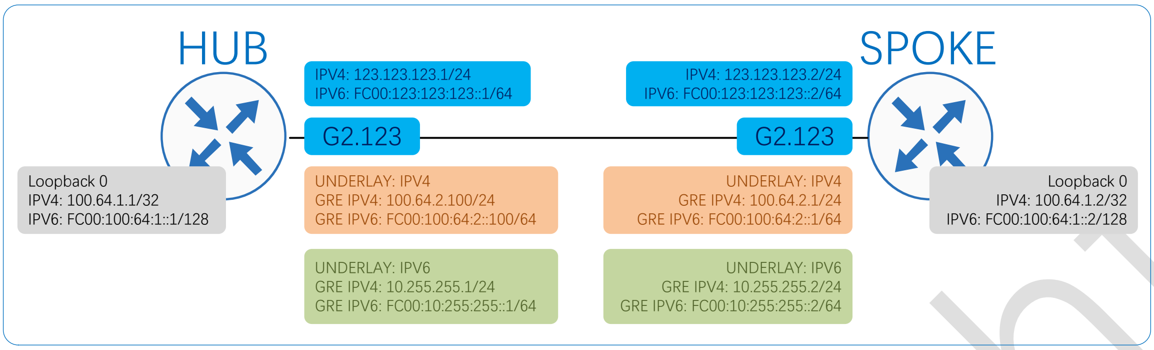
CISCO IOS XE DMVPN DESIGN GUIDE

PHASE 3/IKEV2 SMART DEFAULT CONFIGURATION (16.7.1 FUJI)

TABLE OF CONTENT

TOPOLOGY INFO UNDERLAY NETWORK


HUB
SPOKE
IPV4: 123.123.123.1/24
IPV6: FC00:123:123:123::1/64
IPV4: 123.123.123.2/24
IPV6: FC00:123:123:123::2/64
G2.123
G2.123
Loopback 0
IPV4: 100.64.1.1/32
IPV6: FC00:100:64:1::1/128
UNDERLAY: IPV4
GRE IPV4: 100.64.2.100/24
GRE IPV6: FC00:100:64:2::100/64
UNDERLAY: IPV4
GRE IPV4: 100.64.2.1/24
GRE IPV6: FC00:100:64:2::1/64
Loopback 0
IPV4: 100.64.1.2/32
IPV6: FC00:100:64:1::2/128
UNDERLAY: IPV6
GRE IPV4: 10.255.255.1/24
GRE IPV6: FC00:10:255:255::1/64
UNDERLAY: IPV6
GRE IPV4: 10.255.255.2/24
GRE IPV6: FC00:10:255:255::2/64

GLOBAL SETTINGS WITH IKEV2 CONFIGURATION

```
IPv6 unicast-routing
crypto ikev2 keyring IKEV2-KEYRING
 peer ANY-IPV4
  address 0.0.0.0 0.0.0.0
  pre-shared-key c1sco123
 !
 peer ANY-IPV6
  address ::/0
  pre-shared-key c1sco123
 !
crypto ikev2 profile default
 match fvrf any
 match identity remote address 0.0.0.0
 match identity remote address ::/0
 authentication remote pre-share
 authentication local pre-share
 keyring local IKEV2-KEYRING
crypto IPsec security-association replay window-size 1024
```

IPV4 OVER IPV4 TUNNEL

HUB configuration

```
interface TUNNEL64
 description IPV4-UNDERLAY-DMVPN-HUB
 IP address 100.64.2.100 255.255.255.0
 no IP redirects
 IP mtu 1400
 IP NHRP network-id 101
 IP NHRP redirect
 IP tcp adjust-mss 1360
 IP OSPF network point-to-multipoint
 IP OSPF mtu-ignore
 IP OSPF 1 area 0
 Tunnel source GigabitEthernet2.123
 Tunnel mode gre multipoint
 Tunnel key 101
 Tunnel protection IPsec profile default shared
```

SPOKE configuration

```
interface TUNNEL64
 description IPV4-UNDERLAY-DMVPN-SPOKE
 IP address 100.64.2.1 255.255.255.0
 no IP redirects
 IP mtu 1400
 IP NHRP network-id 101
 IP NHRP shortcut
 IP NHRP nhs 100.64.2.100 nbma 123.123.123.1 multicast
 IP tcp adjust-mss 1360
 IP OSPF network point-to-multipoint
 IP OSPF mtu-ignore
 IP OSPF 1 area 0
 Tunnel source GigabitEthernet2.123
 Tunnel mode gre multipoint
 Tunnel key 101
 Tunnel protection IPsec profile default shared
end
```

VERIFYING DMVPN FOR IPV4 OVER IPV4 CONFIGURATION

```
SPOKE#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

Tunnel-id Local              Remote              fvrf/ivrf          Status
2         123.123.123.2/500     123.123.123.1/500     none/none            READY
     Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK,
Auth verify: PSK
     Life/Active Time: 86400/6 sec
SPOKE#show crypto IPsec sa

interface: TUNNEL64
   Crypto map tag: default-head-1, local addr 123.123.123.2

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (123.123.123.2/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (123.123.123.1/255.255.255.255/47/0)
  current_peer 123.123.123.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 58, #pkts encrypt: 58, #pkts digest: 58
   #pkts decaps: 41, #pkts decrypt: 41, #pkts verify: 41
   #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.: 123.123.123.2, remote crypto endpt.: 123.123.123.1
    plaintext mtu 1458, path mtu 1500, IP mtu 1500, IP mtu idb GigabitEthernet2.123
    current outbound spi: 0x5DEB8336(1575715638)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0x11ADE970(296610160)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Transport, }
       conn id: 2062, flow_id: CSR:62, sibling_flags FFFFFFFF80000008, crypto map:
default-head-1
       sa timing: remaining key lifetime (k/sec): (4607993/3460)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 1024
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x5DEB8336(1575715638)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Transport, }
       conn id: 2061, flow_id: CSR:61, sibling_flags FFFFFFFF80000008, crypto map:
default-head-1
       sa timing: remaining key lifetime (k/sec): (4607994/3460)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 1024
       Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:

SPOKE#show IP NHRP detail
100.64.2.100/32 via 100.64.2.100
  TUNNEL64 created 00:03:44, never expire
  Type: static, Flags:
  NBMA address: 123.123.123.1
  Preference: 255
SPOKE #

HUB#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
       N - NATed, L - Local, X - No Socket
       T1 - Route Installed, T2 - Nexthop-override
       C - CTS Capable, I2 - Temporary
       # 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: TUNNEL64, IPv4 NHRP Details
Type:Hub, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
    1 123.123.123.2       100.64.2.1    UP 00:04:26     D

HUB#show IP OSPF neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
222.222.222.2     0   FULL/  -        00:01:32    100.64.2.1      TUNNEL64
```

IPV6 OVER IPV4 TUNNEL

HUB configuration

```
interface TUNNEL64
 description IPV4-UNDERLAY-DMVPN-HUB
IPv6 address FC00:100:64:2::100/64
 IPv6 NHRP network-id 101
 IPv6 NHRP redirect
 IPv6 OSPF 1 area 0
 IPv6 OSPF network point-to-multipoint
 IPv6 OSPF mtu-ignore
 Tunnel source GigabitEthernet2.123
 Tunnel mode gre multipoint
 Tunnel key 101
 Tunnel protection IPsec profile default shared
```

SPOKE configuration

```
interface TUNNEL64
 description IPV4-UNDERLAY-DMVPN-SPOKE
 IPv6 address FC00:100:64:2::1/64
 IPv6 NHRP network-id 101
 IPv6 NHRP nhs FC00:100:64:2::100 nbma 123.123.123.1 multicast
 IPv6 OSPF 1 area 0
 IPv6 OSPF network point-to-multipoint
 IPv6 OSPF mtu-ignore
 Tunnel source GigabitEthernet2.123
 Tunnel mode gre multipoint
 Tunnel key 101
 Tunnel protection IPsec profile default shared
```

VERIFYING DMVPN FOR IPV6 OVER IPV4 CONFIGURATION

```
SPOKE#show dmvpn IPv6
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # 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: TUNNEL64, IPv6 NHRP Details
Type:Spoke, Total NBMA Peers (v4/v6): 1
    1.Peer NBMA Address: 123.123.123.1
        Tunnel IPv6 Address: FC00:100:64:2::100
```

```
       IPv6 Target Network: FC00:100:64:2::100/128
       # Ent: 1, Status: UP, UpDn Time: 00:15:54, Cache Attrib: S

HUB#show dmvpn IPv6
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
       N - NATed, L - Local, X - No Socket
       T1 - Route Installed, T2 - Nexthop-override
       C - CTS Capable, I2 - Temporary
       # 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: TUNNEL64, IPv6 NHRP Details
Type:Hub, Total NBMA Peers (v4/v6): 1
   1.Peer NBMA Address: 123.123.123.2
       Tunnel IPv6 Address: FC00:100:64:2::1
       IPv6 Target Network: FC00:100:64:2::1/128
       # Ent: 1, Status: UP, UpDn Time: 00:16:33, Cache Attrib: D

HUB#show IPv6 OSPF neighbor

          OSPFv3 Router with ID (100.64.1.1) (Process ID 1)

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
100.64.1.4        0   FULL/  -        00:01:58    25              TUNNEL64
```

IPV6 OVER IPV6 TUNNEL

HUB configuration

```
interface Tunnel46
 description IPV6-UNDERLAY-DMVPN-HUB
 IPv6 address FC00:10:255:255::1/64
 IPv6 mtu 1400
 IPv6 tcp adjust-mss 1340
 IPv6 NHRP network-id 102
 IPv6 NHRP redirect
 IPv6 OSPF 1 area 0
 IPv6 OSPF network point-to-multipoint
 IPv6 OSPF mtu-ignore
 Tunnel source GigabitEthernet2.123
 Tunnel mode gre multipoint IPv6
 Tunnel key 102
 Tunnel path-mtu-discovery
 Tunnel protection IPsec profile default shared
end
```

SPOKE configuration

```
interface Tunnel46
 description IPV6-UNDERLAY-DMVPN-HUB
 IPv6 address FC00:10:255:255::2/64
 IPv6 mtu 1400
 IPv6 tcp adjust-mss 1340
 IPv6 NHRP network-id 102
 IPv6 NHRP nhs FC00:10:255:255::1 nbma FC00:123:123:123::1 multicast
 IPv6 OSPF 1 area 0
 IPv6 OSPF network point-to-multipoint
 IPv6 OSPF mtu-ignore
 Tunnel source GigabitEthernet2.123
 Tunnel mode gre multipoint IPv6
 Tunnel key 102
 Tunnel path-mtu-discovery
 Tunnel protection IPsec profile default shared
end
```

VERIFYING DMVPN FOR IPV6 OVER IPV6 CONFIGURATION

```
SPOKE#show crypto ikev2 sa
****
 IPv6 Crypto IKEv2  SA

Tunnel-id    fvrf/ivrf            Status
3         none/none            READY
Local  FC00:123:123:123::2/500
Remote  FC00:123:123:123::1/500
     Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK,
Auth verify: PSK
     Life/Active Time: 86400/6 sec

SPOKE#show dmvpn IPv6
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
       N - NATed, L - Local, X - No Socket
       T1 - Route Installed, T2 - Nexthop-override
       C - CTS Capable, I2 - Temporary
       # 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: Tunnel46, IPv6 NHRP Details
Type:Spoke, Total NBMA Peers (v4/v6): 1
   1.Peer NBMA Address: FC00:123:123:123::1
       Tunnel IPv6 Address: FC00:10:255:255::1
       IPv6 Target Network: FC00:10:255:255::1/128
       # Ent: 1, Status: UP, UpDn Time: 00:01:26, Cache Attrib: S

SPOKE#show IPv6 OSPF neighbor

          OSPFv3 Router with ID (100.64.1.4) (Process ID 1)

Neighbor ID     Pri   State          Dead Time   Interface ID    Interface
100.64.1.1        0   FULL/  -       00:01:43    27             Tunnel46
```

IPV4 OVER IPV6 TUNNEL

HUB configuration

```
interface Tunnel46
 description IPV6-UNDERLAY-DMVPN-HUB
 IP address 10.255.255.1 255.255.255.0
 IP NHRP network-id 102
 IP OSPF network point-to-multipoint
 IP OSPF mtu-ignore
 IP OSPF 1 area 0
 Tunnel source GigabitEthernet2.123
 Tunnel mode gre multipoint IPv6
 Tunnel key 102
 Tunnel path-mtu-discovery
 Tunnel protection IPsec profile default shared
end
```

SPOKE configuration

```
interface Tunnel46
 description IPV6-UNDERLAY-DMVPN-HUB
 IP address 10.255.255.2 255.255.255.0
 IP NHRP network-id 102
 IP NHRP nhs 10.255.255.1 nbma FC00:123:123:123::1 multicast
 IP OSPF network point-to-multipoint
 IP OSPF mtu-ignore
 IP OSPF 1 area 0
 Tunnel source GigabitEthernet2.123
 Tunnel mode gre multipoint IPv6
 Tunnel key 102
 Tunnel path-mtu-discovery
 Tunnel protection IPsec profile default shared
end
```

VERIFYING DMVPN FOR IPV4 OVER IPV6 CONFIGURATION

```
SPOKE#show crypto ikev2 sa
****
 IPv6 Crypto IKEv2  SA

Tunnel-id    fvrf/ivrf              Status
3         none/none              READY
Local  FC00:123:123:123::2/500
Remote  FC00:123:123:123::1/500
     Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK,
Auth verify: PSK
```

```
     Life/Active Time: 86400/6 sec
HUB#show cry IPsec sa
interface: Tunnel46
   Crypto map tag: default-head-1, local addr FC00:123:123:123::1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (FC00:123:123:123::1/128/47/0)
  remote ident (addr/mask/prot/port): (FC00:123:123:123::2/128/47/0)
  current_peer FC00:123:123:123::2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3452, #pkts encrypt: 3452, #pkts digest: 3452
   #pkts decaps: 3262, #pkts decrypt: 3262, #pkts verify: 3262
   #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.: FC00:123:123:123::1,
    remote crypto endpt.: FC00:123:123:123::2
    plaintext mtu 1462, path mtu 1500, IPv6 mtu 1500, IPv6 mtu idb GigabitEthernet2.123
    current outbound spi: 0x54DC849D(1423738013)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0xFBD4D480(4225029248)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Transport, }
       conn id: 2067, flow_id: CSR:67, sibling_flags FFFFFFFF80000009, crypto map:
default-head-1
       sa timing: remaining key lifetime (k/sec): (4607937/452)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 1024
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x54DC849D(1423738013)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Transport, }
       conn id: 2068, flow_id: CSR:68, sibling_flags FFFFFFFF80000009, crypto map:
default-head-1
       sa timing: remaining key lifetime (k/sec): (4607951/452)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 1024
       Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:

HUB#show dmvpn IPv4
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
       N - NATed, L - Local, X - No Socket
       T1 - Route Installed, T2 - Nexthop-override
       C - CTS Capable, I2 - Temporary
       # 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: Tunnel46, IPv4 NHRP Details
Type:Hub, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
    1 FC00:123:123:123::2
                      10.255.255.2    UP 00:06:26     D
SPOKE#show IP OSPF nei

Neighbor ID     Pri   State           Dead Time   Address         Interface
222.222.222.2     0   FULL/  -        00:01:38    10.255.255.2    Tunnel46
```

DESIGN OPTION AND BEST PRACTICE

针对 DMVPN 的 NHRP 协议，OVERLAY 如何封装 GRE 取决与 Tunnel Destination 是谁，NHRP 根据定义的 NHRP mapping 动作触发 NHRP 注册行为到 HUB 节点后，HUB 将会维护 NHRP 表，并且将得知的某个 SPOKE 的真实的 UNDERLAY IP 作为 Tunnel destination 完成 GRE 封包动作，且加入到 CEF 表中完成快速转发。

- IPv4 over IPv4 nhs OVERLAY(v4) UNDERLAY (v4)
- IPv6 over IPv4 nhs OVERLAY(v6) UNDERLAY (v4)
- IPv4 over IPv6 nhs OVERLAY(v4) UNDERLAY (v6)
- IPv6 over IPv6 nhs OVERLAY(v6) UNDERLAY (v6)

DHCP OVER DMVPN

HUB

```
ip dhcp exclude-address X.X.X.X
ip dhcp pool spoke
 network X.X.X.X.0 /Y
ip dhcp support tunnel unicast
```

SPOKE [CSR 1000V FUJI 16.7 Does not support this feature]

```
ip dhcp support tunnel unicast
 Int TUNNEL 64
  ip dhcp client broadcast-flag clear
  Ip address dhcp
```

DYNAMIC TO DYNAMIC DMVPN NHRP MAPPING

HUB/SPOKE

```
ip name-server [DNS-Server-primary IP] [DNS-Server-backup IP]
ip domain lookup
interface g2.X
 description INET-UNDERLAY
 ip address dhcp
 ipv6 address autoconfig
!
Ip route 0.0.0.0 0.0.0.0 [ISP-IPV4] name IPV4-INET
ipv6 route ::/0 [ISP-IPV6] name IPV6-INET
interface tunnel 46/64
no tunnel protection IPsec profile default shared
```

SPOKE

```
interface TUNNEL64
description IPV4-UNDERLAY-DMVPN-SPOKE
ip nhrp nhs 100.64.2.100 nbma hubv4.cisco.com
ipv6 nhrp nhs FC00:100:64:2::100 nbma hubv4.cisco.com multicast
!
interface Tunnel46
```

```
description IPV6-UNDERLAY-DMVPN-SPOKE
ip nhrp nhs 10.255.255.1 nbma hubv6.cisco.com multicast
ipv6 nhrp nhs FC00:10:255:255::1 nbma hubv6.cisco.com multicast
```

VERIFYING DYNAMIC PEER DMVPN CONFIGURATION-UNDERLAY-IPV4

```
SPOKE#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # 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: Tunnel64, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 180.64.1.9        100.64.2.100    UP 00:04:04     S
                (hub.cisco.com)

Interface: Tunnel64, IPv6 NHRP Details
Type:Spoke, Total NBMA Peers (v4/v6): 1
    1.Peer NBMA Address: 180.64.1.9(hubv4.cisco.com)
        Tunnel IPv6 Address: FC00:100:64:2::100
        IPv6 Target Network: FC00:100:64:2::100/128
        # Ent: 1, Status: UP, UpDn Time: 00:04:04, Cache Attrib: S

SPOKE#
SPOKE#ping hubv4.cisco.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 180.64.1.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
SPOKE#ping hubv4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 180.64.1.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
SPOKE#show ip ospf nei

Neighbor ID     Pri   State           Dead Time   Address         Interface
```

```
100.64.1.1        0   FULL/  -        00:01:46    100.64.2.100    Tunnel64
SPOKE#show ipv6 ospf nei

          OSPFv3 Router with ID (100.64.1.4) (Process ID 1)

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
100.64.1.1        0   FULL/  -        00:01:41    14              Tunnel64
SPOKE#
```

VERIFYING DYNAMIC PEER DMVPN CONFIGURATION-UNDERLAY-IPV6

```
SPOKE#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
       N - NATed, L - Local, X - No Socket
       T1 - Route Installed, T2 - Nexthop-override
       C - CTS Capable, I2 - Temporary
       # 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: Tunnel46, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
    1 2001:180:64:1::9
                      10.255.255.1    UP 00:12:33    S
             (hubv6.cisco.com)

Interface: Tunnel46, IPv6 NHRP Details
Type:Spoke, Total NBMA Peers (v4/v6): 1
   1.Peer NBMA Address: 2001:180:64:1::9(hubv6.cisco.com)
       Tunnel IPv6 Address: FC00:10:255:255::1
       IPv6 Target Network: FC00:10:255:255::1/128
       # Ent: 1, Status: UP, UpDn Time: 00:12:33, Cache Attrib: S

SPOKE#ping hubv6.cisco.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:180:64:1::9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
SPOKE#ping hubv6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:180:64:1::9, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
SPOKE#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
100.64.1.1        0   FULL/  -        00:01:40    10.255.255.1    Tunnel46
SPOKE#show ipv6 ospf neighbor

          OSPFv3 Router with ID (100.64.1.4) (Process ID 1)

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
100.64.1.1        0   FULL/  -        00:01:39    12              Tunnel46
SPOKE#
```

IKEV2 WITH FQDN AUTHENTICATION METHOD-UNDERLAY-IPV4

HUB

```
crypto ikev2 keyring IKEV2-KEYRING
 peer ANY-IPV4
  address 0.0.0.0 0.0.0.0
  identity fqdn spokev4.cisco.com
  pre-shared-key c1sco123
!
crypto ikev2 profile default
 match identity remote fqdn spokev4.cisco.com
 identity local fqdn hubv4.cisco.com
interface tunnel 64
 tunnel protection ipsec profile default shared
```

SPOKE

```
crypto ikev2 keyring IKEV2-KEYRING
 peer ANY-IPV4
  address 0.0.0.0 0.0.0.0
  identity fqdn hubv4.cisco.com
  pre-shared-key c1sco123
 !
crypto ikev2 profile default
 match identity remote fqdn hubv4.cisco.com
 identity local fqdn spokev4.cisco.com
interface tunnel 64
 tunnel protection ipsec profile default shared
```

VERIFYING IKEV2 WITH FQDN CONFIGURATION-UNDERLAY-IPV4

```
HUB#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         180.64.1.9/500        180.64.2.3/500        none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK,
Auth verify: PSK
      Life/Active Time: 86400/370 sec

 IPv6 Crypto IKEv2  SA

HUB#
HUB#show crypto ipsec sa

interface: Tunnel100
```

```
    Crypto map tag: default-head-1, local addr 180.64.1.9

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (180.64.1.9/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (180.64.2.3/255.255.255.255/47/0)
   current_peer 180.64.2.3 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 77, #pkts encrypt: 77, #pkts digest: 77
    #pkts decaps: 64, #pkts decrypt: 64, #pkts verify: 64
    #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.: 180.64.1.9, remote crypto endpt.: 180.64.2.3
     plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet2.181
     current outbound spi: 0x37540255(928252501)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x338F84AD(865043629)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2007, flow_id: CSR:7, sibling_flags FFFFFFFF80000008, crypto map:
default-head-1
        sa timing: remaining key lifetime (k/sec): (4607990/3214)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 1024
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x37540255(928252501)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2008, flow_id: CSR:8, sibling_flags FFFFFFFF80000008, crypto map:
default-head-1
        sa timing: remaining key lifetime (k/sec): (4607991/3214)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 1024
        Status: ACTIVE(ACTIVE)
     outbound ah sas:

     outbound pcp sas:
HUB#
```

IKEV2 WITH FQDN AUTHENTICATION METHOD-UNDERLAY-IPV6

HUB

```
crypto ikev2 keyring IKEV2-KEYRING
peer ANY-IPV6
  address ::/0
  identity fqdn spokev6.cisco.com
  pre-shared-key c1sco123
!
crypto ikev2 profile default
 match identity remote fqdn spokev6.cisco.com
 identity local fqdn hubv6.cisco.com
interface tunnel 46
 tunnel protection ipsec profile default shared
```

SPOKE

```
crypto ikev2 keyring IKEV2-KEYRING
peer ANY-IPV6
  address ::/0
  identity fqdn hubv6.cisco.com
  pre-shared-key c1sco123
 !
crypto ikev2 profile default
 match identity remote fqdn hubv6.cisco.com
 identity local fqdn spokev6.cisco.com
interface tunnel 46
 tunnel protection ipsec profile default shared
```

VERIFYING IKEV2 WITH FQDN CONFIGURATION-UNDERLAY-IPV6

```
HUB#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

 IPv6 Crypto IKEv2  SA

Tunnel-id    fvrf/ivrf             Status
1         none/none             READY
Local  2001:180:64:1::9/500
Remote  2001:180:64:2:250:56FF:FE99:2783/500
     Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK,
Auth verify: PSK
```

```
     Life/Active Time: 86400/14 sec

HUB#show crypto ipsec sa

interface: Tunnel46
   Crypto map tag: default-head-1, local addr 2001:180:64:1::9

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (2001:180:64:1::9/128/47/0)
  remote ident (addr/mask/prot/port): (2001:180:64:2:250:56FF:FE99:2783/128/47/0)
  current_peer 2001:180:64:2:250:56FF:FE99:2783 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 43, #pkts encrypt: 43, #pkts digest: 43
   #pkts decaps: 57, #pkts decrypt: 57, #pkts verify: 57
   #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.: 2001:180:64:1::9,
    remote crypto endpt.: 2001:180:64:2:250:56FF:FE99:2783
    plaintext mtu 1462, path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb GigabitEthernet2.181
    current outbound spi: 0x242E9CE7(607034599)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0x77C03AFC(2009086716)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Transport, }
       conn id: 2009, flow_id: CSR:9, sibling_flags FFFFFFFF80000009, crypto map:
default-head-1
       sa timing: remaining key lifetime (k/sec): (4607991/3427)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 1024
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x242E9CE7(607034599)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Transport, }
```

```
        conn id: 2010, flow_id: CSR:10, sibling_flags FFFFFFFF80000009, crypto map: 
default-head-1
        sa timing: remaining key lifetime (k/sec): (4607994/3427)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 1024
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
HUB#
```

IGP/BGP OVER DMVPN

OSPFv2 v3

- IP/IPv6 OSPF network type point-multIPoint （无 DR-BDR 角色）
- IP/IPv6 OSPF mtu-ignore （忽略 MTU 校验-EXSTART State，如调整 Tunnel 接口 MTU，OSPF 不会受到影响）
- IP/IPv6 OSPF prefix-suppression (节约 RIB 表)

EIGRPv4 v6

- Address-family mode

BGP

- HUB BGP RR listening-mode
- SPOKE BGP Speaker

CLI REFERENCE

```
router eigrp OVERLAY
 !
 address-family ipv4 unicast autonomous-system 500
  !
  topology base
  exit-af-topology
  network 100.64.1.0 0.0.0.255
  network 192.168.10.0
  eigrp router-id 11.11.11.11
 exit-address-family
```

HUB configuration

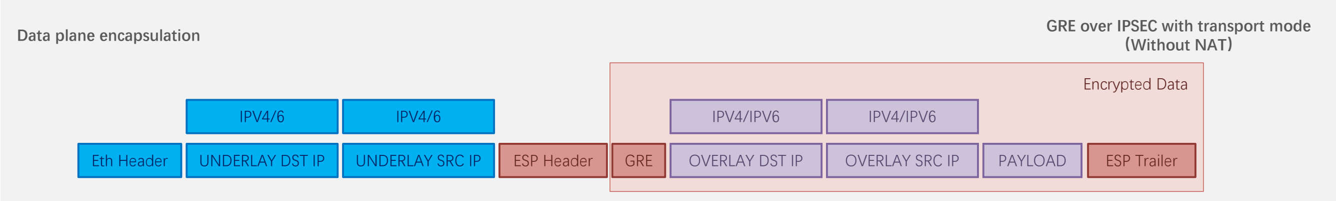
```
router bgp 9000
 bgp router-id 100.64.1.4
 bgp log-neighbor-changes
 bgp listen range [SPOKE-TUNNEL-IP/MASK]/16 peer-group SPOKE
 neighbor SPOKE peer-group
 neighbor SPOKE remote-as 9000
 neighbor SPOKE update-source TUNNEL 64
 !
 address-family IPv4
```

```
  neighbor SPOKE activate
  neighbor SPOKE route-reflector-client
 exit-address-family
```

SPOKE configuration

```
router bgp 9000
 bgp router-id 100.64.22.2
 bgp log-neighbor-changes
 neighbor [HUB-TUNNEL-IP] remote-as 9000
 neighbor [HUB-TUNNEL-IP] update-source TUNNEL 64
 !
address-family ipv4
  neighbor [HUB-TUNNEL-IP] activate
 exit-address-family
```

PACKET CAPTURE



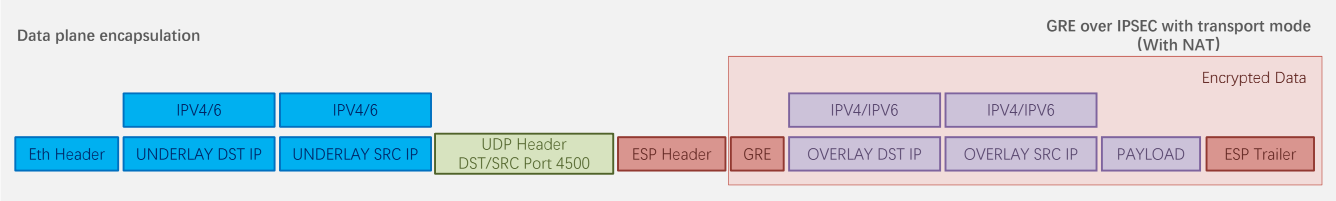
Data plane encapsulation

GRE over IPSEC with transport mode
(Without NAT)

Encrypted Data

IPV4/6 | IPV4/6 | IPV4/IPV6 | IPV4/IPV6

Eth Header | UNDERLAY DST IP | UNDERLAY SRC IP | ESP Header | GRE | OVERLAY DST IP | OVERLAY SRC IP | PAYLOAD | ESP Trailer



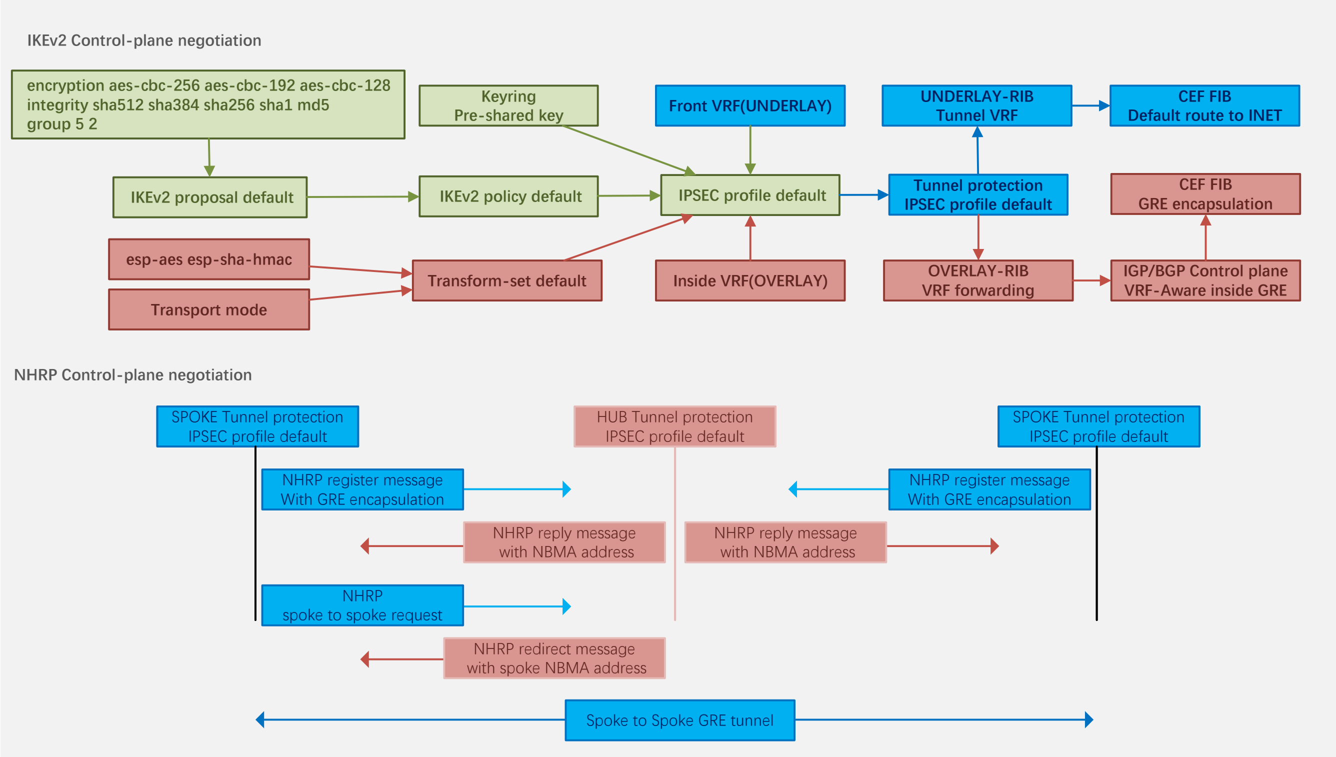
Data plane encapsulation

GRE over IPSEC with transport mode
(With NAT)

Encrypted Data

IPV4/6 | IPV4/6 | IPV4/IPV6 | IPV4/IPV6

Eth Header | UNDERLAY DST IP | UNDERLAY SRC IP | UDP Header DST/SRC Port 4500 | ESP Header | GRE | OVERLAY DST IP | OVERLAY SRC IP | PAYLOAD | ESP Trailer



IKEv2 Control-plane negotiation

encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
integrity sha512 sha384 sha256 sha1 md5
group 5 2

Keyring
Pre-shared key

Front VRF(UNDERLAY)

UNDERLAY-RIB
Tunnel VRF

CEF FIB
Default route to INET

IKEv2 proposal default

IKEv2 policy default

IPSEC profile default

Tunnel protection
IPSEC profile default

CEF FIB
GRE encapsulation

esp-aes esp-sha-hmac

Transport mode

Transform-set default

Inside VRF(OVERLAY)

OVERLAY-RIB
VRF forwarding

IGP/BGP Control plane
VRF-Aware inside GRE

NHRP Control-plane negotiation

SPOKE Tunnel protection
IPSEC profile default

HUB Tunnel protection
IPSEC profile default

SPOKE Tunnel protection
IPSEC profile default

NHRP register message
With GRE encapsulation

NHRP register message
With GRE encapsulation

NHRP reply message
with NBMA address

NHRP reply message
with NBMA address

NHRP
spoke to spoke request

NHRP redirect message
with spoke NBMA address

Spoke to Spoke GRE tunnel

MTU Setting

IPSEC Headers & Trailers

AH and ESP both add headers to the TCP/IP packet itself, ESP also adds an Initialisation Vector (IV) and a trailer. The size of this additional data depends on the IPsec protocol and mode used, as follows;

- Tunnel Mode: 20 Byte header regardless of protocol used
- Transport Mode: No additional data, headers or trailers
- AH: 24 Byte header
- ESP: 40 Bytes (8 Byte header (SPI and Sequence Number,) 16 Byte IV and 16 Byte trailer)

Reference Note: The Initialisation Vector (IV) is always be the same as the encryption block size – RFC3602, Section 2.1

Transmitting 1 Byte of Data

This might seem unlikely but programs such as Telnet and SSH transmit a packet for every character sent or received during a session.

- Add 15 Bytes for AES padding to reach the 16 Byte AES block size (1 16 Byte block)
- Add 1 bit for the padding identifier
- Add 8 Bytes for the SHA-1 message length information
- Add 39 Bytes, 7 bits padding to reach the 64 Byte SHA-1 block size (1 64 Byte block)
- Add 20 Bytes for the ESP tunnel mode header
- Add 8 Bytes for the ESP header
- Add 16 Bytes for the ESP IV
- Add 16 Byes for the ESP trailer
- Total packet size (minus TCP/IP headers) is now: 124 Bytes – an increase of 12,300%

Transmitting 1000 Bytes of Data

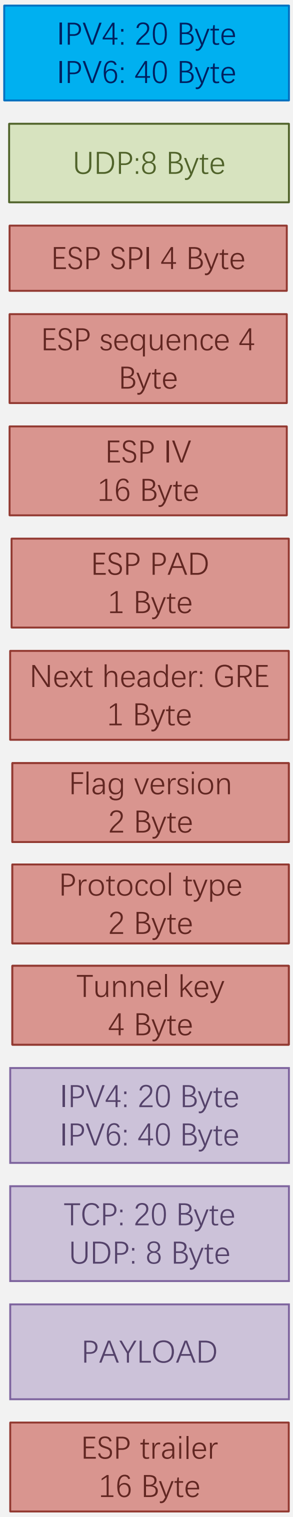
- Add 8 Bytes for AES padding to reach the 16 Byte AES block size (63 16 Byte blocks)
- Add 1 bit for the padding identifier
- Add 8 Bytes for the SHA-1 message length information
- Add 7 Bytes, 7 bits padding to reach the 64 Byte SHA-1 block size (16 64 Byte blocks)
- Add 20 Bytes for the ESP tunnel mode header
- Add 8 Bytes for the ESP header
- Add 16 Bytes for the ESP IV
- Add 16 Byes for the ESP trailer
- Total packet size (minus TCP/IP headers) is now: 1084 Bytes – an increase of 8.4%

Transmitting 1328 Bytes of Data

- Add 0 Bytes for AES padding to reach the 16 Byte AES block size (83 16 Byte blocks)
- Add 0 bit for the padding identifier
- Add 8 Bytes for the SHA-1 message length information
- Add 8 Bytes padding to reach the 64 Byte SHA-1 block size (21 64 Byte blocks)
- Add 20 Bytes for the ESP tunnel mode header
- Add 8 Bytes for the ESP header
- Add 16 Bytes for the ESP IV
- Add 16 Byes for the ESP trailer
- Total packet size (minus TCP/IP headers) is now: 1404 Bytes – an increase of 5.72%

Transmitting 1460 Bytes of Data

- Add 12 Bytes for AES padding to reach the 16 Byte AES block size (92 16 Byte blocks)
- Add 1 bit for the padding identifier
- Add 8 Bytes for the SHA-1 message length information
- Add 55 Bytes, 7 bits padding to reach the 64 Byte SHA-1 block size (24 64 Byte blocks)
- Add 20 Bytes for the ESP tunnel mode header
- Add 8 Bytes for the ESP header
- Add 16 Bytes for the ESP IV
- Add 16 Byes for the ESP trailer
- Total packet size (minus TCP/IP headers) is now: 1596 Bytes – an increase of 9.32%



IPV4: 20 Byte
IPV6: 40 Byte

UDP:8 Byte

ESP SPI 4 Byte

ESP sequence 4 Byte

ESP IV
16 Byte

ESP PAD
1 Byte

Next header: GRE
1 Byte

Flag version
2 Byte

Protocol type
2 Byte

Tunnel key
4 Byte

IPV4: 20 Byte
IPV6: 40 Byte

TCP: 20 Byte
UDP: 8 Byte

PAYLOAD

ESP trailer
16 Byte