Troubleshooting Dynamic Multipoint VPN (DMVPN)

BRKSEC-3012

© 2009 Cisco Systems, Inc. All rights reserved.
Cisco Public

Agenda

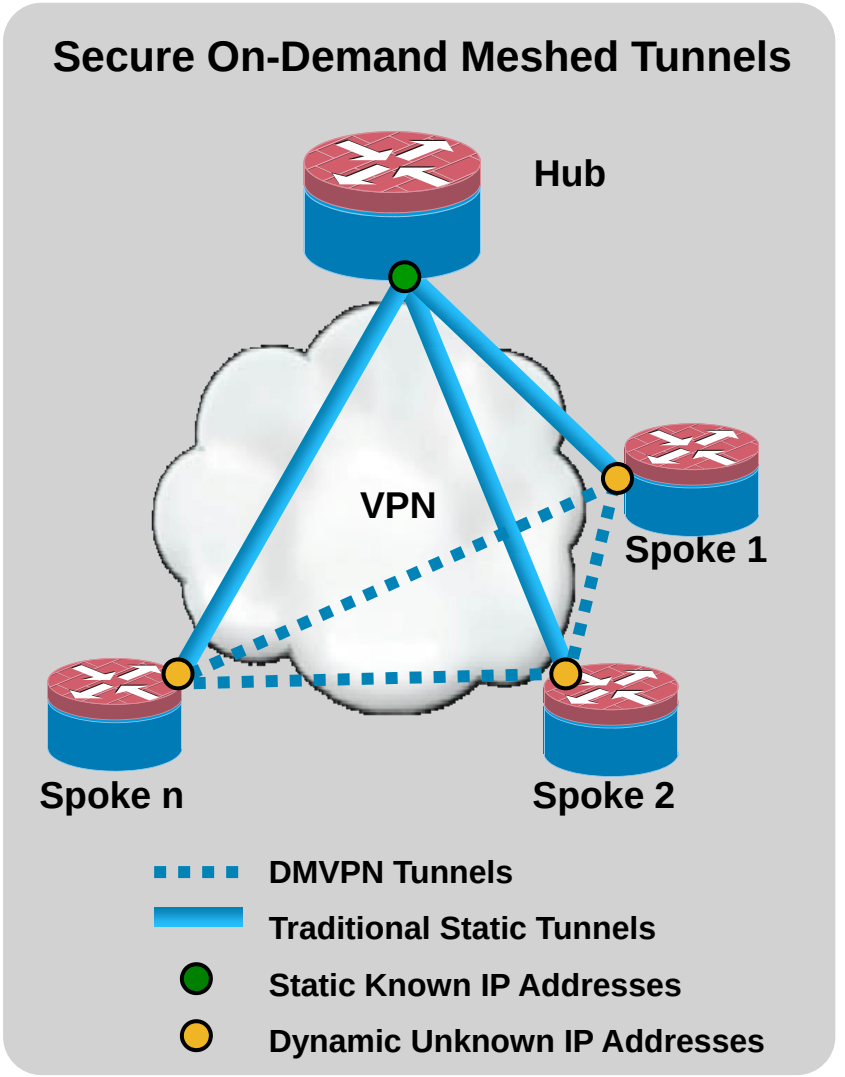
- DMVPN Overview
- Four Layer Troubleshooting Methodology
  - Common Issues
- Case Study
- DMVPN Best Practice Configuration
- Q & A

© 2008 Cisco Systems, Inc. All rights reserved.

DMVPN Overview

Dynamic Multipoint VPN

- Provides full meshed connectivity with simple configuration of hub and spoke
- Supports dynamically addressed spokes
- Facilitates zero-touch configuration for addition of new spokes
- Features automatic IPsec triggering for building an IPsec tunnel



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

What Is Dynamic Multipoint VPN?

- DMVPN is a Cisco IOS Software solution for building IPsec+GRE VPNs in an easy, dynamic and scalable manner
- DMVPN relies on two proven technologies
  - Next Hop Resolution Protocol (NHRP)
    - Creates a distributed (NHRP) mapping database of all the spoke's tunnel to real (public interface) addresses
  - Multipoint GRE Tunnel Interface
    - Single GRE interface to support multiple GRE/IPsec tunnels
    - Simplifies size and complexity of configuration

© 2008 Cisco Systems, Inc. All rights reserved.

DMVPN—How It Works

- Spokes have a dynamic permanent GRE/IPsec tunnel to the hub, but not to other spokes; they register as clients of the NHRP server
- When a spoke needs to send a packet to a destination (private) subnet behind another spoke, it queries the NHRP server for the real (outside) address of the destination spoke
- Now the originating spoke can initiate a dynamic GRE/IPsec tunnel to the target spoke (because it knows the peer address
- The spoke-to-spoke tunnel is built over the mGRE interface

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Dynamic Multipoint VPN (DMVPN) Major Features

- Configuration reduction and no-touch deployment
- IP unicast, IP multicast and dynamic routing protocols
- Spokes with dynamically assigned addresses
- NAT—spoke routers behind dynamic NAT and hub routers behind static NAT
- Dynamic spoke-spoke tunnels for scaling partial/full mesh VPNs
- Can be used without IPsec encryption
- VRFs—GRE tunnels and/or data packets in VRFs
- 2547oDMVPN—MPLS switching over tunnels
- QoS—aggregate; static/manual per-tunnel
- Transparent to most data packet level features
- Wide variety of network designs and options

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

DMVPN Components

- **Next Hop Resolution Protocol (NHRP)**

  Creates a distributed (NHRP) mapping database of all the spoke's tunnel to real (public interface) addresses

- **Multipoint GRE Tunnel Interface (MGRE)**

  Single GRE interface to support multiple GRE/IPsec tunnels

  Simplifies size and complexity of configuration

- **IPsec tunnel protection**

  Dynamically creates and applies encryption policies

- **Routing**

  Dynamic advertisement of branch networks; almost all routing protocols (EIGRP, RIP, OSPF, BGP, ODR) are supported

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

“Static” Spoke-Hub, Hub-Hub Tunnels

- **GRE, NHRP and IPsec configuration**
  - p-pGRE or mGRE on spokes; mGRE on hubs
- **NHRP registration**
  - Dynamically addressed spokes (DHCP, NAT,…)
- **Routing protocol, NHRP, and IP multicast**
  - On spoke-hub and hub-hub tunnels
- **Data traffic on spoke-hub tunnels**
  - All traffic for hub-and-spoke only networks
  - Spoke-spoke traffic while building spoke-spoke tunnels

© 2008 Cisco Systems, Inc. All rights reserved.

Dynamic Spoke-Spoke Tunnels

- **GRE, NHRP and IPsec configuration**
  - mGRE on both hub and spokes
- **Spoke-spoke unicast data traffic**
  - Reduced load on hubs
  - Reduced latency
    - Single IPsec encrypt/decrypt
- **On demand tunnel creates when need it**
- **NHRP resolutions and redirects**
  - Find NHRP mappings for spoke-spoke tunnels

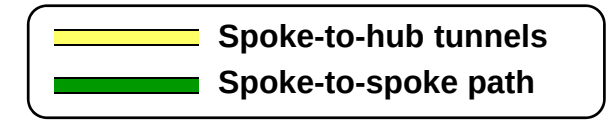
© 2008 Cisco Systems, Inc. All rights reserved.

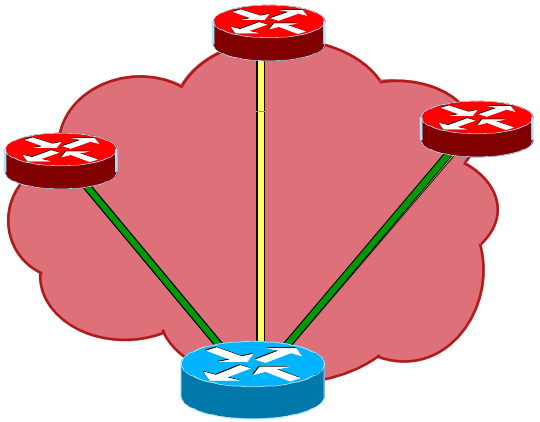
DMVPN Phases

Phase 1	Phase 2	Phase 3
• Hub and spoke functionality 12.2(13)T • Simplified and smaller config for hub & spoke • Support dynamically address CPE • Support for multicast traffic from hub to spoke • Summarize routing at hub	• Spoke to spoke functionality 12.3(4)T • Single mGRE interface in spokes • Direct spoke to spoke data traffic reduced load on hub • Cannot summarize spoke routes on hub • Route on spoke must have IP next hop of remote spoke	• Architecture and scaling 12.4(6)T • Increase number of hub with same hub and spoke ratio • No hub daisy-chain • Spokes don't need full routing table • OSPF routing protocol not limited to 2 hubs • Cannot mix phase 2 and phase 3 in same DMVPN cloud

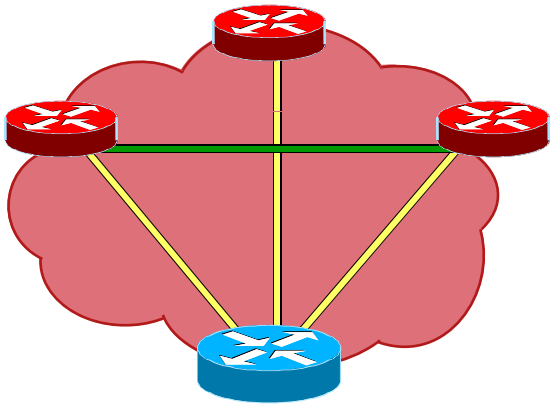
© 2008 Cisco Systems, Inc. All rights reserved.

Network Designs

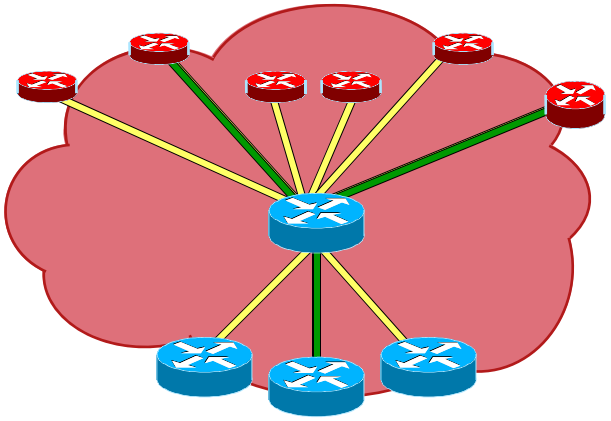




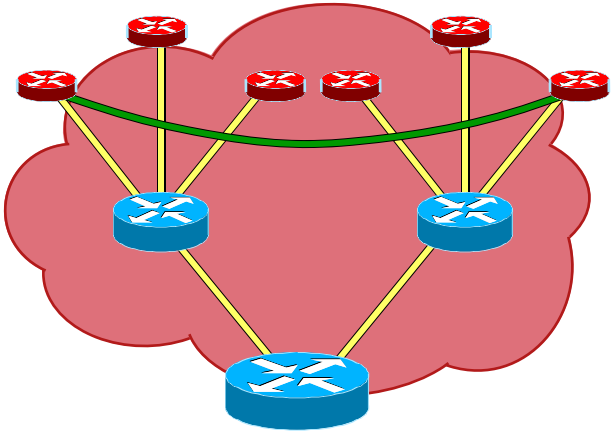
Hub and spoke (Phase 1)



Spoke-to-spoke (Phase 2)



Server Load Balancing



Hierarchical (Phase 3)

© 2008 Cisco Systems, Inc. All rights reserved.

Four Layer Troubleshooting Methodology

Before You Begin

- Sync up the timestamps between the hub and spoke
- Enable msec debug and log timestamps

  service timestamps debug date time msec

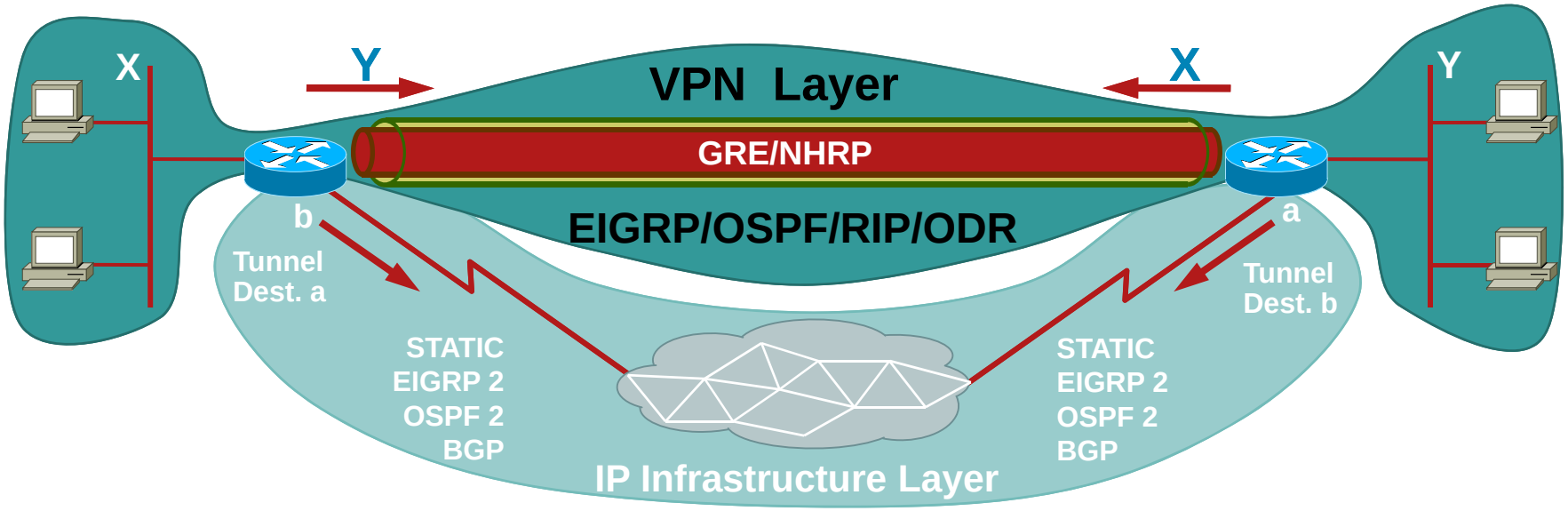
  service timestamps log date time msec
- Enable “terminal exec prompt timestamp” for the debugging sessions.

  This way you can easily correlate the debug output with the show command output

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layer Troubleshooting Methodology

- Four layers for troubleshooting
  - Physical and routing layer
  - IPsec encryption layer—IPsec/ISAKMP
  - GRE encapsulation layer—NHRP
  - VPN routing layer—routing and IP data

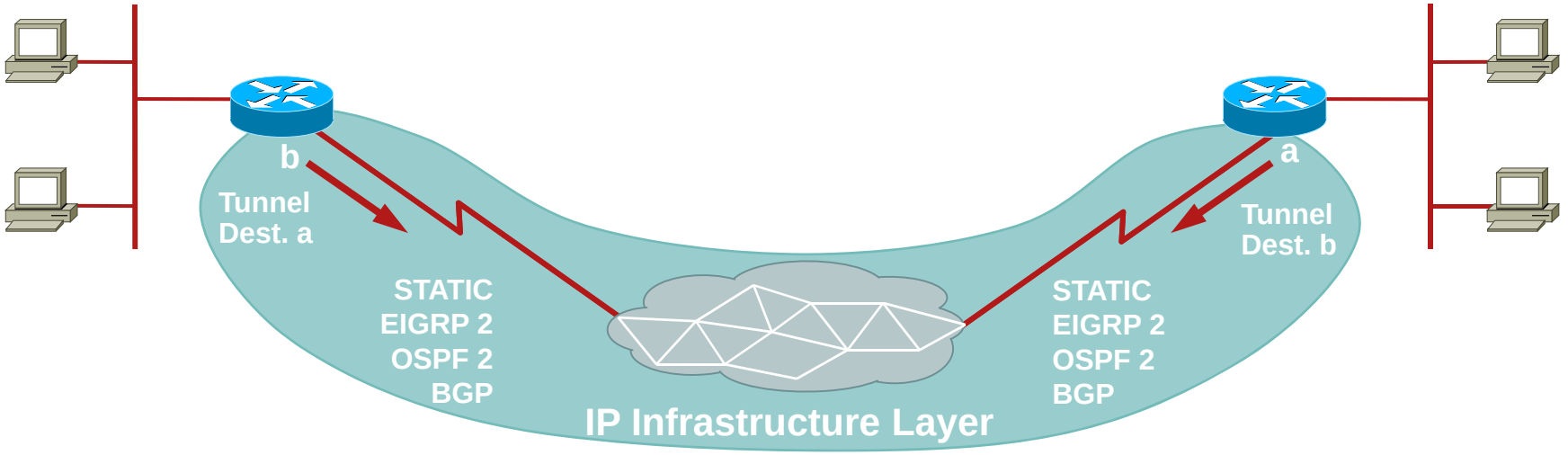


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: Physical and Routing Layer

- Physical (NBMA or tunnel endpoint) routing layer

  This is getting the encrypted tunnel packets between the tunnel endpoints (DMVPN hub and spoke or between spoke and spoke routers)



© 2008 Cisco Systems, Inc. All rights reserved.

Four Layers for Troubleshooting: Physical and Routing Layer

- Ping from the hub to the spoke's using NBMA addresses (and reverse):
  - These pings should go directly out the physical interface, not through the DMVPN tunnel
  - Hopefully there isn't a firewall that blocks ping packets
  - If this doesn't work, check the routing and any firewalls between the hub and spoke routers
- Also use traceroute to check the path that the encrypted tunnel packets are taking
- Check for “administratively prohibited” (ACL) messages

© 2008 Cisco Systems, Inc. All rights reserved.

Four Layers for Troubleshooting: Physical and Routing Layer (Cont.)

- **Debugs and show commands use if no connectivity**

  debug ip icmp

  Valuable tool used to troubleshoot connectivity issues

  Helps you determine whether the router is sending or receiving ICMP messages

```
ICMP: rcvd type 3, code 1, from 172.17.0.1
ICMP: src 172.17.0.1, dst 172.16.1.1, echo reply
ICMP: dst (10.120.1.0) port unreachable rcv from 10.120.1.15
ICMP: src 172.17.0.5, dst 172.16.1.1, echo reply
```

Debug icmp field descriptions: http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_il.html#wp1011953

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: Physical and Routing Layer (Cont.)

- **Debugs and show commands use if no connectivity (cont.)**

  debug ip packet [*access-list-number*] [detail] [dump]

  Useful tool use for troubleshooting end to end communication

  IP packet debugging captures the packets that are process switched including received, generated and forwarded packets

```
IP: s=172.16.1.1 (local), d=172.17.0.1 (FastEthernet0/1), len 100, sending
        ICMP type=8, code=0
IP: table id=0, s=172.17.0.1 (FastEthernet0/1), d=172.16.1.1 (FastEthernet0/1), routed via RIB
IP: s=172.17.0.1 (FastEthernet0/1), d=172.16.1.1 (FastEthernet0/1), len 100, rcvd 3
        ICMP type=0, code=0
```

Caution: Debug IP packet command can generate a substantial amount of output and uses a substantial amount of system resources. This command should be used with caution in production networks. Always use with an ACL.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: Physical and Routing Layer

Common Issues:

- ACL in firewall/ISP side block ISAKMP traffic
- Traffic filtering resulting traffic flows one direction

© 2008 Cisco Systems, Inc. All rights reserved.

Common Issues:
ACL in Firewall/ISP Side Block ISAKMP Traffic

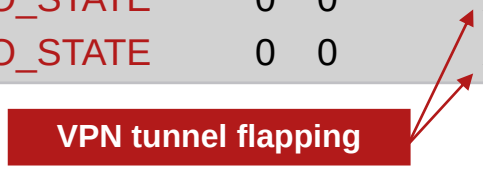
Problem:

- Network connectivity between hub and spoke is fine
- IPsec tunnel is not coming up
- How to detect?

show crypto isa sa

IPv4 Crypto ISAKMP SA

Dst	src	state	conn-id	slot	status	
172.17.0.1	172.16.1.1	MM_NO_STATE	0	0	ACTIVE	
172.17.0.1	172.16.1.1	MM_NO_STATE	0	0	ACTIVE	(deleted)
172.17.0.5	172.16.1.1	MM_NO_STATE	0	0	ACTIVE	
172.17.0.5	172.16.1.1	MM_NO_STATE	0	0	ACTIVE	(deleted)



© 2008 Cisco Systems, Inc. All rights reserved.

Common Issues:
ACL in Firewall/ISP Side Block ISAKMP Traffic

- Further check debug crypto isakmp to verify spoke router is sending udp 500 packet

debug crypto isakmp

```
04:14:44.450: ISAKMP:(0):Old State = IKE_READY  New State = IKE_I_MM1
04:14:44.450: ISAKMP:(0): beginning Main Mode exchange
04:14:44.450: ISAKMP:(0): sending packet to 172.17.0.1 my_port 500 peer_port 500 (I) MM_NO_STATE
04:14:44.450: ISAKMP:(0):Sending an IKE IPv4 Packet.
04:14:54.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
04:14:54.450: ISAKMP (0:0): incrementing error counter on sa, attempt 1 of 5: retransmit phase 1
04:14:54.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
04:14:54.450: ISAKMP:(0): sending packet to 172.17.0.1 my_port 500 peer_port 500 (I) MM_NO_STATE
04:14:54.450: ISAKMP:(0):Sending an IKE IPv4 Packet.
04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
04:15:04.450: ISAKMP (0:0): incrementing error counter on sa, attempt 2 of 5: retransmit phase 1
04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
04:15:04.450: ISAKMP:(0): sending packet to 172.17.0.1 my_port 500 peer_port 500 (I) MM_NO_STATE
04:15:04.450: ISAKMP:(0):Sending an IKE IPv4 Packet.
```

Above debug output shows spoke router is sending udp 500 packet every 10 secs

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Common Issues:
ACL in Firewall/ISP Side Block ISAKMP Traffic

- How to fix?

  Check with either firewall admin OR ISP admin if spoke router is directly connected to ISP router to make sure they are allowing udp 500 traffic

  After ISP or Firewall admin allowed udp 500 add inbound ACL in egress interface which is tunnel source to allow udp 500 to make sure UDP 500 traffic coming into the router show access-list to verify hit counts are incrementing

show access-lists 101

```
Extended IP access list 101
    10 permit udp host 172.17.0.1 host 172.16.1.1 eq isakmp log (4 matches)
    20 permit udp host 172.17.0.5 host 172.16.1.1 eq isakmp log (4 matches)
    30 permit ip any any (295 matches)
```

Caution: Make sure you have ‘ip any any’ allowed in your access-list otherwise all other traffic will be blocked by this acl applied inbound on egress interface.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Common Issues:
ACL in Firewall/ISP Side Block ISAKMP Traffic

- How to verify?

show crypto isa sa

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id  slot  status
172.17.0.1      172.16.1.1      QM_IDLE           1009    0    ACTIVE
172.17.0.5      172.16.1.1      QM_IDLE           1008    0    ACTIVE
```

Phase 1 is UP, UDP 500 packet received

debug crypto isa

```
ISAKMP:(0):Old State = IKE_READY  New State =IKE_I_MM1
ISAKMP:(0): beginning Main Mode exchange
ISAKMP:(0): sending packet to 172.17.0.1 my_port 500 peer_port 500 (I) MM_NO_STATE
ISAKMP (0:0): received packet from 172.17.0.1 dport 500 sport 500 Global (I) MM_NO_STATE
ISAKMP:(0):Sending an IKE IPv4 Packet Old State = IKE_R_MM1  New State = IKE_R_MM2
ISAKMP:(0):atts are acceptable
…
ISAKMP:(1009):Old State = IKE_R_MM3  New State IKE_R_MM3
…
ISAKMP:(1009):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Common Issues:
Traffic Filtering, Traffic Flows One Direction

Problem

- VPN tunnel between spoke to spoke router is UP
- Unable to pass data traffic
- How to detect?

```
spoke1# show crypto ipsec sa peer 172.16.2.11
  local  ident (addr/mask/prot/port):    (172.16.1.1/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
   #pkts encaps: 110, #pkts encrypt: 110,  #pkts decaps: 0, #pkts decrypt: 0,
local crypto endpt.: 172.16.1.1,  remote crypto endpt.: 172.16.2.11
     inbound esp sas:  spi: 0x4C36F4AF(1278669999)
     outbound esp sas:  spi: 0x6AC801F4(1791492596)
```

```
spoke2#show crypto ipsec sa peer 172.16.1.1
  local  ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
  #pkts encaps: 116, #pkts encrypt: 116,  #pkts decaps: 110, #pkts decrypt: 110,
local crypto endpt.: 172.16.2.11,  remote crypto endpt.: 172.16.1.1
    inbound esp sas: spi: 0x6AC801F4(1791492596)
    outbound esp sas: spi: 0x4C36F4AF(1278669999)
```

There is no decap packets in Spoke 1, which means ESP packets are dropped some where in the path return from Spoke 2 towards Spoke1

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Common Issues: Traffic Filtering, Traffic Flows One Direction

- **How to fix?**

  Spoke 2 router shows both encap and decap which means either firewall in spoke 2 customer side ahead of router or ISP device in spoke 2 or any where in path between spoke 2 router and spoke 1 router filter ESP traffic

- **How to verify?**

```
spoke1# show crypto ipsec sa peer 172.16.2.11
  local  ident (addr/mask/prot/port):    (172.16.1.1/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
   #pkts encaps: 300, #pkts encrypt: 300
   #pkts decaps: 200, #pkts decrypt: 200,
```

```
spoke2#sh cry ipsec sa peer 172.16.1.1
  local  ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
  #pkts encaps: 316, #pkts encrypt: 316,
  #pkts decaps: 300, #pkts decrypt: 310,
```

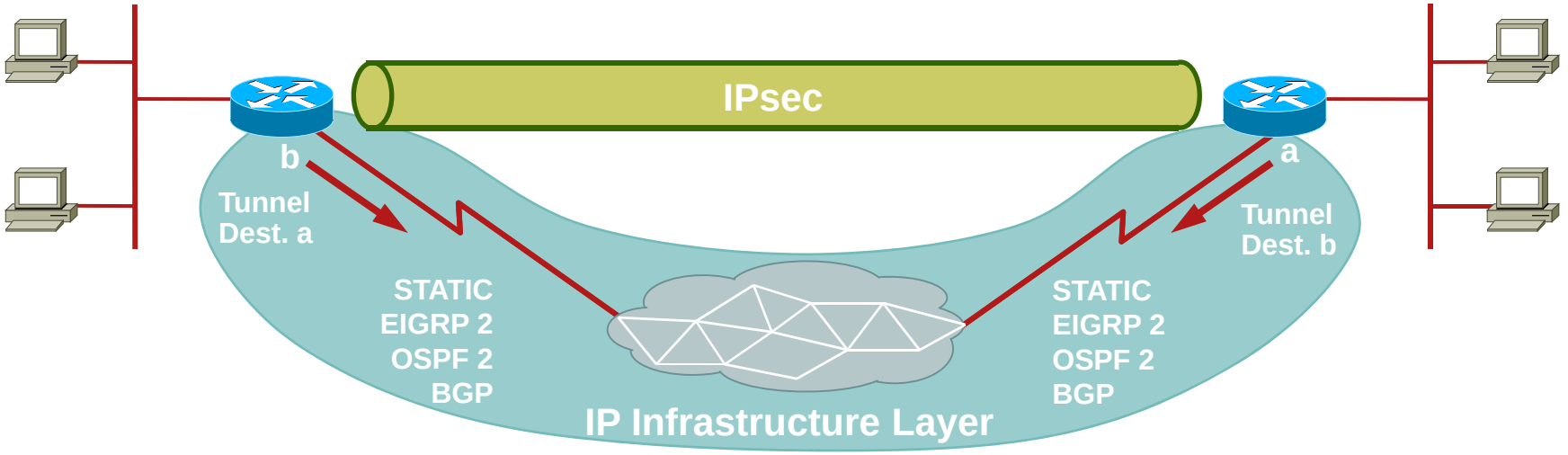
After allowed ESP (IP protocol 50) Spoke 1 and Spoke 2 both shows encaps and decaps, counters are incrementing.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: IPsec Encryption Layer

- The IPsec encryption layer—

  This is encrypting the GRE tunnel packet going out and decrypting the IPsec packet coming in to reveal the GRE encapsulated packet



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: IPsec Encryption Layer—IPsec Component

DMVPN Component-IPsec

- DMVPN introduced tunnel protection
- The profile must be applied on the tunnel interface

  tunnel protection ipsec profile prof
- Internally Cisco IOS Software will treat this as a dynamic crypto map and it derives the local-address, set peer and match address parameters from the tunnel parameters and the NHRP cache
- This must be configured on the hub and spoke tunnels

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: IPsec Encryption Layer—IPsec Component

DMVPN Component-IPsec (Cont.)

- A transform set must be defined:

```
crypto ipsec transform-set ts esp-3des esp-sha-hmac
  mode transport
```

- An IPsec profile replaces the crypto map

```
crypto ipsec profile prof
  set transform-set ts
```

- The IPsec profile is like a crypto map without “set peer” and “match address”

```
Interface Tunnel0
 Ip address 10.0.0.1 255.255.255.0
 :
 tunnel source fast ethernet0/0

 tunnel protection ipsec profile prof
```

Note: GRE Tunnel Keepalives are not supported in combination with Tunnel Protection

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: IPsec Encryption Layer

IPsec Layer Verification-show commands

- Verify that ISAKMP SAs and IPsec SAs between the NBMA addresses of the hub and spoke have being created

  show crypto isakmp sa detail

  show crypto IPsec sa peer <NBMA-address-peer>

- Notice SA lifetime values

  If they are close to the configured lifetimes (default --24 hrs for ISAKMP and 1 hour for IPsec) then that means these SAs have been recently negotiated

  If you look a little while later and they have been re-negotiated again, then the ISAKMP and/or IPsec may be bouncing up and down

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: IPsec Encryption Layer

IPsec Layer Verification-show commands (Cont.)

- New show commands for dmvpn introduced in 12.4(9)T that has brief and detail output

show dmvpn detail

Covers both Isakmp phase 1 and IPsec phase 2 status

Does not show remaining life time for both Isakmp phase1 and IPsec phase 2 ,to check life time still use old commands

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


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: IPsec Encryption Layer

IPsec Layer Verification-debug commands

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

  debug crypto isakmp

  debug crypto ipsec

  debug crypto engine

  New command debug dmvpn detail crypto

  Introduced in 12.4(9)T

- Use conditional debugging on the hub router to restrict the crypto debugs to only show debugs for the particular spoke in question:

  debug crypto condition peer ipv4 <nbma address>

  debug dmvpn condition peer <nbma|tunnel>

- Verify the communication between NHRP and IPsec by showing the crypto map and socket tables

  show crypto map

  show crypto socket

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: IPsec Encryption Layer—Show Commands

show crypto isakmp sa

```
Router# show crypto isakmp sa
dst             src          state          connid    slot
172.17.0.1   172.16.1.1     QM_IDLE           1         0
```

IKE Phase 1 status UP

show crypto isakmp sa detail

```
Router# show crypto isakmp sa detail
Codes: C - IKE configuration mode,
       D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
        psk - Preshared key, rsig - RSA signature,   renc - RSA encryption

C-id  Local           Remote        I-VRF Encr Hash Auth DH Lifetime Cap.
1     172.16.1.1      172.17.0.1          3des sha  psk  1  23:59:40
       Connection-id:Engine-id =  1:1(hardware)
```

Encryption:3des
Authentication :Pre-shared key
Remaining lifetime before phase 1 re-key

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: IPsec Encryption Layer—Show Commands

show crypto ipsec sa

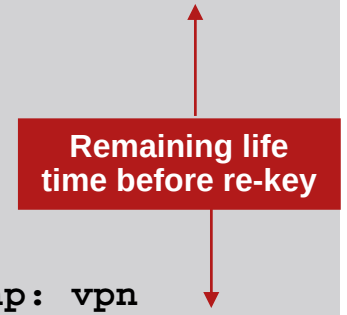
```
Router# show crypto ipsec sa
interface: Ethernet0/3
    Crypto map tag: vpn, local addr. 172.17.0.1
  local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
  current_peer: 172.17.0.1:500
    PERMIT, flags={origin_is_acl,}
  #pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19
  #pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compr'ed: 0, #pkts compr. failed: 0, #pkts decompr. failed: 0
  #send errors 1, #recv errors 0
   local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.17.0.1
   path mtu 1500, media mtu 1500
   current outbound spi: 8E1CB77A
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: IPsec Encryption Layer—Show Commands

show crypto ipsec sa (cont.)

```
 inbound esp sas:
      spi: 0x4579753B(1165587771)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4456885/3531)
        IV size: 8 bytes
        replay detection support: Y
outbound esp sas:
      spi: 0x8E1CB77A(2384246650)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4456885/3531)
        IV size: 8 bytes
        replay detection support: Y
```



© 2008 Cisco Systems, Inc. All rights reserved.

Four Layers for Troubleshooting: IPsec Encryption Layer—Show Commands

show dmvpn

```
HUB-1#show dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer

Tunnel1, Type:Hub, NHRP Peers:2,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1          1.1.1.1      172.20.1.1    UP 00:04:32 D
     1          2.2.2.2      172.20.1.2    UP 00:01:25 D

SPOKE-1#show dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incompletea
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer

Tunnel1, Type:Spoke, NHRP Peers:1,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1          3.3.3.3    172.20.1.100    UP 00:21:56 S
```

Learn Dynamically, Entry shows either in hub or in spoke for spoke to spoke tunnels

Static NHRP mapping

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: IPsec Encryption Layer—Show Commands

show dmvpn detail

```
HUB-1#show dmvpn detail

Legend: Attrb --> S - Static, D - Dynamic, I - Incompletea
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer

 ------------- Interface Tunnel1 info: -------------
Intf. is up, Line Protocol is up, Addr. is 172.20.1.100
   Source addr: 3.3.3.3, Dest addr: MGRE
  Protocol/Transport: "multi-GRE/IP", Protect "gre_prof",
Tunnel VRF "", ip vrf forwarding ""

NHRP Details:
Type:Hub, NBMA Peers:2
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1         1.1.1.1      172.20.1.1    UP 00:26:38 D         172.20.1.1/32

  IKE SA: local 3.3.3.3/500 remote 1.1.1.1/500 Active
  Crypto Session Status: UP-ACTIVE
  fvrf: (none)
  IPSEC FLOW: permit 47 host 3.3.3.3 host 1.1.1.1
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0xB28957C6, transform : esp-3des esp-sha-hmac
    Socket State: Open
```

Only One Peer Shown

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: IPsec Encryption Layer—debug crypto condition

- The crypto conditional debug CLIs **(debug crypto condition, debug crypto condition unmatched, and show crypto debug-condition)** allow you to specify conditions (filter values) in which to generate and display debug messages related only to the specified conditions
- The router will perform conditional debugging only after at least one of the global crypto debug commands **(debug crypto isakmp, debug crypto ipsec,** or **debug crypto engine)** has been enabled. This requirement helps to ensure that the performance of the router will not be impacted when conditional debugging is not being used.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: IPsec Encryption Layer—debug crypto Condition

- To enable crypto conditional debugging:

  debug crypto condition <cond-type> <cond-value>
  debug crypto { isakmp | ipsec | engine }

- To view crypto condition debugs that have been enabled:

  show crypto debug-condition [all | peer | fvrf | ivrf | isakmp | username | connid | spi]

- To disable crypto condition debugs:

  debug crypto condition reset

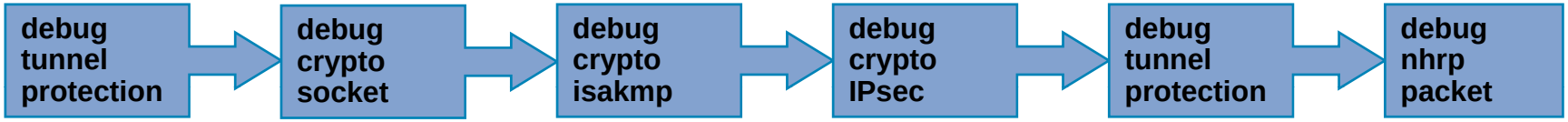
© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: IPsec Encryption Layer—debug crypto Condition

Fvrf	The name string of a virtual private network (VPN) routing and forwarding (VRF) instance. Relevant debug messages will be shown if the current IPsec operation uses this VRF instance as its front-door VRF (FVRF).
ivrf	The name string of a VRF instance. Relevant debug messages will be shown if the current IPsec operation uses this VRF instance as its inside VRF (IVRF).
isakmp profile	The name string of the isakmp profile to be matched against for debugging.
Local ipv4	The ip address string of the local IKE endpoint.
Peer group	A ezvpn group name string. Relevant debug messages will be shown if the peer is using this group name as its identity.
Peer ipv4	A single IP address. Relevant debug messages will be shown if the current IPsec operation is related to the IP address of this peer.
Peer subnet	A subnet and a subnet mask that specify a range of peer IP addresses. Relevant debug messages will be shown if the IP address of the current IPsec peer falls into the specified subnet range.
Peer hostname	A fully qualified domain name (FQDN) string. Relevant debug messages will be shown if the peer is using this string as its identity.
username	The username string (XAuth username or PKI-aaa username obtained from a certificate).

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: IPsec Encryption Layer—debug dmvpn detail all



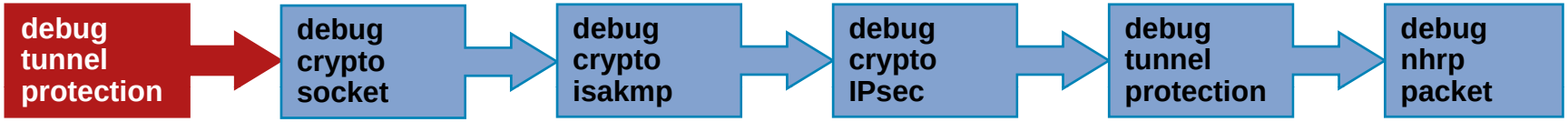
- debug dmvpn introduced in 12.4(9)T

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

- One complete debug to help troubleshoot dmvpn issues

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: IPsec Encryption Layer—debug dmvpn detail all (Cont.)

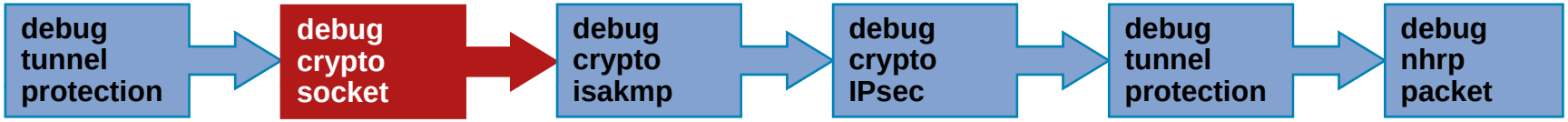


- Tunnel protection configured on tunnel interface open crypto socket as soon as either router or tunnel came up

```
IPSEC-IFC MGRE/Tu0: Checking tunnel status
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): Opening a socket with profile dmvpn
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): connection lookup returned 0
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): Triggering tunnel immediately.
IPSEC-IFC MGRE/Tu0: tunnel coming up
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): Opening a socket with profile dmvpn
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): connection lookup returned 83884274
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): Socket is already being opened. Ignoring
```


© 2008 Cisco Systems, Inc. All rights reserved.

Four Layers for Troubleshooting: IPsec Encryption Layer—debug dmvpn detail all (Cont.)



- Shows socket state
- Crypto socket debug shows creation of local and remote proxy id

CRYPTO_SS (TUNNEL SEC): **Application started listening**

insert of map into mapdb AVL failed, map + ace pair already exists on the mapdb

CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

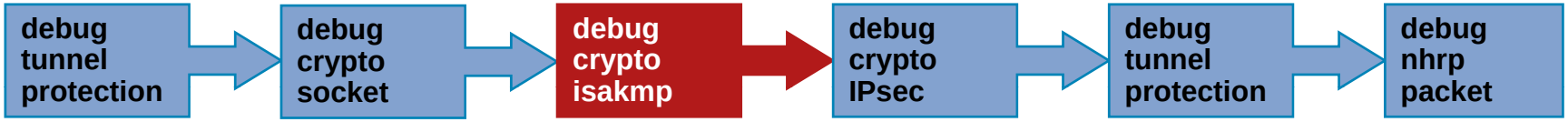
CRYPTO_SS(TUNNEL SEC): **Active open**, socket info:

local 172.16.2.11 172.16.2.11/255.255.255.255/0,

remote 172.17.0.1 172.17.0.1/255.255.255.255/0, prot 47, ifc Tu0

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: IPsec Encryption Layer—debug dmvpn detail all (Cont.)



- IKE negotiation
- Shows six packet exchange(MM1-MM6) in main mode
- See Appendix for complete crypto debugs

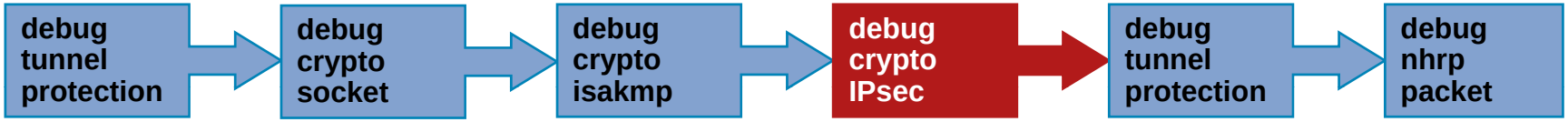
```
ISAKMP:(0):Old State = IKE_READY  New State = IKE_I_MM1
ISAKMP:(0): beginning Main Mode exchange
ISAKMP:(0): sending packet to 172.17.0.1 my_port 500 peer_port 500 (I) MM_NO_STATE
ISAKMP:(0):Sending an IKE IPv4 Packet
ISAKMP:(0):Old State = IKE_I_MM1  New State = IKE_I_MM2
ISAKMP:(0):Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:(0):atts are acceptable. Next payload is 0
ISAKMP:(0):Old State = IKE_I_MM2  New State = IKE_I_MM3
ISAKMP:(0):Old State = IKE_I_MM3  New State = IKE_I_MM4
ISAKMP:(1051):Old State = IKE_I_MM4  New State = IKE_I_MM5
ISAKMP:(1051):Old State = IKE_I_MM5  New State = IKE_I_MM6
ISAKMP:(1051):Old State = IKE_I_MM6  New State = IKE_P1_COMPLETE
```

IKE has found matching policy

IKE complete authentication

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: IPsec Encryption Layer—debug dmvpn detail all (Cont.)



- IKE negotiates to set up the IP Security (IPsec) SA by searching for a matching transform set
- Creation of inbound and outbound security association database (SADB)

```
ISAKMP:(1051):beginning Quick Mode exchange, M-ID of 1538742728
ISAKMP:(1051):Old State = IKE_QM_READY  New State = IKE_QM_I_QM1
ISAKMP:(1051):atts are acceptable.
INBOUND local= 172.16.2.11, remote= 172.17.0.5,
local_proxy= 172.16.2.11/255.255.255.255/47/0 (type=1),
remote_proxy= 172.17.0.5/255.255.255.255/47/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac  (Transport),
ISAKMP:(1051): Creating IPsec SAs
inbound SA from 172.17.0.5 to 172.16.2.11 (f/i)  0/ 0
 (proxy 172.17.0.5 to 172.16.2.11)
has spi 0xE563BB42 and conn_id 0
outbound SA from 172.16.2.11 to 172.17.0.5 (f/i) 0/0
(proxy 172.16.2.11 to 172.17.0.5)
has spi  0xFE745CBD and conn_id 0
ISAKMP:(1051):Old State = IKE_QM_I_QM1  New State = IKE_QM_PHASE2_COMPLETE
```

Phase 2 Complete

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: IPsec Encryption Layer

Common Issues:

- Incompatible ISAKMP Policy
- DMVPN Hub and Ezvpn server in same Router.
- Incompatible IPsec transform set

© 2008 Cisco Systems, Inc. All rights reserved.

Common Issues: Incompatible ISAKMP Policy

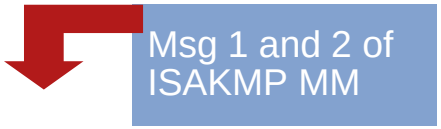
- If the configured ISAKMP policies don't match the proposed policy by the remote peer, the router tries the default policy of 65535, and if that does not match either, it fails ISAKMP negotiation

```
Default protection suite
encryption algorithm:   DES—Data Encryption Standard (56 bit keys).
hash algorithm:         Secure Hash Standard
authentication method:  Rivest-Shamir-Adleman Signature
Diffie-Hellman group:   #1 (768 bit)
lifetime:               86400 seconds, no volume limit
```

- A show crypto isakmp sa shows the ISAKMP SA to be in MM_NO_STATE, meaning that main-mode failed

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Common Issues: Incompatible ISAKMP Policy (Cont.)




```
ISAKMP (0:1): processing SA payload.
message ID = 0

ISAKMP (0:1): found peer pre-shared
key matching 209.165.200.227

ISAKMP (0:1): Checking ISAKMP
transform 1 against priority 1 policy

ISAKMP:       encryption 3DES-CBC

ISAKMP:       hash MD5

ISAKMP:       default group 1

ISAKMP:       auth pre-share

ISAKMP:       life type in seconds

ISAKMP:       life duration (VPI) of
0x0 0x1 0x51 0x80

ISAKMP (0:1): Hash algorithm offered
does not match policy!

ISAKMP (0:1): atts are not acceptable.
Next payload is 0
```

```
ISAKMP (0:1): Checking ISAKMP
transform 1 against priority 65535
policy

ISAKMP:       encryption 3DES-CBC

ISAKMP:       hash MD5

ISAKMP:       default group 1

ISAKMP:       auth pre-share

ISAKMP:       life type in seconds

ISAKMP:       life duration (VPI) of
0x0 0x1 0x51 0x80

ISAKMP (0:1): Encryption algorithm
offered does not match policy!

ISAKMP (0:1): atts are not acceptable.
Next payload is 0

ISAKMP (0:1): no offers accepted!

ISAKMP (0:1): phase 1 SA not
acceptable!
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

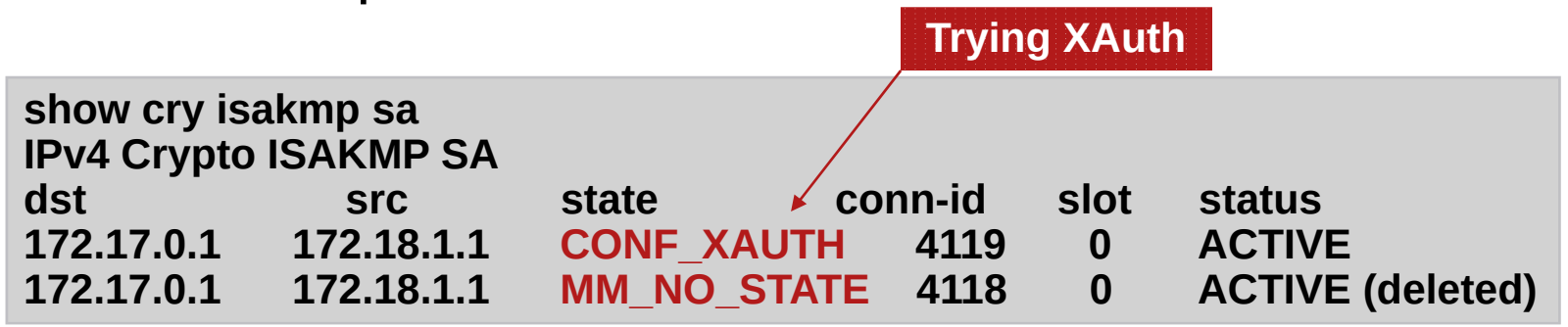
Common Issues:
DMVPN Hub and Ezvpn server in same Router

Problem Description:

DMVPN hub and Ezvpn server configured in same router which result DMVPN spokes unable to connect only Ezvpn hardware and software clients are connecting.

How to Detect?

- Check Isakmp status



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Common Issues:
DMVPN Hub and Ezvpn server in same Router

- Run Isakmp debug to verify what you see in show command.

```
ISAKMP:(4119):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(4119):Old State = IKE_R_MM4  New State = IKE_R_MM5
ISAKMP:(4119): processing ID payload. message ID = 0
ISAKMP (0:4119): ID payload
        next-payload : 8
        type         : 1
        address      : 10.1.1.1
        protocol     : 17
        port         : 0
        length       : 12
bring down existing phase 1 and 2 SA's with local 172.17.0.1 remote 172.18.1.1 remote port 1024
ISAKMP:(4119):returning IP addr to the address pool
ISAKMP:(4118):received initial contact, deleting SA
ISAKMP:(4118):deleting SA reason "Receive initial contact" state (R) CONF_XAUTH    (peer 172.18.1.1)
ISAKMP:(4119):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(4119):Old State = IKE_R_MM5  New State = IKE_R_MM5
ISAKMP: set new node 616549739 to CONF_XAUTH
ISAKMP:(4118):Input = IKE_MESG_INTERNAL, IKE_PHASE1_DEL
ISAKMP:(4118):Old State = IKE_XAUTH_REQ_SENT  New State = IKE_DEST_SA
ISAKMP:(4119):Need XAUTH
ISAKMP: set new node -701088864 to CONF_XAUTH
ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2
ISAKMP:(4119): initiating peer config to 172.18.1.1. ID = -701088864
ISAKMP:(4119): sending packet to 172.18.1.1 my_port 4500 peer_port 1024 (R) CONF_XAUTH
ISAKMP:(4119):Sending an IKE IPv4 Packet.
ISAKMP:(4119):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP:(4119):Old State = IKE_P1_COMPLETE  New State = IKE_XAUTH_REQ_SENT
```

© 2008 Cisco Systems, Inc. All rights reserved.

Common Issues:
DMVPN Hub and Ezvpn server in same Router

- Check existing configuration that don't allow DMVPN spoke to come up and give **CONF_XAUTH message in debugs**

```
crypto isakmp client configuration group vpnclient
 key cisco123
 pool vpn
 acl 190
crypto ipsec transform-set t3 esp-3des esp-md5-hmac
crypto dynamic-map test 10
 set transform-set t3

crypto map test isakmp authorization list groupauthor
crypto map test client configuration address respond
crypto map test 100 IPSec-isakmp dynamic test

interface FastEthernet0/0
 ip address 172.17.0.1 255.255.255.252
 crypto map test
```

© 2008 Cisco Systems, Inc. All rights reserved.

Common Issues:
DMVPN Hub and Ezvpn server in same Router

```
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0

crypto ipsec transform-set t2 esp-3des esp-md5-hmac
  mode transport

crypto ipsec profile vpnprof
  set transform-set t2

interface Tunnel0
  ip address 10.0.0.8 255.255.255.0
  tunnel protection ipsec profile vpnprofi
```

© 2008 Cisco Systems, Inc. All rights reserved.

Common Issues:
DMVPN Hub and Ezvpn server in same Router

How to Fix ?

- By default Spoke tunnel terminate on Ezvpn group if you have both Ezvpn server and DMVPN configured in same router which looks for **CONF_XAUTH**.
- Separate Ezvpn server and DMVPN configuration by using Isakmp Profile.
- Match Ezvpn software/hardware clients in Group name and DMVPN spokes in match identity address in Isakmp profile.

```
crypto keyring dmvpn
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
crypto isakmp profile dmvpn
      keyring dmvpn
       match identity address 0.0.0.0
crypto ipsec profile vpnprof
     set transform-set t2
     set isakmp-profile dmvpn
```

© 2008 Cisco Systems, Inc. All rights reserved.

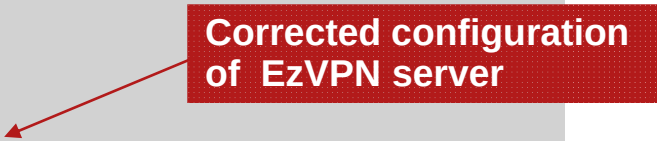
Common Issues:
DMVPN Hub and Ezvpn server in same Router

```
crypto isakmp client configuration group vpnclient
  key cisco123
  pool vpn
  acl 190

crypto isakmp profile remotevpn
  match identity group vpnclient

crypto dynamic-map test 10
  set transform-set t3
  set isakmp-profile remotevpn

crypto map test isakmp authorization list groupauthor
crypto map test client configuration address respond
crypto map test 100 ipsec-isakmp dynamic test
```



© 2008 Cisco Systems, Inc. All rights reserved.

Common Issues:
DMVPN Hub and Ezvpn server in same Router

How to Verify ?

```
ISAKMP:(0):found peer pre-shared key matching 172.18.1.1
ISAKMP:(0): local preshared key found
ISAKMP:(0):Checking ISAKMP transform 1 against priority 2 policy
ISAKMP:(0):atts are acceptable. Next payload is 0
ISAKMP:(0):Old State = IKE_R_MM1  New State = IKE_R_MM1
ISAKMP:(0):Old State = IKE_R_MM1  New State = IKE_R_MM2
ISAKMP:(0):Old State = IKE_R_MM2  New State = IKE_R_MM3
ISAKMP:(4157):Old State = IKE_R_MM3  New State = IKE_R_MM4
ISAKMP:(4157):Old State = IKE_R_MM4  New State = IKE_R_MM5
ISAKMP:(4157): processing ID payload. message ID = 0
ISAKMP (0:4157): ID payload
        next-payload : 8
        type         : 1
        address      : 10.1.1.1
        protocol     : 17
        port         : 0
        length       : 12
ISAKMP:(4157):Found ADDRESS key in keyring dmvpn
ISAKMP:(4157):Old State = IKE_R_MM5  New State = IKE_R_MM5
```

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Common Issues:
DMVPN Hub and Ezvpn server in same Router

```
ISAKMP:(4157):Old State = IKE_R_MM5  New State = IKE_P1_COMPLETE
ISAKMP:(4157):SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP (0:4157): ID payload
        next-payload : 8
        type         : 1
        address      : 172.17.0.1
        protocol     : 17
        port         : 0
        length       : 12
ISAKMP:(4157):Old State = IKE_R_MM5  New State = IKE_P1_COMPLETE
ISAKMP:(4157):Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP:(4157):atts are acceptable.
ISAKMP:(4157): Creating IPSec SA
        inbound SA from 172.18.1.1 to 172.17.0.1 (f/i)  0/ 0
        (proxy 172.18.1.1 to 172.17.0.1)
        has spi 0x936AA23D and conn_id 0
       outbound SA from 172.17.0.1 to 172.18.1.1 (f/i) 0/0
        (proxy 172.17.0.1 to 172.18.1.1)
        has spi  0xD37F43CB and conn_id 0
ISAKMP:(4157):Old State = IKE_QM_R_QM2  New State = IKE_QM_PHASE2_COMPLETE
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.0.0.11 (Tunnel0) is up: new adjacency
```

VPN Tunnel established

© 2008 Cisco Systems, Inc. All rights reserved.

Common Issues:
DMVPN Hub and Ezvpn server in same Router

EzVPN profile

```
show crypto  isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id  slot  status
172.17.0.1      172.19.87.148   QM_IDLE           4158    0   ACTIVE remotevpn
172.17.0.1      172.16.1.1      QM_IDLE           4152    0   ACTIVE dmvpn
172.17.0.1      172.18.1.1      QM_IDLE           4157    0   ACTIVE dmvpn
172.17.0.6      172.17.0.1      QM_IDLE           4156    0   ACTIVE dmvpn
```

DMVPN Profile

```
show crypto  ipsec sa peer 172.18.1.1
  local  ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (172.18.1.1/255.255.255.255/47/0)
  current_peer 172.18.1.1 port 1024
  #pkts encaps: 18, #pkts encrypt: 18, #pkts digest: 18
   #pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
 current outbound spi: 0xD37F43CB(3548333003)
 inbound esp sas:
spi: 0x936AA23D(2473239101)
outbound esp sas:
 spi: 0xD37F43CB(3548333003)
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Common Issues: Incompatible IPsec Transform Set

- If the ipsec transform-set is not compatible or mismatched on the two IPsec devices, the IPsec negotiation will fail, with the router complaining about "**atts not acceptable**" for the IPsec proposal

ISAKMP (0:2): Checking IPsec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 3600
ISAKMP: SA life type in kilobytes
ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 0) not supported
ISAKMP (0:2): atts not acceptable. Next payload is 0
ISAKMP (0:2): SA not acceptable!

Phase II Parameters

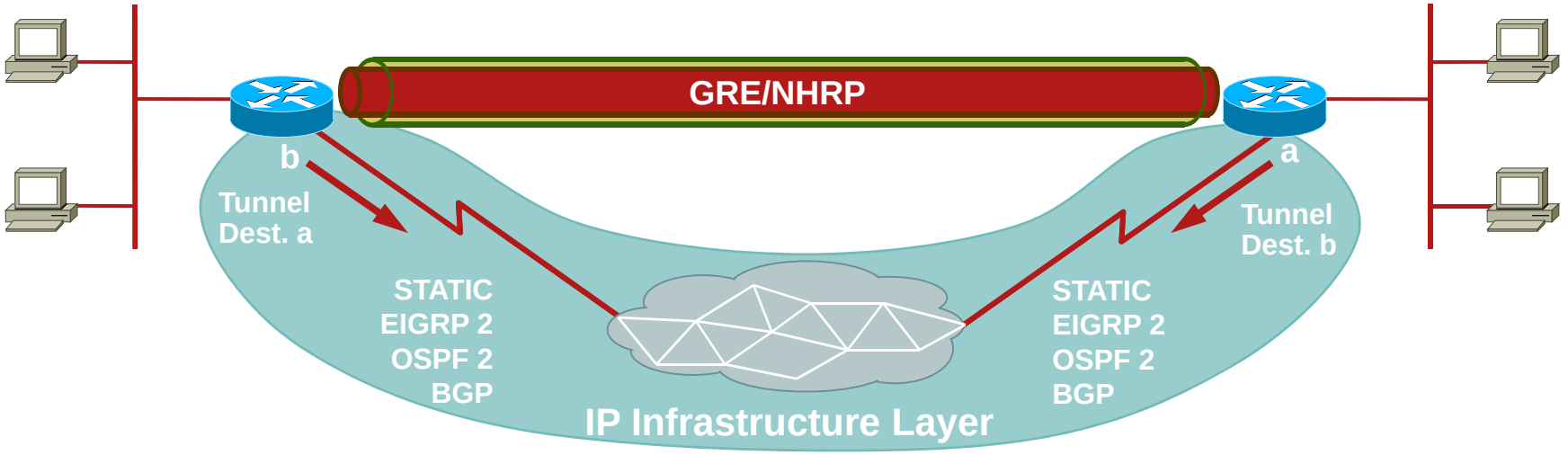
```
IPsec mode (tunnel or transport)
Encryption algorithm
Authentication algorithm
PFS group
IPsec SA Lifetime
Proxy identities
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: GRE Encapsulation Layer

- The GRE Encapsulation layer—NHRP

  This is GRE encapsulating the data IP packet going out and GRE decapsulating the GRE packet (after IPsec encryption) coming in to get the data IP packet



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: GRE Encapsulation Layer

DMVPN Component-GRE/NHRP

- Multipoint GRE Tunnel Interface
  - Single GRE interface to support multiple GRE/IPsec tunnels
  - Simplifies size and complexity of configuration
- Next Hop Resolution Protocol (NHRP)
  - Creates a distributed (NHRP) mapping database of all the spoke's tunnel to real (public interface) addresses

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: GRE Encapsulation Layer

DMVPN Component-mGRE

- A p-pGRE interface definition includes
  - An IP address
  - A tunnel source
  - A tunnel destination
  - An optional tunnel key

```
interface Tunnel
   ip address 10.0.0.1 255.0.0.0
   tunnel source Dialer1
   tunnel destination 172.16.0.2
   tunnel key 1
```

- An mGRE interface definition includes
  - An IP address
  - A tunnel source
  - An option tunnel key

```
interface Tunnel
   ip address 10.0.0.1 255.0.0.0
   tunnel source Dialer1
   tunnel mode gre multipoint
   tunnel key 1
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: GRE Encapsulation Layer

DMVPN Component-mGRE (Cont.)

- Single tunnel interface (multipoint)
  - Non-Broadcast Multi-Access (NBMA) Network
  - Smaller hub configuration
  - Multicast/broadcast support
- 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

© 2008 Cisco Systems, Inc. All rights reserved.

Four Layers for Troubleshooting: GRE Encapsulation Layer—What Is NHRP

DMVPN Component-NHRP

- NHRP is a layer two resolution protocol and cache like ARP or Reverse ARP (Frame Relay)
- It is used in DMVPN to map a tunnel IP address to an NBMA address
- Like ARP, NHRP can have static and dynamic entries
- NHRP has worked fully dynamically since Release 12.2(13)T

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting:GRE Encapsulation Layer—Basic NHRP Configuration

DMVPN Component-NHRP (Cont.)

- In order to configure an mGRE interface to use NHRP, the following command is necessary:

  ip nhrp network-id <id>

- Where <id> is a unique number (recommend same on hub and all spokes)
- <id> has nothing to do with tunnel key
- The network ID defines an NHRP domain
- Several domains can co-exist on the same router
- Without having this command, tunnel interface won't come UP

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: GRE Encapsulation Layer—Adding NHRP Cache

DMVPN Component-NHRP (Cont.)

- Three ways to populate the NHRP cache:
  - Manually add static entries
  - Hub learns via registration requests
  - Spokes learn via resolution requests
- "Resolution" is for spoke to spoke

© 2008 Cisco Systems, Inc. All rights reserved.

Four Layers for Troubleshooting: GRE Encapsulation Layer—Initial NHRP Caches

DMVPN Component-NHRP (Cont.)

- Initially, the hub has an empty cache
- The spoke has one static entry mapping the hub's tunnel address to the hub's NBMA address:

  ip nhrp map 10.0.0.1 172.17.0.1

- Multicast traffic must be sent to the hub

  ip nhrp map multicast 172.17.0.1

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: GRE Encapsulation Layer—Spoke Must Register with Hub

DMVPN Component-NHRP (Cont.)

- In order for the spokes to register themselves to the hub, the hub must be declared as a Next Hop Server (NHS):

```
ip nhrp nhs 10.0.0.1
ip nhrp holdtime 300 (recommended; default =7200)
ip nhrp registration no-unique (recommended*)
```

- Spokes control the cache on the hub

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

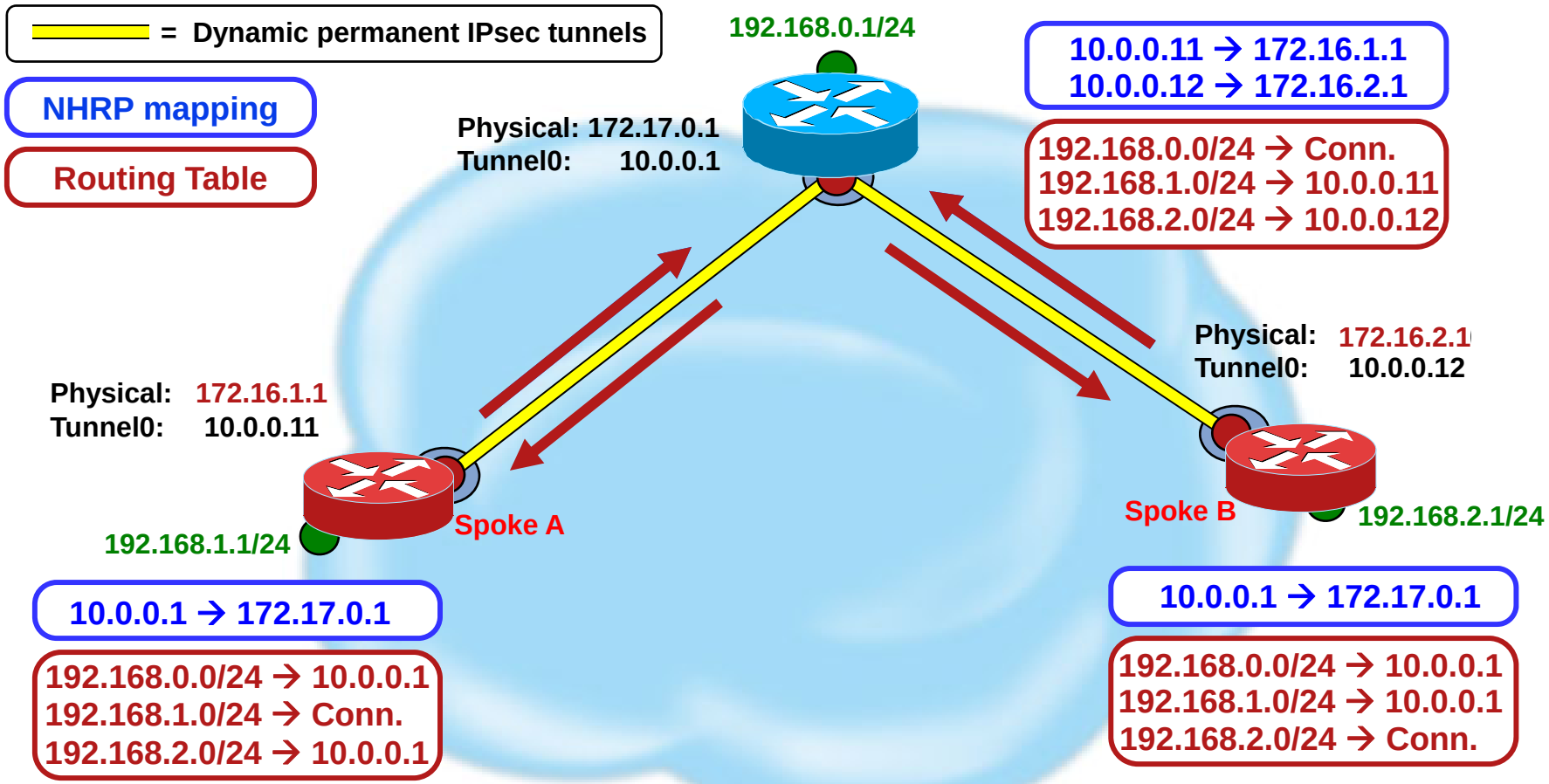
Four Layers for Troubleshooting: GRE Encapsulation Layer—NHRP Registration

DMVPN Component-NHRP (Cont.)

- NHRP Registration
  - Spoke dynamically registers its mapping with NHS
  - Supports spokes with dynamic NBMA addresses or NAT
- NHRP Resolutions and Redirects
  - Supports building dynamic spoke-spoke tunnels
  - Control and Multicast traffic still via hub
  - Unicast data traffic direct, reduced load on hub routers

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

NHRP Registration Example
Dynamically Addressed Spokes



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

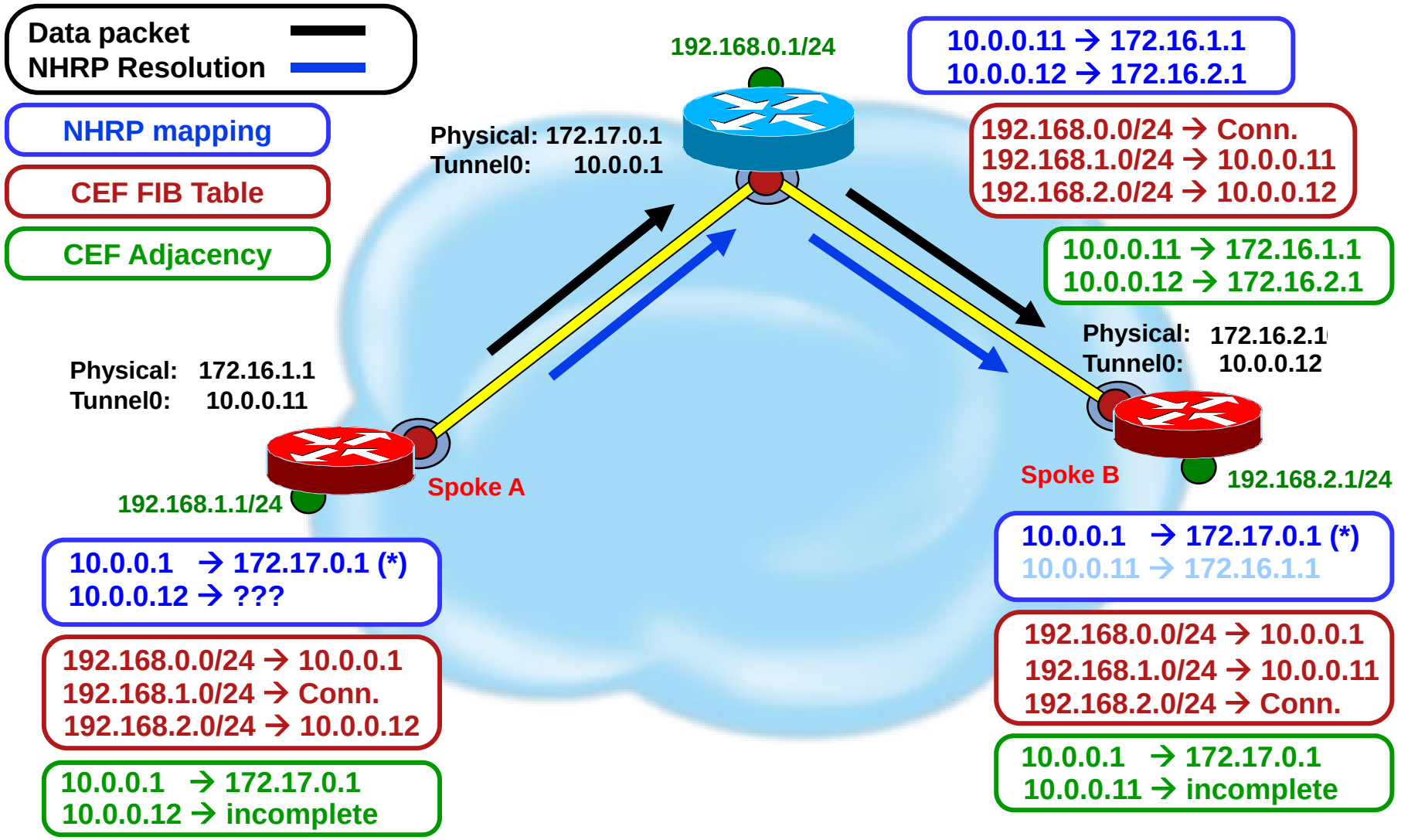
Four Layers for Troubleshooting: GRE Encapsulation Layer—NHRP Registration (Cont.)

DMVPN Component-NHRP (Cont.)

- Builds base hub-and-spoke network
  - Hub-and-spoke data traffic
  - Control traffic; NHRP, Routing protocol, IP multicast
- Next Hop Client (NHC) has static mapping for Next Hop Servers (NHSs)
- Registration time is configurable
  - ip nhrp registration timer <value> (default = 1/3 nhrp hold time)
- NHS registration reply gives liveliness of NHS
  - Important for Phase 2 networks

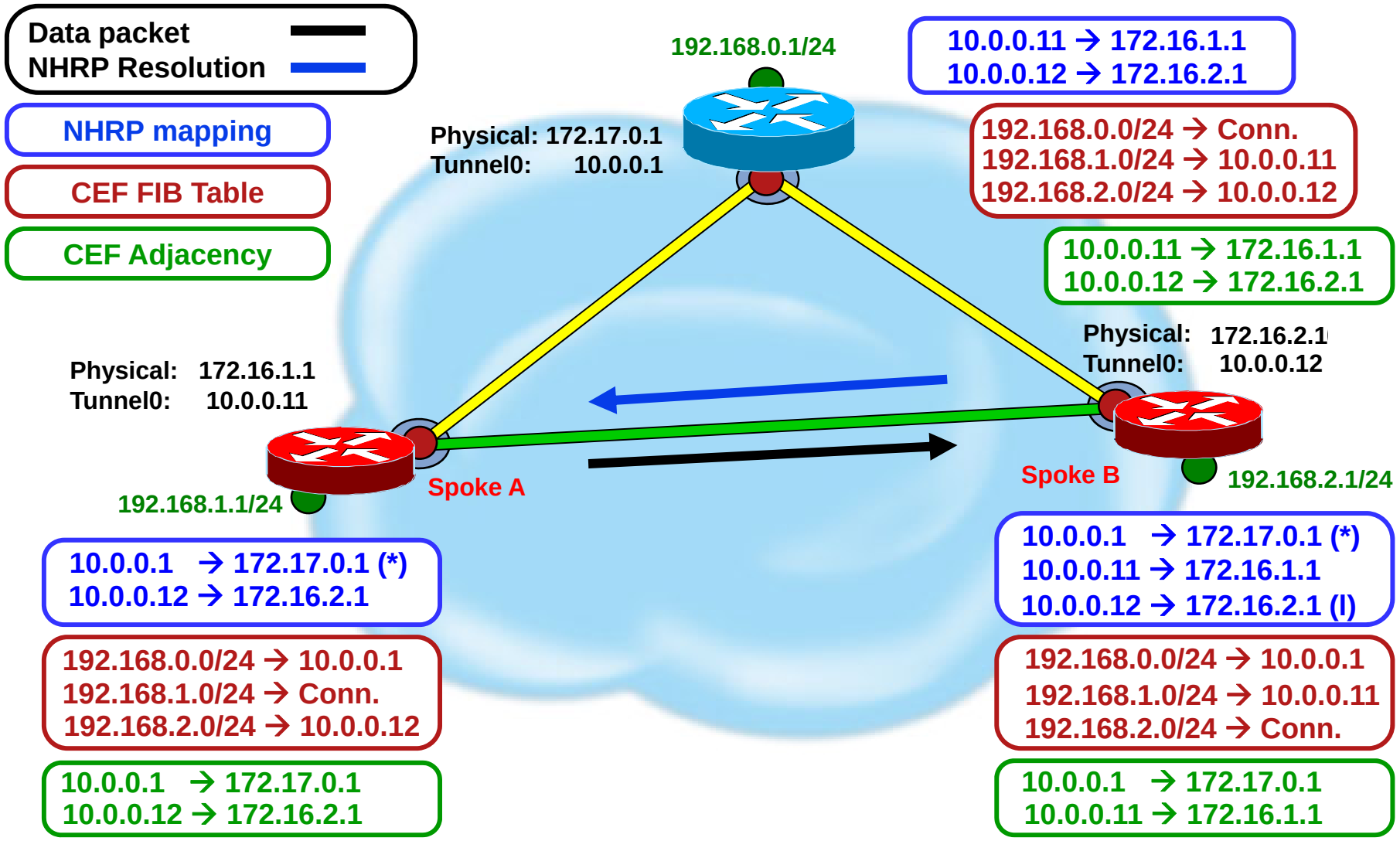
© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Dynamic Mesh: Phase 2
NHRP Resolutions



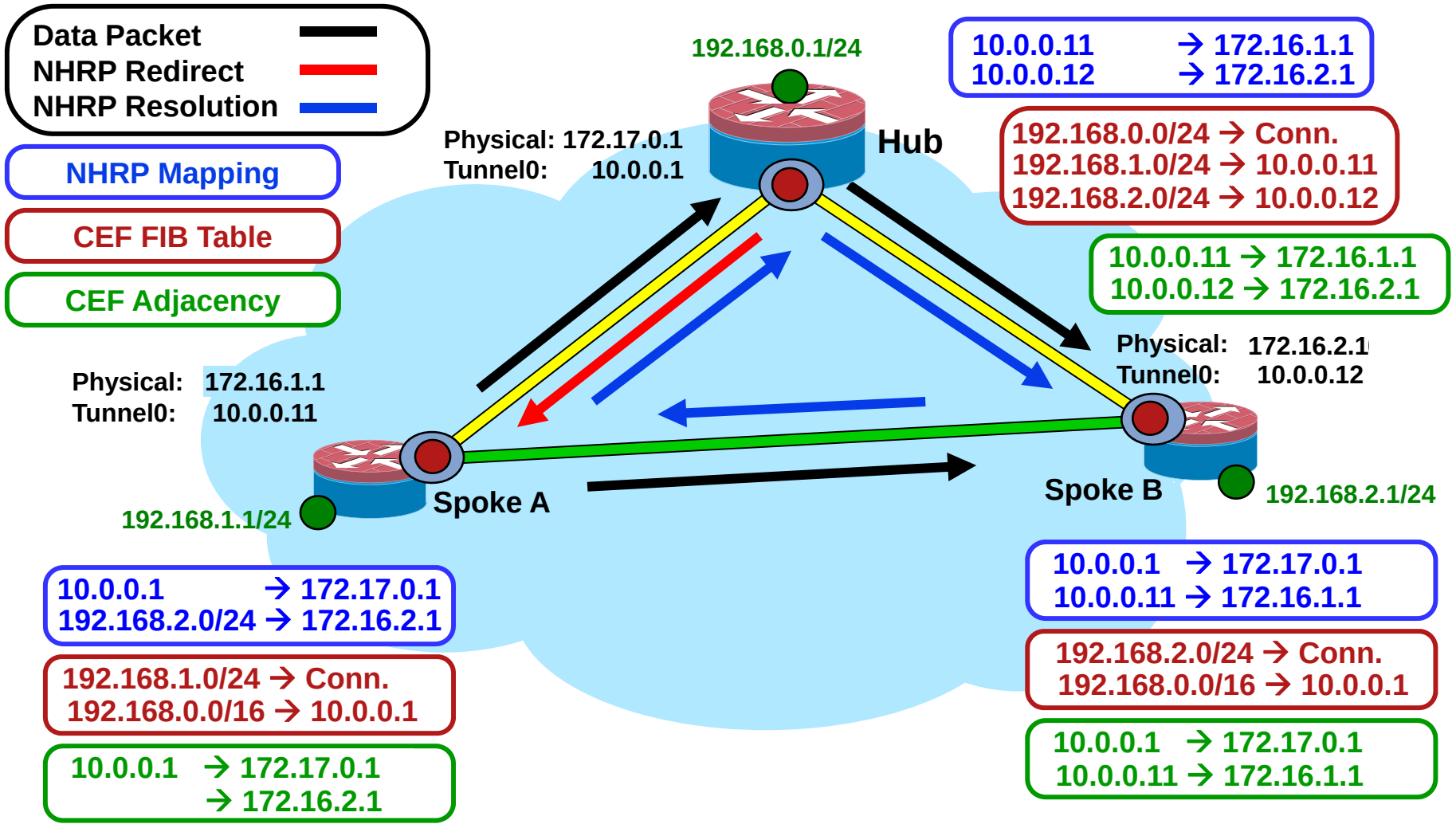
© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Dynamic Mesh: Phase 2
NHRP Resolutions (cont)



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

NHRP Resolutions and Redirects (Phase 3)



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: GRE Encapsulation Layer

- Look at NHRP. The spoke should be sending an NHRP registration packet on a regular basis, every 1/3 NHRP hold time (on spoke) or 'ip nhrp registration timeout <seconds>' value.

  On the Spoke: **show ip nhrp nhs detail**

  On the hub: **show ip nhrp <spoke-tunnel-ip-address>**

- Check the 'created' and 'expire' timer :

  'created' timer: how long this NHRP mapping entry has continuously been in the NHRP mapping table.

  'expire' timer: how long before this NHRP mapping entry would be deleted, if the hub were not to receive another NHRP registration from the spoke.

  If the 'created' timer is low and gets reset a lot then that means that the NHRP mapping entry is getting reset

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: GRE Encapsulation Layer

- Verify pings from the hub to the spoke's tunnel ip address and the reverse.
- Use the following debugs on the hub router.

  debug nhrp condition peer <nbma|tunnel>

  debug nhrp

  debug tunnel protection

  debug crypto socket

  (these last two show communication between NHRP and IPsec)

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: GRE Encapsulation Layer—Show Commands

show ip nhrp detail

```
10.0.0.5/32 via 10.0.0.5, Tunnel0 created 03:36:47, never expire
 Type: static, Flags: used
 NBMA address: 172.17.0.5
10.0.0.9/32 via 10.0.0.9, Tunnel0 created 03:26:26, expire 00:04:04
  Type: dynamic, Flags: unique nat registered
  NBMA address: 110.110.110.2
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 01:55:43, expire 00:04:15
  Type: dynamic, Flags: unique nat registered
  NBMA address: 120.120.120.2
```

show ip nhrp nhs detail

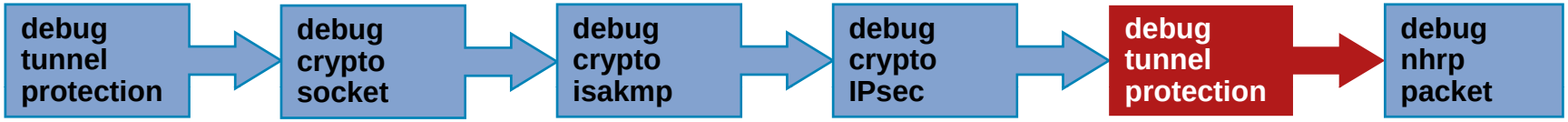
```
Legend: E=Expecting replies, R=Responding

Tunnel0: 10.0.0.1 RE  req-sent 654 req-failed 0 repl-recv 590 (00:00:09 ago)
         10.0.0.5 RE  req-sent 632 req-failed 0 repl-recv 604 (00:00:09 ago)
```

NHRP Flag Information:
http://www.cisco.com/en/US/docs/ios/12_4/ip_addr/configuration/guide/hadnhrp_ps6350_TSD_Products_Configuration_Guide_Chapter.html#wp1067931

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting:GRE Encapsulation Layer—debug dmvpn detail all



- Tunnel protection start again after Phase 2 came UP
- Connection lookup id should be same used when tunnel start
- Syslog message shows socket came UP
- Signal NHRP after socket UP

ID value has to be same when socket open in the beginning

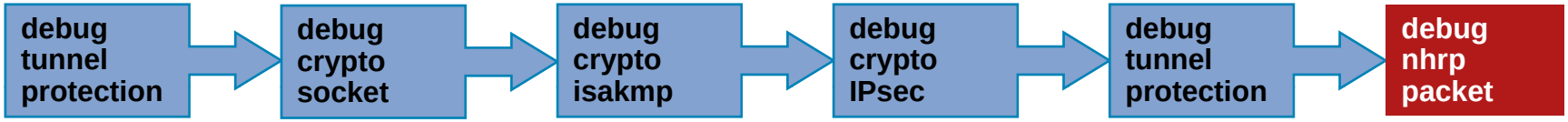
```
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): connection lookup returned 83884274
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.5): tunnel_protection_socket_up
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.5): Signalling NHRP
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.5): connection lookup returned 83DD7B30
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): connection lookup returned 83884274
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): tunnel_protection_socket_up
IPSEC-IFC MGRE/Tu0(172.16.2.11/172.17.0.1): Signalling NHRP
```

Syslog message:

%DMVPN-7-CRYPTO_SS: Tunnel0-172.16.2.11 socket is UP

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: GRE Encapsulation Layer-debug dmvpn detail all (Cont.)



- Spoke send NHRP registration request.
- Req id has to be same in both registration request and response.

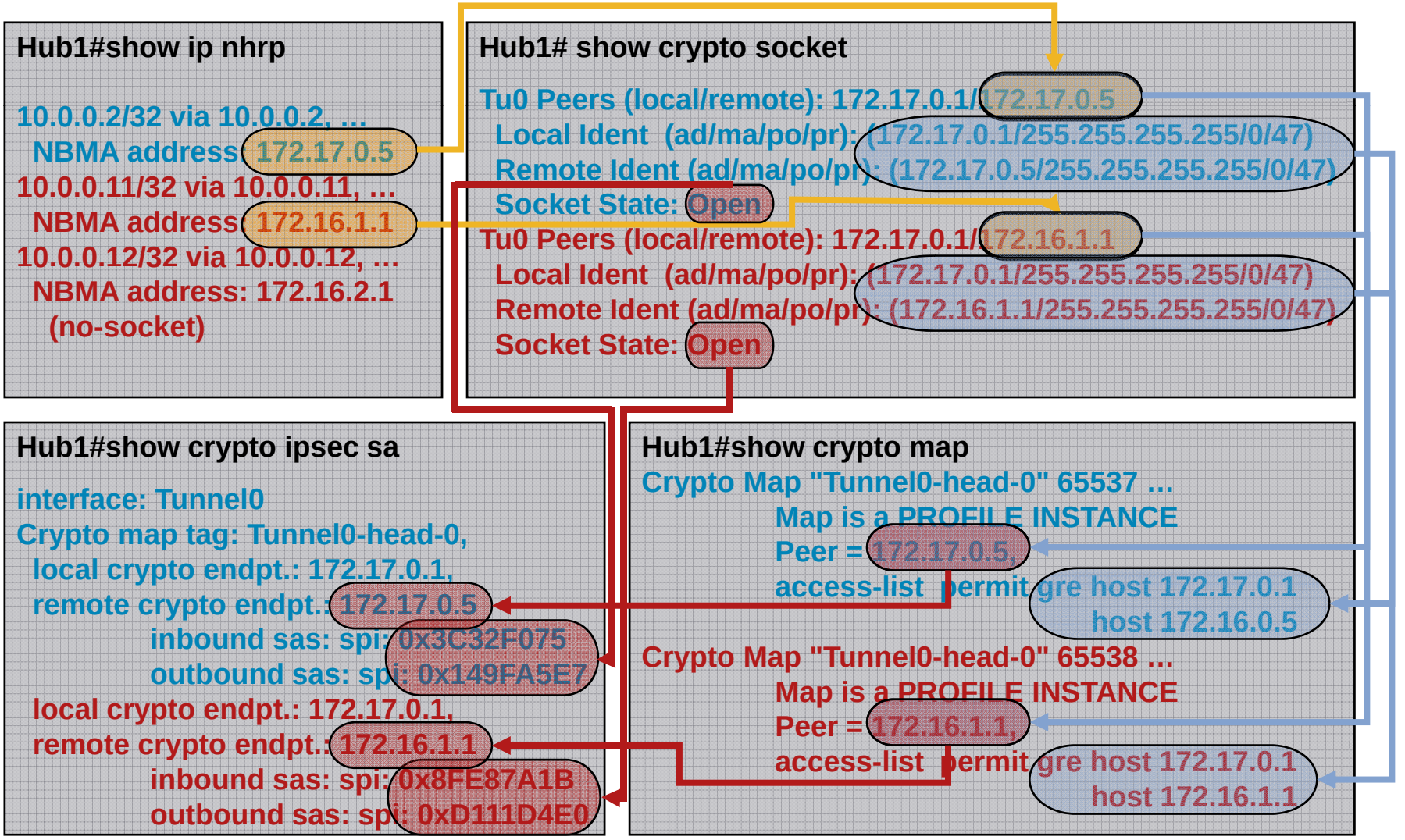
NHRP: Send Registration Request via Tunnel0
vrf 0, packet size: 104
src: 10.0.0.9, dst: 10.0.0.1
(F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
shtl: 4(NSAP), sstl: 0(NSAP)
(M) flags: "unique nat ", reqid: **1279**
src NBMA: 172.16.1.1
src protocol: 10.0.0.9, dst protocol: 10.0.0.1
(C-1) code: no error(0)
prefix: 255, mtu: 1514, hd_time: 300
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0

NHRP: Receive Registration Reply via Tunnel0
vrf 0, packet size: 124
(F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
shtl: 4(NSAP), sstl: 0(NSAP)
(M) flags: "unique nat ", reqid: **1279**
src NBMA: 172.16.1.1.
src protocol: 10.0.0.9, dst protocol: 10.0.0.1
(C-1) code: no error(0)
prefix: 255, mtu: 1514, hd_time: 300
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0

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

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

DMVPN Data Structures Interaction



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: GRE Encapsulation Layer

Common Issues

- NHRP Registration fails
- Dynamic NBMA address change in spoke resulting inconsistent NHRP mapping in hub

© 2008 Cisco Systems, Inc. All rights reserved.

Common Issues: NHRP Registration Fails

How to Detect?

- VPN tunnel between hub and spoke is up but unable to pass data traffic.

Show crypto isa sa

dst	src	state	conn-id	slot	status
172.17.0.1	172.16.1.1	QM_IDLE	1082	0	ACTIVE

Show crypto IPsec sa

local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
#pkts encaps: 154, #pkts encrypt: 154, #pkts digest: 154
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
inbound esp sas:
spi: 0xF830FC95(4163959957)
outbound esp sas:
spi: 0xD65A7865(3596253285)

Return traffic not coming back from other end of tunnel

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Common Issues: NHRP Registration Fails (Cont.)

- Check NHS entry in spoke router.

```
Show  ip nhrp nhs detail
Legend: E=Expecting replies, R=Responding
Tunnel0:      172.17.0.1  E  req-sent 0  req-failed 30  repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 4371, Ret 64  NHS 172.17.0.1
```

NHS Request fail

How to Fix?

- Check spoke router tunnel interface configuration to make sure correct ip address of NHS server is configured

Wrong NHS server address

```
interface Tunnel0
 ip address 10.0.0.9 255.255.255.0
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1
 ip nhrp nhs 172.17.0.1
```

```
interface Tunnel0
 ip address 10.0.0.9 255.255.255.0
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1
 ip nhrp nhs 10.0.0.1
```

Correct NHS configuration is IP address of Hub tunnel interface

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Common Issues: NHRP Registration Fails (Cont.)

How to verify?

- Verify NHS entry and ipsec encrypt/decrypt counters

sh ip nhrp nhs detail

```
Legend: E=Expecting replies, R=Responding
Tunnel0:       10.0.0.1 RE  req-sent 4  req-failed 0  repl-recv 3 (00:01:04 ago)
```

No request fail

Show crypto ipsec sa

```
local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
#pkts encaps: 121, #pkts encrypt: 121, #pkts digest: 121
#pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118
inbound esp sas:
  spi: 0x1B7670FC(460747004)
outbound esp sas:
  spi: 0x3B31AA86(993110662)
```

- Verify routing protocol neighbor

sh ip eigrp neighbors

```
IP-EIGRP neighbors for process 10
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q   Seq
                                            (sec)         (ms)       Cnt Num
1   10.0.0.1                Tu0               11 00:21:20   18   200  0   497
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

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

- **Problem Description:**

  "Dynamic NBMA address change in spoke resulting inconsistent NHRP mapping in hub until NHRP registration with previous NBMA address expired"

- Show commands in hub before NBMA address change

```
Hub# show ip nhrp
10.0.0.11/32 via 10.0.0.11,Tunnel0 created 16:18:11,expire 00:28:47
Type: dynamic, Flags: unique nat registered,
NBMA address: 172.16.2.2
```

```
Hub # Show crypto socket
Tu0 Peers (local/remote): 172.17.0.1/172.16.2.2
      Local Ident  (addr/mask/port/prot): (172.17.0.1/255.255.255.255/0/47)
      Remote Ident (addr/mask/port/prot): (172.16.2.2/255.255.255.255/0/47)
      IPsec Profile: "dmvpn"
      Socket State: Open)
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

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

```
Hub# Show crypto ipsec sa
interface: Tunnel0
Crypto map tag: Tunnel0-head-0,
local crypto endpoint:172.17.0.1
Remote crypto endpoint:172.16.2.2
#pkts encaps: 13329,
#pkts decaps: 13326,
inbound esp sas:
  spi: 0xFEAB438C(4272636812)
outbound esp sas:
  spi: 0xDD07C33A(3708273466)
```

```
Hub# Show crypto map
Crypto Map "Tunnel0-head-0" 65540
Map is a PROFILE INSTANCE.
Peer = 172.16.2.2
      Extended IP access list
      access-list  permit gre host 172.17.0.1  host 172.16.2.2
      Current peer: 172.16.2.2
```

How to Detect?

- Inconsistency after NBMA address change in spoke

```
Hub# show ip nhrp
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 17:37:25, expire 00:09:34
Type: dynamic, Flags: unique nat registered used
NBMA address: 172.16.2.2
```

NHRP shows no entry for 172.16.2.3 still holding entry for previous NBMA address 172.16.2.2

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

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

How to Detect? (Cont.)

```
Hub# show crypto map
Crypto Map "Tunnel0-head-0" 65540 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 172.16.2.2
        Extended IP access list
        access-list  permit gre host 172.17.0.1 host 172.16.2.2
        Current peer: 172.16.2.2
Crypto Map "Tunnel0-head-0" 65541 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 172.16.2.3
        Extended IP access list
        access-list  permit gre host 172.17.0.1  host 172.16.2.3
        Current peer: 172.16.2.3
```

Crypto map entry for both previous and new NBMA address of spoke

```
Hub# Show crypto socket
Tu0 Peers (local/remote): 172.17.0.1/172.16.2.2
      Local Ident  (addr/mask/port/prot): (172.17.0.1/255.255.255.255/0/47)
      Remote Ident (addr/mask/port/prot): (172.16.2.2/255.255.255.255/0/47)
      IPsec Profile: "dmvpn"
      Socket State: Open
Tu0 Peers (local/remote): 172.17.0.1/172.16.2.3
      Local Ident  (addr/mask/port/prot): (172.17.0.1/255.255.255.255/0/47)
      Remote Ident (addr/mask/port/prot): (172.16.2.3/255.255.255.255/0/47)
      IPsec Profile: "dmvpn"
      Socket State: Open
```

Old NBMA address

New NBMA address

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

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

How to Detect? (Cont.)

- debug nhrp packet in hub router to check NHRP registration request /reply.

```
Hub# debug nhrp packet
NHRP: Receive Registration Request via Tunnel0 vrf 0, packet size: 104
  (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
    shtl: 4(NSAP), sstl: 0(NSAP)
  (M) flags: "unique nat ", reqid: 9480
    src NBMA: 172.16.2.3
    src protocol: 10.0.0.11, dst protocol: 10.0.0.1
  (C-1) code: no error(0)
    prefix: 255, mtu: 1514, hd_time: 600
NHRP: Attempting to send packet via DEST 10.0.0.11
NHRP: Encapsulation succeeded.  Tunnel IP addr 172.16.2.3
NHRP: Send Registration Reply via Tunnel0 vrf 0, packet size: 124,  src: 10.0.0.1, dst: 10.0.0.11
  (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
    shtl: 4(NSAP), sstl: 0(NSAP)
  (M) flags: " unique nat ", reqid: 9480
    src NBMA: 172.16.2.3
    src protocol: 10.0.0.11, dst protocol: 10.0.0.1
  (C-1) code: unique address registered already(14)
    prefix: 255, mtu: 1514, hd_time: 600
```

C-1 code shows NBMA address is already registered , that is why it is not updating nhrp mapping table with new NBMA address

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

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

- Spoke router shows the error message indicating about NBMA address already registered

```
%NHRP-3-PAKREPLY: Receive Registration Reply packet with error - unique address registered already(14)
```

How to Fix?

- "ip nhrp registration no-unique" command in tunnel interface of dynamic
- NBMA address spoke router

```
Spoke# show run interface tunnel0
interface Tunnel0
 ip address 10.0.0.11 255.255.255.0
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.0.1
 ip nhrp registration no-unique
 :
tunnel protection ipsec profile dmvpn
```

To enable the client to not set the unique flag in the Next Hop Resolution Protocol (NHRP) request and reply packets

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

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

How to Verify?

```
Hub# debug nhrp packet
NHRP: Receive Registration Request via Tunnel0 vrf 0, packet size: 104
  (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
    shtl: 4(NSAP), sstl: 0(NSAP)
  (M) flags: "nat ", reqid: 9462
    src NBMA: 172.16.2.4
    src protocol: 10.0.0.11, dst protocol: 10.0.0.1
  (C-1) code: no error(0)
    prefix: 255, mtu: 1514, hd_time: 600
NHRP: Tu0: Creating dynamic multicast mapping  NBMA: 172.16.2.4
NHRP: Attempting to send packet via DEST 10.0.0.11
NHRP: Encapsulation succeeded.  Tunnel IP addr 172.16.2.4
NHRP: Send Registration Reply via Tunnel0 vrf 0, packet size: 124
    src: 10.0.0.1, dst: 10.0.0.11
  (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
    shtl: 4(NSAP), sstl: 0(NSAP)
  (M) flags: "nat ", reqid: 9462
    src NBMA: 172.16.2.4
    src protocol: 10.0.0.11, dst protocol: 10.0.0.1
  (C-1) code: no error(0)
    prefix: 255, mtu: 1514, hd_time: 600
```

Unique address command result no unique flag
C-1 code shows no error

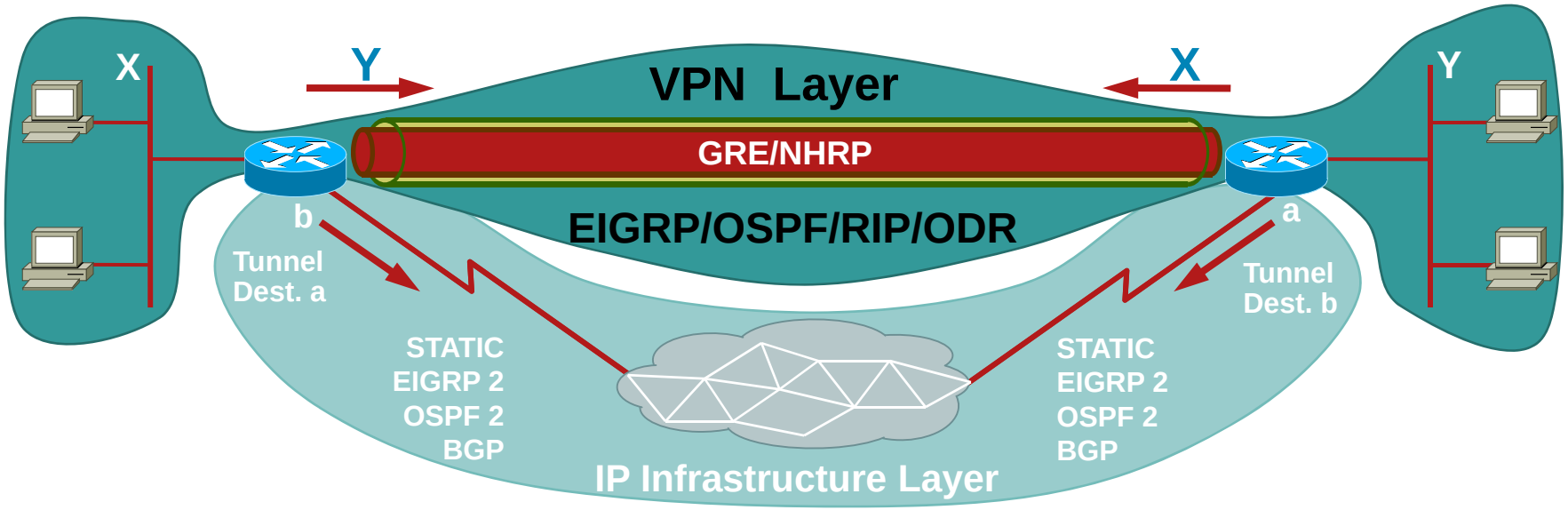
```
Hub#sh ip nhrp
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 01:04:32, expire 00:07:06
  Type: dynamic, Flags: nat registered
  NBMA address: 172.16.2.4
```

Unique flag not set

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: VPN Routing Layer

- The VPN routing layer—this is routing packets in/out of the p-pGRE and/or mGRE interfaces on the tunnel endpoint routers. This is done by running a dynamic routing protocol over the DMVPN tunnels



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: VPN Routing Layer

- DMVPN Component-routing
- Regular IP networks

  IP routing updates and data packets traverse same physical/logical links

  Routing Protocol monitors state of all links that data packets can use

- DMVPN IP networks

  IP routing updates and IP multicast data packets only traverse hub-and-spoke tunnels

  Unicast IP data packets traverse both hub-and-spoke and direct dynamic spoke-spoke tunnels

  Routing protocol doesn't monitor state of spoke-spoke tunnels

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: VPN Routing Layer

- Check for routing neighbor and lifetime
  - show ip route [eigrp | ospf | rip]
  - show ip protocol
  - show ip [eigrp | ospf] neighbor
- Check multicast replication and connectivity
  - show ip nhrp multicast
  - ping [224.0.0.10 (eigrp) | 224.0.0.5 (ospf) | 224.0.0.9 (rip)]
  - ping <tunnel-subnet-broadcast-address>
    - Example: 10.0.0.0/24 → 10.0.0.255
- Debug
  - Various debug commands depending on routing protocol

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: VPN Routing Layer—Common Issues

Common Issues:

- Routing protocol neighbor not established

© 2008 Cisco Systems, Inc. All rights reserved.

Four Layers for Troubleshooting: VPN Routing Layer—Common Issues

Problem

- Spokes unable to establish routing protocol neighbor relationship
- **How to detect?**

```
Hub# show ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address         Interface   Hold   Uptime     SRTT   RTO    Q     Seq
                                (sec)             (ms)        Cnt   Num
2   10.0.0.9        Tu0         13     00:00:37   1      5000   1     0
0   10.0.0.5        Tu0         11     00:00:47   1587   5000   0     1483
1   10.0.0.11       Tu0         13     00:00:56   1      5000   1     0
```

Syslog message

%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10: Neighbor 10.0.0.9 (Tunnel0) is down: retry limit exceeded

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: VPN Routing Layer—Common Issues (Cont.)

```
Hub# show ip route eigrp
                172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, FastEthernet0/0
    10.0.0.0/24 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 172.17.0.100
```

- **How to fix?**

  Verify NHRP multicast mapping is configured, in hub it is require to have dynamic nhrp multicast mapping configured in hub tunnel interface

```
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 no ip next-hop-self eigrp 10
 ip nhrp authentication test
 ip nhrp network-id 10
 no ip split-horizon eigrp 10
 tunnel mode gre multipoint
```

```
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 no ip next-hop-self eigrp 10
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 10
 no ip split-horizon eigrp 10
 tunnel mode gre multipoint
```

Allows NHRP to automatically add spoke routers to the multicast NHRP mappings

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Four Layers for Troubleshooting: VPN Routing Layer—Common Issues (Cont.)

- **How to verify?**

```
Hub # sh ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address                 Interface       Hold Uptime   SRTT      RTO    Q    Seq
                                            (sec)         (ms)             Cnt  Num
2   10.0.0.9                Tu0               12  00:16:48   13     200    0    334
1   10.0.0.11               Tu0               13  00:17:10   11     200    0    258
0   10.0.0.5                Tu0               12  00:48:44 1017    5000   0    1495

Hub# show ip route

     172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, FastEthernet0/0
D    192.168.11.0/24 [90/2944000] via 10.0.0.11, 00:16:12, Tunnel0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, FastEthernet0/1
D    192.168.2.0/24 [90/2818560] via 10.0.0.9, 00:15:45, Tunnel0
S*   0.0.0.0/0 [1/0] via 172.17.0.100
```

Spokes routes learned via EIGRP protocol

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Case Study


[communication]
[leadership]
[invention]
[inspiration]
[knowledge]
[collaboration]

Case Study

- Customer wants to disable split tunneling in spoke and also wants to build spoke to spoke DMVPN tunnel.

© 2008 Cisco Systems, Inc. All rights reserved.

Problem Description

Customer has corporate security policies that disable split-tunneling and advertise default route over the tunnel to all spokes.

He wants to build spoke to spoke tunnel and at the same time wants all internet traffic will go through DMVPN hub located in main corporate office.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Solution: Default Route From ISP And Over the Tunnel

- In Spoke to Spoke model, we need an ISP default route to reach other spoke.
- Default route over the Tunnel should not overwrite the ISP default route for spoke to spoke communication to work
- **Solution:** Use Virtual Routing and Forwarding (VRF) instance to handle both default routes

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

VRF and DMVPN

- Typically VRFs are deployed in one of the following two configurations:

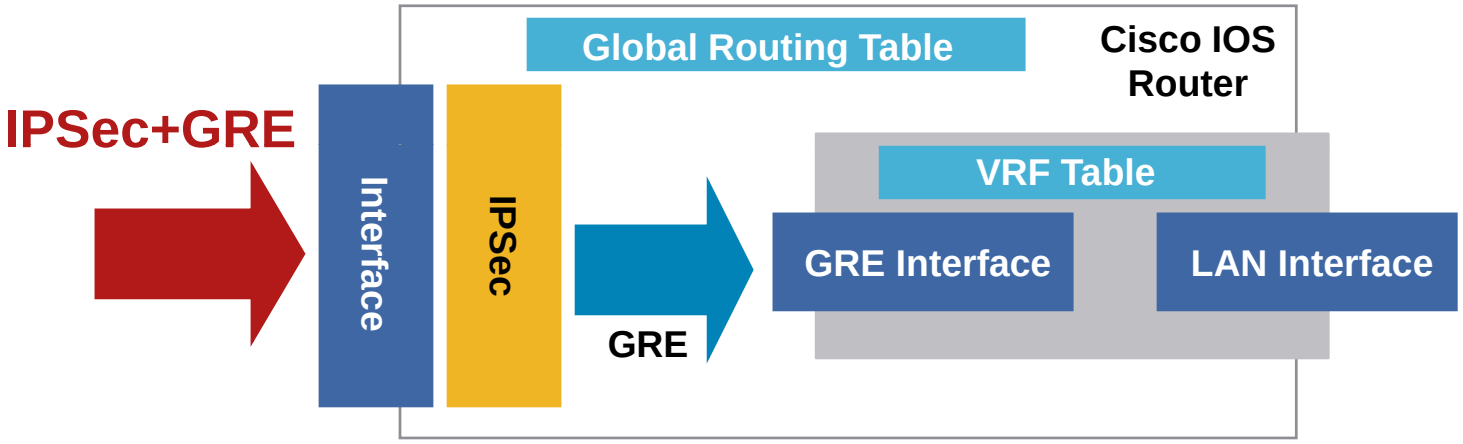
  I-VRF: GRE tunnel and LAN interface are configured in a VRF and public interface (carrying GRE traffic) is in global table

  FVRF: GRE tunnel and LAN interface stay in the global routing table but public interface (carrying GRE traffic) is configured in a VRF

- VRF configurations are a common way of handling dual-default routes

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

DMVPN and I-VRF

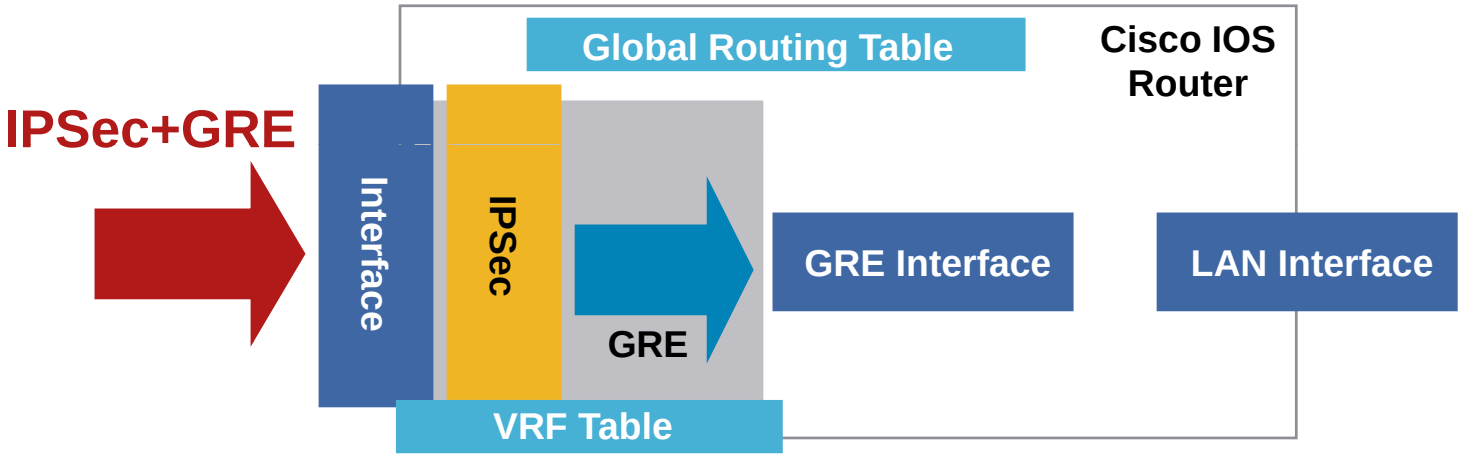


- IPSec packets are forwarded using global routing table
- GRE decapsulated clear-text packets are forwarded using associated VRF

```
Interface Tunnel1
 ip vrf forwarding VRF-1
 tunnel source Serial0/0
!
Interface Serial 0/0
 description in global table
!
Interface FastEthernet 0/0
 ip vrf forwarding VRF-1
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

DMVPN and F-VRF



- IPSec packets are forwarded using VRF routing table
- GRE decapsulated clear-text packets are forwarded using global table

```
Interface Tunnel1
 tunnel source Serial0/0
 tunnel VRF F-VRF
!
Interface Serial 0/0
 ip vrf forwarding F-VRF
!
Interface FastEthernet 0/0
 description In Global Table
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Dual Default Routes
Configuration Example

Since WAN interface in a VRF, pre-shared key needs to be defined in the VRF

Tunnel Destination lookup forced in VRF FVRF

WAN interface defined in the VRF – LAN interface stays in Global Table

```
ip vrf FVRF
 rd 100:1
!
crypto keyring DMVPN vrf FVRF
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
Interface Tunnel0
 ip address 172.50.1.1 255.255.255.0
 ip nhrp authentication HBfR3lpl
 ip nhrp map multicast 3.3.3.3
 ip nhrp map 172.50.1.254 3.3.3.3
 ip nhrp network-id 1
 ip nhrp holdtime 300
 ip nhrp nhs 172.50.1.254
 ip nhrp shortcut
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel vrf FVRF
 tunnel protection ipsec profile dmvpn
end
!
Interface GigabitEthernet 0/0
 description WAN interface to ISP in vrf
 ip address dhcp
 ip vrf forwarding FVRF

Interface GigabitEthernet 0/1
 description LAN interface In Global Table
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Dual Default Routes (Cont.)

Spoke-A VRF Routing Table

```
Spoke-A# show ip route vrf FVRF

Routing Table: FVRF

Gateway of last resort is 192.168.0.254 to network 0.0.0.0

     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.0/24 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 [254/0] via 192.168.0.254
```

Spoke-A Global Routing Table

```
Spoke-A# show ip route

C       172.50.1.0 is directly connected, Tunnel0
C       172.60.1.0 is directly connected, Tunnel1
C       10.0.0.0/24 is directly connected, GigabitEthernet0/1.84
D       0.0.0.0/0 [90/2844160] via 172.50.1.254, 00:03:45, Tunnel1
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

DMVPN Best Practice Configuration Examples

DMVPN Best Practice Configuration

- Use ‘mode transport’ on transform-set
  - NHRP needs for NAT support and saves 20 bytes
- MTU issues
  - ip mtu 1400
  - ip tcp adjust-mss 1360
  - crypto ipsec fragmentation after-encryption (global)
- NHRP
  - ip nhrp holdtime <seconds>(recommended values 300 - 600)
  - ip nhrp registration no-unique
- ISAKMP
  - Call Admission Control (CAC) (on spokes and hubs)
    - call admission limit *percent* (hubs)
    - crypto call admission limit {**ike** {**in-negotiation-sa** *number* | **sa** *number*}}
  - Keepalives on spokes (GRE tunnel keepalives are not supported)
    - crypto isakmp keepalive 15
  - Invalid-SPI recovery not useful

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Recommended Releases

- 6500/7600 with VPN-SPA

  Sup720 - 12.2(33)SRC3,12.2(18)SXF16 for 7600

  12.2(33)SXH4, 122(18)SXF16 for 6500

  (TCP adjust mss command included)

  Caveat: Multicast data handling, 6500 Phase 3 is not supported yet, OSPF routing protocol scaling.

- For 17xx, 26xx, 36xx, 37xx , 720x(NPE-G1), 7301:

  IOS 12.4 Mainline: 12.4(21a)*, 12.4(23)*
  IOS 12.4 T-train: 12.4(9)T7,12.4(15)T8

- For ASR- DMVPN Phase 2 Hub or spoke

  2.2.3 (02.02.02.122-33XNB3)

  2.3.0 (02.03.00.122-33.XNC)

- For 87x, 18xx, 28xx, 38xx:

  IOS 12.4 Mainline: 12.4(21a)*, 12.4(23)*
  IOS 12.4 T-train: 12.4(9)T7, 12.4(15)T8

- For 720x(NPE-G2+VSA): IOS 12.4 T-train:

  IOS 12.4 XD-train: 12.4(4)XD10,
  IOS 12.4 T-train: 12.4(15)T8

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Q & A


[communication]
[leadership]
[invention]
[inspiration]
[knowledge]
[collaboration]

Other On-Site VPN Sessions Networkers 2009

- SEC-2010: Deploying Remote Access IP Security and SSL VPNs
- SEC-2015: PKI for Large scale IPSEC Deployments
- SEC-3010: Troubleshooting Remote Access VPN
- SEC-3011: Troubleshooting GET-VPNs
- SEC-4010: Advanced Topics in Encryption Standards and Protocols
- SEC-4011: Advanced IPsec with GET VPN
- SEC-4012: Advanced IPsec Deployments with DMVPN

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Other Online VPN Sessions Networkers 2009

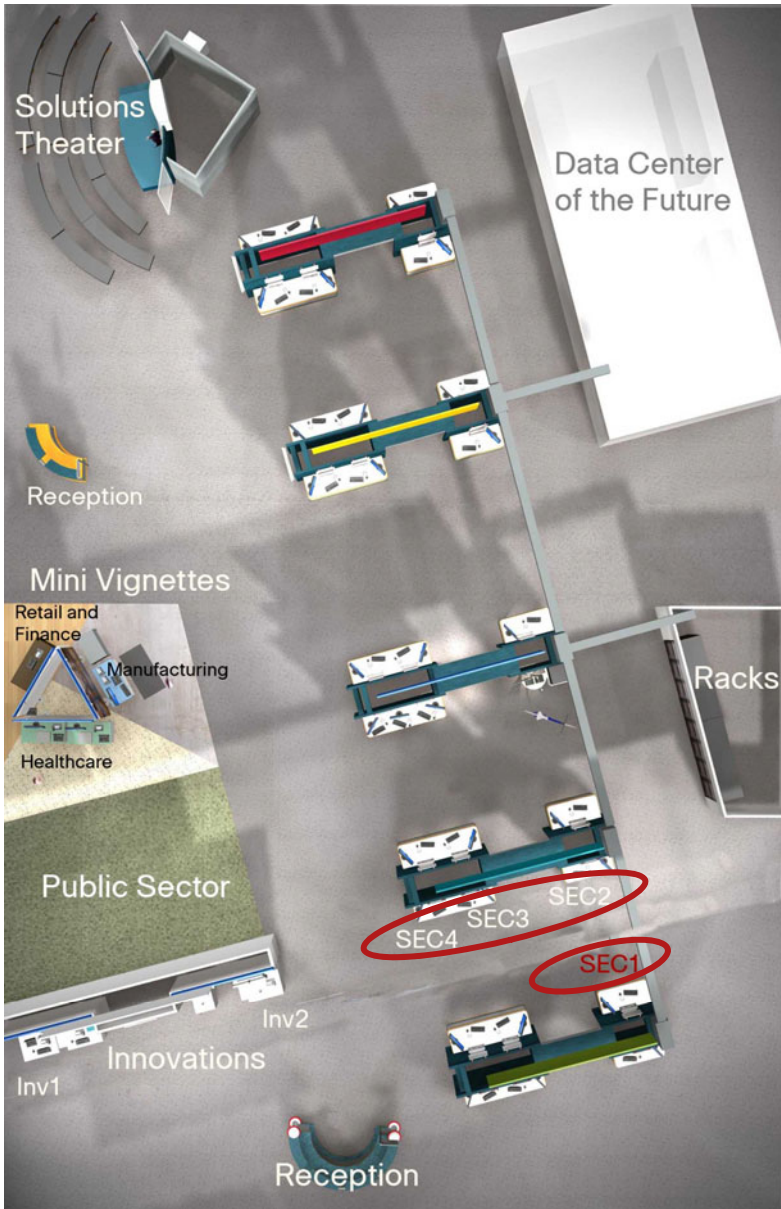
- SEC-2012: Deploying Dynamic Multipoint VPN
- SEC-2011: Deploying Site-to-Site IP Security VPNs

© 2008 Cisco Systems, Inc. All rights reserved.

Please Visit the Cisco Booth in the World of Solutions

See the technology in action

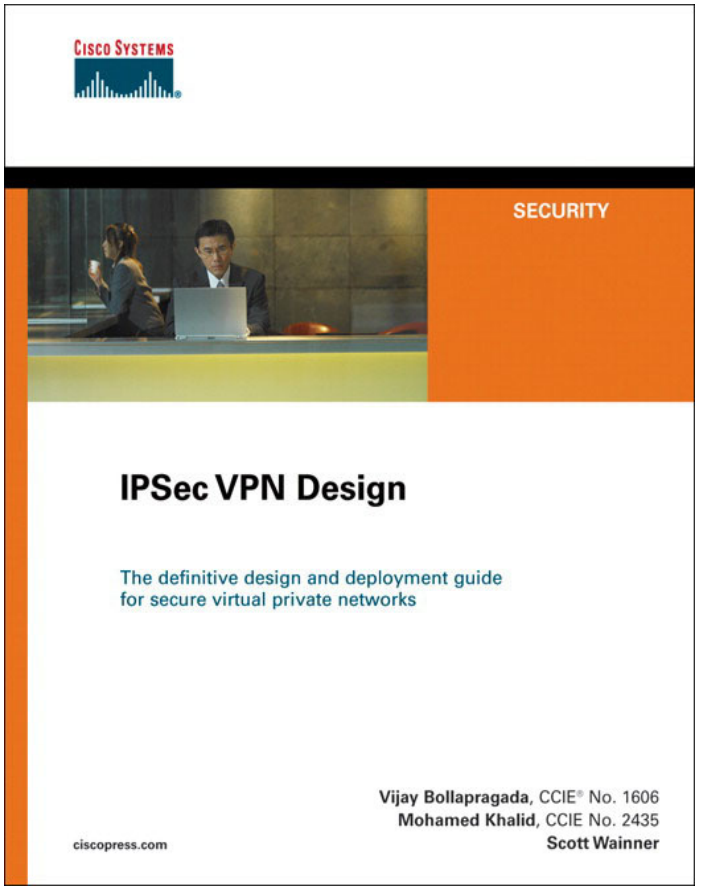
- Security
  - SEC1 – Data Loss Prevention Solutions and Services
  - SEC2 – Global Correlation Stops Threats
  - SEC3 – Cisco Identity-Based Security Solutions
  - SEC4 – Cisco Virtual Office Securing Remote Workers



© 2008 Cisco Systems, Inc. All rights reserved.

Recommended Reading

- Continue your Cisco Live learning experience with further reading from Cisco Press
- Check the Recommended Reading flyer for suggested books



Available Onsite at the Cisco Company Store

© 2008 Cisco Systems, Inc. All rights reserved.

Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Passport points for each session evaluation you complete.
- Complete your session evaluation online now (open a browser through our wireless network to access our portal) or visit one of the Internet stations throughout the Convention Center.

Don’t forget to activate your Cisco Live Virtual account for access to all session material, communities, and on-demand and live activities throughout the year. Activate your account at the Cisco booth in the World of Solutions or visit www.ciscolive.com.

© 2008 Cisco Systems, Inc. All rights reserved.

 © 2008 Cisco Systems, Inc. All rights reserved.

Appendix

- Configuration Simplicity
- Complete debug dmvpn detail all
- Case Study
- How to Open a TAC Case

© 2008 Cisco Systems, Inc. All rights reserved.

Configuration Simplicity

DMVPN Phases

- Phase 1: Hub and spoke functionality
- Phase 2: Spoke-to-spoke functionality
- Phase 3: Architecture and scaling

© 2008 Cisco Systems, Inc. All rights reserved.

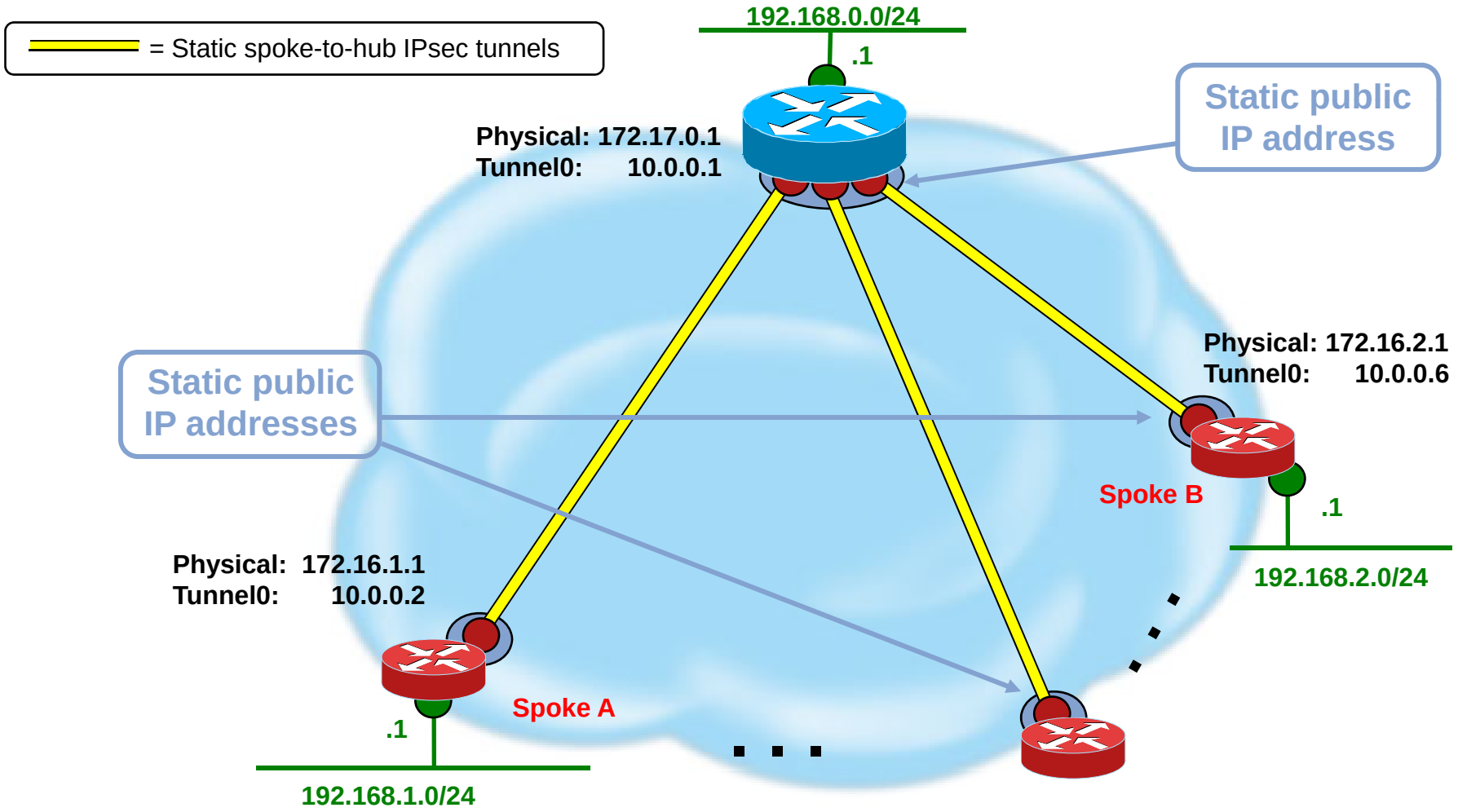
DMVPN Phase 1
Hub and Spoke Functionality

Phase 1 Hub and Spoke Benefits:

- Simplified and smaller configs for hub and spoke
- Zero touch provisioning for adding spokes to the VPN
- Easily supports dynamically addressed CPEs
- Support for multicast traffic from hub to spoke

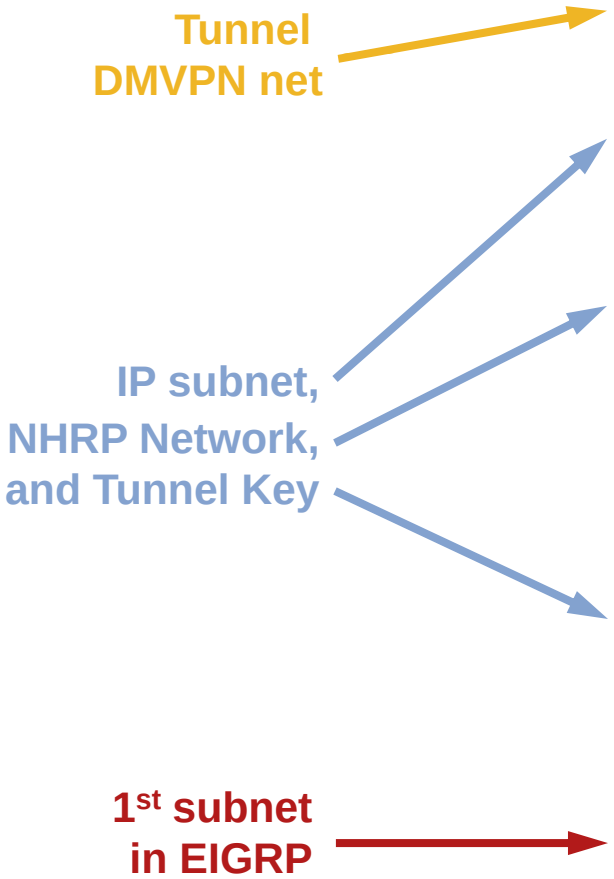
© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Single DMVPN Single Hub



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

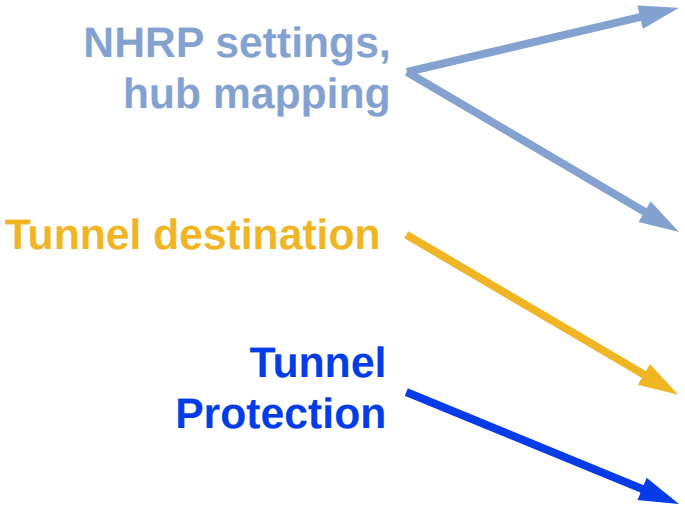
Single DMVPN Single Hub
Hub Configuration




```
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 network-id 100000
      ip nhrp holdtime 360
      ip summary-address eigrp 1 192.168.0.0 255.255.0.0
      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
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

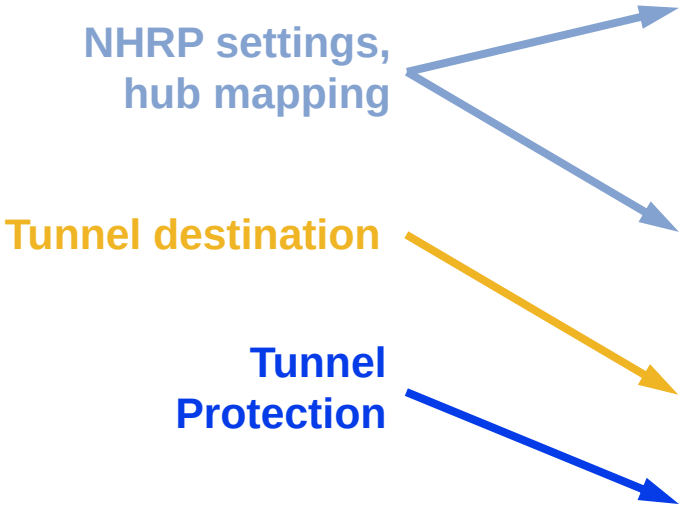
Single DMVPN Single Hub Spoke A Configuration




```
interface Tunnel0
    bandwidth 1000
    ip address 10.0.0.2 255.255.255.0
    ip mtu 1400
    ip nhrp authentication test
    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 nhrp nhs 10.0.0.1
    delay 1000
    ip tcp adjust-mss 1360
    tunnel source Serial1/0
    tunnel destination 172.17.0.1
    tunnel key 100000
    tunnel protection ipsec profile vpnprof
!
interface Serial1/0
    ip address negotiated
```


© 2008 Cisco Systems, Inc. All rights reserved.

Single DMVPN Single Hub Spoke B Configuration




```
interface Tunnel0
    bandwidth 1000
    ip address 10.0.0.6 255.255.255.0
    ip mtu 1400
    ip nhrp authentication test
    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 nhrp nhs 10.0.0.1
    delay 1000
    ip tcp adjust-mss 1360
    tunnel source Serial1/0
    tunnel destination 172.17.0.1
    tunnel key 100000
    tunnel protection ipsec profile vpnprof
!
interface Serial1/0
    ip address 172.16.2.1 255.255.255.252
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Hub and Spoke Design Summary

- Spoke-to-spoke traffic via hub
  - Hub router capabilities limit VPN
  - Simple example: 45Mb hub, (180) 256Kb spokes
- GRE tunnels
  - mGRE on hubs, p-pGRE or mGRE on spokes
- Summarize routing at hub
  - Spokes have smaller routing tables
  - Reduced load on hub routing protocol
- Add new spoke routers without changes
  - NHRP and routing protocol distribute information
- Redundancy and scaling
  - Multiple hub routers provide multiple paths

© 2008 Cisco Systems, Inc. All rights reserved.

DMVPN Phase 2
Spoke to Spoke Functionality

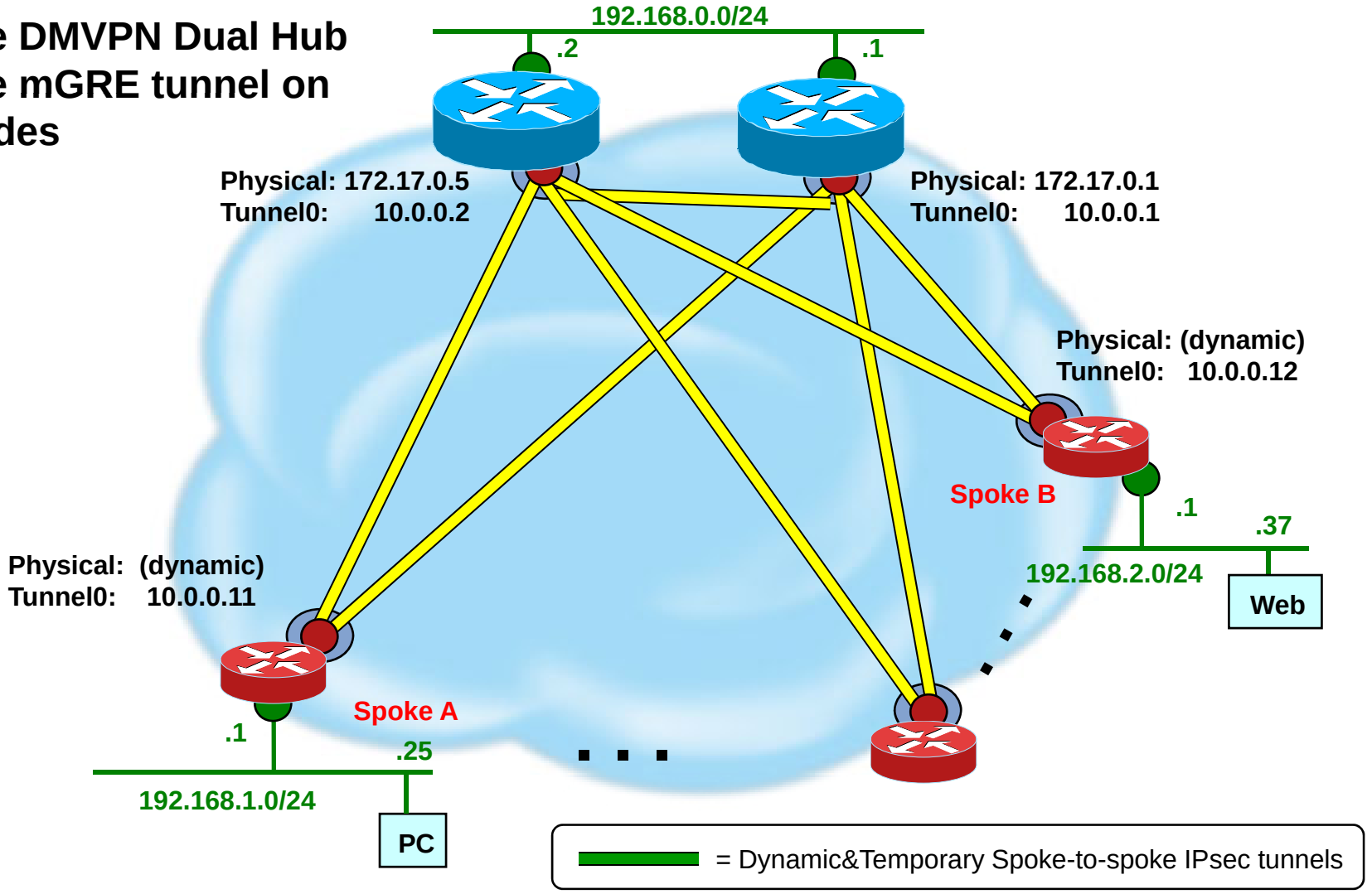
Phase 2—Spoke-to-Spoke Features

- Single mGRE interface with 'tunnel protection …'
  - On hubs and spokes
- Spoke-spoke data traffic direct
  - Reduced load on hub
  - Reduced latency
    - Single IPsec encrypt/decrypt
- Routing protocol
  - Still hub-and-spoke
  - Cannot summarize spoke routes on hub
  - Routes on spokes must have IP next-hop of remote spoke

© 2008 Cisco Systems, Inc. All rights reserved.

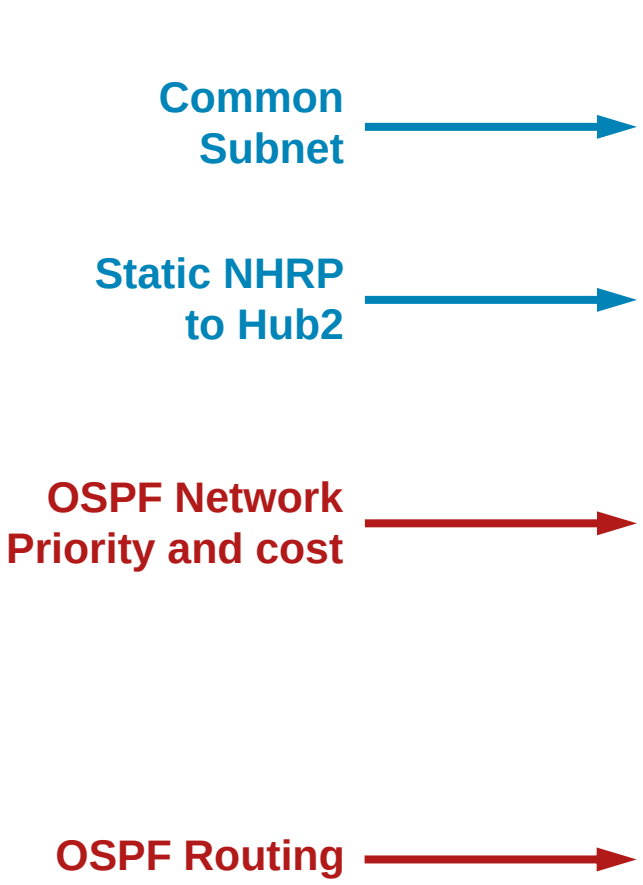
Single DMVPN Dual Hub Spoke to Spoke

Single DMVPN Dual Hub
Single mGRE tunnel on all nodes



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

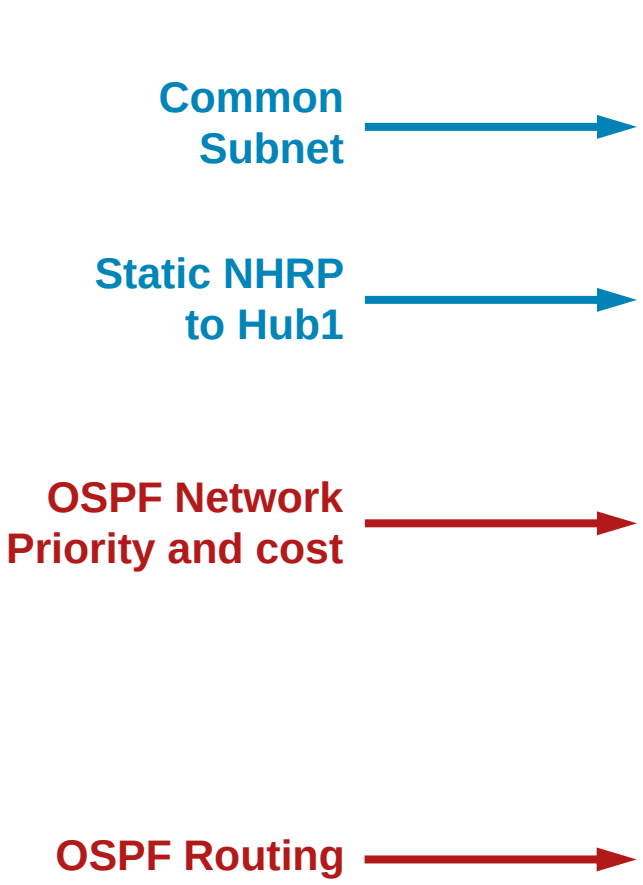
Single DMVPN Dual Hub
Hub1




```
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
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

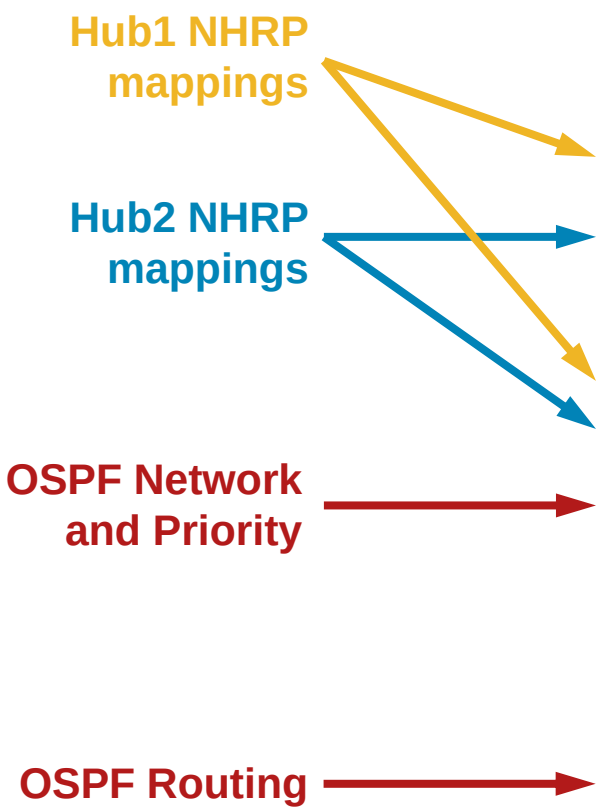
Single DMVPN Dual Hub
Hub2




```
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 1
     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
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Single DMVPN Dual Hub Spokes




```
interface Tunnel0
    bandwidth 1000
    ip address 10.0.0.<x> 255.255.255.0        ! <x> = 11,12,…
    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.<y>.0 0.0.0.255 area 1    ! <y> = 1,2,…
    distance 111 192.168.0.2 0.0.0.0
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

DMVPN Dynamic Spoke-Spoke Phase 2: Summary

- Increase network size
  - Add more hub routers ➔ larger hub router **daisy-chain**
    - Increase data and NHRP packet delay and hub load
      - Packets process-switched through daisy-chain
    - Greater complexity and load for routing protocol
- OSPF routing protocol ➔ only two hub routers
  - Network broadcast mode—DR, BDR
  - Single OSPF area
- Spokes must have full routing tables
  - Load on small spokes
  - Load on routing protocol on hub
    - 1000 spokes, 1 route per spoke → hub advertises 1000 routes to 1000 spokes → 1,000,000 advertisements

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

DMVPN Phase 3 Features

- Used to increase scale of DMVPN networks
  - Increase number of spokes, with same spoke/hub ratio
  - Distribution hubs off load central hub
    - Manage local spoke-spoke tunnels
    - IP multicast and routing protocol
- No hub daisy-chain
  - Use routing and CEF switching to forward data and NHRP packets optimally through hubs
  - Reduces complexity and load for routing protocol
- OSPF routing protocol not limited to two hubs
  - Network point-multipoint mode
  - Still single OSPF area

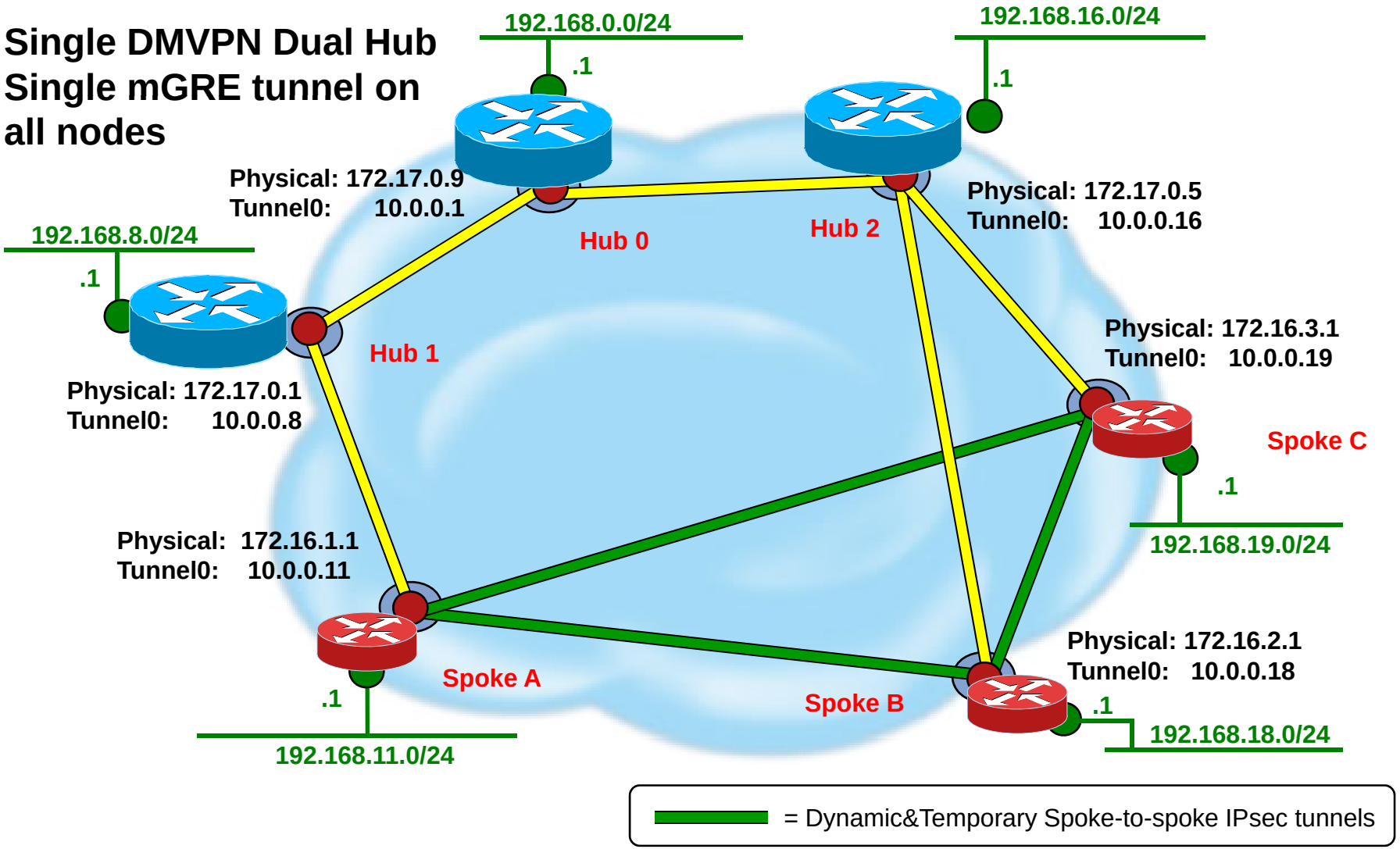
© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

DMVPN Phase 3 Features (Cont.)

- Spokes do not need full routing tables
  - Can summarize routes at the hub
  - Reduced space and load on small spokes
  - Reduced routing protocol load on hub
    - 1000 spokes, 1 route per spoke
    - Hub advertises 1 route to 1000 spokes →1000 advertisements
- Not available on 6500 or 7600
- Cannot mix Phase 2 and Phase 3 on same DMVPN
  - Migrate spokes from Phase 2 DMVPN to Phase 3 DMVPN

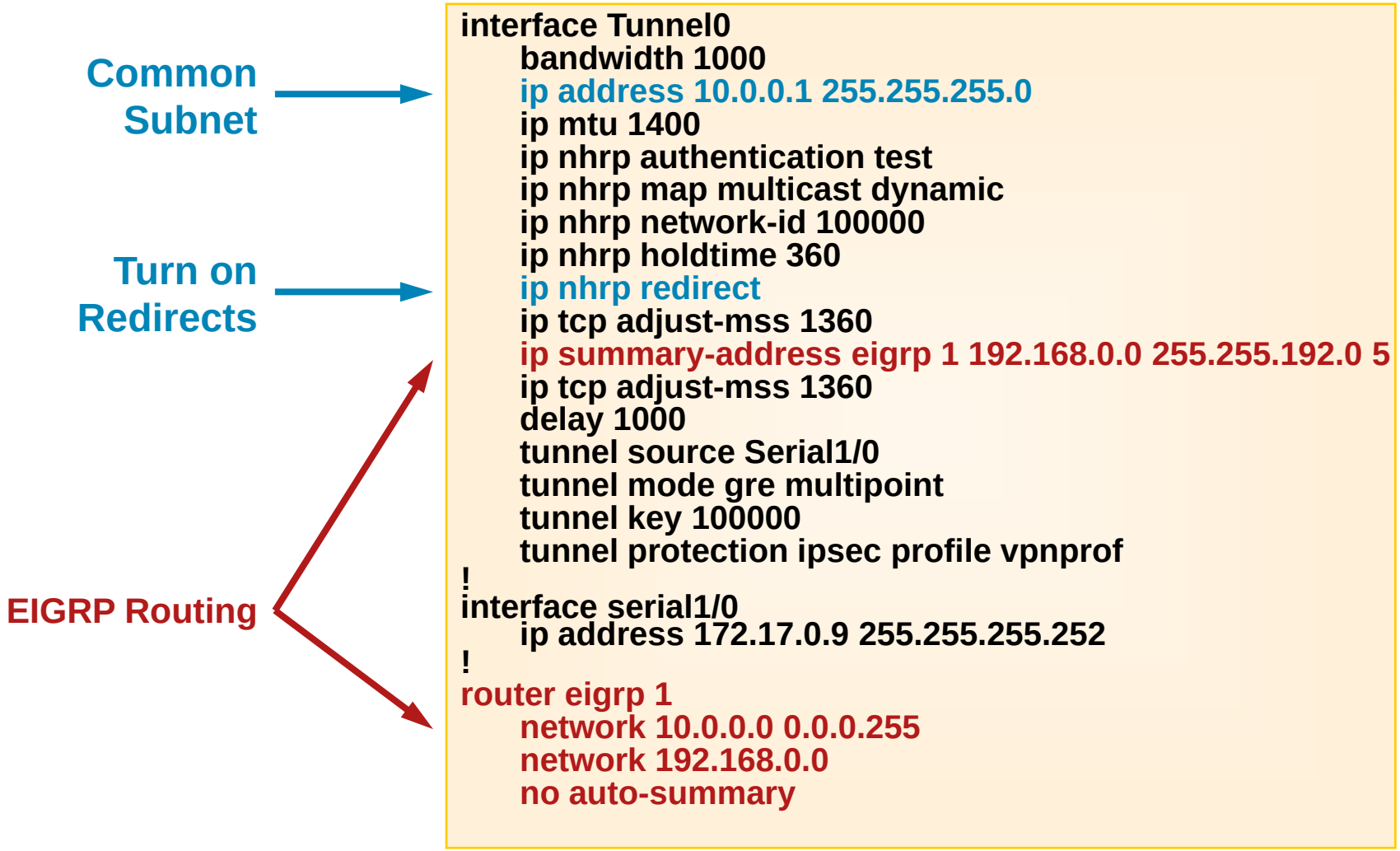
© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

DMVPN Hierarchical Hub (Phase 3)



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

DMVPN Hierarchical Hub
Hub0 (Central Hub)



© 2008 Cisco Systems, Inc. All rights reserved.

DMVPN Hierarchical Hub
Hub1 and Hub2 (Regional Hubs)

Hub 1

Common Subnet

Set Hub0 as NHS

Regional EIGRP summary route

```
interface Tunnel0
     ip address 10.0.0.8 255.255.255.0
     …
     ip nhrp map 10.0.0.1 172.17.0.9
     ip nhrp map multicast 172.17.0.9
     ip nhrp nhs 10.0.0.1
     …
     ip summary-address eigrp 1
                192.168.8.0 255.255.248.0 5
!
interface Ethernet0/0
     ip address 192.168.8.1 255.255.255.0
```

Hub 2

Common Subnet

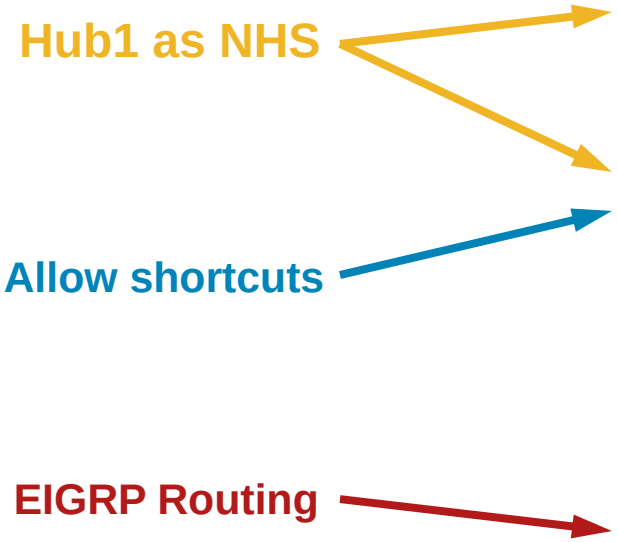
Set Hub0 as NHS

Regional EIGRP summary route

```
interface Tunnel0
     ip address 10.0.0.16 255.255.255.0
     …
     ip nhrp map 10.0.0.1 172.17.0.9
     ip nhrp map multicast 172.17.0.9
     ip nhrp nhs 10.0.0.1
     …
     ip summary-address eigrp 1
                192.168.16.0 255.255.248.0 5
!
interface Ethernet0/0
     ip address 192.168.16.1 255.255.255.0
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

DMVPN Hierarchical 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 10.0.0.8 172.17.0.1
      ip nhrp network-id 100000
      ip nhrp holdtime 360
      ip nhrp nhs 10.0.0.8
      ip nhrp shortcut
      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 192.168.11.0
      no auto-summary
!
interface Ethernet0/0
      ip address 192.168.11.1 255.255.255.0
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

DMVPN Hierarchical Hub
Spoke B and Spoke C

Spoke B

Common Subnet

Hub2 as NHS

EIGRP Routing

```
interface Tunnel0
      ip address 10.0.0.18 255.255.255.0
      …
      ip nhrp map 10.0.0.16 172.17.0.5
      ip nhrp map multicast 172.17.0.5
      ip nhrp nhs 10.0.0.16
!
      network 192.168.18.0
!
interface Ethernet0/0
      ip address 192.168.18.1 255.255.255.0
```

Spoke C

Common Subnet

Hub2 as NHS

EIGRP Routing

```
interface Tunnel0
      ip address 10.0.0.19 255.255.255.0
      …
      ip nhrp map 10.0.0.16 172.17.0.5
      ip nhrp map multicast 172.17.0.5
      ip nhrp nhs 10.0.0.16
!
      network 192.168.19.0
!
interface Ethernet0/0
      ip address 192.168.19.1 255.255.255.0
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

DMVPN Hierarchical Hub Phase 3 Summary

- Distribution hubs offload central hub
  - Increase scale of DMVPN network
  - Still allows spoke-spoke tunnels between regions
- Routing and CEF switching used to forward data and NHRP packets optimally through hubs
- Reduces complexity and load for routing protocol
- OSPF routing protocol not limited to two hubs
- Spokes do not need full routing tables

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

debug crypto isakmp
debug crypto ipsec

```
ISAKMP:(0):Old State = IKE_READY  New State = IKE_I_MM1
ISAKMP:(0): beginning Main Mode exchange
ISAKMP:(0): sending packet to 172.17.0.1 my_port 500 peer_port 500 (I) MM_NO_STATE
ISAKMP:(0):Sending an IKE IPv4 Packet.
ISAKMP (0:0): received packet from 172.17.0.1 dport 500 sport 500 Global (I) MM_NO_STATE
ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):Old State = IKE_I_MM1  New State = IKE_I_MM2
ISAKMP:(0): processing SA payload. message ID = 0
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
ISAKMP (0:0): vendor ID is NAT-T v7
ISAKMP:(0):found peer pre-shared key matching 172.17.0.1
ISAKMP:(0): local preshared key found
ISAKMP:(0):Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP:(0):atts are acceptable. Next payload is 0
```


© 2008 Cisco Systems, Inc. All rights reserved.

debug crypto isakmp
debug crypto ipsec (cont)

```
ISAKMP:(0):Acceptable atts:actual life: 0
ISAKMP:(0):Acceptable atts:life: 0
ISAKMP:(0):Fill atts in sa vpi_length:4
ISAKMP:(0):Fill atts in sa life_in_seconds:86400
ISAKMP:(0):Returning Actual lifetime: 86400
ISAKMP:(0)::Started lifetime timer: 86400.
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
ISAKMP (0:0): vendor ID is NAT-T v7
ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(0):Old State = IKE_I_MM2  New State = IKE_I_MM2
ISAKMP:(0): sending packet to 172.17.0.1 my_port 500 peer_port 500 (I) MM_SA_SETUP
ISAKMP:(0):Sending an IKE IPv4 Packet.
ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(0):Old State = IKE_I_MM2  New State = IKE_I_MM3
ISAKMP (0:0): received packet from 172.17.0.1 dport 500 sport 500 Global (I) MM_SA_SETUP
ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):Old State = IKE_I_MM3  New State = IKE_I_MM4
ISAKMP:(0): processing KE payload. message ID = 0
ISAKMP:(0): processing NONCE payload. message ID = 0
ISAKMP:(0):found peer pre-shared key matching 172.17.0.1
ISAKMP:(1034): processing vendor id payload
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

debug crypto isakmp
debug crypto ipsec (cont)

```
ISAKMP:(1034): vendor ID is Unity
ISAKMP:(1034): processing vendor id payload
ISAKMP:(1034): vendor ID is DPD
ISAKMP:(1034): processing vendor id payload
ISAKMP:(1034): speaking to another IOS box!
ISAKMP:(1034):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1034):Old State = IKE_I_MM4  New State = IKE_I_MM4
ISAKMP:(1034):Send initial contact
ISAKMP:(1034):SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP (0:1034): ID payload
    next-payload       : 8
    type               :    1
    address            : 172.16.1.1
    protocol           : 17
    port               : 500
    length             : 12
ISAKMP:(1034):Total payload length: 12
ISAKMP:(1034): sending packet to 172.17.0.1 my_port 500 peer_port 500 (I) MM_KEY_EXCH
ISAKMP:(1034):Sending an IKE IPv4 Packet.
ISAKMP:(1034):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1034):Old State = IKE_I_MM4  New State = IKE_I_MM5
ISAKMP (0:1034): received packet from 172.17.0.1 dport 500 sport 500 Global (I) MM_KEY_EXC
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

debug crypto isakmp
debug crypto ipsec (cont)

```
ISAKMP:(1034):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1034):Old State = IKE_I_MM4  New State = IKE_I_MM5
ISAKMP (0:1034): received packet from 172.17.0.1 dport 500 sport 500 Global (I) MM_KEY_EXCH
ISAKMP:(1034): processing ID payload. message ID = 0
ISAKMP (0:1034): ID payload
    next-payload      : 8
    type              : 1
    address           : 172.17.0.1
    protocol          : 17
    port              : 500
    length            : 12
ISAKMP:(1034): processing HASH payload. message ID = 0
ISAKMP:(1034):SA authentication status: authenticated
ISAKMP:(1034):SA has been authenticated with 172.17.0.1
ISAKMP:(1034):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(1034):Old State = IKE_I_MM5  New State = IKE_I_MM6
ISAKMP:(1034):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1034):Old State = IKE_I_MM6  New State = IKE_I_MM6
ISAKMP:(1034):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1034):Old State = IKE_I_MM6  New State = IKE_P1_COMPLETE
```


© 2008 Cisco Systems, Inc. All rights reserved.

debug crypto isakmp
debug crypto ipsec (cont)

```
ISAKMP:(1034):beginning Quick Mode exchange, M-ID of -814520840
ISAKMP:(1034):QM Initiator gets spi
ISAKMP:(1034): sending packet to 172.17.0.1 my_port 500 peer_port 500 (I) QM_IDLE
ISAKMP:(1034):Sending an IKE IPv4 Packet.
ISAKMP:(1034):Node -814520840, Input = IKE_MESG_INTERNAL, IKE_INIT_QM
ISAKMP:(1034):Old State = IKE_QM_READY  New State = IKE_QM_I_QM1
ISAKMP:(1034):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP:(1034):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE
ISAKMP (0:1034): received packet from 172.17.0.1 dport 500 sport 500 Global (I) QM_IDLE
ISAKMP:(1034): processing HASH payload. message ID = -814520840
ISAKMP:(1034): processing SA payload. message ID = -814520840
ISAKMP:(1034):Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      encaps is 2 (Transport)
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (basic) of 3600
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:(1034):atts are acceptable.
ISAKMP:(1034): processing NONCE payload. message ID = -814520840
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

debug crypto isakmp
debug crypto ipsec (cont)

```
ISAKMP:(1034): processing ID payload. message ID = -814520840
ISAKMP:(1034): processing ID payload. message ID = -814520840
ISAKMP:(1034): Creating IPSec SAs
     inbound SA from 172.17.0.1 to 172.16.1.1 (f/i)  0/ 0
    (proxy 172.17.0.1 to 172.16.1.1)
    has spi 0x846912E and conn_id 0
    lifetime of 3600 seconds
    lifetime of 4608000 kilobytes
    outbound SA from 172.16.1.1 to 172.17.0.1 (f/i) 0/0
    (proxy 172.16.1.1 to 172.17.0.1)
    has spi  0x42DE56D2 and conn_id 0
    lifetime of 3600 seconds
    lifetime of 4608000 kilobytes
ISAKMP:(1034): sending packet to 172.17.0.1 my_port 500 peer_port 500 (I) QM_IDLE
ISAKMP:(1034):Sending an IKE IPv4 Packet.
ISAKMP:(1034):deleting node -814520840 error FALSE reason "No Error"
ISAKMP:(1034):Node -814520840, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1034):Old State = IKE_QM_I_QM1  New State = IKE_QM_PHASE2_COMPLETE
```


© 2008 Cisco Systems, Inc. All rights reserved.

Four Layers for Troubleshooting: GRE Encapsulation Layer—debug nhrp

debug nhrp packet

```
NHRP: Send Registration Request via Tunnel0 vrf 0, packet size: 104 src: 10.0.0.9, dst: 10.0.0.1
  (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
    shtl: 4(NSAP), sstl: 0(NSAP)
  (M) flags: "unique nat ", reqid: 1279
    src NBMA: 172.16.1.1
    src protocol: 10.0.0.9, dst protocol: 10.0.0.1
  (C-1) code: no error(0)
    prefix: 255, mtu: 1514, hd_time: 300
    addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0

NHRP: Receive Registration Reply via Tunnel0 vrf 0, packet size: 124
  (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
    shtl: 4(NSAP), sstl: 0(NSAP)
  (M) flags: "unique nat ", reqid: 1279
    src NBMA: 172.16.1.1.
    src protocol: 10.0.0.9, dst protocol: 10.0.0.1
  (C-1) code: no error(0)
     prefix: 255, mtu: 1514, hd_time: 300
     addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Case Study


[communication]
[leadership]
[invention]
[inspiration]
[knowledge]
[collaboration]

Case Study

- Some TCP based applications are not passing traffic through DMVPN network

© 2008 Cisco Systems, Inc. All rights reserved.

Problem Description

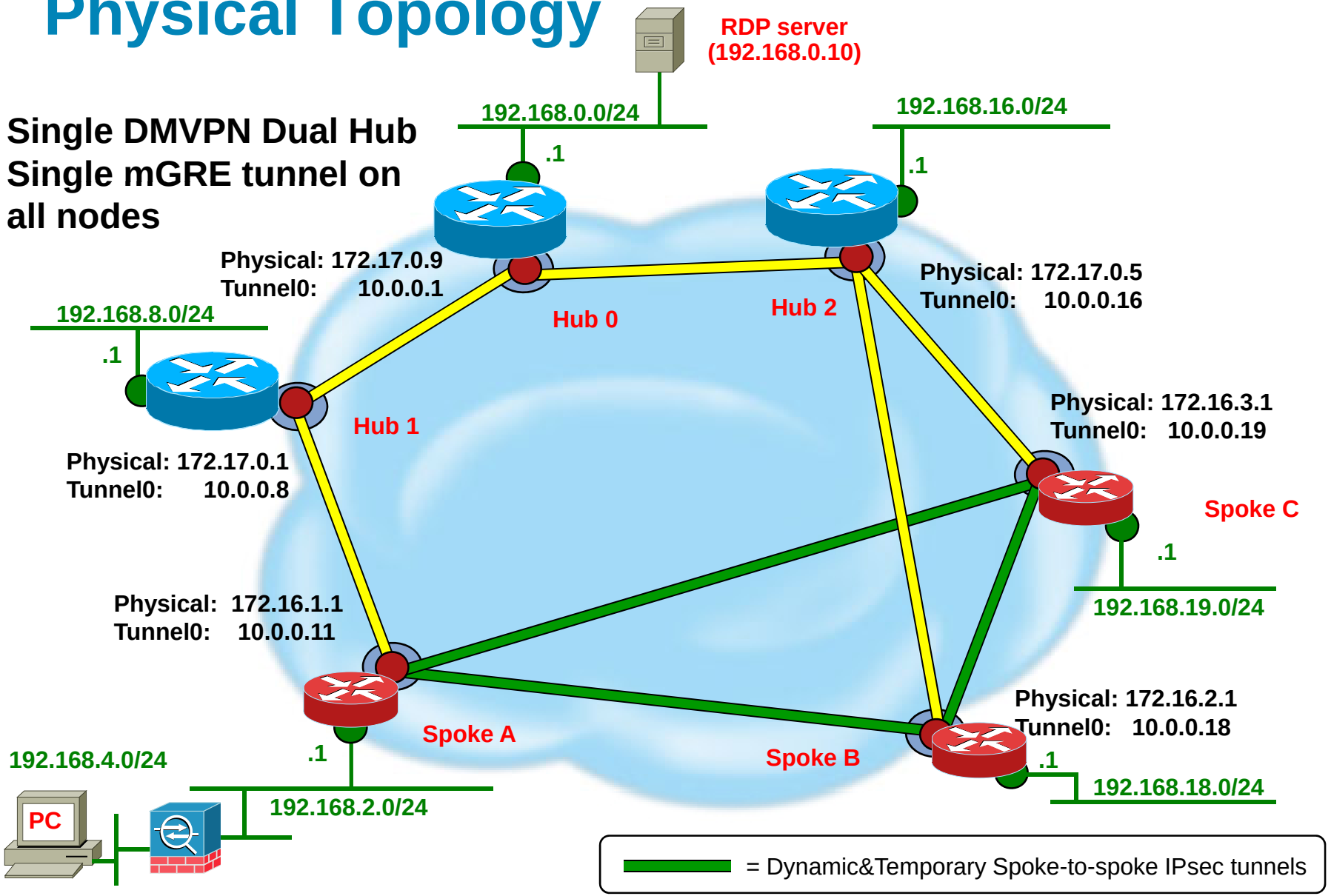
It is observed that data traffic between a TCP client and server is not passing through DMVPN network.

For example, Access Remote Desktop TCP application in which the server is located behind the hub router and the client is located behind one of the DMVPN spoke routers are unable to pass data traffic.

However they can access the same server locally without going through the DMVPN network.

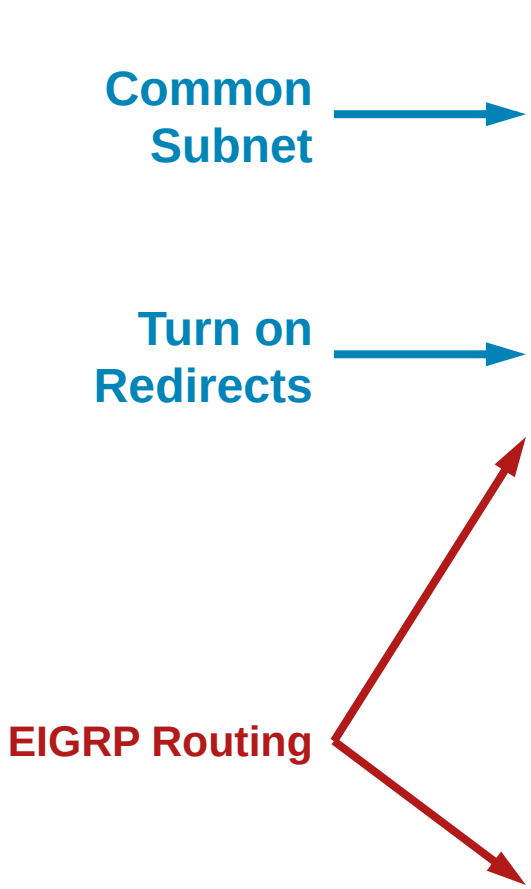
© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Physical Topology



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Hub0 Configuration—Central Hub

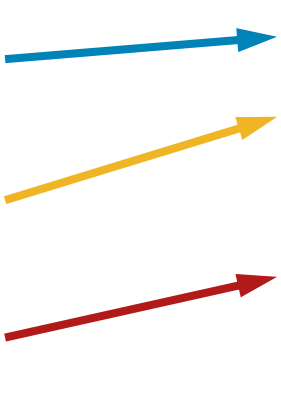



```
interface Tunnel0
      bandwidth 1000
      ip address 10.0.0.1 255.255.255.0
      ip mtu 1400
      ip nhrp authentication test
      ip nhrp map multicast dynamic
      ip nhrp network-id 100000
      ip nhrp holdtime 360
      ip nhrp redirect
      ip summary-address eigrp 1 192.168.0.0 255.255.192.0 5
      delay 1000
      tunnel source Serial1/0
      tunnel mode gre multipoint
      tunnel key 100000
      tunnel protection ipsec profile vpnprof
!
interface serial1/0
      ip address 172.17.0.9 255.255.255.252
!
router eigrp 1
      network 10.0.0.0 0.0.0.255
      network 192.168.0.0
      no auto-summary
```


© 2008 Cisco Systems, Inc. All rights reserved.

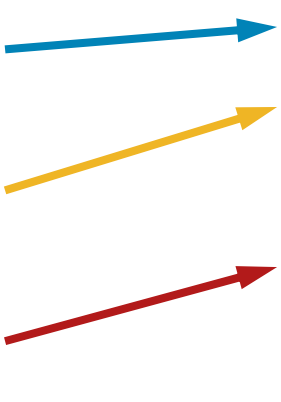
Hub1 and Hub2 (Regional Hubs) Configuration

Hub 1




```
interface Tunnel0
     ip address 10.0.0.8 255.255.255.0
     …
     ip nhrp map 10.0.0.1 172.17.0.9
     ip nhrp map multicast 172.17.0.9
     ip nhrp nhs 10.0.0.1
     …
     ip summary-address eigrp 1
                192.168.8.0 255.255.248.0 5
!
interface Ethernet0/0
     ip address 192.168.8.1 255.255.255.0
```

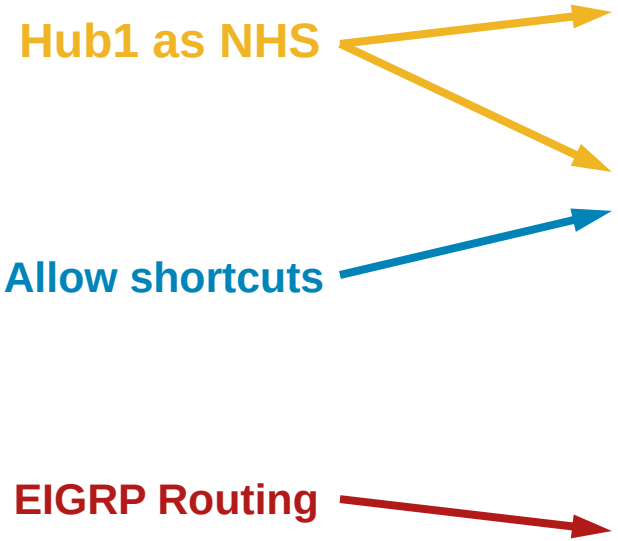
Hub 2




```
interface Tunnel0
     ip address 10.0.0.16 255.255.255.0
     …
     ip nhrp map 10.0.0.1 172.17.0.9
     ip nhrp map multicast 172.17.0.9
     ip nhrp nhs 10.0.0.1
     …
     ip summary-address eigrp 1
                192.168.16.0 255.255.248.0 5
!
interface Ethernet0/0
     ip address 192.168.16.1 255.255.255.0
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Spoke A Configuration




```
interface Tunnel0
      bandwidth 1000
      ip address 10.0.0.9 255.255.255.0
      ip mtu 1400
      ip nhrp authentication test
      ip nhrp map multicast 172.17.0.1
      ip nhrp map 10.0.0.8 172.17.0.1
      ip nhrp network-id 100000
      ip nhrp holdtime 360
      ip nhrp nhs 10.0.0.8
      ip nhrp shortcut
      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
      no auto-summary
!
interface Ethernet0/0
      ip address 192.168.2.1 255.255.255.0
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Spoke B and Spoke C Configuration

Spoke B

Common Subnet

Hub2 as NHS

EIGRP Routing

```
interface Tunnel0
     ip address 10.0.0.18 255.255.255.0
     …
     ip nhrp map 10.0.0.16 172.17.0.5
     ip nhrp map multicast 172.17.0.5
     ip nhrp nhs 10.0.0.16
!
     network 192.168.18.0
!
interface Ethernet0/0
     ip address 192.168.18.1 255.255.255.0
```

Spoke C

Common Subnet

Hub2 as NHS

EIGRP Routing

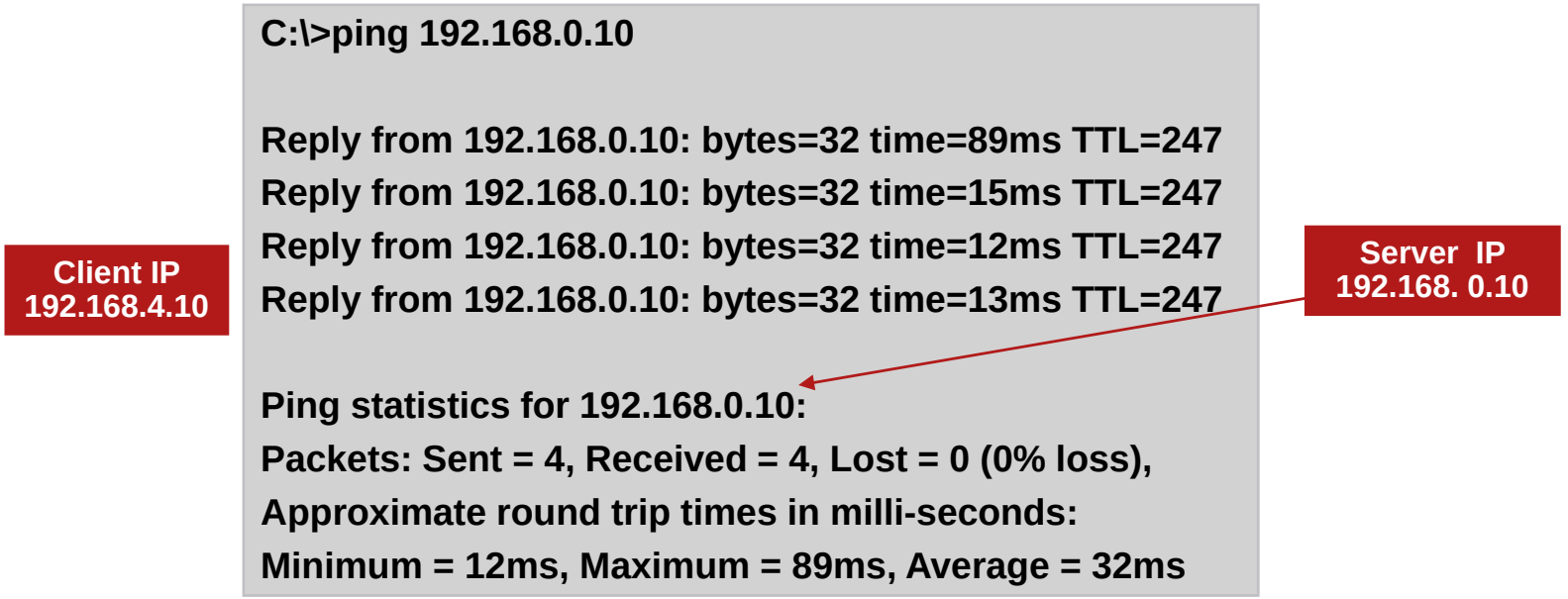
```
interface Tunnel0
     ip address 10.0.0.19 255.255.255.0
     …
     ip nhrp map 10.0.0.16 172.17.0.5
     ip nhrp map multicast 172.17.0.5
     ip nhrp nhs 10.0.0.16
!
     network 192.168.19.0
!
interface Ethernet0/0
     ip address 192.168.19.1 255.255.255.0
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Troubleshooting

Physical and Routing Layer

- Ping test between TCP client and server to make sure we have end to end connectivity



© 2008 Cisco Systems, Inc. All rights reserved.

Troubleshooting (Cont.)

IPsec Encryption Layer—

- Verify IKE Phase 1 status

```
Spoke# show crypto  isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id  slot       status
172.16.1.1      172.17.0.1      QM_IDLE           1071    0       ACTIVE
```

- Verify IPsec Phase 2 status

```
Spoke #show crypto ipsec sa peer 172.17.0.1
  Crypto map tag: Tunnel0-head-0, local addr 172.16.1.1
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
   current_peer 172.17.0.1 port 500
   #pkts encaps: 178014, #pkts encrypt: 178014, #pkts digest: 178014
   #pkts decaps: 178996, #pkts decrypt: 178996, #pkts verify: 178996
    local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.17.0.1
    path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
    inbound esp sas:
     spi: 0xA24D132D(2722960173)
    outbound esp sas:
     spi: 0x2EB5DA79(783669881)
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Troubleshooting (Cont.)

The GRE Encapsulation Layer—NHRP

- Verify NHRP mapping in hub

```
Hub# show ip nhrp
10.0.0.9/32 via 10.0.0.9, Tunnel0 created 1w2d, expire 00:04:52
  Type: dynamic, Flags: unique nat registered used
  NBMA address: 172.16.1.1
```

- Verify crypto socket status

```
Hub # show crypto socket
Tu0 Peers (local/remote): 172.17.0.1/172.16.1.1
      Local Ident  (addr/mask/port/prot): (172.17.0.1/255.255.255.255/0/47)
      Remote Ident (addr/mask/port/prot): (172.16.1.1/255.255.255.255/0/47)
      IPsec Profile: "dmvpn"
      Socket State: Open
      Client: "TUNNEL SEC" (Client State: Active)
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Troubleshooting (Cont.)

VPN Routing Layer

```
Spoke#show ip route 192.168.0.0

Routing entry for 192.168.0.0/24
  Known via "eigrp 10", distance 90, metric 2818560, type internal
  Redistributing via eigrp 10
  Last update from 10.0.0.1 on Tunnel0, 03:37:17 ago
  Routing Descriptor Blocks:
  * 10.0.0.1, from 10.0.0.1, 03:37:17 ago, via Tunnel0
      Route metric is 2818560, traffic share count is 1
      Total delay is 10100 microseconds, minimum bandwidth is 1000 Kbit
      Reliability 255/255, minimum MTU 1400 bytes
      Loading 1/255, Hops 1
```

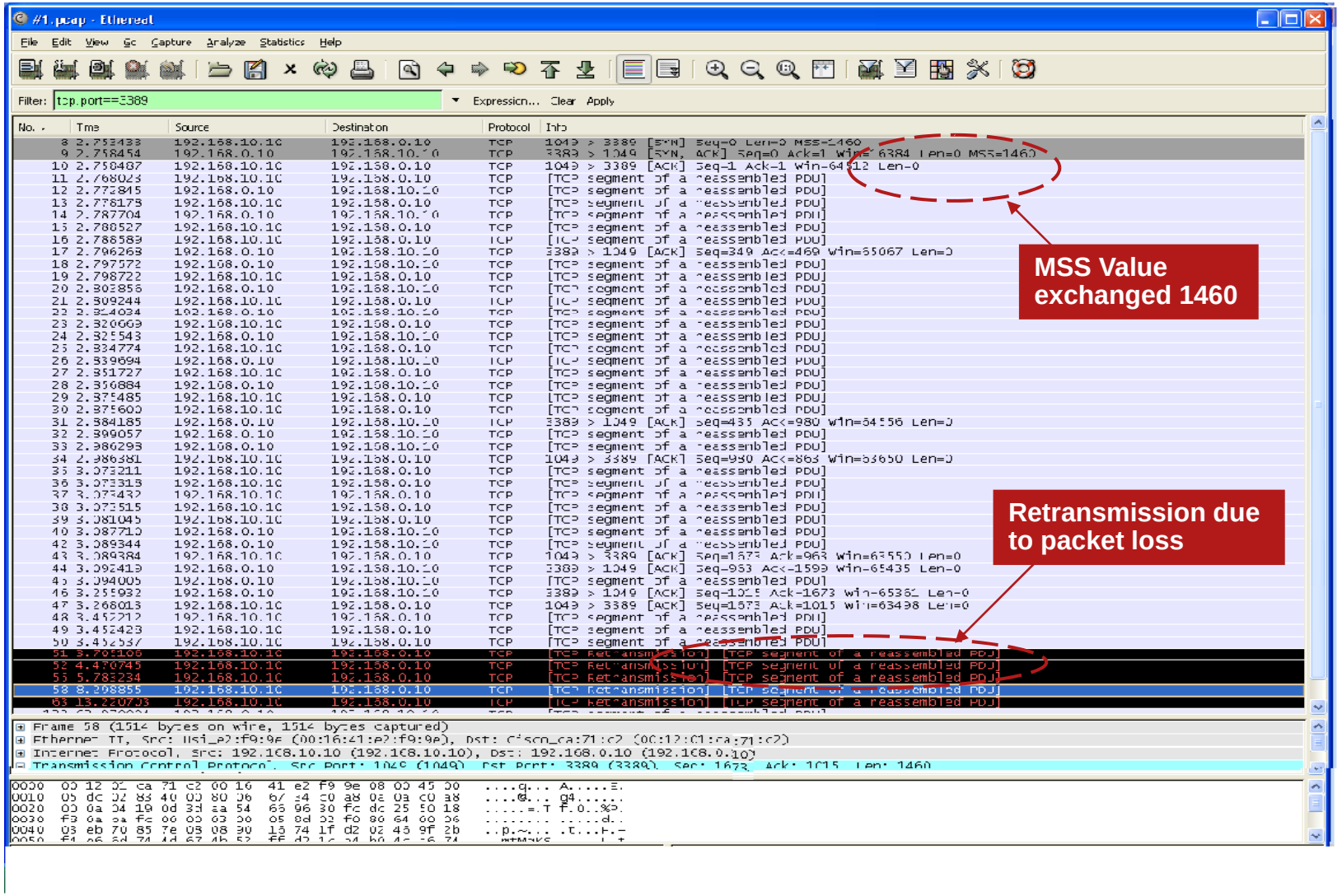
Route for RDP Server network

```
Spoke# show ip route

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, FastEthernet0/1
D    192.168.11.0/24 [90/3200000] via 10.0.0.11, 05:17:21, Tunnel0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Tunnel0
D    192.168.0.0/24 [90/2818560] via 10.0.0.1, 03:38:30, Tunnel0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 172.16.1.2
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

How to detect – Sniffer capture



Solution

- Configured “ip tcp adjust-mss 1360” on tunnel interface
- MSS is the Maximum Segment Size—or the maximum amount of data that can be sent in a single packet
- The MSS is set in the SYN packets
- The device that receives the MSS advertisement cannot send more data in a single packet to the peer than specified by the MSS

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Solution (Cont.)

- Best practice Configure tcp adjust mss value in all tunnel interfaces in DMVPN network.

Spoke (A,B,C)

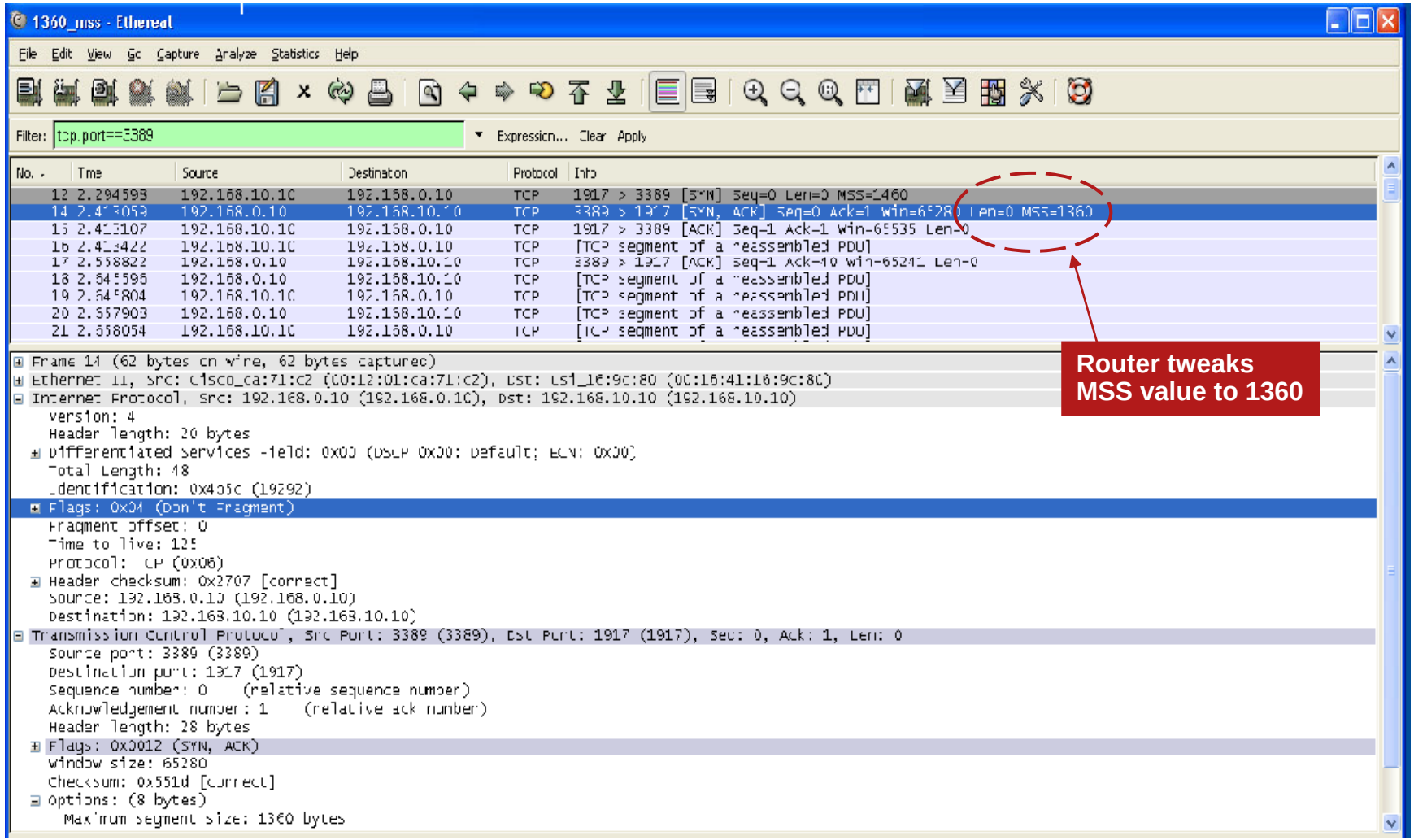
```
interface Tunnel0
    …
    ip mtu 1400
    …
    ip tcp adjust-mss 1360
    …
```

Hub (0,1,2)

```
interface Tunnel0
    …
    ip mtu 1400
    …
    ip tcp adjust-mss 1360
    …
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Verification-Sniffer Capture



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

Opening a TAC Case

- If after using all your troubleshooting tools you still cannot resolve the problem, please open a TAC case:

  http://www.cisco.com/techsupport/servicerequest/

- At a minimum include

  Detailed problem description

  Output from “show tech”

- Optionally include

  Syslogs captured during time of problem

  Capture debug dmvpn detail all at the time of problem and show dmvpn detail

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Public