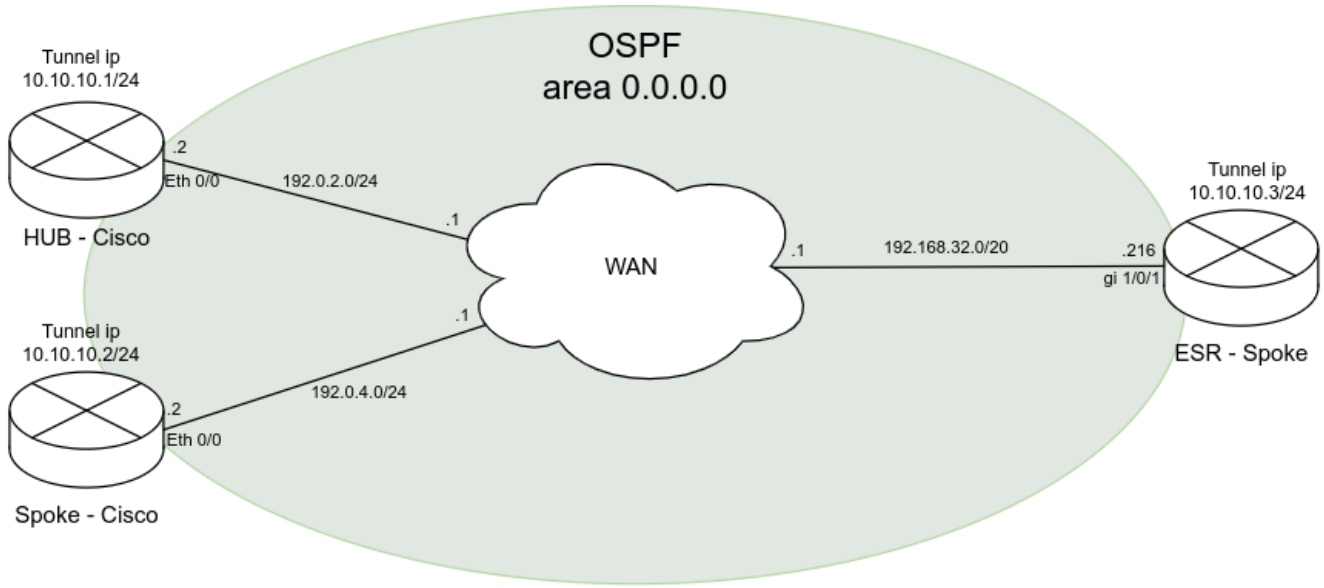
NHRP (Cisco-HUB, ESR-Spoke, Cisco-Spoke)/DMVPN over IPSEC (Cisco-HUB, ESR-Spoke, Cisco-Spoke)

:



:

NHRP- ESR-Spoke Cisco-HUB Cisco-Spoke. OSPF.

Cisco-HUB:

1) :

```
interface Tunnel1
ip address 10.10.10.1 255.255.255.0
no ip redirects
ip mtu 1472
ip nhrp authentication <password>
ip nhrp map multicast dynamic
ip nhrp network-id 60
ip nhrp holdtime 360
ip nhrp registration no-unique
ip nhrp registration timeout 60
ip tcp adjust-mss 1432
ip ospf network broadcast
ip ospf priority 255
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel key 60
!
!
interface Ethernet0/0
ip address 192.0.2.2 255.255.255.0
!
!
router ospf 1
router-id 10.10.10.1
log-adjacency-changes
auto-cost reference-bandwidth 10000
network 10.10.10.1 0.0.0.0 area 0
!
ip route 192.0.4.0 255.255.255.0 192.0.2.1
ip route 192.168.32.0 255.255.240.0 192.0.2.1
```

2) OSPF NHRP:

```
Router#show ip nhrp
10.10.10.2/32 via 10.10.10.2
Tunnel1 created 01:18:10, expire 00:05:14
Type: dynamic, Flags: registered
NBMA address: 192.0.4.2
10.10.10.3/32 via 10.10.10.3
Tunnel1 created 01:04:52, expire 00:05:44
Type: dynamic, Flags: unique registered
NBMA address: 192.168.39.216

Router#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
10.10.10.2 1 FULL/DROTHER 00:00:34 10.10.10.2 Tunnel1
10.10.10.3 128 FULL/DR 00:00:31 10.10.10.3 Tunnel1
```

ESR-Spoke:

1)

```
esr# show running-config
router ospf log-adjacency-changes
router ospf 1
router-id 10.10.10.3
area 0.0.0.0
enable
exit
enable
exit

interface gigabitethernet 1/0/1
ip firewall disable
ip address 192.168.39.216/20
exit

tunnel gre 1
key 60
ttl 30
mtu 1472
multipoint
ip firewall disable
local interface gigabitethernet 1/0/1
ip address 10.10.10.3/24
ip ospf instance 1
ip ospf
ip tcp adjust-mss 1432
ip nhrp authentication <password>
ip nhrp holding-time 360
ip nhrp map 10.10.10.1 192.0.2.2
ip nhrp nhs 10.10.10.1/24
ip nhrp multicast nhs
ip nhrp enable
enable
exit

ip route 192.0.2.0/24 192.168.39.1
ip route 192.0.4.0/24 192.168.39.1
```

2) OSPF NHRP:

```
esr# show ip ospf neighbors
Router ID  Pri State    DTime Interface         Router IP
---------  --- -----    ----- ----------------- ---------
10.10.10.1 255 Full/BDR 00:36 gre 1             10.10.10.1

esr# show ip nhrp
Tunnel address   NBMA address     Interface Peer type       Expire    Created    Flags
---------------- ---------------- --------- --------------- --------- ---------- ---------
10.10.10.1       192.0.2.2        gre 1     static          --        --         register,
                                                                                  lower-up,
                                                                                  up

10.10.10.2       192.0.4.2        gre 1     cached           0:05:49  00:00:10   used,
                                                                                  lower-up,
                                                                                  up
```

Cisco-Spoke:

1) :

```
interface Tunnel1
ip address 10.10.10.2 255.255.255.0
no ip redirects
ip mtu 1472
ip nhrp authentication <password>
ip nhrp map 10.10.10.1 192.0.2.2
ip nhrp map multicast 192.0.2.2
ip nhrp network-id 60
ip nhrp holdtime 360
ip nhrp nhs 10.10.10.1
ip nhrp registration no-unique
ip nhrp registration timeout 60
ip tcp adjust-mss 1432
ip ospf network broadcast
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel key 60
!
!
interface Ethernet0/0
ip address 192.0.4.2 255.255.255.0
!
!
router ospf 1
router-id 10.10.10.2
log-adjacency-changes
auto-cost reference-bandwidth 10000
network 10.10.10.2 0.0.0.0 area 0
!
!
ip route 192.0.2.0 255.255.255.0 192.0.4.1
ip route 192.168.32.0 255.255.240.0 192.0.4.1
```

2) OSPF NHRP:

```
Router#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
10.10.10.1 255 FULL/DR 00:00:31 10.10.10.1 Tunnel1

Router#show ip nhrp
10.10.10.1/32 via 10.10.10.1
Tunnel1 created 01:36:26, never expire
Type: static, Flags: used
NBMA address: 192.0.2.2
10.10.10.2/32 via 10.10.10.2
Tunnel1 created 00:01:00, expire 00:04:59
Type: dynamic, Flags: router unique local
NBMA address: 192.0.4.2
(no-socket)
10.10.10.3/32 via 10.10.10.3
Tunnel1 created 00:01:00, expire 00:04:59
Type: dynamic, Flags: router
NBMA address: 192.168.39.216
```

DMVPN over IPSEC (Cisco-HUB, ESR-Spoke, Cisco-Spoke)

:

NHRP- ESR-Spoke Cisco-HUB Cisco-Spoke transport . IPSEC. OSPF. Loopback.

HUB(Cisco):

1)

```
crypto isakmp policy 10
 encr aes 192
 authentication pre-share
 group 2
crypto isakmp key password address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set DMVPN-TR esp-aes 192 esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN
 set transform-set DMVPN-TR
!
interface Loopback1
 ip address 1.1.1.1 255.255.255.255
!
interface Tunnel0
 bandwidth 10000
 ip address 10.10.10.1 255.255.255.0
 no ip redirects
 ip mtu 1472
 ip nhrp authentication <password>
 ip nhrp map multicast dynamic
 ip nhrp network-id 60
 ip nhrp holdtime 360
 ip tcp adjust-mss 1432
 ip ospf network broadcast
 ip ospf cost 25
 ip ospf priority 255
 ip ospf mtu-ignore
 load-interval 30
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 60
 tunnel ttl 250
 tunnel protection ipsec profile DMVPN shared
 !
interface FastEthernet0/0
 ip address 192.0.2.2 255.255.255.0
 duplex auto
 speed auto
 !
router ospf 1
 router-id 10.10.10.1
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 network 1.1.1.1 0.0.0.0 area 0.0.0.0
 network 10.10.10.0 0.0.0.255 area 0.0.0.0
 distance 200
 !
ip route 192.0.4.2 255.255.255.255 192.0.2.1
ip route 192.168.39.216 255.255.255.255 192.0.2.1
```

2)

```
Router#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.0.2.2       192.168.39.216  QM_IDLE           1002 ACTIVE
192.0.2.2       192.0.4.2       QM_IDLE           1004 ACTIVE

IPv6 Crypto ISAKMP SA

Router#sh crypto ipsec sa
interface: Tunnel0
    Crypto map tag: DMVPN-head-1, local addr 192.0.2.2

   protected vrf: (none)
```

```
   local  ident (addr/mask/prot/port): (192.0.2.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.39.216/255.255.255.255/47/0)
   current_peer 192.168.39.216 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5623, #pkts encrypt: 5623, #pkts digest: 5623
    #pkts decaps: 5412, #pkts decrypt: 5412, #pkts verify: 5412
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.0.2.2, remote crypto endpt.: 192.168.39.216
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0xCD1A3CBE(3441048766)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x1096A95(17394325)
        transform: esp-192-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2007, flow_id: FPGA:7, sibling_flags 80000046, crypto map: DMVPN-head-1
        sa timing: remaining key lifetime (k/sec): (4518380/1494)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xCD1A3CBE(3441048766)
        transform: esp-192-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:8, sibling_flags 80000046, crypto map: DMVPN-head-1
        sa timing: remaining key lifetime (k/sec): (4518365/1494)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.0.2.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.0.4.2/255.255.255.255/47/0)
   current_peer 192.0.4.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 609, #pkts encrypt: 609, #pkts digest: 609
    #pkts decaps: 453, #pkts decrypt: 453, #pkts verify: 453
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

Router#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.2        2   FULL/DROTHER    00:00:39    10.10.10.2      Tunnel0
10.238.70.250   128   FULL/BDR        00:00:30    10.10.10.3      Tunnel0
Router#
Router#sh ip ro
Router#sh ip route os
Router#sh ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

      2.0.0.0/32 is subnetted, 1 subnets
O E2     2.2.2.2 [200/10000] via 10.10.10.3, 01:19:34, Tunnel0
      3.0.0.0/32 is subnetted, 1 subnets
O        3.3.3.3 [200/26] via 10.10.10.2, 00:52:46, Tunnel0
```

Spoke(ESR)

1)

```
router ospf log-adjacency-changes
router ospf 1
  router-id 10.10.10.3
  area 0.0.0.0
    network 2.2.2.2/32
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/1
  ip firewall disable
  ip address 192.168.39.216/20
exit
interface loopback 1
  ip address 2.2.2.2/32
exit

tunnel gre 1
  key 60
  ttl 250
  mtu 1472
  multipoint
  ip firewall disable
  local interface gigabitethernet 1/0/1
  ip address 10.10.10.3/24
  ip ospf instance 1
  ip ospf
  ip tcp adjust-mss 1432
  ip nhrp authentication <password>
  ip nhrp holding-time 360
  ip nhrp map 10.10.10.1 192.0.2.2
  ip nhrp nhs 10.10.10.1/24
  ip nhrp ipsec IPSECVPN_HUB static
  ip nhrp ipsec IPSECVPN_SPOKE dynamic
  ip nhrp multicast nhs
  ip nhrp enable
  enable
exit

security ike proposal IKEPROP
  encryption algorithm aes192
  dh-group 2
exit

security ike policy IKEPOLICY
  pre-shared-key ascii-text <password>
  proposal IKEPROP
exit

security ike gateway IKEGW_HUB
  ike-policy IKEPOLICY
  local address 192.168.39.216
  local network 192.168.39.216/32 protocol gre
  remote address 192.0.2.2
  remote network 192.0.2.2/32 protocol gre
```

```
  mode policy-based
exit

security ike gateway IKEGW_SPOKE
  ike-policy IKEPOLICY
  local address 192.168.39.216
  local network 192.168.39.216/32 protocol gre
  remote address any
  remote network any
  mode policy-based
exit

security ipsec proposal IPSECPROP
  encryption algorithm aes192
exit

security ipsec policy IPSECPOLICY
  proposal IPSECPROP
exit

security ipsec vpn IPSECVPN_HUB
  mode ike
  type transport
  ike establish-tunnel route
  ike gateway IKEGW_HUB
  ike ipsec-policy IPSECPOLICY
  enable
exit

security ipsec vpn IPSECVPN_SPOKE
  mode ike
  type transport
  ike establish-tunnel route
  ike gateway IKEGW_SPOKE
  ike ipsec-policy IPSECPOLICY
  enable
exit

security passwords history 0

ip route 192.0.2.2/32 192.168.39.1
ip route 192.0.4.2/32 192.168.39.1
```

2)

```
ESR# sh security ipsec vpn status
Name                              Local host        Remote host       Initiator spi        Responder spi
State
-------------------------------   ---------------   ---------------   ------------------   ------------------
-----------
IPSECVPN_HUB                      192.168.39.216    192.0.2.2         0x121319af1595214c   0xa3d8bd202e50320b
Established
IPSECVPN_SPOKE                    192.168.39.216    192.0.4.2         0x997a2d4ddc2a3cac   0x887bd45f6a25028e
Established
ESR#
ESR#
ESR# sh security ipsec vpn status IPSECVPN_HUB
Currently active IKE SA:
    Name:                       IPSECVPN_HUB
    State:                      Established
    Version:                    v1-only
    Unique ID:                  1
    Local host:                 192.168.39.216
    Remote host:                192.0.2.2
    Role:                       Initiator
    Initiator spi:              0x121319af1595214c
    Responder spi:              0xa3d8bd202e50320b
    Encryption algorithm:       aes192
    Authentication algorithm:   sha1
    Diffie-Hellman group:       2
```

```
    Established:               1 hour, 27 minutes and 46 seconds ago
    Rekey time:                1 hour, 27 minutes and 46 seconds
    Reauthentication time:     1 hour, 15 minutes and 12 seconds
    Child IPsec SAs:
        Name:                      dmvpn_192.168.39.216_192.0.2.2-7
        State:                     Installed
        Protocol:                  esp
        Mode:                      Tunnel
        Encryption algorithm:      aes192
        Authentication algorithm:  sha1
        Rekey time:                2 minutes and 44 seconds
        Life time:                 14 minutes and 55 seconds
        Established:               45 minutes and 5 seconds ago
        Traffic statistics:
            Input bytes:           45592
            Output bytes:          32192
            Input packets:         436
            Output packets:        319
        ------------------------------------------------------------
ESR# sh security ipsec vpn status IPSECVPN_SPOKE
Currently active IKE SA:
    Name:                      IPSECVPN_SPOKE
    State:                     Connecting
    Version:                   v1-only
    Unique ID:                 13
    Local host:                192.168.39.216
    Remote host:               224.0.0.5
    Role:                      Initiator
    Initiator spi:             0x35ece26be25cec50
    Responder spi:             0x0000000000000000
Currently active IKE SA:
    Name:                      IPSECVPN_SPOKE
    State:                     Established
    Version:                   v1-only
    Unique ID:                 14
    Local host:                192.168.39.216
    Remote host:               192.0.4.2
    Role:                      Initiator
    Initiator spi:             0x997a2d4ddc2a3cac
    Responder spi:             0x887bd45f6a25028e
    Encryption algorithm:      aes192
    Authentication algorithm:  sha1
    Diffie-Hellman group:      2
    Established:               1 minute and 37 seconds ago
    Rekey time:                1 minute and 37 seconds
    Reauthentication time:     2 hours, 48 minutes and 34 seconds
    Child IPsec SAs:
        Name:                      dmvpn_192.168.39.216_192.0.4.2-9
        State:                     Installed
        Protocol:                  esp
        Mode:                      Tunnel
        Encryption algorithm:      aes192
        Authentication algorithm:  sha1
        Rekey time:                46 minutes and 1 second
        Life time:                 58 minutes and 23 seconds
        Established:               1 minute and 37 seconds ago
        Traffic statistics:
            Input bytes:           1396
            Output bytes:          1344
            Input packets:         12
            Output packets:        12
        ------------------------------------------------------------
ESR#
ESR# sh ip ospf neighbors
Router ID        Pri  State          DTime  Interface          Router IP
---------        ---  -----          -----  -----------------  ---------
10.10.10.1       255  Full/DR        00:31  gre 1              10.10.10.1
ESR#
ESR# sh ip route ospf
O     * 1.1.1.1/32         [150/11]          via 10.10.10.1 on gre 1           [ospf1 13:58:42]  (10.10.10.1)
O       10.10.10.0/24      [150/10]          dev gre 1                         [ospf1 13:58:37]  (10.10.10.1)
```

```
O     * 3.3.3.3/32         [150/11]          via 10.10.10.2 on gre 1           [ospf1 14:25:24]  (10.10.10.2)
```

Spoke(Cisco)

1)

```
crypto isakmp policy 10
 encr aes 192
 authentication pre-share
 group 2
crypto isakmp key password address 0.0.0.0
!
!
crypto ipsec transform-set DMVPN-TR esp-aes 192 esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN
 set transform-set DMVPN-TR
!
!
interface Loopback1
 ip address 3.3.3.3 255.255.255.255
!
interface Tunnel0
 bandwidth 10000
 ip address 10.10.10.2 255.255.255.0
 no ip redirects
 ip mtu 1472
 ip nhrp authentication <password>
 ip nhrp network-id 60
 ip nhrp holdtime 360
 ip nhrp nhs 10.10.10.1 nbma 192.0.2.2 multicast
 ip tcp adjust-mss 1432
 ip ospf network broadcast
 ip ospf priority 2
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 60
 tunnel ttl 250
 tunnel protection ipsec profile DMVPN shared
!
interface FastEthernet0/0
 ip address 192.0.4.2 255.255.255.0
 duplex full
!
router ospf 1
 router-id 10.10.10.2
 auto-cost reference-bandwidth 10000
 network 3.3.3.3 0.0.0.0 area 0.0.0.0
 network 10.10.10.0 0.0.0.255 area 0.0.0.0
!
!
ip route 192.0.2.2 255.255.255.255 192.0.4.1
ip route 192.168.39.216 255.255.255.255 192.0.4.1
```

2)

```
Router#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.0.4.2       192.168.39.216  QM_IDLE           1004 ACTIVE
192.0.2.2       192.0.4.2       QM_IDLE           1002 ACTIVE

IPv6 Crypto ISAKMP SA

Router#
Router#sh crypto ipsec sa

interface: Tunnel0
    Crypto map tag: DMVPN-head-1, local addr 192.0.4.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.0.4.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.0.2.2/255.255.255.255/47/0)
   current_peer 192.0.2.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 577, #pkts encrypt: 577, #pkts digest: 577
    #pkts decaps: 739, #pkts decrypt: 739, #pkts verify: 739
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

    protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.0.4.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.39.216/255.255.255.255/47/0)
   current_peer 192.168.39.216 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 992, #pkts encrypt: 992, #pkts digest: 992
    #pkts decaps: 988, #pkts decrypt: 988, #pkts verify: 988
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0


Router#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.1      255   FULL/DR         00:00:36    10.10.10.1      Tunnel0
Router#
Router#sh ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
O        1.1.1.1 [110/1001] via 10.10.10.1, 01:12:35, Tunnel0
      2.0.0.0/32 is subnetted, 1 subnets
O E2     2.2.2.2 [110/10000] via 10.10.10.3, 01:12:35, Tunnel0
```