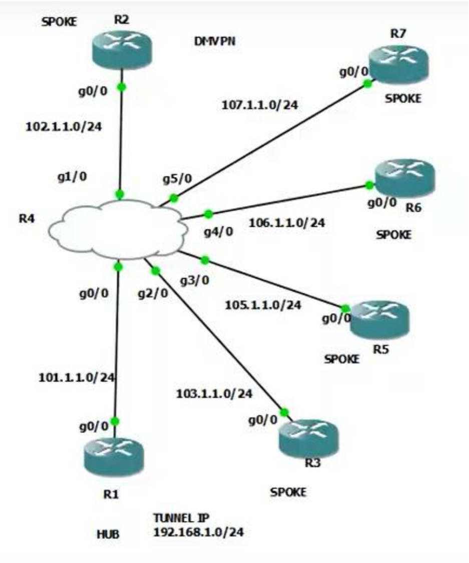
Recording Class

Dynamic Multipoint VPN

##Topology

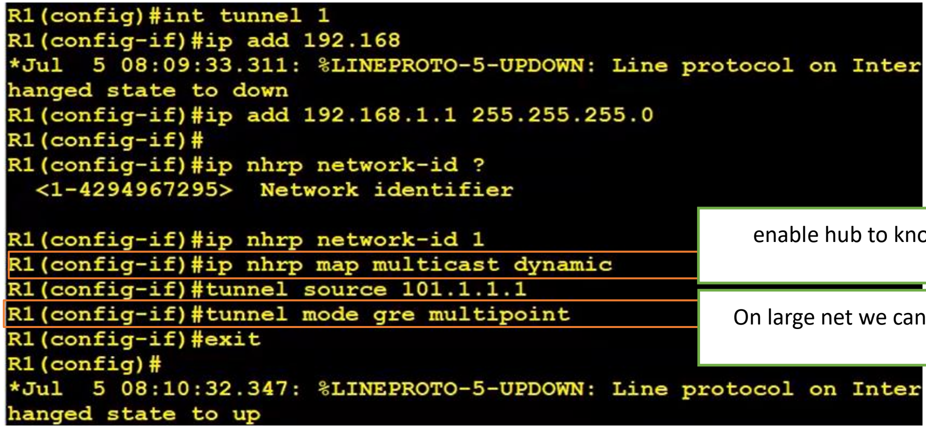


****config all ips on all routes along with loopbacks**
**** config the default route to ISP gateway that all spokes can communicate each other.**

## Phase-1 (spokes only maps to hub)

##Tunnel

#R1 [HUB]

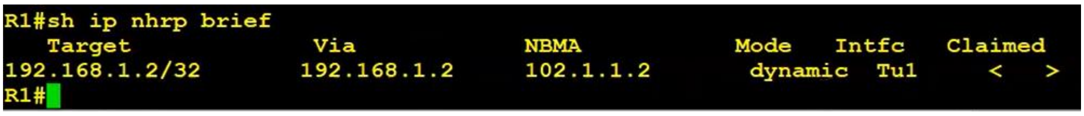


```
R1(config)#int tunnel 1
R1(config-if)#ip add 192.168
*Jul  5 08:09:33.311: %LINEPROTO-5-UPDOWN: Line protocol on Inter
hanged state to down
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#
R1(config-if)#ip nhrp network-id ?
  <1-4294967295>  Network identifier

R1(config-if)#ip nhrp network-id 1
R1(config-if)#ip nhrp map multicast dynamic
R1(config-if)#tunnel source 101.1.1.1
R1(config-if)#tunnel mode gre multipoint
R1(config-if)#exit
R1(config)#
*Jul  5 08:10:32.347: %LINEPROTO-5-UPDOWN: Line protocol on Inter
hanged state to up
```

enable hub to know about spokes when spokes gets mapped towards Hub.

On large net we can't use every-time destination CMD that's we use multipoint

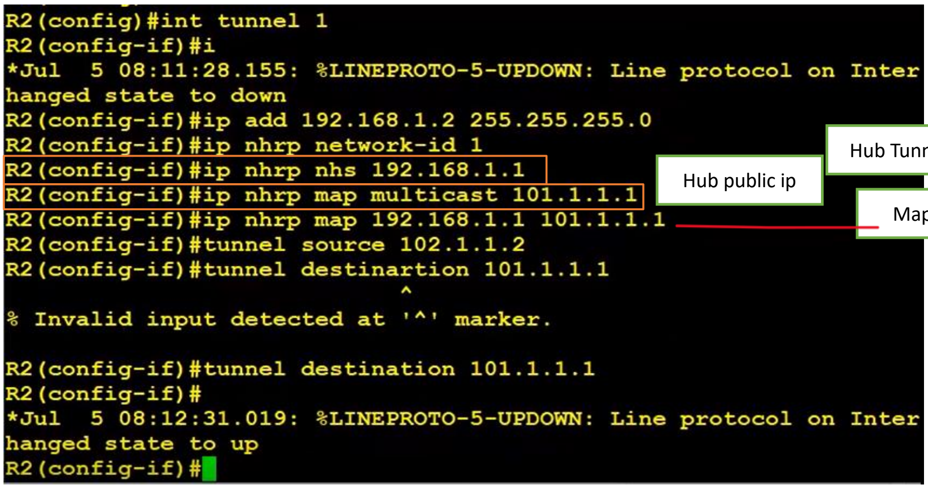
**** network-id need to same on all hub and spokes (network-is for registration)**



```
R1#sh ip nhrp brief
   Target             Via            NBMA           Mode   Intfc   Claimed
192.168.1.2/32     192.168.1.2    102.1.1.2        dynamic   Tu1      <   >
R1#
```

**** after config of Spoke will auto detect its nei**

#R2



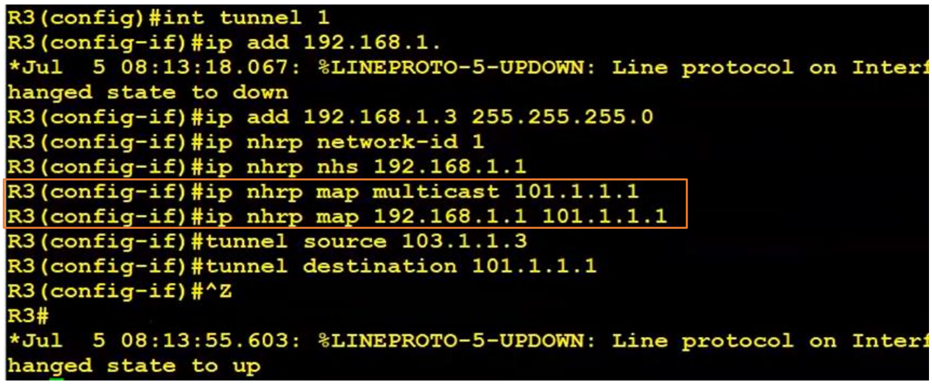
```
R2(config)#int tunnel 1
R2(config-if)#i
*Jul  5 08:11:28.155: %LINEPROTO-5-UPDOWN: Line protocol on Inter
hanged state to down
R2(config-if)#ip add 192.168.1.2 255.255.255.0
R2(config-if)#ip nhrp network-id 1
R2(config-if)#ip nhrp nhs 192.168.1.1
R2(config-if)#ip nhrp map multicast 101.1.1.1
R2(config-if)#ip nhrp map 192.168.1.1 101.1.1.1
R2(config-if)#tunnel source 102.1.1.2
R2(config-if)#tunnel destinartion 101.1.1.1
                                ^
% Invalid input detected at '^' marker.

R2(config-if)#tunnel destination 101.1.1.1
R2(config-if)#
*Jul  5 08:12:31.019: %LINEPROTO-5-UPDOWN: Line protocol on Inter
hanged state to up
R2(config-if)#
```

Hub Tunnel IP

Hub public ip

Maps tunnel to public ip Of HUB

#R3

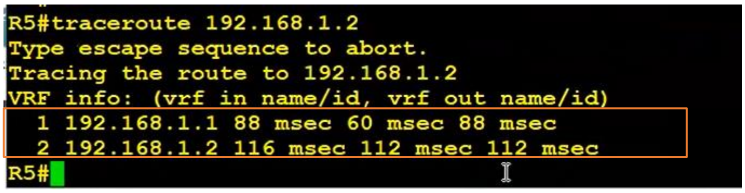


```
R3(config)#int tunnel 1
R3(config-if)#ip add 192.168.1.
*Jul  5 08:13:18.067: %LINEPROTO-5-UPDOWN: Line protocol on Interf
hanged state to down
R3(config-if)#ip add 192.168.1.3 255.255.255.0
R3(config-if)#ip nhrp network-id 1
R3(config-if)#ip nhrp nhs 192.168.1.1
R3(config-if)#ip nhrp map multicast 101.1.1.1
R3(config-if)#ip nhrp map 192.168.1.1 101.1.1.1
R3(config-if)#tunnel source 103.1.1.3
R3(config-if)#tunnel destination 101.1.1.1
R3(config-if)#^Z
R3#
*Jul  5 08:13:55.603: %LINEPROTO-5-UPDOWN: Line protocol on Interf
hanged state to up
```

** mapping to HUB router

** config same on the #R5

#R5

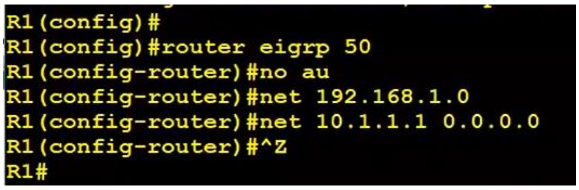


```
R5#traceroute 192.168.1.2
Type escape sequence to abort.
Tracing the route to 192.168.1.2
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.1.1 88 msec 60 msec 88 msec
  2 192.168.1.2 116 msec 112 msec 112 msec
R5#
```

** if spoke want ping other spokes means they will ping through the HUB

## IF we want to ping for the loopback address we need config prefer EIGRP

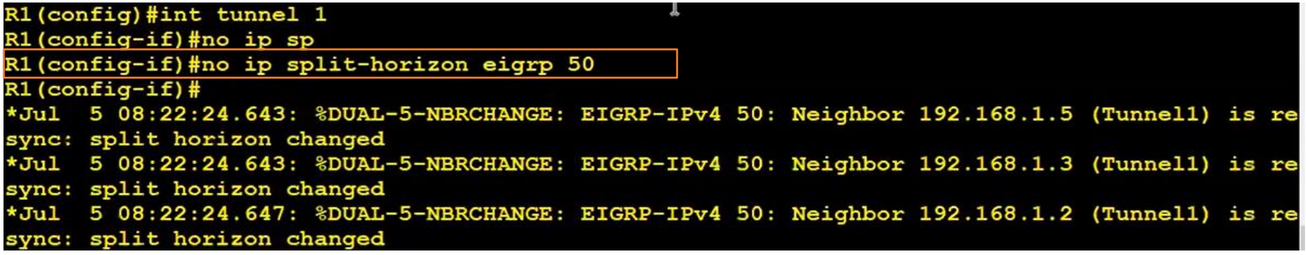
#R1



```
R1(config)#
R1(config)#router eigrp 50
R1(config-router)#no au
R1(config-router)#net 192.168.1.0
R1(config-router)#net 10.1.1.1 0.0.0.0
R1(config-router)#^Z
R1#
```

**config eigrp on all routers

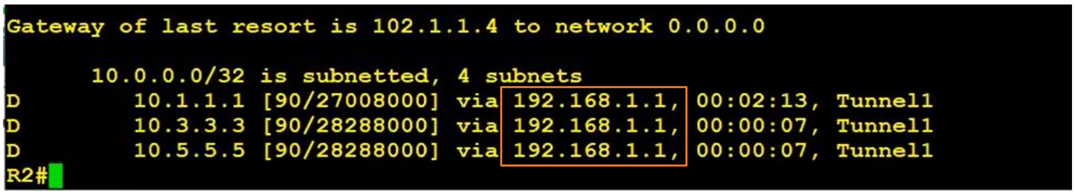
** all the routers will have only HUB loopback in routing-table [due to eigrp split-horizon to avoid Collison the router interface only advertise one address)



```
R1(config)#int tunnel 1
R1(config-if)#no ip sp
R1(config-if)#no ip split-horizon eigrp 50
R1(config-if)#
*Jul  5 08:22:24.643: %DUAL-5-NBRCHANGE: EIGRP-IPv4 50: Neighbor 192.168.1.5 (Tunnel1) is re
sync: split horizon changed
*Jul  5 08:22:24.643: %DUAL-5-NBRCHANGE: EIGRP-IPv4 50: Neighbor 192.168.1.3 (Tunnel1) is re
sync: split horizon changed
*Jul  5 08:22:24.647: %DUAL-5-NBRCHANGE: EIGRP-IPv4 50: Neighbor 192.168.1.2 (Tunnel1) is re
sync: split horizon changed
```

** we have disable the spilt-horizon. [they will get all routers]

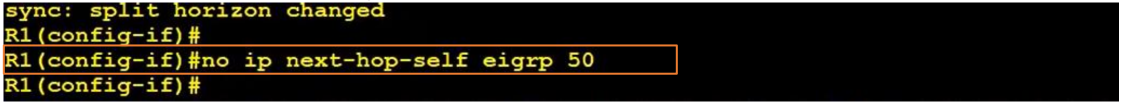
** now all routers will receive all loopbacks



```
Gateway of last resort is 102.1.1.4 to network 0.0.0.0

      10.0.0.0/32 is subnetted, 4 subnets
D        10.1.1.1 [90/27008000] via 192.168.1.1, 00:02:13, Tunnel1
D        10.3.3.3 [90/28288000] via 192.168.1.1, 00:00:07, Tunnel1
D        10.5.5.5 [90/28288000] via 192.168.1.1, 00:00:07, Tunnel1
R2#
```

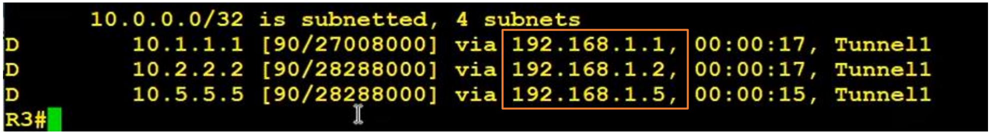
** the next-hop is always R1[hub]

** we have disable next-hop-self

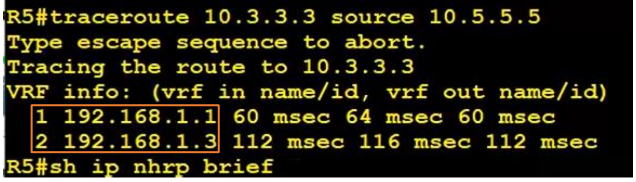


```
sync: split horizon changed
R1(config-if)#
R1(config-if)#no ip next-hop-self eigrp 50
R1(config-if)#
```

** now they will receive next-hop-self correct



```
      10.0.0.0/32 is subnetted, 4 subnets
D        10.1.1.1 [90/27008000] via 192.168.1.1, 00:00:17, Tunnel1
D        10.2.2.2 [90/28288000] via 192.168.1.2, 00:00:17, Tunnel1
D        10.5.5.5 [90/28288000] via 192.168.1.5, 00:00:15, Tunnel1
R3#
```



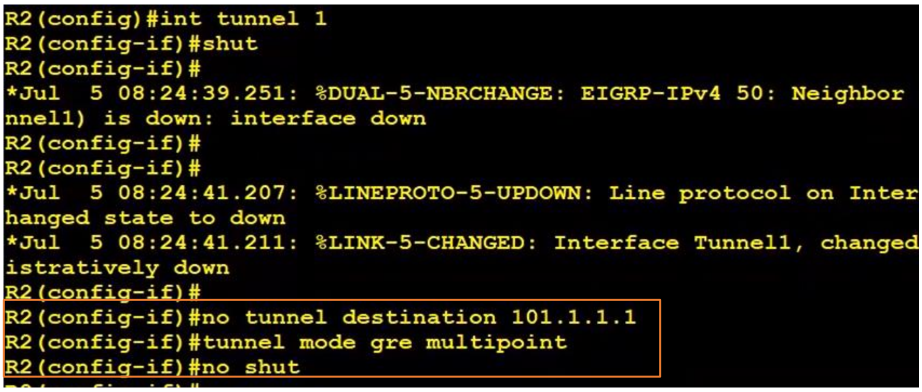
```
R5#traceroute 10.3.3.3 source 10.5.5.5
Type escape sequence to abort.
Tracing the route to 10.3.3.3
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.1.1 60 msec 64 msec 60 msec
  2 192.168.1.3 112 msec 116 msec 112 msec
R5#sh ip nhrp brief
```

**every-time we are getting routes from HUB. At sometime it will get congested for all routers

**[Phase-1]

##Phase-2 [spoke-to-spoke without getting off to HUB router]

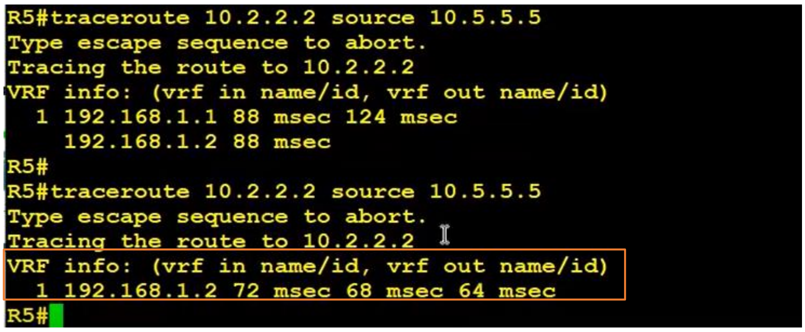
#R2



```
R2(config)#int tunnel 1
R2(config-if)#shut
R2(config-if)#
*Jul  5 08:24:39.251: %DUAL-5-NBRCHANGE: EIGRP-IPv4 50: Neighbor
nnel1) is down: interface down
R2(config-if)#
R2(config-if)#
*Jul  5 08:24:41.207: %LINEPROTO-5-UPDOWN: Line protocol on Inter
hanged state to down
*Jul  5 08:24:41.211: %LINK-5-CHANGED: Interface Tunnel1, changed
istratively down
R2(config-if)#
R2(config-if)#no tunnel destination 101.1.1.1
R2(config-if)#tunnel mode gre multipoint
R2(config-if)#no shut
```

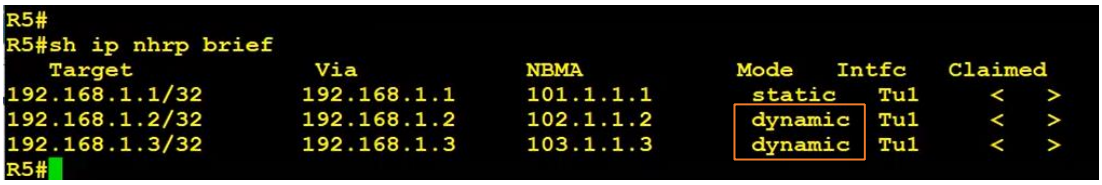
** 1st shut the tunnel to avoid loops and remove dst and config the gre-multipoint

** config same on all routers



```
R5#traceroute 10.2.2.2 source 10.5.5.5
Type escape sequence to abort.
Tracing the route to 10.2.2.2
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.1.1 88 msec 124 msec
    192.168.1.2 88 msec
R5#
R5#traceroute 10.2.2.2 source 10.5.5.5
Type escape sequence to abort.
Tracing the route to 10.2.2.2
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.1.2 72 msec 68 msec 64 msec
R5#
```

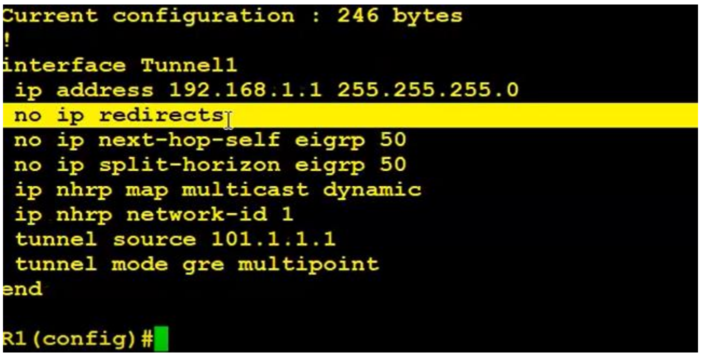
** 1st they get through Hub after they get directly



```
R5#
R5#sh ip nhrp brief
   Target              Via            NBMA           Mode     Intfc   Claimed
192.168.1.1/32       192.168.1.1     101.1.1.1        static    Tu1      <   >
192.168.1.2/32       192.168.1.2     102.1.1.2        dynamic   Tu1      <   >
192.168.1.3/32       192.168.1.3     103.1.1.3        dynamic   Tu1      <   >
R5#
```

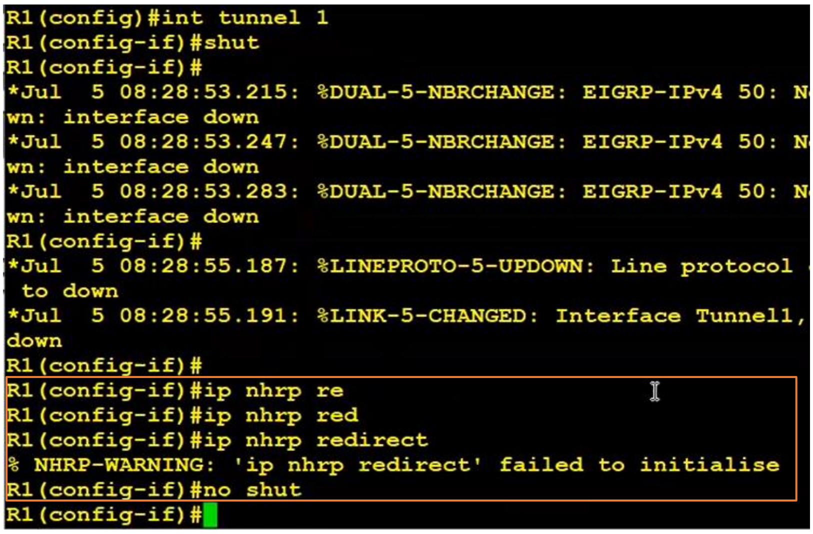
##Phase-3

#R1



```
Current configuration : 246 bytes
!
interface Tunnel1
 ip address 192.168.1.1 255.255.255.0
 no ip redirects
 no ip next-hop-self eigrp 50
 no ip split-horizon eigrp 50
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 tunnel source 101.1.1.1
 tunnel mode gre multipoint
end

R1(config)#
```

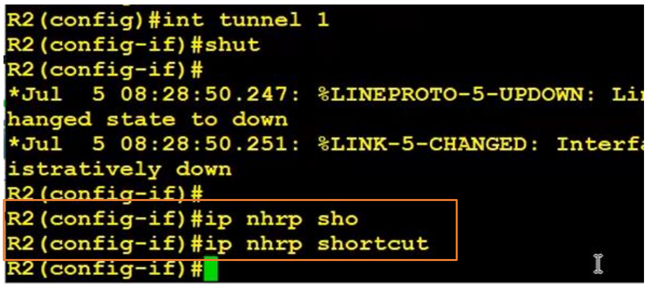
** we have to make redirect



```
R1(config)#int tunnel 1
R1(config-if)#shut
R1(config-if)#
*Jul  5 08:28:53.215: %DUAL-5-NBRCHANGE: EIGRP-IPv4 50: N
wn: interface down
*Jul  5 08:28:53.247: %DUAL-5-NBRCHANGE: EIGRP-IPv4 50: N
wn: interface down
*Jul  5 08:28:53.283: %DUAL-5-NBRCHANGE: EIGRP-IPv4 50: N
wn: interface down
R1(config-if)#
*Jul  5 08:28:55.187: %LINEPROTO-5-UPDOWN: Line protocol
 to down
*Jul  5 08:28:55.191: %LINK-5-CHANGED: Interface Tunnel1,
down
R1(config-if)#
R1(config-if)#ip nhrp re
R1(config-if)#ip nhrp red
R1(config-if)#ip nhrp redirect
% NHRP-WARNING: 'ip nhrp redirect' failed to initialise
R1(config-if)#no shut
R1(config-if)#
```

** ignore the error msg

#R2



```
R2(config)#int tunnel 1
R2(config-if)#shut
R2(config-if)#
*Jul  5 08:28:50.247: %LINEPROTO-5-UPDOWN: Li
hanged state to down
*Jul  5 08:28:50.251: %LINK-5-CHANGED: Interf
istratively down
R2(config-if)#
R2(config-if)#ip nhrp sho
R2(config-if)#ip nhrp shortcut
R2(config-if)#
```

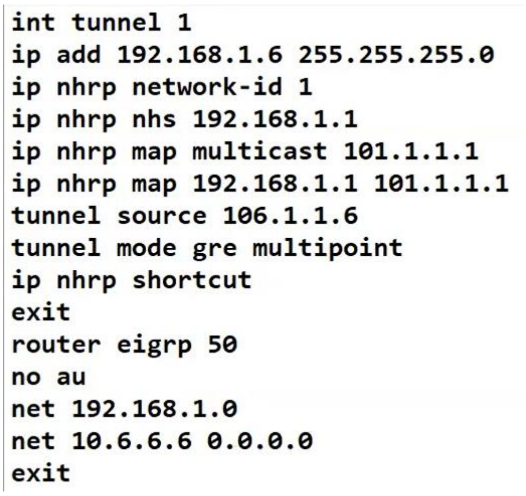
** on every router use this CMD

###[after gre-tunnel default time 24 hours it will not ask hub router to register the network and get spoke-to-spoke mapping]

ZTP[zero-touch-provisioning]

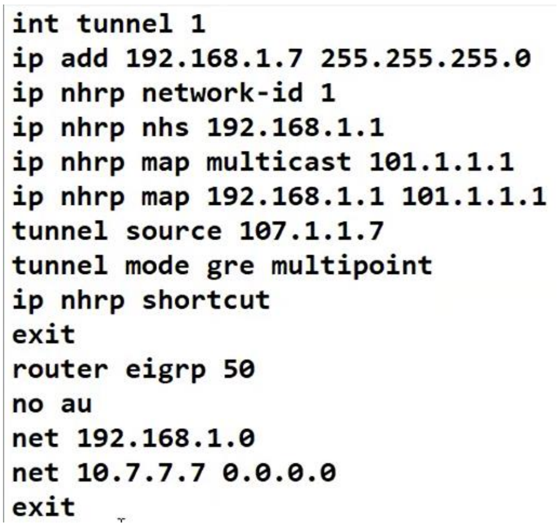
** if any new spoke will add without running single cmd on HUB they will get negotiation.

#R6



```
int tunnel 1
ip add 192.168.1.6 255.255.255.0
ip nhrp network-id 1
ip nhrp nhs 192.168.1.1
ip nhrp map multicast 101.1.1.1
ip nhrp map 192.168.1.1 101.1.1.1
tunnel source 106.1.1.6
tunnel mode gre multipoint
ip nhrp shortcut
exit
router eigrp 50
no au
net 192.168.1.0
net 10.6.6.6 0.0.0.0
exit
```

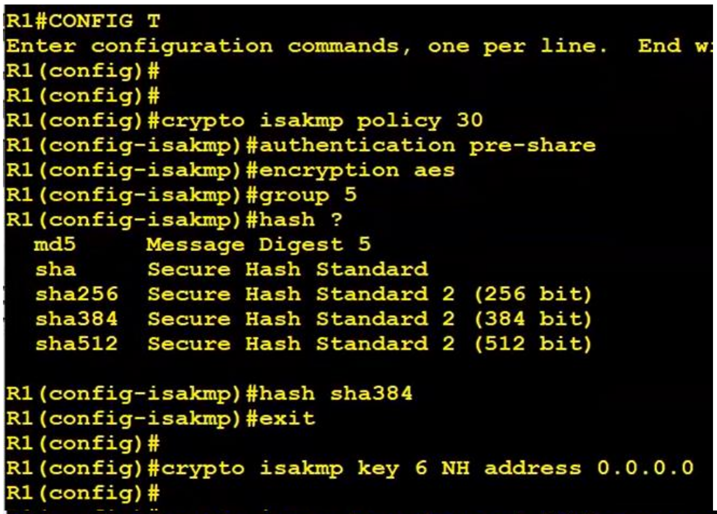
#R7



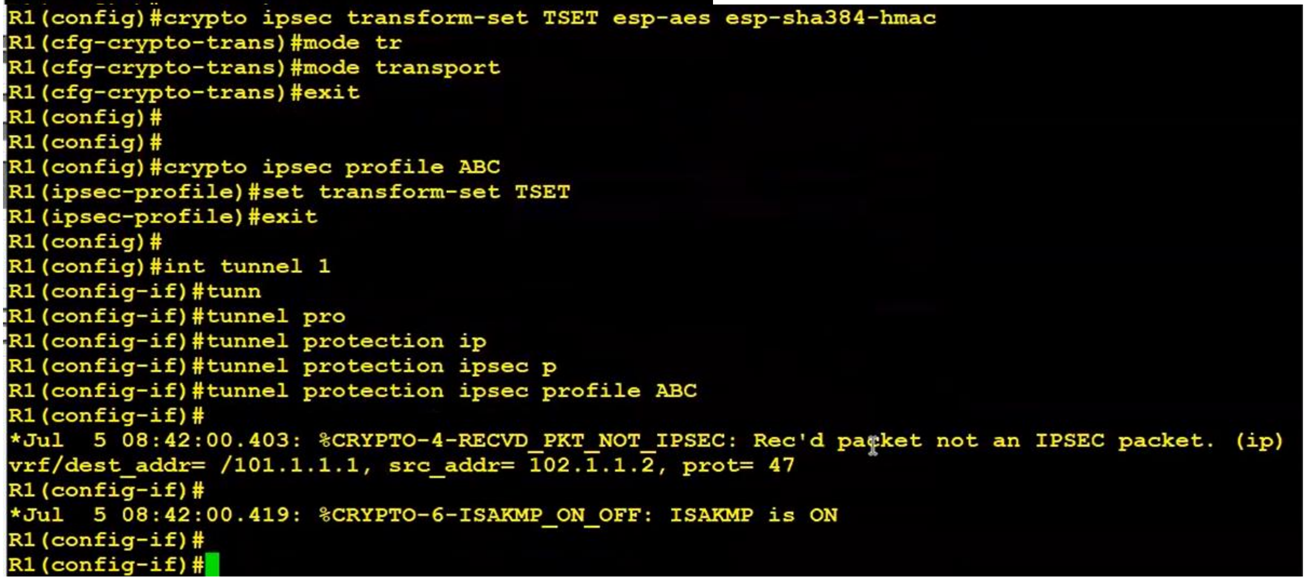
```
int tunnel 1
ip add 192.168.1.7 255.255.255.0
ip nhrp network-id 1
ip nhrp nhs 192.168.1.1
ip nhrp map multicast 101.1.1.1
ip nhrp map 192.168.1.1 101.1.1.1
tunnel source 107.1.1.7
tunnel mode gre multipoint
ip nhrp shortcut
exit
router eigrp 50
no au
net 192.168.1.0
net 10.7.7.7 0.0.0.0
exit
```

##config the IP-SEC

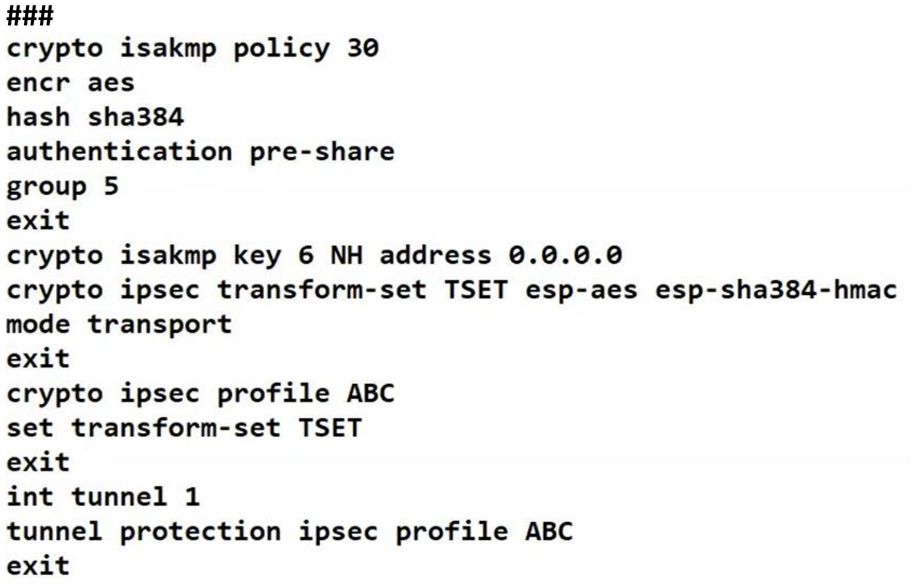
#R1



```
R1#CONFIG T
Enter configuration commands, one per line.  End w
R1(config)#
R1(config)#
R1(config)#crypto isakmp policy 30
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption aes
R1(config-isakmp)#group 5
R1(config-isakmp)#hash ?
  md5     Message Digest 5
  sha     Secure Hash Standard
  sha256  Secure Hash Standard 2 (256 bit)
  sha384  Secure Hash Standard 2 (384 bit)
  sha512  Secure Hash Standard 2 (512 bit)

R1(config-isakmp)#hash sha384
R1(config-isakmp)#exit
R1(config)#
R1(config)#crypto isakmp key 6 NH address 0.0.0.0
R1(config)#
```



```
R1(config)#crypto ipsec transform-set TSET esp-aes esp-sha384-hmac
R1(cfg-crypto-trans)#mode tr
R1(cfg-crypto-trans)#mode transport
R1(cfg-crypto-trans)#exit
R1(config)#
R1(config)#
R1(config)#crypto ipsec profile ABC
R1(ipsec-profile)#set transform-set TSET
R1(ipsec-profile)#exit
R1(config)#
R1(config)#int tunnel 1
R1(config-if)#tunn
R1(config-if)#tunnel pro
R1(config-if)#tunnel protection ip
R1(config-if)#tunnel protection ipsec p
R1(config-if)#tunnel protection ipsec profile ABC
R1(config-if)#
*Jul  5 08:42:00.403: %CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet. (ip)
vrf/dest_addr= /101.1.1.1, src_addr= 102.1.1.2, prot= 47
R1(config-if)#
*Jul  5 08:42:00.419: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
R1(config-if)#
```



```
###
crypto isakmp policy 30
encr aes
hash sha384
authentication pre-share
group 5
exit
crypto isakmp key 6 NH address 0.0.0.0
crypto ipsec transform-set TSET esp-aes esp-sha384-hmac
mode transport
exit
crypto ipsec profile ABC
set transform-set TSET
exit
int tunnel 1
tunnel protection ipsec profile ABC
exit
```

**config this on every-router