ADVANCED IPSEC DEPLOYMENTS AND CONCEPTS OF DMVPN NETWORKS
SESSION SEC-4010

Other VPN sessions
Networkers 2004

• 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

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

• Network design
  Design, Redundancy and Scaling

• Routing
  Dynamic routing protocols

• Encryption peers
  Finding, mapping and authenticating

• Management
  Deploying, Monitoring, and Maintaining

Network Design

• 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

- 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

- 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

- 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

- 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

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

- 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

VPN Layer

EIGRP 1/OSPF 1/RIP/ODR

IP Infrastructure Layer

STATIC
EIGRP 2
OSPF 2
BGP

STATIC
EIGRP 2
OSPF 2
BGP

NHRP Peer Mapping

- **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

- 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

- 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

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

DMVPN DETAILS
Dynamic Multipoint VPN (DMVPN) Major Features

- 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

- 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

• 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

• 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

NHRP mapping

Routing Table

Physical: 172.16.1.1
Tunnel0: 10.0.0.1

192.168.1.0/24
10.0.0.1 → 172.17.0.1

192.168.0.0/24 Conn.
192.168.1.0/24 → 10.0.0.1
192.168.2.0/24 → 10.0.0.12

192.168.0.0/24 Conn.
192.168.1.0/24 → 10.0.0.1
192.168.2.0/24 → 10.0.0.12

Spoke A

Physical: 192.168.1.1/24

Spoke B

Physical: (dynamic)
Tunnel0: 10.0.0.11

Physical: (dynamic)
Tunnel0: 10.0.0.12

10.0.0.1
Æ
172.17.0.1
Æ
172.17.0.1
Æ
172.17.0.1
Æ
172.16.1.1
Æ
172.16.2.1

Building Hub-and-Spoke tunnels

NHRP Registration

IKE Initialization
IKE/IPsec Established
NHRP Regist. Req.
Routing Adjacency
Routing Update
Encrypted

IKE Initialization
IKE/IPsec Established
NHRP Regist. Req.
Routing Adjacency
Routing Update
Encrypted
Dynamic Spoke-Spoke Tunnels

- 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

- 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

- 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

- 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

- 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

- 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**

- **Spoke 1 to Spoke 2**
  - NHRP Resolution Request
  - IKE Initialization
  - IKE/IPsec Established
  - NHRP Resolution Replies
  - Encrypted

### NHRP Resolution Switching

**Process Switching**

- **Spoke A**
  - Physical: 172.16.1.1
  - Tunnel: 10.0.0.1
  - 192.168.1.0/24
  - 172.17.0.1 (*)
  - 192.168.0.1/24

- **Spoke B**
  - Physical: 172.16.2.1
  - Tunnel: 10.0.0.12
  - 192.168.2.0/24
  - 172.16.2.1 (*)

- **Host 1 to Host 2**
  - 10.0.0.11 \(\rightarrow\) 172.16.1.1
  - 10.0.0.12 \(\rightarrow\) 172.16.2.1

- **NHRP Mapping**
  - 192.168.2.0/24 \(\rightarrow\) 172.16.2.1
  - 192.168.1.0/24 \(\rightarrow\) 172.16.1.1

- **Routing Table**
  - 10.0.0.1 \(\rightarrow\) 172.17.0.1 (*)
  - 10.0.0.12 \(\rightarrow\) 172.16.2.1
  - 192.168.1.0/24 \(\rightarrow\) 172.16.1.1 (l)
Building Spoke-Spoke Tunnels
CEF Switching

Host1 Spoke1 Hubs Spoke2 Host2

NHRP Res. Request
NHRP Res. Reply
IKE Initialization
IKE/IPSec Established
Encrypted

CEF FIB Table
CEF Adjacency

NHRP Resolution
CEF Switching

NHRP mapping (*NHS)

CEF FIB Table
CEF Adjacency

Spoke A

Spoke B

192.168.1.1/24

192.168.0.0/24

192.168.1.0/24

192.168.2.0/24

10.0.0.1

10.0.0.11

10.0.0.12

172.16.0.0/24

172.16.1.0/24

172.16.2.0/24

172.17.0.0/24

172.17.1.0/24

172.17.2.0/24

172.18.0.0/24

172.18.1.0/24

172.18.2.0/24

10.0.0.11

10.0.0.12

172.16.1.1

172.16.2.1

172.17.1.1

172.17.2.1

172.18.1.1

172.18.2.1

Conn.

Conn.

Conn.
DMVPN
Data Structures

- **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**

### 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

```
SpokeA#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

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

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

SpokeA#show 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 = 172.16.0.5, 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 = 172.16.2.2, access-list permit gre host 172.17.0.1 host 172.16.2.2
  SA lifetime: 4608000 KB/3600 s, PFS (Y/N): N, Transform sets={ trans1, }

DMVPN Crypto IPsec SAs

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# show 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,}
outbound esp sas: spi: 0x3B44DBD0(994368464) {Transport,}

DMVPN Routing Tables

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, 00:42:38, 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, 00:42:39, 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, 00:42:39, Tunnel0
S* 0.0.0.0/0 [1/0] via 172.16.1.1
Agenda

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

EXAMPLE DMVPN DEPLOYMENTS
Example DMVPN Deployments

- **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

- **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

Single DMVPN Dual Hub
Single mGRE tunnel on all nodes

192.168.0.0/24

192.168.1.0/24

192.168.2.0/24

Physical: 172.17.0.1
Tunnel0: 10.0.0.2

Physical: 172.17.0.1
Tunnel0: 10.0.0.1

Physical: (dynamic)
Tunnel0: 10.0.0.11

Physical: (dynamic)
Tunnel0: 10.0.0.12

Physical: 172.17.0.5
Tunnel0: 10.0.0.1

Spoke A

Spoke B

PC

Copyright © 2003, Cisco Systems, Inc. All rights reserved. Printed in USA.
Presentation_ID.scr

Single DMVPN Dual Hub
Crypto and Interface Configuration

crypto ca trustpoint msca-root
crypto ca certificate chain msca-root
certificate <router-certificate-id>
certificate ca 1244325DE0369880465F977A18F61CA8

crypto isakmp policy 1
crypto isakmp 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.<x>.<x> 255.255.255.0

interface Serial1/0
ip address 172.<x>|<x> 255.255.255.252
DMVPN Dual Hub

Hub1

- 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
Spoke A

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 multicast 172.17.0.5
  ip nhrp network-id 100000
  ip nhrp holdtime 360
  ip nhrp nh 10.0.0.1
  ip nhrp nh 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

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 multicast 172.17.0.5
  ip nhrp network-id 100000
  ip nhrp holdtime 360
  ip nhrp nh 10.0.0.1
  ip nhrp nh 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 NHRP tables

**Hub 1**

<table>
<thead>
<tr>
<th>Route: 10.0.0.2/32 via 10.0.0.2</th>
<th>Tunnel created 02:58:13, never expire</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type: static, Flags: authoritative used</td>
<td></td>
</tr>
<tr>
<td>NBMA address: 172.17.0.5</td>
<td></td>
</tr>
<tr>
<td>Route: 10.0.0.1/32 via 10.0.0.11</td>
<td>Tunnel created 02:51:46, expire 00:04:13</td>
</tr>
<tr>
<td>Type: dynamic, Flags: authoritative unique registered used</td>
<td></td>
</tr>
<tr>
<td>NBMA address: 172.16.1.1</td>
<td></td>
</tr>
<tr>
<td>Route: 10.0.0.12/32 via 10.0.0.12</td>
<td>Tunnel created 02:51:26, expire 00:04:33</td>
</tr>
<tr>
<td>Type: dynamic, Flags: authoritative unique registered used</td>
<td></td>
</tr>
<tr>
<td>NBMA address: 172.16.2.1</td>
<td></td>
</tr>
</tbody>
</table>

**Hub 2**

<table>
<thead>
<tr>
<th>Route: 10.0.0.1/32 via 10.0.0.1</th>
<th>Tunnel created 02:48:42, never expire</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type: static, Flags: authoritative used</td>
<td></td>
</tr>
<tr>
<td>NBMA address: 172.17.0.1</td>
<td></td>
</tr>
<tr>
<td>Route: 10.0.0.2/32 via 10.0.0.2</td>
<td>Tunnel created 02:51:20, never expire</td>
</tr>
<tr>
<td>Type: static, Flags: authoritative used</td>
<td></td>
</tr>
<tr>
<td>NBMA address: 172.17.0.5</td>
<td></td>
</tr>
<tr>
<td>Route: 10.0.0.11/32 via 10.0.0.11</td>
<td>Tunnel created 02:43:05, expire 00:05:01</td>
</tr>
<tr>
<td>Type: dynamic, Flags: authoritative unique registered</td>
<td></td>
</tr>
<tr>
<td>NBMA address: 172.16.1.1</td>
<td></td>
</tr>
<tr>
<td>Route: 10.0.0.12/32 via 10.0.0.12</td>
<td>Tunnel created 02:44:08, expire 00:05:20</td>
</tr>
<tr>
<td>Type: dynamic, Flags: authoritative unique registered used</td>
<td></td>
</tr>
<tr>
<td>NBMA address: 172.16.2.1</td>
<td></td>
</tr>
</tbody>
</table>

### DMVPN Dual Hub
#### Spoke NHRP tables

**Spoke A**

<table>
<thead>
<tr>
<th>Route: 10.0.0.1/32 via 10.0.0.1</th>
<th>Tunnel created 02:51:20, never expire</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type: static, Flags: authoritative used</td>
<td></td>
</tr>
<tr>
<td>NBMA address: 172.17.0.1</td>
<td></td>
</tr>
<tr>
<td>Route: 10.0.0.2/32 via 10.0.0.2</td>
<td>Tunnel created 02:51:20, never expire</td>
</tr>
<tr>
<td>Type: static, Flags: authoritative used</td>
<td></td>
</tr>
<tr>
<td>NBMA address: 172.17.0.5</td>
<td></td>
</tr>
<tr>
<td>Route: 10.0.0.12/32 via 10.0.0.12</td>
<td>Tunnel created 00:00:06, expire 00:05:05</td>
</tr>
<tr>
<td>Type: dynamic, Flags: router unique used</td>
<td></td>
</tr>
<tr>
<td>NBMA address: 172.16.2.1</td>
<td></td>
</tr>
</tbody>
</table>

**Spoke B**

<table>
<thead>
<tr>
<th>Route: 10.0.0.1/32 via 10.0.0.1</th>
<th>Tunnel created 02:51:18, never expire</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type: static, Flags: authoritative used</td>
<td></td>
</tr>
<tr>
<td>NBMA address: 172.17.0.1</td>
<td></td>
</tr>
<tr>
<td>Route: 10.0.0.2/32 via 10.0.0.2</td>
<td>Tunnel created 02:51:18, never expire</td>
</tr>
<tr>
<td>Type: static, Flags: authoritative used</td>
<td></td>
</tr>
<tr>
<td>NBMA address: 172.17.0.5</td>
<td></td>
</tr>
<tr>
<td>Route: 10.0.0.11/32 via 10.0.0.11</td>
<td>Tunnel created 00:00:24, expire 00:04:27</td>
</tr>
<tr>
<td>Type: dynamic, Flags: router unique used</td>
<td></td>
</tr>
<tr>
<td>NBMA address: 172.16.1.1</td>
<td></td>
</tr>
</tbody>
</table>
DMVPN Dual Hub Summary

- 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

- 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

• 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

• 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

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

Physical: 172.17.0.1
Tunnel0: 10.0.0.1

Spoke A

192.168.1.0/24

Spoke B

192.168.2.0/24

Spoke C

192.168.3.0/24

DMVPN Multi-Hub Hub1

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

route eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.0.0
  no auto-summary
**DMVPN Multi-Hub**

**Hub2**

```
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 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**

```
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 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
Spoke A

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

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

Hub3 NHRP mappings

Hub NHRP tables

Hub 1
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

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

- 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

• 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

• 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

**CAT6500**

**VPNSM**

- VLAN 11
- VPNSM 10
- VLAN 10 10.1.0.0
- SLB VIP 172.18.7.32
- VLAN 100 10.1.1.0

**MFSC**

- VLAN 10 10.1.0.0
- VLAN 100 10.1.1.0
- SLB VIP 172.18.7.32
- VLAN 100 10.1.1.0

**MWAM**

- Module 2
- Port 1 allowed-vlan 1,100
- Port 2 allowed-vlan 1,100
- Port 6 allowed-vlan 1,100
- IP SLB probe PING-PROBE
- 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: SLB Configuration

**MWAM Routers**

- SLB

---
DMVPN High Concentration Hub
MSFC Configuration

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 11,1002-1005
  switchport mode trunk

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
  ip address 10.1.1.2 255.255.255.0

interface Vlan100
  ip address 10.1.1.1 255.255.255.0

SAME SECONDARY FOR SPOKE NEIGHBOR

EIGRP and BGP ROUTING
DMVPN High Concentration Hub Spoke

```
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

- **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

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

• 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

• 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

Spoke A
192.168.1.1/24

10.0.0.11 \rightarrow 172.16.1.1
10.0.0.12 \rightarrow 172.16.2.1

Peer – 172.16.1.1
Peer – 172.16.2.2

NAT: 172.16.1.1 \rightarrow 172.18.101.1

NHRP mapping

Crypto Map Table

Spoke B

Physical: 172.16.1.1
Tunnel0: 10.0.0.1

10.0.0.11 \rightarrow 172.17.0.1
10.0.0.12 \rightarrow 172.17.0.2

Peer – 172.17.0.1

192.168.0.1/24

DMVPN and NAT-T
Transport Mode

Spoke A
192.168.1.1/24

10.0.0.11 \rightarrow 172.18.101.1*
10.0.0.12 \rightarrow 172.18.102.2*

Peers – 172.18.101.1*:
Peers – 172.18.102.2*

NAT: 172.18.101.1* \rightarrow 172.17.0.1

NHRP mapping *(NAT-T)

Crypto Map Table

Spoke B

Physical: 172.16.2.1
Tunnel0: 10.0.0.1

10.0.0.11 \rightarrow 172.17.0.1
10.0.0.12 \rightarrow 172.17.0.2

Peer – 172.17.0.1

192.168.2.1/24*
DMVPN and VRF
GRE Tunnel Packets in VRF

- 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

- 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

• Outbound spoke bandwidth smaller than 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

• Outbound hub bandwidth higher than 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

- Local outbound bandwidth could be higher or lower than 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?

- 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

• Advanced Design
• DMVPN Details
• Example DMVPN Deployments
• Interaction with other Features
• Management
• Performance and Futures
Management: A Case Study

- 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, QoS, Multicast) with Security as it’s primary concern.”

– Cisco IT

ECT Technology Overview

<table>
<thead>
<tr>
<th>Connectivity</th>
<th>Security</th>
<th>Network Integration</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Class Teleworker (ECT)</td>
<td>Public Key Infrastructure</td>
<td>DMVPN</td>
<td>Touchless Provisioning (ISC)</td>
</tr>
<tr>
<td></td>
<td>• PKI-AAA Integration</td>
<td></td>
<td>• Bootstrap PKI Certificates</td>
</tr>
<tr>
<td></td>
<td>• Auto Enrollment</td>
<td></td>
<td>• Dynamic Addressing and Call Home</td>
</tr>
<tr>
<td></td>
<td>• Multiple Trust Points</td>
<td></td>
<td>• Policy Push for IPsec, QoS, Firewall, IDS, NAT, Routing</td>
</tr>
<tr>
<td>Full Service Branch (FSB)</td>
<td>• Secure RSA Private Key</td>
<td></td>
<td>• Hub-and-spoke, full and partial mesh topologies</td>
</tr>
<tr>
<td></td>
<td>• Device and User Authentication</td>
<td></td>
<td>Ongoing Management (ISC)</td>
</tr>
<tr>
<td></td>
<td>• Secure ARP</td>
<td></td>
<td>• Management Tunnel</td>
</tr>
<tr>
<td>Enterprise Aggregation</td>
<td>• Authentication Proxy/ISAKMP</td>
<td></td>
<td>• Configuration Change</td>
</tr>
<tr>
<td></td>
<td>Device and User Authentication</td>
<td></td>
<td>• Notification</td>
</tr>
<tr>
<td></td>
<td>• Stateful Firewall</td>
<td></td>
<td>• Audit Checks</td>
</tr>
<tr>
<td>Service Provider Edge</td>
<td>Intrusion Protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SEC-4010
9830_06_2004_X2 © 2004 Cisco Systems, Inc. All rights reserved
ECT
Large Scale VPN Management Challenges

- 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

- 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

- 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

Device Abstraction Layer

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

ECT Management Tools Used

- 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

- 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)

- 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

- 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

- 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.)**

- 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**

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

- 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

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

- Code and platform support
- Performance
- Futures
Cisco IOS Code and Platform Support

- **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**

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

- **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

• 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

• 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

- 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
Recommended Reading

- 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!

**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

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

Two Hubs, single mGRE tunnel on all nodes

Physical: 172.17.0.5
Tunnel0: 10.0.0.2

Physical: 172.17.0.1
Tunnel0: 10.0.0.1

Physical: (dynamic)
Tunnel0: 10.0.0.11

Physical: (dynamic)
Tunnel0: 10.0.0.12

Physical: 172.17.0.5
Tunnel0: 10.0.0.2

Physical: 172.17.0.1
Tunnel0: 10.0.0.1

Spoke A

Spoke B

PC

Web

192.168.0.0/24

192.168.1.0/24

192.168.2.0/24

192.168.1.0/24

192.168.1.0/24

Single DMVPN Dual Hub

Hub1 Configuration

crypto ca trustpoint msca-root
  enrollment terminal
  crl optional
  rsakeypair hub1

crypto ca certificate chain msca-root
  certificate 2368DB55000000000B4E
  certificate ca 124432DE0369880465F977A18F61CA8

  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.)

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

crypto ca trustpoint msca-root
    enrollment terminal
crl optional
rsakeypair hub2
crypto ca certificate chain msca-root
    certificate 2279F316000000000000B40
    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.)

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

   route 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

crypto ca trustpoint msca-root
   enrollment terminal
crl optional
   rsakeypair spoke1
crypto ca certificate chain msca-root
   certificate 236FD38000000000000B4F
   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.)

```plaintext
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

```plaintext
crypto ca trustpoint msca-root
  enrollment terminal
  crl optional
  rsakeypair spoke1

crypto ca certificate chain msca-root
  certificate 2376A085000000000B50
  certificate 2376A085000000000B50

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.)

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

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

#### Hub1 Configuration

```plaintext
crypto ca trustpoint msca-root
    enrollment terminal
crl optional
rsakeypair hub1
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

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

#### Hub1 Configuration (Cont.)
Single DMVPN Multi-hub
Hub2 Configuration

crypto ca trustpoint msca-root
  enrollment terminal
crl optional
rsakeypair hub2

crypto ca certificate chain msca-root
  certificate 2368DB5500000000000B40
  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

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

```
crypto ca trustpoint msca-root
  enrollment terminal
  crl optional
  rsa keypair hub3

crypto ca certificate chain msca-root
  certificate 236DB5500000000000B48
  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


tunnel endpoint 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

```
crypto ca trustpoint msca-root
    enrollment terminal
crl optional
    rsakeypair spoke1
crypto ca certificate chain msca-root
    certificate 236FD38000000000000B4F
    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.)

```
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

```plaintext
crypto ca trustpoint msca-root
    enrollment terminal
    crl optional
    rsakeypair spoke1
crypto ca certificate chain msca-root
certificate 2376A0850000000000850
    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.)

```plaintext
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

```
crypto ca trustpoint msca-root
  enrollment terminal
  crl optional
  rsakeypair spoke1
crypto ca certificate chain msca-root
  certificate 2376A0850000000000B51
  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.)

```
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
```