Demystifying DMVPN

Ranjana Jwalaniah (CCIE # 10246)
BRKSEC-3052
“The important thing is not to stop questioning. Curiosity has it’s own reason for existing”
Cisco Spark

Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

Cisco Spark spaces will be available until July 3, 2017.

cs.co/clus17/#BRKSEC-3052
Reference/Hidden Slides

They are mainly for your reference which can be used as needed.
There is an Appendix with additional reference information in the slide deck
Agenda

• Overview
• DMVPN Modules
  Common Issues
• Case Study
• Best Configuration Practices
• Q & A
DMVPN Overview
What is Dynamic Multipoint VPN?

DMVPN is Cisco’s IOS software solution to building GRE+IPSec VPN in an easy, dynamic and scalable manner.
Terminology and Features

- **Overlay Addresses**
  - **Core Network**: 192.168.128.0/17
  - **Networks**:
    - Spoke 1: 192.168.1.0/24
    - Spoke 2: 192.168.2.0/24
    - Hub 1: 192.168.101.0/24
    - Hub 2: 192.168.102.0/24

- **Tunnel Addresses**
  - **Spoke 1 to Hub 1**:
    - Tunnel: 10.0.0.101
    - Physical: 172.16.101.1
  - **Spoke 2 to Hub 2**:
    - Tunnel: 10.0.0.2
    - Physical: 172.16.2.1
  - **Spoke 1 to Hub 2**:
    - Tunnel: 10.0.0.102
    - Physical: 172.16.102.1

- **GRE/IPsec Tunnels**
- **On Demand Spoke Tunnels**
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 Implementation

Hub and spoke (Phase 1)

Spoke-to-spoke (Phase 2)

VRF-lite

Server Load Balancing

Hierarchical (Phase 3)

2547oDMVPN

Spoke-to-hub tunnels
Spoke-to-spoke tunnels
2547oDMVPN tunnels
STOP! ENABLE TIMESTAMPS!!

• Sync up the timestamps between the hub and spoke

• Enable msec debug and log timestamps
  
  service timestamps debug datetime msec
  service timestamps log datetime msec

• Enable terminal exec prompt timestamp for the debugging sessions. This way you can easily correlate the debug output with the show command output
DMVPN Modules

Modules
- Physical Layer
- Encryption—IPsec/IKEv1/IKEv2
- GRE/NHRP
- Routing—routing and IP data

Troubleshooting Approach
- Understand Interaction between Modules
- Identify the Problem Module
- Fix the Problem
DMVPN Modules: Physical Layer

Physical (NBMA or tunnel endpoint) routing

Responsible for routing of the tunnel creation packets and subsequent encrypted traffic between the tunnel endpoints.
(DMVPN hub and spoke or between spoke and spoke routers)
DMVPN Modules
Physical Layer

Ping from the spoke to the hub using the NBMA address (and reverse):
Traceroute to check the path of the encrypted tunnel packets
Embedded Packet Capture (EPC)

These pings should directly go through the physical interface and not the DMVPN tunnel interface to avoid recursive routing
DMVPN Modules
Physical Layer (Cont)

Debugs and show commands used if no connectivity

```
debug ip icmp
```

```
ICMP: echo reply rcvd, src 172.17.0.1, dst 172.16.1.1
ICMP: dst (10.120.1.0) port unreachable rcv from 10.120.1.15
ICMP: echo reply sent, src 172.17.0.1, dst 172.16.1.1
```

Debug icmp field descriptions:

DMVPN Modules
Physical Layer

Debugs and show commands used if no connectivity (cont.)

EPC

- monitor capture buffer <buffer-name>  filter access-list <acl-name>  max-size 1514
- monitor capture point ip cef <capture-name> <interface-name> both
- monitor capture point associate <capture-name> <buffer-name>
- monitor capture <capture-name> start
- monitor capture <capture-name> stop
- monitor capture <buffer-name> export <location>

Tool to generate EPC commands and decode the EPC captures
https://cway.cisco.com/tools/CaptureGenAndAnalyse/
DMVPN Modules
Physical Layer (Cont.)

Debugs and show commands used if no connectivity (cont.)

```
debug ip packet [access-list-number] [detail]
```

Forget the access-list if you want to try crashing the router!! 😊

```
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
```
DMVPN Modules
Physical Layer (Cont.)

Common Issues:
ACL in the firewall/ISP router block IKEv2 traffic
Traffic filtering resulting in unidirectional flows
Common Issues: 
ACL in Firewall/ISP Router Block IKE Traffic

Problem

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

How to detect?

```
show crypto ikev2 sa
IPv4 Crypto IKEv2 SA

<table>
<thead>
<tr>
<th>Tunnel-id</th>
<th>Local</th>
<th>Remote</th>
<th>fvrf/ivrf</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>172.16.1.1/500</td>
<td>172.17.0.1/500</td>
<td>none/none</td>
<td>IN-NEG</td>
</tr>
</tbody>
</table>

Encr: Unknown - 0, Hash: None, DH Grp:0, Auth sign: Unknown - 0, Auth verify: Unknown - 0
Life/Active Time: 86400/0 sec
```
Common Issues: ACL in Firewall/ISP Router Block IKEv2 Traffic

debug crypto ikev2

Jun 10 12:50:09.758: Generating IKE_SA_INIT message
Jun 10 12:50:09.758: IKEv2:(SA ID = 1):IKE Proposal: 1, SPI size: 0 (initial negotiation), Num. transforms: 4
  AES-CBC  SHA256  SHA256  DH_GROUP_1024_MODP/Group 2
Jun 10 12:50:09.758: IKEv2:(SA ID = 1):Sending Packet [To 172.17.0.1:500/From 172.16.1.1:500/VRF i0:f0]
Initiator SPI : 015D69B8458458AB - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
  SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP)
Jun 10 12:50:11.742: IKEv2:(SA ID = 1):Sending Packet [To 172.17.0.1:500/From 172.16.1.1:500/VRF i0:f0]
Initiator SPI : 015D69B8458458AB - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
  SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP)
Common Issues: ACL in Firewall/ISP Router Block IKEv2 Traffic

How to fix?

Check with the firewall / ISP admin to make sure they are allowing udp 500 traffic

```
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)
```

"permit ip any any" has to be configured as the last line of this ACL to ensure that all ingress traffic is allowed.

Inbound ACL on the egress interface
Check ACL log hit counts!!
Common Issues:
ACL in Firewall/ISP Side Block IKEv2 Traffic

show crypto ikev2 sa
Tunnel-id  Local          Remote         fvr/fvr    Status
1          172.17.0.1/500  172.16.1.1/500 none/none READY

Initiator SPI : 2A5247403E51BD37 - Responder SPI : 3D9179C80AAA8D0 Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE

Generating IKE_SA_INIT message

Jun 10 13:15:00.791: IKEv2:(SA ID = 1): Sending Packet [To 172.17.0.1:500/From 172.16.1.1:500/VRF i0:f0]
Jun 10 13:15:00.799: IKEv2:(SA ID = 1): Received Packet [From 172.17.0.1:500/To 172.16.1.1:500/VRF i0:f0]
Initiator SPI : 2A5247403E51BD37 - Responder SPI : 3D9179C80AAA8D0 Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE

Jun 10 13:15:00.807: IKEv2:(SA ID = 1): IKEV2 SA created; inserting SA into database. SA lifetime timer (86400 sec) started
Jun 10 13:15:00.807: IKEv2:(SA ID = 1): Session with IKE ID PAIR (172.17.0.1, 172.16.1.1) is UP
Common Issues:
Traffic Filtering resulting in unidirectional flows

Problem
Unable to pass data traffic across the tunnel

```
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)
```
Common Issues:
Traffic Filtering resulting in unidirectional flows

How to fix?
Ensure that ESP (IP 50) packets are being allowed from Spoke 2 to Spoke 1

```
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# 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: 316, #pkts_encrypt: 316,
#pkts_decaps: 300, #pkts_decrypt: 310,
```

Spoke 1 and Spoke 2 has encap and decaps, counters increment.
DMVPN Modules
Encryption

This layer encrypts/decrypts GRE tunnel packets
DMVPN Modules
Encryption

Tunnel Protection

The profile must be applied on the tunnel interface (on both hub and spoke)

```
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

```
Interface Tunnel0
   Ip address 10.0.0.1 255.255.255.0
   :
   tunnel source fast ethernet0/0
tunnel protection ipsec profile prof
```
DMVPN Modules
Encryption - Tunnel Protection Components

Transform set:

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

- IPSec Profile (in lieu of crypto map)

```
crypto ipsec profile <name>
  set transform-set <name of transform-set>
  set ikev2-profile <IKEv2 profile name>
```

IKEv2 specific configuration
DMVPN Modules
Encryption - Keepalive

IKEv1/v2 Keepalive (Only on spokes)

On-Demand Keepalive is preferred to Periodic

```
crypto ikev2 dpd keepalive <keepalive interval> <Retry interval> <on-demand|Periodic>
crypto ikev2 nat keepalive <interval>

crypto isakmp keepalive <keepalive interval> <Retry interval> <on-demand|Periodic>
crypto isakmp nat keepalive <interval>
```

Use “periodic” if there is a Firewall in the path

Gre Tunnel Keepalives are not supported in combination with Tunnel Protection
DMVPN Modules
Encryption - Show Commands

show crypto map

```
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
```

show crypto socket

```
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
```
DMVPN Modules
Encryption - Show Commands

Verify that IKEv1/v2 SAs and IPSec SAs between the NBMA addresses of the hub and spoke are being created

show crypto ikev2 sa detail
show crypto IPSec sa peer <NBMA-address-peer>

show crypto isakmp sa detail
show crypto IPSec sa peer <NBMA-address-peer>
### DMVPN Modules

### Encryption - Show Commands

<table>
<thead>
<tr>
<th>Tunnel-id</th>
<th>Local</th>
<th>Remote</th>
<th>fvrf/ivrf</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>172.17.0.1/500</td>
<td>172.16.1.1/500</td>
<td>none/none</td>
<td>READY</td>
</tr>
</tbody>
</table>

- **Encr:** AES-CBC, **keysize:** 128, **Hash:** SHA256, **DH Grp:** 2, **Auth sign:** PSK, **Auth verify:** PSK
- **Life/Active Time:** 86400/472 sec
**DMVPN Modules**
**Encryption - Show Commands**

```
Router# show crypto ipsec sa
interface: Ethernet0/3
  Crypto map tag: Tunnel1-head-0, 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
```
DMVPN Modules
Encryption - Show Commands

show crypto ipsec sa (contd)

**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
DMVPN Modules
Encryption - Show Commands

show dmvpn detail

A single command to display both the IKEv1/IKEv2 AND IPSec Status

Show dmvpn [ {interface <i/f>} | {vrf <vrf-name> } | {ipv4|ipv6 >} | {peer {nbma | tunnel } <ip-addr> } | {network <ip-addr> <mask>}} ]

[detail]

Prior to 15.x version, it does not show the remaining lifetime, use the IKEv2 and IPSec show commands

Introduced in 12.4(9)T
DMVPN Modules

Encryption - Show Commands

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 Network
--------  ------------  ----------------  ----  ------  ------  -----  ---------------
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
DMVPN Modules
Encryption - Show Commands

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

IKEv2 Session
Crypto Session status
Socket State
DMVPN Modules
Encryption - Debug Commands

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

- `debug crypto ikev2`
- `debug crypto ipsec`
- `debug crypto engine`

Use new command:
- `debug dmvpn detail crypto`

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>`

Introduced in 12.4(9)T
DMVPN Modules Encryption

Debug dmvpn detail

debug dmvpn

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

Introduced in 12.4(9)T
DMVPN Modules: Encryption - Debug Commands

depend dmvpn detail all (Cont.)

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.
DMVPN Modules: Encryption - Debug Commands (Cont.)

depth dmvpn detail all

- Debug tunnel protection
- Debug crypto socket
- Debug crypto ikev2
- Debug crypto IPsec
- Debug nhrp packet

**Socket State**: Open, Active

**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

**Local and Remote Proxy Id Created**
DMVPN Modules: Encryption - Debug Commands

diff dmvpn detail all (Cont.)

• IKEv2 negotiation

Generating IKE_SA_INIT message

... ...
... ...
Jun 10 13:15:00.791: IKEv2:(SA ID = 1): Sending Packet [To 172.17.0.1:500/From 172.16.1.1:500/VRF i0:f0]
Jun 10 13:15:00.799: IKEv2:(SA ID = 1): Received Packet [From 172.17.0.1:500/To 172.16.1.1:500/VRF i0:f0]
Initiator SPI: 2A5247403E51BD37 - Responder SPI: 3D91798C80AAA8D0 Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE

... ...
... ...
Jun 10 13:15:00.807: IKEv2:(SA ID = 1): IKEv2 SA created; inserting SA into database. SA lifetime timer (86400 sec) started
Jun 10 13:15:00.807: IKEv2:(SA ID = 1): Session with IKE ID PAIR (172.17.0.1, 172.16.1.1) is UP

IKE complete authentication
IKE negotiates to set up the inbound and outbound IP Security (IPsec) SA by searching for a matching transform set

```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).
........
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
DMVPN Modules
Encryption

Common Issues:
Incompatible IKEV2 Proposal
DMVPN Hub and Ezvpn server in same Router

Specific to IKEv1
Common Issues: Incompatible IKEv2 Proposal

If the configured IKE proposal does not match that of the remote peer, it fails IKE negotiation.

IKE Proposal from the Spoke does not match the Hub's configure proposal

---

IKEv2:(SA ID = 1):Verify SA init message
IKEv2:(SA ID = 1):Insert SA
IKEv2:Searching Policy with fvr0, local address 172.16.1.1
IKEv2:Found Policy 'pol1'
IKEv2:(SA ID = 1):Processing IKE_SA_INIT message
IKEv2:(SA ID = 1):Failed to find a matching policy
IKEv2:(SA ID = 1):Received Policies: Proposal 1: AES-CBC-128 SHA256 SHA256 DH_GROUP_1024_MODP/Group 2

..........

..........
IKEv2:(SA ID = 1):Failed SA init exchange
IKEv2:(SA ID = 1):Initial exchange failed

---

IKEv2:(SA ID = 1):Sending Packet [To 172.16.1.1:500/From 172.17.0.1:500/VRF i0:f0]
Initiator SPI : 9EC973276C9D03D9 - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP)
NOTIFY(NAT_DETECTION_DESTINATION_IP)
IKEv2:(SA ID = 1):Insert SA
IKEv2:(SA ID = 1):Received Packet [From 172.16.1.1:500/To 172.17.0.1:500/VRF i0:f0]
Initiator SPI : 9EC973276C9D03D9 - Responder SPI : 86BDD0FD1E4251C2 Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE
Payload contents:
NOTIFY(NO_PROPOSAL_CHOSEN)

..........
IKEv2:(SA ID = 1):Received no proposal chosen notify
IKEv2:(SA ID = 1):Failed SA init exchange
IKEv2:(SA ID = 1):Initial exchange failed

---

DMVPN Hub

DMVPN Spoke
Common Issues:
DMVPN Hub and EzVPN server in same Router

Problem Description:
DMVPN spokes unable to connect to the DMVPN Hub and EzVPN Server.

How to Detect?
Check isakmp status

<table>
<thead>
<tr>
<th>Show crypto isakmp sa</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Crypto ISAKMP SA</td>
</tr>
<tr>
<td>dst</td>
</tr>
<tr>
<td>172.17.0.1</td>
</tr>
<tr>
<td>172.17.0.1</td>
</tr>
</tbody>
</table>
Common Issues:
DMVPN Hub and Ezvpn server in same Router

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

Check existing configuration

crypto isakmp client configuration group vpnclient
text cisco123
text pool vpn
text acl 190
crypto ipsec transform-set t3 esp-3des esp-md5-hmac
crypto dynamic-map test 10
text 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
text ip address 172.17.0.1 255.255.255.252
crypto map test
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 terminates on the EzVPN group in this scenario

Separate EzVPN server and DMVPN configuration by using ISAKMP Profile.

Match EzVPN 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
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

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

Verifying...
### Common Issues:
DMVPN Hub and EzVPN server on same Router

**show 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>
</tbody>
</table>

**EzVPN profile matched for EzVPN clients**

**DMVPN Profile matched for DMVPN spokes**

Verify?
DMVPN Modules
GRE/NHRP

GRE Encapsulation/Decapsulation of the Data

After GRE Encapsulation

NHRP is transported over GRE
DMVPN Modules
GRE/NHRP

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 Module
GRE/NHRP — What Is NHRP

DMVPN Component-NHRP

NHRP is a resolution protocol and caches 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
Spoke Registration

Hub
192.168.254.0/24

NHRP table
10.0.0.1 → 172.16.1.1
10.0.0.2 → 172.16.2.1

Spoke 1
192.168.0.0/29

Physical: 172.16.1.1
Tunnel: 10.0.0.1

NHRP table
10.0.0.254 → 172.16.254.1

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

ip nhrp network-id 1
ip nhrp nhs 10.0.0.254 nbma 172.16.254.1 multicast
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

Physical: 172.16.1.1
Tunnel: 10.0.0.1

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

NHRP table
10.0.0.254 → 172.16.254.1

Physical: 172.16.1.1
Tunnel: 10.0.0.1

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

NHRP table
10.0.0.254 → 172.16.254.1

ip nhrp map multicast dynamic

ip nhrp nhs 10.0.0.254 nbma 172.16.254.1 multicast

IT DEPENDS: phase 2 or 3?
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: 172.16.254.1
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

Hub
192.168.254.0/24

ip nhrp redirect

ip ospf network point-to-multipoint
No ip split-horizon eigrp <as>

ip nhrp shortcut

ip ospf network point-to-multipoint

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

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

Hub
192.168.254.0/24

ip nhrp redirect

ip ospf network point-to-multipoint
No ip split-horizon eigrp <as>

ip nhrp shortcut

ip ospf network point-to-multipoint

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
DMVPN phase 3 (Spoke-Spoke Communication)

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
Physical: 172.16.2.1
Tunnel: 10.0.0.2
Physical: 172.16.254.1
Tunnel: 10.0.0.254

Hub
192.168.254.0/24

Spoke 1
192.168.0.0/29

Spoke 2
192.168.0.8/29

Routing table
C 10.0.0.0/29 → 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

NHRP table
10.0.0.1 → 172.16.1.1
10.0.0.2 → 172.16.2.1

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

NHRP table
10.0.0.254 → 172.16.254.1
DMVPN phase 3 (Spoke-Spoke Communication-contd.)

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 → 172.16.2.1
10.0.0.2 → 172.16.2.1

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

NHRP table
10.0.0.254 → 172.16.254.1
10.0.0.1 → 172.16.1.1

Physical: 172.16.254.0/24
Tunnel: 10.0.0.254

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
DMVPN phase 3 (Spoke-Spoke Communication-contd.)

Spoke 1
192.168.0.0/29

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

Physical: 172.16.254.1
Tunnel: 10.0.0.254

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

Physical: 172.16.2.1
Tunnel: 10.0.0.2

Physical: 172.16.2.54

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

Hub
192.168.254.0/24
Phase 3 (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: 172.16.254.1
Tunnel: 10.0.0.254

Hub
192.168.254.0/24

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

Indirection (192.168.0.0)

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

NHRP table
10.0.0.254 → 172.16.254.1

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

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 192.168.0.0/16 → 10.0.0.254
Phase 3 (2) – 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

Physical:
172.16.2.1
tunnel:
10.0.0.2

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
H 192.168.0.8/29 → 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 Modules: GRE/NHRP
Show commands

show ip nhrp <spoke-tunnel-ip-address>

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

If the 'created' timer is low and gets reset frequently then that means that the NHRP mapping entry is getting reset
DMVPN Modules: GRE/NHRP
Show Commands

```
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)
```

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

DMVPN Modules: GRE/NHRP

dbg dmvpn detail all

tunnel protection

crypto socket

crypto ikev2

crypto IPsec

tunnel protection

dbg nhrp packet

Tunnel protection starts again after IPSec Phase 2 came UP

Connection lookup id

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

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): Signaling 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): Signaling NHRP
DMVPN Modules: GRE/NHRP

debug dmvpn detail all

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

Syslog message:
%DMVPN-5-NHRP_NHS: Tunnel0 10.0.0.1 is UP

NHRP: Receive Registration Reply via Tunnel0 vrf 0, packet size: 124
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
DMVPN Modules: GRE/NHRP

Common Issues

NHRP Registration fails

Dynamic NBMA address change in spoke leading to inconsistent NHRP mapping in hub
Common Issues:
NHRP Registration Fails

Show crypto ikev2 sa
<table>
<thead>
<tr>
<th>Tunnel-id</th>
<th>Local</th>
<th>Remote</th>
<th>fvr/ivrf</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>172.16.1.1/500</td>
<td>172.17.0.1/500</td>
<td>none/none</td>
<td>READY</td>
</tr>
</tbody>
</table>

Life/Active Time: 86400/472 sec

Packets are encrypted and sent to hub

DMVPN Spoke

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: 154, #pkts encrypt: 154, #pkts digest: 154
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

DMVPN Spoke

Return Traffic is missing

DMVPN Hub

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: 0, #pkts encrypt: 154, #pkts digest: 154
#pkts decaps: 154, #pkts decrypt: 0, #pkts verify: 0

Decaps increment but no encap at the hub

DMVPN 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 30  req-failed 30  repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 4371, Ret 64  NHS 172.17.0.1

Check the tunnel key?

```
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
```

Typo in tunnel key on Spoke

Typo in tunnel key on Spoke
Common Issues: NHRP Registration Fails (Cont.)

show ip nhrp nhs detail
Legend: E=Expecting replies, R=Responding
Tunnel0: 10.0.0.1 RE req-sent 4 req-failed 0 repl-rev 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 encpas: 121, #pkts encrypt: 121, #pkts digest: 121
#pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118
Problem Description

Dynamic NBMA address change in spoke resulting inconsistent NHRP mapping in hub until NHRP registration with previous NBMA address expired
Common Issues: Dynamic NBMA Address Change in Spoke Resulting in incorrect NHRP Mapping in Hub

How to Detect?

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

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
Common Issues: Dynamic NBMA Address Change in Spoke Resulting in incorrect NHRP Mapping in Hub

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
  IKEv2 Profile: DMVPN
  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
  IKEv2 Profile: DMVPN
  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 old and new NBMA address of spoke
Common Issues: Dynamic NBMA Address Change in Spoke Resulting in incorrect NHRP Mapping in Hub

```
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)
```
Common Issues: Dynamic NBMA Address Change in Spoke Resulting in incorrect 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

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

Spoke does not set the “Unique” flag in the NHRP packets
Common Issues: Dynamic NBMA Address Change in Spoke Resulting in incorrect NHRP Mapping in Hub

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: 172.16.2.3
  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: 172.16.2.3
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: "nat ", reqid: 9462
  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

Hub# show 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: 172.16.2.3

"Unique" Flag not set

Verify?
DMVPN Modules: Routing

Dynamic routing protocol over DMVPN tunnel
Routing packets in/out of the p-p GRE and/or mGRE interfaces
DMVPN Modules: Routing

Regular IP network
IP routing updates and data packets traverse the same physical/logical links
Routing Protocol monitors the state of all links that data packets can use

DMVPN IP network
IP routing updates and IP multicast data packets only traverse the **hub-and-spoke tunnels**
Unicast IP data packets traverse both the **hub-and-spoke** and **on demand spoke-spoke** tunnels
Routing protocol doesn’t monitor the state of **on demand spoke-spoke** tunnels
DMVPN Modules: Routing

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>

Debug: Various debug commands depending on routing protocol
DMVPN Modules: Routing
Common Issues

A requirement to route all traffic from the spoke through the hub except for traffic between spokes
Common Issues: A requirement to route all traffic from the spoke through the hub except for traffic between spokes

Spoke to spoke tunnels need an ISP default route to reach other.

Default route over the Tunnel should not overwrite the ISP default route for spoke to spoke communication to work.

Virtual Routing and Forwarding (VRF) instance to handle both default routes.
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 Dual Default Routes

Since WAN interface is 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: A requirement to route all traffic from the spoke through the hub except for traffic between spoke (contd)

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

FVRF routing table Spoke-A

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

Global routing table Spoke-A

Verify?
Case Study
High Level Customer Network Topology

Spoke 1
192.168.1.0/24
NBMA: 172.16.1.1
Tunnel: 10.0.0.1

Spoke 2
192.168.2.0/24
NBMA: 172.16.254.1
Tunnel: 10.0.0.254

Hub 1
192.168.254.254/24
NBMA: 172.16.254.1
Tunnel: 10.0.0.254

Hub 2
192.168.254.253/24
NBMA: 172.16.253.1
Tunnel: 10.0.0.253

Hub 1
192.168.254.254/24
NBMA: 172.16.254.1
Tunnel: 10.0.0.254

Hub 2
192.168.254.253/24
NBMA: 172.16.253.1
Tunnel: 10.0.0.253

Spoke 2
192.168.2.0/24
NBMA: 172.16.2.1
Tunnel: 10.0.0.2

Spoke 1
192.168.1.0/24
NBMA: 172.16.1.1
Tunnel: 10.0.0.1
Problem 1

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.
Problem 1– Checking IKE

<table>
<thead>
<tr>
<th>spoke1# show crypto ikev2 sa</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel-id</td>
<td>Local</td>
</tr>
<tr>
<td>1</td>
<td>172.16.2.1/500</td>
</tr>
<tr>
<td>Life/Active Time:</td>
<td>86400/3622 sec</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hub1# show crypto ikev2 sa</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel-id</td>
<td>Local</td>
</tr>
<tr>
<td>1</td>
<td>172.16.254.1/500</td>
</tr>
<tr>
<td>Life/Active Time:</td>
<td>86400/3620 sec</td>
</tr>
</tbody>
</table>

Yay!!! IKE SA is up!! 😄
Problem 1 – Checking IPsec SA’s

spoke1# show crypto 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# show crypto 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,}

Yay!!! IPsec SA is up!! 😄
Problem 1 – Checking NHRP

spoke1# show ip nhrp nhs det

Legend: E=Expecting replies, R=Responding
Tunnel0: 10.0.0.253 E req-sent 14 req-failed 14 repl-recv 0

Hub1# show ip nhrp 10.0.0.1

Hub1#

Spoke’s NHRP registration has gone missing on the hub!!!
This is not good!! 😞
Problem 1 – ESP Encapsulation

spoke1# show crypto 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,}

        #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6
        #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

hub1# show crypto 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,}

        #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
        #pkts decaps: 6, #pkts decrypt: 0, #pkts verify: 0

Missing ESP packets on HUB and SPOKE 😞
Problem 1 – Deeper into NHRP

```
hub1# clear ip nhrp counters interface tunnel 0
hub1# show 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 5 Registration Request
  0 Registration Reply 0 Purge Request 0 Purge Reply
  0 Error indication 0 Traffic Indication
```

0 Registration Reply Sent!!!
5 Registration Request Received!!!

Weird NHRP behavior on Hub 😞
Problem 1 – NHRP Debugging

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# show debug
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 debugs to the rescue!! 😃
Problem 1 – Analyzing Debugs

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>*Mar 1</td>
<td>02:04:14.423</td>
<td>NHRP: Receive Registration Request via Tunnel0 vrf 0, packet size: 92</td>
</tr>
<tr>
<td>*Mar 1</td>
<td>02:04:14.423</td>
<td>NHRP: netid_in = 100, to_us = 0</td>
</tr>
<tr>
<td>*Mar 1</td>
<td>02:04:14.423</td>
<td>NHRP: Registration request is being forwarded</td>
</tr>
<tr>
<td>*Mar 1</td>
<td>02:04:14.423</td>
<td>NHRP: Finding next idb with in_pak id: 0</td>
</tr>
<tr>
<td>*Mar 1</td>
<td>02:04:14.427</td>
<td>NHRP: Attempting to send packet via DEST 10.0.0.253</td>
</tr>
<tr>
<td>*Mar 1</td>
<td>02:04:14.427</td>
<td>NHRP: Forwarding Registration Request via Tunnel0 vrf 0, packet size: 112</td>
</tr>
<tr>
<td>*Mar 1</td>
<td>02:04:14.427</td>
<td>src: 10.0.0.254, dst: 10.0.0.253</td>
</tr>
<tr>
<td>*Mar 1</td>
<td>02:04:14.427</td>
<td>NHRP: Encapsulation failed for destination 10.0.0.253 out Tunnel0</td>
</tr>
<tr>
<td>*Mar 1</td>
<td>02:04:14.427</td>
<td>NHRP: Attempting to send packet via DEST 10.0.0.1</td>
</tr>
<tr>
<td>*Mar 1</td>
<td>02:04:14.427</td>
<td>NHRP: Send Error Indication via Tunnel0 vrf 0, packet size: 252</td>
</tr>
<tr>
<td>*Mar 1</td>
<td>02:04:14.427</td>
<td>src: 10.0.0.254, dst: 10.0.0.1</td>
</tr>
<tr>
<td>*Mar 1</td>
<td>02:04:14.427</td>
<td>NHRP: Encapsulation failed for destination 10.0.0.1 out Tunnel0</td>
</tr>
</tbody>
</table>

Why is Hub1 forwarding it to another NHS Server?
Problem 1 – Solution

```bash
spoke1# show 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 10.0.0.254 172.16.254.1
 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
```

NHS should have been 10.0.0.254

Self learning spokes or magic? 😊
Problem 2

The users behind all spokes are suddenly unable to reach the data center behind DMVPN Hub
Problem 2– Checking IKE

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# show crypto isakmp sa
IPv4 Crypto ISAKMP SA

dst src state conn-id status
172.16.2.1 172.16.254.1 MM_KEY_EXCH 1003 ACTIVE

IKE is not coming up 😞
Problem 2– Why is IKE failing?

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)

SPOKE1#debug crypto ikev2
IKEv2:(SA ID = 3):[IKEv2 -> PKI] Validating certificate chain
IKEv2:(SA ID = 3):[PKI -> IKEv2] Validation of certificate chain FAILED
IKEv2-ERROR:: Negotiation context locked currently in use
%PKI-3-SOCKETSELECT: Failed to select the socket.
IKEv2:(SESSION ID = 3788,SA ID = 3):Verify cert failed
IKEv2:(SESSION ID = 3788,SA ID = 3):Verification of peer’s authentication data FAILED

ISAKMP:(1004): processing CERT payload. message ID = 0
CRYPTO_PKI: Checking certificate revocation…
CRYPTO_PKI: Starting CRL revocation
CRYPTO_CS: write SCEP: unregistered and unbound service SCEP_WRTE_DB
CRYPTO_PKI_SCEP: CS Sending CRL in CertRep response (3646)
CRYPTO_CS: msg not sent due to HTTP server error: 2, bytes sent: 0
CRYPTO_CS: CRL not sent due to HTTP server error

certificate / signature payload (MM5 packet) failure
Certificate Issue ??

debug crypto isakmp
debug crypto pki messages
debug crypto pki transaction
debug crypto pki validation
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`

Time to go shopping for a new server!! 😊
Problem 3

The tunnel flaps constantly and no traffic is flowing from spoke to Hub.
Problem 3 – What is Really Flapping?

Hub1# show 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</th>
<th>Seq</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

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
Problem 3 – Drilling Down on the Spoke

spoke1# ping 10.0.0.254
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 neighbor
IP-EIGRP neighbors for process 1

spoke1# show 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# show 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 interface Tunnel0
!
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

This meant that multicast packets were not sent to spokes
The 2 way multicast discovery failed
Problem 4

All problems resolved, it’s a Friday – exciting weekend plans! 😊
The phone starts ringing 😞
EIGRP neighbor relationship bouncing intermittently on some spokes.
Problem 4 – Is it EIGRP and/or IPSEC flap?

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

How can we confirm ipsec tunnel also flapped?

- IKEv2 Keepalives (DPD)
- Logging Crypto session

What Next??
Problem 4 – EEM to the Rescue!

EEM – Embedded Event Manager

**Check connectivity to Hub’s Public/WAN IP 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`
- `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!"

**Check connectivity to Hub’s tunnel IP from spoke**

- `ip sla 200`
  - `icmp-echo 10.0.0.254` source-interface Tunnel0
  - frequency 5
- `ip sla schedule 200 life forever start-time now`
- `track 200 ip sla 200`
  - delay down 15 up 15
- `event manager applet ipsla200down`
  - event track 200 state down
  - action 1.0 syslog msg "Tunnel SLA probe failed!"
- `event manager applet ipsla200up`
  - event track 200 state up
  - action 1.0 syslog msg "Tunnel SLA probe came up!"

Send ping every 5 sec

Will only trigger when 3 consecutive pings fail

Syslog when tracked object goes up or down

Problem 4 – The Solution!

Hub1#
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!

Ping probes failing indicates intermittent connectivity issues to the ISP

Hub1#
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!

ISP worked to stabilize the circuits and issue not seen afterwards

ISP to the Rescue!!!!
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}}
- crypto ikev2 dpd interval retry-interval {on-demand | periodic} (GRE tunnel keepalives are not supported)
Complete Your Online Session Evaluation

• Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 gift card.

• Complete your session surveys through the Cisco Live mobile app or on www.CiscoLive.com/us.

Don’t forget: Cisco Live sessions will be available for viewing on demand after the event at www.CiscoLive.com/Online.
Other Related sessions

BRKSEC-4054  :  Advanced Concept of DMVPN

LABIOT-2012  :  Implementing Dynamic Multipoint VPN

BRKSEC-3001  :  Advanced IKEv2 Protocol
Thank you
You're it

Cisco live!
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 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.
“Static” Spoke-Hub, Hub-Hub Tunnels

Requirements

- **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
Dynamic Spoke-Spoke Tunnels
Requirements

• 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 created as needed

• 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>
DMVPN Modules
DMVPN Modules
Encryption - 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
  ```
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
Common Issues: No split tunneling on DMVPN spoke

DMVPN and F-VRF

IPSec+GRE

Cisco IOS Router

Global Routing Table

LAN Interface

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

IPSec packets are forwarded using VRF routing table
GRE decapsulated clear-text packets are forwarded using global table
DMVPN Modules: GRE/NHRP
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
DMVPN Modules: GRE/NHRP
Adding NHRP Cache

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 Modules: GRE/NHRP

Initial NHRP Cache

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 Modules: GRE/NHRP
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
DMVPN Modules: GRE/NHRP

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
Hub & Spoke design

Routing table
C 10.0.0.0 → Tunnel0
C 192.168.254.0 → Eth0
D 192.168.0.254/29 → 10.0.0.1
D 192.168.0.254/29 → 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

NHRP table
10.0.0.254 → 172.16.254.1

Physical: 172.16.1.1
Tunnel: 10.0.0.1

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 → 10.0.0.0/254

Hub via transport network

192.168.0.0/16 encrypted & tunneled to hub

ip ospf network point-to-multipoint

No ip split-horizon eigrp <as>

ip ospf network point-to-multipoint

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public

BRKSEC-3052
DMVPN phase 2 design

Hub advertises back individual prefixes pointing to corresponding spoke.

**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

**Physical:** 172.16.254.1
**Tunnel:** 10.0.0.254

**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 192.168.0.0/24 → Eth0
- C 10.0.0.0 → Tunnel0
- S 0.0.0.0/0 → Dialer0
- D 192.168.0.0/29 → 10.0.0.1

**Routing table**
- C 192.168.0.0/24 → Eth0
- C 10.0.0.0 → Tunnel0
- S 0.0.0.0/0 → Dialer0
- D 192.168.0.0/29 → 10.0.0.1

Lots of individual prefixes

Tunnels via transport network

For your reference:
- BRKSEC-3052
- 134
DMVPN phase 2 (2) (Spoke-Spoke Communication)

### 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:** 172.16.254.0/24
- **Tunnel:** 10.0.0.254

### 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
- 10.0.0.1 → 172.16.1.1

### NHRP Table
- 10.0.0.254 → 172.16.254.1
- 10.0.0.1 → 172.16.1.1

### 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

### 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
DMVPN phase 2 (1) (Spoke-Spoke Communication)

**Routing table**
- C 10.0.0.0 → Tunnel0
- C 192.168.254.0/24 → Eth0
- D 192.168.0.29 → 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
- 172.16.254.1

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

**NHRP table**
- 10.0.0.254 → 172.16.254.1
- 10.0.0.2 → 172.16.254.1

**Spoke 1**
- 192.168.0.0/29
- 10.0.0.1

**Spoke 2**
- 192.168.0.8/29
- 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 192.168.0.8/29 → 10.0.0.2

**Hub**
- 192.168.254.0/24

**Physical:**
- 172.16.254.1
- 172.16.2.1

**Tunnel:**
- 10.0.0.254

**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
- S 0.0.0.0/0 → Dialer0
- D 192.168.0.0/29 → 10.0.0.1
DMVPN phase 3 design

Hub advertises back summary prefix pointing to hub.

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

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
10.0.0.1 -> 172.16.1.1
10.0.0.2 -> 172.16.2.1

NHRP table
10.0.0.254 -> 172.16.254.1

Physical: 172.16.254.1
Tunnel: 10.0.0.254

Physical: 172.16.254.1
Tunnel: 10.0.0.2

Physical: 172.16.1.1
Tunnel: 10.0.0.1

Physical: 172.16.2.1
Tunnel: 10.0.0.2

192.168.0.0/16 summary tunneled to hub

Hub
192.168.254.0/24

Spoke 1
192.168.0.0/29

Spoke 2
192.168.0.8/29

Tunnels via transport network
DMVPN Modules: GRE/NHRP

Debugs

Nhrp debug commands

debug nhrp condition peer <nbma|tunnel>
debug nhrp
debug tunnel protection
debug crypto socket

debugs to show communication between NHRP and IPsec
DMVPN Modules: 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
DMVPN and I-VRF

- 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 serial 0/0

Interface Serial0/0
description in global table

Interface FastEthernet 0/0
ip vrf forwarding VRF-1
```
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
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 ikev2 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 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 ikev2 sa

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

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

DMVPN Design Guide


IOS IPSEC and IKE Troubleshooting


Automation with EEM (Embedded Event Manager)


https://supportforums.cisco.com/search/site/EEM?f[0]=sm_og_group_ref%3Anode%3A5941