SECURE YOUR WAN THE RIGHT WAY

DMVPN OVER IPSec

Hussain

NETWORKING

Table of Contents

DMVPN Phase 3 Over IPsec Technical Explanation & Configuration Guide

Introduction

Dynamic Multipoint VPN (DMVPN) is a Cisco WAN overlay technology that creates scalable, encrypted VPN topologies using multipoint GRE combined with IPsec.

This document explains Phase 3 behaviour, NHRP operations, routing, IPsec encryption, full configurations, and additional tunnel source and addressing options.

DMVPN Architecture Overview

DMVPN Core Technologies

Multipoint GRE (mGRE)

Allows one logical tunnel interface to establish dynamic GRE tunnels to multiple remote peers.

NHRP (Next Hop Resolution Protocol)

Provides tunnel IP to NBMA IP mapping so spokes can discover each other dynamically.

IPsec Transport Mode

Encrypts GRE packets without adding unnecessary tunnel headers, ideal for DMVPN.

DMVPN Phase 3 Behaviour

Hub Operation

Hub configuration includes:

```
ip nhrp map multicast dynamic

ip nhrp redirect
```

This allows spokes to send the first packet to the hub, then receive an NHRP Redirect to switch to direct spoke-to-spoke forwarding.

Spoke Operation

Each spoke uses:

```
ip nhrp shortcut

ip nhrp nhs <Hub-Tunnel-IP>
```

These commands enable the spoke to install dynamic shortcuts after receiving NHRP redirects, creating Phase 3 direct tunnels.

Dual-Hub, Dual-Cloud DMVPN Design

Cloud 1 (Primary Path)

Tunnel1 → Hub1

network-id 1

tunnel key 100

Lower EIGRP delay (preferred path)

Cloud 2 (Backup Path)

Tunnel2 → Hub2

network-id 2

tunnel key 200

Higher EIGRP delay (used only if Hub1 path fails)

Routing preference is controlled by:

delay 1000 (Primary)

delay 5000 (Backup)

Tunnel Source Options (Loopback vs Physical Interface)

Physical Interface as Tunnel Source

tunnel source Serial1/1

Used for simple ISP WAN links. Tunnel depends directly on the physical link.

Loopback Interface as Tunnel Source

tunnel source Loopback0

Used when multiple WAN uplinks or routing redundancy is required. Loopback must be routable across the WAN.

Dual Tunnels with Different Sources

```
interface Tunnel1
 tunnel source Serial1/1
interface Tunnel2
 tunnel source Loopback0
```

Valid as long as both sources are reachable from the hubs.

Tunnel Addressing Options

Host IPs per Hub/Spoke (Recommended)

Example:

Hub: 126.1.1.1/28

Spokes: 126.1.1.3, 126.1.1.4, 126.1.1.5

Using 0.0.0.0/0 (Not Recommended)

Tunnel interfaces need unique IPs for routing, making this impractical.

Hubs Advertise Networks, Spokes Match Networks

```
network 126.1.1.0 0.0.0.15
network 126.1.2.0 0.0.0.15
```

Supports scalable overlays.

Hub Configurations

Hub 1 Tunnel

```
interface Tunnel1
 ip address 126.1.1.1 255.255.255.240
 ip nhrp authentication DMVPN
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel source Serial1/1
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile DMVPN-PROFILE shared
```

Hub 1 EIGRP

```
router eigrp DMVPN
 address-family ipv4 unicast autonomous-system 126
  af-interface Tunnel1
   no split-horizon
  exit-af-interface
  network 126.1.1.0 0.0.0.15
  network 1.1.1.1 0.0.0.0
 exit-address-family
```

Hub 2 Tunnel

```
interface Tunnel2
 ip address 126.1.2.1 255.255.255.240
 ip nhrp authentication DMVPN
 ip nhrp map multicast dynamic
 ip nhrp network-id 2
 ip nhrp redirect
 tunnel source Serial1/1
 tunnel mode gre multipoint
 tunnel key 200
 tunnel protection ipsec profile DMVPN-PROFILE shared
```

Hub 2 EIGRP

```
router eigrp DMVPN
 address-family ipv4 unicast autonomous-system 126
  af-interface Tunnel2
   no split-horizon
  exit-af-interface
  network 126.1.2.0 0.0.0.15
  network 2.2.2.2 0.0.0.0
 exit-address-family
```

Spoke Configuration Template

Spoke Tunnel1 (Primary)

```
interface Tunnel1
 ip address 126.1.1.X 255.255.255.240
 ip nhrp authentication DMVPN
 ip nhrp map 126.1.1.1 47.0.0.26
 ip nhrp map multicast 47.0.0.26
 ip nhrp nhs 126.1.1.1
 ip nhrp network-id 1
 ip nhrp shortcut
 delay 1000
 tunnel source Serial1/1
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile DMVPN-PROFILE shared
```

Spoke Tunnel2 (Backup)

```
interface Tunnel2
 ip address 126.1.2.X 255.255.255.240
 ip nhrp authentication DMVPN
 ip nhrp map 126.1.2.1 47.0.0.22
 ip nhrp map multicast 47.0.0.22
 ip nhrp nhs 126.1.2.1
 ip nhrp network-id 2
 ip nhrp shortcut
 delay 5000
 tunnel source Serial1/1
 tunnel mode gre multipoint
 tunnel key 200
 tunnel protection ipsec profile DMVPN-PROFILE shared
```

Spoke EIGRP

```
router eigrp DMVPN
 address-family ipv4 unicast autonomous-system 126
  network 126.1.1.0 0.0.0.15
  network 126.1.2.0 0.0.0.15
  network <Loopback-IP> 0.0.0.0
 exit-address-family
```

IPsec Configuration

IKE Phase 1

```
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
 group 14
 lifetime 3600
```

IKE Phase 2

```
crypto ipsec transform-set DMVPN-SET esp-aes 256 esp-sha-hmac
 mode transport
```

IPsec Profile

```
crypto ipsec profile DMVPN-PROFILE
 set transform-set DMVPN-SET
```

Pre-Shared Key

```
crypto isakmp key DMVPN address 47.0.0.0 255.255.255.192
```

Phase 3 Packet Flow

1. Spoke registers with hub via NHRP.
2. Routing adjacency forms over GRE/IPsec.
3. Spoke sends first packet → hub receives it.
4. Hub sends NHRP Redirect.
5. Spoke queries NHRP for the destination spoke.
6. Spokes form direct encrypted tunnel.
7. Traffic bypasses the hub.