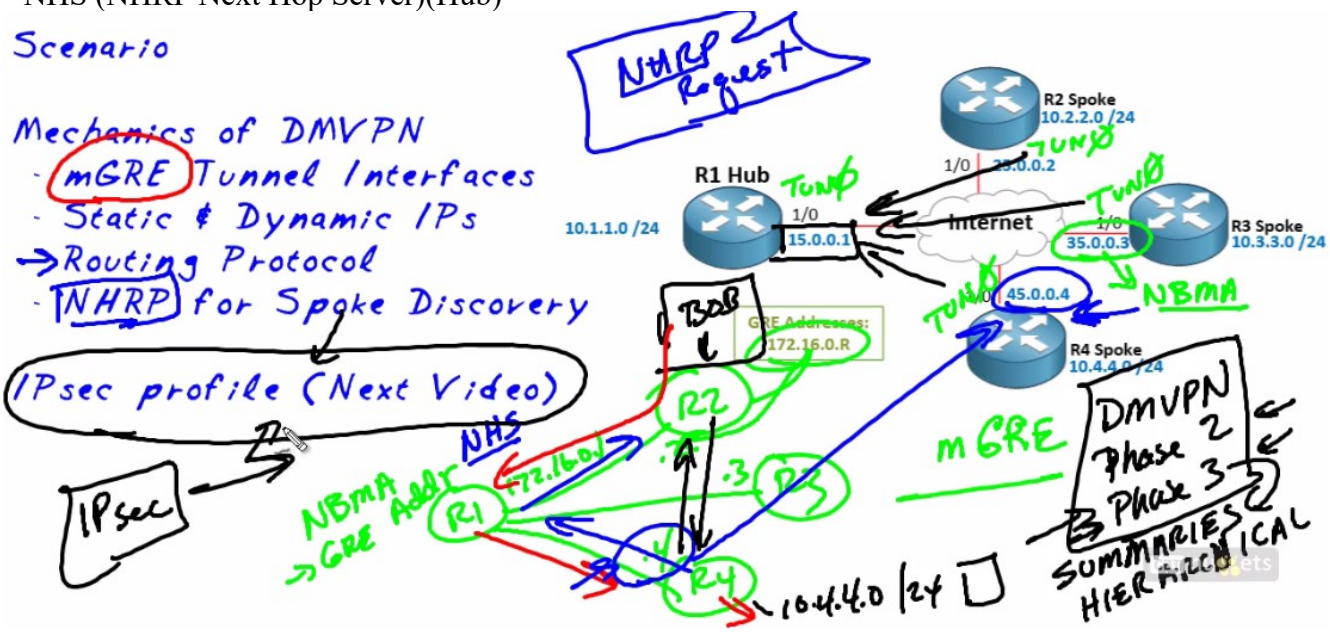
SUITE B CRYPTO. NIST /NSA/ NSS

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Encryption	FIPS Pub 197	128 bit keys for SECRET 256 bit keys for TOP SECRET
Elliptic Curve Diffie-Hellman (ECDH)	Key Exchange	NIST SP 800-56A	Curve P-256 for SECRET Curve P-384 for TOP SECRET
Elliptic Curve Digital Signature Algorithm (ECDSA)	Digital Signature	FIPS Pub 186-4	Curve P-256 for SECRET Curve P-384 for TOP SECRET
Secure Hash Algorithm (SHA)	Hashing	FIPS Pub 180-4	SHA-256 for SECRET SHA-384 for TOP SECRET

- IKEv1 IPsec
- IKEv2 IPsec
- IOS and ASA
- PSK and RSA-Sig
- VTIs
- Site to Site VPN
- Remote Access VPN
- Clientless / WebVPN
- AnyConnect
- DMVPN
- FlexVPN
- GETVPN
- Troubleshooting

Dynamic Multipoint VPN:

Naked DMVPN:
NHRP(Next Hop Resolution Protocol)
NBMA(Non Broadcast Multi Access)
NHS (NHRP Next Hop Server)(Hub)



DMVPN NHRP Config:
<u>R1 (Hub):</u>
int tunnel 0
tunnel source gig 1/0
tunnel mode gre multipoint
tunnel key 6783 (need to be the same on all)
ip nhrp network-id 1 (need to be the same on all)

ip nhrp authentication cisco123 (need to be the same on all)
ip nhrp multicast dynamic
ip nhrp shortcut
ip nhrp redirect
ip address 172.16.0.1 255.255.255.0
tunnel path-mtu-discovery
no tunnel path-mtu-discovery
ip mtu 1400
ip tcp adjust-mss 1360

R2 (Spoke):
int tunnel 0
tunnel mode gre multipoint
tunnel source gig 1/0
key 6783
ip nhrp network-id 1
ip nhrp authentication cisco123
ip nhrp shortcut
ip nhrp nhs 172.16.0.1
ip nhrp map 172.16.0.1 15.0.0.1
ip nhrp map multicast 15.0.0.1
ip address 172.16.0.2 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360

R3 (Spoke):
int tunnel 0
tunnel mode gre multipoint
tunnel source gig 1/0
key 6783
ip nhrp network-id 1
ip nhrp authentication cisco123
ip nhrp shortcut
ip nhrp nhs 172.16.0.1
ip nhrp map 172.16.0.1 15.0.0.1
ip nhrp map multicast 15.0.0.1
ip address 172.16.0.3 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360

R4 (Spoke):
int tunnel 0
tunnel mode gre multipoint
tunnel source gig 1/0
key 6783
ip nhrp network-id 1
ip nhrp authentication cisco123
ip nhrp shortcut
ip nhrp nhs 172.16.0.1
ip nhrp map 172.16.0.1 15.0.0.1
ip nhrp map multicast 15.0.0.1

ip address 172.16.0.4 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360

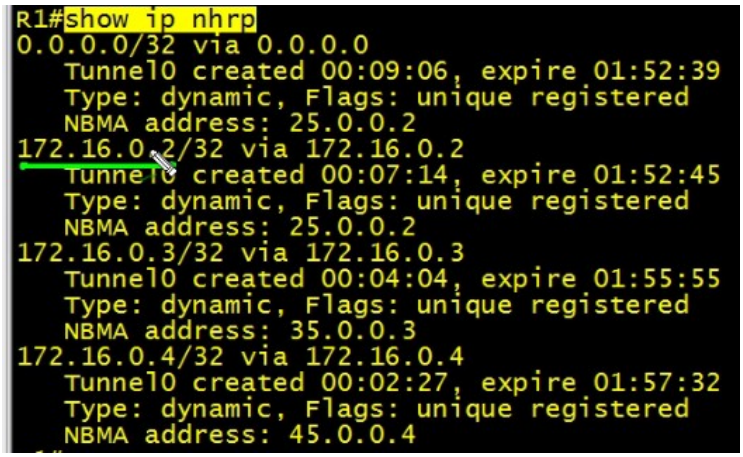
Routing Config:
R1 (Hub):
router eigrp 777
no auto-summary
network 10.0.0.0
network 172.16.0.0

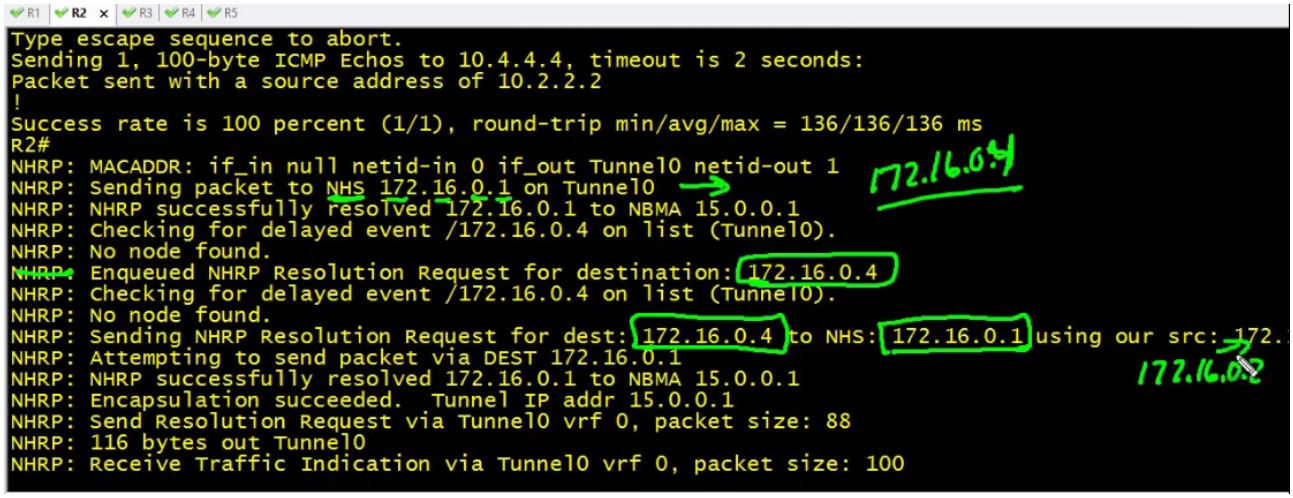
int tunnel 0
no ip next-hop-self eigrp 777
no ip split-horizon eigrp 777

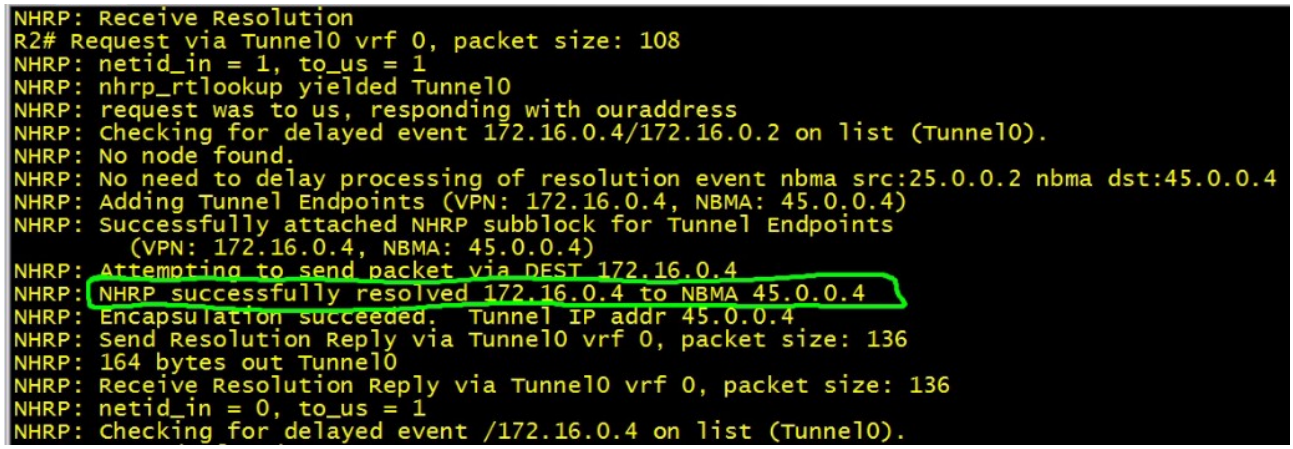
R2:
router eigrp 777
no auto-summary
network 10.0.0.0
network 172.16.0.0

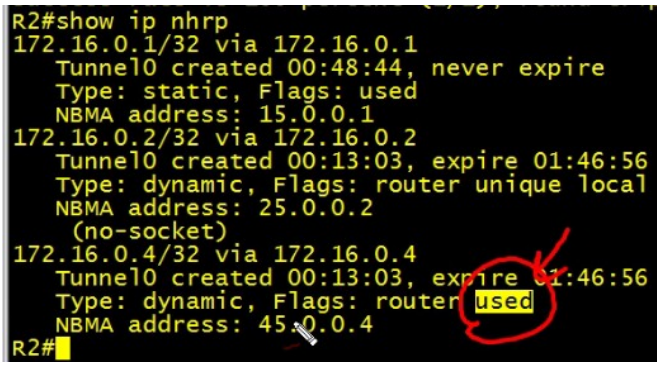
R3:
router eigrp 777
no auto-summary
network 10.0.0.0
network 172.16.0.0

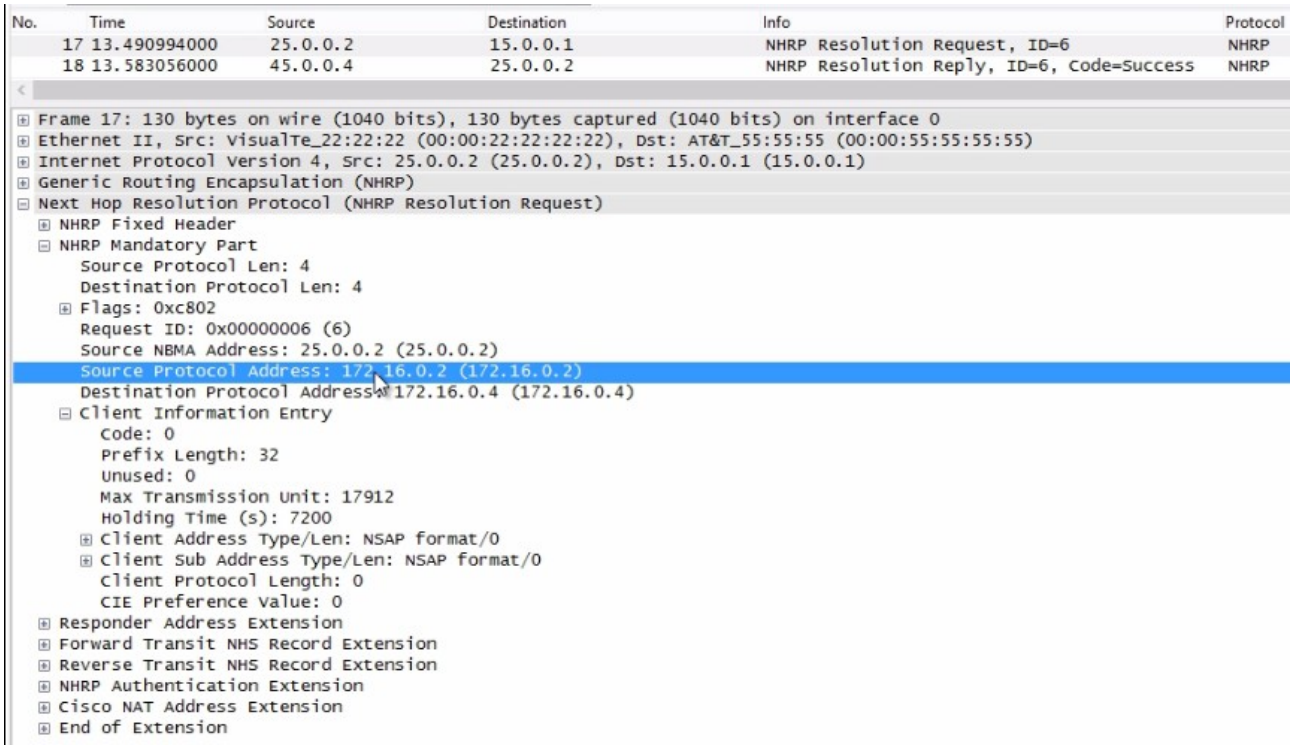
R4:
router eigrp 777
no auto-summary
network 10.0.0.0
network 172.16.0.0



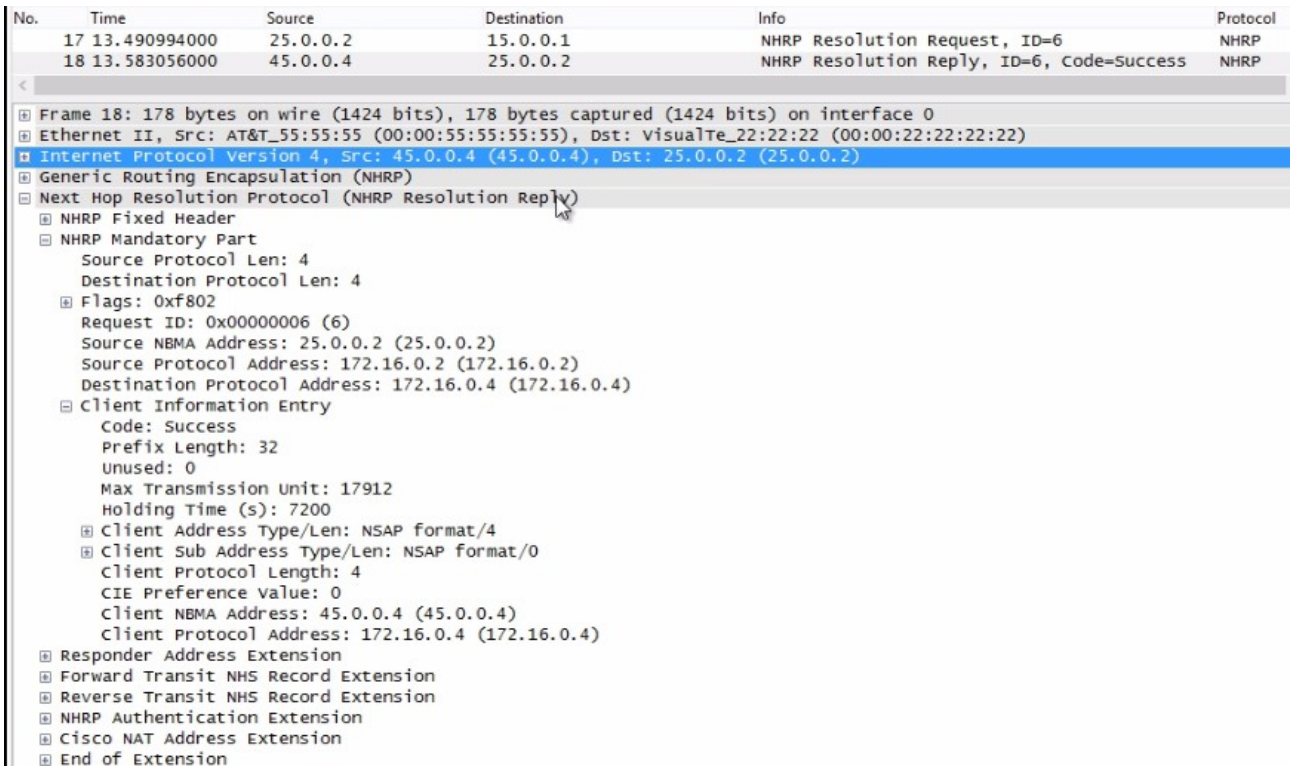

R1
R2
R3
R4
R5
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 10.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 10.2.2.2
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 136/136/136 ms
R2#
NHRP: MACADDR: if_in null netid-in 0 if_out Tunnel0 netid-out 1
NHRP: Sending packet to NHS 172.16.0.1 on Tunnel0
NHRP: NHRP successfully resolved 172.16.0.1 to NBMA 15.0.0.1
NHRP: Checking for delayed event /172.16.0.4 on list (Tunnel0).
NHRP: No node found.
NHRP: Enqueued NHRP Resolution Request for destination: 172.16.0.4
NHRP: Checking for delayed event /172.16.0.4 on list (Tunnel0).
NHRP: No node found.
NHRP: Sending NHRP Resolution Request for dest: 172.16.0.4 to NHS: 172.16.0.1 using our src: 172.
NHRP: Attempting to send packet via DEST 172.16.0.1
NHRP: NHRP successfully resolved 172.16.0.1 to NBMA 15.0.0.1
NHRP: Encapsulation succeeded. Tunnel IP addr 15.0.0.1
NHRP: Send Resolution Request via Tunnel0 vrf 0, packet size: 88
NHRP: 116 bytes out Tunnel0
NHRP: Receive Traffic Indication via Tunnel0 vrf 0, packet size: 100
172.16.0.4
172.16.0.2


NHRP: Receive Resolution
R2# Request via Tunnel0 vrf 0, packet size: 108
NHRP: netid_in = 1, to_us = 1
NHRP: nhrp_rtlookup yielded Tunnel0
NHRP: request was to us, responding with ouraddress
NHRP: Checking for delayed event 172.16.0.4/172.16.0.2 on list (Tunnel0).
NHRP: No node found.
NHRP: No need to delay processing of resolution event nbma src:25.0.0.2 nbma dst:45.0.0.4
NHRP: Adding Tunnel Endpoints (VPN: 172.16.0.4, NBMA: 45.0.0.4)
NHRP: Successfully attached NHRP subblock for Tunnel Endpoints
(VPN: 172.16.0.4, NBMA: 45.0.0.4)
NHRP: Attempting to send packet via DEST 172.16.0.4
NHRP: NHRP successfully resolved 172.16.0.4 to NBMA 45.0.0.4
NHRP: Encapsulation succeeded. Tunnel IP addr 45.0.0.4
NHRP: Send Resolution Reply via Tunnel0 vrf 0, packet size: 136
NHRP: 164 bytes out Tunnel0
NHRP: Receive Resolution Reply via Tunnel0 vrf 0, packet size: 136
NHRP: netid_in = 0, to_us = 1
NHRP: Checking for delayed event /172.16.0.4 on list (Tunnel0).


R2#show ip nhrp
172.16.0.1/32 via 172.16.0.1
Tunnel0 created 00:48:44, never expire
Type: static, Flags: used
NBMA address: 15.0.0.1
172.16.0.2/32 via 172.16.0.2
Tunnel0 created 00:13:03, expire 01:46:56
Type: dynamic, Flags: router unique local
NBMA address: 25.0.0.2
(no-socket)
172.16.0.4/32 via 172.16.0.4
Tunnel0 created 00:13:03, expire 01:46:56
Type: dynamic, Flags: router used
NBMA address: 45.0.0.4
R2#



```
No.     Time           Source          Destination     Info                                        Protocol
    17 13.490994000   25.0.0.2        15.0.0.1        NHRP Resolution Request, ID=6               NHRP
    18 13.583056000   45.0.0.4        25.0.0.2        NHRP Resolution Reply, ID=6, Code=Success   NHRP

⊞ Frame 17: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface 0
⊞ Ethernet II, Src: VisualTe_22:22:22 (00:00:22:22:22:22), Dst: AT&T_55:55:55 (00:00:55:55:55:55)
⊞ Internet Protocol Version 4, Src: 25.0.0.2 (25.0.0.2), Dst: 15.0.0.1 (15.0.0.1)
⊞ Generic Routing Encapsulation (NHRP)
⊟ Next Hop Resolution Protocol (NHRP Resolution Request)
  ⊞ NHRP Fixed Header
  ⊟ NHRP Mandatory Part
      Source Protocol Len: 4
      Destination Protocol Len: 4
    ⊞ Flags: 0xc802
      Request ID: 0x00000006 (6)
      Source NBMA Address: 25.0.0.2 (25.0.0.2)
      Source Protocol Address: 172.16.0.2 (172.16.0.2)
      Destination Protocol Address: 172.16.0.4 (172.16.0.4)
    ⊟ Client Information Entry
        Code: 0
        Prefix Length: 32
        Unused: 0
        Max Transmission Unit: 17912
        Holding Time (s): 7200
      ⊞ Client Address Type/Len: NSAP format/0
      ⊞ Client Sub Address Type/Len: NSAP format/0
        Client Protocol Length: 0
        CIE Preference Value: 0
  ⊞ Responder Address Extension
  ⊞ Forward Transit NHS Record Extension
  ⊞ Reverse Transit NHS Record Extension
  ⊞ NHRP Authentication Extension
  ⊞ Cisco NAT Address Extension
  ⊞ End of Extension
```



```
No.     Time           Source          Destination     Info                                        Protocol
    17 13.490994000   25.0.0.2        15.0.0.1        NHRP Resolution Request, ID=6               NHRP
    18 13.583056000   45.0.0.4        25.0.0.2        NHRP Resolution Reply, ID=6, Code=Success   NHRP

⊞ Frame 18: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface 0
⊞ Ethernet II, Src: AT&T_55:55:55 (00:00:55:55:55:55), Dst: VisualTe_22:22:22 (00:00:22:22:22:22)
⊞ Internet Protocol Version 4, Src: 45.0.0.4 (45.0.0.4), Dst: 25.0.0.2 (25.0.0.2)
⊞ Generic Routing Encapsulation (NHRP)
⊟ Next Hop Resolution Protocol (NHRP Resolution Reply)
  ⊞ NHRP Fixed Header
  ⊟ NHRP Mandatory Part
      Source Protocol Len: 4
      Destination Protocol Len: 4
    ⊞ Flags: 0xf802
      Request ID: 0x00000006 (6)
      Source NBMA Address: 25.0.0.2 (25.0.0.2)
      Source Protocol Address: 172.16.0.2 (172.16.0.2)
      Destination Protocol Address: 172.16.0.4 (172.16.0.4)
    ⊟ Client Information Entry
        Code: Success
        Prefix Length: 32
        Unused: 0
        Max Transmission Unit: 17912
        Holding Time (s): 7200
      ⊞ Client Address Type/Len: NSAP format/4
      ⊞ Client Sub Address Type/Len: NSAP format/0
        Client Protocol Length: 4
        CIE Preference Value: 0
        Client NBMA Address: 45.0.0.4 (45.0.0.4)
        Client Protocol Address: 172.16.0.4 (172.16.0.4)
  ⊞ Responder Address Extension
  ⊞ Forward Transit NHS Record Extension
  ⊞ Reverse Transit NHS Record Extension
  ⊞ NHRP Authentication Extension
  ⊞ Cisco NAT Address Extension
  ⊞ End of Extension
```

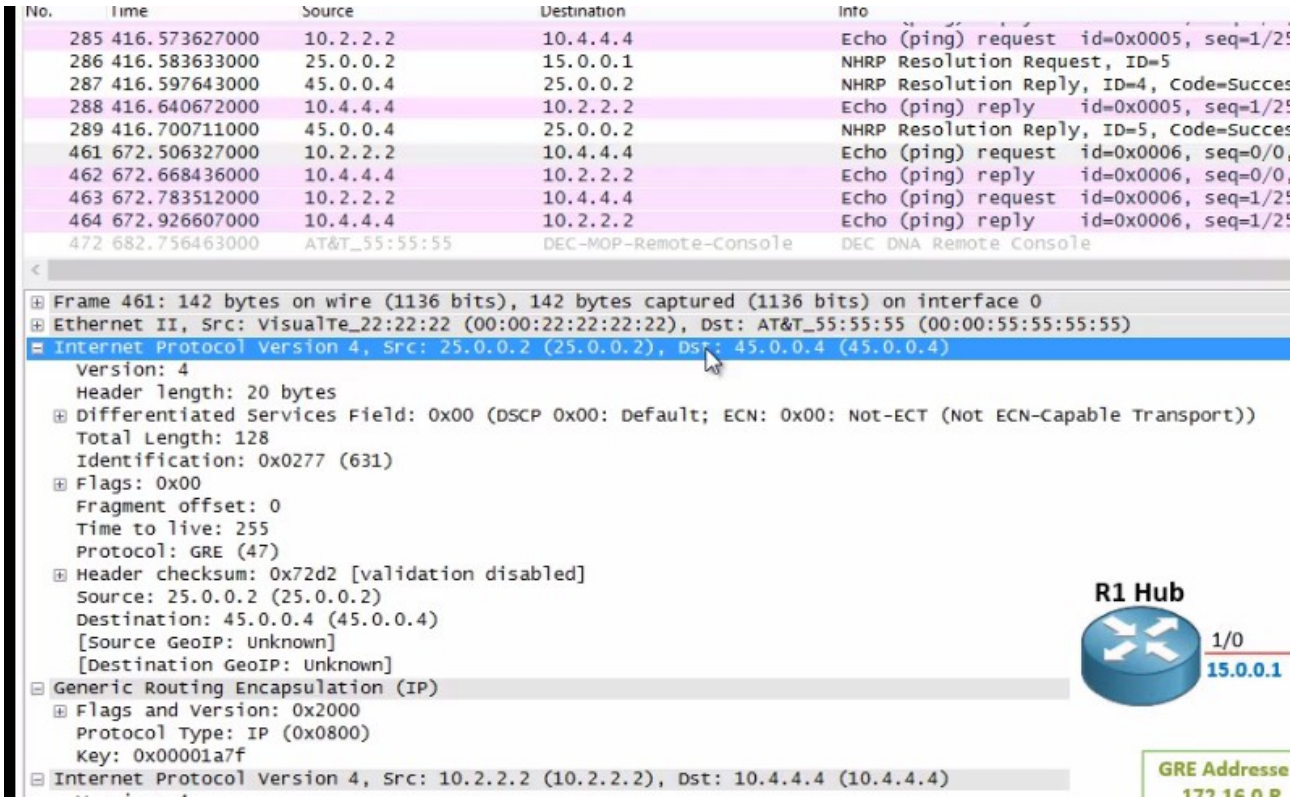
show dmvpn

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

Interface: Tunnel0, IPv4 NHRP Details

IPv4 NHS: 172.16.0.1 RE
Type:Spoke, Total NBMA Peers (v4/v6): 2

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    2       45.0.0.4      172.16.0.4    UP 00:00:41    D       10.4.4.4/32
    0       45.0.0.4      172.16.0.4    UP 00:00:41    D       172.16.0.4/32

    1       15.0.0.1      172.16.0.1    UP 00:27:05    S       172.16.0.1/32


R2#
```

Filter: (!(eigrp)) && !(loop)) && !(cdp) Expression... Clear Apply Save

No.	Time	Source	Destination	Info	Protoco
112	164.815258000	AT&T_55:55:55	DEC-MOP-Remote-Console	DEC DNA Remote Console	0x600
254	377.150481000	VisualTe_22:22:22	DEC-MOP-Remote-Console	DEC DNA Remote Console	0x600
281	416.431532000	10.2.2.2	10.4.4.4	Echo (ping) request id=0x0005, seq=0/0, ttl	ICMP
282	416.441539000	25.0.0.2	15.0.0.1	NHRP Resolution Request, ID=4	NHRP
283	416.469557000	15.0.0.1	25.0.0.2	NHRP Traffic Indication	NHRP
284	416.533601000	10.4.4.4	10.2.2.2	Echo (ping) reply id=0x0005, seq=0/0, ttl	ICMP
285	416.573627000	10.2.2.2	10.4.4.4	Echo (ping) request id=0x0005, seq=1/256, t	ICMP
286	416.583633000	25.0.0.2	15.0.0.1	NHRP Resolution Request, ID=5	NHRP
287	416.597643000	45.0.0.4	25.0.0.2	NHRP Resolution Reply, ID=4, Code=Success	NHRP
288	416.640672000	10.4.4.4	10.2.2.2	Echo (ping) reply id=0x0005, seq=1/256, t	ICMP
289	416.700711000	45.0.0.4	25.0.0.2	NHRP Resolution Reply, ID=5, Code=Success	NHRP
461	672.506327000	10.2.2.2	10.4.4.4	Echo (ping) request id=0x0006, seq=0/0, ttl	ICMP
462	672.668436000	10.4.4.4	10.2.2.2	Echo (ping) reply id=0x0006, seq=0/0, ttl	ICMP
463	672.783512000	10.2.2.2	10.4.4.4	Echo (ping) request id=0x0006, seq=1/256, t	ICMP
464	672.926607000	10.4.4.4	10.2.2.2	Echo (ping) reply id=0x0006, seq=1/256, t	ICMP
472	682.756463000	AT&T_55:55:55	DEC-MOP-Remote-Console	DEC DNA Remote Console	0x600

```
⊞ Frame 281: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0
⊞ Ethernet II, Src: VisualTe_22:22:22 (00:00:22:22:22:22), Dst: AT&T_55:55:55 (00:00:55:55:5
⊞ Internet Protocol Version 4, Src: 25.0.0.2 (25.0.0.2), Dst: 15.0.0.1 (15.0.0.1)
⊞ Generic Routing Encapsulation (IP)
⊞ Internet Protocol Version 4, Src: 10.2.2.2 (10.2.2.2), Dst: 10.4.4.4 (10.4.4.4)
⊞ Internet Control Message Protocol
```



Protected DMVPN:

IPSec Config:

R1:

crypto isakmp policy 5
hash sha
authentication pre-share
group 5
lifetime 86400
encryption aes 256
exit
crypto isakmp keycisco123 address 0.0.0.0 (0.0.0.0 anybody wildcard/don't do it in production)
crypto ipsec transform-set OURSET esp-aes 256 esp-sha-hmac
mode transport
exit
crypto ipsec profile OUR_IPSEC_PROFILE
set transform-set OURSET
exit
interface tunnel 0
tunnel protection ipsec profile OUR_IPSEC_PROFILE

R2:

crypto isakmp policy 5
hash sha
authentication pre-share
group 14
lifetime 86400
encryption aes 256
exit
crypto isakmp keycisco123 address 0.0.0.0 (0.0.0.0 anybody wildcard/don't do it in production)
crypto ipsec transform-set OURSET esp-aes 256 esp-sha-hmac

mode transport
exit
crypto ipsec profile OUR_IPSEC_PROFILE
set transform-set OURSET
exit
interface tunnel 0
tunnel protection ipsec profile OUR_IPSEC_PROFILE

R3:
crypto isakmp policy 5
hash sha
authentication pre-share
group 14
lifetime 86400
encryption aes 256
exit
crypto isakmp keycisco123 address 0.0.0.0 (0.0.0.0 anybody wildcard/don't do it in production)
crypto ipsec transform-set OURSET esp-aes 256 esp-sha-hmac
mode transport
exit
crypto ipsec profile OUR_IPSEC_PROFILE
set transform-set OURSET
exit
interface tunnel 0
tunnel protection ipsec profile OUR_IPSEC_PROFILE

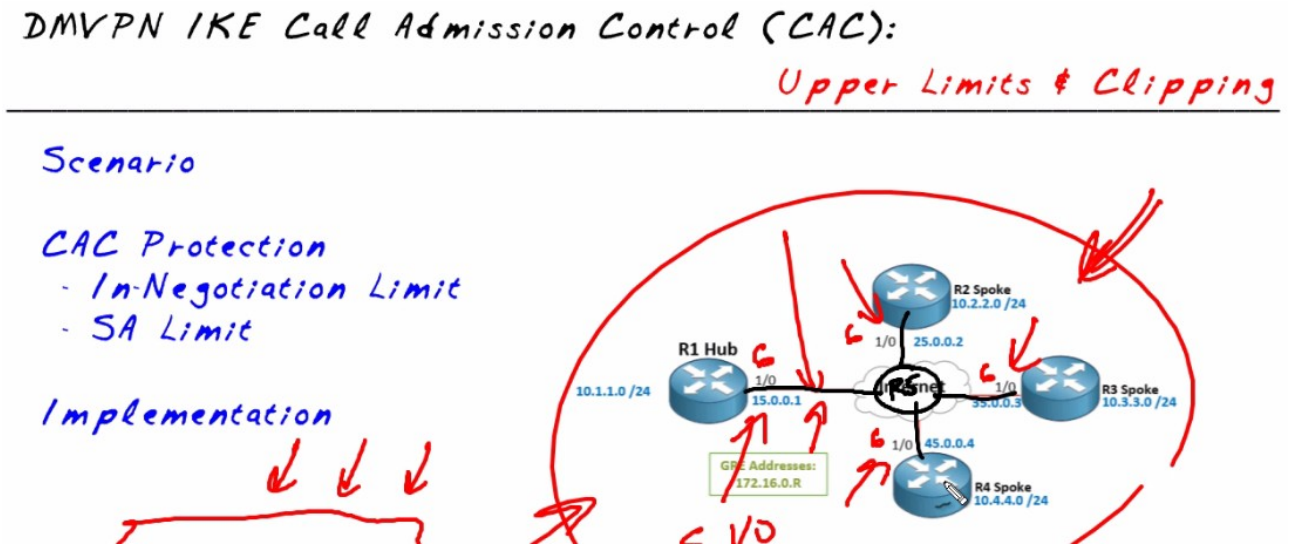
R4:
crypto isakmp policy 5
hash sha
authentication pre-share
group 14
lifetime 86400
encryption aes 256
exit
crypto isakmp keycisco123 address 0.0.0.0 (0.0.0.0 anybody wildcard/don't do it in production)
crypto ipsec transform-set OURSET esp-aes 256 esp-sha-hmac
mode transport
exit
crypto ipsec profile OUR_IPSEC_PROFILE
set transform-set OURSET
exit
interface tunnel 0
tunnel protection ipsec profile OUR_IPSEC_PROFILE

Verification and Tshoot:
show ip protocol
show ip eigrp neighbors
show ip route eigrp
show ip route 10.4.4.4 (from R2's perspective)
show ip nhrp summary
show ip nhrp
clear ip nhrp 172.16.0.4 (R2's perspective)

show dmvpn
show dmvpn detail
show crypto isakmp policy
show crypto iskmp sa
show crypto engine connections active
show crypto iskmp sa detail
show crypto ipsec sa peer 45.0.0.4 (R2's perpective)
clear crypto isakmp
show dmvpn peer nbma 45.0.0.4 detail (R2's perspective)
show run tunnel 0

Debugging (be careful with debugs in production, especially logging on the console):
debug nhrp
debug crypto isakmp (phase 1)
debug crypto ipsec (phase 2)
undebug all

Tshoot:
1. Basic connectivity (ping and traceroute)(UDP:500 and UDP4500 and Procotol 50 (ESP) are allowed)
2. keys and IDs
3. Crypto Policies (test removing ipsec profile from the tunnels on both hub and/or spoke, but don't do it in production as other spokes will be affected)
(debug phase 1 and/or phase2)
(failed its sanity check or is malformed is mostly wrong pre-shared key)
4. Routing (e.g EIGRP)




```
R2#show crypto call admission statistics
----------------------------------------------------------------
            Crypto Call Admission Control Statistics
----------------------------------------------------------------
System Resource Limit:        0 Max IKE SAs:      0 Max in nego:  1000
Total IKE SA Count:           5 active:           5 negotiating:     0
Incoming IKE Requests:        2 accepted:         2 rejected:        0
Outgoing IKE Requests:        3 accepted:         3 rejected:        0
Rejected IKE Requests:        0 rsrc low:         0 SA limit:        0
IKE packets dropped at dispatch:        0
```

```
R2#show crypto call admission statistics
----------------------------------------------------------------
              Crypto Call Admission Control Statistics
----------------------------------------------------------------
System Resource Limit:        0 Max IKE SAs:     2 Max in nego:     10
Total IKE SA Count:           2 active:          2 negotiating:     0
Incoming IKE Requests:        3 accepted:        3 rejected:        0
Outgoing IKE Requests:        6 accepted:        5 rejected:        1
Rejected IKE Requests:        1 rsrc low:        0 SA limit:        1
IKE packets dropped at dispatch:       0

R2#
```

DMVPN IKE Call Admission Control (CAC):
Too many IKE phase1 messages (botnet with thousands of devices trying to do tunnel negotiations with the spoke) can be mitigated by DMVPN IKE Call Admission Control (CAC).
Setting up an upper limit i.e. SA Limit for IKE Phase1.

crypto call admission limit ike sa 2 (setting sa limit)
crypto call admission limit ike in-negotiation-sa 10 (max negotiations)

clear crypto sa
clear crypto isakmp

```
R2#ping 10.4.4.4 source 10.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.4.4, timeout is 2 seconds:
Packet sent with a source address of 10.2.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 172/216/280 ms
R2#
%CRYPTO-4-IKE_DENY_SA_REQ: IKE denied an OUTGOING SA request from 25.0.0.2 to 45.0.0.4 due to IKE
REACHED
R2#
R2#
R2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
25.0.0.2        45.0.0.4        QM_IDLE           1008 ACTIVE
15.0.0.1        25.0.0.2        QM_IDLE           1007 ACTIVE

IPv6 Crypto ISAKMP SA
```

```
R2#ping 10.3.3.3 source 10.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 10.2.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 156/202/232 ms
R2#
%CRYPTO-4-IKE_DENY_SA_REQ: IKE denied an INCOMING SA request from 35.0.0.3 to 25.0.0.2 due to IKE
REACHED
```

```
R2#traceroute 10.3.3.3 source 10.2.2.2

Type escape sequence to abort.
Tracing the route to 10.3.3.3

  1 172.16.0.1 120 msec 120 msec 84 msec
  2 172.16.0.3 260 msec 188 msec 160 msec
R2#
%CRYPTO-4-IKE_DENY_SA_REQ: IKE denied an OUTGOING SA request from 25.0.0.2 to 35.0.0.3 due to IKE
REACHED
R2#
```