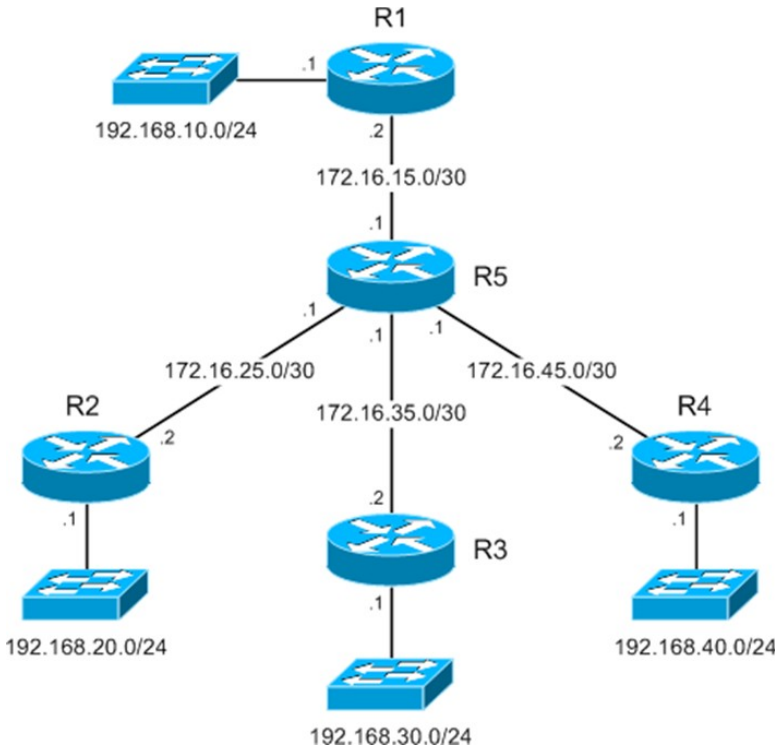
LAB1: DMVPN Theory

Disclaimer

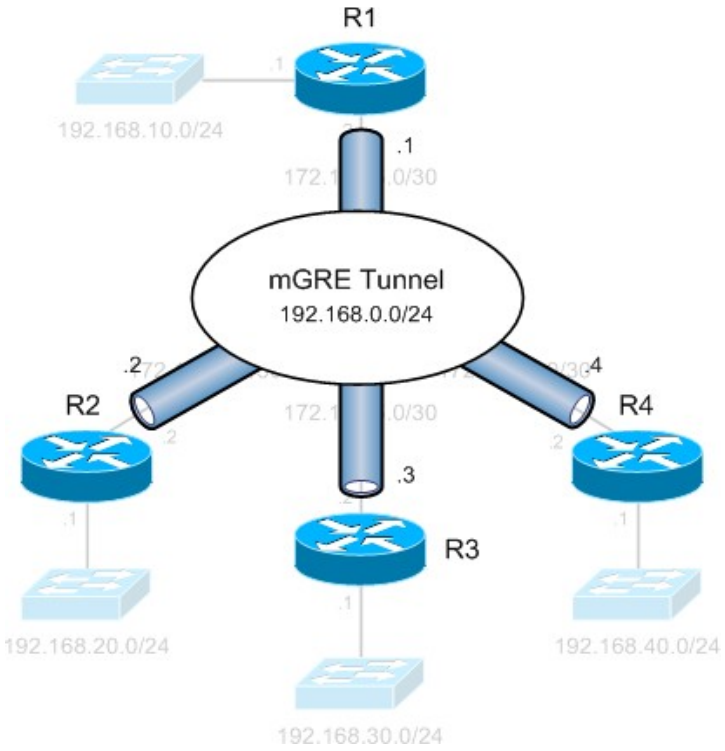
This Configuration Guide is designed to assist members to enhance their skills in respective technology area. While every effort has been made to ensure that all material is as complete and accurate as possible, the enclosed material is presented on an “as is” basis. Neither the authors nor Forum assume any liability or responsibility to any person or entity with respect to loss or damages incurred from the information contained in this guide. This Lab Guide was developed by RSTForum. Any similarities between material presented in this configuration guide and any other material is completely coincidental.

INTRODUCTION

- Dynamic Multipoint VPN
    1. Provides dynamic secure overlay networks.
- DMVPN is combination of the following technologies
    1. Multipoint GRE (mGRE)
    2. Next-Hop Resolution Protocol (NHRP)
    3. Dynamic Routing Protocol (EIGRP, RIP, OSPF, BGP)
    4. Dynamic IPsec encryption
    5. Cisco Express Forwarding (CEF)
- A Dynamic Multipoint VPN is an evolved iteration of hub and spoke tunneling.
- DMVPN itself is not a protocol but merely a design concept.
- A generic hub and spoke topology implement static tunnels between a centrally located hub router and its spokes, which generally attach branch offices.
- Tunnel can be GRE or IPsec (typically IPsec)
- Each new spoke requires additional configuration on the hub router and traffic between spokes must be detoured through the hub to exit one tunnel and enter another.
- While this may be an acceptable solution on a small scale, it becomes a mess as spokes multiply in number.
- DMVPN offers an elegent solution to this problem: multipoint GRE tunneling

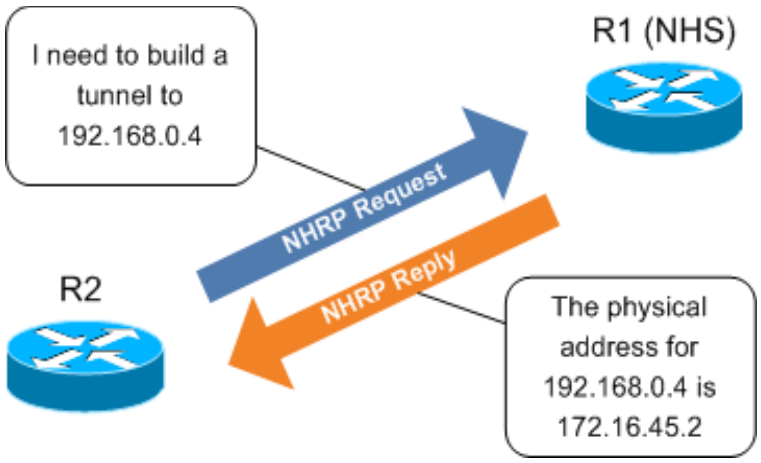


- A GRE tunnel encapsulations IP packets with a GRE header and a new IP header.
- A Point-to-point GRE tunnel has exactly two endpoints.
- Conversely, a multipoint GRE tunnel allows for more than two endpoints and is treated as a non-broadcast multipoint access (NBMA) network.



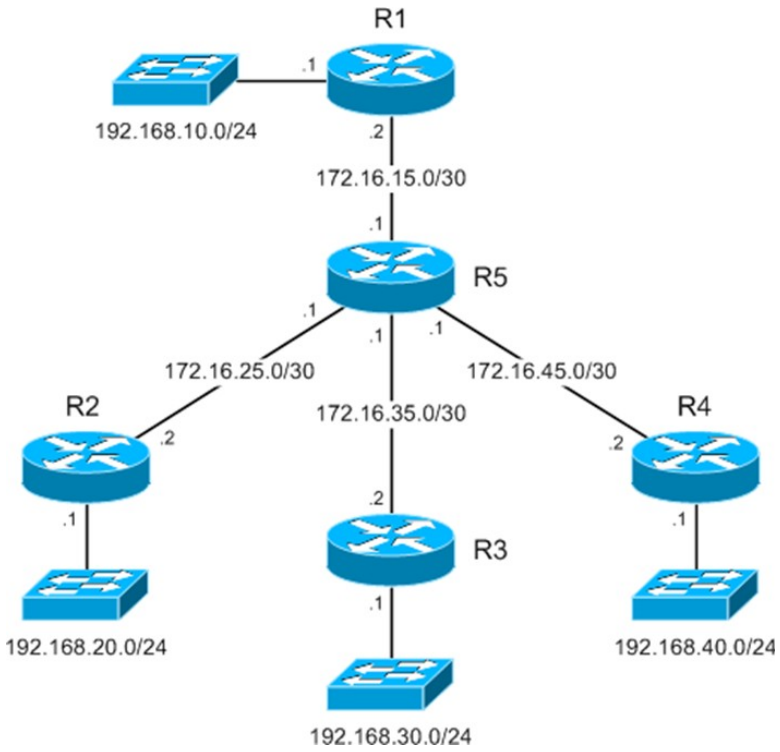
- Legacy hub and spoke setup would require three separate tunnels spanning from R1 to each of the spoke routers.
- Conversely mGRE allows all four routers to have a single tunnel interface in the same IP subnet (192.168.0.0/24).
- This NBMA configuration is enabled by Next Hop Resolution Protocol, which allows multipoint tunnels to be built dynamically.

NEXT HOP RESOLUTION PROTOCOL



- NHRP facilitates dynamic tunnel establishment providing tunnel-to-physical interface address resolution.
- NHRP clients (spoke routers) issue requests to the next hop server (hub router) to obtain the physical address of another spoke router.

DMVPN CONFIGURATION



R1:
interface fastethernet 0/0
ip address 172.16.1.2 255.255.255.252
no shutdown
exit

interface tunnel 0
ip address 192.168.0.1 255.255.255.0
ip nhrp map multicast dynamic
!(Enables forwarding of multicast traffic across the tunnel to dynamic spokes required by most routing protocol)
ip nhrp network-id 1
!(Uniquely identifies the DMVPN network; tunnels will not form between router with differing network IDs.)
tunnel source 172.16.1.2
tunnel mode gre multipoint

!(Here tunnel does not have an explicit destination specified because multipoint tunnels are built dynamically from the spokes to the hub router; the hub router doesn't need to be preconfigured with spoke addresses.)

R2:

```
interaface fastethernet0/0
ip address 172.168.2.2 255.255.255.252
no shutdown
exit
interface tunnel 0
ip address 192.168.0.2 255.255.255.0
ip nhrp map 192.168.0.1 172.16.1.2
! (Statically maps the NHS address to R1's physically address)
ip nhrp map multicast 172.16.1.2
! (Multicast traffic is only allowed from spokes to the hub, not from spoke to spoke.)
ip nhrp network-id 1
ip nhrp nhs 192.168.0.1
! (ip nhrp nhs 192.168.0.1 designates R1 as the Next Hop Server)
tunnel source 172.168.2.2
tunnel mode gre multipoint
```

Note: R3 and R4 create similar configuration on all spoke routers.

Verify DMVPN Sessions

R1# show 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
Tunnel0, Type:Hub, NHRP Peers:3,
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
—– ——————— ——————— ——————————- ——————— ———–
1 172.16.25.2 192.168.0.2 UP 00:57:47 D
1 172.16.35.2 192.168.0.3 UP 00:45:56 D
1 172.16.45.2 192.168.0.4 UP 00:45:46 D
```

Dynamic Tunneling

- Brilliance of DMVPN lies in its ability to dynamically establish spoke-to-spoke tunnels.
- In a legacy hub and spoke design a packet destined from R2 to R4 would need to be routed through R1 to exit the R2 tunnel and the get re-encapsulated to enter the R4 tunnel.

- Clearly a better path lies directly via R5 and DMVPN allows us to take advantage of this.

Verify

- Packet capture of traffic from R2 to R4. Traffic initially follows the path through R1 as described above while a dynamic tunnel is built from R2 to R4 using NHRP.
- After the new tunnel has been an established traffic flow across it bypassing R1 completely.
- We can see a new tunnel has been established after traffic destined for R4 is detected:

```
R2# show dmvpn
Tunnel0, Type:Spoke, NHRP Peers:1,
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
—– ——————— ——————— —– ——– —–
1 172.16.1.2 192.168.0.1 UP 01:08:02 S

R2# ping 192.168.0.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.4, timeout is 2 seconds:
! ! ! ! !
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/37/56 ms

R2# show dmvpn
Tunnel0, Type:Spoke, NHRP Peers:2,
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
—– ——————— ——————— —– ——– —–
1 172.16.1.2 192.168.0.1 UP 01:08:27 S
1 172.16.4.2 192.168.0.4 UP 00:00:03 D
```

Notice that the tunnel to R4 has been flagged as dynamic, in contrast to the static tunnel to the hub/NHS.

IPSEC: ADDING CRYPTO

- IPsec protection policy is applied on the tunnel interface of each router.

- A simple IPsec profile using a pre-shared ISAKMP key is included below for demonstration.

```
crypto isakmp policy 10
authentication pre-share
crypto isakmp key P4ssw0rd address 172.16.0.0 255.255.0.0
!
crypto ipsec transform-set My TransformSet esp-aes esp-sha-hmac
!
crypto ipsec profile MyProfile
set transform-set My TransformSet
!
Interface tunnel 0
Tunnel protection ipsec profile MyProfile
```

(After bumping the tunnel interfaces, we can see the DMVPN sessions have been rebuilt, this time sporting some slick military-grade encryption.)

Verification

```
R1# show dmvpn

Tunnel0, Type:Hub, NHRP Peers:3,
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
—– ——————— ——————— —– ——— —–
1 172.16.2.2 192.168.0.2 UP 00:02:28 D
1 172.16.3.2 192.168.0.3 UP 00:02:26 D
1 172.16.4.2 192.168.0.4 UP 00:02:25 D

R1# show crypto isakmp sa

IPv4 Crypto ISAKMP SA
dst src state conn-id slot status
172.16.1.2 172.16.3.2 QM_IDLE 1002 0 ACTIVE
172.16.1.2 172.16.2.2 QM_IDLE 1001 0 ACTIVE
172.16.1.2 172.16.4.2 QM_IDLE 1003 0 ACTIVE
```