NETWORKERS 2004

# ADVANCED IPSEC DEPLOYMENTS AND CONCEPTS OF DMVPN NETWORKS

**SESSION SEC-4010**





## Other VPN sessions Networkers 2004

Cisco.com

- **SEC-1000 Introduction to Network Security**
- **SEC-2010: Deploying Remote Access IPSec and SSL VPNs**
- **SEC-2011: Deploying Site-to-Site IPSec VPNs**
- **SEC-3010: Troubleshooting Cisco IOS Firewall-Based and Cisco Secure PIX Firewall-Based IPSec VPNs**
- **SEC-3011: Troubleshooting Cisco VPN 3000 IPSec and SSL Implementations**
- **SEC-4011: Advanced IPSec Algorithms and Protocols**

## Agenda

Cisco.com

- **Advanced Design**
- **DMVPN Details**
- **Example DMVPN Deployments**
- **Interaction with other Features**
- **Management**
- **Performance and Futures**





## ADVANCED DESIGN

## Advanced Design Issues

Cisco.com

- **Network design**
  - Design, Redundancy and Scaling
- **Routing**
  - Dynamic routing protocols
- **Encryption peers**
  - Finding, mapping and authenticating
- **Management**
  - Deploying, Monitoring, and Maintaining





## Network Design

Cisco.com

- **Hub-and-spoke**
  - All VPN traffic must go via hub
    - Hub bandwidth and CPU utilization limit VPN
  - Number of tunnels = O(n)
- **Dynamic-Mesh – Dynamic spoke-spoke tunnels**
  - Control traffic — Hub to Hub and Hub and spoke
    - Next Hop Resolution Protocol (NHRP), Dynamic Routing, IP Multicast
  - Data traffic — Dynamic mesh
    - Spoke routers only need to support spoke-hub and spoke-spoke tunnels currently in use.
    - Hub only supports spoke-hub traffic and overflow from spoke-spoke traffic.
  - Number of tunnels > O(n), << O(n2)

## Network Design: Redundancy and Scaling Hub and Spoke

Cisco.com

- Configure spokes to use two hubs (primary, secondary).
- Can use multiple mGRE tunnel interfaces on Hub router
  - Increases number of spokes supported per hub
  - Use same tunnel source and 'tunnel protection … shared'
  - Each mGRE interface is a separate DMVPN network
    - Different Tunnel key, NHRP network id and IP subnet
- Hubs can be interconnected directly over physical links, mGRE tunnels or p-pGRE tunnels.
- Hub routers may pass routing information for DMVPN network through any of these paths.





## Network Design: Redundancy and Scaling Dynamic-Mesh

Cisco.com

- Configure spokes to use two hubs (primary, secondary)
- Hub routers can only have one mGRE tunnel interface
  - Reduces number of spokes supported per hub router
- Hub routers must exchange routing information for DMVPN network through mGRE tunnel interfaces.
- Hub routers point to other hub routers as NHSs in a daisy-chain or pair wise fashion
  - Used for forwarding NHRP packets and data packets while dynamic spoke-spoke tunnels are being created

## Routing
## New IP Routing/Forwarding Model

Cisco.com

- **Regular IP networks**
  - **IP routing updates and data packets traverse same physical/logical links**
- **DMVPN IP networks**
  - **IP routing updates only traverse hub-and-spoke tunnels**
  - **IP data packets traverse both hub-and-spoke and direct dynamic spoke-spoke tunnels**
  - **Routing protocol doesn't monitor state of spoke-spoke tunnels**





## Routing
## Dynamic Routing Protocols

Cisco.com

- **EIGRP**
  - **Good for hub-and-spoke and spoke-spoke**
  - **More control, medium overhead, faster convergence**
- **OSPF**
  - **Okay for hub-and-spoke, maximum of 2 hubs for spoke-spoke**
  - **Less control, medium overhead, faster convergence**
- **RIP**
  - **Okay for hub-and-spoke and spoke-spoke**
  - **Okay control, medium overhead, slower convergence**
- **ODR**
  - **Good for hub-and-spoke (non-split tunneling), no spoke-spoke**
  - **Less control, low overhead, slower convergence, most scalable**
- **BGP**
  - **Okay for hub-and-spoke and spoke-spoke**
  - **Good control, lower overhead, slower convergence, static neighbor configuration**

## Routing
## Dynamic Routing Configuration

Cisco.com

### Hub-and-spoke

- EIGRP
  - no ip split-horizon eigrp <as>
- OSPF
  - ip ospf network point-multipoint
- RIP
  - no ip split-horizon
- ODR
  - distribute-list <acl> out
- BGP
  - Hub is route reflector
  - next-hop self

### Dynamic Spoke-spoke

- EIGRP
  - no ip split-horizon eigrp <as>
  - no ip next-hop-self eigrp <as>
  - no auto-summary
- OSPF
  - ip ospf network broadcast
  - ip ospf priority (2(hub)|0(spoke))
- RIP
  - no ip split-horizon
  - no auto-summary
- BGP
  - Hub is route reflector





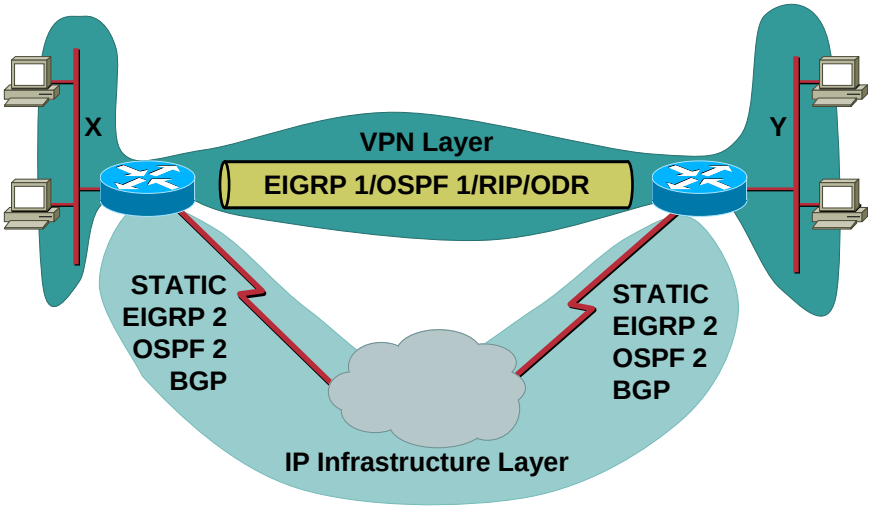
## Finding/Mapping Peers

Cisco.com

- Two layers of IP addresses
  - VPN layer, IP infrastructure (NBMA) layer
- Mapping between VPN and IP Infrastructure
  - Next Hop Resolution Protocol (NHRP)
- Authenticating peers
  - Pre-shared keys, certificates

## Two Layers of IP Addresses

Cisco.com








## NHRP Peer Mapping

Cisco.com

- **Static mappings on spokes for Hub (NHS)**
  - Needed to “start the game”
- **NHRP Registration**
  - Dynamically register spoke’s VPN to NBMA address mapping with hub (NHS).
- **NHRP Resolutions**
  - Dynamically resolve remote spoke’s VPN to NBMA mapping to build spoke-spoke tunnels.
  - CEF switching – Forwarded along NHS path (spoke – hub – … – hub)
  - Process switching – Forwarded along routed path (spoke – hub – … – hub – spoke)

## Authenticating Peers

Cisco.com

- Pre-shared keys – Hub-and-spoke only
- Wildcard pre-shared keys – Insecure
- Certificates
  - Certificate Authority/Server (CA/CS)
  - Certificate distribution—enrollment
    - Manual (terminal, tftp), Automatic (SCEP)
  - Some requirements for use
    - Accurate time—NTP, SNTP
    - Check for revocation—'crl optional'





## Configuring and Maintaining

Cisco.com

- Provisioning
  - Bootstrap PKI Certificates
  - Dynamic Addressing and Call Home
  - Policy Push for IPsec, QoS, Firewall, IDS, NAT, Routing
  - Hub-and-spoke, full and partial mesh topologies
- Ongoing Management (ISC)
  - Separate Management Tunnel
  - Router Configuration and Image Control
  - Configuration Change Notification
  - Audit Checks

## Agenda

Cisco.com

- Advanced Design
- DMVPN Details
- Example DMVPN Deployments
- Interaction with other Features
- Management
- Performance and Futures





## DMVPN DETAILS

## Dynamic Multipoint VPN (DMVPN) Major Features

Cisco.com

- Supports encrypting IP unicast, multicast and dynamic routing protocols
- Supports remote IPsec peers with dynamically assigned addresses and NAT-T
- Configuration reduction
- Dynamic spoke-spoke tunnels for scaling partial/full mesh VPNs





## Multipoint GRE (mGRE) Tunnels

Cisco.com

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

## NHRP Overview

Cisco.com

- NBMA Next Hop Resolution Protocol
  - RFC2332

**Resolve IP to NBMA address mappings for hosts/routers directly connected to an NBMA; and determine egress points from the NBMA when the destination is not directly connected to the NBMA.**





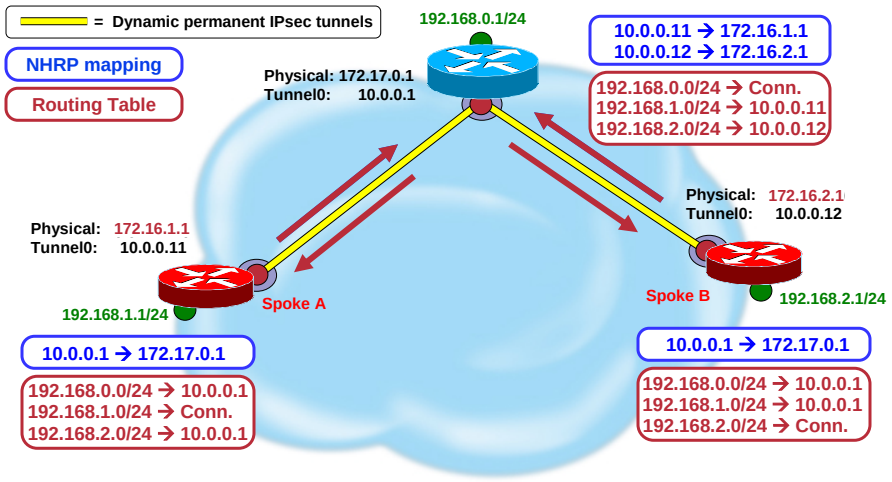
## NHRP Functionality

Cisco.com

- Address mapping/resolution
  - Next Hop Client (NHC) registration with Next Hop Server (NHS)
  - Resolution of VPN to NBMA mapping
    - Routing: destination → VPN IP next-hop
    - NHRP: VPN IP next-hop → NBMA address
- Short-cut forwarding
  - Single hop instead of multiple hops across NBMA network
  - NHRP Resolution requests/replies forwarded via NHS

# NHRP Registration
# Dynamically Addressed Spokes

Cisco.com

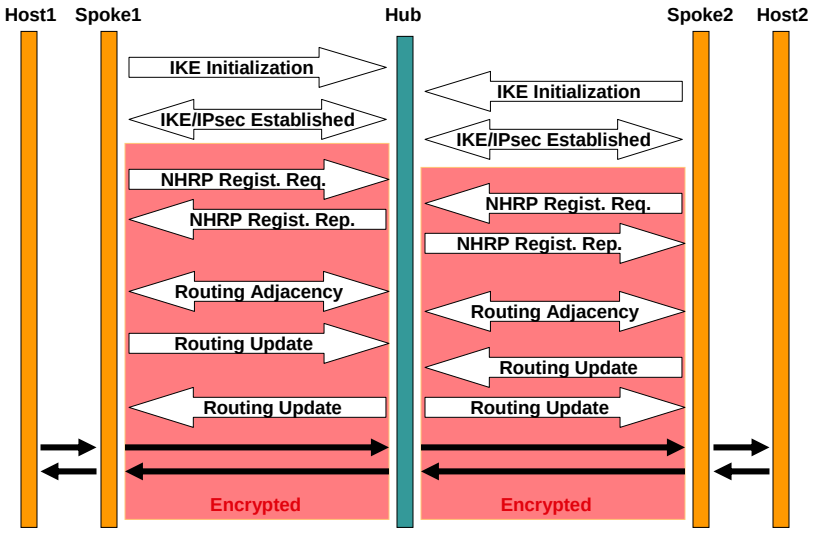







# Building Hub-and-Spoke tunnels
# NHRP Registration

Cisco.com



## Dynamic Spoke-Spoke Tunnels

Cisco.com

- mGRE/NHRP+IPsec configuration
  - On both hub and spokes
  - ISAKMP authentication information
    - Certificates, wildcard pre-shared keys (not secure)
- Spoke-spoke data traffic direct
  - Reduced load on hub
  - Reduced latency
    - Single IPsec encrypt/decrypt





## Dynamic Spoke-Spoke Tunnels Forwarding Data Packets

Cisco.com

- Process-switching
  - Routing selects outgoing interface and IP next-hop
  - NHRP overrides IP next-hop from routing
- CEF switching
  - IP Next-hop from routing table
    - Next-hop → hub ➔ data packets via hub
    - Next-hop → spoke ➔ data packets direct
- Data packets via hub while spoke-spoke tunnel is coming up, then direct

## NHRP: Data Packet Forwarding Process Switching

Cisco.com

- IP Data packet is forwarded out tunnel interface to IP next-hop from routing table
- NHRP looks in mapping table for IP destination
  - Found Entry (socket)
    - Forward to NBMA from mapping table – overriding IP next-hop
  - Found Entry (no socket)
    - If tunnel is not source interface convert to (socket)
  - Not found
    - Forward to IP next-hop (if in table) otherwise to NHS
    - If arriving interface was not tunnel interface
      - Initiate NHRP Resolution Request for IP destination





## NHRP: Data Packet Forwarding CEF Switching

Cisco.com

- IP Data packet is forwarded out tunnel interface to IP next-hop from CEF FIB table
- Adjacency is of type Valid
  - Packet is encapsulated and forwarded by CEF out tunnel interface – NHRP not involved
- Adjacency is of type Glean or Incomplete
  - Punt packet to process switching
  - If arriving interface was not tunnel interface
    - Initiate NHRP Resolution Request for IP next-hop
    - Resolution reply is used to create NHRP mapping and to complete the Adjacency

## NHRP Resolution Request/Response Forwarding

Cisco.com

- Insert protocol source to NBMA source address mapping, from request into mapping table (no socket)
- Lookup protocol destination in mapping table
  - If found (authoritative) – Answer Request
- Lookup protocol destination in routing table
  - If Outbound interface is not the tunnel
    - This node is the “exit” point – Answer Request
- Look up IP next-hop in mapping table
  - Found Entry (socket)
    - Forward to NBMA from mapping table
  - Not found or Found Entry (no socket)
    - Forward to NHS





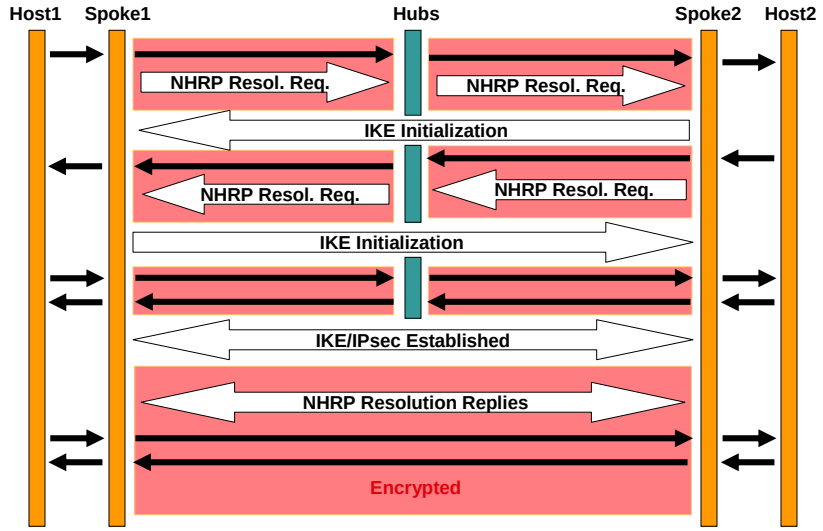
## NHRP Resolution Response

Cisco.com

- Lookup protocol destination in routing table for matching network, subnet mask and IP next-hop.
- Create NHRP local mapping entry for protocol destination network with mask-length to NBMA address
- Create NHRP Resolution Response with protocol destination, NBMA address and mask-length.
- Forwarding Resolution Response
  - Look up protocol destination in mapping table
    - Found Entry (socket)
      - Forward to NBMA from mapping table
    - Not found or Found Entry (no socket)
      - Forward to IP next-hop (if in table) otherwise to NHS

# Building Spoke-Spoke Tunnels Process Switching

Cisco.com

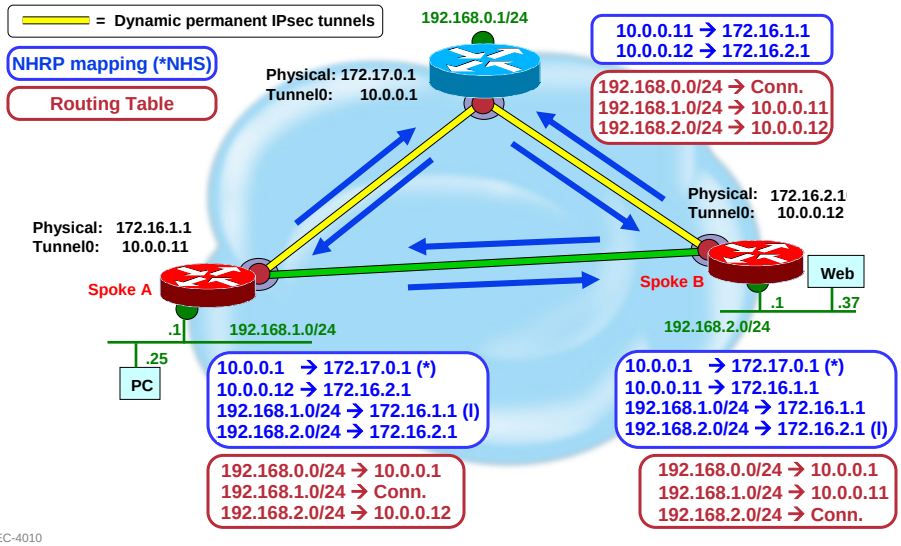






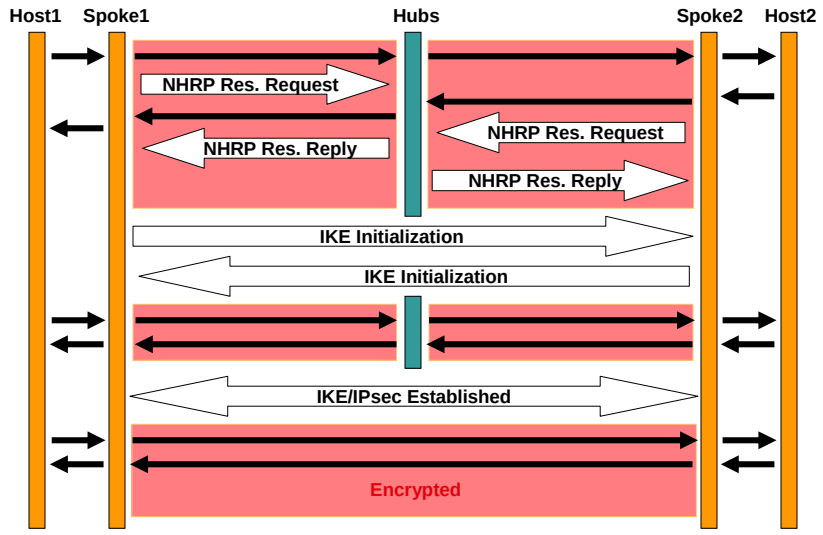

# NHRP Resolution Process Switching

Cisco.com



# Building Spoke-Spoke Tunnels
# CEF Switching

Cisco.com

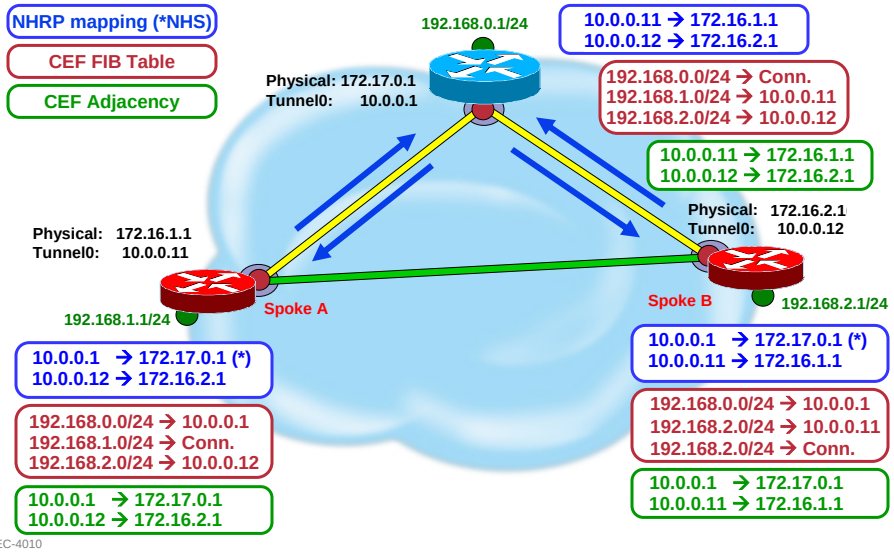







# NHRP Resolution
# CEF Switching

Cisco.com



# DMVPN
# Data Structures

Cisco.com

- **NHRP Mapping Table**
  - Maps VPN and Tunnel IP addresses to NBMA (Physical address)
    - show ip nhrp, debug nhrp { packet | cache | extension }
- **Crypto Socket Table**
  - Mapping between NHRP and IPsec
    - show crypto socket, debug crypto socket,
      show crypto ipsec profile, debug tunnel {protection}
- **Crypto Map Table**
  - Dynamic Crypto map for each mGRE tunnel
    or for each IPsec profile ('tunnel protection … shared')
    - show crypto map
- **IPsec SA Table**
  - show crypto ipsec sa { | include Tag|peer|spi|endpt }





# DMVPN
# NHRP Mapping Tables

Cisco.com

**Hub1**

```
Hub1#show ip nhrp

10.0.0.2/32 via 10.0.0.2, Tunnel0 created 01:03:41, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.5
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 01:03:38, expire 00:04:18
  Type: dynamic, Flags: authoritative unique registered used
  NBMA address: 172.16.1.2
10.0.0.12/32 via 10.0.0.12, Tunnel0 created 00:00:15, expire 00:05:44
  Type: dynamic, Flags: router implicit
  NBMA address: 172.16.2.2
    (no-socket)
```

**Spoke A**

```
SpokeB#show ip nhrp

10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:03:37, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
10.0.0.12/32 via 10.0.0.12, Tunnel0 created 00:00:11, expire 00:04:26
  Type: dynamic, Flags: router
  NBMA address: 172.16.2.2
```

# DMVPN
# Crypto Socket Tables

Cisco.com

**Hub1**

```
Hub1# show crypto socket

Number of Crypto Socket connections 2
Tu0 Peers (local/remote): 172.17.0.1/172.17.0.5
    Local Ident  (addr/mask/port/prot): (172.17.0.1/255.255.255.255/0/47)
    Remote Ident (addr/mask/port/prot): (172.17.0.5/255.255.255.255/0/47)
    Socket State: Open, Client: "TUNNEL SEC" (Client State: Active)
Tu0 Peers (local/remote): 172.17.0.1/172.16.1.2
    Local Ident  (addr/mask/port/prot): (172.17.0.1/255.255.255.255/0/47)
    Remote Ident (addr/mask/port/prot): (172.16.1.2/255.255.255.255/0/47)
    Socket State: Open, Client: "TUNNEL SEC" (Client State: Active)
Crypto Sockets in Listen state:
1   TUNNEL SEC Profile: "vpnprof" Map-name "Tunnel0-head-0"
```

**Spoke A**

```
SpokeA#show cry socket

Number of Crypto Socket connections 2
Tu0 Peers (local/remote): 172.16.1.2/172.17.0.1
    Local Ident  (addr/mask/port/prot): (172.16.1.2/255.255.255.255/0/47)
    Remote Ident (addr/mask/port/prot): (172.17.0.1/255.255.255.255/0/47)
    Socket State: Open, Client: "TUNNEL SEC" (Client State: Active)
Tu0 Peers (local/remote): 172.16.1.2/172.16.2.2
    Local Ident  (addr/mask/port/prot): (172.16.1.2/255.255.255.255/0/47)
    Remote Ident (addr/mask/port/prot): (172.16.2.2/255.255.255.255/0/47)
    Socket State: Open, Client: "TUNNEL SEC" (Client State: Active)
Crypto Sockets in Listen state:
1   TUNNEL SEC Profile: "vpnprof" Map-name "Tunnel0-head-0"
```





# DMVPN
# Crypto Map Tables

Cisco.com

**Hub1**

```
Hub1#show crypto map

Crypto Map "Tunnel0-head-0" 65536 ipsec-isakmp
    Profile name: vpnprof
    SA lifetime: 4608000 KB/3600 s, PFS (Y/N): N, Trans sets={ trans1, }
Crypto Map "Tunnel0-head-0" 65537 ipsec-isakmp, PROFILE INSTANCE.
    Peer = 172.16.0.5, access-list  permit gre host 172.17.0.1 host 172.16.0.5
    SA lifetime: 4608000 KB/3600 s, PFS (Y/N): N, Transform sets={ trans1, }
Crypto Map "Tunnel0-head-0" 65538 ipsec-isakmp, PROFILE INSTANCE.
    Peer = 172.16.1.2, access-list  permit gre host 172.17.0.1 host 172.16.1.2
    SA lifetime: 4608000 KB/3600 s, PFS (Y/N): N, Transform sets={ trans1, }
```

**Spoke A**

```
Spoke1#sho crypto map

Crypto Map "Tunnel0-head-0" 65536 ipsec-isakmp
    Profile name: vpnprof
    SA lifetime: 4608000 KB/3600 s, PFS (Y/N): N ,Transform sets={trans1, }
Crypto Map "Tunnel0-head-0" 65537 ipsec-isakmp, PROFILE INSTANCE.
    Peer = 172.17.0.1, access-list  permit gre host 172.16.1.2 host 172.17.0.1
    SA lifetime: 4608000 KB/3600 s, PFS (Y/N): N, Transform sets={trans1, }
Crypto Map "Tunnel0-head-0" 65538 ipsec-isakmp, PROFILE INSTANCE.
    Peer = 172.16.2.2, access-list  permit gre host 172.16.1.2 host 172.16.2.2
    SA lifetime: 4608000 KB/3600 s, PFS (Y/N): N, Transform sets={trans1, }
```

# DMVPN
# Crypto IPsec SAs

Cisco.com

**Hub1**

```
Hub1#show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr. 172.17.0.1
  local crypto endpt.: 172.17.0.1, remote crypto endpt.: 172.16.1.2
    current outbound spi: D111D4E0
    inbound esp sas: spi: 0x8FE87A1B(2414377499) {Transport, }
    outbound esp sas: spi: 0xD111D4E0(3507606752) {Transport, }
  local crypto endpt.: 172.17.0.1, remote crypto endpt.: 172.17.0.5
    current outbound spi: 149FA5E7
    inbound esp sas: spi: 0x3C32F075(1009971317) {Transport, }
    outbound esp sas: spi: 0x149FA5E7(346007015) {Transport, }
```

**Spoke A**

```
SpokeA#sho crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr. 172.16.1.2
  local crypto endpt.: 172.16.1.2, remote crypto endpt.: 172.17.0.1
    current outbound spi: 8FE87A1B
    inbound esp sas: spi: 0xD111D4E0(3507606752) {Transport, }
    outbound esp sas: spi: 0x8FE87A1B(2414377499) {Transport, }
  local crypto endpt.: 172.16.1.2, remote crypto endpt.: 172.16.2.2
    current outbound spi: 32E65B6D
    inbound esp sas: spi: 0x3B44DBD0(994368464) {Transport, }
                     spi: 0x8B07B649(2332538441) {Transport, }
    outbound esp sas: spi: 0x8CCD4943(2362263875) {Transport, }
                      spi: 0x32E65B6D(853957485) {Transport, }
```





# DMVPN
# Routing Tables

Cisco.com

**Hub1**

```
Hub1# show ip route

C   172.17.0.0/30 is directly connected, Serial1/0
C   10.0.0.0/24 is directly connected, Tunnel0
C   192.168.0.0/24 is directly connected, Ethernet0/0
D   192.168.1.0/24 [90/2611200] via 10.0.0.11, 00:42:39, Tunnel0
D   192.168.2.0/24 [90/2636800] via 10.0.0.12, 00:42:37, Tunnel0
S*  0.0.0.0/0 [1/0] via 172.17.0.2
```

**Spoke A**

```
SpokeA# show ip route

C   172.16.1.0/30 is directly connected, Serial1/0
C   10.0.0.0/24 is directly connected, Tunnel0
D    192.168.0.0/24 [90/297372416] via 10.0.0.1, 00:42:34, Tunnel0
C    192.168.1.0/24 is directly connected, Ethernet0/0
D    192.168.2.0/24 [90/297321216] via 10.0.0.12, 00:42:34, Tunnel0
S*   0.0.0.0/0 [1/0] via 172.16.1.1
```

## Agenda

Cisco.com

- Advanced Design
- DMVPN Details
- Example DMVPN Deployments
- Interaction with other Features
- Management
- Performance and Futures





## EXAMPLE DMVPN DEPLOYMENTS

## Example DMVPN Deployments

Cisco.com

- **DMVPN Dual Hub**
  - Redundancy
  - Routing and Load Balancing
- **DMVPN Multi-hub**
  - Redundancy, Scaling
  - NHRP Resolution Forwarding
- **DMVPN High Concentration Hub**
  - Server Load Balancing (SLB)
  - CAT6500/7600, VPNSM, MWAM





## DMVPN Dual Hub Features

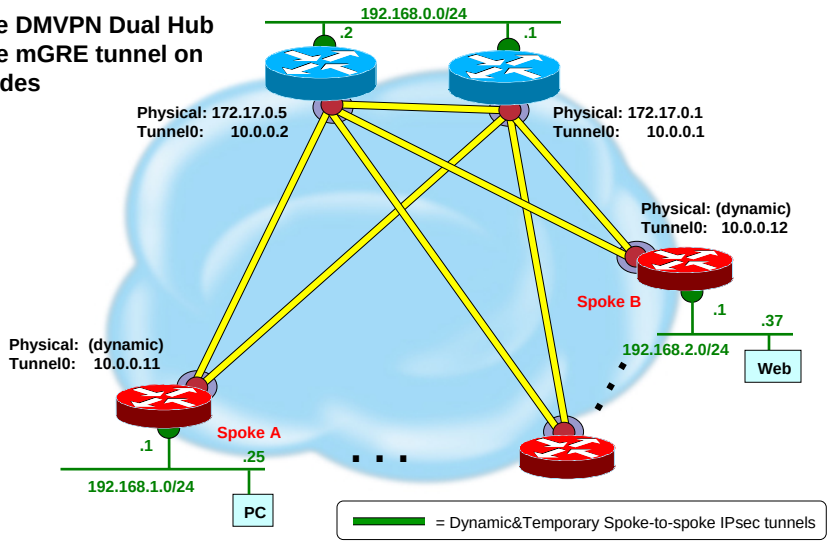
Cisco.com

- **Redundancy**
  - Two spoke-hub links for each spoke
  - All spokes connected to both hubs
  - Can lose 1 hub and spoke not isolated
- **Routing and load balancing**
  - Both spoke-hub links always up
  - Dynamic routing controls packet flow for redundancy and/or load balancing

# DMVPN Dual Hub

Cisco.com

**Single DMVPN Dual Hub**
**Single mGRE tunnel on all nodes**








# Single DMVPN Dual Hub Crypto and Interface Configuration

Cisco.com

```
crypto ca trustpoint msca-root
     enrollment terminal
     crl optional
     rsakeypair <hostname>
crypto ca certificate chain msca-root
     certificate <router-certificate-id>
     certificate ca 1244325DE0369880465F977A18F61CA8
!
crypto isakmp policy 1
     encryption 3des
!
crypto ipsec transform-set trans1 esp-3des esp-md5-hmac
     mode transport required
!
crypto ipsec profile vpnprof
     set transform-set trans1
!
interface Ethernet0/0  ! < inside interface >
     ip address 192.168.<x>.<x> 255.255.255.0
!
interface Serial1/0  ! < outside interface >
     ip address 172.<16|17>.<x>.<x> 255.255.255.252
```

# DMVPN Dual Hub
# Hub1

Cisco.com

Common Subnet

Static NHRP to Hub2

OSPF Network Priority and cost

OSPF Routing

```
interface Tunnel0
     bandwidth 1000
     ip address 10.0.0.1 255.255.255.0
     ip mtu 1400
     ip nhrp authentication test
     ip nhrp map multicast dynamic
     ip nhrp map 10.0.0.2 172.17.0.5
     ip nhrp map multicast 172.17.0.5
     ip nhrp network-id 100000
     ip nhrp holdtime 360
     ip tcp adjust-mss 1360
     ip ospf network broadcast
     ip ospf priority 2
     ip ospf cost 100
     tunnel source Serial1/0
     tunnel mode gre multipoint
     tunnel key 100000
     tunnel protection ipsec profile vpnprof
!
router ospf 1
     network 10.0.0.0 0.0.0.255 area 1
     network 192.168.0.0 0.0.0.255 area 0
```





# DMVPN Dual Hub
# Hub2

Cisco.com

Common Subnet

Static NHRP to Hub1

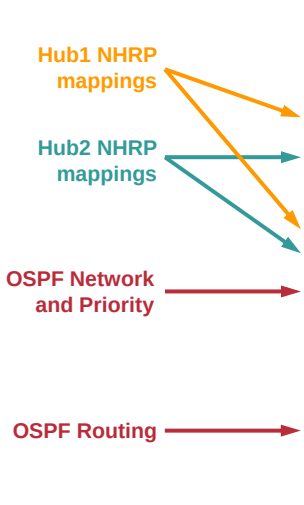
OSPF Network Priority and cost

OSPF Routing

```
interface Tunnel0
     bandwidth 1000
     ip address 10.0.0.2 255.255.255.0
     ip mtu 1400
     ip nhrp authentication test
     ip nhrp map multicast dynamic
     ip nhrp map 10.0.0.1 172.17.0.1
     ip nhrp map multicast 172.17.0.1
     ip nhrp network-id 100000
     ip nhrp holdtime 360
     ip tcp adjust-mss 1360
     ip ospf network broadcast
     ip ospf priority 2
     ip ospf cost 105
     tunnel source Serial1/0
     tunnel mode gre multipoint
     tunnel key 100000
     tunnel protection ipsec profile vpnprof
!
router ospf 1
     network 10.0.0.0 0.0.0.255 area 1
     network 192.168.0.0 0.0.0.255 area 0
```

# DMVPN Dual Hub Spoke A

Cisco.com



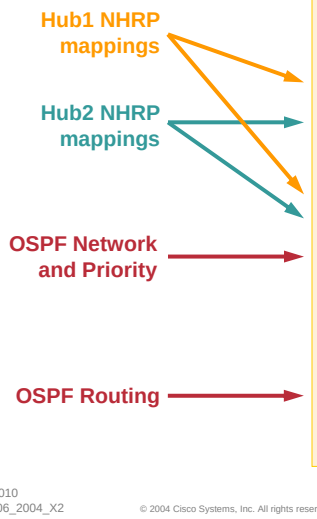

```
interface Tunnel0
      bandwidth 1000
      ip address 10.0.0.11 255.255.255.0
      ip mtu 1400
      ip nhrp authentication test
      ip nhrp map multicast 172.17.0.1
      ip nhrp map 10.0.0.1 172.17.0.1
      ip nhrp map multicast 172.17.0.5
      ip nhrp map 10.0.0.2 172.17.0.5
      ip nhrp network-id 100000
      ip nhrp holdtime 360
      ip nhrp nhs 10.0.0.1
      ip nhrp nhs 10.0.0.2
      ip tcp adjust-mss 1360
      ip ospf network broadcast
      ip ospf priority 0
      tunnel source Serial1/0
      tunnel mode gre multipoint
      tunnel key 100000
      tunnel protection ipsec profile vpnprof
!
router ospf 1
      network 10.0.0.0 0.0.0.255 area 1
      network 192.168.1.0 0.0.0.255 area 1
      distance 111 192.168.0.2 0.0.0.0
```





# DMVPN Dual Hub Spoke B

Cisco.com




```
interface Tunnel0
      bandwidth 1000
      ip address 10.0.0.12 255.255.255.0
      ip mtu 1400
      ip nhrp authentication test
      ip nhrp map multicast 172.17.0.1
      ip nhrp map 10.0.0.1 172.17.0.1
      ip nhrp map multicast 172.17.0.5
      ip nhrp map 10.0.0.2 172.17.0.5
      ip nhrp network-id 100000
      ip nhrp holdtime 360
      ip nhrp nhs 10.0.0.1
      ip nhrp nhs 10.0.0.2
      ip tcp adjust-mss 1360
      ip ospf network broadcast
      ip ospf priority 0
      tunnel source Serial1/0
      tunnel mode gre multipoint
      tunnel key 100000
      tunnel protection ipsec profile vpnprof
!
router ospf 1
      network 10.0.0.0 0.0.0.255 area 1
      network 192.168.2.0 0.0.0.255 area 1
      distance 111 192.168.0.2 0.0.0.0
```

# DMVPN Dual Hub
# Hub Routing Tables

Cisco.com

**Hub1**

```
C    172.17.0.0/30 is directly connected, Serial1/0
C    10.0.0.0/24 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, Ethernet0/0
O    192.168.1.0/24 [110/110] via 10.0.0.11, 00:36:53, Tunnel0
O    192.168.2.0/24 [110/110] via 10.0.0.12, 00:36:53, Tunnel0
     . . .
S*   0.0.0.0/0 [1/0] via 172.17.0.2
```

**Hub 2**

```
C    172.17.0.4/30 is directly connected, Serial1/0
C    10.0.0.0/24 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, Ethernet0/0
O    192.168.1.0/24 [110/115] via 10.0.0.11, 00:42:02, Tunnel0
O    192.168.2.0/24 [110/115] via 10.0.0.12, 00:42:02, Tunnel0
     . . .
S*   0.0.0.0/0 [1/0] via 172.17.0.6
```





# DMVPN Dual Hub
# Spoke Routing Tables

Cisco.com

**Spoke A**

```
C    172.16.1.0/30 is directly connected, Serial1/0
C    10.0.0.0/24 is directly connected, Tunnel0
O IA 192.168.0.0/24 [110/110] via 10.0.0.1, 00:46:20, Tunnel0
C    192.168.1.0/24 is directly connected, Ethernet0/0
O    192.168.2.0/24 [110/110] via 10.0.0.12, 00:46:20, Tunnel0
     . . .
S*   0.0.0.0/0 [1/0] via 172.16.1.2
```

**Spoke B**

```
C    172.16.2.0/30 is directly connected, Serial1/0
C    10.0.0.0/24 is directly connected, Tunnel0
O IA 192.168.0.0/24 [110/110] via 10.0.0.1, 00:53:14, Tunnel0
O    192.168.1.0/24 [110/110] via 10.0.0.11, 00:53:14, Tunnel0
C    192.168.2.0/24 is directly connected, Ethernet0/0
     . . .
S*   0.0.0.0/0 [1/0] via 172.16.2.2
```

## DMVPN Dual Hub
## Hub NHRP tables

Cisco.com

**Hub1**

```
10.0.0.2/32 via 10.0.0.2, Tunnel0 created 02:58:13, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.5
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 02:51:46, expire 00:04:13
  Type: dynamic, Flags: authoritative unique registered used
  NBMA address: 172.16.1.1
10.0.0.12/32 via 10.0.0.12, Tunnel0 created 02:51:26, expire 00:04:33
  Type: dynamic, Flags: authoritative unique registered used
  NBMA address: 172.16.2.1
```

**Hub 2**

```
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 02:48:42, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 02:43:05, expire 00:05:01
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 172.16.1.1
10.0.0.12/32 via 10.0.0.12, Tunnel0 created 02:44:08, expire 00:05:20
  Type: dynamic, Flags: authoritative unique registered used
  NBMA address: 172.16.2.1
```





## DMVPN Dual Hub
## Spoke NHRP tables

Cisco.com

**Spoke A**

```
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 02:51:20, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
10.0.0.2/32 via 10.0.0.2, Tunnel0 created 02:51:20, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.5
10.0.0.12/32 via 10.0.0.12, Tunnel0 created 00:00:06, expire 00:05:05
  Type: dynamic, Flags: router unique used
  NBMA address: 172.16.2.1
```

**Spoke B**

```
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 02:51:18, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
10.0.0.2/32 via 10.0.0.2, Tunnel0 created 02:51:18, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.5
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 00:00:24, expire 00:04:27
  Type: dynamic, Flags: router unique used
  NBMA address: 172.16.1.1
```

## DMVPN Dual Hub Summary

Cisco.com

- Network design
  - Hub and spoke—routing
  - Dynamic mesh—data traffic
- Add spoke routers without hub or other spoke router changes
  - NHRP and dynamic routing propagate information
- Hub redundancy
  - Must lose both before spoke isolated





## Example DMVPN Deployments

Cisco.com

- DMVPN Dual Hub
  - Redundancy
  - Routing and Load Balancing
- DMVPN Multi-hub
  - Redundancy, Scaling
  - NHRP Resolution Forwarding
- DMVPN High Concentration Hub
  - Server Load Balancing (SLB)
  - CAT6500/7600, VPNSM, MWAM

## DMVPN Multi-Hub Features

Cisco.com

- **Redundancy**
  - Two spoke-hub links for each spoke (example only shows one for clarity)
  - Can lose 1 hub and spoke not isolated – hub-and-spoke
- **Routing and load balancing**
  - Both spoke-hub links always up
  - Dynamic routing controls packet flow for redundancy and/or load balancing
  - Dynamic routing configuration more complex





## DMVPN Multi-Hub Hub Daisy Chaining

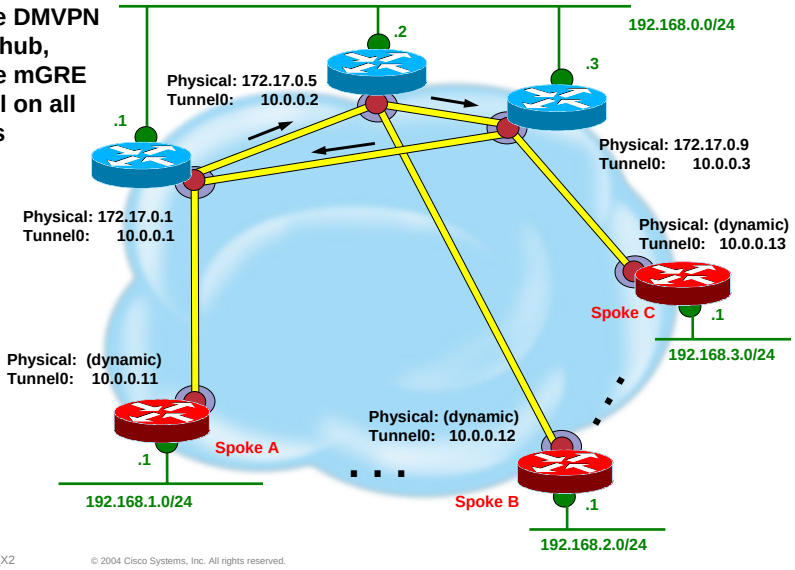
Cisco.com

- **Daisy chain styles**
  - Single daisy chain through all hubs
    - Spoke's two tunnels distributed across hubs equally
  - Two single daisy chains one through primary hubs and other through secondary hubs.
    - Spokes connected to both a primary and secondary hub
- **Loss of Hub breaks daisy chain**
  - No new spoke-spoke dynamic tunnels until hub back online
  - Cross-connect between primary and secondary hubs restores spoke-spoke data traffic, but goes through hubs.

# DMVPN Multi-Hub

Cisco.com

Single DMVPN Multi-hub, Single mGRE tunnel on all nodes








# DMVPN Multi-Hub Hub1

Cisco.com

Common Subnet

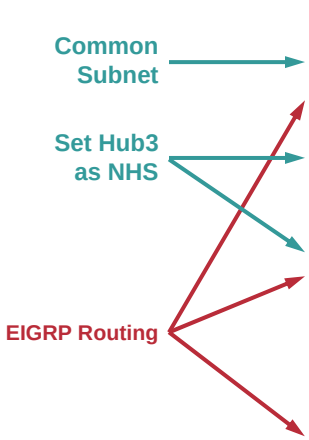
Set Hub2 as NHS

EIGRP Routing

```
interface Tunnel0
     bandwidth 1000
     ip address 10.0.0.1 255.255.255.0
     ip mtu 1400
     no ip next-hop-self eigrp 1
     ip nhrp authentication test
     ip nhrp map multicast dynamic
     ip nhrp map 10.0.0.2 172.17.0.5
     ip nhrp map multicast 172.17.0.5
     ip nhrp network-id 100000
     ip nhrp holdtime 360
     ip tcp adjust-mss 1360
     ip nhrp nhs 10.0.0.2
     no ip split-horizon eigrp 1
     ip tcp adjust-mss 1360
     delay 1000
     tunnel source Serial1/0
     tunnel mode gre multipoint
     tunnel key 100000
     tunnel protection ipsec profile vpnprof
!
router eigrp 1
     network 10.0.0.0 0.0.0.255
     network 192.168.0.0
     no auto-summary
```

# DMVPN Multi-Hub Hub2

Cisco.com




```
interface Tunnel0
     bandwidth 1000
     ip address 10.0.0.2 255.255.255.0
     ip mtu 1400
     no ip next-hop-self eigrp 1
     ip nhrp authentication test
     ip nhrp map multicast dynamic
     ip nhrp map 10.0.0.3 172.17.0.9
     ip nhrp map multicast 172.17.0.9
     ip nhrp network-id 100000
     ip nhrp holdtime 360
     ip tcp adjust-mss 1360
     ip nhrp nhs 10.0.0.3
     no ip split-horizon eigrp 1
     ip tcp adjust-mss 1360
     delay 1000
     tunnel source Serial1/0
     tunnel mode gre multipoint
     tunnel key 100000
     tunnel protection ipsec profile vpnprof
!
router eigrp 1
     network 10.0.0.0 0.0.0.255
     network 192.168.0.0
     no auto-summary
```





# DMVPN Multi-Hub Hub3

Cisco.com


```
interface Tunnel0
     bandwidth 1000
     ip address 10.0.0.3 255.255.255.0
     ip mtu 1400
     no ip next-hop-self eigrp 1
     ip nhrp authentication test
     ip nhrp map multicast dynamic
     ip nhrp map 10.0.0.1 172.17.0.5
     ip nhrp map multicast 172.17.0.5
     ip nhrp network-id 100000
     ip nhrp holdtime 360
     ip tcp adjust-mss 1360
     ip nhrp nhs 10.0.0.1
     no ip split-horizon eigrp 1
     ip tcp adjust-mss 1360
     delay 1000
     tunnel source Serial1/0
     tunnel mode gre multipoint
     tunnel key 100000
     tunnel protection ipsec profile vpnprof
!
router eigrp 1
     network 10.0.0.0 0.0.0.255
     network 192.168.0.0
     no auto-summary
```

# DMVPN Multi-Hub Spoke A

Cisco.com

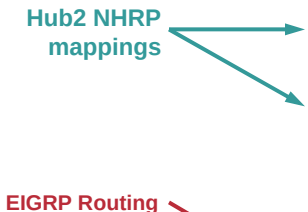

```
interface Tunnel0
     bandwidth 1000
     ip address 10.0.0.11 255.255.255.0
     ip mtu 1400
     ip nhrp authentication test
     ip nhrp map multicast 172.17.0.1
     ip nhrp map 10.0.0.1 172.17.0.1
     ip nhrp network-id 100000
     ip nhrp holdtime 360
     ip nhrp nhs 10.0.0.1
     ip tcp adjust-mss 1360
     delay 1000
     tunnel source Serial1/0
     tunnel mode gre multipoint
     tunnel key 100000
     tunnel protection ipsec profile vpnprof
!
router eigrp 1
     network 10.0.0.0 0.0.0.255
     network 192.168.1.0 0.0.0.255
     no auto-summary
```





# DMVPN Multi-Hub Spoke B

Cisco.com




```
interface Tunnel0
     bandwidth 1000
     ip address 10.0.0.12 255.255.255.0
     ip mtu 1400
     ip nhrp authentication test
     ip nhrp map multicast 172.17.0.5
     ip nhrp map 10.0.0.2 172.17.0.5
     ip nhrp network-id 100000
     ip nhrp holdtime 360
     ip nhrp nhs 10.0.0.2
     ip tcp adjust-mss 1360
     delay 1000
     tunnel source Serial1/0
     tunnel mode gre multipoint
     tunnel key 100000
     tunnel protection ipsec profile vpnprof
!
router eigrp 1
     network 10.0.0.0 0.0.0.255
     network 192.168.2.0 0.0.0.255
     no auto-summary
```

# DMVPN Multi-Hub
# Spoke C

Cisco.com

Hub3 NHRP mappings

EIGRP Routing

```
interface Tunnel0
      bandwidth 1000
      ip address 10.0.0.13 255.255.255.0
      ip mtu 1400
      ip nhrp authentication test
      ip nhrp map multicast 172.17.0.9
      ip nhrp map 10.0.0.3 172.17.0.9
      ip nhrp network-id 100000
      ip nhrp holdtime 360
      ip nhrp nhs 10.0.0.3
      ip tcp adjust-mss 1360
      delay 1000
      tunnel source Serial1/0
      tunnel mode gre multipoint
      tunnel key 100000
      tunnel protection ipsec profile vpnprof
!
router eigrp 1
      network 10.0.0.0 0.0.0.255
      network 192.168.3.0 0.0.0.255
      no auto-summary
```





# DMVPN Multi-Hub
# Hub NHRP tables

Cisco.com

**Hub1**

```
10.0.0.2/32, NBMA addr: 172.17.0.5 (stat, auth, used)
10.0.0.3/32, NBMA addr: 172.17.0.9 (dyn, auth, uniq, reg)
10.0.0.11/32, NBMA addr: 172.16.1.2 (dyn, auth, uniq, reg)
10.0.0.13/32, NBMA addr: 172.16.3.2 (no-socket) (dyn, router)
```

**Hub 2**

```
10.0.0.1/32, NBMA addr: 172.17.0.1 (dyn, auth, uniq, reg)
10.0.0.3/32, NBMA addr: 172.17.0.9 (stat, auth, used)
10.0.0.11/32, NBMA addr: 172.16.1.2 (no-socket) (dyn, router)
10.0.0.12/32, NBMA addr: 172.16.2.2 (dyn, auth, uniq, reg)
```

**Hub 3**

```
10.0.0.1/32, NBMA addr: 172.17.0.1 (stat, auth, used)
10.0.0.2/32, NBMA addr: 172.17.0.5 (dyn, auth, uniq, reg)
10.0.0.11/32, NBMA addr: 172.16.1.2 (no-socket) (dyn, router)
10.0.0.13/32, NBMA addr: 172.16.3.2 (dyn, auth, uniq, reg)
```

## DMVPN Multi-Hub Spoke NHRP tables

Cisco.com

**Spoke A**

```
10.0.0.1/32, Tunnel0 created 1d10h, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
10.0.0.13/32, Tunnel0 created 00:00:12, expire 00:04:18
  Type: dynamic, Flags: router used
  NBMA address: 172.16.3.2
```

**Spoke C**

```
10.0.0.3/32, Tunnel0 created 1d10h, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.9
10.0.0.11/32, Tunnel0 created 00:00:54, expire 00:03:36
  Type: dynamic, Flags: router
  NBMA address: 172.16.1.2
```





## DMVPN Multi-Hub Summary

Cisco.com

- **Multi-hub and spoke (redundant DMVPN)**
  - **Use to increase the number of spokes in DMVPN cloud**
  - **Daisy-chain hubs as NHSs of each other**
- **Daisy-chaining**
  - **Currently “fragile”—lose one hub and can’t create new dynamic spoke-spoke tunnels**
- **Consider setting up smaller regional DMVPN networks interconnected with dedicated high speed physical links**
  - **Probably will give better performance then cross-country spoke-spoke dynamic tunnels**

## Example DMVPN Deployments

Cisco.com

- DMVPN Dual Hub
  - Redundancy
  - Routing and Load Balancing
- DMVPN Multi-hub
  - Redundancy, Scaling
  - NHRP Resolution Forwarding
- DMVPN High Concentration Hub
  - Hub-and-Spoke
  - Server Load Balancing (SLB)
  - CAT6500/7600, VPNSM, MWAM





## DMVPN High Concentration Hub Features

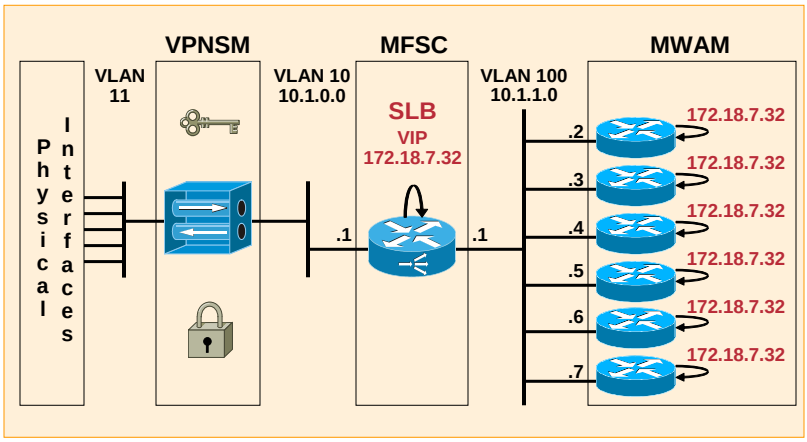
Cisco.com

- Single hub-and-spoke tunnel per spoke
- Server Load Balancing (SLB) is used to load balance mGRE tunnels (after decryption) between MWAM processors or 7200 router farm
- If you lose an MWAM processor then SLB will redistribute tunnels to other processors
  - Loss of traffic until spoke sends next NHRP registration
- Routing
  - Use EIGRP for routing between hub (MWAM) and spoke
  - Use BGP for routing between hubs

# DMVPN High Concentration Hub

Cisco.com

**CAT6500**

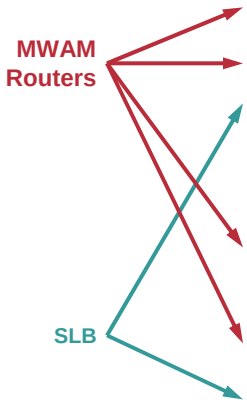







# DMVPN High Concentration Hub
# MSFC: SLB Configuration

Cisco.com




```
mwam module 2 port 1 allowed-vlan 1,100
mwam module 2 port 2 allowed-vlan 1,100
...
mwam module 2 port 6 allowed-vlan 1,100
!
ip slb probe PING-PROBE ping
     faildetect 3
!
ip slb serverfarm MWAM-FARM
     predictor leastconns
     failaction purge
     probe PING-PROBE
     !
     real 10.0.0.2
          maxconns 750
          inservice
     ...
     !
     real 10.0.0.7
          maxconns 750
          inservice
!
ip slb vserver GRE
     virtual 172.18.7.32 255.255.255.252 gre
     serverfarm MWAM-FARM
     no advertise
     sticky 17
     inservice
```

# DMVPN High Concentration Hub MSFC Configuration

Cisco.com

```
!
interface Loopback0
 ip address 172.18.7.32 255.255.255.255
!
interface GigabitEthernet7/1
  no ip address
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,10,1002-1005
  switchport mode trunk
!
interface GigabitEthernet7/2
  no ip address
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,11,1002-1005
  switchport mode trunk
```

```
vlan 10-11,100
!
interface FastEthernet4/1
  no ip address
  switchport
  switchport access vlan 11
  switchport mode access
...
!
interface Vlan10
  ip address 10.1.0.1 255.255.255.0
  crypto map cm
!
interface Vlan11
  no ip address
  crypto connect vlan 10
!
interface Vlan100
  ip address 10.1.1.1 255.255.255.0
```





# DMVPN High Concentration Hub MWAM Routers

Cisco.com

Same secondary for spoke neighbor

EIGRP and BGP Routing

```
interface Loopback0
      ip address 172.18.7.32 255.255.255.255
!
interface Tunnel0
      bandwidth 1000
      ip mtu 1400
      ip address 10.0.0.1 255.255.0.0 secondary
      ip address 10.0.0.<x> 255.255.0.0       ! x = 2,3,4,5,6,7
      no ip next-hop-self eigrp 1
      ip nhrp map multicast dynamic
      ip nhrp network-id 100000
      ip nhrp holdtime 360
      no ip split-horizon eigrp 1
      delay 1000
      ip tcp adjust-mss 1360
      tunnel source Loopback0
      tunnel mode gre multipoint
      tunnel key 100000
!
interface GigabitEthernet0/0.100
      encapsulation dot1Q 100
      ip address 10.1.1.<x> 255.255.255.0
!
router eigrp 1
      network 10.0.0.0 0.0.255.255
      no auto-summary
router bgp 1
      bgp router-id 10.0.0.<x>
      redistribute eigrp 1
      neighbor 10.0.0.1 remote-as 1
```

# DMVPN High Concentration Hub Spoke

Cisco.com

Hub NHRP mappings

EIGRP Routing

```
interface Tunnel0
     bandwidth 1000
     ip address 10.0.0.<z> 255.255.0.0
     ip mtu 1400
     ip nhrp authentication test
     ip nhrp map multicast 172.18.7.32
     ip nhrp map 10.0.0.1 172.18.7.32
     ip nhrp network-id 100000
     ip nhrp holdtime 360
     ip nhrp nhs 10.0.0.1
     ip tcp adjust-mss 1360
     delay 1000
     tunnel source Serial1/0
     tunnel mode gre multipoint
     tunnel key 100000
     tunnel protection ipsec profile vpnprof
!
router eigrp 1
     network 10.0.0.0 0.0.255.255
     network <local-network> <inverse-mask>
     no auto-summary
```





# DMVPN High Concentration Hub Summary

Cisco.com

- **Spokes load balanced by SLB over six MWAM processors**
  - **Single Hub per Spoke, but dynamically redundant MWAM and VPNSM processors.**
  - **Use another 6500/7600, VPNSM, MWAM as a second hub**
- **Use as a hub for DMVPN**
  - **Uses dynamic crypto-map on VPNSM so it cannot initiate IPsec tunnels**
- **Possibly use as a high bandwidth spoke**
  - **Rely on DMVPN initiating spoke-spoke tunnels from both sides**

## Agenda

Cisco.com

- Advanced Design
- DMVPN Details
- Example DMVPN Deployments
- Interaction with other Features
- Management
- Performance and Futures





## INTERACTION WITH OTHER TECHNOLOGIES

## Interaction with Other Features

Cisco.com

- NAT Traversal (NAT-T)
  - Tunnel Mode IPsec
  - Transport Mode IPsec
- VRF
  - Tunnel packets in VRF
  - Data traffic in VRF
- QoS
  - Multipoint GRE Interfaces



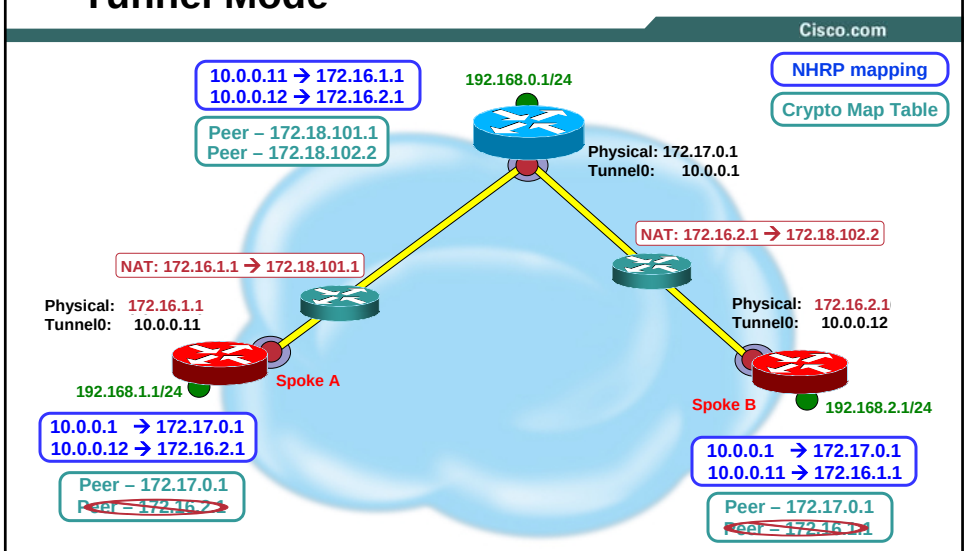


## DMVPN and NAT-T

Cisco.com

- Spoke routers must be NAT translated to a unique outside NAT address
- Tunnel Mode IPsec
  - NHRP registration uses inside NAT spoke address on hub
  - Spoke routers must have unique inside NAT address.
  - Requires coordination of inside NAT address for all spokes in DMVPN network. Multiple ISPs may be involved.
- Transport Mode IPsec
  - NHRP registration uses outside NAT spoke address on hub
  - Spoke routers may have the same inside NAT address
  - Also supports Hub router behind static NAT
- Spoke-spoke dynamic tunnels are not supported to/from NAT translated spokes—spoke-spoke traffic goes via the hub

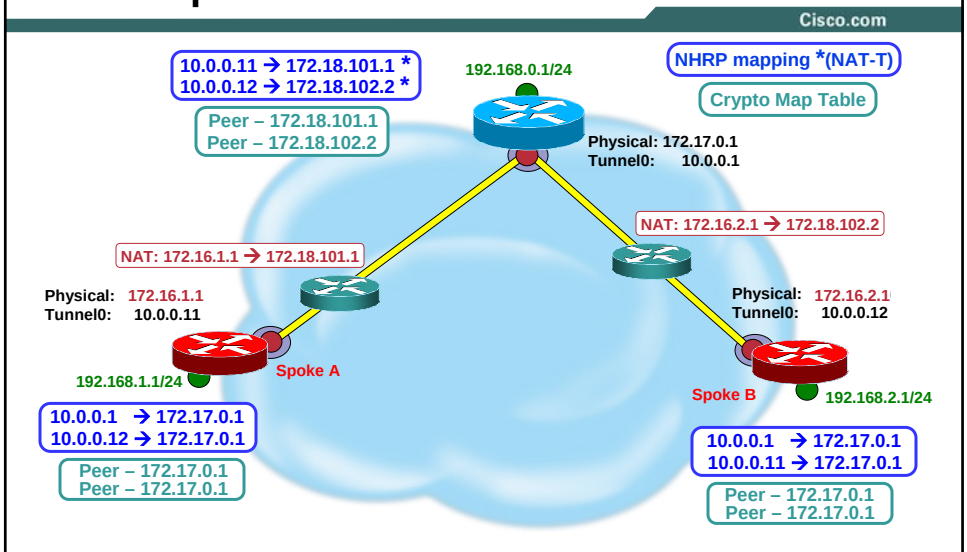
# DMVPN and NAT-T Tunnel Mode








# DMVPN and NAT-T Transport Mode



## DMVPN and VRF
## GRE Tunnel Packets in VRF

Cisco.com

- **Configuration**

```
interface tunnel0
  tunnel vrf <vrf-name>

Interface <physical>
  ip vrf-forwarding <vrf-name>
```

- **GRE tunnel packets use VRF routing table**
- **Data packets use global routing table after GRE decapsulation**
- **Routing protocol updates use global routing table**
- **NHRP uses global routing table for forwarding NHRP control packets**





## DMVPN and VRF
## Tunnel Data Packets in VRF

Cisco.com

- **Configuration**

```
interface tunnel0
  ip vrf forwarding <vrf-name>
```

- **Data packets injected into VRF after GRE decapsulation**
- **Routing protocol updates use VRF routing table**
- **NHRP uses VRF routing table for forwarding NHRP control packets**
- **GRE tunnel packets use global routing table for forwarding**
- **Can use both ‘vrf-forwarding …’ and ‘tunnel vrf …’**

## DMVPN and QoS
## Spoke → Hub Traffic

Cisco.com

- Outbound spoke bandwidth smaller then Hub inbound bandwidth
- Few tunnel endpoints
- Need to keep spoke from overrunning its own outbound bandwidth
- Need to prefer high priority (voice, control) over lower priority (data) traffic
- Aggregate traffic from all spokes could overrun Hub inbound bandwidth





## DMVPN and QoS
## Hub → Spoke Traffic

Cisco.com

- Outbound hub bandwidth higher then Spoke inbound bandwidth
- Many tunnel endpoints – single mGRE interface
- Need to keep Hub router from:
  - Overrunning crypto engine input queue – multicast traffic
  - Overrunning its own outbound interface bandwidth
  - Overrunning inbound spoke interface bandwidth
- Would like to QoS shape/police per application per spoke

## DMVPN and QoS
## Spoke → Spoke Traffic

Cisco.com

- Local outbound bandwidth could be higher or lower then remote inbound bandwidth
- Few or many tunnel endpoints outbound and inbound
- Need to keep from:
  - Overrunning local outbound interface bandwidth
  - Overrunning remote spoke inbound interface bandwidth
  - Remote spokes from overrunning local inbound bandwidth
- Would like to QoS shape/police per application per remote spoke





## DMVPN and QoS
## What Can You Do?

Cisco.com

- QoS is not configurable on mGRE tunnel interface
- Apply QoS on the outbound physical interface
  - Configure 'qos pre-classify' on mGRE interface to use data packet parameters for classification
  - IPsec anti-replay may drop packets if low priority packets are delayed too much
  - If Tunnel destinations are dynamic (DHCP, PPP)
    - Can classify unicast traffic per spoke – doesn't scale
    - Cannot classify multicast traffic per spoke
  - Otherwise can configure QoS policy using known tunnel destinations – hub-spoke, spoke-hub traffic only

## Agenda

Cisco.com

- Advanced Design
- DMVPN Details
- Example DMVPN Deployments
- Interaction with other Features
- Management
- Performance and Futures





## MANAGEMENT

## Management: A Case Study

Cisco.com

- Cisco: Enterprise Class Teleworker (ECT) Network
- What is ECT?

**"ECT is a SOHO Remote Access IOS based VPN solution for enterprise users using the public Internet service while providing additional services (VoIP, QoSS, Multicast) with *Security* as it's primary concern."**

***– Cisco IT***

## ECT Technology Overview

Cisco.com

**ECT**

| Connectivity | Security | Network Integration | Management |
|---|---|---|---|
| **Enterprise Class Teleworker (ECT)**<br>• Cisco 83x, 17xx series<br>**Full Service Branch (FSB)**<br>• Cisco 17xx, 26xx, 37xx series<br>**Enterprise Aggregation**<br>• Cisco 37xx, 72xx series<br>**Service Provider Edge**<br>• Cisco 72xx series | **Public Key Infrastructure**<br>• PKI-AAA Integration<br>• Auto Enrolment<br>• Multiple Trust Points<br>• Secure RSA Private Key<br>**Device and User Authentication**<br>• Secure ARP<br>• Authentication Proxy/802.1x<br>**Stateful Firewall**<br>**Intrusion Protection** | **DMVPN**<br>• Dynamic Addressing for Spoke-to-Hub<br>• On-Demand Spoke-to-Spoke Tunnels<br>**V³PN**<br>• QoS<br>• VoIP<br>• Video<br>• Multicast<br>**Resiliency**<br>• Self-Healing and Load Balancing<br>**Scalability**<br>• Full Mesh up to 1000 Sites | **Touchless Provisioning (ISC)**<br>• Bootstrap PKI Certificates<br>• Dynamic Addressing and Call Home<br>• Policy Push for IPsec, QoS, Firewall, IDS, NAT, Routing<br>• Hub-and-spoke, full and partial mesh topologies<br>**Ongoing Management (ISC)**<br>• Management Tunnel<br>• Configuration Change Notification<br>• Audit Checks |

## ECT
## Large Scale VPN Management Challenges

Cisco.com

- Ease of large scale deployment with minimal end-user intervention
- Distribution of updated configurations and security policies
- Varying third party provider network connections (cable modem, DSL)
- Ongoing security monitoring and auditing
- Automated software update





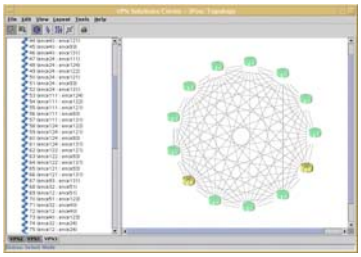
## ECT
## Management and Provisioning

Cisco.com

- Touchless provisioning of routing, IPsec, NAT, QoS, firewall, IDS
- Bootstrapping and call home
  - Automatic registration and policy push, no user intervention
- Automatic CA enrolment for PKI certificates
- Dedicated management tunnel facilitates outsourcing of management
- Per-user or per-group configuration policies
- Email notification on spoke events: config change, or policy audit violations

# Cisco IP Solution Center 3.0: Carrier-Class Network and Service Management

Cisco.com



- Site–to-site VPN
- Remote Access VPN
- DMVPN
- Easy VPN
- Managed firewall
- NAT
- Managed IDS
- Network-based IPsec

Device Abstraction Layer

IOS Router | PIX® Appliance | VPN 3000 | IDS

- Hub-and-spoke, full and partial mesh topologies
- Design and deploy complex firewall rules
- Cisco IOS IDS provisioning and tuning
- Integrated routing—OSPF, EIGRP, RIP
- Automate provisioning of failover and load balancing
- QoS provisioning
- NAT configuration deployment
- PKI-based end-to-end authentication and audit checks





# ECT Management Tools Used

Cisco.com

- ISC – IP Solution Center for deploying and managing configurations
- CNS – provide event based management
  - Intelligence Engine 2100 – CNS server
  - CNS Event Gateway and Auto Update Server
  - CNS agent – running on IOS in the spoke routers
- CA Servers
  - IOS Certificate Server - bootstrap certificate
  - Production CA Server - certificate for data tunnels
- AAA server - RADIUS

## ISC Touchless Provisioning

Cisco.com

- Home routers are bootstrapped before given to the end-users
- Permanent management tunnel to provide secured connectivity to management servers to perform
  - Initial configuration of home router upon call-home
  - Listen to config changes
  - Automatic software update
- Separate VPN gateway devices
  - Management Gateway to terminate management tunnels
  - Data Gateway to tunnel traffic into the corporate network





## Initial Provisioning (Bootstrapping)

Cisco.com

- Two methods
  - Bootstrap in the corporate network using ISC
  - Bootstrap remotely using EzSDD (Ez Secure Device Deployment)
- Bootstrap in the corporate network requires less end-user intervention
- EzSDD provides total automatic device deployment without initial bootstrapping home routers in the corporate network

## Corporate Network Bootstrapping Steps

Cisco.com

- Enterprise orders the router for end-user
- The following basic configuration is bootstrapped on the router using ISC
  - IP Connectivity (Cable, PPPoE, etc.)
  - Certificate for authenticating to the management gateway
  - Crypto policy used for the management tunnel
  - CNS Agent configuration to communicate with IE2100
  - External NTP server configurations





## EzSDD

Cisco.com

- User submits request via on-line forms
- Once request is approved, the following is created
  - AAA profile for user and device authentication
  - ISC configuration for initial bootstrap using EzSDD
  - ISC full security policy for data traffic
- User takes the router home with instructions on how to activate service from home
- User brings the router online

## EzSDD (Cont.)

Cisco.com

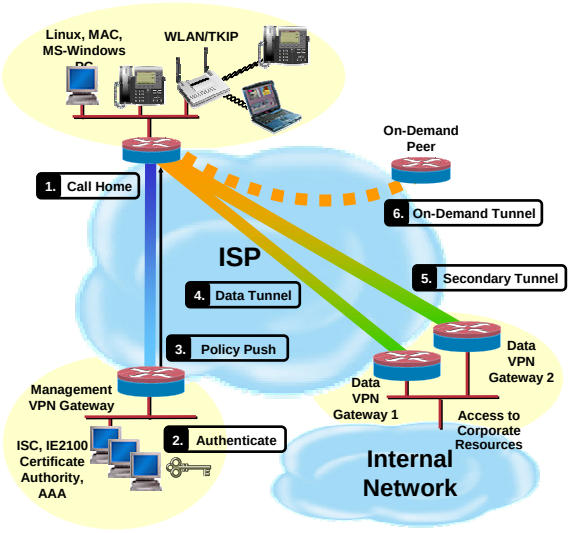
- User connects to the EzSDD server and authenticates using one-time password
- EzSDD server gets the initial configuration for the management tunnel from ISC and pushes to the home router
- Management tunnel comes up triggering CNS agent which connects to IE2100
- IE2100 notifies ISC that device is online
- ISC pushes down the full data tunnel configuration, including data tunnel certificate, security policies, and full DMVPN configurations





## Deployment in Action

Cisco.com




1. Remote routers “call home” and management tunnel is set up.
2. Management server authenticates remote router using certificate authority and AAA servers.
3. Management server pushes policy including new certificate.
4. Remote router establishes primary data tunnel, access to corporate resources.
5. Secondary tunnel established, stays active for instant failover.
6. When required, remote router establishes direct spoke-to-spoke tunnel with other authorized remotes and torn down after use.

## ECT
## Ongoing Management

Cisco.com

- Management tunnel maintained throughout the operations of the router
- Event-driven notification and regular audit checks used to satisfy security requirements
  - Attempt to downgrade/upgrade IOS
  - Password recovery
  - Enable/vty password change
  - Modified/disabled CNS Agent
- IOS image management via CNS Image Agent





## Agenda

Cisco.com

- Advanced Design
- DMVPN Details
- Example DMVPN Deployments
- Interaction with other Features
- Management
- Performance and Futures

# PERFORMANCE AND FUTURES





## Performance and Futures

Cisco.com

- Code and platform support
- Performance
- Futures

## Cisco IOS Code and Platform Support

Cisco.com

- DMVPN hub-and-spoke
  - 12.3(6), 12.3(7)T
- DMVPN dynamic spoke-spoke
  - 12.3(9), 12.3(8)T1
- Platforms
  - 6500/7600 with VPNSM and MWAM or 7200 Farm (DMVPN Hub)
  - 7204/6, 36xx, 37xx, 26xx, 17xx
  - 83x support in 12.3T





## DMVPN Hub-and-Spoke Hub Throughput

Cisco.com

| 7200, NPE-G1, VAM2, mGRE | Encrypted (PPS) | Encrypted (Mbps) |
|---|---|---|
| 350 EIGRP – IMIX, 75% CPU | 27,000 | 87.3 |
| 325 OSPF – IMIX, 75% CPU | 27,000 | 87.3 |
| 1200 ODR – IMIX, 75% CPU | 26,000 | 79.3 |
| 800 EIGRP – EMIX, 82% CPU<br>2 mGRE, 2 VAM2 | 45,212 | 104.2 |
| 3576 EIGRP – EMIX, ~24% CPU (MSFC, MWAM)<br>CAT6500, VPNSM, MWAM | 453,000 | 1004 |

- EMIX – Enterprise Mix
  - Average packet size 188B(down)/144B(up) (FTP, VoIP, WWW, POP3)
- IMIX – Internet Mix
  - Average packet size 344B (7x64B, 4x570B, 1x1400B)

## Futures
## DMVPN CEF Routing Model

Cisco.com

- CEF and NHRP interaction to be more like process-switching
  - Packets will be forwarded to routing table ‘ip next-hop’
  - NHRP will be triggered to find short-cut tunnel
  - NHRP adds/removes subnet route for ‘ip destination’ to short-cut ‘ip next-hop’
- Benefits
  - Removes restrictions for routing protocols
    - Allows route summarization, OSPF support for >2 hubs
  - Removes Hub ‘daisy-chaining’
    - Forward NHRP packets via ‘ip next-hop’ rather then NHS





## Futures
## QoS

Cisco.com

- Current issues
  - Anti-replay
  - QoS per spoke
  - Overrun local encryption engine
- Enhancements
  - Move QoS to after IPsec SA selection but before encryption
  - Packets ordered correctly before being encrypted
  - Packets policed/shaped per peer (IKE identity)
  - QoS queues protect encryption engine
- Useful for IPsec, EzVPN, IPsec+GRE and DMVPN

# Futures Management

Cisco.com

- **New DMVPN tunnel concept**
  - **Encompasses NHRP, Crypto Socket, IPsec Crypto map and IPsec SA data structures.**
  - **New show and debug commands**
  - **Possibly a new MIB**
- **Managing dynamic spoke-spoke tunnels**
  - **Use Service Assurance Agent (SAA)**
  - **GRE keepalives for mGRE interfaces**



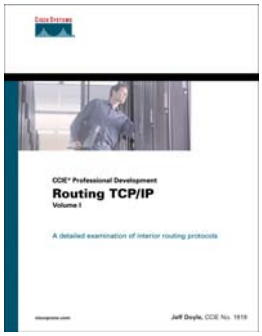


# Q and A

## Recommended Reading

Cisco.com

- Continue your Networkers learning experience with further reading for this session from Cisco Press.
- Check the Recommended Reading flyer for suggested books.




**Available on-site at the Cisco Company Store**





## Complete Your Online Session Evaluation!

Cisco.com

**WHAT:** Complete an online session evaluation and your name will be entered into a daily drawing

**WHY:** Win fabulous prizes! Give us your feedback!

**WHERE:** Go to the Internet stations located throughout the Convention Center

**HOW:** Winners will be posted on the onsite Networkers Website; four winners per day






## Some Extras

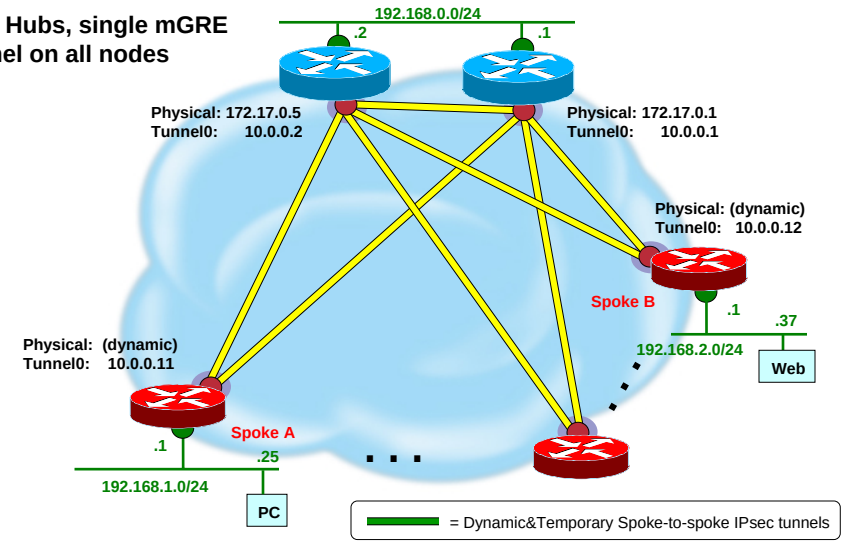
Cisco.com

- **IOS Configuration Examples**
  - **Single DMVPN Dual Hub**
  - **Single DMVPN Multi-hub**

# Single DMVPN Dual Hub

Cisco.com

Two Hubs, single mGRE tunnel on all nodes








# Single DMVPN Dual Hub Hub1 Configuration

Cisco.com

```
crypto ca trustpoint msca-root
    enrollment terminal
    crl optional
    rsakeypair hub1
crypto ca certificate chain msca-root
    certificate 2368DB55000000000B4E
    certificate ca 1244325DE0369880465F977A18F61CA8
!
crypto isakmp policy 1
    encryption 3des
!
crypto ipsec transform-set trans1 esp-3des esp-md5-hmac
    mode transport required
!
crypto ipsec profile vpnprof
    set transform-set trans1
!
interface Ethernet0/0
    ip address 192.168.0.1 255.255.255.0
!
interface Serial1/0
    ip address 172.17.0.1 255.255.255.252
```

## Single DMVPN Dual Hub Hub1 Configuration (Cont.)

Cisco.com

```
interface Tunnel0
    bandwidth 1000
    ip address 10.0.0.1 255.255.255.0
    ip mtu 1400
    ip nhrp authentication test
    ip nhrp map multicast dynamic
    ip nhrp map 10.0.0.2 172.17.0.5
    ip nhrp map multicast 172.17.0.5
    ip nhrp network-id 100000
    ip nhrp holdtime 360
    ip tcp adjust-mss 1360
    ip ospf network broadcast
    ip ospf priority 2
    ip ospf cost 100
    tunnel source Serial1/0
    tunnel mode gre multipoint
    tunnel key 100000
    tunnel protection ipsec profile vpnprof
!
router ospf 1
    network 10.0.0.0 0.0.0.255 area 1
    network 192.168.0.0 0.0.0.255 area 0
```





## Single DMVPN Dual Hub Hub2 Configuration

Cisco.com

```
crypto ca trustpoint msca-root
    enrollment terminal
    crl optional
    rsakeypair hub2
crypto ca certificate chain msca-root
    certificate 2279F316000000000B40
    certificate ca 1244325DE0369880465F977A18F61CA8
!
crypto isakmp policy 1
    encryption 3des
!
crypto ipsec transform-set trans1 esp-3des esp-md5-hmac
    mode transport required
!
crypto ipsec profile vpnprof
    set transform-set trans1
!
interface Ethernet0/0
    ip address 192.168.0.2 255.255.255.0
!
interface Serial1/0
    ip address 172.17.0.5 255.255.255.252
```

## Single DMVPN Dual Hub Hub2 Configuration (Cont.)

Cisco.com

```
interface Tunnel0
    bandwidth 1000
    ip address 10.0.0.2 255.255.255.0
    ip mtu 1400
    ip nhrp authentication test
    ip nhrp map multicast dynamic
    ip nhrp map 10.0.0.1 172.17.0.1
    ip nhrp map multicast 172.17.0.1
    ip nhrp network-id 100000
    ip nhrp holdtime 360
    ip tcp adjust-mss 1360
    ip ospf network broadcast
    ip ospf priority 2
    ip ospf cost 105
    tunnel source Serial1/0
    tunnel mode gre multipoint
    tunnel key 100000
    tunnel protection ipsec profile vpnprof
!
router ospf 1
    network 10.0.0.0 0.0.0.255 area 1
    network 192.168.0.0 0.0.0.255 area 0
```





## Single DMVPN Dual Hub Spoke A Configuration

Cisco.com

```
crypto ca trustpoint msca-root
    enrollment terminal
    crl optional
    rsakeypair spoke1
crypto ca certificate chain msca-root
    certificate 236FD380000000000B4F
    certificate ca 1244325DE0369880465F977A18F61CA8
!
crypto isakmp policy 1
    encryption 3des
!
crypto ipsec transform-set trans1 esp-des esp-md5-hmac
    mode transport required
!
crypto ipsec profile vpnprof
    set transform-set trans1
!
interface Ethernet0/0
    ip address 192.168.1.1 255.255.255.0
!
interface Serial1/0
    ip address 172.16.1.1 255.255.255.252
```

# Single DMVPN Dual Hub Spoke A Configuration (Cont.)

Cisco.com

```
interface Tunnel0
     bandwidth 1000
     ip address 10.0.0.11 255.255.255.0
     ip mtu 1400
     ip nhrp authentication test
     ip nhrp map multicast 172.17.0.1
     ip nhrp map 10.0.0.1 172.17.0.1
     ip nhrp map multicast 172.17.0.5
     ip nhrp map 10.0.0.2 172.17.0.5
     ip nhrp network-id 100000
     ip nhrp holdtime 360
     ip nhrp nhs 10.0.0.1
     ip nhrp nhs 10.0.0.2
     ip tcp adjust-mss 1360
     ip ospf network broadcast
     ip ospf priority 0
     tunnel source Serial1/0
     tunnel mode gre multipoint
     tunnel key 100000
     tunnel protection ipsec profile vpnprof
!
router ospf 1
     network 10.0.0.0 0.0.0.255 area 1
     network 192.168.1.0 0.0.0.255 area 1
     distance 111 192.168.0.2 0.0.0.0
```





# Single DMVPN Dual Hub Spoke B Configuration

Cisco.com

```
crypto ca trustpoint msca-root
     enrollment terminal
     crl optional
     rsakeypair spoke1
crypto ca certificate chain msca-root
     certificate 2376A085000000000B50
     certificate ca 1244325DE0369880465F977A18F61CA8
!
crypto isakmp policy 1
     encryption 3des
!
crypto ipsec transform-set trans1 esp-des esp-md5-hmac
     mode transport required
!
crypto ipsec profile vpnprof
     set transform-set trans1
!
interface Ethernet0/0
     ip address 192.168.2.1 255.255.255.0
!
interface Serial1/0
     ip address 172.16.2.1 255.255.255.252
```

# Single DMVPN Dual Hub Spoke B Configuration (Cont.)

Cisco.com

```
interface Tunnel0
     bandwidth 1000
     ip address 10.0.0.12 255.255.255.0
     ip mtu 1400
     ip nhrp authentication test
     ip nhrp map multicast 172.17.0.1
     ip nhrp map 10.0.0.1 172.17.0.1
     ip nhrp map multicast 172.17.0.5
     ip nhrp map 10.0.0.2 172.17.0.5
     ip nhrp network-id 100000
     ip nhrp holdtime 360
     ip nhrp nhs 10.0.0.1
     ip nhrp nhs 10.0.0.2
     ip tcp adjust-mss 1360
     ip ospf network broadcast
     ip ospf priority 0
     tunnel source Serial1/0
     tunnel mode gre multipoint
     tunnel key 100000
     tunnel protection ipsec profile vpnprof
!
router ospf 1
     network 10.0.0.0 0.0.0.255 area 1
     network 192.168.2.0 0.0.0.255 area 1
     distance 111 192.168.0.2 0.0.0.0
```

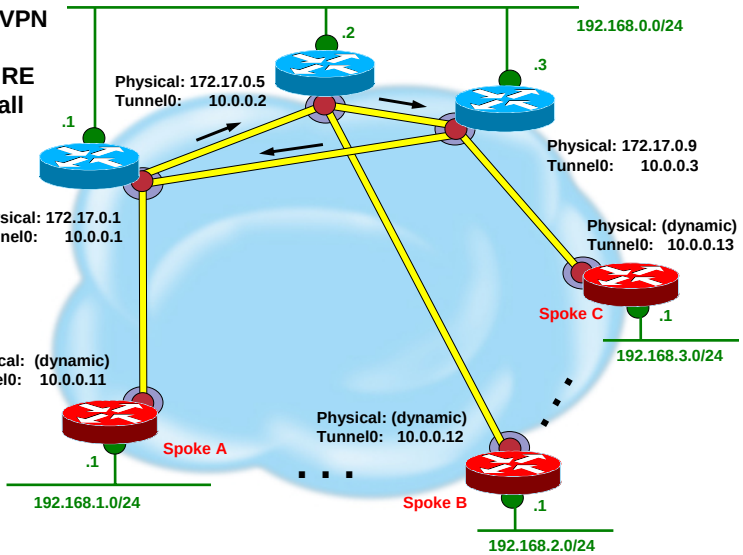




# Single DMVPN Multi-hub

Cisco.com

Single DMVPN Multi-hub, Single mGRE tunnel on all nodes



# Single DMVPN Multi-hub Hub1 Configuration

Cisco.com

```
crypto ca trustpoint msca-root
     enrollment terminal
     crl optional
     rsakeypair hub1
crypto ca certificate chain msca-root
     certificate 2368DB55000000000B4E
     certificate ca 1244325DE0369880465F977A18F61CA8
!
crypto isakmp policy 1
     encryption 3des
!
crypto ipsec transform-set t1 esp-3des esp-md5-hmac
     mode transport required
!
crypto ipsec profile vpnprof
     set transform-set t1
!
interface Ethernet0/0
     bandwidth 1000
     ip address 192.168.0.1 255.255.255.0
     delay 500
!
interface Serial1/0
     ip address 172.17.0.1 255.255.255.252
!
ip route 0.0.0.0 0.0.0.0 172.17.0.2
```





# Single DMVPN Multi-hub Hub1 Configuration (Cont.)

Cisco.com

```
interface Tunnel0
     bandwidth 1000
     ip address 10.0.0.1 255.255.255.0
     ip mtu 1400
     no ip next-hop-self eigrp 1
     ip nhrp authentication test
     ip nhrp map multicast dynamic
     ip nhrp map 10.0.0.2 172.17.0.5
     ip nhrp map multicast 172.17.0.5
     ip nhrp network-id 100000
     ip nhrp holdtime 360
     ip tcp adjust-mss 1360
     ip nhrp nhs 10.0.0.2
     no ip split-horizon eigrp 1
     ip tcp adjust-mss 1360
     delay 1000
     tunnel source Serial1/0
     tunnel mode gre multipoint
     tunnel key 100000
     tunnel protection ipsec profile vpnprof
!
router eigrp 1
     network 10.0.0.0 0.0.0.255
     network 192.168.0.0
     no auto-summary
```

# Single DMVPN Multi-hub Hub2 Configuration

Cisco.com

```
crypto ca trustpoint msca-root
     enrollment terminal
     crl optional
     rsakeypair hub2
crypto ca certificate chain msca-root
     certificate 2368DB55000000000B40
     certificate ca 1244325DE0369880465F977A18F61CA8
!
crypto isakmp policy 1
     encryption 3des
!
crypto ipsec transform-set t1 esp-des esp-sha-hmac
     mode transport required
!
crypto ipsec profile vpnprof
     set transform-set t1
!
interface Ethernet0/0
     bandwidth 1000
     ip address 192.168.0.2 255.255.255.0
     delay 500
!
interface Serial1/0
     ip address 172.17.0.5 255.255.255.252
!
ip route 0.0.0.0 0.0.0.0 172.17.0.6
```





# Single DMVPN Multi-hub Hub2 Configuration (Cont.)

Cisco.com

```
interface Tunnel0
     bandwidth 1000
     ip address 10.0.0.2 255.255.255.0
     ip mtu 1400
     no ip next-hop-self eigrp 1
     ip nhrp authentication test
     ip nhrp map multicast dynamic
     ip nhrp map 10.0.0.3 172.17.0.9
     ip nhrp map multicast 172.17.0.9
     ip nhrp network-id 100000
     ip nhrp holdtime 360
     ip tcp adjust-mss 1360
     ip nhrp nhs 10.0.0.3
     no ip split-horizon eigrp 1
     ip tcp adjust-mss 1360
     delay 1000
     tunnel source Serial1/0
     tunnel mode gre multipoint
     tunnel key 100000
     tunnel protection ipsec profile vpnprof
!
router eigrp 1
     network 10.0.0.0 0.0.0.255
     network 192.168.0.0
     no auto-summary
```

# Single DMVPN Multi-hub Hub3 Configuration

Cisco.com

```
crypto ca trustpoint msca-root
     enrollment terminal
     crl optional
     rsakeypair hub3
crypto ca certificate chain msca-root
     certificate 2368DB55000000000B48
     certificate ca 1244325DE0369880465F977A18F61CA8
!
crypto isakmp policy 1
     encryption 3des
!
crypto ipsec transform-set t1 esp-des esp-sha-hmac
     mode transport required
!
crypto ipsec profile vpnprof
     set transform-set t1
!
interface Ethernet0/0
     bandwidth 1000
     ip address 192.168.0.3 255.255.255.0
     delay 500
!
interface Serial1/0
     ip address 172.17.0.9 255.255.255.252
!
ip route 0.0.0.0 0.0.0.0 172.17.0.10
```





# Single DMVPN Multi-hub Hub3 Configuration (Cont.)

Cisco.com

```
interface Tunnel0
     bandwidth 1000
     ip address 10.0.0.3 255.255.255.0
     ip mtu 1400
     no ip next-hop-self eigrp 1
     ip nhrp authentication test
     ip nhrp map multicast dynamic
     ip nhrp map 10.0.0.1 172.17.0.1
     ip nhrp map multicast 172.17.0.1
     ip nhrp network-id 100000
     ip nhrp holdtime 360
     ip tcp adjust-mss 1360
     ip nhrp nhs 10.0.0.1
     no ip split-horizon eigrp 1
     ip tcp adjust-mss 1360
     delay 1000
     tunnel source Serial1/0
     tunnel mode gre multipoint
     tunnel key 100000
     tunnel protection ipsec profile vpnprof
!
router eigrp 1
     network 10.0.0.0 0.0.0.255
     network 192.168.0.0
     no auto-summary
```

# Single DMVPN Multi-hub Spoke A Configuration

Cisco.com

```
crypto ca trustpoint msca-root
    enrollment terminal
    crl optional
    rsakeypair spoke1
crypto ca certificate chain msca-root
    certificate 236FD380000000000B4F
    certificate ca 1244325DE0369880465F977A18F61CA8
!
crypto isakmp policy 1
    encryption 3des
!
crypto ipsec transform-set trans1 esp-des esp-md5-hmac
    mode transport required
!
crypto ipsec profile vpnprof
    set transform-set trans1
!
interface Ethernet0/0
    ip address 192.168.1.1 255.255.255.0
!
interface Serial1/0
    ip address 172.16.1.1 255.255.255.252
```





# Single DMVPN Multi-hub Spoke A Configuration (Cont.)

Cisco.com

```
interface Tunnel0
    bandwidth 1000
    ip address 10.0.0.11 255.255.255.0
    ip mtu 1400
    ip nhrp authentication test
    ip nhrp map multicast 172.17.0.1
    ip nhrp map 10.0.0.1 172.17.0.1
    ip nhrp network-id 100000
    ip nhrp holdtime 360
    ip nhrp nhs 10.0.0.1
    ip tcp adjust-mss 1360
    delay 1000
    tunnel source Serial1/0
    tunnel mode gre multipoint
    tunnel key 100000
    tunnel protection ipsec profile vpnprof
!
router eigrp 1
    network 10.0.0.0 0.0.0.255
    network 192.168.1.0 0.0.0.255
    no auto-summary
```

## Single DMVPN Dual Hub Spoke B Configuration

Cisco.com

```
crypto ca trustpoint msca-root
    enrollment terminal
    crl optional
    rsakeypair spoke1
crypto ca certificate chain msca-root
    certificate 2376A085000000000B50
    certificate ca 1244325DE0369880465F977A18F61CA8
!
crypto isakmp policy 1
    encryption 3des
!
crypto ipsec transform-set trans1 esp-des esp-md5-hmac
    mode transport required
!
crypto ipsec profile vpnprof
    set transform-set trans1
!
interface Ethernet0/0
    ip address 192.168.2.1 255.255.255.0
!
interface Serial1/0
    ip address 172.16.2.1 255.255.255.252
```





## Single DMVPN Multi-hub Spoke B Configuration (Cont.)

Cisco.com

```
interface Tunnel0
    bandwidth 1000
    ip address 10.0.0.12 255.255.255.0
    ip mtu 1400
    ip nhrp authentication test
    ip nhrp map multicast 172.17.0.5
    ip nhrp map 10.0.0.2 172.17.0.5
    ip nhrp network-id 100000
    ip nhrp holdtime 360
    ip nhrp nhs 10.0.0.2
    ip tcp adjust-mss 1360
    delay 1000
    tunnel source Serial1/0
    tunnel mode gre multipoint
    tunnel key 100000
    tunnel protection ipsec profile vpnprof
!
router eigrp 1
    network 10.0.0.0 0.0.0.255
    network 192.168.2.0 0.0.0.255
    no auto-summary
```

## Single DMVPN Dual Hub Spoke C Configuration

Cisco.com

```
crypto ca trustpoint msca-root
    enrollment terminal
    crl optional
    rsakeypair spoke1
crypto ca certificate chain msca-root
    certificate 2376A085000000000B51
    certificate ca 1244325DE0369880465F977A18F61CA8
!
crypto isakmp policy 1
    encryption 3des
!
crypto ipsec transform-set trans1 esp-des esp-md5-hmac
    mode transport required
!
crypto ipsec profile vpnprof
    set transform-set trans1
!
interface Ethernet0/0
    ip address 192.168.3.1 255.255.255.0
!
interface Serial1/0
    ip address 172.16.3.1 255.255.255.252
```





## Single DMVPN Multi-hub Spoke C Configuration (Cont.)

Cisco.com

```
interface Tunnel0
    bandwidth 1000
    ip address 10.0.0.13 255.255.255.0
    ip mtu 1400
    ip nhrp authentication test
    ip nhrp map multicast 172.17.0.9
    ip nhrp map 10.0.0.3 172.17.0.9
    ip nhrp network-id 100000
    ip nhrp holdtime 360
    ip nhrp nhs 10.0.0.3
    ip tcp adjust-mss 1360
    delay 1000
    tunnel source Serial1/0
    tunnel mode gre multipoint
    tunnel key 100000
    tunnel protection ipsec profile vpnprof
!
router eigrp 1
    network 10.0.0.0 0.0.0.255
    network 192.168.3.0 0.0.0.255
    no auto-summary
```