DMVPN with IPsec – Enterprise WAN Lab Documentation

1. Project Overview

This project documents the design, implementation, and verification of a **secure enterprise WAN** using **Dynamic Multipoint VPN (DMVPN) with IPsec**. The lab is built to reflect real-world enterprise requirements such as scalability, high availability, secure communication, and simplified branch deployment.

The topology uses a **multi-hub, multi-spoke architecture**, allowing branches (spokes) to dynamically connect to central sites (hubs) while maintaining encrypted communication over an untrusted network.

---

2. Objectives

The main objectives of this lab are:

- Design a scalable WAN using DMVPN
- Secure all tunnel traffic using IPsec
- Implement multiple hubs for redundancy and failover
- Enable dynamic spoke registration using NHRP
- Run a dynamic routing protocol over the DMVPN tunnels
- Verify hub-and-spoke and spoke-to-spoke communication
- Understand real-world DMVPN behavior and troubleshooting considerations

---

3. Network Topology Description

3.1 Logical Design

- **Hubs**: Central routers acting as DMVPN hubs, providing connectivity and redundancy
- **Spokes**: Remote branch routers dynamically connecting to hubs
- **Transport Network**: Simulated public network representing the Internet

The design follows a **hub-and-spoke model** with support for **dynamic spoke-to-spoke tunnels**.

3.2 Role of Each Component

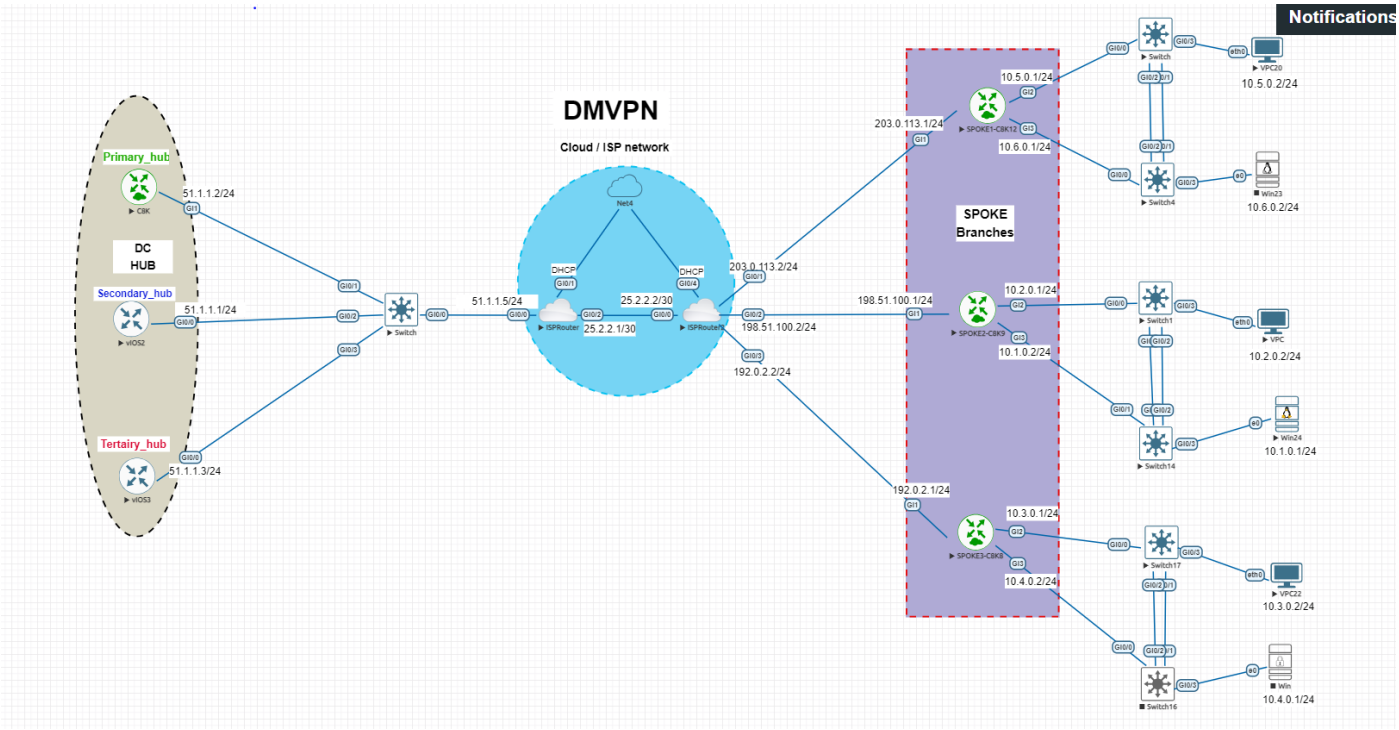
- **Hub Routers**:
    - Act as NHRP servers (NHS)
    - Maintain tunnel reachability information

- Provide initial forwarding path for spoke-to-spoke traffic

- **Spoke Routers**:
  - Register dynamically with the hubs
  - Form GRE tunnels protected by IPsec
  - Use dynamic routing to reach other sites

3.3 Network Diagram

The diagram below illustrates the logical layout of the DMVPN topology, including hub routers, spoke routers, transport network, and tunnel relationships. It provides a high-level view of connectivity and redundancy within the WAN design.



---

4. DMVPN Architecture

4.1 DMVPN Overview

DMVPN allows the creation of dynamic GRE tunnels between sites without the need for static point-to-point tunnel configuration. This significantly reduces administrative overhead in large WAN deployments.

Key DMVPN components used in this lab:

- **mGRE (Multipoint GRE)**
- **NHRP (Next Hop Resolution Protocol)**
- **Dynamic Routing Protocol**

4.2 DMVPN Phase Selection

This lab is designed around **DMVPN Phase 3**, which provides:

- Dynamic spoke-to-spoke tunnels
- Optimized routing paths
- Improved scalability compared to Phase 1 and Phase 2

---

5. NHRP Design

5.1 Purpose of NHRP

NHRP enables spokes to dynamically discover the public (NBMA) addresses of hubs and other spokes. This allows dynamic tunnel creation without manual mapping.

5.2 NHRP Roles

- **Hubs** act as NHRP servers
- **Spokes** act as NHRP clients and register with hubs

5.3 Redirect and Shortcut Behavior

- **NHRP Redirect (Hub)**: Informs spokes of better paths for spoke-to-spoke traffic
- **NHRP Shortcut (Spoke)**: Allows spokes to establish direct tunnels after receiving redirect messages

---

6. IPsec Security Design

6.1 Purpose of IPsec

IPsec is used to:

- Encrypt all GRE tunnel traffic
- Ensure data confidentiality and integrity
- Protect communication over untrusted networks

6.2 IPsec Implementation Approach

- GRE tunnels are protected using IPsec profiles

- A consistent security policy is applied across hubs and spokes
- Tunnel protection ensures that all routing and data traffic is encrypted

---

7. Routing Protocol Design

7.1 Routing Protocol Selection

A dynamic routing protocol is deployed over the DMVPN tunnels to:

- Automatically advertise branch networks
- Support redundancy and failover
- Simplify route management

7.2 Routing Design Considerations

- Single autonomous system across hubs and spokes
- Hub-based route aggregation for scalability
- Prevention of routing loops and instability

---

8. High Availability and Redundancy

8.1 Multi-Hub Design

Multiple hubs are deployed to provide:

- Redundant entry points into the WAN
- Improved availability if one hub fails
- Load distribution possibilities

8.2 Hub Preference and Failover

Spokes are configured to:

- Prefer a primary hub under normal conditions
- Automatically fail over to secondary hubs
- Maintain connectivity without manual intervention

---

9. Traffic Flow Explanation

9.1 Hub-and-Spoke Traffic

- Initial traffic between spokes flows through the hub
- The hub acts as a control point for tunnel resolution

9.2 Spoke-to-Spoke Traffic Optimization

- After initial communication, NHRP redirect messages are sent
- Spokes dynamically establish direct tunnels
- Traffic bypasses the hub, improving latency and efficiency

---

10. Verification and Validation

10.1 Connectivity Verification

Verification includes:

- Hub-to-spoke reachability
- Spoke-to-spoke communication
- End-to-end application traffic flow

10.2 Control Plane Verification

Key checks include:

- Tunnel status
- NHRP registration tables
- Routing protocol neighbor relationships
- IPsec security associations

10.3 Tunnel and NHRP Verification

#show dmvpn

This command displays a combined high-level view of the DMVPN control plane. It pulls information from NHRP, tunnel interfaces and routing behavior into one output, showing DMVPN status at a glance as seen in the figure 2 below.

R1

```
HUB1(config-if)#
*Jan  2 12:57:24.886: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.16.123.13 (Tunnel0) is resync:
split horizon changed
*Jan  2 12:57:24.887: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.16.123.11 (Tunnel0) is resync:
split horizon changed
*Jan  2 12:57:24.891: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.16.123.10 (Tunnel0) is resync:
split horizon changed
HUB1(config-if)#end
HUB1#
*Jan  2 13:00:29.238: %SYS-5-CONFIG_I: Configured from console by console
HUB1#sh dm
HUB1#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Hub, NHRP Peers:3,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 203.0.113.1       172.16.123.10    UP 03:08:25     D
     1 198.51.100.1      172.16.123.11    UP 03:07:09     D
     1 192.0.2.1         172.16.123.13    UP 00:20:29     D

HUB1#show ip nhrp
172.16.123.10/32 via 172.16.123.10
   Tunnel0 created 03:09:28, expire 00:08:28
   Type: dynamic, Flags: registered nhop
   NBMA address: 203.0.113.1
172.16.123.11/32 via 172.16.123.11
   Tunnel0 created 03:08:11, expire 00:08:13
   Type: dynamic, Flags: registered nhop
   NBMA address: 198.51.100.1
172.16.123.13/32 via 172.16.123.13
   Tunnel0 created 00:21:31, expire 00:08:38
   Type: dynamic, Flags: registered nhop
   NBMA address: 192.0.2.1
HUB1#
```

#show ip nhrp

The following command confirms successful NHRP registration between hubs and spokes.

SPOKE1

```
SPOKE1#
SPOKE1#sh ip nhrp
10.5.0.0/24 via 172.16.123.10
   Tunnel0 created 00:10:23, expire 00:02:53
   Type: dynamic, Flags: router unique local
   NBMA address: 203.0.113.1
    (no-socket)
172.16.123.1/32 via 172.16.123.1
   Tunnel0 created 03:51:30, never expire
   Type: static, Flags: used
   NBMA address: 51.1.1.2
172.16.123.11/32 via 172.16.123.11
   Tunnel0 created 00:10:23, expire 00:00:28
   Type: dynamic, Flags: router implicit nhop
   NBMA address: 198.51.100.1
172.16.123.13/32 via 172.16.123.13
   Tunnel0 created 00:07:56, expire 00:02:53
   Type: dynamic, Flags: router implicit nhop
   NBMA address: 192.0.2.1
SPOKE1#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:3,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 51.1.1.2          172.16.123.1    UP 00:44:42     S
     1 198.51.100.1      172.16.123.11    UP 00:10:33     D
     1 192.0.2.1         172.16.123.13    UP 00:08:06     D
```

10.5 IPsec Verification

This output confirms that IPsec security associations are established and actively encrypting tunnel traffic**.**

R1

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/161/262 ms
HUB1#ping 10.3.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/63/78 ms
HUB1#
HUB1#
HUB1#show cr
HUB1#show cry
HUB1#show crypto is
HUB1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
203.0.113.1     51.1.1.2        QM_IDLE           1002 ACTIVE
51.1.1.2        192.0.2.1       QM_IDLE           1004 ACTIVE
51.1.1.2        203.0.113.1     QM_IDLE           1001 ACTIVE
51.1.1.2        198.51.100.1    QM_IDLE           1003 ACTIVE

IPv6 Crypto ISAKMP SA

HUB1#show crypto engine connections active
Crypto Engine Connections

   ID  Type    Algorithm           Encrypt  Decrypt LastSeqN IP-Address
    3  IPsec   AES256+SHA512             0        0        0 51.1.1.2
    4  IPsec   AES256+SHA512             0        0        0 51.1.1.2
    5  IPsec   AES256+SHA512             0      377      377 51.1.1.2
    6  IPsec   AES256+SHA512           383        0        0 51.1.1.2
    7  IPsec   AES256+SHA512             0        4        4 51.1.1.2
    8  IPsec   AES256+SHA512             1        0        0 51.1.1.2
    9  IPsec   AES256+SHA512             0      266      266 51.1.1.2
   10  IPsec   AES256+SHA512           274        0        0 51.1.1.2
   13  IPsec   AES256+SHA512             0      169      169 51.1.1.2
   14  IPsec   AES256+SHA512           174        0        0 51.1.1.2
 1001  IKE     SHA512+AES256             0        0        0 51.1.1.2
 1002  IKE     SHA512+AES256             0        0        0 51.1.1.2
 1003  IKE     SHA512+AES256             0        0        0 51.1.1.2
 1004  IKE     SHA512+AES256             0        0        0 51.1.1.2
```

R1

```
HUB1#show crypto map
        Interfaces using crypto map NiStTeSt1:

Crypto Map IPv4 "Tunnel0-head-0" 65536 ipsec-isakmp
        Profile name: MY-IPSEC-PROFILE
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                dobre-SET:  { esp-256-aes esp-sha512-hmac  } ,
        }

Crypto Map IPv4 "Tunnel0-head-0" 65539 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 203.0.113.1
        Extended IP access list
            access-list  permit gre host 51.1.1.2 host 203.0.113.1
        Current peer: 203.0.113.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                dobre-SET:  { esp-256-aes esp-sha512-hmac  } ,
        }

Crypto Map IPv4 "Tunnel0-head-0" 65540 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 198.51.100.1
        Extended IP access list
            access-list  permit gre host 51.1.1.2 host 198.51.100.1
        Current peer: 198.51.100.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                dobre-SET:  { esp-256-aes esp-sha512-hmac  } ,
        }

Crypto Map IPv4 "Tunnel0-head-0" 65541 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 192.0.2.1
        Extended IP access list
            access-list  permit gre host 51.1.1.2 host 192.0.2.1
        Current peer: 192.0.2.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
```

R1

```
HUB1#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 51.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (51.1.1.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.0.2.1/255.255.255.255/47/0)
   current_peer 192.0.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 186, #pkts encrypt: 186, #pkts digest: 186
    #pkts decaps: 181, #pkts decrypt: 181, #pkts verify: 181
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 51.1.1.2, remote crypto endpt.: 192.0.2.1
     plaintext mtu 1442, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0
/0
     current outbound spi: 0xFBB79D6(263944662)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xC5F98A93(3321465491)
        transform: esp-256-aes esp-sha512-hmac ,
        in use settings ={Transport, }
        conn id: 13, flow_id: SW:13, sibling_flags 80004000, crypto map: Tunnel0
-head-0
        sa timing: remaining key lifetime (k/sec): (4266586/2942)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xFBB79D6(263944662)
        transform: esp-256-aes esp-sha512-hmac ,
        in use settings ={Transport, }
        conn id: 14, flow_id: SW:14, sibling_flags 80004000, crypto map: Tunnel0
-head-0
        sa timing: remaining key lifetime (k/sec): (4266585/2942)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
```

10.6 End-to-End Traffic Validation

- Initial traffic path
- Optimized path after DMVPN shortcut

VPC20

```
Press '?' to get help.

VPCS> ip 10.5.0.2 255.255.255.0 10.5.0.1
Checking for duplicate address...
VPCS : 10.5.0.2 255.255.255.0 gateway 10.5.0.1

VPCS> save
Saving startup configuration to startup.vpc
.  done

VPCS> ping 51.1.1.2

84 bytes from 51.1.1.2 icmp_seq=1 ttl=254 time=73.350 ms
84 bytes from 51.1.1.2 icmp_seq=2 ttl=254 time=234.811 ms
84 bytes from 51.1.1.2 icmp_seq=3 ttl=254 time=76.573 ms
84 bytes from 51.1.1.2 icmp_seq=4 ttl=254 time=145.302 ms
84 bytes from 51.1.1.2 icmp_seq=5 ttl=254 time=166.258 ms

VPCS> ping 10.2.0.2

84 bytes from 10.2.0.2 icmp_seq=1 ttl=61 time=748.652 ms
84 bytes from 10.2.0.2 icmp_seq=2 ttl=61 time=243.803 ms
84 bytes from 10.2.0.2 icmp_seq=3 ttl=61 time=252.094 ms
84 bytes from 10.2.0.2 icmp_seq=4 ttl=61 time=314.886 ms
84 bytes from 10.2.0.2 icmp_seq=5 ttl=61 time=236.269 ms

VPCS> ping 10.3.0.2

10.3.0.2 icmp_seq=1 timeout
84 bytes from 10.3.0.2 icmp_seq=2 ttl=61 time=655.600 ms
84 bytes from 10.3.0.2 icmp_seq=3 ttl=61 time=162.202 ms
84 bytes from 10.3.0.2 icmp_seq=4 ttl=61 time=247.829 ms
84 bytes from 10.3.0.2 icmp_seq=5 ttl=61 time=171.803 ms

VPCS> ping 10.3.0.2

84 bytes from 10.3.0.2 icmp_seq=1 ttl=61 time=207.231 ms
84 bytes from 10.3.0.2 icmp_seq=2 ttl=61 time=488.465 ms
84 bytes from 10.3.0.2 icmp_seq=3 ttl=61 time=533.086 ms
84 bytes from 10.3.0.2 icmp_seq=4 ttl=61 time=113.111 ms
84 bytes from 10.3.0.2 icmp_seq=5 ttl=61 time=215.242 ms

VPCS>
```

SPOKE1

```
SPOKE1#traceroute 10.2.0.2 source 10.5.0.1
Type escape sequence to abort.
Tracing the route to 10.2.0.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.123.1 318 msec 345 msec 118 msec
  2 172.16.123.11 453 msec 125 msec 192 msec
  3 10.2.0.2 311 msec 365 msec 194 msec
SPOKE1#traceroute 10.2.0.2 source 10.5.0.1
Type escape sequence to abort.
Tracing the route to 10.2.0.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.123.1 483 msec 410 msec 107 msec
  2 172.16.123.11 273 msec 173 msec 366 msec
  3 10.2.0.2 860 msec 278 msec 430 msec
SPOKE1#traceroute 10.3.0.2 source 10.5.0.1
Type escape sequence to abort.
Tracing the route to 10.3.0.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.123.1 205 msec 54 msec 56 msec
  2 172.16.123.13 111 msec 92 msec 125 msec
  3 10.3.0.2 110 msec 92 msec 67 msec
SPOKE1#
SPOKE1#
```

---

11. Troublesbleshooting, Challenges, and Observations

This lab intentionally exposed several real-world challenges commonly encountered in enterprise DMVPN deployments. Addressing these issues required structured troubleshooting and a deep understanding of control-plane behavior.

11.1 Challenges Faced

EIGRP Adjacency Instability (Flapping):
When EIGRP was enabled simultaneously on multiple DMVPN hubs, neighbor relationships between hubs and spokes became unstable. Adjacencies would repeatedly form and tear down, particularly with secondary and tertiary hubs.

DMVPN Phase 3 Shortcut Behavior:
Despite correct configuration of ip nhrp redirect on hubs and ip nhrp shortcut on spokes, dynamic spoke-to-spoke shortcuts did not always install as expected. In some cases, shortcuts were not visible even though end-to-end connectivity was functional.

Multi-Hub Complexity:
Introducing multiple hubs significantly increased design complexity. Static NHRP mappings, routing protocol behavior, and tunnel resolution order had a direct impact on stability and optimization.

11.2 Troubleshooting and Isolation Process

To isolate issues effectively, a methodical troubleshooting approach was followed:

- Verified tunnel status and basic connectivity before investigating routing or NHRP

- Confirmed NHRP registrations and hub/spoke roles using DMVPN and NHRP verification commands
- Isolated routing behavior by temporarily removing EIGRP from secondary and tertiary hubs
- Validated traffic paths to confirm whether traffic was transiting hubs as expected
- Incrementally reintroduced features to identify the specific causes of instability

This step-by-step isolation strategy made it possible to distinguish between tunnel issues, routing protocol behavior, and DMVPN phase-related behavior.

11.3 Key Lessons Learned

Several important real-world lessons emerged from this lab:

- Multi-hub DMVPN designs require intentional routing control; routing protocols do not inherently understand hub preference
- DMVPN Phase 3 optimization depends on dynamic NHRP behavior and correct traffic flow through hubs
- Virtual lab environments may not always exhibit ideal shortcut behavior despite correct configurations and also some lower OS versions don’t support DMVPN phase 3 .
- Stability and scalability are often prioritized over full optimization in production networks
- Effective troubleshooting relies more on understanding protocol behavior than on configuration syntax

These lessons closely reflect real enterprise network operations, where design trade-offs and operational stability are more critical than theoretical perfection.

---

12. Device Configuration Sections

12.1 Hub Router Configuration

Hub 1 Configuration:

```
hostname HUB1
crypto isakmp policy 1
 encr aes 256
 hash sha512
 authentication pre-share
 group 16
crypto isakmp key Cisco!23 address 0.0.0.0
crypto ipsec transform-set dobre-SET esp-aes 256 esp-sha512-hmac
```

```
 mode transport
crypto ipsec profile MY-IPSEC-PROFILE
 set transform-set dobre-SET
!
!
interface Tunnel0
 description DMVPN PRIMARY HUB
 ip address 172.16.123.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 no ip next-hop-self eigrp 1
 no ip split-horizon eigrp 1
 ip nhrp authentication cisco!23
 ip nhrp network-id 123
 ip nhrp redirect
 ip tcp adjust-mss 1360
 delay 10000
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 6785
 tunnel protection ipsec profile MY-IPSEC-PROFILE
interface GigabitEthernet0/0
 ip address 51.1.1.2 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
!
!
router eigrp 1
 network 10.0.0.0
 network 172.16.123.0 0.0.0.255
```

```
!
ip route 0.0.0.0 0.0.0.0 51.1.1.5
```

Hub 2 Configuration:

```
hostname HUB2
interface Tunnel0
 description DMVPN SECONDARY HUB
 ip address 172.16.123.2 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco!23
 ip nhrp network-id 123
 ip nhrp redirect
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 6785
!
interface GigabitEthernet0/0
 ip address 51.1.1.1 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
!
router eigrp 1
 network 10.0.0.0
 network 172.16.123.0 0.0.0.255
!
ip route 0.0.0.0 0.0.0.0 51.1.1.5
```

Hub 3 Configuration:

```
hostname HUB3
interface Tunnel0
 description DMVPN TERTAIRY HUB
 ip address 172.16.123.3 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco!23
 ip nhrp network-id 123
 ip nhrp redirect
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 6785
!
interface GigabitEthernet0/0
 ip address 51.1.1.3 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
!
!
router eigrp 1
 network 10.0.0.0
 network 172.16.123.0 0.0.0.255
!
ip route 0.0.0.0 0.0.0.0 51.1.1.5
```

12.2 Spoke Router Configuration

Spoke 1 Configuration:

```
hostname SPOKE1
crypto isakmp policy 1
```

```
 encr aes 256
 hash sha512
 authentication pre-share
 group 16
crypto isakmp key Cisco!23 address 0.0.0.0
crypto ipsec transform-set dobre-SET esp-aes 256 esp-sha512-hmac
 mode transport
crypto ipsec profile MY-IPSEC-PROFILE
 set transform-set dobre-SET
!
interface Tunnel0
 description DMVPN SPOKE 1
 ip address 172.16.123.10 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco!23
 ip nhrp map multicast 51.1.1.2
 ip nhrp map 172.16.123.1 51.1.1.2
 ip nhrp network-id 123
 ip nhrp nhs 172.16.123.2 priority 2
 ip nhrp nhs 172.16.123.3 priority 3
 ip nhrp nhs 172.16.123.1 priority 1
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 6785
 tunnel protection ipsec profile MY-IPSEC-PROFILE
!
interface GigabitEthernet0/0
 ip address 203.0.113.1 255.255.255.0
 duplex auto
```

```
 speed auto
!
interface GigabitEthernet0/1
 ip address 10.6.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 10.5.0.1 255.255.255.0
 duplex auto
 speed auto
!
router eigrp 1
 network 10.0.0.0
 network 172.16.123.0 0.0.0.255
!
ip route 25.2.2.0 255.255.255.252 203.0.113.2
ip route 51.1.1.0 255.255.255.0 203.0.113.2
```

Spoke 2 Configuration:

```
hostname SPOKE2
crypto isakmp policy 1
 encr aes 256
 hash sha512
 authentication pre-share
 group 16
crypto isakmp key Cisco!23 address 0.0.0.0
!
crypto ipsec transform-set dobre-SET esp-aes 256 esp-sha512-hmac
 mode transport
```

```
!
crypto ipsec profile MY-IPSEC-PROFILE
 set transform-set dobre-SET
!
interface Tunnel0
 description DMVPN SPOKE 2
 ip address 172.16.123.11 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco!23
 ip nhrp map multicast 51.1.1.2
 ip nhrp map 172.16.123.1 51.1.1.2
 ip nhrp network-id 123
 ip nhrp nhs 172.16.123.1 priority 1
 ip nhrp nhs 172.16.123.2 priority 2
 ip nhrp nhs 172.16.123.3 priority 3
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 6785
 tunnel protection ipsec profile MY-IPSEC-PROFILE
!
interface GigabitEthernet0/0
 ip address 198.51.100.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 10.2.0.1 255.255.255.0
 duplex auto
 speed auto
```

```
!
interface GigabitEthernet0/2
 ip address 10.1.0.2 255.255.255.0
 duplex auto
 speed auto
!
router eigrp 1
 network 10.0.0.0
 network 172.16.123.0 0.0.0.255
!
ip route 25.2.2.0 255.255.255.252 198.51.100.2
ip route 51.1.1.0 255.255.255.0 198.51.100.2
```

Spoke 3 Configuration:

```
hostname SPOKE3
crypto isakmp policy 1
 encr aes 256
 hash sha512
 authentication pre-share
 group 16
crypto isakmp key Cisco!23 address 0.0.0.0
!
crypto ipsec transform-set dobre-SET esp-aes 256 esp-sha512-hmac
 mode transport
!
crypto ipsec profile MY-IPSEC-PROFILE
 set transform-set dobre-SET
!
interface Tunnel0
 description DMVPN SPOKE 3
 ip address 172.16.123.13 255.255.255.0
```

```
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco!23
 ip nhrp map multicast 51.1.1.2
 ip nhrp map 172.16.123.1 51.1.1.2
 ip nhrp network-id 123
 ip nhrp nhs 172.16.123.1 priority 1
 ip nhrp nhs 172.16.123.2 priority 2
 ip nhrp nhs 172.16.123.3 priority 3
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 6785
 tunnel protection ipsec profile MY-IPSEC-PROFILE
!
interface GigabitEthernet0/0
 ip address 192.0.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 10.3.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 10.4.0.2 255.255.255.0
 duplex auto
 speed auto
!
router eigrp 1
```

```
 network 10.0.0.0
 network 172.16.123.0 0.0.0.255
!
ip route 25.2.2.0 255.255.255.252 192.0.2.2
ip route 51.1.1.0 255.255.255.0 192.0.2.2
```

---

13. Conclusion

This lab demonstrates the design and implementation of a **secure, scalable, and resilient enterprise WAN** using DMVPN with IPsec. It reflects real-world networking challenges, including redundancy, security, and operational troubleshooting.

The project reinforces practical skills in enterprise routing, VPN technologies, and secure WAN design, aligning closely with CCNP-level and real production network expectations.

---

14. Future Enhancements

Possible future improvements include:

- Dual-ISP DMVPN design
- Integration with firewall or SD-WAN solutions
- Migration to BGP-based DMVPN
- Performance tuning and traffic engineering