is using Tunnel key 10, then the spoke must use tunnel key 10 as well, if not then they will not be able to communicate.

6-
Troubleshooting commands:
sh dmvpn
sh dmvpn detail
sh dmvpn peer nbma 120.120.120.1
sh dmvpn peer tunnel 192.168.100.2
sh dmvpn interface tunnel 1

sh ip nhrp
sh ip nhrp summ
sh ip nhrp multicast
sh ip nhrp traffic
sh ip nhrp nhs
sh ip nhrp incomplete
sh ip nhrp brief

cbtme-Hub# debug dmvpn ?
 all   enable all level debugging
 condition  conditional debugging for enabled
 detail   detailed reports
 error    error reports
 packet   packet level debugging

cbtme-Hub# debug nhrp ?
 attribute  NHRP attribute
 cache    NHRP cache operations
 condition  NHRP conditional debugging
 error     NHRP errors
 extension  NHRP extension processing
 group     NHRP groups
 packet    NHRP activity
 rate      NHRP rate limiting
 routing   NHRP routing
DMVPN with FQDN

spoke could use local dns server
ip domain-lookup
ip host hub1.cbtme.com 110.110.110.1

but lest external DNS (internet Router)
ip domain-lookup
ip name-server 120.120.120.2

Internet router
ip dns server
ip host hub1.cbtme.com 110.110.110.1

spoke 1
interface Tunnel1
ip address 192.168.100.2 255.255.255.0
no ip redirects
ip nhrp network-id 111
ip nhrp nhs dynamic nbma hub1.cbtme.com multicast
ip nhrp registration no-unique
ip nhrp registration timeout 10
ip nhrp shortcut
tunnel source 120.120.120.1
tunnel mode gre multipoint

cbtme-Spoke2#sh dmvpn
# Ent  Peer NBMA Addr  Peer Tunnel Add  State  UpDn Tm Attrib
-----  ---------------  ---------------  ----  --------  ----  ------  -----  -------
1 110.110.110.1  192.168.100.1  UP  00:04:53  S
(hub1.cbtme.com)

cbtme-Spoke1#sh dmvpn
# Ent  Peer NBMA Addr  Peer Tunnel Add  State  UpDn Tm Attrib
-----  ---------------  ---------------  ----  --------  ----  ------  -----  -------
1 110.110.110.1  192.168.100.1  UP  00:01:39  S
(hub1.cbtme.com)
DMVPN DHCP Tunnel support

- DHCP broadcast packets from a spoke are converted to unicast towards the hub router
- DHCP broadcast packets from a spoke are not relayed to other spokes

Restrictions for DHCP Tunnels Support

A DHCP server cannot be deployed on a DMVPN hub. A DMVPN hub must act as a relay agent and the DHCP server must be deployed adjacent to the DMVPN hub.

The DHCP functionality of address validation is not supported on DMVPN.

spokes

int tunnel 1
ip add dhcp

Configuring the DHCP Relay Agent to Unicast DHCP Replies
Perform this task to configure the DHCP relay agent to unicast DHCP replies.

By default, the DHCP replies are broadcast from the DMVPN hub to the spoke. Therefore a bandwidth burst occurs. The DHCP--Tunnels Support feature does not function if the DHCP messages are broadcast. Hence, you must configure the DHCP relay agent to unicast the DHCP messages for the DHCP to be functional in a DMVPN environment.

hub

config t
ip dhcp support tunnel unicast

Configuring a DMVPN Spoke to Clear the Broadcast Flag
Perform this task to configure a DMVPN spoke to clear the broadcast flag.

By default, DMVPN spokes set the broadcast flag in the DHCP DISCOVER and REQUEST messages. Therefore the DHCP relay agent is forced to broadcast the DHCP replies back to the spokes, even though the relay agent has sufficient information to unicast DHCP replies. Hence, you must clear the broadcast flag from the DMVPN spoke.

spokes

int tunnel 1
ip dhcp client broadcast-flag clear
Internet
ip route 200.200.200.0 255.255.255.0 110.110.110.1

Spoke 1
ip route 200.200.200.0 255.255.255.0 120.120.120.2

spoke 2
ip route 200.200.200.0 255.255.255.0 130.130.130.2

Hub
int f0/1
ip add 200.200.200.100 255.255.255.0
no sh

R5
int f0/1
ip add 200.200.200.200 255.255.255.0
no sh
ip route 0.0.0.0 0.0.0.0 200.200.200.100

ip dhcp pool 192
network 192.168.100.0 255.255.255.0
exit
ip dhcp excluded-address 192.168.100.1
ip dhcp excluded-address 192.168.100.4 192.168.100.254

Hub
ip dhcp support tunnel unicast
int tunnel 1
ip helper-address 200.200.200.200
spoke 1
  in tunnel 1
  ip add dhcp
  ip dhcp client broadcast-flag clear

spoke 2
  in tunnel 1
  ip add dhcp
  ip dhcp client broadcast-flag clear

cbtme-Spoke2#sh int br | i Tunnel
Tunnel1     192.168.100.3   YES DHCP   up                    up

cbtme-Spoke1#sh int br | i Tunnel
Tunnel1     192.168.100.2   YES DHCP   up                    up
IPv6 over IPv4 DMVPN

Restrictions for IPv6 over DMVPN
IPv6 can be configured only on a protected network.
IPv6 VRFs are not fully supported by IPv6 routing protocols such as EIGRP or OSPF. Therefore, DMVPN for IPv6 does not support IPv6 VRFs.

IPv6 Addressing and Restrictions
IPv6 allows multiple unicast addresses on a given IPv6 interface. IPv6 also allows special address types, such as anycast, multicast, link-local addresses, and unicast addresses.

DMVPN for IPv6 has the following addressing restrictions:

Every IPv6 NHRP interface is configured with one IPv6 unicast address. This address can be a globally reachable or unique local address.
Every IPv6 NHRP interface is configured with one IPv6 link-local address that is unique across all DMVPN hosts in the DMVPN cloud (that is, the hubs and spokes).
If no other tunnels on the device are using the same tunnel source, then the tunnel source address can be embedded into an IPv6 address.
If the device has only one DMVPN IPv6 tunnel, then manual configuration of the IPv6 link-local address is not required. Instead, use the ipv6 enable command to autogenerate a link-local address.
If the device has more than one DMVPN IPv6 tunnel, then the link-local address must be manually configured using the ipv6 address fe80::2001 link-local command.

IPv6 DMVPN Types:
In IPv6 over IPv4 DMVPN we already have ipv4 dmvpn and will use it to transport ipv6

In DMVPN over IPv6 Transport we already have ipv6 global address and will create dmvpn for it in this case “tunnel mode gre multipoint ipv6” and we can use IKEv2 for optional IPsec.

Our Lab will be IPv6 over IPv4 DMVPN:

hub
ipv6 uni
int tunnel 1
ipv6 add 2001:db8:1:1::70/64
ipv6 add fe80::2001 link-local
ipv6 nhrp map multicast dynamic
ipv6 nhrp network-id 111
ipv6 nhrp redirect
ipv6 eigrp 100
spoke 1
ipv6 uni
int tunnel 1
ipv6 add 2001:db8:1:1::71/64
ipv6 nhrp network-id 111
ipv6 nhrp map 2001:db8:1:1::70/64 110.110.110.1
ipv6 nhrp shortcut
ipv6 nhrp map multicast 110.110.110.1
ipv6 nhrp nhs 2001:db8:1:1::70
ipv6 eigrp 100

spoke 2
ipv6 uni
int tunnel 1
ipv6 add 2001:db8:1:1::72/64
ipv6 nhrp network-id 111
ipv6 nhrp map 2001:db8:1:1::70/64 110.110.110.1
ipv6 nhrp shortcut
ipv6 nhrp map multicast 110.110.110.1
ipv6 nhrp nhs 2001:db8:1:1::70
ipv6 eigrp 100

cbtme-Hub#sh dmvpn
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrib
----- ------------------ ------ --------- ----- ------- -----
1  120.120.120.1     192.168.100.2    UP 00:44:33     D
1  130.130.130.1     192.168.100.3    UP 00:44:19     D

Interface: Tunnel1, IPv6 NHRP Details
Type:Hub, Total NBMA Peers (v4/v6): 2
1.Peer NBMA Address: 120.120.120.1
   Tunnel IPv6 Address: 2001:DB8:1:1::71
   IPv6 Target Network: 2001:DB8:1:1::71/128
   # Ent: 1, Status: UP, UpDn Time: 00:01:47, Cache Attrib: D
2.Peer NBMA Address: 130.130.130.1
   Tunnel IPv6 Address: 2001:DB8:1:1::72
   IPv6 Target Network: 2001:DB8:1:1::72/128
   # Ent: 1, Status: UP, UpDn Time: 00:00:36, Cache Attrib: D

cbtme-Spoke2#ping 2001:DB8:1:1::71
!!!!
cbtme-Spoke2#sh dmvpn

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
----- --------------------- ----- ----- ----- ----- ----- ----
1  110.110.110.1     192.168.100.1    UP  00:44:09     S

Interface: Tunnel1, IPv6 NHRP Details
Type: Spoke, Total NBMA Peers (v4/v6): 2
1. Peer NBMA Address: 110.110.110.1
   Tunnel IPv6 Address: 2001:DB8:1:1::70
   IPv6 Target Network: 2001:DB8:1:1::/64
   # Ent: 1, Status: UP, UpDn Time: 00:00:26, Cache Attrib: S
2. Peer NBMA Address: 120.120.120.1
   Tunnel IPv6 Address: 2001:DB8:1:1::71
   IPv6 Target Network: 2001:DB8:1:1::71/128
   # Ent: 1, Status: UP, UpDn Time: 00:00:04, Cache Attrib: D

cbtme-Hub# sh dmvpn ipv6

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
      N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==========================================================================
Interface: Tunnel1, IPv6 NHRP Details
Type: Hub, Total NBMA Peers (v4/v6): 2
1. Peer NBMA Address: 120.120.120.1
   Tunnel IPv6 Address: 2001:DB8:1:1::71
   IPv6 Target Network: 2001:DB8:1:1::71/128
   # Ent: 1, Status: UP, UpDn Time: 00:04:10, Cache Attrib: D
2. Peer NBMA Address: 130.130.130.1
   Tunnel IPv6 Address: 2001:DB8:1:1::72
   IPv6 Target Network: 2001:DB8:1:1::72/128
   # Ent: 1, Status: UP, UpDn Time: 00:02:59, Cache Attrib: D
DMVPN IPsec VRF aware

Hub
interface Loopback0
    ip address 1.1.1.1 255.255.255.0

interface Loopback1
    ip address 11.11.11.11 255.255.255.0

interface Tunnel1
    ip address 192.168.100.1 255.255.255.0
    no ip redirects
    no ip split-horizon eigrp 100
    ip nhrp map multicast dynamic
    ip nhrp network-id 111
    ip nhrp redirect
    tunnel source 110.110.110.1
    tunnel mode gre multipoint

interface FastEthernet0/0
    ip address 110.110.110.0 255.255.255.0

router eigrp 100
    network 1.1.1.1 0.0.0.0
    network 11.11.11.11 0.0.0.0
    network 192.168.100.1 0.0.0.0
**Spoke 1**
interface Loopback0
   ip address 2.2.2.2 255.255.255.0
!
interface Loopback1
   ip address 22.22.22.22 255.255.255.0
!
interface Tunnel1
   ip address 192.168.100.2 255.255.255.0
   no ip redirects
   ip nhrp map 192.168.100.1 110.110.110.1
   ip nhrp map multicast 110.110.110.1
   ip nhrp network-id 111
   ip nhrp nhs 192.168.100.1
   ip nhrp shortcut
   tunnel source 120.120.120.1
   tunnel mode gre multipoint
!
interface FastEthernet0/0
   ip address 120.120.120.1 255.255.255.0

router eigrp 100
   network 2.2.2.2 0.0.0.0
   network 22.22.22.22 0.0.0.0
   network 192.168.100.2 0.0.0.0

**spoke 2**
interface Loopback0
   ip address 3.3.3.3 255.255.255.0
!
interface Loopback1
   ip address 33.33.33.33 255.255.255.0
!
interface Tunnel1
   ip address 192.168.100.3 255.255.255.0
   no ip redirects
   ip nhrp map 192.168.100.1 110.110.110.1
   ip nhrp map multicast 110.110.110.1
   ip nhrp network-id 111
   ip nhrp nhs 192.168.100.1
   ip nhrp shortcut
   tunnel source 130.130.130.1
   tunnel mode gre multipoint
!
interface FastEthernet0/0
   ip address 130.130.130.1 255.255.255.0

router eigrp 100
network 3.3.3.3 0.0.0.0
network 33.33.33.33 0.0.0.0
network 192.168.100.3 0.0.0.0

INTERNET
interface FastEthernet0/0
  ip address 110.110.110.2 255.255.255.0
!
interface FastEthernet0/1
  ip address 120.120.120.2 255.255.255.0
!
interface FastEthernet1/0
  ip address 130.130.130.2 255.255.255.0

router bgp 123
  bgp log-neighbor-changes
  network 110.110.110.0 mask 255.255.255.0
  network 120.120.120.0 mask 255.255.255.0
  network 130.130.130.0 mask 255.255.255.0

  neighbor 110.110.110.1 remote-as 100
  neighbor 120.120.120.1 remote-as 200
  neighbor 130.130.130.1 remote-as 300

Hub
  ip vrf cbtme
  rd 45678:45678
  interface f0/0
  ip vrf for cbtme
  ip address 110.110.110.1 255.255.255.0

Router bgp 100
  Bgp router-id 110.110.110.1
  add ipv4 vrf cbtme
  Neighbor 110.110.110.2 remote-as 123

spoke 1
  ip vrf cbtme
  rd 45678:45678
  interface f0/0
  ip vrf for cbtme
  ip address 120.120.120.1 255.255.255.0

Router bgp 200
  Bgp router-id 120.120.120.1
  add ipv4 vrf cbtme
  Neighbor 120.120.120.2 remote-as 123
spoke 2
ip vrf cbtme
rd 45678:45678
interface f0/0
ip vrf for cbtme
ip address 130.130.130.1 255.255.255.0

Router bgp 300
Bgp router-id 130.130.130.1
add ipv4 vrf cbtme
Neighbor 130.130.130.2 remote-as 123

HUB
crypto keyring DMVPN vrf cbtme
pre-shared-key address 0.0.0.0 0.0.0.0 key CCIE
crypto isakmp policy 10
authentication pre-share
group 2
crypto ipsec transform-set CCIEXFORM ah-sha-hmac esp-aes 256
mode transport
crypto ipsec profile DMVPNPROFILE
set transform-set CCIEXFORM
interface Tunnel1
tunnel protection ipsec profile DMVPNPROFILE
tunnel vrf cbtme

Spoke1
crypto keyring DMVPN vrf cbtme
pre-shared-key address 0.0.0.0 0.0.0.0 key CCIE
crypto isakmp policy 10
authentication pre-share
group 2
crypto ipsec transform-set CCIEXFORM ah-sha-hmac esp-aes 256
mode transport
crypto ipsec profile DMVPNPROFILE
set transform-set CCIEXFORM
interface Tunnel1
tunnel protection ipsec profile DMVPNPROFILE
tunnel vrf cbtme
spoke 2
crypto keyring DMVPN vrf cbtme
pre-shared-key address 0.0.0.0 0.0.0.0 key CCIE
crypto isakmp policy 10
authentication pre-share
group 2
crypto ipsec transform-set CCIEXFORM ah-sha-hmac esp-aes 256
mode transport
crypto ipsec profile DMVPNPROFILE
set transform-set CCIEXFORM
interface Tunnel1
tunnel protection ipsec profile DMVPNPROFILE
tunnel vrf Cbtme

Good Luck
CCSI: Yasser Auda
https://www.facebook.com/YasserRamzyAuda
https://learningnetwork.cisco.com/people/yasser.r.a?view=documents
https://www.youtube.com/user/yasserramzyauda