TOMORROW starts here.
Troubleshooting Dynamic Multipoint VPN (DMVPN)

BRKSEC-3052

Sheikh Rehan (CCIE # 8665  R&S/Security)
Technical Leader Services
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 Virtual: [www.ciscolivevirtual.com](http://www.ciscolivevirtual.com)
Reference Slides

- They are mainly for your reference when back at work ;-) 
- Those slides won’t be explained in detail.
DMVPN Overview
Agenda

- DMVPN Overview
- Four Layer Troubleshooting Methodology
  Common Issues
- Case Study
- DMVPN Best Practice Configuration
- Q & A
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
What is Dynamic Multipoint VPN?

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

- Relies on two proven technologies
  - Next Hop Resolution Protocol (NHRP)
    - Creates a distributed mapping database of VPN (tunnel interface) to real (public interface) addresses
  - Multipoint GRE Tunnel Interface
    - Single GRE interface to support multiple GRE/IPsec tunnels and endpoints
    - Simplifies size and complexity of configuration
    - Supports dynamic tunnel creation
DMVPN—How It Works

- Spokes have a dynamic permanent GRE/IPsec tunnel to the hub, but not to other spokes; they register as clients of the NHRP server.
- When a spoke needs to send a packet to a destination (private) subnet behind another spoke, it 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 (because it knows the peer address).
- The spoke-to-spoke tunnel is built over the mGRE interface.
- When traffic ceases then the spoke-to-spoke tunnel is removed.
DMVPN Major Features

- Configuration reduction and no-touch deployment
- Supports:
  - Passenger protocols (IP(v4/v6) unicast, multicast and dynamic Routing Protocols)
  - Transport protocols (NBMA) (IPv4 and IPv6)
  - Remote peers with dynamically assigned transport addresses.
  - Spoke routers behind dynamic NAT; Hub routers behind static NAT.
- Dynamic spoke-spoke tunnels for partial/full mesh scaling.
- Can be used without IPsec Encryption
- Works with MPLS; GRE tunnels and/or data packets in VRFs and MPLS switching over the tunnels
- 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
“Static” Spoke-Hub, Hub-Hub Tunnels

- **GRE, NHRP and IPsec configuration**
  - p-pGRE or mGRE on spokes; mGRE on hubs

- **NHRP registration**
  - Dynamically addressed spokes (DHCP, NAT,…)

- **Routing protocol, NHRP, and IP multicast**
  - On spoke-hub and hub-hub tunnels

- **Data traffic on spoke-hub tunnels**
  - All traffic for hub-and-spoke only networks
  - Spoke-spoke traffic while building spoke-spoke tunnels

For your reference
Dynamic Spoke-Spoke Tunnels

- GRE, NHRP and IPsec configuration
  - mGRE on both hub and spokes

- Spoke-spoke unicast data traffic
  - Reduced load on hubs
  - Reduced latency
  - Single IPsec encrypt/decrypt

- On demand tunnel creates when need it

- NHRP resolutions and redirects
  - Find NHRP mappings for spoke-spoke tunnels
## DMVPN Phases

<table>
<thead>
<tr>
<th>Phase 1 – 12.2(13)T</th>
<th>Phase 2 – 12.3(4)T (Phase 1 +)</th>
<th>Phase 3 – 12.4.(6)T (Phase 2 +)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Hub and spoke functionality</td>
<td>• Spoke to spoke functionality</td>
<td>• Increase architecture designs and scaling</td>
</tr>
<tr>
<td>• p-pGRE interface on spokes, mGRE on hubs</td>
<td>• mGRE interface on spokes</td>
<td>• Same Spoke to Hub ratio</td>
</tr>
<tr>
<td>• Simplified and smaller configuration on hubs</td>
<td>• Direct spoke to spoke data traffic reduces load on hubs</td>
<td>• No hub daisy-chain</td>
</tr>
<tr>
<td>• Support dynamically addressed CPEs (NAT)</td>
<td>• Hubs must interconnect in daisy-chain</td>
<td>• Spokes don’t need full routing table – can summarize</td>
</tr>
<tr>
<td>• Support for routing protocols and multicast</td>
<td>• Spoke must have full routing table – no summarization</td>
<td>• Spoke-spoke tunnel triggered by hubs</td>
</tr>
<tr>
<td>• Spokes don’t need full routing table – can summarize on hubs</td>
<td>• Spoke-spoke tunnel triggered by spoke itself</td>
<td>• Remove routing protocol limitations</td>
</tr>
<tr>
<td></td>
<td>• Routing protocol limitations</td>
<td>• NHRP routes/next-hops in RIB (15.2(1)T)</td>
</tr>
</tbody>
</table>
Network Designs

Hub and spoke (Phase 1)

Spoke-to-spoke (Phase 2)

VRF-lite

Server Load Balancing

Hierarchical (Phase 3)

2547oDMVPN
Before You Begin

- Sync up the timestamps between the hub and spoke
- 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. This way you can 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

- Troubleshooting Approach
  - Solution Troubleshooting (of features)
  - Understand/Isolate Building Blocks
  - Understand Interaction between blocks
  - Find the Right Layer
“A problem well stated is a problem half solved.”

Charles F. Kettering
Four Layers for Troubleshooting: Physical and Routing Layer

- **Physical (NBMA or tunnel endpoint) routing layer**
  - This is getting the encrypted tunnel packets between the tunnel endpoints (DMVPN hub and spoke or between spoke and spoke routers)
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.
  Hopefully there isn't a firewall that blocks ping packets.
  If this doesn't work, 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 use if no connectivity
  - `debug ip icmp`
  - Valuable tool used to troubleshoot connectivity issues
  - Helps you determine whether the router is sending or receiving ICMP messages

```plaintext
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:

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

- Debugs and show commands use if no connectivity (cont.)
  - debug ip packet [access-list-number] [detail] [dump]
    - Useful tool for troubleshooting end to end communication
    - IP packet debugging captures the packets that are process switched including received, generated and forwarded packets.

```plaintext
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: The debug IP packet command can generate a substantial amount of output and use a substantial amount of system resources. This command should be used with caution in production networks. Always use with an ACL.
Common Issues:

- ACL in firewall/ISP side block ISAKMP traffic
- Traffic filtering resulting traffic flows one direction
Common Issues:
ACL in Firewall/ISP Side Block ISAKMP Traffic

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

How to detect?

```
show crypto isa sa
```
IPv4 Crypto ISAKMP SA

<table>
<thead>
<tr>
<th>Dst</th>
<th>src</th>
<th>state</th>
<th>conn-id</th>
<th>slot</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.17.0.1</td>
<td>172.16.1.1</td>
<td>MM_NO_STATE</td>
<td>0</td>
<td>0</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>172.17.0.1</td>
<td>172.16.1.1</td>
<td>MM_NO_STATE</td>
<td>0</td>
<td>0</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>172.17.0.5</td>
<td>172.16.1.1</td>
<td>MM_NO_STATE</td>
<td>0</td>
<td>0</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>172.17.0.5</td>
<td>172.16.1.1</td>
<td>MM_NO_STATE</td>
<td>0</td>
<td>0</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

DMVPN Spoke

VPN tunnel flapping
Common Issues: ACL in Firewall/ISP Side Block ISAKMP Traffic

- Further check debug crypto isakmp to verify spoke router is sending udp 500 packet

```plaintext
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
04:14:54.450: 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
04:15:04.450: 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
```

Above debug output shows spoke router is sending udp 500 packet every 10 secs.
Common Issues: ACL in Firewall/ISP Side Block ISAKMP Traffic

- How to fix?

Check with either firewall admin OR ISP admin if spoke router is directly connected to ISP router to make sure they are allowing udp 500 traffic. After ISP or Firewall admin allowed udp 500 add inbound ACL in egress interface which is tunnel source interface to allow udp 500 to make sure UDP 500 traffic coming into the router show access-list to verify hit counts are incrementing.

```
show access-lists 101
Extended IP access list 101
   10 permit udp host 172.17.0.1 host 172.16.1.1 eq isakmp log (4 matches)
   20 permit udp host 172.17.0.5 host 172.16.1.1 eq isakmp log (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: ACL in Firewall/ISP Side Block ISAKMP Traffic

How to verify?

```
show crypto isa sa
IPv4 Crypto ISAKMP SA

<table>
<thead>
<tr>
<th>dst</th>
<th>src</th>
<th>state</th>
<th>conn-id</th>
<th>slot</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.17.0.1</td>
<td>172.16.1.1</td>
<td>QM_IDLE</td>
<td>1009</td>
<td>0</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>172.17.0.5</td>
<td>172.16.1.1</td>
<td>QM_IDLE</td>
<td>1008</td>
<td>0</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>
```

```
debug crypto isa
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
```
Common Issues: Traffic Filtering, Traffic Flows One Direction

Problem

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

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 dropped some where in the path return from Spoke 2 towards Spoke 1
Common Issues: Traffic Filtering, Traffic Flows One Direction

- **How to fix?**
  
  Spoke 2 router shows both *encap* and *decap* which means either firewall in spoke 2 customer side ahead of router or ISP device in spoke 2 or any where in path between spoke 2 router and spoke 1 router filter ESP traffic.

- **How to verify?**

  ```sh
  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 allowed ESP (IP protocol 50) Spoke 1 and Spoke 2 both shows encap and decaps, counters are incrementing.
Four Layers for Troubleshooting: IPsec Encryption Layer

- **The IPsec encryption layer**—
  This is encrypting the GRE tunnel packet going out and decrypting the IPsec packet coming in to reveal the GRE encapsulated packet.
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”

```bash
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 being created
  
  show crypto isakmp sa detail
  
  show crypto IPsec sa peer <NBMA-address-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 Isakmp phase 1 and IPsec phase 2 status
  - Prior to 15.x version, it does not show remaining life time for both Isakmp phase 1 and IPsec phase 2, to check life time still use old commands

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

- 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**

```plaintext
Router# show crypto isakmp sa

dst       src       state     connid slot
172.17.0.1 172.16.1.1      QM_IDLE   1  0
```

**show crypto isakmp sa detail**

```plaintext
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 I-VRF 3des sha psk 1 23:59:40

Connection-id:Engine-id = 1:1(hardware)
```

**IKE Phase 1 status UP**

**Encryption:3des**

**Authentication :Pre-shared key**

**Remaining lifetime before phase 1 re-key**

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

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 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
```
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,

<table>
<thead>
<tr>
<th># Ent</th>
<th>Peer NBMA Addr</th>
<th>Peer Tunnel Add</th>
<th>State</th>
<th>UpDn</th>
<th>Tm</th>
<th>Attrb</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.1.1.1</td>
<td>172.20.1.1</td>
<td>UP</td>
<td>00:04:32</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2.2.2.2</td>
<td>172.20.1.2</td>
<td>UP</td>
<td>00:01:25</td>
<td>D</td>
<td></td>
</tr>
</tbody>
</table>

SPOKE-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: Spoke, NHRP Peers: 1,

<table>
<thead>
<tr>
<th># Ent</th>
<th>Peer NBMA Addr</th>
<th>Peer Tunnel Add</th>
<th>State</th>
<th>UpDn</th>
<th>Tm</th>
<th>Attrb</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3.3.3.3</td>
<td>172.20.1.100</td>
<td>UP</td>
<td>00:21:56</td>
<td>S</td>
<td></td>
</tr>
</tbody>
</table>

Learn Dynamically, Entry shows either in hub or in spoke for spoke to spoke tunnels

Static NHRP mapping
Four Layers for Troubleshooting: IPsec Encryption Layer—Show Commands

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

<table>
<thead>
<tr>
<th># Ent</th>
<th>Peer NBMA Addr</th>
<th>Peer Tunnel Add</th>
<th>State</th>
<th>UpDn Tm</th>
<th>Attrb</th>
<th>Target Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>172.17.0.9</td>
<td>10.10.10.2</td>
<td>UP</td>
<td>18:15:07</td>
<td>S</td>
<td>10.10.10.2/32</td>
</tr>
<tr>
<td>2</td>
<td>172.16.7.2</td>
<td>10.10.10.7</td>
<td>UP</td>
<td>00:02:36</td>
<td>D</td>
<td>10.10.10.7/32</td>
</tr>
<tr>
<td>0</td>
<td>172.16.7.2</td>
<td>10.10.10.7</td>
<td>UP</td>
<td>00:02:36</td>
<td>DT1</td>
<td>192.168.19.0/24</td>
</tr>
<tr>
<td>1</td>
<td>172.16.2.1</td>
<td>10.10.10.6</td>
<td>UP</td>
<td>00:02:36</td>
<td>DLX</td>
<td>192.168.18.0/24</td>
</tr>
</tbody>
</table>

Learn Dynamically,
- DLX:Dynamic Local no socket
- DT1: Dynamic tunnel for spoke to spoke
Four Layers for Troubleshooting: IPsec Encryption Layer—Show Commands -contd

**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
  Active SAs: 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
```
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
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.)

- 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)

```plaintext
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 in 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

<table>
<thead>
<tr>
<th>Default protection suite</th>
</tr>
</thead>
<tbody>
<tr>
<td>encryption algorithm:</td>
</tr>
<tr>
<td>hash algorithm:</td>
</tr>
<tr>
<td>authentication method:</td>
</tr>
<tr>
<td>Diffie-Hellman group:</td>
</tr>
<tr>
<td>lifetime:</td>
</tr>
</tbody>
</table>

- A show crypto isakmp sa shows the ISAKMP SA to be in MM_NO_STATE, meaning that main-mode failed
Common Issues: Incompatible ISAKMP Policy (Cont.)

- **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 in 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

```
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)
```

Trying XAuth
Common Issues: DMVPN Hub and Ezvpn server in same Router

- Run isakmp debug to verify what you see in show command

```plaintext
ISAKMP:(4119):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(4119):Old State = IKE_R_MM4 New State = IKE_R_MM5
ISAKMP (0:4119): ID payload
  next-payload  : 8
  type           : 1
  address        : 10.1.1.1
  protocol       : 17
  port           : 0
  length         : 12

bring down existing phase 1 and 2 SA's with local 172.17.0.1 remote 172.18.1.1 remote port 1024
ISAKMP:(4119):returning IP addr to the address pool
ISAKMP:(4118):received initial contact, deleting SA
ISAKMP:(4118):deleting SA reason "Receive initial contact" state (R) CONF_XAUTH (peer 172.18.1.1)
ISAKMP:(4119):Old State = IKE_R_MM5 New State = IKE_R_MM5
ISAKMP: set new node 616549739 to CONF_XAUTH
ISAKMP:(4118):Input = IKE_MESG_INTERNAL, IKE_PHASE1_DEL
ISAKMP:(4118):Old State = IKE_XAUTH_REQ_SENT New State = IKE_DEST_SA
ISAKMP:(4119):Need 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 Hub

Looking for Xauth

BRKSEC-3052 © 2013 Cisco and/or its affiliates. All rights reserved. Cisco Public
Common Issues: DMVPN Hub and Ezvpn server in same Router

- Check existing configuration that don’t allow DMVPN spoke to come up and give CONF_XAUTH message in debugs

```plaintext
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
DMVPN Hub Configuration

Common Issues: DMVPN Hub and Ezvpn server in 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
Common Issues: DMVPN Hub and Ezvpn server in same Router

How to Fix?
By default Spoke tunnel terminate on Ezvpn group if you have both Ezvpn server and DMVPN configured in same router which looks for CONF_XAUTH.

Separate 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 Of DMVPN Hub
Common Issues: DMVPN Hub and Ezvpn server in 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 in 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

Keying scan in debugs
Common Issues: DMVPN Hub and EzVPN server on same Router

```
show crypto isakmp sa
IPv4 Crypto ISAKMP SA

<table>
<thead>
<tr>
<th>dst</th>
<th>src</th>
<th>state</th>
<th>conn-id</th>
<th>slot</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.17.0.1</td>
<td>172.19.87.148</td>
<td>QM_IDLE</td>
<td>4158</td>
<td>0</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>172.17.0.1</td>
<td>172.16.1.1</td>
<td>QM_IDLE</td>
<td>4152</td>
<td>0</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>172.17.0.1</td>
<td>172.18.1.1</td>
<td>QM_IDLE</td>
<td>4157</td>
<td>0</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>172.17.0.6</td>
<td>172.17.0.1</td>
<td>QM_IDLE</td>
<td>4156</td>
<td>0</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

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)
```

EzVPN profile matched for EzVPN clients

DMVPN Profile matched for DMVPN spokes
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:
  - encaps is 1
  - SA life type in seconds
  - SA life duration (basic) of 3600
  - SA life type in kilobytes
  - 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
  GRE encapsulation of the data packet going out or GRE de-capsulation of the GRE packet (after IPsec decrypted) to switch the data packet

![Diagram of GRE Encapsulation](image)

**IP Infrastructure Layer**
- STATIC EIGRP 2
- OSPF 2
- BGP

**Tunnel Dest. a**
- b

**Tunnel Dest. b**
- a

**After GRE Encapsulation**
- GRE IP Header: 20 bytes
- GRE header: 4 bytes
- Original DATA IP header: 20 bytes
- Original DATA payload

NHRP is also transported over GRE
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

- An mGRE interface definition includes:
  An IP address
  A tunnel source
  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

interface Tunnel
ip address 10.0.0.1 255.0.0.0
tunnel source Dialer1
tunnel mode gre multipoint
tunnel key 1
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 address
- Like ARP, NHRP can have static and dynamic entries
- NHRP has worked fully dynamically since Release 12.2(13)T
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
DMVPN Component-NHRP (Cont.)

- Three ways to populate the NHRP cache:
  - Manually add static entries
  - Hub learns via registration requests
  - Spokes learn via resolution requests

- “Resolution” is for spoke to spoke
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
  ```
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
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
Spoke Registration

```
ip address 10.0.0.254 255.255.255.0
ip nhrp network-id 1
```

NHRP table
10.0.0.1 → 172.16.1.1
10.0.0.2 → 172.16.2.1

```
ip address 10.0.0.1 255.255.255.0
ip nhrp network-id 1
ip nhrp map 10.0.0.254 172.16.254.1
ip nhrp nhs 10.0.0.254
```

Hub
192.168.254.0/24

Physical: 172.16.254.1
Tunnel: 10.0.0.254

Spoke 1
192.168.0.0/29

Physical: 172.16.1.1
Tunnel: 10.0.0.1

Registration Request

Spoke 2
192.168.0.8/29

Physical: 172.16.2.1
Tunnel: 10.0.0.2

NHRP table
10.0.0.254 → 172.16.254.1

NHRP table
10.0.0.254 → 172.16.254.1
Route exchange

Routing table
C 10.0.0.0 → Tunnel0
D 192.168.0.0/29 → 10.0.0.1
D 192.168.0.8/29 → 10.0.0.2

NHRP table
10.0.0.1 → 172.16.1.1
10.0.0.2 → 172.16.2.1

NHRP table
10.0.0.254 → 172.16.254.1

Routing table
C 192.168.0.0/29 → Eth0
C 10.0.0.0 → Tunnel0

IT DEPENDS: phase 2 or 3?

ip nhrp map multicast dynamic

Hub
192.168.254.0/24

Physical: 172.16.254.1
Tunnel: 10.0.0.254

Spoke 1
192.168.0.0/29

Physical: 172.16.1.1
Tunnel: 10.0.0.1

Spoke 2
192.168.0.8/29

Physical: 172.16.2.1
Tunnel: 10.0.0.2

Routing Update

NHRP table
10.0.0.254 → 172.16.254.1

Routing table
C 192.168.0.8/29 → Eth0
C 10.0.0.0 → Tunnel0

Routing table
C 192.168.0.0/29 → Tunnel0

it depends: phase 2 or 3?
Hub & Spoke design

Routing table
C 10.0.0.0 → Tunnel0
C 192.168.254.0 → Eth0
D 192.168.0.0/29 → 10.0.0.1
D 192.168.0.8/29 → 10.0.0.2

NHRP table
10.0.0.1 → 172.16.1.1
10.0.0.2 → 172.16.2.1

Physical: 172.16.1.1
Tunnel: 10.0.0.1

Spoke 1
192.168.0.0/29

Hub via transport network
192.168.0.0/16 encrypted & tunneled to hub

NHRP table
10.0.0.254 → 172.16.254.1

Physical: 172.16.2.1
Tunnel: 10.0.0.2

Spoke 2
192.168.0.8/29

Routing table
C 192.168.0.8/29 → Eth0
C 10.0.0.0 → Tunnel0
S 172.16.254.1 → Dialer0
D 192.168.0.0/16 → 10.0.0.254

Hub
192.168.254.0/24

Physical: 172.16.254.1
Tunnel: 10.0.0.254

Routing table
C 192.168.0.0/29 → Eth0
C 10.0.0.0 → Tunnel0
S 172.16.254.1 → Dialer0
D 192.168.0.0/16 → 10.0.0.254
**DMVPN phase 2 design**

**Routing table**
- C 10.0.0.0 → Tunnel0
- C 192.168.254.0/24 → Eth0
- D 192.168.0.0/29 → 10.0.0.1
- D 192.168.0.8/29 → 10.0.0.2

**NHRP table**
- 10.0.0.1 → 172.16.1.1
- 10.0.0.2 → 172.16.2.1

**Spoke 1**
- Physical: 172.16.1.1
- Tunnel: 10.0.0.1

**Spoke 2**
- Physical: 172.16.2.1
- Tunnel: 10.0.0.2

**Hub**
- Physical: 192.168.254.0/24

**NHRP table**
- 10.0.0.254 → 172.16.254.1

**Tunnels via transport network**

**Lots of individual prefixes**

**Spoke 2 subnet → Spoke 2 Tunnel**
DMVPN phase 2 shortcuts (1)

Routing table
C 10.0.0.0 → Tunnel0
C 192.168.254.0/24 → Eth0
D 192.168.0.0/29 → 10.0.0.1
D 192.168.0.8/29 → 10.0.0.2

NHRP table
10.0.0.1 → 172.16.1.1
10.0.0.2 → 172.16.2.1

Physical: 172.16.1.1
Tunnel: 10.0.0.1

NHRP table
10.0.0.254 → 172.16.254.1
10.0.0.2 → 172.16.2.1

Physical: 172.16.2.1
Tunnel: 10.0.0.2

NHRP table
10.0.0.254 → 172.16.254.1

Routing table
C 192.168.0.0/29 → Eth0
C 10.0.0.0 → Tunnel0
S 0.0.0.0/0 → Dialer0
D 192.168.0.8/29 → 10.0.0.2

Routing table
C 192.168.0.8/29 → Eth0
C 10.0.0.0 → Tunnel0
S 0.0.0.0/0 → Dialer0
D 192.168.0.0/29 → 10.0.0.1
**DMVPN phase 2 shortcuts (2)**

**Routing table**
- C 10.0.0.0 → Tunnel0
- C 192.168.254.0/24 → Eth0
- D 192.168.0.0/29 → 10.0.0.1
- D 192.168.0.8/29 → 10.0.0.2

**NHRP table**
- 10.0.0.1 → 172.16.1.1
- 10.0.0.2 → 172.16.2.1

**Physical:**
- 172.16.1.1
- 172.16.2.1
- 172.16.254.1
- 192.168.0.0/29
- 192.168.0.8/29

**Tunnel:**
- 10.0.0.1
- 10.0.0.2
- 10.0.0.254

**Resolution Reply**
- Spoke 1 to Spoke 2
- Spoke 2 to Spoke 1
DMVPN phase 2 shortcuts (3)

Routing table
C 10.0.0.0 → Tunnel0
C 192.168.254.0/24 → Eth0
D 192.168.0.0/29 → 10.0.0.1
D 192.168.0.8/29 → 10.0.0.2

NHRP table
10.0.0.1 → 172.16.1.1
10.0.0.2 → 172.16.2.1

Physical: 172.16.1.1
Tunnel: 10.0.0.1

Spoke 1
192.168.0.0/29

NHRP table
10.0.0.254 → 172.16.254.1
10.0.0.2 → 172.16.2.1

Physical: 172.16.254.1
Tunnel: 10.0.0.254

Hub
192.168.254.0/24

Physical: 172.16.254.1
Tunnel: 10.0.0.254

NHRP table
10.0.0.254 → 172.16.254.1

Physical: 172.16.2.1
Tunnel: 10.0.0.2

Spoke 2
192.168.0.8/29

Routing table
C 192.168.0.0/29 → Eth0
C 10.0.0.0 → Tunnel0
S 0.0.0.0/0 → Dialer0
D 192.168.0.8/29 → 10.0.0.2

Routing table
C 192.168.0.8/29 → Eth0
C 10.0.0.0 → Tunnel0
S 0.0.0.0/0 → Dialer0
D 192.168.0.0/29 → 10.0.0.1

NHRP table
10.0.0.254 → 172.16.254.1

Routing table
C 192.168.0.0/29 → Eth0
C 10.0.0.0 → Tunnel0
S 0.0.0.0/0 → Dialer0
D 192.168.0.0/29 → 10.0.0.1
DMVPN phase 3 design

**Routing table**
- **C 10.0.0.0 → Tunnel0**
- **C 192.168.254.0/24 → Eth0**
- **D 192.168.0.0/29 → 10.0.0.1**
- **D 192.168.0.8/29 → 10.0.0.2**

**NHRP table**
- **10.0.0.1 → 172.16.1.1**
- **10.0.0.2 → 172.16.2.1**

**Physical:**
- **172.16.1.1**
- **172.16.2.1**
- **172.16.254.1**

**Tunnel:**
- **10.0.0.1**
- **10.0.0.254**
- **10.0.0.254**

**Spoke 1**
- 192.168.0.0/29

**Spoke 2**
- 192.168.0.8/29

**Hub**
- 192.168.254.0/24

**Tunnels via transport network**

**192.168.0.0/16 summary tunneled to hub**

**Hub advertises back summary prefix pointing to hub.**

**Routing table**
- **C 192.168.0.0/29 → Eth0**
- **C 10.0.0.0 → Tunnel0**
- **S 0.0.0.0/0 → Dialer0**
- **D 192.168.0.0/16 → 10.0.0.254**

**NHRP table**
- **10.0.0.254 → 172.16.254.1**

**Physical:**
- **172.16.2.1**

**Tunnel:**
- **10.0.0.2**

© 2013 Cisco and/or its affiliates. All rights reserved.
DMVPN phase 3 design

**Routing table**
- C 10.0.0.0 → Tunnel0
- C 192.168.254.0/24 → Eth0
- D 192.168.0.0/29 → 10.0.0.1
- D 192.168.0.8/29 → 10.0.0.2

**NHRP table**
- 10.0.0.1 → 172.16.1.1
- 10.0.0.2 → 172.16.2.1

**Physical**
- 172.16.1.1
- 172.16.2.1

**Tunnel**
- 10.0.0.1
- 10.0.0.2

**NHRP table**
- 10.0.0.254 → 172.16.254.1

**Physical**
- 172.16.254.1

**Tunnel**
- 10.0.0.254

**Routing table**
- C 192.168.0.0/29 → Eth0
- C 10.0.0.0 → Tunnel0
- S 0.0.0.0/0 → Dialer0
- D 192.168.0.0/16 → 10.0.0.254

**ip nhrp redirect**

**Hub**
- 192.168.254.0/24

**Spoke 1**
- 192.168.0.0/29

**Spoke 2**
- 192.168.0.8/29

**ip nhrp shortcut**

**NHRP table**
- 10.0.0.254 → 172.16.254.1

**Physical**
- 172.16.2.1

**Tunnel**
- 10.0.0.2

**Routing table**
- C 192.168.0.0/29 → Eth0
- C 10.0.0.0 → Tunnel0
- S 0.0.0.0/0 → Dialer0
- D 192.168.0.0/29 → 10.0.0.254
DMVPN phase 3 shortcuts (1)

**Routing table**
- **C 10.0.0.0** → **Tunnel0**
- **C 192.168.254.0/24** → **Eth0**
- **D 192.168.0.0/29** → **10.0.0.1**
- **D 192.168.0.8/29** → **10.0.0.2**

**NHRP table**
- 10.0.0.1 → 172.16.1.1
- 10.0.0.2 → 172.16.2.1

**Routing table**
- **C 192.168.0.0/29** → **Eth0**
- **C 10.0.0.0** → **Tunnel0**
- **S 0.0.0.0/0** → **Dialer0**
- **D 192.168.0.0/16** → **10.0.0.254**

**NHRP table**
- 10.0.0.254 → 172.16.254.1
DMVPN phase 3 shortcuts (2)

<table>
<thead>
<tr>
<th>Routing table</th>
</tr>
</thead>
<tbody>
<tr>
<td>C 10.0.0.0 → Tunnel0</td>
</tr>
<tr>
<td>C 192.168.254.0/24 → Eth0</td>
</tr>
<tr>
<td>D 192.168.0.0/29 → 10.0.0.1</td>
</tr>
<tr>
<td>D 192.168.0.8/29 → 10.0.0.2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NHRP table</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1 → 172.16.1.1</td>
</tr>
<tr>
<td>10.0.0.2 → 172.16.2.1</td>
</tr>
</tbody>
</table>

| Physical: 172.16.1.1 |
| Tunnel: 10.0.0.1 |

| Physical: 172.16.2.1 |
| Tunnel: 10.0.0.2 |

<table>
<thead>
<tr>
<th>NHRP table</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.254 → 172.16.254.1</td>
</tr>
<tr>
<td>10.0.0.2 → 172.16.2.1</td>
</tr>
<tr>
<td>192.168.0.8/29 → 172.16.2.1</td>
</tr>
</tbody>
</table>

Routing table
C 192.168.0.0/29 → Eth0
C 10.0.0.0 → Tunnel0
S 0.0.0.0/0 → Dialer0
D 192.168.0.0/16 → 10.0.0.254

Routing table
C 192.168.0.8/29 → Eth0
C 10.0.0.0 → Tunnel0
S0.0.0.0/0 → Dialer0
D 192.168.0.0/29 → 10.0.0.254

NHRP table
10.0.0.254 → 172.16.254.1
10.0.0.2 → 172.16.2.1
192.168.0.8/29 → 172.16.2.1

Resolution Reply
192.168.0.8/29 → 10.0.0.2 → 172.16.2.1

Hub
192.168.254.0/24

Spoke 1
192.168.0.0/29

Spoke 2
192.168.0.8/29

Physical: 172.16.254.1
Tunnel: 10.0.0.254

Physical: 172.16.2.1
Tunnel: 10.0.0.2

Routing table
C 192.168.0.0/29 → Eth0
C 10.0.0.0 → Tunnel0
S0.0.0.0/0 → Dialer0
D 192.168.0.0/29 → 10.0.0.254

Cisco live!
DMVPN phase 3 shortcuts (3)

Routing table
C 10.0.0.0 → Tunnel0
C 192.168.254.0/24 → Eth0
D 192.168.0.0/29 → 10.0.0.1
D 192.168.0.8/29 → 10.0.0.2

NHRP table
10.0.0.1 → 172.16.1.1
10.0.0.2 → 172.16.2.1

Physical: 172.16.254.1
Tunnel: 10.0.0.254

Spoke 1
192.168.0.0/29

NHRP table
10.0.0.254 → 172.16.254.1
10.0.0.2 → 172.16.2.1

Routing table
C 192.168.0.0/29 → Eth0
C 10.0.0.0 → Tunnel0
S 0.0.0.0/0 → Dialer0
D 192.168.0.0/16 → 10.0.0.254

Physical: 172.16.1.1
Tunnel: 10.0.0.1

Spoke 2
192.168.0.8/29

NHRP table
10.0.0.254 → 172.16.254.1
10.0.0.1 → 172.16.1.1

Routing table
C 192.168.0.8/29 → Eth0
C 10.0.0.0 → Tunnel0
S 0.0.0.0/0 → Dialer0
D 192.168.0.0/29 → 10.0.0.254

Physical: 172.16.2.1
Tunnel: 10.0.0.2

Hub
192.168.254.0/24
DMVPN phase 3 data packet forwarding

- **Route lookup** determines output interface and next-hop
  - The packet and next-hop are passed to the interface
  - Assuming the interface is NHRP enabled

- **Destination address** is looked up in the NHRP cache
  - If success, use entry to encapsulate

- **Next-hop address** is looked up in the NHRP cache
  - If success, use entry to encapsulate

- **Fallback**: send packet to configured NHS
  - Use NHS NHRP entry
  - Resolve next-hop address via resolution-request
DMVPN phase 3 resolution triggers

- If packet forwarding falls back to NHS
  - Issue resolution-request for next-hop address (/32)

- If router receives indirection-notification
  - Aka “NHRP Redirect”
  - Issue resolution-request for address in notification
  - A /32 address is looked-up
DMVPN phase 3 resolution forwarding

- **Address look up in NHRP cache**
  - If authoritative entry present, answer w/ entry
- **Otherwise lookup address in routing table (RIB)**
- **If next-hop belongs to same DMVPN**
  - i.e., nhrp network-id of next-hop same as incoming request
  - Treat found next-hop as NHS
  - Forward resolution-request to next-hop
- **If next-hop does not belong to DMVPN**
  - i.e. Network-id is different or interface not NHRP-enabled
  - Respond with full prefix found in routing table – maybe < /32
Phase 3 shortcuts (1) – ASR1K & 15.2T

Routing table
C 10.0.0.0 → Tunnel0
C 192.168.254.0/24 → Eth0
D 192.168.0.0/29 → 10.0.0.1
D 192.168.0.8/29 → 10.0.0.2

NHRP table
10.0.0.1 → 172.16.1.1
10.0.0.2 → 172.16.2.1

Physical:
172.16.1.1
Tunnel:
10.0.0.1

Indirection (192.168.0.9)

Physical:
172.16.254.0/24

NHRP table
10.0.0.254 → 172.16.254.1

Physical:
172.16.2.1
Tunnel:
10.0.0.2

Routing table
C 192.168.0.0/29 → Eth0
C 10.0.0.0 → Tunnel0
S 0.0.0.0/0 → Dialer0
D 192.168.0.0/16 → 10.0.0.254

Spoke 1
192.168.0.0/29

Spoke 2
192.168.0.8/29

Routing table
C 192.168.0.8/29 → Eth0
C 10.0.0.0 → Tunnel0
S 0.0.0.0/0 → Dialer0
D 192.168.0.0/29 → 10.0.0.254
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**

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)

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

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 isa sa

<table>
<thead>
<tr>
<th>dst</th>
<th>src</th>
<th>state</th>
<th>conn-id</th>
<th>slot</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.17.0.1</td>
<td>172.16.1.1</td>
<td>QM_IDLE</td>
<td>1082</td>
<td>0</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

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)

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

Packets are encrypted and sent to 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)

Packets are not encrypted sending out to 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-received 0
Pending Registration Requests:
Registration Request: Reqid 4371, Ret 64 NHS 172.17.0.1

How to Fix?

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

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 100000

Look for tunnel key in both hub and spoke
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

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

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

```
sh ip eigrp neighbors
IP-EIGRP neighbors for process 10
H  Address     Interface  Hold (sec) Uptime SRTT (ms) RTO   Q  Cnt Seq Num
1  10.0.0.1    Tu0        11  00:21:20 18  200  0   497
No request fail
```
Common Issues: Dynamic NBMA Address Change in Spoke Resulting Inconsistent NHRP Mapping in Hub

- **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 Resulting Inconsistent NHRP Mapping in Hub

How to Detect?
Inconsistency after 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

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
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

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

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

Old NBMA address
New NBMA address
Common Issues: Dynamic NBMA Address Change in Spoke Resulting Inconsistent NHRP Mapping in Hub

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 Resulting Inconsistent NHRP Mapping in Hub

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) request and reply packets
Common Issues: Dynamic NBMA Address Change in Spoke Resulting Inconsistent NHRP Mapping in Hub

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

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

Unique flag not set
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
  Collect spoke network routes from spokes
  Advertise spoke and local networks to all spokes

All Phases:
- Turn off split-horizon (EIGRP, RIP)
- Single area and no summarization when using OSPF

Phase 1 & 3:
- Hubs can not preserve original IP next-hop; Can Summarize
  - 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 summarize
  - EIGRP (no ip next-hop-self); BGP (default)
  - OSPF (network broadcast); Only 2 hubs

- Hubs are routing neighbors with other hubs and local network
  Phase 1 & 3: Can use different routing protocol than hub-spoke tunnels
  Phase 2: Must use same routing protocol as hub-spoke tunnels
Common Issues:

- Looking for a way to disable split tunneling in spoke router, so all traffic from spoke goes to Hub router even internet traffic but at the same time spoke to spoke traffic doesn’t go through hub.
Common Issues: No split tunneling on DMVPN spoke

Problem Description:

Customer has corporate security policies that disable split-tunneling 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.
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: No split tunneling 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: No split tunneling on DMVPN spoke DMVPN and I-VRF

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

```
Cisco IOS Router
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Global Routing Table</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>Cisco IOS Router</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>VRF Table</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
GRE Interface    |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Tunnel1</td>
</tr>
<tr>
<td>Ip vrf forwarding VRF-1</td>
</tr>
<tr>
<td>Tunnel source serial 0/0</td>
</tr>
<tr>
<td>Interface Serial0/0</td>
</tr>
<tr>
<td>description in global table</td>
</tr>
<tr>
<td>Interface FastEthernet 0/0</td>
</tr>
<tr>
<td>Ip vrf forwarding VRF-1</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>LAN Interface</td>
</tr>
</tbody>
</table>
```
Common Issues: No split tunneling on DMVPN spoke DMVPN 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: No split tunneling on DMVPN spoke
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: No split tunneling on DMVPN spoke
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
High Level Customer Network Topology

Spoke 1
192.168.1.0/24
Physical: 172.16.1.1
Tunnel: 10.0.0.1

Hub
192.168.254.254/24

Spoke 2
192.168.2.0/24
Physical: 172.16.2.1
Tunnel: 10.0.0.2

Hub2
192.168.254.253/24

Physical: 172.16.253.1
Tunnel: 10.0.0.253

Physical: 172.16.254.1
Tunnel: 10.0.0.254
“Users behind some spokes can’t reach any network other than the local LAN. Connectivity to the Data Center behind DMVPN HUB is not working. It was working yesterday – I did not change anything! 😊”
Problem 1– Checking IKE

spoke1# sh cry isa sa
IPv4 Crypto ISAKMP SA
dstsrc state conn-id slot status
172.16.254.1 172.16.2.1 QM_IDLE 1009 0 ACTIVE

Hub1# sh cry isa sa
IPv4 Crypto ISAKMP SA
dstsrc state conn-id slot status
172.16.254.1 172.16.2.1 QM_IDLE 1006 0 ACTIVE

Fact 1: IKE is up
Problem 1 – Checking IPsec SA’s

Fact 2: IPsec SA’s are negotiated

spoke1#sh cry ipsec sa
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 172.16.2.1
protected vrf: (none)
local  ident (addr/mask/prot/port): (172.16.2.1/255.255.255.255/47/0)
remote  ident (addr/mask/prot/port): (172.16.254.1/255.255.255.255/47/0)
current_peer 172.16.254.1 port 500
   PERMIT, flags={origin_is_acl,}

hub1#sh cry ipsec sa
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 172.16.254.1
protected vrf: (none)
local  ident (addr/mask/prot/port): (172.16.254.1/255.255.255.255/47/0)
remote  ident (addr/mask/prot/port): (172.16.2.1/255.255.255.255/47/0)
current_peer 172.16.2.1 port 500
   PERMIT, flags={origin_is_acl,}
Problem 1 – Checking NHRP

spoke1# sh ip nhrp nhs det
Legend: E=Expecting replies, R=Responding
Tunnel0: 10.0.0.253 E req-sent 14 req-failed 0 repl-recev 0

Hub1# sh ip nhrp 10.0.0.1
Hub1#

Fact3:
- Spoke NHRP registration missing on hub…
- Why ???
Problem 1 – ESP Encapsulation?

Fact 4:

- ESP packets are received on the hub
- The hub never seems to reply, though…
Problem 1 – Deeper into NHRP

```
hub1#clear ip nhrp counters interface tunnel 0
hub1#sh ip nhrp traffic
Tunnel0: Max-send limit:100Pkts/10Sec, Usage:0%
   Sent: Total 0
       0 Resolution Request  0 Resolution Reply  0 Registration Request
       0 Registration Reply  0 Purge Request  0 Purge Reply
       0 Error Indication  0 Traffic Indication

Rcvd: Total 5
       0 Resolution Request  0 Resolution Reply
       0 Registration Reply  5 Registration Request
       0 Purge Request  0 Purge Reply
       0 Error Indication  0 Traffic Indication
```

Fact 5:

- Hub receives registration requests
- Hub does not reply
- This looks like an NHRP protocol level issue
Problem 1 – NHRP Debugging

```plaintext
hub1#debug nhrp condition peer nbma 172.16.1.1
hub1#debug nhrp
NHRP protocol debugging is on
hub1#debug nhrp cache
NHRP cache operations debugging is on
hub1#debug nhrp error
NHRP errors debugging is on
hub1#sh deb
NHRP:
   NHRP protocol debugging is on
   NHRP cache operations debugging is on
   NHRP errors debugging is on
hub1#show nhrp debug-condition
NBMA addresses under debug are:
   172.16.1.1,
```

- **NHRP conditional debug:**
  - Enabling debug will let us see what hub does with the registration request.
  - Conditional debug makes it both readable and safe: we do not want hundreds of spokes NHRP debugs.
Problem 1 – Analyzing Debugs

- HUB1 receives the registration request
- It attempts to forward it to another address – but why?
- The protocol address in the packet is wrong:

  NHS on the spoke is not valid

DMVPN Hub
spoke1#sh run int tun0
!
interface Tunnel0
  ip address 10.0.0.1 255.255.255.0
  no ip redirects
  ip nhrp map multicast 172.16.254.1
  ip nhrp map 10.0.0.253 172.16.254.1
  ip nhrp network-id 100
  ip nhrp nhs 10.0.0.253
  tunnel source FastEthernet0/0
  tunnel mode gre multipoint
  tunnel protection ipsec profile prof0
end

Should have been 10.0.0.254

Did the config get changed somehow ?? !! Oh well 😊
“Everything was working till yesterday. Today some spokes are unable to reach the data center behind DMVPN Hub. “
Problem 2– Checking IKE

Fact 1: IKE is not coming up?

SPOKE1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
172.16.254.1 172.16.2.1 MM_KEY_EXCH 1003 ACTIVE
172.16.254.1 172.16.2.1 MM_NO_STATE 1002 ACTIVE (deleted)

Hub1# sh cry isa sa
IPv4 Crypto ISAKMP SA
dst src state conn-id slot status
172.16.254.1 172.16.2.1 QM_IDLE 1006 0 ACTIVE
Problem 2—Why is IKE failing?

SPOKE1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA

<table>
<thead>
<tr>
<th>dst</th>
<th>src</th>
<th>state</th>
<th>conn-id</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.254.1</td>
<td>172.16.2.1</td>
<td>MM_KEY_EXCH</td>
<td>1003</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>172.16.254.1</td>
<td>172.16.2.1</td>
<td>MM_NO_STATE</td>
<td>1002</td>
<td>ACTIVE (deleted)</td>
</tr>
</tbody>
</table>

12:27:40: ISAKMP (1003): received packet from 172.16.254.1 dport 500 sport 500 Global (I) MM_KEY_EXCH
12:27:40: ISAKMP:(1003): phase 1 packet is a duplicate of a previous packet.
12:27:40: ISAKMP:(1003): retransmitting due to retransmit phase 1
12:27:41: ISAKMP:(1003): retransmitting phase 1 MM_KEY_EXCH...
12:27:41: ISAKMP (1003): incrementing error counter on sa, attempt 3 of 5: retransmit phase

ISAKMP:(1004): processing CERT payload. message ID = 0

CRYPTO_PKI: Checking certificate revocation...
CRYPTO_PKI: Starting CRL revocation

GET /crls/myca.crl HTTP/1.0
CRYPTO_PKI: status = 65535: failed to send out the pki message
CRYPTO_PKI: Certificate validation failed

%CRYPTO-5-IKMP_INVAL_CERT: Certificate received from 172.16.2.1 is bad: CA request failed!
Problem 2 – Solution

- HTTP server where CRL (certificate revocation list) was stored was down.
- Fix was to restore the server
- Workaround: `revocation-check crl none`

Identified by one of following means:
- PKI debugs
- Embedded packet capture on router
- Debug ip packet `<acl>`
- External packet capture

“none” will bypass CRL revocation if CRL server is not reachable. Configure if your security policy allows it.
Problem 3

“The tunnel flaps constantly and no traffic is flowing from spoke to Hub.”
Hub1#sh ip eigrp neighbors
IP-EIGRP neighbors for process 1

<table>
<thead>
<tr>
<th>H</th>
<th>Address</th>
<th>Interface</th>
<th>Hold Uptime (sec)</th>
<th>SRTT (ms)</th>
<th>RTO</th>
<th>Q Cnt</th>
<th>Seq Num</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>10.0.0.1</td>
<td>Tu0</td>
<td>10 00:01:00</td>
<td>1</td>
<td>5000</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

Hub1#
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.0.0.1 (Tunnel0) is down: retry limit exceeded
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.0.0.1 (Tunnel0) is up: new adjacency
Hub1#

- The HUB sees an EIGRP neighbor (the spoke)
  - It does not stay up; it flaps
- No flap is visible on the spoke
- So this is not a tunnel flap but an EIGRP flap
spoke1#ping 10.0.0.254 (Hub’s tunnel ip)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/12 ms
spoke1#sh ip eigrp nei
IP-EIGRP neighbors for process 1

spoke1#sh ip nhrp
10.0.0.254/32 via 10.0.0.254, Tunnel0 created 00:18:22, never expire
  Type: static, Flags: used
  NBMA address: 172.16.254.1
spoke1#sh ip nhrp nhs
Legend: E=Expecting replies, R=Responding
Tunnel0: 10.0.0.254 RE

- The spoke does not have EIGRP neighbor ship with the hub
- NHRP looks ok on hub and spoke (NHS is “R” responding)
- ➔ IPsec/IKE are up, NHS configuration is OK
- Only EIGRP seems to be affected!
Problem 3 – The Solution

hub1# show run int tun0
!
interface Tunnel0
 ip address 10.0.0.254 255.255.255.0
 no ip redirects
 ip nhrp network-id 100
 ip nhrp map multicast dynamic
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel protection ipsec profile prof0
end

- EIGRP detects neighbors using multicast
- The hub lacked the dynamic multicast dynamic setting
- This means that multicast packets are not sent to spokes
- The 2 way multicast discovery could not happen

Allow multicast dynamic NHRP mapping on the HUB
“Everything seems to have been taken care of. But as soon I said that - I hear that some of spoke sites are losing EIGRP neighborship with the hub. But they come back up momentarily. Now what I do ?? 😊”
Problem 4 – Is it just EIGRP Flap or IPSEC also?

The Spoke and Hub both see an EIGRP neighbor flap for over 30 seconds

How can we confirm ipsec tunnel also flapped?

- Isakmp keepalives (DPD) on spoke - might explain a IPSEC issue?
- Crypto logging session

Customer enabled that there is indication of tunnel failure,

- but what’s the cause of it?? Connectivity, rekey, other??

%CRYPTO-5-SESSION_STATUS: Crypto tunnel is **DOWN**. Peer 172.16.254.1:500 Id: 172.16.254.1
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP. Peer 172.16.254.1:500 Id: 172.16.254.1
Problem 4 – EEM to the Rescue!

- EEM – Embedded Event Manager (Automation directly on your router)
- Troubleshoot Transient conditions (like network flaps) by monitoring and automation
- Take proactive actions based on configurable events

Check connectivity to Hub's Public/WAN IP addr from Spoke

```
ip sla 100
  icmp-echo 172.16.254.1 source-interface FastEthernet4
  frequency 5
ip sla schedule 100 life forever start-time now
```

**Send ping every 5 secs**

**track 100 ip sla 100**
- delay down 15 up 15

**event manager applet ipsla100down**
- event track 100 state down
- action 1.0 syslog msg "Public/WAN SLA probe failed!"

**event manager applet ipsla100up**
- event track 100 state up
- action 1.0 syslog msg "Public/WAN SLA probe came up!"

Detailed Example:
Problem 4 – And the Verdict Is?

Spoke1#
11:04:56: %HA_EM-6-LOG: ipsla100down: Public/WAN SLA probe failed!
11:04:58: %HA_EM-6-LOG: ipsla200down: Tunnel SLA probe failed!

Both ping probes failed which is indicative of an ISP Intermittent connectivity failure.

Spoke1#
11:05:27: %HA_EM-6-LOG: ipsla100up: Public/WAN SLA probe came up!
11:05:34: %HA_EM-6-LOG: ipsla200up: Tunnel SLA probe came up!

Solution – ISP worked to stabilize the circuits and issue not seen afterwards 😊
Troubleshooting Summary – Hub Perspective

- Do we receive traffic from the peer?
  - access-group in on the public interface with acl permit

- Do we have an IKE (ISAKMP) SA with the spoke?
  - show crypto isakmp sa (or show crypto session)

- Do we have an IPsec SA with the spoke?
  - show crypto ipsec sa peer <spoke public ip addr>

- Do we have a proper GRE layer (key is right?)
  - show run interface tunnel0 | incl key
  - show interface tunnel0 | incl GRE

- Do we have an NHRP cache for the spoke?
  - show ip nhrp <spoke tunnel ip addr>
Troubleshooting Summary – Spoke Perspective

- Do we have connectivity to the hub public ip ?
  - ping <hub public ip addr> source <tunnel source interface>

- Do we have an IKE (ISAKMP) SA ?
  - show crypto isakmp sa

- Do we have an IPsec SA ?
  - show crypto ipsec sa peer <Hub or other spoke ip >

- Do we have a proper GRE layer (key is right ?)
  - show run interface tunnel0 | incl key
  - show interface tunnel0 | incl GRE

- Do we have an NHRP cache / NHS registration ok ?
  - show ip nhrp, show ip nhrp nhs, sh ip nhrp traffic

For your reference
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

- **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)

  (Release 7): 3.9.0S (03.09.00.153-2.S), 3.4.2S (03.04.02.153-2.S)

- **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)M10, 15.1(4)M6, 15.1(3)T4

- **For 720x(NPE-G2+VSA): IOS 12.4 T-train:**
  
  IOS 12.4: 12.4(25)g, IOS 12.4 T-train: 12.4(15)T17, 12.4(24)T8
  
  IOS 15.0 Mainline: 15.0(1)M10, 15.1(4)M6

  IOS 15 S-train: 15.2(4)S2

- **For 89x,19xx,29xx,39xx:**
  
  IOS 15 Mainline/T-train: 15.0(1)M10, 15.1(4)M6, 15.1(2)T3, 15.2(2)T
Other Related sessions
Cisco Live 2013

- BRKSEC-3051: Troubleshooting GETVPN deployments.
- BRKSEC-2054: Deploying GET to Secure VPN.
- BRKSEC-4054: Advanced Concept of DMVPN.
- BRKSEC-1050: Are you choosing the right VPN for your network?
Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Cisco Daily Challenge points for each session evaluation you complete.
- Complete your session evaluation online now through either the mobile app or internet kiosk stations.

Maximize your Cisco Live experience with your free Cisco Live 365 account. Download session PDFs, view sessions on-demand and participate in live activities throughout the year. Click the Enter Cisco Live 365 button in your Cisco Live portal to log in.
Useful Links

DMVPN Design Guide

IOS IPSEC and IKE Troubleshooting

DMVPN Troubleshooting

Automation with EEM (Embedded Event Manager)
  • https://supportforums.cisco.com/community/netpro/network-infrastructure/eem (support community)
  • https://supportforums.cisco.com/community/netpro/network-infrastructure/eem (support community)
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