Cisco live!

What You Make Possible

TOMORROW
starts here.

cisco

Troubleshooting DMVPNs

BRKSEC-3052

TOMORROW starts here.

Housekeeping

- We value your feedback- don't forget to complete your online session evaluations after each session & the Overall Conference Evaluation which will be available online from Thursday
- Visit the World of Solutions and Meet the Engineer
- Visit the Cisco Store to purchase your recommended readings
- Please switch off your mobile phones
- After the event don’t forget to visit Cisco Live 365: www.ciscolive365.com

Agenda

- DMVPN Overview
- Four Layer Troubleshooting Methodology

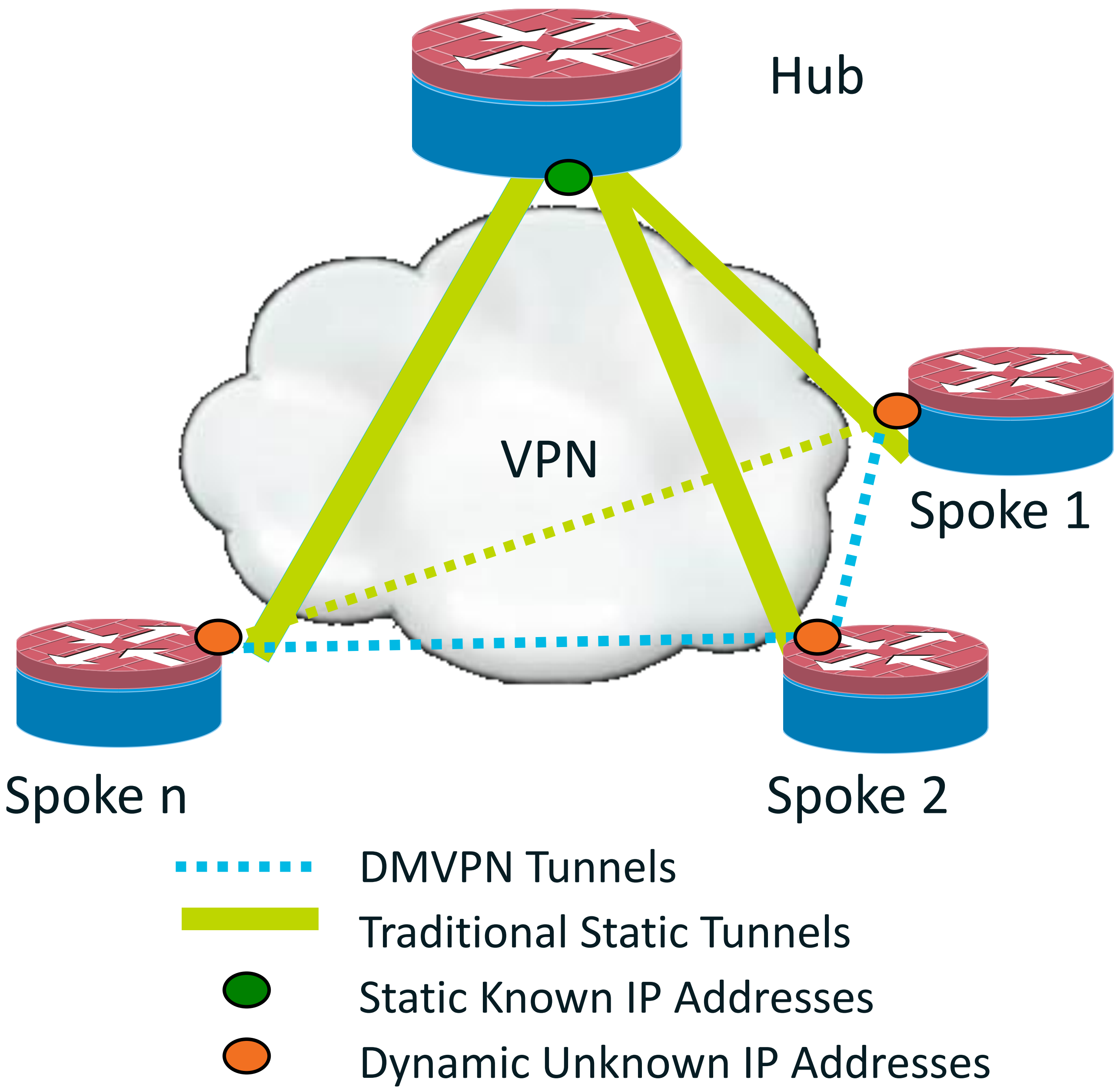
  Common Issues
- DMVPN Best Practice Configuration
- Q & A

DMVPN Overview

Dynamic Multipoint VPN

- Provides full meshed connectivity with simple configuration of hub and spoke
- Supports dynamically addressed spokes
- Facilitates zero-touch configuration for addition of new spokes
- Features automatic IPsec triggering for building an IPsec tunnel

Secure On-Demand Meshed Tunnels

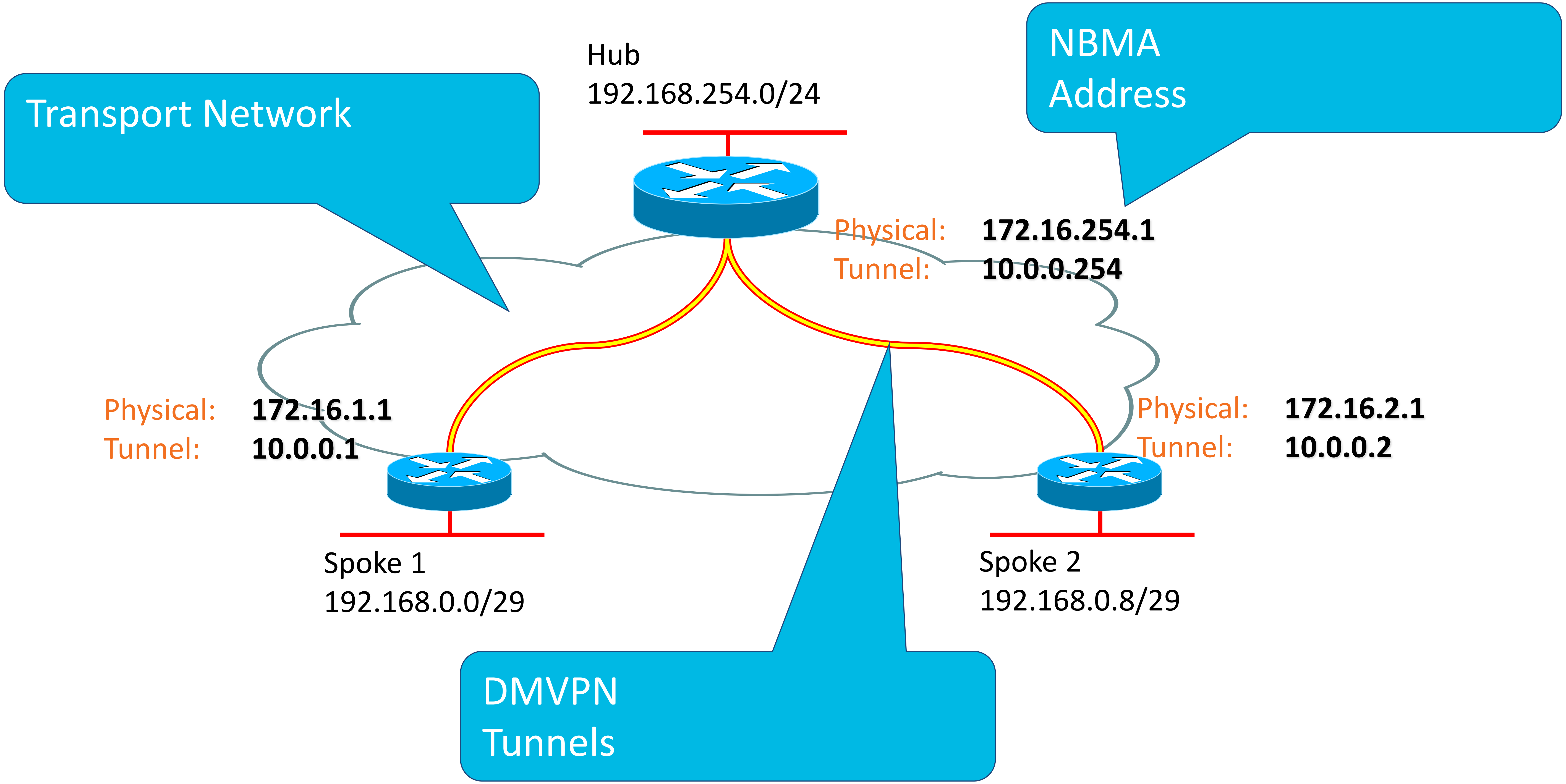

Hub
VPN
Spoke 1
Spoke n
Spoke 2
DMVPN Tunnels
Traditional Static Tunnels
Static Known IP Addresses
Dynamic Unknown IP Addresses

What Is Dynamic Multipoint VPN?

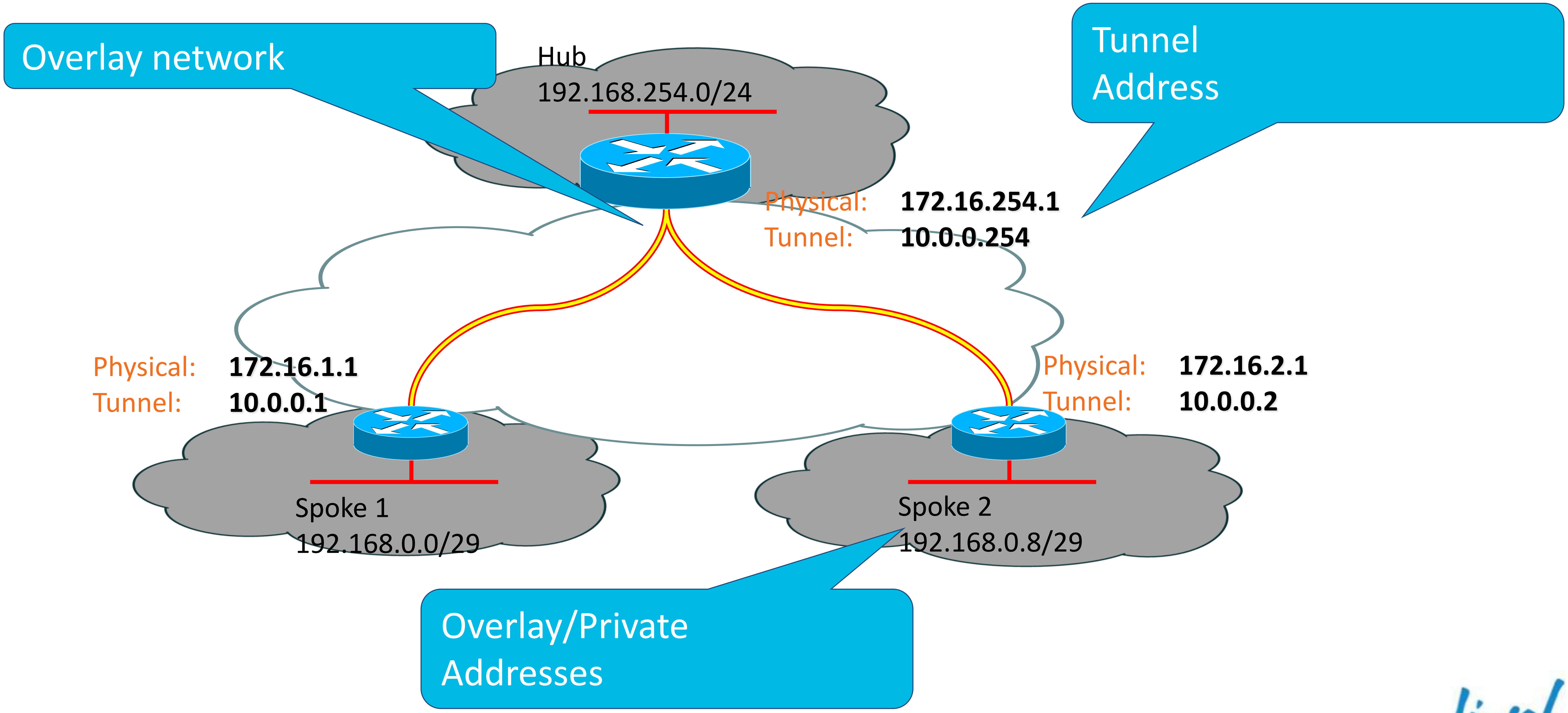
- DMVPN is a Cisco IOS Software solution for building IPsec+GRE VPNs in an easy, dynamic and scalable manner

- DMVPN relies on two proven technologies
  - Next Hop Resolution Protocol (NHRP)
    - Creates a distributed (NHRP) mapping database of all the spoke’s tunnel to real (public interface) addresses
  - Multipoint GRE Tunnel Interface
    - Single GRE interface to support multiple GRE/IPsec tunnels
    - Simplifies size and complexity of configuration

Nomenclature – Transport



Nomenclature – Overlay



Overlay network

Hub
192.168.254.0/24

Tunnel
Address

Physical: 172.16.254.1
Tunnel: 10.0.0.254

Physical: 172.16.1.1
Tunnel: 10.0.0.1

Physical: 172.16.2.1
Tunnel: 10.0.0.2

Spoke 1
192.168.0.0/29

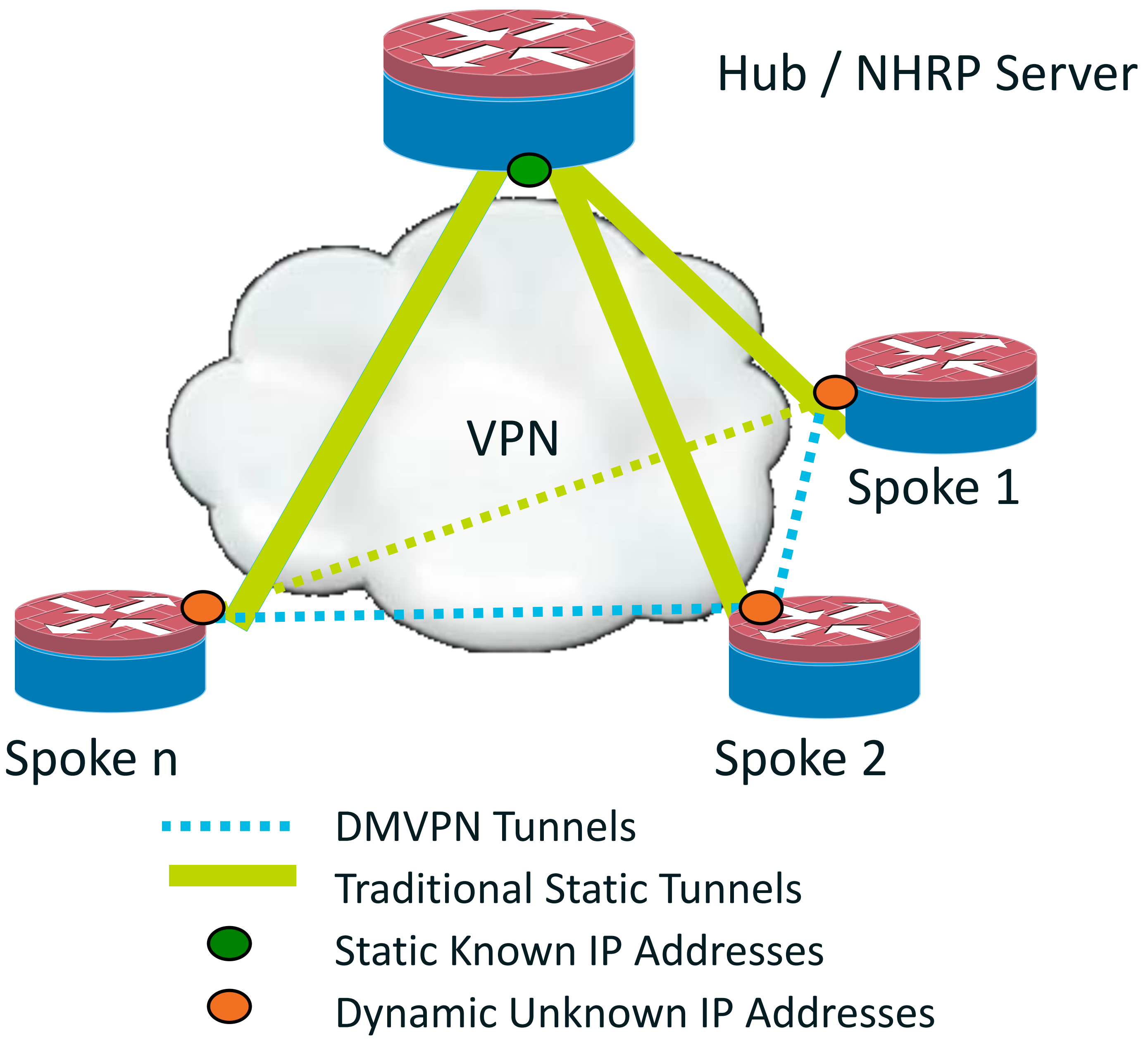
Spoke 2
192.168.0.8/29

Overlay/Private
Addresses

DMVPN—How It Works

- Spokes have a dynamic permanent GRE/IPsec tunnel to the hub; they register as clients of the NHRP server.
- Based on on-demand traffic, spoke queries the NHRP server for the real (outside) address of the destination spoke
- Now the originating spoke can initiate a dynamic GRE/IPsec tunnel to the target spoke
- The spoke-to-spoke tunnel is built over the mGRE interface.
- When traffic ceases then the spoke-to-spoke tunnel is torn down.

Secure On-Demand Meshed Tunnels


Hub / NHRP Server
VPN
Spoke 1
Spoke n
Spoke 2
DMVPN Tunnels
Traditional Static Tunnels
Static Known IP Addresses
Dynamic Unknown IP Addresses

Dynamic Multipoint VPN (DMVPN) Major Features

- Configuration reduction and no-touch deployment
- IP(v4/v6) unicast, IP multicast and dynamic routing protocols.
- Spokes with dynamically assigned addresses
- NAT—spoke routers behind dynamic NAT and hub routers behind static NAT
- Dynamic spoke-spoke tunnels for scaling partial/full mesh VPNs
- Can be used without IPsec encryption
- VRFs—GRE tunnels and/or data packets in VRFs
- 2547oDMVPN—MPLS switching over tunnels
- QoS—aggregate; static/manual per-tunnel
- Transparent to most data packet level features
- Wide variety of network designs and options

DMVPN Components

- **Next Hop Resolution Protocol (NHRP)**

  Creates a distributed (NHRP) mapping database of all the spoke's tunnel to real (public interface) addresses

- **Multipoint GRE Tunnel Interface (MGRE)**

  Single GRE interface to support multiple GRE/IPsec tunnels

  Simplifies size and complexity of configuration

- **IPsec tunnel protection**

  Dynamically creates and applies encryption policies

- **Routing**

  Dynamic advertisement of branch networks; almost all routing protocols (EIGRP, RIP, OSPF, BGP, ODR) are supported

DMVPN Phases

Phase 1

- Hub and spoke functionality 12.2(13)T
- Simplified and smaller config for hub & spoke
- Support dynamically address CPE
- Support for multicast traffic from hub to spoke
- Summarise routing at hub

Phase 2

- Spoke to spoke functionality 12.3(4)T
- Single mGRE interface in spokes
- Direct spoke to spoke data traffic - reduced load on hub
- Cannot summarise spoke routes on hub
- Route on spoke must have IP next hop of remote spoke

Phase 3

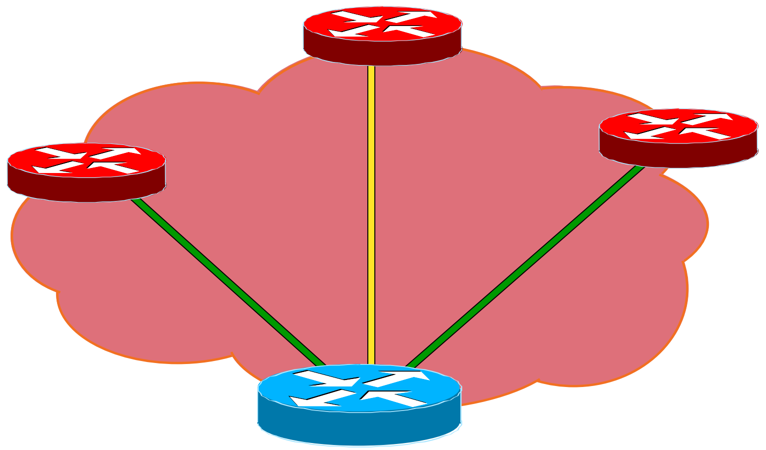
- Architecture and scaling 12.4(6)T
- Increase number of hub with same hub and spoke ratio
- No hub daisy-chain
- Spokes don’t need full routing table
- OSPF routing protocol not limited to 2 hubs
- Cannot mix phase 2 and phase 3 in same DMVPN cloud

Network Designs

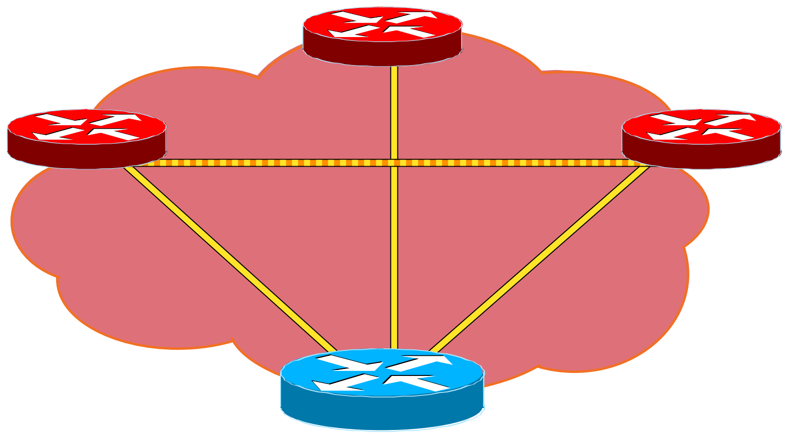
Spoke-to-hub tunnels

Spoke-to-spoke tunnels

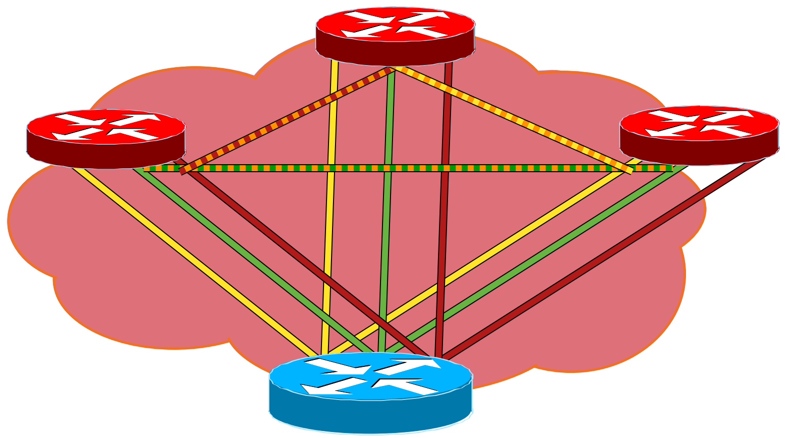
2547oDMVPN tunnels



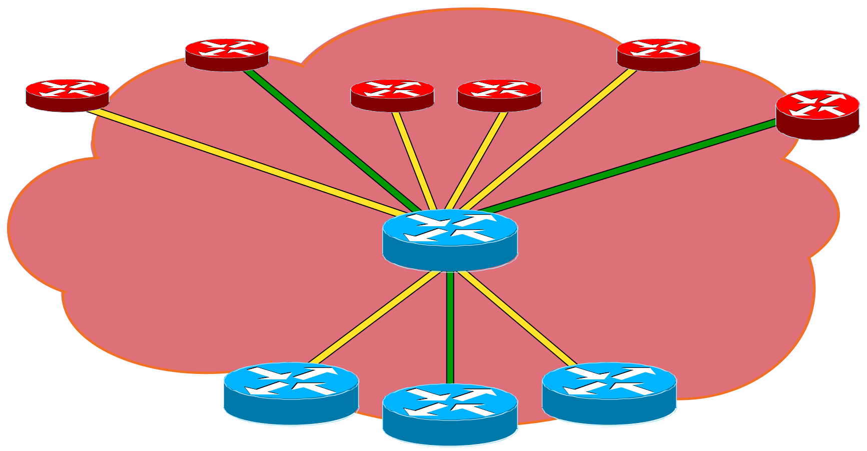
Hub and spoke (Phase 1)



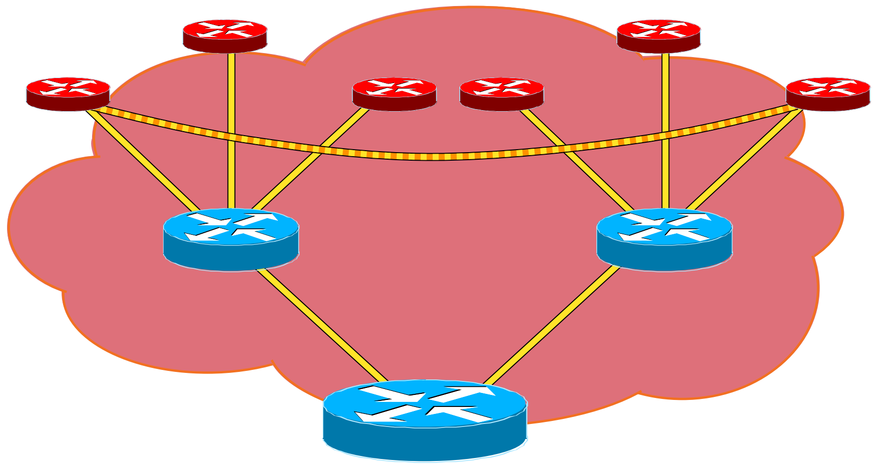
Spoke-to-spoke (Phase 2)



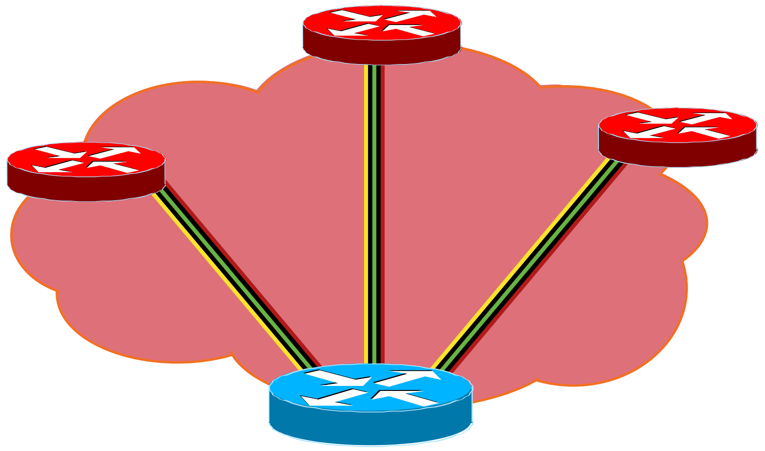
VRF-lite



Server Load Balancing



Hierarchical (Phase 3)



2547oDMVPN

Four Layer Troubleshooting Methodology

Before You Begin

- Sync up the timestamps between the hub and spoke
  - Preferably using NTP
- Enable msec debug and log timestamps
  - service timestamps debug date time msec
  - service timestamps log date time msec
- Enable “terminal exec prompt timestamp” for the debugging sessions.
  - Easily correlate the debug output with the show command output

Four Layer Troubleshooting Methodology

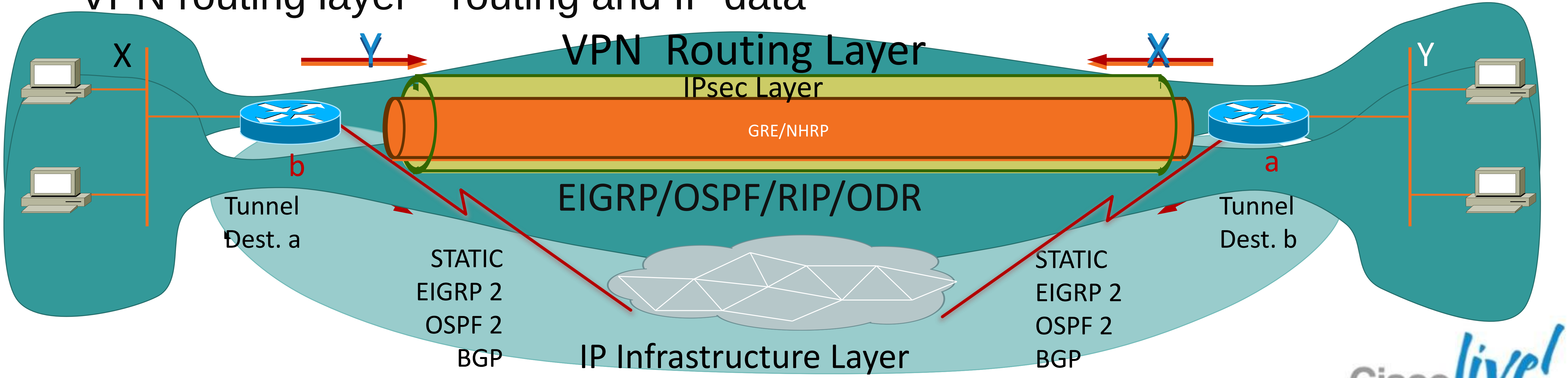
- **Four layers for troubleshooting**

  Physical and routing layer

  IPsec encryption layer—IPsec/ISAKMP

  GRE encapsulation layer—NHRP

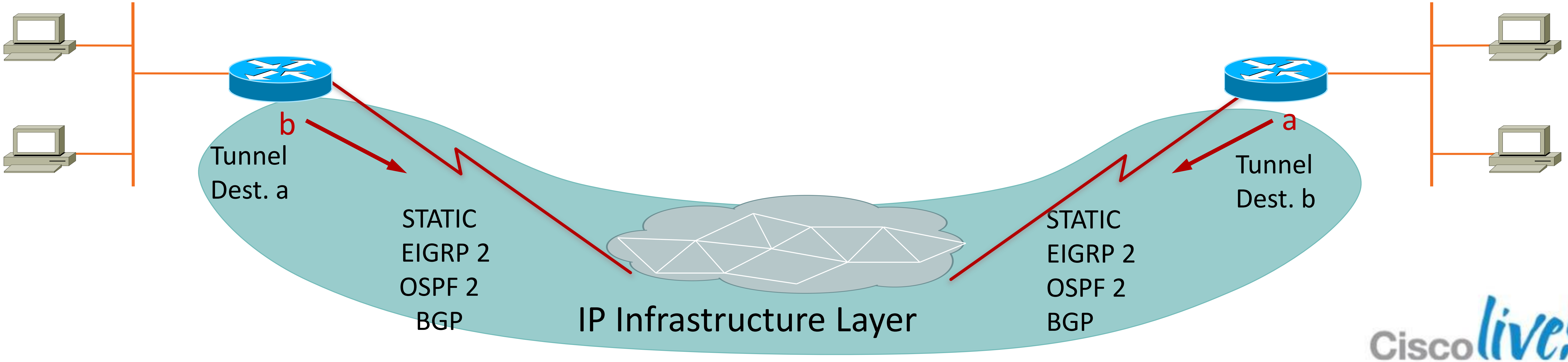
  VPN routing layer—routing and IP data



Four Layers for Troubleshooting: Physical and Routing Layer

- **Physical (NBMA or tunnel endpoint) routing layer**

  This gets the encrypted tunnel packets between the tunnel endpoints



Four Layers for Troubleshooting: Physical and Routing Layer

- Ping from the hub to the spoke's using NBMA addresses (and reverse):

  These pings should go directly out the physical interface, not through the DMVPN tunnel

  If pings are failing, check the routing and any firewalls between the hub and spoke routers

- Also use traceroute to check the path that the encrypted tunnel packets are taking
- Check for “administratively prohibited” (ACL) messages

Four Layers for Troubleshooting: Physical and Routing Layer (Cont)

- **Debugs and show commands to use for connectivity issues**

  debug ip icmp

  Valuable tool used to troubleshoot connectivity issues

  Helps you determine whether the router is sending or receiving ICMP messages

```
ICMP: rcvd type 3, code 1, from 172.17.0.1

ICMP: src 172.17.0.1, dst 172.16.1.1, echo reply

ICMP: dst (10.120.1.0) port unreachable rcv from 10.120.1.15

ICMP: src 172.17.0.5, dst 172.16.1.1, echo reply
```

Debug icmp field descriptions:

http://www.cisco.com/en/US/docs/ios/12_3/debug/command/referencedbg_i1g.html#wp1017595

Four Layers for Troubleshooting: Physical and Routing Layer (Cont.)

- **Debugs and show commands to troubleshoot connectivity issues**

debug ip packet [*access-list-number*] [detail] [dump]

Useful tool use for troubleshooting end to end communication

IP packet debugging captures the packets that are process switched including received, generated and forwarded packets.

```
IP: s=172.16.1.1 (local), d=172.17.0.1 (FastEthernet0/1), len 100, sending ICMP type=8, code=0
IP: table id=0, s=172.17.0.1 (FastEthernet0/1), d=172.16.1.1 (FastEthernet0/1), routed via RIB
IP: s=172.17.0.1 (FastEthernet0/1), d=172.16.1.1 (FastEthernet0/1), len 100, rcvd 3 ICMP
type=0, code=0
```

Caution: Debug IP packet command can generate a substantial amount of output and uses a substantial amount of system resources. This command should be used with caution in production networks. Always use with an ACL.

Four Layers for Troubleshooting: Physical and Routing Layer (Cont.)

Common Issues:

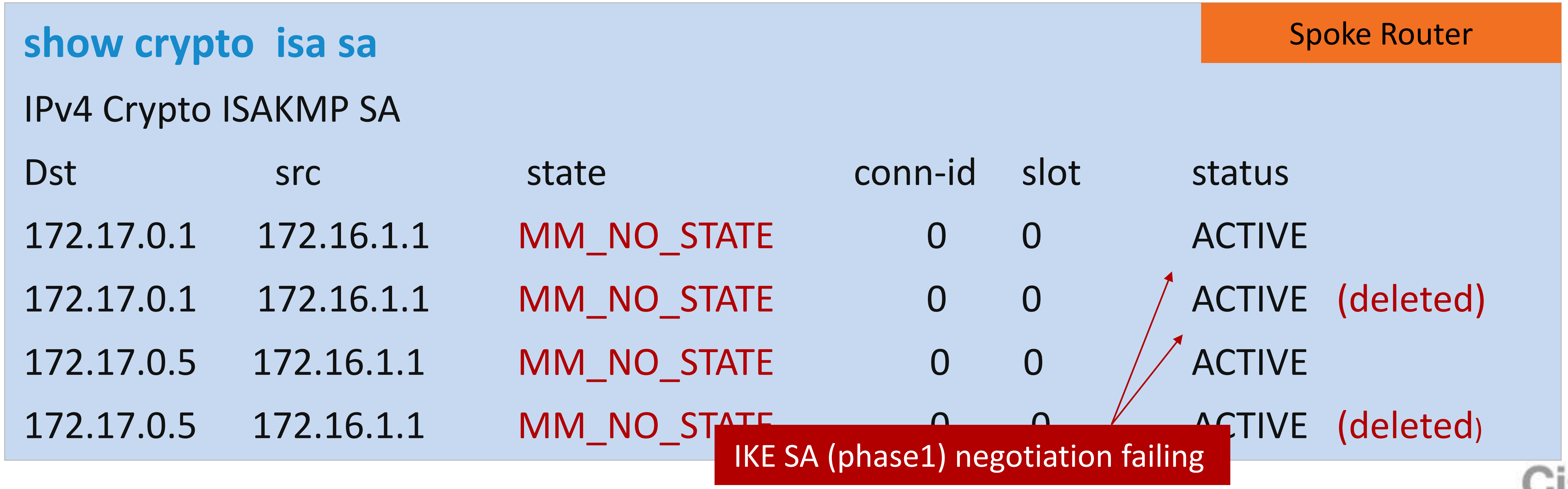
- ACL in firewall/ISP side blocking ISAKMP traffic
- Traffic filtering resulting traffic flows one direction

Common Issues:
Firewall or ISP Blocking IKE

Problem:

- IPsec tunnel is not coming up
- Network connectivity between hub and spoke is fine

How to detect?



Spoke Router

show crypto isa sa

```
IPv4 Crypto ISAKMP SA
Dst          src          state          conn-id   slot    status
172.17.0.1   172.16.1.1   MM_NO_STATE       0       0      ACTIVE
172.17.0.1   172.16.1.1   MM_NO_STATE       0       0      ACTIVE  (deleted)
172.17.0.5   172.16.1.1   MM_NO_STATE       0       0      ACTIVE
172.17.0.5   172.16.1.1   MM_NO_STATE       0       0      ACTIVE  (deleted)
```

IKE SA (phase1) negotiation failing

Common Issues:
Firewall or ISP Blocking IKE

- Run “debug crypto isakmp” to verify spoke router is sending udp 500 packet

Spoke Router

```
debug crypto isakmp
04:14:44.450: ISAKMP:(0):Old State = IKE_READY  New State = IKE_I_MM1
04:14:44.450: ISAKMP:(0): beginning Main Mode exchange
04:14:44.450: ISAKMP:(0): sending packet to 172.17.0.1 my_port 500 peer_port 500 (I) MM_NO_STATE
04:14:44.450: ISAKMP:(0):Sending an IKE IPv4 Packet.
04:14:54.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
04:14:54.450: ISAKMP (0:0): incrementing error counter on sa, attempt 1 of 5: retransmit phase 1
04:14:54.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
04:14:54.450: ISAKMP:(0): sending packet to 172.17.0.1 my_port 500 peer_port 500 (I) MM_NO_STATE
04:14:54.450: ISAKMP:(0):Sending an IKE IPv4 Packet.
04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
04:15:04.450: ISAKMP (0:0): incrementing error counter on sa, attempt 2 of 5: retransmit phase 1
04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
04:15:04.450: ISAKMP:(0): sending packet to 172.17.0.1 my_port 500 peer_port 500 (I) MM_NO_STATE
04:15:04.450: ISAKMP:(0):Sending an IKE IPv4 Packet.
```

Above debug output shows spoke router is sending udp 500 packet every 10 secs

Common Issues: IKE Traffic Blocked

- **How to fix?**

  Check and allow UDP port 500 in all intermediate devices and ISP

  After UDP port 500 is allowed in the inbound ACL on WAN(public) interface , verify that hit counts are incrementing on the ACL using “show access-list <acl>” command

Hub Router

```
show access-lists 101
Extended IP access list 101
    10 permit udp host 172.17.0.1 host 172.16.1.1 eq isakmp  (4 matches)
    20 permit udp host 172.17.0.5 host 172.16.1.1 eq isakmp  (4 matches)
    30 permit ip any any (295 matches)
```

Caution: Make sure you have IP any any allowed in your access-list otherwise all other traffic will be blocked by this acl applied inbound on egress interface.

Common Issues: IKE Traffic Blocked

- **How to verify it is working ?**

Spoke Router

```
show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst            src            state          conn-id  slot     status
172.17.0.1     172.16.1.1     QM_IDLE           1009    0      ACTIVE
172.17.0.5     172.16.1.1     QM_IDLE           1008    0      ACTIVE
```

```
debug crypto isakmp
ISAKMP:(0):Old State = IKE_READY  New State =IKE_I_MM1
ISAKMP:(0): beginning Main Mode exchange
ISAKMP:(0): sending packet to 172.17.0.1 my_port 500 peer_port 500 (I) MM_NO_STATE
ISAKMP (0:0): received packet from 172.17.0.1 dport 500 sport 500 Global (I) MM_NO_STATE
ISAKMP:(0):Sending an IKE IPv4 Packet Old State = IKE_R_MM1  New State = IKE_R_MM2
ISAKMP:(0):atts are acceptable
…
ISAKMP:(1009):Old State = IKE_R_MM3  New State IKE_R_MM3
…
ISAKMP:(1009):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE
```

Phase 1 is UP, UDP 500 packet received

Common Issues:
Traffic Filtering, Uni-directional Traffic

Problem

- Unable to pass data traffic
- VPN tunnel between spoke to spoke router is UP

How to detect?

```
spoke1# show crypto ipsec sa peer 172.16.2.11
  local  ident (addr/mask/prot/port):    (172.16.1.1/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
   #pkts encaps: 110, #pkts encrypt: 110,  #pkts decaps: 0, #pkts decrypt: 0,
  local crypto endpt.: 172.16.1.1,  remote crypto endpt.: 172.16.2.11
    inbound esp sas:  spi: 0x4C36F4AF(1278669999)
    outbound esp sas:  spi: 0x6AC801F4(1791492596)
```

```
spoke2#show crypto ipsec sa peer 172.16.1.1
  local  ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
  #pkts encaps: 116, #pkts encrypt: 116,  #pkts decaps: 110, #pkts decrypt: 110,
  local crypto endpt.: 172.16.2.11,  remote crypto endpt.: 172.16.1.1
   inbound esp sas: spi: 0x6AC801F4(1791492596)
   outbound esp sas: spi: 0x4C36F4AF(1278669999)
```

There is no decap packets in Spoke 1, which means ESP packets are likely getting dropped some where in the path from Spoke 2 towards Spoke1

Common Issues:
Traffic Filtering, Uni-directional Traffic

- **How to fix?**

  Spoke 2 router shows both encap and decap which means either firewall in spoke 2 end or ISP is blocking ESP. Check and allow the ESP traffic.

- **How to verify?**

```
spoke1# show crypto ipsec sa peer 172.16.2.11
  local  ident (addr/mask/prot/port):   (172.16.1.1/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
   #pkts encaps: 300, #pkts encrypt: 300
   #pkts decaps: 200, #pkts decrypt: 200,
```

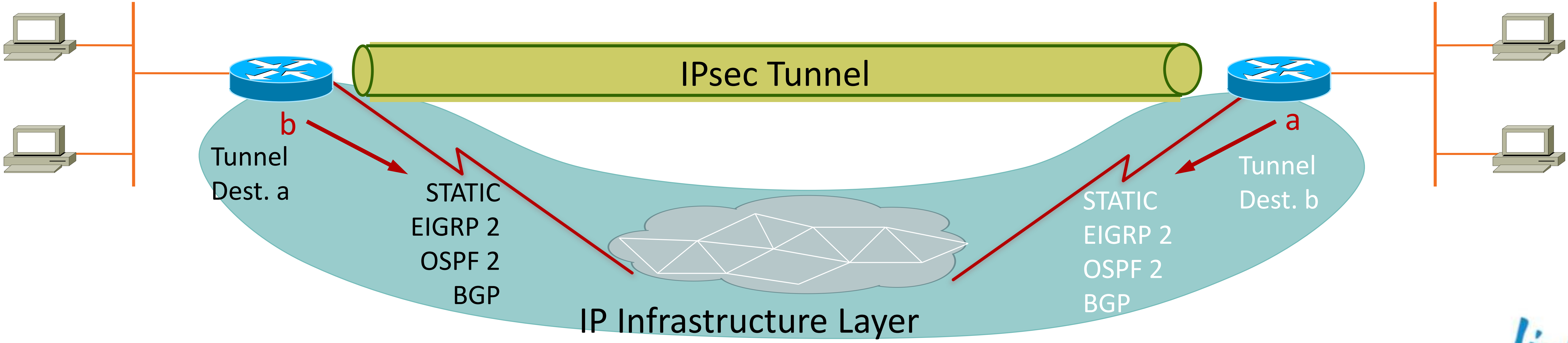
```
spoke2#sh cry ipsec sa peer 172.16.1.1
  local  ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
  #pkts encaps: 316, #pkts encrypt: 316,
  #pkts decaps: 300, #pkts decrypt: 310,
```

After ESP (IP protocol 50) is allowed, Spoke 1 and 2 encaps and decaps are incrementing

Four Layers for Troubleshooting: IPsec Encryption Layer

- **The IPsec encryption layer—**

  This layer encrypts the GRE tunnel packet going out and decrypts the IPsec packet coming in to reveal the GRE encapsulated packet



Four Layers for Troubleshooting: IPsec Encryption Layer—IPsec Component

DMVPN Component-Ipsec

- DMVPN introduced tunnel protection
- The profile must be applied on the tunnel interface

```
tunnel protection ipsec profile prof
```

- Internally Cisco IOS Software will treat this as a dynamic crypto map and it derives the local-address, set peer and match address parameters from the tunnel parameters and the NHRP cache
- This must be configured on the hub and spoke tunnels

Four Layers for Troubleshooting: IPsec Encryption Layer—IPsec Component

DMVPN Component-IPsec (Cont.)

- A transform set must be defined:

```
crypto ipsec transform-set ts esp-3des esp-sha-hmac
  mode transport
```

- An IPsec profile replaces the crypto map

```
crypto ipsec profile prof
  set transform-set ts
```

- The IPsec profile is like a crypto map without “set peer” and “match address”

```
Interface Tunnel0
 Ip address 10.0.0.1 255.255.255.0
 :
 tunnel source fast ethernet0/0

 tunnel protection ipsec profile prof
```

Note: GRE Tunnel Keepalives are not supported in combination with Tunnel Protection

Four Layers for Troubleshooting: IPsec Encryption Layer

IPsec Layer Verification-show commands

- Verify that ISAKMP SAs and IPsec SAs between the NBMA addresses of the hub and spoke have been created

  ```
  show crypto isakmp sa detail
  show crypto IPsec sa peer <NBMA-address-of-peer>
  ```

- Notice SA lifetime values

  If they are close to the configured lifetimes (default --24 hrs for ISAKMP and 1 hour for IPsec) then that means these SAs have been recently negotiated

  If you look a little while later and they have been re-negotiated again, then the ISAKMP and/or IPsec may be bouncing up and down

Four Layers for Troubleshooting: IPsec Encryption Layer

IPsec Layer Verification-show commands (Cont.)

- New show commands for DMVPN introduced in 12.4(9)T that has brief and detail output

show dmvpn detail

Covers both IPsec phase 1 and phase 2 status

```
Show dmvpn [ {interface <i/f>} |
             {vrf <vrf-name>} |
             {peer  {{nbma | tunnel } <ip-addr> } |
                  {network <ip-addr> <mask>}} ]
             [detail]
```

Note: Prior to 15.x version , it does not show remaining life time for both IPsec phase 1 and phase 2. Use legacy commands for lifetime.

Four Layers for Troubleshooting: IPsec Encryption Layer

IPsec Layer Verification-debug commands

- Check the debug output on both the spoke and the hub at the same time

```
debug crypto isakmp
debug crypto ipsec
debug crypto engine
```

New command

```
debug dmvpn detail crypto
```

Introduced in 12.4(9)T

- Use conditional debugging on the hub router to restrict the crypto debugs to only show debugs for the particular spoke in question:

```
debug crypto condition peer ipv4 <nbma address>
debug dmvpn condition peer <nbma|tunnel>
```

- Verify the communication between NHRP and IPsec by showing the crypto map and socket tables

```
show crypto map
show crypto socket
```

Four Layers for Troubleshooting: IPsec Encryption Layer—Show Commands

show crypto isakmp sa

```
Router# show crypto isakmp sa
dst              src           state               connid   slot
172.17.0.1   172.16.1.1     QM_IDLE                   1        0
```

IKE Phase 1 status UP

show crypto isakmp sa detail

```
Router# show crypto isakmp sa detail
Codes: C - IKE configuration mode,
       D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
        psk - Preshared key, rsig - RSA signature, renc - RSA encryption

C-id  Local          Remote         I-VRF Encr Hash Auth DH Lifetime Cap.
1     172.16.1.1     172.17.0.1           3des sha  psk  1  23:59:40
       Connection-id:Engine-id =  1:1(hardware)
```

Encryption:3des
Authentication :Pre-shared key
Remaining lifetime before phase 1 re-key

Four Layers for Troubleshooting: IPsec Encryption Layer—Show Commands

show crypto ipsec sa

```
Router# show crypto ipsec sa
interface: Ethernet0/3
   Crypto map tag: vpn, local addr. 172.17.0.1
  local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
  current_peer: 172.17.0.1:500
    PERMIT, flags={origin_is_acl,}
  #pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19
  #pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compr'ed: 0, #pkts compr. failed: 0, #pkts decompr. failed: 0
  #send errors 1, #recv errors 0
   local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.17.0.1
   path mtu 1500, media mtu 1500
   current outbound spi: 8E1CB77A
```

Four Layers for Troubleshooting: IPsec Encryption Layer—Show Commands

show crypto ipsec sa (cont.)

```
 inbound esp sas:
      spi: 0x4579753B(1165587771)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4456885/3531)
        IV size: 8 bytes
        replay detection support: Y
outbound esp sas:
      spi: 0x8E1CB77A(2384246650)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4456885/3531)
        IV size: 8 bytes
        replay detection support: Y
```

Remaining life time before re-key

Four Layers for Troubleshooting: IPsec Encryption Layer—Show Commands

show dmvpn

```
HUB-1# 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

Tunnel1, Type:Hub, NHRP Peers:2,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1         1.1.1.1      172.20.1.1    UP 00:04:32 D
     1         2.2.2.2      172.20.1.2    UP 00:01:25 D

SPOKE-1#show dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incompletea
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer

Tunnel1, Type:Spoke, NHRP Peers:1,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1         3.3.3.3    172.20.1.100    UP 00:21:56 S
```

Dynamic entry can be built either in hub or in spoke(spoke to spoke tunnels)

Static NHRP mapping

Four Layers for Troubleshooting: IPsec Encryption Layer—Show Commands

show dmvpn detail

```
R600_spokeB#show dmvpn detail
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, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
 ==================
Interface Tunnel0 is up/up, Addr. is 10.10.10.6, VRF ""
Tunnel Src./Dest. addr: 172.16.2.1/MGRE, Tunnel VRF ""
Protocol/Transport: "multi-GRE/IP", Protect "dmvpn-ikev2”

IPv4 NHS:
10.10.10.2  RE priority = 0 cluster = 0
Type:Spoke, Total NBMA Peers (v4/v6): 3
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Networ
k----- --------------- -------------- ----- -------- ----- -----------------
1      172.17.0.9     10.10.10.2    UP 18:15:07    S      10.10.10.2/32
2     172.16.7.2     10.10.10.7    UP 00:02:36    D      10.10.10.7/32
0     172.16.7.2     10.10.10.7    UP 00:02:36  DT1    192.168.19.0/24
1      172.16.2.1     10.10.10.6    UP 00:02:36  DLX    192.168.18.0/24
```

Learnt Dynamically,
DLX:Dynamic Local no socket
DT1: Dynamic tunnel for spoke to spoke

Four Layers for Troubleshooting: IPsec Encryption Layer - Show Commands - contd

show dmvpn detail

```
R600_spokeB#show dmvpn detail
Crypto Session Details:
 --------------------------------------------------------------------------------
Interface: Tunnel0
Session: [0x0916D430]
 IKEv2 SA: local 172.16.2.1/500 remote 172.17.0.9/500 Active
           Capabilities:(none) connid:1 lifetime:05:44:52
 Crypto Session Status: UP-ACTIVE
 fvrf: (none),Phase1_id: 172.17.0.9
 IPSEC FLOW: permit 47 host 172.16.2.1 host 172.17.0.9
           Active SAs: 2, origin: crypto map
           Inbound:  #pkts dec'ed 14818 drop 0 life (KB/Sec) 4200810/3377
           Outbound: #pkts enc'ed 28979 drop 0 life (KB/Sec) 4200805/3377
           Outbound SPI : 0x25C41C2C, transform : esp-3des esp-sha-hmac
            Socket State: Open
Interface: Tunnel0
Session: [0x0916D330]
IKEv1 SA: local 172.16.2.1/500 remote 172.16.7.2/500 Active
            Capabilities:(none) connid:1039 lifetime:23:57:22
Crypto Session Status: UP-ACTIVE
 fvrf: (none),Phase1_id: 172.16.7.2
IPSEC FLOW: permit 47 host 172.16.2.1 host 172.16.7.2
            0 life (KB/Sec) 4305525/3443
            Outbound: #pkts enc'ed 41 drop 0 life (KB/Sec) 4305525/3443
Outbound SPI : 0x57A1D6F6, transform : esp-3des esp-sha-hmac
 Socket State: Open
```

IKEv2 Session
Crypto session status
Socket state

IKEv1 Session
Crypto session status
Socket state

Four Layers for Troubleshooting: IPsec Encryption Layer - debug crypto Condition

- To enable crypto conditional debugging:

```
debug crypto condition <cond-type> <cond-value>
debug crypto { isakmp | ipsec | engine }
```

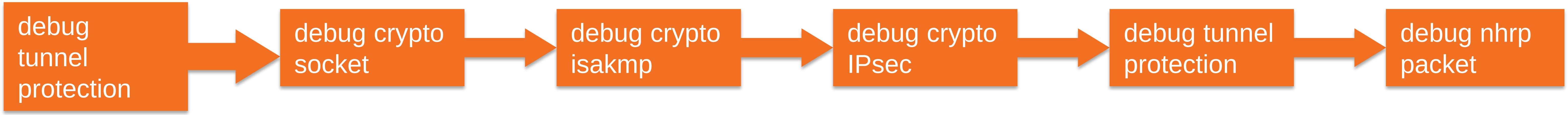
- To view crypto condition debugs that have been enabled:

```
show crypto debug-condition [ all | peer | fvrf | ivrf |
isakmp | username | connid | spi ]
```

- To disable crypto condition debugs:

```
debug crypto condition reset
```

Four Layers for Troubleshooting: IPsec Encryption Layer—debug dmvpn detail all

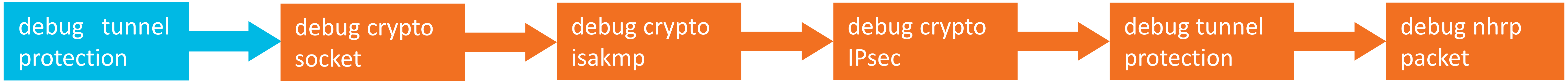


- debug dmvpn introduced in 12.4(9)T

```
debug dmvpn {[{condition [unmatched] |
      [peer [nbma | tunnel {ip-address}]] |
      [vrf {vrf-name}] |
      [interface {tunnel number}]}] |
      [{error | detail | packet | all}
       {nhrp | crypto | tunnel | socket | all}]}
```

- One complete debug to help troubleshoot dmvpn issues

Four Layers for Troubleshooting: IPsec Encryption Layer—debug dmvpn detail all (Cont.)

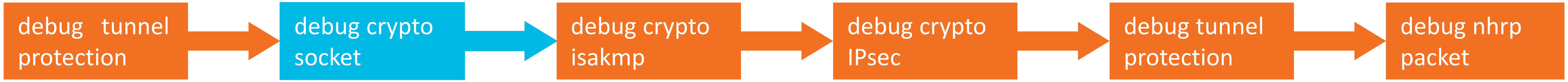


debug tunnel protection → debug crypto socket → debug crypto isakmp → debug crypto IPsec → debug tunnel protection → debug nhrp packet

Tunnel protection configured on tunnel interface open crypto socket as soon as either router or tunnel interface come up

```
IPSEC-IFC MGRE/Tu0: Checking tunnel status

IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): Opening a socket with profile dmvpn

IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): connection lookup returned 0

IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): Triggering tunnel immediately.

IPSEC-IFC MGRE/Tu0: tunnel coming up

IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): Opening a socket with profile dmvpn

IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): connection lookup returned 83884274

IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): Socket is already being opened. Ignoring.
```

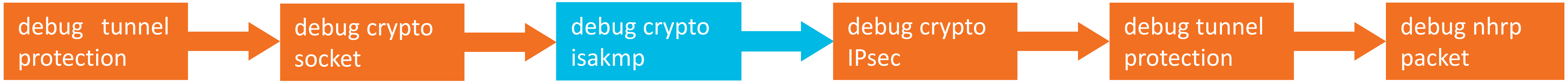
Four Layers for Troubleshooting: IPsec Encryption Layer—debug dmvpn detail all (Cont.)



- Shows socket state
- Crypto socket debug shows creation of local and remote proxy id

```
CRYPTO_SS (TUNNEL SEC): Application started listening

insert of map into mapdb AVL failed, map + ace pair already exists on the mapdb

CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

CRYPTO_SS(TUNNEL SEC): Active open, socket info:
          local 172.16.2.11 172.16.2.11/255.255.255.255/0,
          remote  172.17.0.1 172.17.0.1/255.255.255.255/0,  prot 47, ifc Tu0
```

Four Layers for Troubleshooting: IPsec Encryption Layer—debug dmvpn detail all (Cont.)



debug tunnel protection → debug crypto socket → debug crypto isakmp → debug crypto IPsec → debug tunnel protection → debug nhrp packet

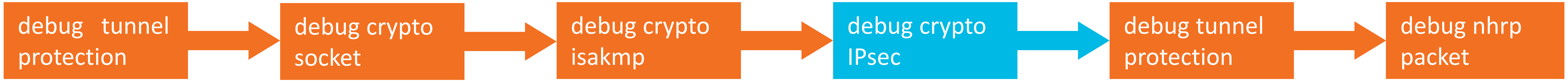
- IKE negotiation
- Shows six packet exchange(MM1-MM6) in main mode

```
ISAKMP:(0):Old State = IKE_READY  New State = IKE_I_MM1
ISAKMP:(0): beginning Main Mode exchange
ISAKMP:(0): sending packet to 172.17.0.1 my_port 500 peer_port 500 (I) MM_NO_STATE
ISAKMP:(0):Sending an IKE IPv4 Packet
ISAKMP:(0):Old State = IKE_I_MM1  New State = IKE_I_MM2
ISAKMP:(0):Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:(0):atts are acceptable. Next payload is 0
ISAKMP:(0):Old State = IKE_I_MM2  New State = IKE_I_MM3
ISAKMP:(0):Old State = IKE_I_MM3  New State = IKE_I_MM4
ISAKMP:(1051):Old State = IKE_I_MM4  New State = IKE_I_MM5
ISAKMP:(1051):Old State = IKE_I_MM5  New State = IKE_I_MM6
ISAKMP:(1051):Old State = IKE_I_MM6  New State = IKE_P1_COMPLETE
```

IKE has found matching policy

IKE complete authentication

Four Layers for Troubleshooting: IPsec Encryption Layer—debug dmvpn detail all (Cont.)



- IKE negotiates to set up the IP Security (IPsec) SA by searching for a matching transform set
- Creation of inbound and outbound security association database (SADB)

```
ISAKMP:(1051):beginning Quick Mode exchange, M-ID of 1538742728
ISAKMP:(1051):Old State = IKE_QM_READY  New State = IKE_QM_I_QM1
ISAKMP:(1051):atts are acceptable.
INBOUND local= 172.16.2.11, remote= 172.17.0.5,
local_proxy= 172.16.2.11/255.255.255.255/47/0 (type=1),
remote_proxy= 172.17.0.5/255.255.255.255/47/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac  (Transport),
ISAKMP:(1051): Creating IPsec SAs
inbound SA from 172.17.0.5 to 172.16.2.11 (f/i)  0/ 0
 (proxy 172.17.0.5 to 172.16.2.11)
has spi 0xE563BB42 and conn_id 0
outbound SA from 172.16.2.11 to 172.17.0.5 (f/i) 0/0
(proxy 172.16.2.11 to 172.17.0.5)
has spi  0xFE745CBD and conn_id 0
ISAKMP:(1051):Old State = IKE_QM_I_QM1  New State = IKE_QM_PHASE2_COMPLETE
```

Phase 2 Complete

Four Layers for Troubleshooting: IPsec Encryption Layer

Common Issues:

- Incompatible ISAKMP Policy
- DMVPN Hub and EzVPN server on same Router.
- Incompatible IPsec transform set

Common Issues: Incompatible ISAKMP Policy

- If the configured ISAKMP policies don’t match the proposed policy by the remote peer, the router tries the default policy of 65535, and if that does not match either, it fails ISAKMP negotiation

```
Default protection suite
encryption algorithm:   DES—Data Encryption Standard (56 bit keys).
hash algorithm:         Secure Hash Standard
authentication method:  Rivest-Shamir-Adleman Signature
Diffie-Hellman group:   #1 (768 bit)
lifetime:               86400 seconds, no volume limit
```

- show crypto isakmp sa command output shows the IKE SA to be in MM_NO_STATE status, indicative of main mode negotiation failure

Common Issues: Incompatible ISAKMP Policy (Cont.)

Message 1 of IPsec main mode

```
ISAKMP (0:1): processing SA payload. message ID
= 0

ISAKMP (0:1): found peer pre-shared key
matching 209.165.200.227

ISAKMP (0:1): Checking ISAKMP transform 1
against priority 1 policy

ISAKMP:       encryption 3DES-CBC

ISAKMP:       hash MD5

ISAKMP:       default group 1

ISAKMP:       auth pre-share

ISAKMP:       life type in seconds

ISAKMP:       life duration (VPI) of  0x0 0x1
0x51 0x80

ISAKMP (0:1): Hash algorithm offered does not
match policy!

ISAKMP (0:1): atts are not acceptable. Next
payload is 0
```

```
ISAKMP (0:1): Checking ISAKMP transform 1
against priority 65535 policy

ISAKMP:       encryption 3DES-CBC

ISAKMP:       hash MD5

ISAKMP:       default group 1

ISAKMP:       auth pre-share

ISAKMP:       life type in seconds

ISAKMP:       life duration (VPI) of  0x0 0x1
0x51 0x80

ISAKMP (0:1): Encryption algorithm offered does
not match policy!

ISAKMP (0:1): atts are not acceptable. Next
payload is 0

ISAKMP (0:1): no offers accepted!

ISAKMP (0:1): phase 1 SA not acceptable!
```

Common Issues:

DMVPN Hub and EzVPN server on same Router

Problem Description:

DMVPN hub and EzVPN server configured in same router which result DMVPN spokes unable to connect only. EzVPN hardware and software clients are connecting.

How to Detect?

- Check isakmp status

Trying XAuth

```
show cry isakmp sa
IPv4 Crypto ISAKMP SA
dst            src            state          conn-id   slot  status
172.17.0.1     172.18.1.1     CONF_XAUTH       4119     0    ACTIVE
172.17.0.1     172.18.1.1     MM_NO_STATE      4118     0    ACTIVE (deleted)
```

Common Issues:
DMVPN Hub and EzVPN server on same Router

- Run isakmp debug to verify problem

DMVPN Hub

```
ISAKMP:(4119):returning IP addr to the address pool
ISAKMP:(4119):Old State = IKE_R_MM5  New State = IKE_R_MM5
ISAKMP: set new node 616549739 to CONF_XAUTH
ISAKMP:(4119):Need XAUTH
ISAKMP: set new node -701088864 to CONF_XAUTH
ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2
ISAKMP:(4119): initiating peer config to 172.18.1.1. ID = -701088864
ISAKMP:(4119): sending packet to 172.18.1.1 my_port 4500 peer_port 1024 (R) CONF_XAUTH
ISAKMP:(4119):Sending an IKE IPv4 Packet.
ISAKMP:(4119):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP:(4119):Old State = IKE_P1_COMPLETE  New State = IKE_XAUTH_REQ_SENT
```

DMVPN spoke inbound connection has Xauth and fails

- By default when crypto map is used for EzVPN, Xauth is enabled globally and thus enabled for all ipsec sessions including DMVPN.

Common Issues:

DMVPN Hub and EzVPN server on same Router

- Check existing configuration that prevents DMVPN spoke to complete IKE negotiation as Xauth is enabled globally

```
crypto isakmp client configuration group vpnclient
 key cisco123
 pool vpn
 acl 190
crypto ipsec transform-set t3 esp-3des esp-md5-hmac
crypto dynamic-map test 10
 set transform-set t3

crypto map test isakmp authorization list groupauthor
crypto map test client configuration address respond
crypto map test 100 IPSec-isakmp dynamic test

interface FastEthernet0/0
 ip address 172.17.0.1 255.255.255.252
 crypto map test
```

EzVPN Server Configuration

Common Issues:
DMVPN Hub and EzVPN server on same Router

```
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0

crypto ipsec transform-set t2 esp-3des esp-md5-hmac
  mode transport

crypto ipsec profile vpnprof
  set transform-set t2

interface Tunnel0
  ip address 10.0.0.8 255.255.255.0
  .
  .
  tunnel protection ipsec profile vpnprof
```

DMVPN Hub Configuration

Common Issues:
DMVPN Hub and EzVPN server on same Router

How to Fix ?

- Disable Xauth globally by Separating EzVPN server and DMVPN configuration by using ISAKMP Profile.
- Match EzVPN software/hardware clients in Group name and DMVPN spokes in match identity address in Isakmp profile.

```
crypto keyring dmvpn
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
crypto isakmp profile dmvpn
      keyring dmvpn
       match identity address 0.0.0.0
crypto ipsec profile vpnprof
     set transform-set t2
     set isakmp-profile dmvpn
```

Corrected Configuration
On DMVPN Hub

Common Issues:
DMVPN Hub and EzVPN server on same Router

```
crypto isakmp client configuration group vpnclient
  key cisco123
  pool vpn
  acl 190

crypto isakmp profile remotevpn
  match identity group vpnclient

crypto dynamic-map test 10
  set transform-set t3
  set isakmp-profile remotevpn

crypto map test isakmp authorization list groupauthor
crypto map test client configuration address respond
crypto map test 100 ipsec-isakmp dynamic test
```

Corrected configuration of EzVPN server

Common Issues:
DMVPN Hub and EzVPN server on same Router

How to Verify ?

```
ISAKMP:(0):found peer pre-shared key matching 172.18.1.1
ISAKMP:(0): local preshared key found
ISAKMP:(0):Checking ISAKMP transform 1 against priority 2 policy
ISAKMP:(0):atts are acceptable. Next payload is 0
ISAKMP:(0):Old State = IKE_R_MM1  New State = IKE_R_MM1
ISAKMP:(0):Old State = IKE_R_MM1  New State = IKE_R_MM2
ISAKMP:(0):Old State = IKE_R_MM2  New State = IKE_R_MM3
ISAKMP:(4157):Old State = IKE_R_MM3  New State = IKE_R_MM4
ISAKMP:(4157):Old State = IKE_R_MM4  New State = IKE_R_MM5
ISAKMP (0:4157): ID payload
        next-payload : 8
        type         : 1
        address      : 10.1.1.1
        protocol     : 17
        port         : 0
        length       : 12
ISAKMP:(4157):Found ADDRESS key in keyring dmvpn
ISAKMP:(4157):Old State = IKE_R_MM5  New State = IKE_R_MM5
```

Keyring scan in debugs

Common Issues:
DMVPN Hub and EzVPN server on same Router

```
ISAKMP:(4157):Old State = IKE_R_MM5  New State = IKE_P1_COMPLETE
ISAKMP:(4157):SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP (0:4157): ID payload
        next-payload : 8
        type         : 1
        address      : 172.17.0.1
        protocol     : 17
        port         : 0
        length       : 12
ISAKMP:(4157):Old State = IKE_R_MM5  New State = IKE_P1_COMPLETE
ISAKMP:(4157):Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP:(4157):atts are acceptable.
ISAKMP:(4157): Creating IPSec SA
         inbound SA from 172.18.1.1 to 172.17.0.1 (f/i)  0/ 0
        (proxy 172.18.1.1 to 172.17.0.1)
         has spi 0x936AA23D and conn_id 0
       outbound SA from 172.17.0.1 to 172.18.1.1 (f/i) 0/0
        (proxy 172.17.0.1 to 172.18.1.1)
        has spi  0xD37F43CB and conn_id 0
ISAKMP:(4157):Old State = IKE_QM_R_QM2  New State = IKE_QM_PHASE2_COMPLETE
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.0.0.11 (Tunnel0) is up: new adjacency
```

VPN Tunnel established

Common Issues:
DMVPN Hub and EzVPN server on same Router

```
show crypto  isakmp sa
IPv4 Crypto ISAKMP SA
dst            src                  state       conn-id        slot      status
172.17.0.1     172.19.87.148        QM_IDLE       4158          0       ACTIVE remotevpn
172.17.0.1     172.16.1.1           QM_IDLE       4152          0       ACTIVE dmvpn
172.17.0.1     172.18.1.1           QM_IDLE       4157          0       ACTIVE dmvpn
172.17.0.6     172.17.0.1           QM_IDLE       4156          0       ACTIVE dmvpn
```

EzVPN profile

DMVPN Profile

```
show crypto  ipsec sa peer 172.18.1.1
   local  ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.18.1.1/255.255.255.255/47/0)
   current_peer 172.18.1.1 port 1024
   #pkts encaps: 18, #pkts encrypt: 18, #pkts digest: 18
    #pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
  current outbound spi: 0xD37F43CB(3548333003)
  inbound esp sas:
 spi: 0x936AA23D(2473239101)
 outbound esp sas:
  spi: 0xD37F43CB(3548333003)
```

Common Issues: Incompatible IPsec Transform Set

- If the ipsec transform-set is not compatible or mismatched on the two IPsec devices, the IPsec negotiation will fail, with the router complaining about "atts not acceptable" for the IPsec proposal

Phase II Parameters

```
IPsec mode (tunnel or transport)
Encryption algorithm
Authentication algorithm
PFS group
IPsec SA Lifetime
Proxy identities
```

```
ISAKMP (0:2): Checking IPsec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (basic) of 3600
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 0) not supported
ISAKMP (0:2): atts not acceptable. Next payload is 0
ISAKMP (0:2): SA not acceptable!
```

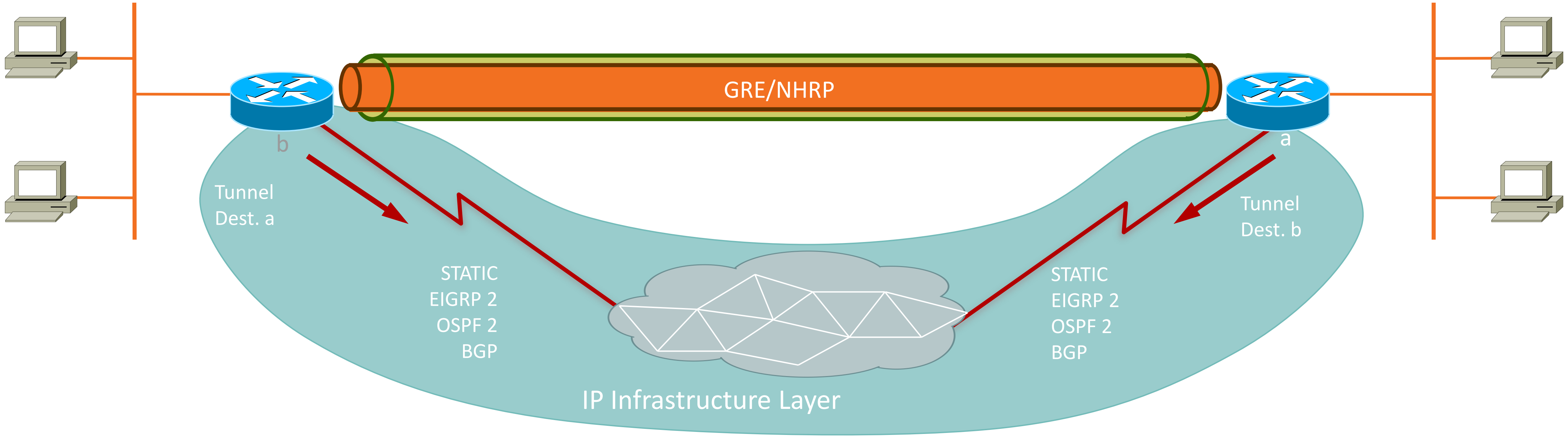
Four Layers for Troubleshooting: GRE Encapsulation Layer

- **The GRE Encapsulation layer**

  This is GRE encapsulation of the data IP packet going out or GRE de-capsulation of the GRE packet (after IPsec decryption) to switch the data packet

- NHRP is also transported over the GRE layer along with data packets

.



Four Layers for Troubleshooting: GRE Encapsulation Layer

DMVPN Component-GRE/NHRP

- Multipoint GRE Tunnel Interface

  Single GRE interface to support multiple GRE/IPsec tunnels

  Simplifies size and complexity of configuration

- Next Hop Resolution Protocol (NHRP)

  Creates a distributed (NHRP) mapping database of all the spoke’s tunnel to real (public interface) addresses

Four Layers for Troubleshooting: GRE Encapsulation Layer

DMVPN Component-mGRE

- A p-pGRE interface definition includes
  - An IP address
  - A tunnel source
  - A tunnel destination
  - An optional tunnel key

```
interface Tunnel
   ip address 10.0.0.1 255.0.0.0
   tunnel source Dialer1
   tunnel destination 172.16.0.2
   tunnel key 1
```

- An mGRE interface definition includes
  - An IP address
  - A tunnel source
  - An option tunnel key

```
interface Tunnel
   ip address 10.0.0.1 255.0.0.0
   tunnel source Dialer1
   tunnel mode gre multipoint
   tunnel key 1
```

Four Layers for Troubleshooting: GRE Encapsulation Layer

DMVPN Component-mGRE (Cont.)

- Single tunnel interface (multipoint)
  - Non-Broadcast Multi-Access (NBMA) Network
  - Smaller hub configuration
  - Multicast/broadcast support
- Dynamic tunnel destination
  - Next Hop Resolution Protocol (NHRP)
  - VPN IP to NBMA IP address mapping
  - Short-cut forwarding
  - Direct support for dynamic addresses and NAT

Four Layers for Troubleshooting: GRE Encapsulation Layer—What Is NHRP

DMVPN Component-NHRP

- NHRP is a layer two resolution protocol and cache like ARP or Reverse ARP (Frame Relay)
- It is used in DMVPN to map a tunnel IP address to an NBMA IP address
- Like ARP, NHRP can have static and dynamic entries
- NHRP has worked fully dynamically since Release 12.2(13)T

Four Layers for Troubleshooting: GRE
Encapsulation Layer—Basic NHRP Configuration

DMVPN Component-NHRP (Cont.)

- In order to configure an mGRE interface to use NHRP, the following command is necessary:

```
ip nhrp network-id <id>
```

- Where <id> is a unique number (recommend same on hub and all spokes)
- <id> has nothing to do with tunnel key
- The network ID defines an NHRP domain
- Several domains can co-exist on the same router
- Without having this command, tunnel interface won’t come UP

Four Layers for Troubleshooting: GRE Encapsulation Layer—Adding NHRP Cache

DMVPN Component-NHRP (Cont.)

- Three ways to populate the NHRP cache for mapping:
  - Manually add static entries
  - Hub learns via registration requests
  - Spokes learn via resolution requests
- “Resolution” is for spoke to spoke

Four Layers for Troubleshooting: GRE Encapsulation Layer—Initial NHRP Caches

DMVPN Component-NHRP (Cont.)

- Initially, the hub has an empty cache
- The spoke has one static entry mapping the hub's tunnel address to the hub's NBMA address:

```
ip nhrp map 10.0.0.1 172.17.0.1
```

- Multicast traffic must be sent to the hub

```
ip nhrp map multicast 172.17.0.1
```

Four Layers for Troubleshooting: GRE Encapsulation Layer—Spoke Must Register with Hub

DMVPN Component-NHRP (Cont.)

- In order for the spokes to register themselves to the hub, the hub must be declared as a Next Hop Server (NHS):

```
ip nhrp nhs 10.0.0.1
ip nhrp holdtime 300 (recommended; default =7200)
ip nhrp registration no-unique (recommended*)
```

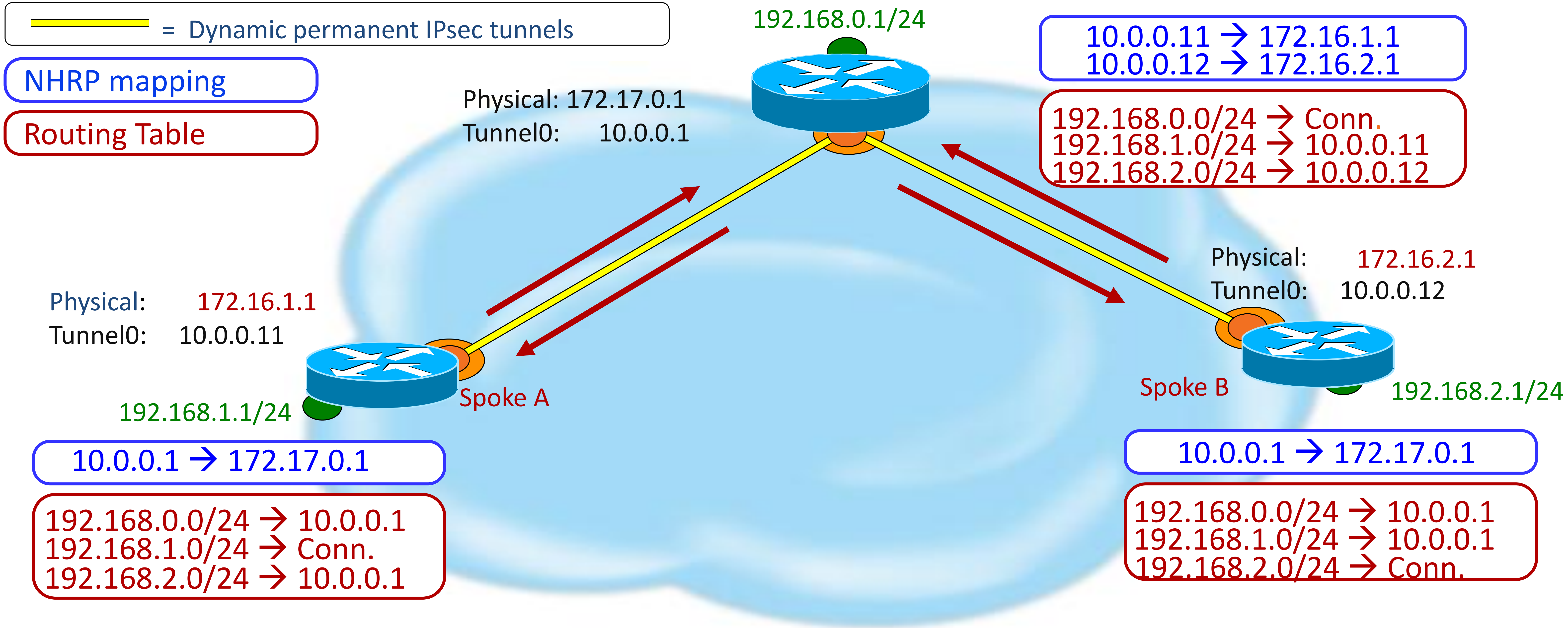
- Spokes control the cache on the hub

Four Layers for Troubleshooting:
GRE Encapsulation Layer—NHRP Registration

DMVPN Component-NHRP (Cont.)

- NHRP Registration
  - Spoke dynamically registers its mapping with NHS
  - Supports spokes with dynamic NBMA addresses or NAT
- NHRP Resolutions and Redirects
  - Supports building dynamic spoke-spoke tunnels
  - Control and Multicast traffic still via hub
  - Unicast data traffic direct, reduced load on hub routers

NHRP Registration Example
Dynamically Addressed Spokes



▬ = Dynamic permanent IPsec tunnels

NHRP mapping

Routing Table

Hub:

192.168.0.1/24

Physical: 172.17.0.1
Tunnel0: 10.0.0.1

10.0.0.11 → 172.16.1.1
10.0.0.12 → 172.16.2.1

192.168.0.0/24 → Conn.
192.168.1.0/24 → 10.0.0.11
192.168.2.0/24 → 10.0.0.12

Spoke A

Physical: 172.16.1.1
Tunnel0: 10.0.0.11

192.168.1.1/24

10.0.0.1 → 172.17.0.1

192.168.0.0/24 → 10.0.0.1
192.168.1.0/24 → Conn.
192.168.2.0/24 → 10.0.0.1

Spoke B

Physical: 172.16.2.1
Tunnel0: 10.0.0.12

192.168.2.1/24

10.0.0.1 → 172.17.0.1

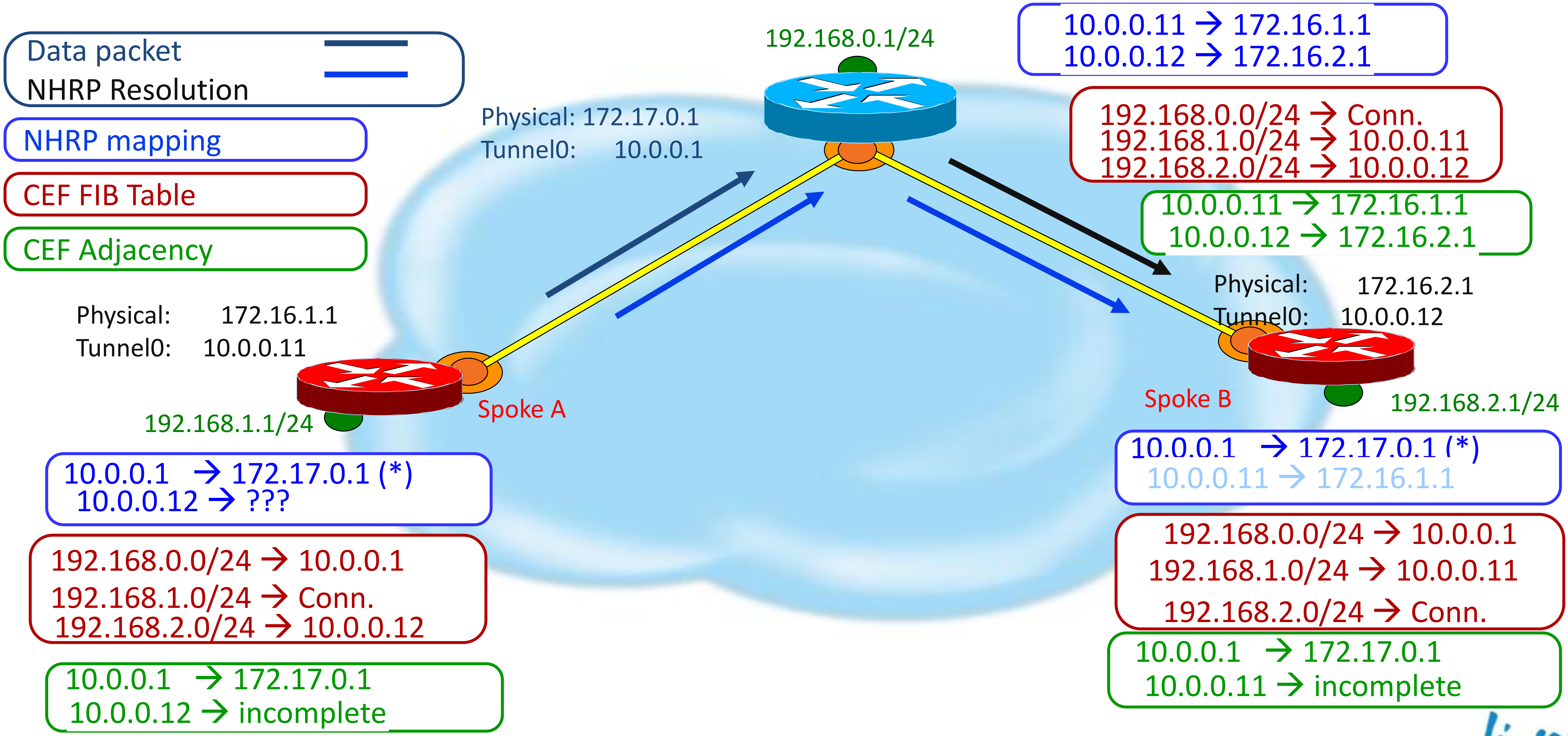
192.168.0.0/24 → 10.0.0.1
192.168.1.0/24 → 10.0.0.1
192.168.2.0/24 → Conn.

Four Layers for Troubleshooting: GRE Encapsulation Layer—NHRP Registration (Cont.)

DMVPN Component-NHRP (Cont.)

- Builds base hub-and-spoke network
  - Hub-and-spoke data traffic
  - Control traffic; NHRP, Routing protocol, IP multicast
- Next Hop Client (NHC) has static mapping for Next Hop Servers (NHSs)
- Registration time is configurable
  - ip nhrp registration timer <value> (default = 1/3 nhrp hold time)
- NHS registration reply gives liveliness of NHS

Dynamic Mesh: Phase 2 NHRP Resolutions



Data packet

NHRP Resolution

NHRP mapping

CEF FIB Table

CEF Adjacency

192.168.0.1/24

Physical: 172.17.0.1
Tunnel0: 10.0.0.1

10.0.0.11 → 172.16.1.1
10.0.0.12 → 172.16.2.1

192.168.0.0/24 → Conn.
192.168.1.0/24 → 10.0.0.11
192.168.2.0/24 → 10.0.0.12

10.0.0.11 → 172.16.1.1
10.0.0.12 → 172.16.2.1

Physical: 172.16.1.1
Tunnel0: 10.0.0.11

Spoke A

192.168.1.1/24

10.0.0.1 → 172.17.0.1 (*)
10.0.0.12 → ???

192.168.0.0/24 → 10.0.0.1
192.168.1.0/24 → Conn.
192.168.2.0/24 → 10.0.0.12

10.0.0.1 → 172.17.0.1
10.0.0.12 → incomplete

Physical: 172.16.2.1
Tunnel0: 10.0.0.12

Spoke B

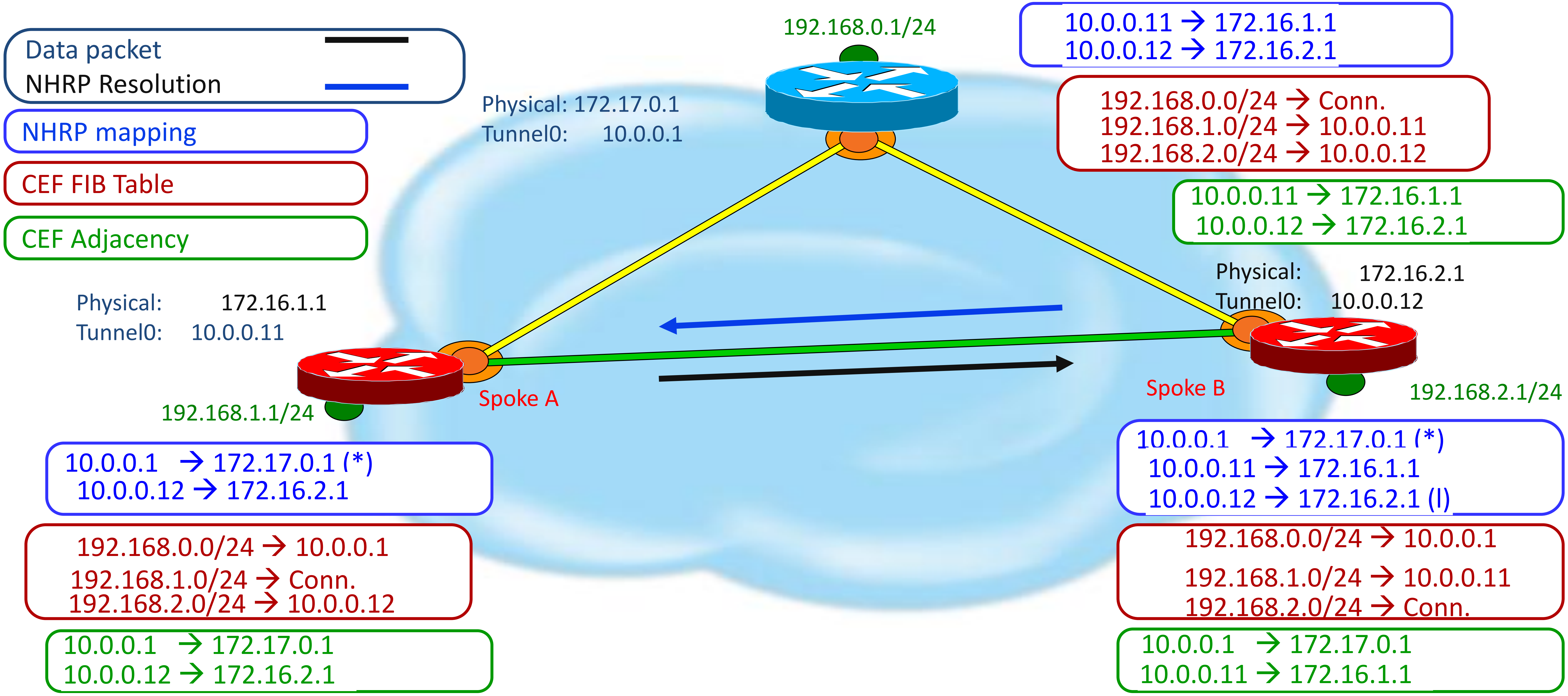
192.168.2.1/24

10.0.0.1 → 172.17.0.1 (*)
10.0.0.11 → 172.16.1.1

192.168.0.0/24 → 10.0.0.1
192.168.1.0/24 → 10.0.0.11
192.168.2.0/24 → Conn.

10.0.0.1 → 172.17.0.1
10.0.0.11 → incomplete

Dynamic Mesh: Phase 2 NHRP Resolutions (cont)



10.0.0.11 → 172.16.1.1
10.0.0.12 → 172.16.2.1

192.168.0.0/24 → Conn.
192.168.1.0/24 → 10.0.0.11
192.168.2.0/24 → 10.0.0.12

10.0.0.11 → 172.16.1.1
10.0.0.12 → 172.16.2.1

10.0.0.1 → 172.17.0.1 (*)
10.0.0.12 → 172.16.2.1

192.168.0.0/24 → 10.0.0.1
192.168.1.0/24 → Conn.
192.168.2.0/24 → 10.0.0.12

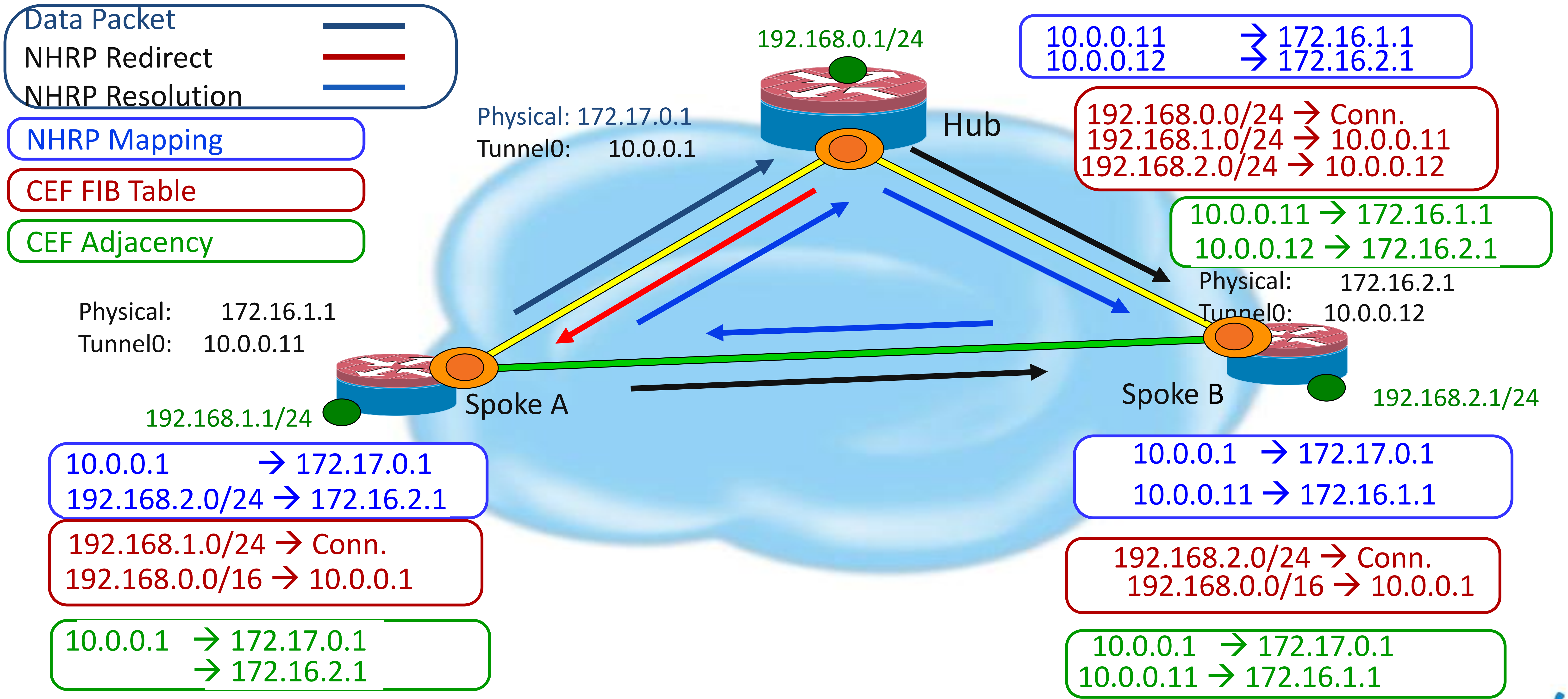
10.0.0.1 → 172.17.0.1
10.0.0.12 → 172.16.2.1

10.0.0.1 → 172.17.0.1 (*)
10.0.0.11 → 172.16.1.1
10.0.0.12 → 172.16.2.1 (I)

192.168.0.0/24 → 10.0.0.1
192.168.1.0/24 → 10.0.0.11
192.168.2.0/24 → Conn.

10.0.0.1 → 172.17.0.1
10.0.0.11 → 172.16.1.1

NHRP Resolutions and Redirects (Phase 3)



Data Packet ▬

NHRP Redirect ▬

NHRP Resolution ▬

NHRP Mapping

CEF FIB Table

CEF Adjacency

Hub: 192.168.0.1/24

Physical: 172.17.0.1

Tunnel0: 10.0.0.1

NHRP Mapping:
10.0.0.11 → 172.16.1.1
10.0.0.12 → 172.16.2.1

CEF FIB Table:
192.168.0.0/24 → Conn.
192.168.1.0/24 → 10.0.0.11
192.168.2.0/24 → 10.0.0.12

CEF Adjacency:
10.0.0.11 → 172.16.1.1
10.0.0.12 → 172.16.2.1

Spoke A: 192.168.1.1/24

Physical: 172.16.1.1

Tunnel0: 10.0.0.11

NHRP Mapping:
10.0.0.1 → 172.17.0.1
192.168.2.0/24 → 172.16.2.1

CEF FIB Table:
192.168.1.0/24 → Conn.
192.168.0.0/16 → 10.0.0.1

CEF Adjacency:
10.0.0.1 → 172.17.0.1
→ 172.16.2.1

Spoke B: 192.168.2.1/24

Physical: 172.16.2.1

Tunnel0: 10.0.0.12

NHRP Mapping:
10.0.0.1 → 172.17.0.1
10.0.0.11 → 172.16.1.1

CEF FIB Table:
192.168.2.0/24 → Conn.
192.168.0.0/16 → 10.0.0.1

CEF Adjacency:
10.0.0.1 → 172.17.0.1
10.0.0.11 → 172.16.1.1

Four Layers for Troubleshooting: GRE Encapsulation Layer

- Look at NHRP. The spoke should be sending an NHRP registration packet on a regular basis, every 1/3 NHRP hold time (on spoke) or 'ip nhrp registration timeout <seconds>' value.

  On the Spoke: show ip nhrp nhs detail

  On the hub: show ip nhrp <spoke-tunnel-ip-address>

- Check the 'created' and 'expire' timer :

  'created' timer: how long this NHRP mapping entry has continuously been in the NHRP mapping table.

  ‘expire' timer: how long before this NHRP mapping entry would be deleted, if the hub were not to receive another NHRP registration from the spoke.

  If the 'created' timer is low and gets reset a lot then that means that the NHRP mapping entry is getting reset

Four Layers for Troubleshooting: GRE Encapsulation Layer

- Verify pings from the hub to the spoke's tunnel ip address and the reverse.
- Use the following debugs on the hub router.

  debug nhrp condition peer <nbma|tunnel>

  debug nhrp

  debug tunnel protection

  debug crypto socket

  (these last two debugs show communication between NHRP and IPsec)

Four Layers for Troubleshooting:
GRE Encapsulation Layer—Show Commands

show ip nhrp detail

```
10.0.0.5/32 via 10.0.0.5, Tunnel0 created 03:36:47, never expire
 Type: static, Flags: used
 NBMA address: 172.17.0.5
10.0.0.9/32 via 10.0.0.9, Tunnel0 created 03:26:26, expire 00:04:04
  Type: dynamic, Flags: unique nat registered
  NBMA address: 110.110.110.2
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 01:55:43, expire 00:04:15
  Type: dynamic, Flags: unique nat registered
  NBMA address: 120.120.120.2
```

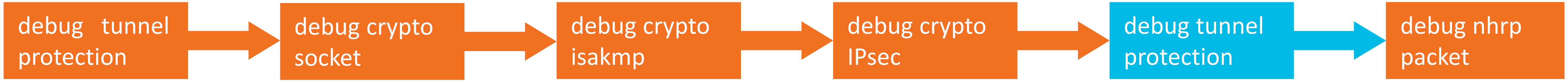
show ip nhrp nhs detail

```
Legend: E=Expecting replies, R=Responding
Tunnel0: 10.0.0.1 RE  req-sent 654 req-failed 0 repl-recv 590 (00:00:09 ago)
              10.0.0.5 RE  req-sent 632 req-failed 0 repl-recv 604 (00:00:09 ago)
```

NHRP Flag Information:

http://www.cisco.com/en/US/docs/ios/12_4/ip_addr/configuration/guide/hadnhrp_ps6350_TSD_Products_Configuration_Guide_Chapter.html#wp1067931

Four Layers for Troubleshooting: GRE Encapsulation Layer—debug dmvpn detail all



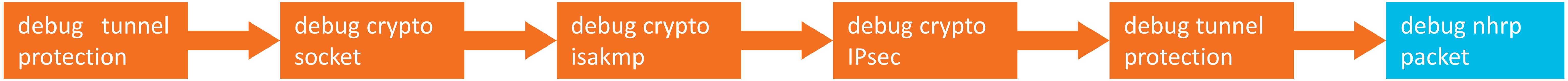
- Tunnel protection start again after IPSec Phase 2 came UP
- Connection lookup id should be same used when tunnel start
- Syslog message shows socket came UP
- Signal NHRP after socket UP

```
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): connection lookup returned 83884274
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.5): tunnel_protection_socket_up
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.5): Signalling NHRP
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.5): connection lookup returned 83DD7B30
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): connection lookup returned 83884274
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): tunnel_protection_socket_up
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): Signalling NHRP
```

ID value has to be same when socket open in the beginning

```
Syslog message:
%DMVPN-7-CRYPTO_SS: Tunnel0-172.16.2.11 socket is UP
```

Four Layers for Troubleshooting: GRE Encapsulation Layer-debug dmvpn detail all (Cont.)



- Spoke send NHRP registration request.
- Req id has to be same in both registration request and response.

```
NHRP: Send Registration Request via Tunnel0 vrf 0, packet
size: 104
src: 10.0.0.9, dst: 10.0.0.1
(F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
 shtl: 4(NSAP), sstl: 0(NSAP)
(M) flags: "unique nat ", reqid: 1279
 src NBMA: 172.16.1.1
 src protocol: 10.0.0.9, dst protocol: 10.0.0.1
(C-1) code: no error(0)
 prefix: 255, mtu: 1514, hd_time: 300
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0,
pref: 0
```

```
NHRP: Receive Registration Reply via Tunnel0 vrf 0, packet
size: 124
(F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
shtl: 4(NSAP), sstl: 0(NSAP)
(M) flags: "unique nat ", reqid: 1279
 src NBMA: 172.16.1.1.
 src protocol: 10.0.0.9, dst protocol: 10.0.0.1
(C-1) code: no error(0)
 prefix: 255, mtu: 1514, hd_time: 300
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref:
0
```

Syslog message:

```
%DMVPN-5-NHRP_NHS: Tunnel0 10.0.0.1 is UP
```

Four Layers for Troubleshooting: GRE Encapsulation Layer

Common Issues

- NHRP Registration fails
- Dynamic NBMA address change in spoke resulting inconsistent NHRP mapping in hub

Common Issues: NHRP Registration Fails

How to Detect?

- VPN tunnel between hub and spoke is up but unable to pass data traffic.

Show crypto isakmp sa

```
dst            src            state          conn-id slot   status
172.17.0.1     172.16.1.1     QM_IDLE           1082    0 ACTIVE
```

Show crypto IPsec sa (spoke)

```
local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
#pkts encaps: 154, #pkts encrypt: 154, #pkts digest: 154
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
inbound esp sas:
spi: 0xF830FC95(4163959957)
outbound esp sas:
spi: 0xD65A7865(3596253285)
```

Packets are encrypted and sent to hub.

Return traffic not coming back from other end of tunnel (hub)

Common Issues: NHRP Registration Fails

Show crypto IPsec sa (Hub)

```
local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
#pkts encaps: 0, #pkts encrypt: 154, #pkts digest: 154
#pkts decaps: 154, #pkts decrypt: 0, #pkts verify: 0
inbound esp sas:
spi: 0xD65A7865(3596253285)
outbound esp sas:
spi: 0xF830FC95(4163959957)
```

Encryption is not happening on Hub towards spoke.

Show interface tunnel0(Spoke)

```
Tunnel0 is up, line protocol is up   Hardware is Tunnel
 Internet address is 10.0.0.12/24
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
Output queue: 0/0 (size/max)
0 packets input, 0 bytes, 0 no buffer
31 packets output, 3318 bytes, 0 underruns
```

Tunnel interface shows zero input packet received from hub

Common Issues:
NHRP Registration Fails (Cont.)

- Check NHS entry in spoke router.

```
Show  ip nhrp nhs detail
Legend: E=Expecting replies, R=Responding
Tunnel0:     172.17.0.1  E  req-sent 0  req-failed 30  repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 4371, Ret 64  NHS 172.17.0.1
```

NHS Request failed

How to Fix?

- Check spoke router tunnel interface configuration to make sure both sides have same tunnel key configured

Look for tunnel key in both hub and spoke

```
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip nhrp authentication test
 ip nhrp map multicast  dynamic
 tunnel key 100000
```

```
interface Tunnel0
 ip address 10.0.0.9 255.255.255.0
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1
 tunnel key 1000000
```

Look carefully determine spoke tunnel key has an extra zero

Common Issues:
NHRP Registration Fails (Cont.)

How to verify?

- Verify NHS entry and ipsec encrypt/decrypt counters

```
show ip nhrp nhs detail
Legend: E=Expecting replies, R=Responding
Tunnel0:      10.0.0.1 RE  req-sent 4  req-failed 0  repl-recv 3 (00:01:04 ago)
```

No failed requests

```
show crypto ipsec sa
local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
#pkts encaps: 121, #pkts encrypt: 121, #pkts digest: 121
#pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118
inbound esp sas:
  spi: 0x1B7670FC(460747004)
outbound esp sas:
  spi: 0x3B31AA86(993110662)
```

- Verify routing protocol neighbor

```
show ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address            Interface       Hold   Uptime   SRTT   RTO  Q     Seq
                                       (sec)           (ms)        Cnt   Num
1   10.0.0.1            Tu0            11     00:21:20    18    200   0      497
```

Common Issues: Dynamic NBMA Address Change in Spoke

- **Problem Description:**

  “Dynamic NBMA address change in spoke resulting inconsistent NHRP mapping in hub until NHRP registration with previous NBMA address expired”

- Show commands in hub before NBMA address change

```
Hub# show ip nhrp
10.0.0.11/32 via 10.0.0.11,Tunnel0 created 16:18:11,expire 00:28:47
Type: dynamic, Flags: unique nat registered,
NBMA address: 172.16.2.2
```

```
Hub # show crypto socket
Tu0 Peers (local/remote): 172.17.0.1/172.16.2.2
    Local Ident  (addr/mask/port/prot): (172.17.0.1/255.255.255.255/0/47)
    Remote Ident (addr/mask/port/prot): (172.16.2.2/255.255.255.255/0/47)
    IPsec Profile: "dmvpn"
    Socket State: Open)
```

Common Issues: Dynamic NBMA Address Change in Spoke

```
Hub# show crypto ipsec sa
interface: Tunnel0
Crypto map tag: Tunnel0-head-0,
local crypto endpoint:172.17.0.1
Remote crypto endpoint:172.16.2.2
#pkts encaps: 13329,
#pkts decaps: 13326,
inbound esp sas:
  spi: 0xFEAB438C(4272636812)
outbound esp sas:
  spi: 0xDD07C33A(3708273466)
```

```
Hub# show crypto map
Crypto Map "Tunnel0-head-0" 65540
Map is a PROFILE INSTANCE.
Peer = 172.16.2.2
        Extended IP access list
        access-list  permit gre host 172.17.0.1  host 172.16.2.2
        Current peer: 172.16.2.2
```

How to Detect?

- Inconsistency after NBMA address change in spoke

```
Hub# show ip nhrp
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 17:37:25, expire 00:09:34
Type: dynamic, Flags: unique nat registered used
NBMA address: 172.16.2.2
```

NHRP shows no entry for 172.16.2.3 still holding entry for previous NBMA address 172.16.2.2

Common Issues: Dynamic NBMA Address Change in Spoke

How to Detect? (Cont.)

```
Hub# show crypto map
Crypto Map "Tunnel0-head-0" 65540 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 172.16.2.2
        Extended IP access list
        access-list  permit gre host 172.17.0.1 host 172.16.2.2
        Current peer: 172.16.2.2
Crypto Map "Tunnel0-head-0" 65541 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 172.16.2.3
        Extended IP access list
        access-list  permit gre host 172.17.0.1  host 172.16.2.3
        Current peer: 172.16.2.3
```

Crypto map entry for both previous and new NBMA address of spoke

```
Hub# show crypto socket
Tu0 Peers (local/remote): 172.17.0.1/172.16.2.2
       Local Ident  (addr/mask/port/prot): (172.17.0.1/255.255.255.255/0/47)
       Remote Ident (addr/mask/port/prot): (172.16.2.2/255.255.255.255/0/47)
       Socket State: Open
Tu0 Peers (local/remote): 172.17.0.1/172.16.2.3
       Local Ident  (addr/mask/port/prot): (172.17.0.1/255.255.255.255/0/47)
       Remote Ident (addr/mask/port/prot): (172.16.2.3/255.255.255.255/0/47)
Socket State: Open
```

Old NBMA address

New NBMA address

Common Issues: Dynamic NBMA Address Change in Spoke

How to Detect? (Cont.)

- debug nhrp packet in hub router to check NHRP registration request /reply.

```
Hub# debug nhrp packet
NHRP: Receive Registration Request via Tunnel0 vrf 0, packet size: 104
 (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
 (M) flags: “unique nat ", reqid: 9480
  src NBMA: 172.16.2.3
  src protocol: 10.0.0.11, dst protocol: 10.0.0.1
 (C-1) code: no error(0)
  prefix: 255, mtu: 1514, hd_time: 600
NHRP: Attempting to send packet via DEST 10.0.0.11
NHRP: Encapsulation succeeded.  Tunnel IP addr 172.16.2.3
NHRP: Send Registration Reply via Tunnel0 vrf 0, packet size: 124,  src: 10.0.0.1, dst: 10.0.0.11
 (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
 (M) flags: “ unique nat ", reqid: 9480
  src NBMA: 172.16.2.3
  src protocol: 10.0.0.11, dst protocol: 10.0.0.1
 (C-1) code: unique address registered already(14)
```

C-1 code shows NBMA address is already registered , that is why it is not updating nhrp mapping table with new NBMA address

Common Issues: Dynamic NBMA Address Change in Spoke

- Spoke router shows the error message indicating about NBMA address already registered

```
%NHRP-3-PAKREPLY: Receive Registration Reply packet with error - unique address registered already(14)
```

How to Fix?

- “ip nhrp registration no-unique” command in tunnel interface of dynamic NBMA address spoke router

```
Spoke# show run interface tunnel0
interface Tunnel0
 ip address 10.0.0.11 255.255.255.0
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.0.1
 ip nhrp registration no-unique
 tunnel protection ipsec profile dmvpn
```

To enable the client to NOT set the unique flag in the Next Hop Resolution Protocol (NHRP) registration request

Common Issues: Dynamic NBMA Address Change in Spoke

How to Verify?

```
Hub# debug nhrp packet
NHRP: Receive Registration Request via Tunnel0 vrf 0, packet size: 104
 (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
 (M) flags: "nat ", reqid: 9462
  src NBMA: 172.16.2.4
  src protocol: 10.0.0.11, dst protocol: 10.0.0.1
 (C-1) code: no error(0)
NHRP: Tu0: Creating dynamic multicast mapping  NBMA: 172.16.2.4
NHRP: Attempting to send packet via DEST 10.0.0.11
NHRP: Encapsulation succeeded.  Tunnel IP addr 172.16.2.4
NHRP: Send Registration Reply via Tunnel0 vrf 0, packet size: 124
  src: 10.0.0.1, dst: 10.0.0.11
 (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
 (M) flags: "nat ", reqid: 9462
  src NBMA: 172.16.2.4
  src protocol: 10.0.0.11, dst protocol: 10.0.0.1
 (C-1) code: no error(0)
  prefix: 255, mtu: 1514, hd_time: 600
```

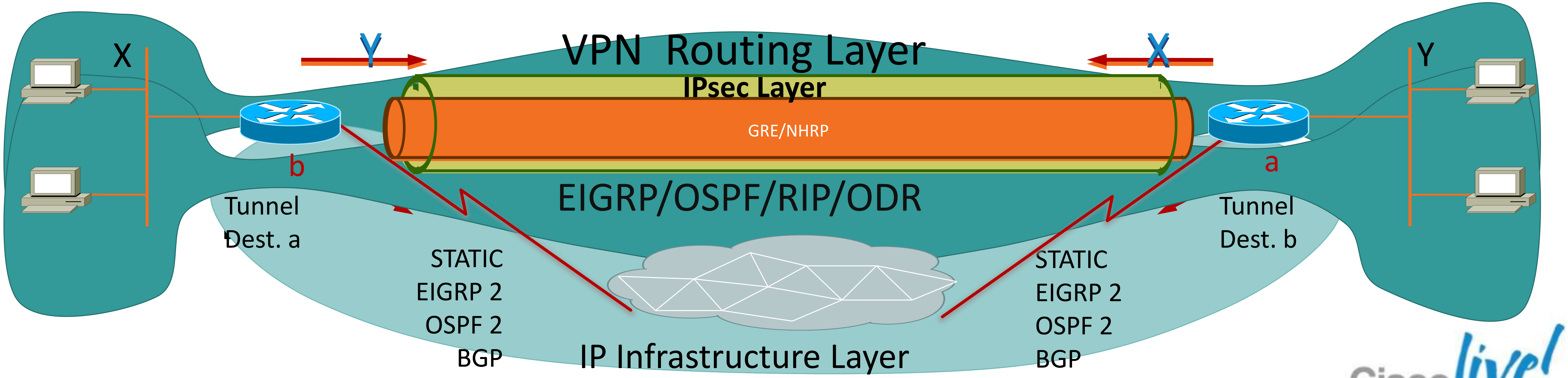
Unique address command
result no unique flag
C-1 code shows no error

```
Hub#sh ip nhrp
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 01:04:32, expire 00:07:06
 Type: dynamic, Flags: nat registered
 NBMA address: 172.16.2.4
```

Unique flag not set

Four Layers for Troubleshooting: VPN Routing Layer

- The VPN routing layer—this is routing packets in/out of the p-pGRE and/or mGRE interfaces on the tunnel endpoint routers. This is done by running a dynamic routing protocol over the DMVPN tunnels



Four Layers for Troubleshooting: VPN Routing Layer

DMVPN Component-routing

- Regular IP networks

  IP routing updates and data packets traverse same physical/logical links

  Routing Protocol monitors state of all links that data packets can use

- DMVPN IP networks

  IP routing updates and IP multicast data packets only traverse hub-and-spoke tunnels

  Unicast IP data packets traverse both hub-and-spoke and direct dynamic spoke-spoke tunnels

  Routing protocol doesn’t monitor state of spoke-spoke tunnels

Four Layers for Troubleshooting: VPN Routing Layer

- Check for routing neighbor and lifetime

  show ip route [eigrp | ospf | rip]

  show ip protocol

  show ip [eigrp | ospf] neighbor

- Check multicast replication and connectivity

  show ip nhrp multicast

  ping [224.0.0.10 (eigrp) | 224.0.0.5 (ospf) | 224.0.0.9 (rip)]

  ping <tunnel-subnet-broadcast-address>

  Example: 10.0.0.0/24 → 10.0.0.255

- Debug: Various debug commands depending on routing protocol

Four Layers for Troubleshooting: VPN Routing Layer: Routing Summary

- Spokes are only routing neighbors with hubs, not with other spokes
  - Spokes advertise local network to hubs
- Hubs are routing neighbors with spokes
  - Advertise spoke and local networks to all spokes
  - All Phases:
    - Turn off split-horizon (EIGRP, RIP)
    - Single area and no summarisation when using OSPF
  - Phase 1 & 3:
    - Hubs can not preserve original IP next-hop; Can Summarise
      - EIGRP, BGP (next-hop-self); RIP, ODR (default)
      - OSPF (network point-multipoint); # hubs not limited
  - Phase 2:
    - Hubs must preserve original IP next-hop; Cannot summarise
      - EIGRP (no ip next-hop-self); BGP (default)
      - OSPF (network broadcast); Only 2 hubs
- Hubs are routing neighbors with other hubs and local network
  - Phase1 & 3: Can use different routing protocol than hub-spoke tunnels
  - Phase 2: Must use same routing protocol as hub-spoke tunnels

Common Issues: Split tunnelling disabled on DMVPN spoke

Problem Description:

Customer has corporate security policies that disable split-tunnelling and advertise default route over the tunnel to all spokes.

He wants to build spoke to spoke tunnel and at the same time wants all internet traffic will go through DMVPN hub located in main corporate office.

Common Issues: Split tunnelling disabled on DMVPN spoke

Solution: Default Route From ISP and Over the Tunnel

- In Spoke to Spoke model, we need an ISP default route to reach other spoke.
- Default route over the Tunnel should not overwrite the ISP default route for spoke to spoke communication to work
- **Solution:** Use Virtual Routing and Forwarding (VRF) instance to handle both default routes

Common Issues: Split tunnelling disabled on DMVPN spoke

VRF and DMVPN

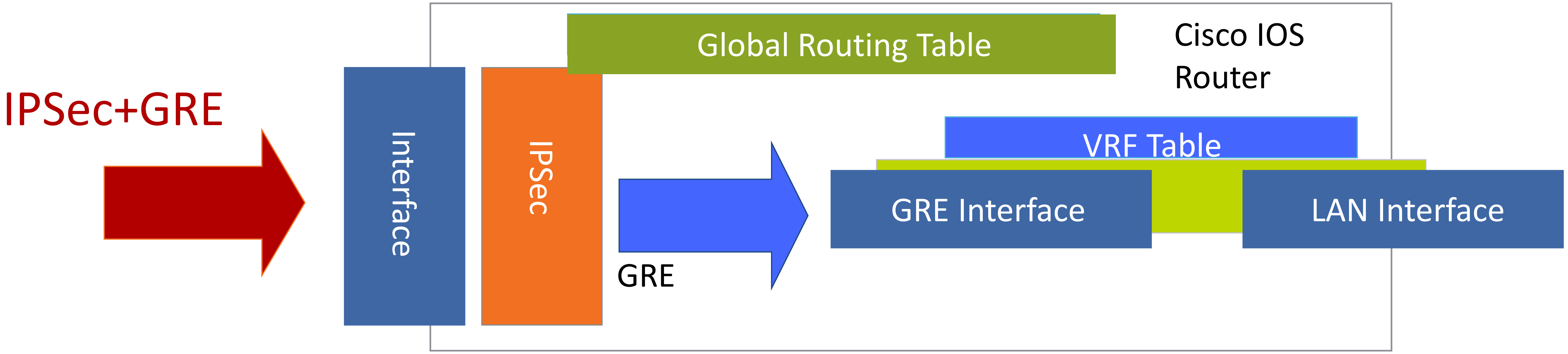
- Typically VRFs are deployed in one of the following two configurations:

  I-VRF: GRE tunnel and LAN interface are configured in a VRF and public interface (carrying GRE traffic) is in global table

  F-VRF: GRE tunnel and LAN interface stay in the global routing table but public interface (carrying GRE traffic) is configured in a VRF

- VRF configurations are a common way of handling dual-default routes

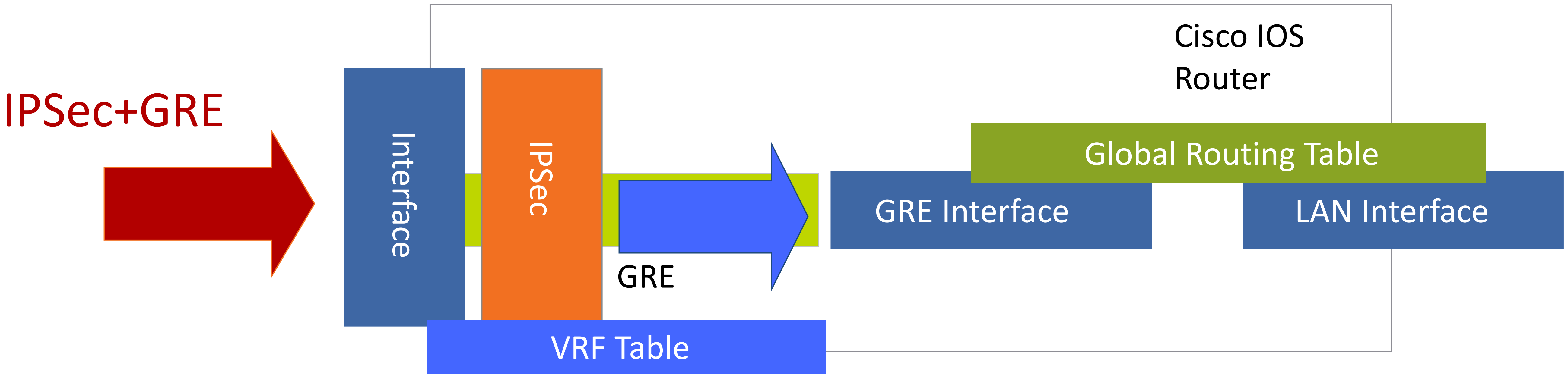
Common Issues: Split tunnelling disabled on DMVPN spoke and I-VRF Implementation



- IPSec packets are forwarded using global routing table
- GRE decapsulated clear-text packets are forwarded using associated VRF

```
Interface Tunnel1
 ip vrf forwarding VRF-1
 tunnel source Serial0/0
!
Interface Serial 0/0
 description in global table
!
Interface FastEthernet 0/0
 ip vrf forwarding VRF-1
```

Common Issues: Split tunnelling disabled on DMVPN spoke and F-VRF



- IPSec packets are forwarded using VRF routing table
- GRE decapsulated clear-text packets are forwarded using global table

```
Interface Tunnel1
 tunnel source Serial0/0
 tunnel VRF F-VRF
!
Interface Serial 0/0
 ip vrf forwarding F-VRF
!
Interface FastEthernet 0/0
 description In Global Table
```

Common Issues: Split tunnelling disabled on DMVPN spoke and Dual Default Routes

Since WAN interface in a VRF, pre-shared key needs to be defined in the VRF

Tunnel Destination lookup forced in VRF FVRF

WAN interface defined in the VRF – LAN interface stays in Global Table

```
ip vrf FVRF
 rd 100:1
!
crypto keyring DMVPN vrf FVRF
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
Interface Tunnel0
 ip address 172.50.1.1 255.255.255.0
 ip nhrp authentication HBfR3lpl
 ip nhrp map multicast 3.3.3.3
 ip nhrp map 172.50.1.254 3.3.3.3
 ip nhrp network-id 1
ip nhrp nhs 172.50.1.254
 ip nhrp shortcut
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel vrf FVRF
 tunnel protection ipsec profile dmvpn
!
Interface GigabitEthernet 0/0
 description WAN interface to ISP in vrf
 ip address dhcp
 ip vrf forwarding FVRF

Interface GigabitEthernet 0/1
 description LAN interface In Global Table
```

Common Issues: Split tunnelling disabled on DMVPN spoke and Dual Default Routes (cont)

How to Verify :

Spoke-A VRF Routing Table

```
Spoke-A# show ip route vrf FVRF

Routing Table: FVRF

Gateway of last resort is 192.168.0.254 to network 0.0.0.0

     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.0/24 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 [254/0] via 192.168.0.254
```

Spoke-A Global Routing Table

```
Spoke-A# show ip route

C       172.50.1.0 is directly connected, Tunnel0
C       172.60.1.0 is directly connected, Tunnel1
C       10.0.0.0/24 is directly connected, GigabitEthernet0/1.84
D       0.0.0.0/0 [90/2844160] via 172.50.1.254, 00:03:45, Tunnel1
```

DMVPN Best Practice Configuration Examples

DMVPN Best Practice Configuration

- Use ‘mode transport’ on transform-set

  NHRP needs for NAT support and saves 20 bytes

- MTU issues

  ip mtu 1400

  ip tcp adjust-mss 1360

  crypto ipsec fragmentation after-encryption (global)

- NHRP

  ip nhrp holdtime <seconds>(recommended values 300 - 600)

  ip nhrp registration no-unique

- ISAKMP

  Call Admission Control (CAC) (on spokes and hubs)

  call admission limit *percent* (hubs)

  crypto call admission limit {**ike** {**in-negotiation-sa** *number* | **sa** *number*}}

  Keepalives on spokes (GRE tunnel keepalives are not supported)

  crypto isakmp keepalive 20 5

  Invalid-SPI recovery not useful

Recommended Releases

- **6500/7600 with VPN-SPA**

  Sup720 : 12.2(33)SRC6,12.2(33)SRD7,12.2(33)SRE5,12.2(18)SXF17b for 7600
  12.2(33)SXH8b, 122(18)SXF17b,12.2(33)SXI7,12.2(33)SXJ1 for 6500

- **For ASR- DMVPN Hub or spoke**

  Phase 2(Release 3): 2.4.4 (02.04.04.122-33.XND4)
  Phase 3(Release 5): 2.6.2 (02.06.02.122-33.XNF2)

  3.5.2S(03.05.02.152-1.S2),3.6.2S(03.06.02.152-2.S2),3.2.2S(03.02.02.151-1.S2), 3.3.2S(03.03.02.151-2.S2), 3.4.4S(03.04.04.151-3.S4)

- **For 87x, 18xx, 28xx, 38xx,**

  IOS 12.4 Mainline: 12.4(23)b, 12.4(25)g
  IOS 12.4 T-train: 12.4(15)T17, 124(24)T8

  IOS 15 Mainline/T-train : 15.0(1)M9, 15.1(4)M5, 15.2(4)M2,15.1(2)T5, 15.1(3)T4

- **For 720x(NPE-G2+VSA): IOS 12.4 T-train**:

  IOS 12.4 : 12.4(25)f, IOS 12.4 T-train: 12.4(15)T17 , 12.4(24)T8
  IOS 15.0 Mainline : 15.0(1)M9, 15.1(4)M5, 15.2(4)M2

  IOS 15 S-train : 15.1(3)S4, 15.2(4)S1

- **For 89x,19xx,29xx,39xx**:

  IOS 15 Mainline/T-train : 15.0(1)M8, 15.1(4)M4, 15.2(4)M1 15.1(3)T4, 15.2(3)T1

Final Thoughts

- Get hands-on experience with the Walk-in Labs located in World of Solutions, booth 1042
- Come see demos of many key solutions and products in the main Cisco booth 2924
- Visit www.ciscoLive365.com after the event for updated PDFs, on-demand session videos, networking, and more!
- Follow Cisco Live! using social media:
  - Facebook: https://www.facebook.com/ciscoliveus
  - Twitter: https://twitter.com/#!/CiscoLive
  - LinkedIn Group: http://linkd.in/CiscoLI

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Cisco live! 365

Don’t forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button. www.ciscoliveaustralia.com/portal/login.ww