NETWORKERS 2003

THE POWER TO TRANSFORM BUSINESS. now.

Cisco Systems

Cisco.com

Deploying Large IPsec VPNs

Session SEC-2001

Franjo Majstor
fmajstor@cisco.com
Cisco Systems, Inc.

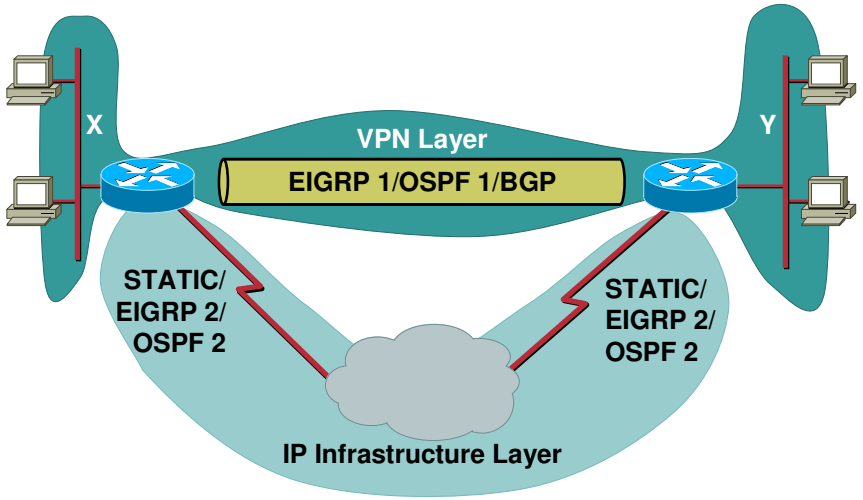
Agenda

Cisco.com

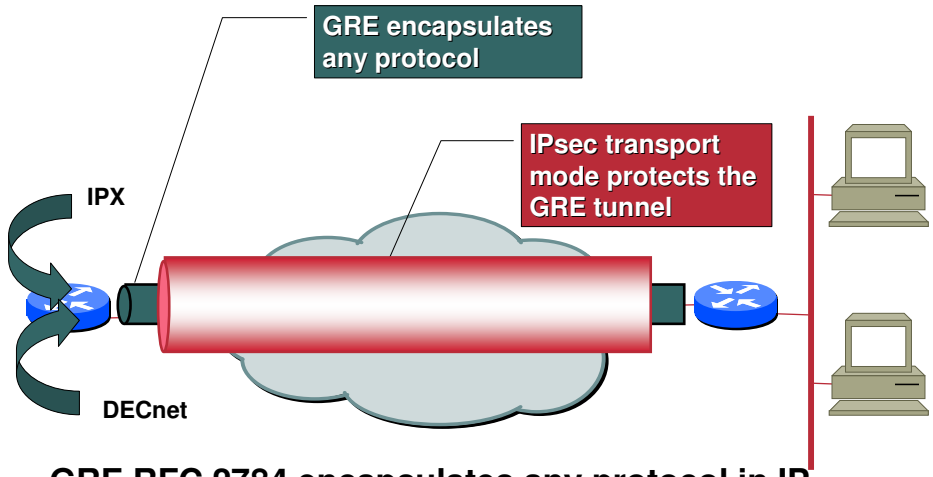
- Introduction
- Topologies
- Resiliency and performance
- Scalable authentication
- Q&A

Introduction

VPN Tunnelling



Tunnelling types - GRE



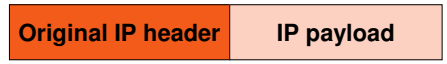
GRE RFC 2784 encapsulates any protocol in IP

GRE (Cont.)

- GRE is RFC2784
- Standards Track by Cisco, Procket and Juniper
- Uses protocol 47
- Works for several IP protocols: IP, IPX, DECnet, IPv6, …
- Works for multicast traffic
- Overhead: 24 bytes

Generic Routing Encapsulation

Original IP datagram *(before forwarding)*



GRE encapsulation *(after forwarding to a GRE tunnel)*

GRE packet with new IP header: protocol 47 *(forwarded using new IP dst)*

GRE: IOS Configuration

Cisco.com

```
interface Tunnel0
 ip address 192.168.100.1 255.255.255.252
 tunnel source 193.193.193.1
 tunnel destination 194.194.194.1
 tunnel mode gre ip
```

GRE is the default tunnel mode, so, this line will not appear in a show running-config

Tunnelling types - IPinIP

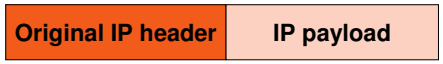
Cisco.com

- IPinIP is RFC2003
- Standards Track by IBM
- Uses protocol 4
- Only works for IP
- Used by IPsec tunnel mode
- Overhead: 20 bytes

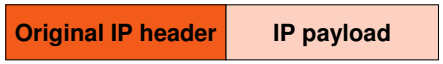
IPinIP Encapsulation

Cisco.com

Original IP datagram *(before forwarding)*



IPinIP encapsulation *(after forwarding to a IPinIP tunnel)*



IPinIP packet with new IP header: protocol 4 *(forwarded using new IP dst)*

IP in IP: IOS configuration

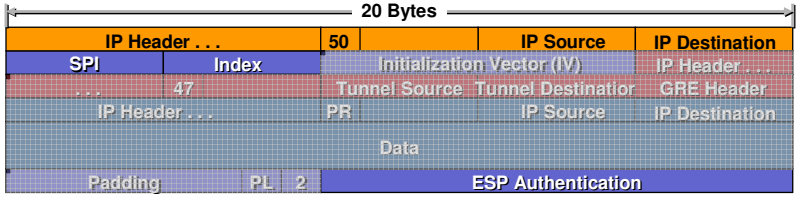
Cisco.com

```
interface Tunnel0
 ip address 192.168.100.1 255.255.255.252
 tunnel source 193.193.193.1
 tunnel destination 194.194.194.1
 tunnel mode ipip
```

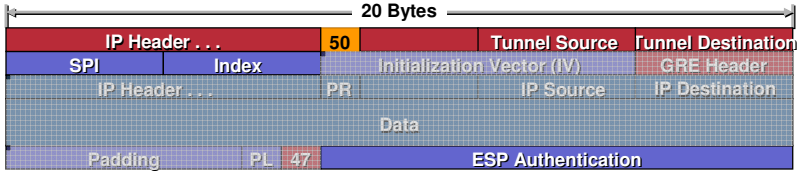
IPsec + GRE Packets

Cisco.com

IPsec Tunnel Mode + GRE



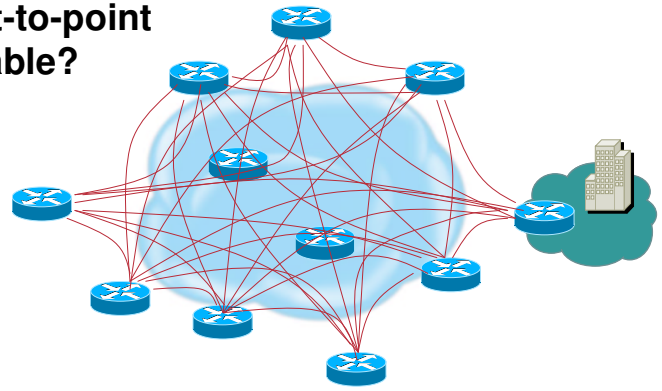
IPsec Transport Mode + GRE



Large Networks : n(n-1)/2 issue

Cisco.com

IPsec point-to-point …manageable?



Large Scale Design Issues

Cisco.com

- **Network design**
  - Hub and spoke, dynamic-mesh and full-mesh
- **Routing**
  - Dynamic routing protocols
- **Encryption peers**
  - Finding, mapping and authenticating
- **Configuring and maintaining**

Agenda

Cisco.com

- **Introduction**
- **Topologies**
- **Resiliency and performance**
- **Scalable authentication**
- **Q&A**

Toplogies

Network Design 1: Hub-and-Spoke

Cisco.com

- Easier to deploy
  - Configuration change on new node and hub to add a new node
  - Can result in unwieldy hub configuration
  - Dynamic routing
- Traffic patterns
  - All traffic must go via hub
    - Two encrypts/decrypts for spoke-to-spoke traffic
    - Hub bandwidth and CPU utilization limit VPN
- Number of tunnels = O(n)

Network Design 2: Full-Mesh

Cisco.com

- Harder to deploy
  - Configuration change on all nodes to add a new node
  - Can result in unwieldy configuration on all nodes
  - Dynamic routing may limit size
- Traffic patterns
  - Direct tunnels between all nodes
    - Single encrypt/decrypt
  - Smaller spoke routers limit VPN size
    - Configuration size, memory and CPU utilization
- Number of tunnels = $O(n^2)$

Network Design 3: Dynamic Mesh

Cisco.com

- Easy to deploy
  - Simplified hub configuration files
  - Adding a node - configure new node and deploy
  - Dynamically addressed spokes - (DSL, Cable)
- Traffic patterns
  - Control traffic (dynamic routing) - hub and spoke
  - Data traffic - dynamic mesh
    - Spoke routers only need to support connections currently in use
- Number of tunnels > O(n), << $O(n^2)$

VPN Peer Mapping

Cisco.com

- **Static mappings**

  Static IP infrastructure address, doesn't scale for IPsec or IPsec+GRE

- **Tunnel Endpoint Discovery (TED)**

  Dynamic peer address, public routable addresses, IPsec only

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

  Dynamic peer address and spoke-spoke tunnels, IPsec+mGRE

Authenticating Peers

Cisco.com

- **Pre-shared keys**

  Per peer (doesn't scale), wildcard (insecure)

- **Certificates**

  Certificate Authority (CA)

  Certificate distribution - enrollment

    Manual (terminal, tftp), SCEP

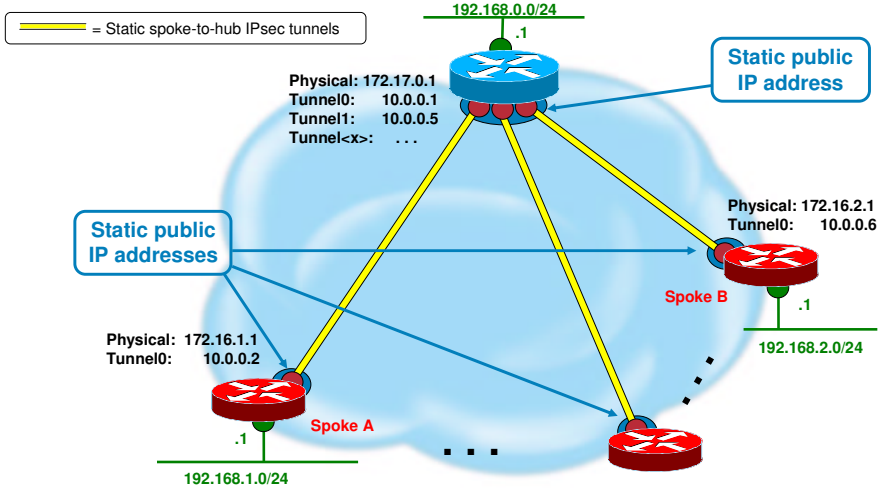
  Some requirements for use

    Accurate time - NTP, SNTP

    Check for revocation - 'crl optional'

IPsec+GRE

Cisco.com



IPsec+GRE

Cisco.com

- **Supports dynamic routing protocols**
- **VPN peer mapping**

  Dynamic on hub, static on spoke

- **Point-to-point GRE tunnel interfaces**

  Single GRE interface for each spoke

  Static tunnel destination

  Large hub configuration

IPsec+GRE
Hub Configuration

Cisco.com

```
crypto ca trustpoint msca-root
      enrollment terminal
      crl optional
      rsakeypair hub1
crypto ca certificate chain msca-root
      certificate 2368DB55000000000B4E
      certificate ca 1244325DE0369880465F977A18F61CA8
!
crypto isakmp policy 1
      encryption 3des
!
crypto ipsec transform-set t1 esp-3des esp-md5-hmac
!
crypto dynamic-map vpndyn 10
      set transform-set t1
!
crypto map vpnmap local-address Serial1/0
crypto map vpnmap 10 ipsec-isakmp dynamic vpndyn
!
interface Serial1/0
      ip address 172.17.0.1 255.255.255.252
      crypto map vpnmap
!
interface Ethernet0/0
      ip address 192.168.0.1 255.255.255.0
```

```
interface Tunnel1
      bandwidth 1000
      ip address 10.0.0.1 255.255.255.252
      ip mtu 1420
      delay 1000
      tunnel source Serial1/0
      tunnel destination 172.16.1.1
!
interface Tunnel2
      bandwidth 1000
      ip address 10.0.0.5 255.255.255.252
      ip mtu 1420
      delay 1000
      tunnel source Serial1/0
      tunnel destination 172.16.2.1
. . .
!
router eigrp 1
      network 10.0.0.0 0.0.0.255
      network 192.168.0.0
      no auto-summary
!
ip route 0.0.0.0 0.0.0.0 172.17.0.2
```


IPsec+GRE
Spoke Configuration

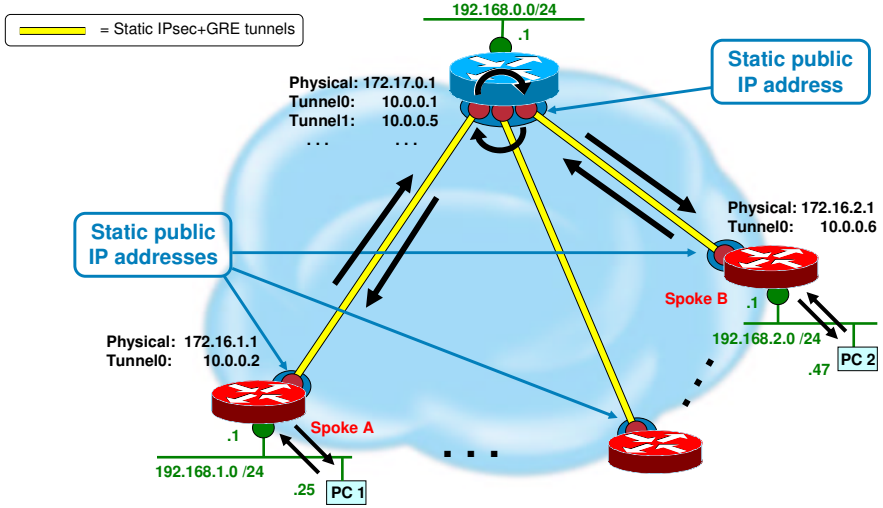
Cisco.com

```
crypto ca trustpoint msca-root
      enrollment terminal
      crl optional
      rsakeypair spoke1
crypto ca certificate chain msca-root
      certificate 236FD380000000000B4F
      certificate ca 1244325DE0369880465F977A18F61CA8
!
crypto isakmp policy 1
      encryption 3des
!
crypto ipsec transform-set t1 esp-3des esp-md5-hmac
!
crypto map vpnmap local-address Serial1/0
crypto map vpnmap 10 ipsec-isakmp
      set peer 172.17.0.1
      set transform-set t1
      match address 110
!
interface Serial1/0
      ip address 172.16.1.1 255.255.255.252
      crypto map vpnmap
```

```
interface Ethernet0/0
      ip address 192.168.1.1 255.255.255.0
!
interface Tunnel0
      bandwidth 1000
      ip address 10.0.0.2 255.255.255.252
      ip mtu 1420
      delay 1000
      tunnel source Serial1/0
      tunnel destination 172.17.0.1
!
router eigrp 1
      network 10.0.0.0 0.0.0.255
      network 192.168.1.0
      no auto-summary
!
ip route 0.0.0.0 0.0.0.0 172.16.1.2
!
access-list 110 –
   permit gre host 172.16.1.1 host 172.17.0.1
```


IPsec+GRE
Host to host ping

Cisco.com



IPsec+GRE
Routing Tables

Cisco.com

Hub

```
C     172.17.0.0/30 is directly connected, Serial1/0
C     10.0.0.0/30 is directly connected, Tunnel0
C     10.0.0.4/30 is directly connected, Tunnel1
      . . .
C    192.168.0.0/24 is directly connected, Ethernet0/0
D    192.168.1.0/24 [90/2841600] via 10.0.0.2, 00:12:30, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.0.0.6, 00:12:28, Tunnel1
      . . .
S*   0.0.0.0/0 [1/0] via 172.17.0.2
```

Spoke A

```
C     172.16.1.0/30 is directly connected, Serial1/0
C     10.0.0.0/30 is directly connected, Tunnel0
D     10.0.0.4/30 [90/3072000] via 10.0.0.1, 00:18:39, Tunnel0
      . . .
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:18:39, Tunnel0
C    192.168.1.0/24 is directly connected, Ethernet0/0
D    192.168.2.0/24 [90/3097600] via 10.0.0.1, 00:18:40, Tunnel0
      . . .
S*   0.0.0.0/0 [1/0] via 172.16.1.2
```

Spoke B

```
C     172.16.2.0/30 is directly connected, Serial1/0
D     10.0.0.0/30 [90/3072000] via 10.0.0.5, 00:21:53, Tunnel0
C     10.0.0.4/30 is directly connected, Tunnel0
      . . .
D    192.168.0.0/24 [90/2841600] via 10.0.0.5, 00:21:53, Tunnel0
D    192.168.1.0/24 [90/3097600] via 10.0.0.5, 00:21:54, Tunnel0
C    192.168.2.0/24 is directly connected, Ethernet0/0
      . . .
S*   0.0.0.0/0 [1/0] via 172.16.2.2
```

IPsec+GRE Scaling Issues:

Cisco.com

- Dynamic routing and IPsec peers
- Static tunnel destination
- Spoke-to-spoke traffic via hub
  - Example: 45Mb hub, (250) 256Kb spokes
    - Bandwidth per spoke: 144Kb (H-S) + 36Kb (S-S)
    - Aggregate bandwidth for VPN: 36Mb + 9Mb = 45Mb
- Hub configuration
  - 1 interface/spoke ➔ 250 spokes = 250 interfaces
  - 7 lines/spoke ➔ 250 spokes = 1750 lines
  - 4 IP addresses/spoke ➔ 250 spokes = 1000 addresses

Dynamic Multipoint VPN Major Features

Cisco.com

- Supports remote IPsec peers with dynamically assigned addresses
  - Cable, DSL, ISDN…
- Configuration reduction
  - Hub and spoke → hub router
- Dynamic spoke-spoke tunnels for scaling partial/full mesh VPNs

NHRP Overview

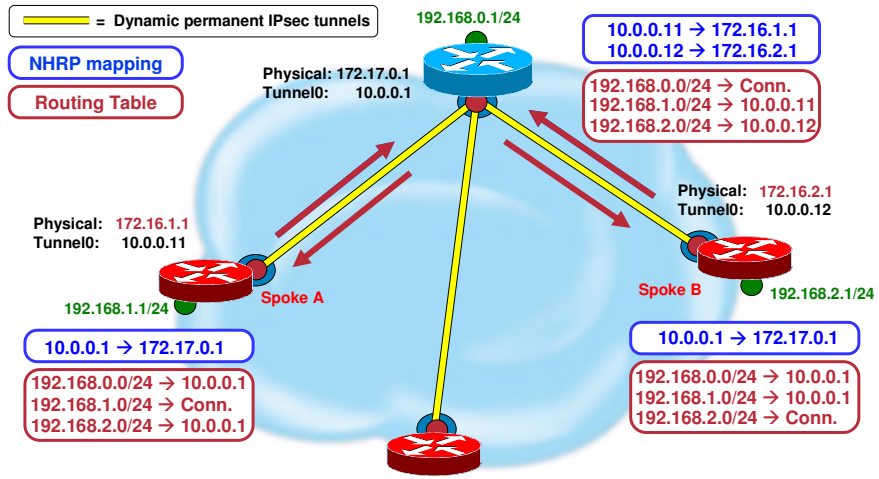
Cisco.com

- NBMA Next Hop Resolution Protocol
  - RFC2332

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

NHRP Registration Dynamically addressed spokes

Cisco.com



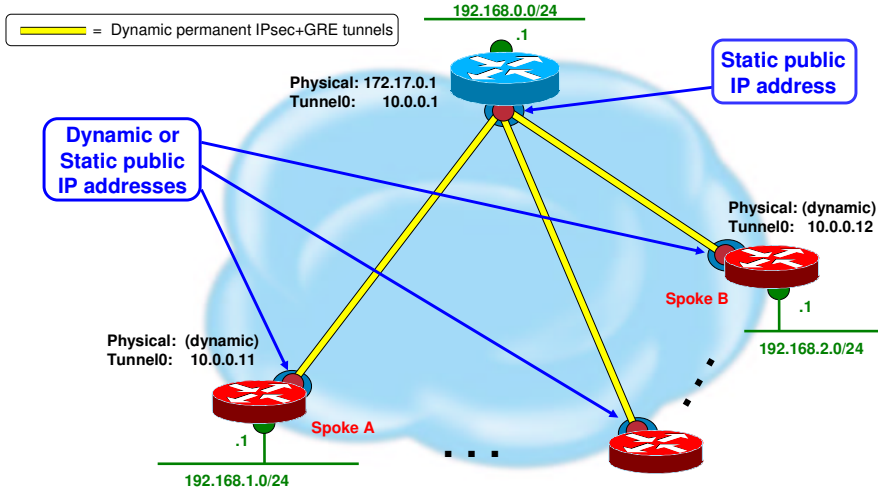
Dynamic Multipoint VPN Hub and Spoke

Cisco.com

- Features
  - Dynamically addressed spokes
  - Reduced and simplified hub configuration
- Changes
  - Convert hub to mGRE tunnel
  - Add NHRP commands to spokes
  - Use IPsec profiles on spokes (optional)

Dynamic Multipoint VPN Hub-and-Spoke

Cisco.com



What is an IPsec Profile?

Cisco.com

- IPsec profile contains:
  - Transform sets
  - PFS settings
  - Lifetimes
  - Acceptable identities
  - IKE profiles
- IPsec profiles are then applied to tunnel interfaces and/or good old crypto maps

Defining an IPSec Profile

Cisco.com

```
crypto ipsec transform-set AES256 esp-aes 256
 mode transport
crypto ipsec transform-set 3DES esp-3des
 mode transport
!
crypto ipsec profile IPSEC_PROFILE
 description Locally defined IPSec profile
 set transform-set AES256 3DES
 set pfs group2
 set isakmp-profile IKE_PROFILE
```

DMVPN Hub and Spoke Configuration Changes - Hub

Cisco.com

Crypto Profile (no peer or ACL)

/24 subnet

NHRP settings

Hub and Spoke Routing

mGRE Tunnel

Tunnel Protection

No ACL or Crypto map

```
crypto ipsec profile vpnprof
    set transform-set t1
!
interface Tunnel0
    bandwidth 1000
    ip address 10.0.0.1 255.255.255.0
    ip mtu 1416
    ip nhrp authentication test
    ip nhrp map multicast dynamic
    ip nhrp network-id 100000
    ip nhrp holdtime 360
    no ip split-horizon eigrp 1
    ip summary-address eigrp 1 192.168.0.0 255.255.0.0
    delay 1000
    tunnel source Serial1/0
    tunnel mode gre multipoint
    tunnel key 100000
    tunnel protection ipsec profile vpnprof
!
interface Serial1/0
    ip address 172.17.0.1 255.255.255.0
```


DMVPN Hub and Spoke Configuration Changes - Spoke (optional)

Cisco.com

Crypto Profile (no peer or ACL)

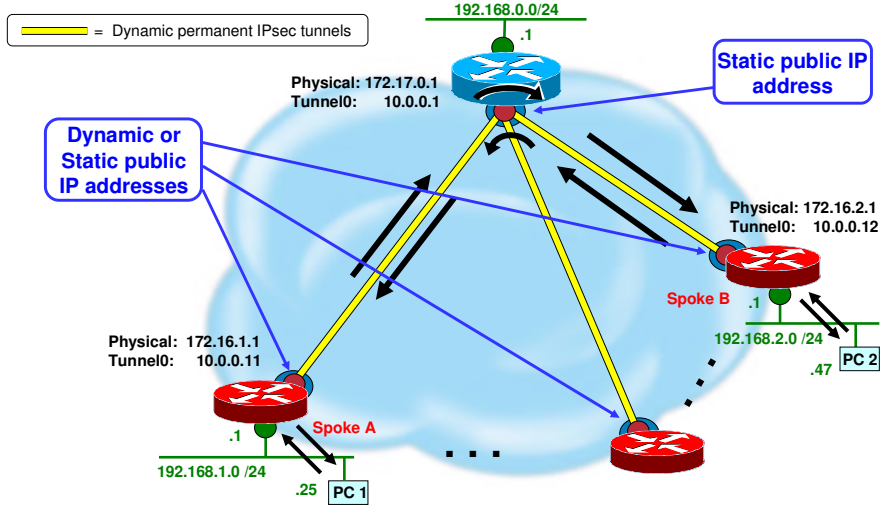
Tunnel Protection

No ACL or Crypto map

```
crypto ipsec profile vpnprof
    set transform-set t1
!
interface Tunnel0
    bandwidth 1000
    ip address 10.0.0.11 255.255.255.0
    ip mtu 1416
    ip nhrp authentication test
    ip nhrp map 10.0.0.1 172.17.0.1
    ip nhrp network-id 100000
    ip nhrp holdtime 600
    ip nhrp nhs 10.0.0.1
    delay 1000
    tunnel source Serial1/0
    tunnel destination 172.17.0.1
    tunnel key 100000
    tunnel protection ipsec profile vpnprof
!
Interface Serial1/0
    ip address negotiated
```


DMVPN Hub and Spoke Host to host ping

Cisco.com



DMVPN Hub and Spoke Routing Tables

Cisco.com

Hub

```
C    172.17.0.0/30 is directly connected, Serial1/0
C    10.0.0.0/24 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, Ethernet0/0
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 22:39:04, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.0.0.12, 22:39:10, Tunnel0
     . . .
S*   0.0.0.0/0 [1/0] via 172.17.0.2
D    192.168.0.0/16 is a summary, 00:04:13, Null0
```

Spoke A

```
C    172.16.1.0/30 is directly connected, Serial1/0
C    10.0.0.0/24 is directly connected, Tunnel0
C    192.168.1.0/24 is directly connected, Ethernet0/0
S*   0.0.0.0/0 is directly connected, Serial1/0
D    192.168.0.0/16 [90/2841600] via 10.0.0.1, 00:00:08, Tunnel0
```

Spoke B

```
C    172.16.2.0/30 is directly connected, Serial1/0
C    10.0.0.0/24 is directly connected, Tunnel0
C    192.168.2.0/24 is directly connected, Ethernet0/0
S*   0.0.0.0/0 is directly connected, Serial1/0
D    192.168.0.0/16 [90/2841600] via 10.0.0.1, 00:00:05, Tunnel0
```

DMVPN Hub and Spoke Dynamic Tables - Hub (Cont)

Cisco.com

Crypto Map

```
Hub1#show crypto map
Crypto Map "Tunnel0-head-0" 1 ipsec-isakmp
        Profile name: vpnprof
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N,  Transform sets={ t1, }
Crypto Map "Tunnel0-head-0" 2 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 172.16.1.1
        Extended IP access list
            access-list  permit gre host 172.17.0.1 host 172.16.1.1
        Current peer: 172.16.1.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N,  Transform sets={ t1, }
Crypto Map "Tunnel0-head-0" 4 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 172.16.2.1
        Extended IP access list
            access-list  permit gre host 172.17.0.1 host 172.16.2.1
        Current peer: 172.16.2.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N,  Transform sets={ t1, }
. . .
Interfaces using crypto map Tunnel0-head-0:
            Tunnel0
```


DMVPN Hub and Spoke Analysis: (Cont.)

Cisco.com

- Spoke-to-spoke traffic via hub
  - Example: 45 Mb hub, (250) 256Kb spokes
    - Bandwidth per spoke: 144Kb (H-S) + 36Kb (S-S)
    - Aggregate bandwidth for VPN: 36Mb + 9Mb = 45Mb
- Configuration
  - 1 interface ➔ 250 spokes = 1 interface
  - 15 lines ➔ 250 spokes = 15 lines
  - 1 IP address/spoke ➔ 250 spokes = 250 addresses

Dynamic Spoke-Spoke Tunnels

Cisco.com

- mGRE/NHRP+IPsec configuration
  - On both hub and spokes
  - ISAKMP authentication information
    - Certificates, wildcard pre-shared keys
- Spoke-spoke data traffic direct
  - Reduced load on hub
  - Reduced latency
    - Single IPsec encrypt/decrypt

Dynamic Multipoint VPN Routing Protocol Configuration

Cisco.com

- EIGRP
  - no ip split-horizon eigrp <as>
  - no ip next-hop-self eigrp <as> ←Cisco IOS: 12.3(2))
  - no auto-summary
- OSPF
  - ip ospf network broadcast
  - ip ospf priority ($2_{(hub)}|0_{(spoke)}$)
- BGP
  - Hub is route reflector
- RIP
  - no ip split-horizon
  - no auto-summary

New IP Routing/Forwarding Model

Cisco.com

- **Regular IP networks**

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

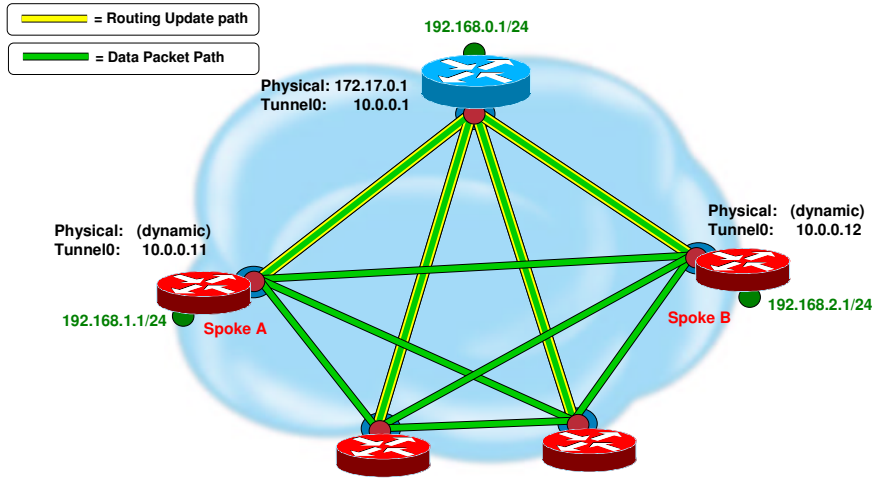
- **New DMVPN IP networks**

  IP routing updates traverse hub and spoke VPN links only

  IP data packets traverse both hub and spoke and direct VPN links between spokes

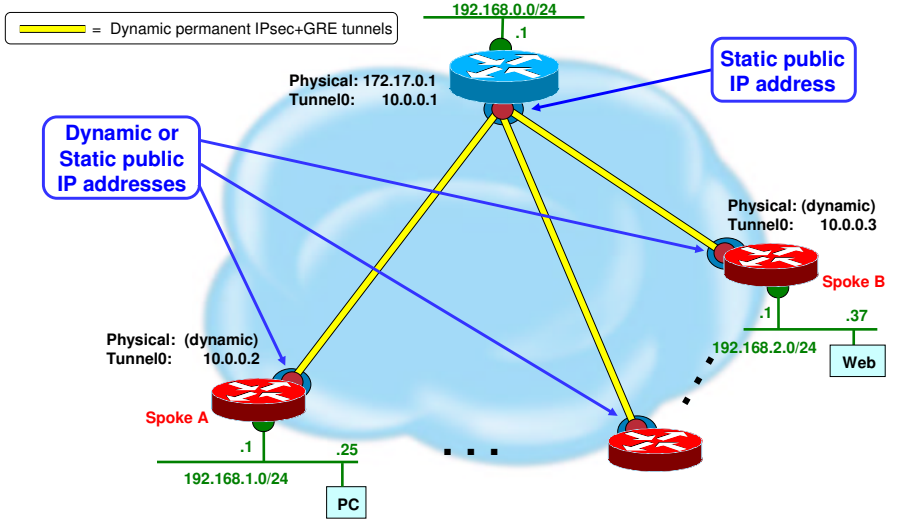
IP Routing Updates vs. Data packet forwarding

Cisco.com



Dynamic Multipoint VPN - Single Hub

Cisco.com



DMVPN Configuration Hub - Changes

Cisco.com

Re-advertise routes with original IP next-hop. No summary.

```
interface Tunnel0
     bandwidth 1000
     ip address 10.0.0.1 255.255.255.0
     ip mtu 1416
     ip nhrp authentication test
     ip nhrp map multicast dynamic
     ip nhrp network-id 100000
     ip nhrp holdtime 360
     no ip spit-horizon eigrp 1
     no ip next-hop-self eigrp 1
     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 0.0.0.255
     no auto-summary
```

DMVPN Configuration
Spoke - Changes

Cisco.com

NHRP static multicast map →

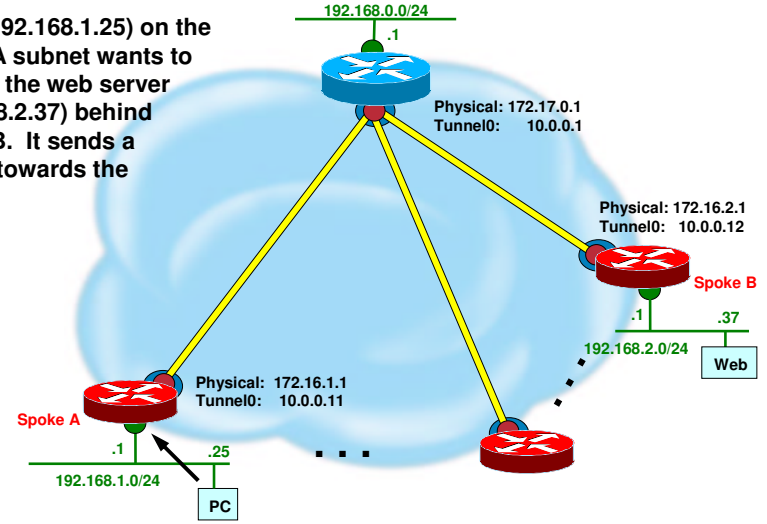
mGRE Tunnel →

```
interface Tunnel0
     bandwidth 1000
     ip address 10.0.0.11 255.255.255.0
     ip mtu 1416
     ip nhrp authentication test
     ip nhrp map multicast 172.17.0.1
     ip nhrp map 10.0.0.1 172.17.0.1
     ip nhrp network-id 100000
     ip nhrp holdtime 360
     ip nhrp nhs 10.0.0.1
     delay 1000
     tunnel source Serial1/0
     tunnel mode gre multipoint
     tunnel key 100000
     tunnel protection ipsec profile vpnprof
!
router eigrp 1
     network 10.0.0.0 0.0.0.255
     network 192.168.1.0 0.0.0.255
     no auto-summary
```


Dynamic Multipoint VPN—Example

Cisco.com

1. A PC (192.168.1.25) on the spoke A subnet wants to contact the web server (192.168.2.37) behind spoke B. It sends a packet towards the server.

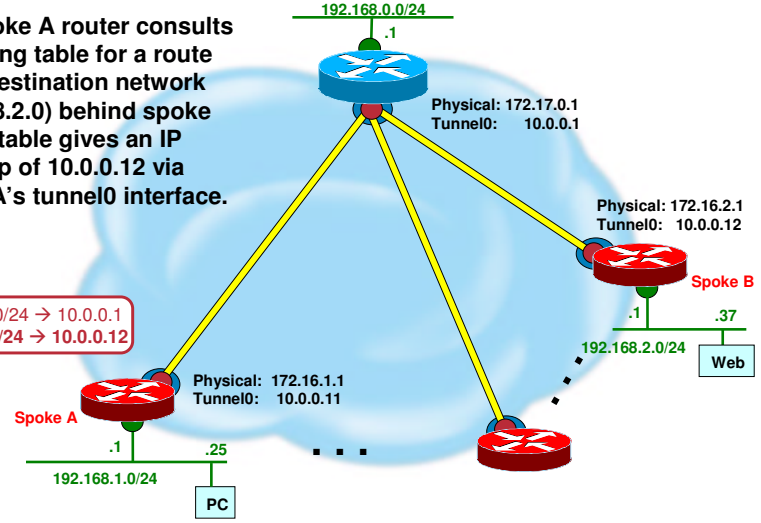


Dynamic Multipoint VPN - Example

Cisco.com

2. The spoke A router consults its routing table for a route to the destination network (192.168.2.0) behind spoke B. The table gives an IP next-hop of 10.0.0.12 via Spoke A's tunnel0 interface.

192.168.0.0/24 → 10.0.0.1
192.168.2.0/24 → 10.0.0.12

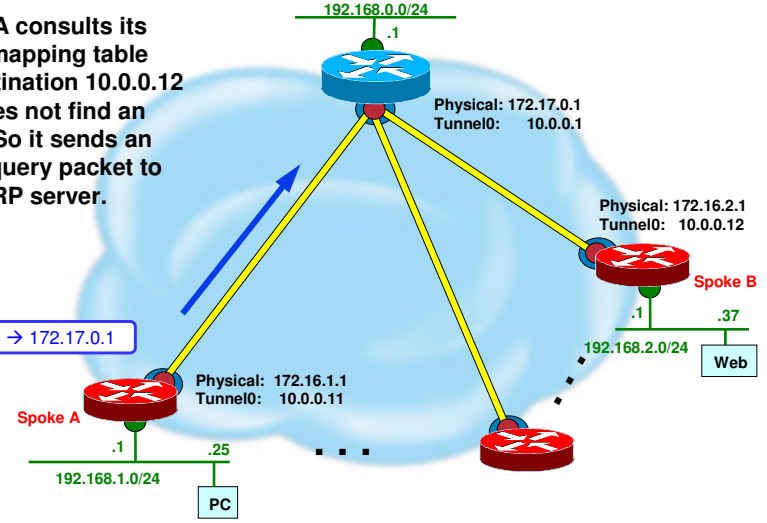


Dynamic Multipoint VPN - Example

Cisco.com

3. Spoke A consults its NHRP mapping table for destination 10.0.0.12 and does not find an entry. So it sends an NHRP query packet to the NHRP server.

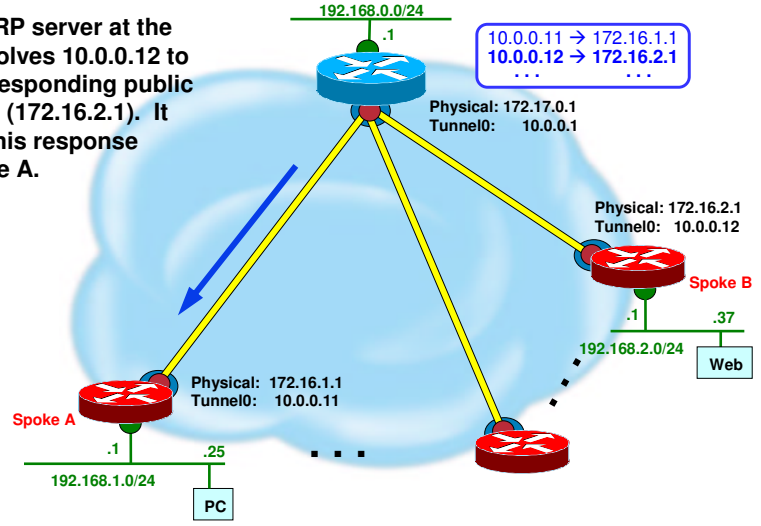
10.0.0.1 → 172.17.0.1



Dynamic Multipoint VPN - Example

Cisco.com

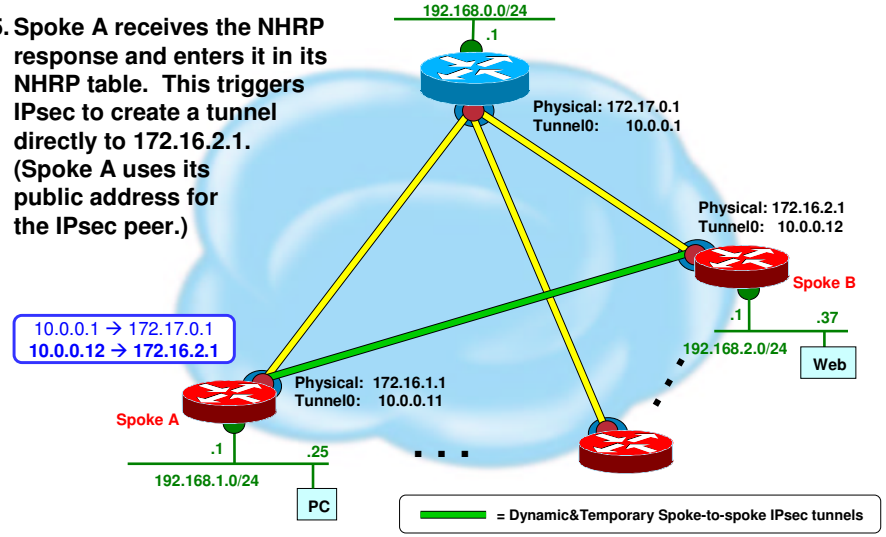
4. The NHRP server at the hub resolves 10.0.0.12 to the corresponding public address (172.16.2.1). It sends this response to Spoke A.



Dynamic Multipoint VPN - Example

Cisco.com

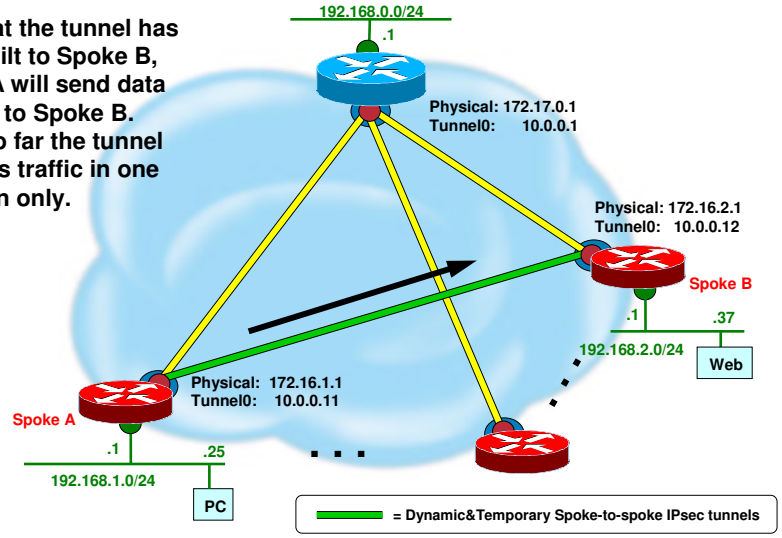
5. Spoke A receives the NHRP response and enters it in its NHRP table. This triggers IPsec to create a tunnel directly to 172.16.2.1. (Spoke A uses its public address for the IPsec peer.)



Dynamic Multipoint VPN - Example

Cisco.com

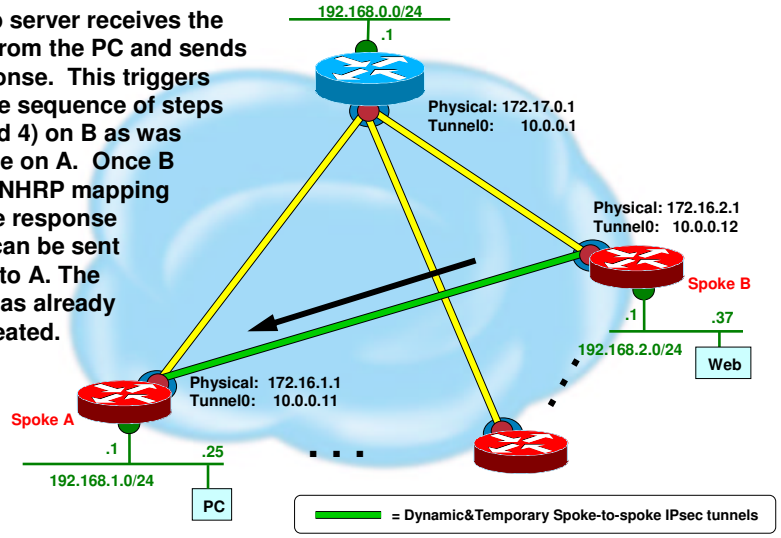
6. Now that the tunnel has been built to Spoke B, Spoke A will send data packets to Spoke B. Note: So far the tunnel can pass traffic in one direction only.



Dynamic Multipoint VPN - Example

Cisco.com

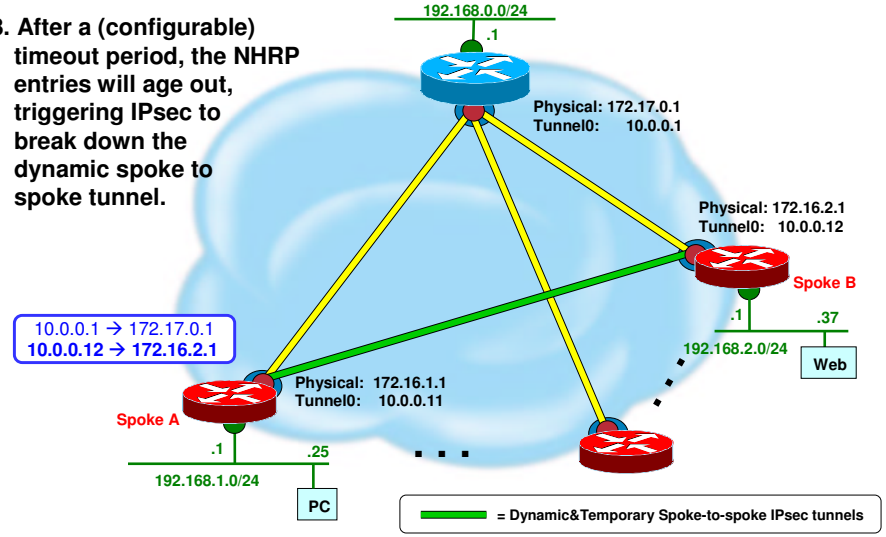
7. The web server receives the packet from the PC and sends its response. This triggers the same sequence of steps (2, 3, and 4) on B as was just done on A. Once B has the NHRP mapping for A the response packet can be sent directly to A. The tunnel has already been created.



Dynamic Multipoint VPN - Example

Cisco.com

8. After a (configurable) timeout period, the NHRP entries will age out, triggering IPsec to break down the dynamic spoke to spoke tunnel.



DMVPN Routing Tables

Cisco.com

Hub

```
C   172.17.0.0/30 is directly connected, Serial1/0
C   10.0.0.0/24 is directly connected, Tunnel0
C   192.168.0.0/24 is directly connected, Ethernet0/0
D   192.168.1.0/24 [90/2841600] via 10.0.0.11, 22:39:04, Tunnel0
D   192.168.2.0/24 [90/2841600] via 10.0.0.12, 22:39:10, Tunnel0
    . . .
S*  0.0.0.0/0 [1/0] via 172.17.0.2
```

Spoke A

```
C   172.16.1.0/30 is directly connected, Serial1/0
C   10.0.0.0/24 is directly connected, Tunnel0
D   192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:03:58, Tunnel0
C   192.168.1.0/24 is directly connected, Ethernet0/0
D   192.168.2.0/24 [90/3097600] via 10.0.0.12, 00:02:02, Tunnel0
    . . .
S*  0.0.0.0/0 is directly connected, Serial1/0
```

Spoke B

```
C   172.16.2.0/30 is directly connected, Serial1/0
C   10.0.0.0/24 is directly connected, Tunnel0
D   192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:03:43, Tunnel0
D   192.168.1.0/24 [90/3097600] via 10.0.0.11, 00:03:43, Tunnel0
C   192.168.2.0/24 is directly connected, Ethernet0/0
    . . .
S*  0.0.0.0/0 is directly connected, Serial1/0
```


DMVPN Single Hub Analysis:

Cisco.com

- GRE tunnels, IPsec peers and Crypto maps
  - Dynamic on hub and spoke
- Add spoke routers without hub or other spoke router changes
  - NHRP and dynamic routing propagate information
- Spoke to spoke traffic doesn't affect hub
  - Example: 45 Mb hub, (250) 256Kb spokes
    - Bandwidth per spoke: 180Kb (H-S) + 76Kb (S-S)
    - Aggregate bandwidth for VPN = 45Mb + 19Mb = 64Mb

DMVPN Dual Hub Examples

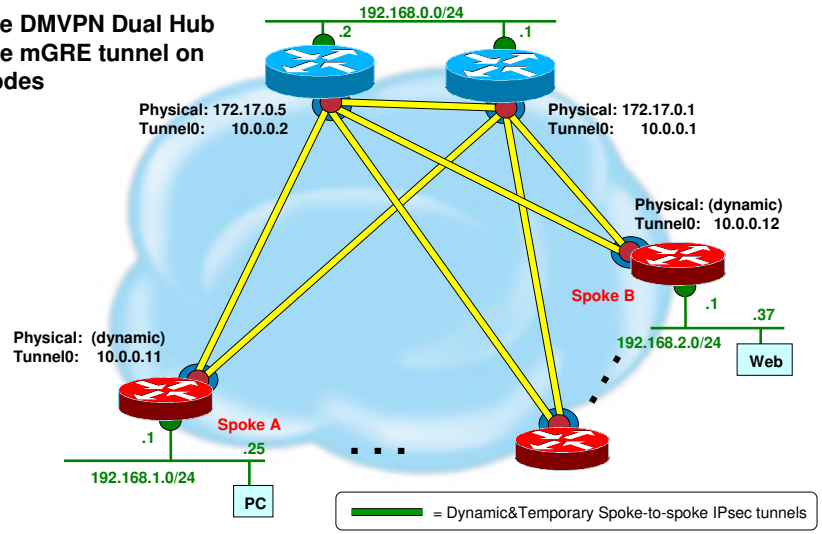
Cisco.com

- Single DMVPN dual hub - example 1
  - Easier to configure
  - Less control of routing and forwarding
  - Spoke-spoke tunnels anywhere
- Dual DMVPN dual hub - example 2

DMVPN Dual Hub - Example 1

Cisco.com

Single DMVPN Dual Hub
Single mGRE tunnel on
all nodes



DMVPN Dual Hub - Example 1 Spoke

Cisco.com

Hub1 NHRP mappings

Hub2 NHRP mappings

OSPF broadcast Force non-DR

OSPF Routing

```
interface Tunnel0
     bandwidth 1000
     ip address 10.0.0.11 255.255.255.0
     ip mtu 1416
     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 10.0.0.1 172.17.0.5
     ip nhrp network-id 100000
     ip nhrp holdtime 360
     ip nhrp nhs 10.0.0.1
     ip nhrp nhs 10.0.0.2
     ip ospf network broadcast
     ip ospf priority 0
     delay 1000
     tunnel source Serial1/0
     tunnel mode gre multipoint
     tunnel key 100000
     tunnel protection ipsec profile vpnprof
!
router ospf 1
     network 10.0.0.0 0.0.0.255 area 1
     network 192.168.1.0 0.0.0.255 area 0
```


DMVPN Dual Hub Examples

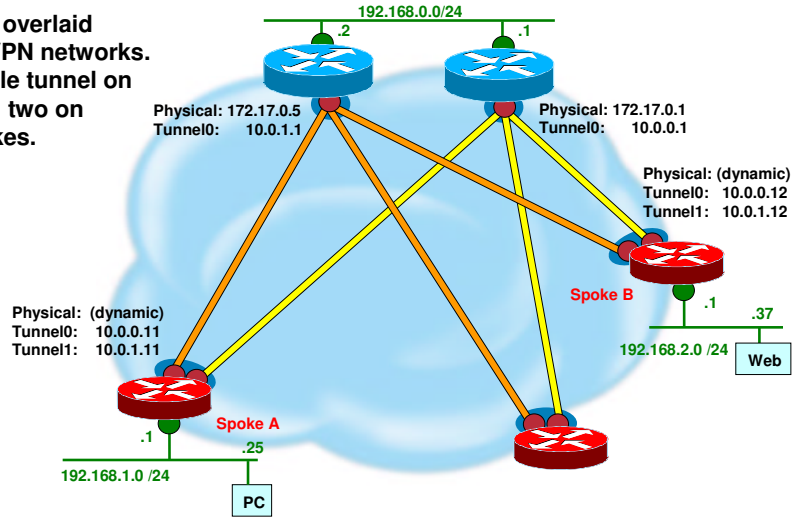
Cisco.com

- Single DMVPN dual hub - example 1
- Dual DMVPN dual hub - example 2
  - Little harder to configure
  - More control of routing and forwarding
  - Spoke-spoke tunnels only within same DMVPN

Dual DMVPN Dual Hub

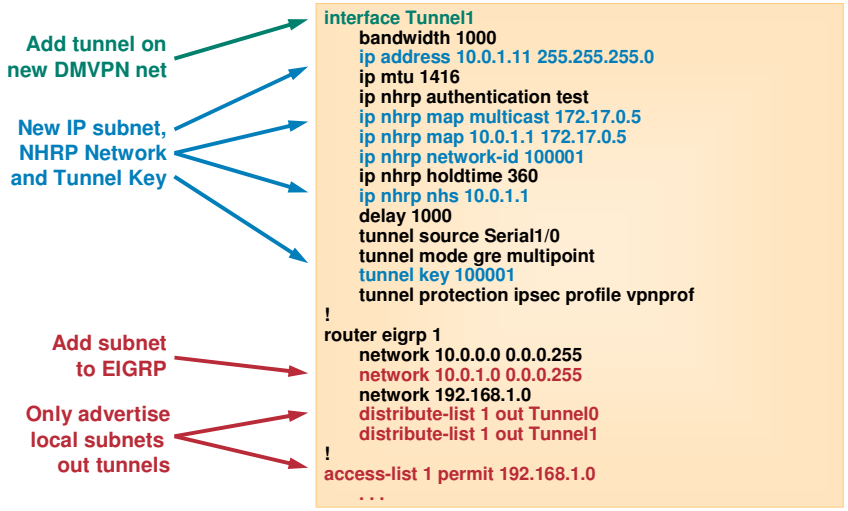
Cisco.com

Two overlaid DMVPN networks. Single tunnel on Hub, two on spokes.



DMVPN Dual Hub - Example 2 Spoke - Changes

Cisco.com



DMVPN Dual Hub Analysis:

Cisco.com

- Network design
  - Dual hub and spoke (redundant DMVPN) - routing
  - Dynamic mesh - data traffic
- GRE tunnels, IPsec peers and Crypto maps
  - Dynamic on hub and spoke
- Add spoke routers without hub or other spoke router changes
  - NHRP and dynamic routing propagate information

DMVPN Dual Hub Analysis: Dynamic Routing

Cisco.com

- Hub redundancy
  - Must lose both before spoke isolated
  - Can distribute spokes across many hubs
- Load balancing between hub routers
  - Configure routing to prefer one hub
    - EIGRP
      - interface cost, ‘distribute-list…’, ‘offset-list…’

DMVPN Features in Summary

Cisco.com

- DMVPN scales IPsec VPNs by
  - Supporting dynamically addressed spokes, IP multicast and IGP routing protocols
  - Eliminating the hassle of adding a spoke
  - Drastically reducing configuration sizes
  - Enabling dynamic spoke-spoke tunnels
- Scalability with less administration!

Cisco IOS Code and Platform Support

Cisco.com

- DMVPN hub-and-spoke

  12.2(13)T (November 2002)

- DMVPN dynamic spoke-spoke

  12.3(2)

- Platforms

  7204/6, 36xx, 37xx, 26xx, 17xx

  830 support in 12.2(13)ZH1, 12.3(1)T

Agenda

Cisco.com

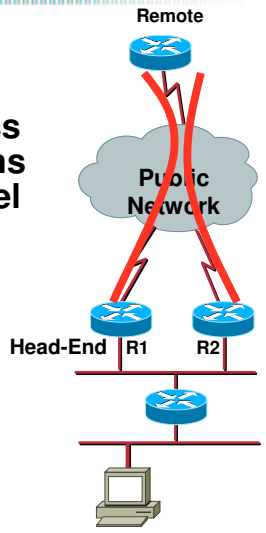
- Introduction
- Topologies
- Resiliency and performance
- Scalable authentication
- Q&A

Resiliency & performance

Adding Resiliency to VPN

Cisco.com

- In order to prevent packet loss over the VPN adding two paths and selecting the active tunnel by:
  - Relying on tunnel mechanism *(keepalives)*
  - Using routing protocol *(EIGRP, OSPF)*



Tuning EIGRP for Faster Link Status

- **EIGRP can be tuned to detect a link failure and converge within 2 seconds** (instead of the default 180 seconds):

```
interface tunnel 0
   ip hello-interval eigrp process-id 1
   ip hold-time eigrp process-id 2
```

NB: be sure to understand the CPU load on the central site and on the utilized bandwidth

Tuning OSPF for Faster Link Status

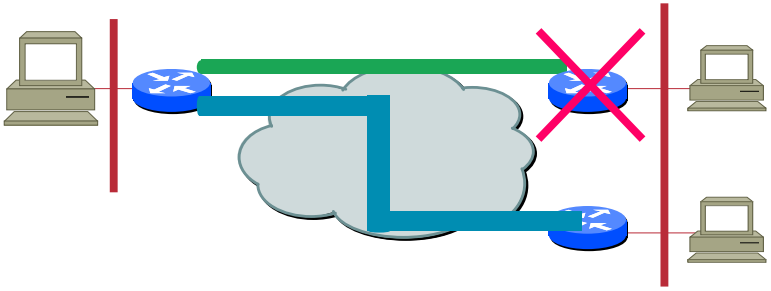
- **OSPF can be tuned to detect a link failure within 2 seconds** (instead of the default 40 seconds):

```
interface Tunnel0
 ip ospf hello-interval 1
 ip ospf dead-interval 2
```

NB: be sure to understand the CPU load on the central site and on the used bandwidth

IPsec and Keepalives

Specific configuration of IPsec/IKE peer to allow resilience/load balancing



Plain IKE can detect failed peer during Main Mode
IKE Keep Alive detects failed peer at any time

www.ietf.org/internet-drafts/draft-ietf-ipsec-dpd-03.txt

Catalyst 6500 / 7600 Router IPsec VPN Services Module Overview

Fabric Enabled

Performance

1.9 Gbps 3DES (500+ byte packets)
1.6 Gbps 3DES (300 byte packets)
Up to 8,000 tunnels
Up to 60 tunnels/second

Ordering Information

Part Number: WS-SVC-IPSEC-1
Requires IOS 12.2(9)YO2

Feature Highlights

Robust IOS site-to-site VPN services
DES, 3DES hardware acceleration
X.509 and shared secret authentication
Diverse PKI support with auto-enrollment
IKE, XAuth, Mode-Config, IPsec
GRE/IPsec with multi-protocol support
Routing over IPsec
RIP1/2, OSPF, EIGRP, BGP4
HSRP support

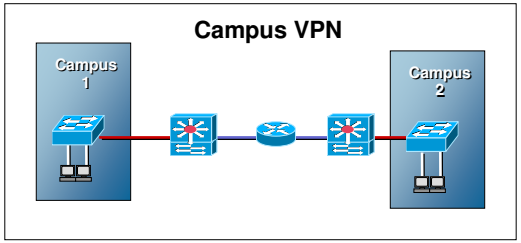
Management

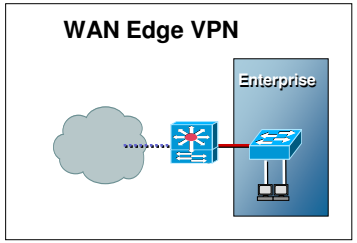
Embedded web-based GUI (VDM)
Router MC and IPSC coming soon!
SNMP with IPsec MIB support
SSH and Kerberized telnet
RADIUS/TACACS+

VPNSM

Current Deployment Scenarios for IPsec VPN Services Module

Cisco.com





Deployment	Description
Campus	Secure LAN traffic between switches, floors, building and specific sensitive network applications such as iSCSI
WAN Edge	Provide VPN termination services on the WAN aggregator router
Link-Layer Encryption Replacement	Replace old ATM and other link-layer encryption with modern a IPSec layer 3 VPN solution
Extranet	Enables partner networks to securely connect and transfer large amounts of data

Recent VPNSM Enhancements

Cisco.com

Recent Features in 12.2(14)SY

- Easy VPN Remote Access IPSec (8k Hardware or Software Clients)
- Integration with FWSM, NAM-1, NAM-2, IDSM-2 in same chassis
- FlexWAN PA Support
- Inter-Chassis IPSec Stateful Fail-Over
- Up to 10 VPNSMs per platform (14 Gbps 3DES! or 5 Mpps)
- On-board GRE Acceleration
- DPD, HSRP+RRI and IPSec NAT Transparency
- On-board LLQ (2-Queue) QoS (ideal for VoIP Applications)
- Look-Ahead fragmentation support
- PKI Enhancements: 2-Tier Chaining, Manual Enrollment and Subject Name Modification

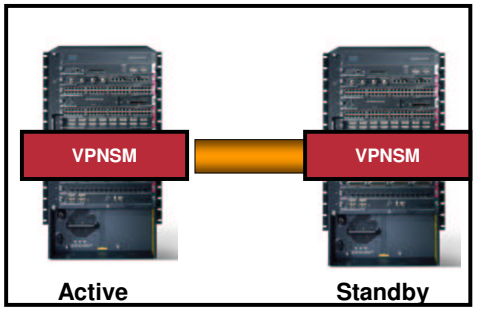
Management

- VMS 2.2 RouterMC 1.2.1 support today
- Router MC 1.3, ISC 3.1 and SolSoft support coming soon!
- SNMP with IPSec MIB support
- SSH and Kerberized telnet
- RADIUS/TACACS+

Inter-Chassis IPsec Stateful Fail-Over

Cisco.com

- Dedicated IPSec tunnel between Active and Standby using State Synchronization Protocol (SSP) Supports IPSec site-to-site tunnels with GRE
- Must use shared secret auth.



	Spokes	Bi-directional Traffic (Mbps)	Bi-directional Traffic (kPPS)	CPU Utilization %	Failover Time
7200 NPE-400 (VAM1)	1040	79.6	26	77	1-2 sec
Catalyst 6500 (VPNSM)	1040	1029.3	488.6	N/A	1-3 sec

Scalability Performance Comparison

Cisco.com

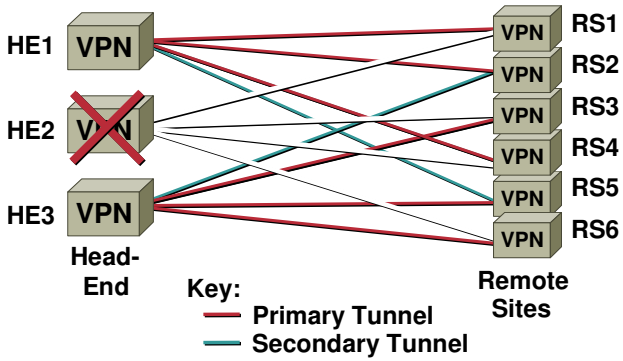
- EIGRP and OSPF relatively equivalent
- DPD/RRI improves throughput roughly 10+%

	GRE/RP (Spokes)	GRE/RP (Mbps)	DPD/RRI (Spokes)	DPD/RRI (Mbps)	Stopping Reason
3745 (AIM-II)	60	17.5	120	22.5	CPU
7200 NPE-400 (VAM1)	240	58.6	1040	72	CPU
7200 NPE-G1 (2xVAM1)	500	60.4	1040	107	CPU
7200 NPE-G1 (2xVAM2)	N/A	N/A	1040	109	CPU
Catalyst 6500 (VPNSM)	500	924	1040	1029	VPNSM HW buffers

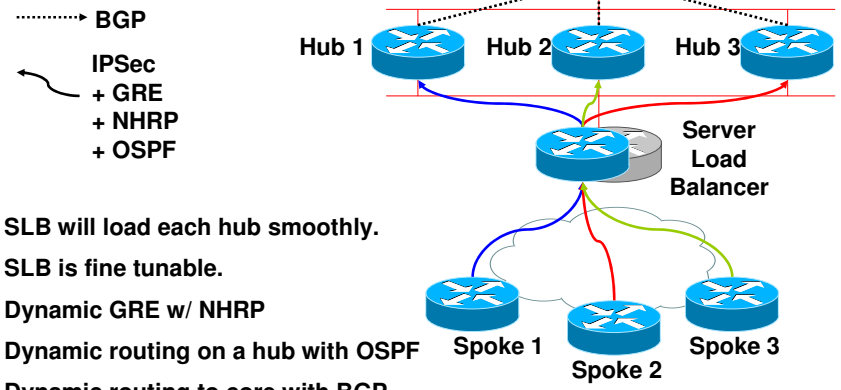
Note: Lab testing best effort results done with small packet size (VoIP traffic)

Load Dispersion on Failure

- When a head-end tunnel termination device fails, its load should be equally shared among the other remaining head-end devices
  - Aids in the resiliency and scalability of the head-end
  - Adds to the configuration complexity

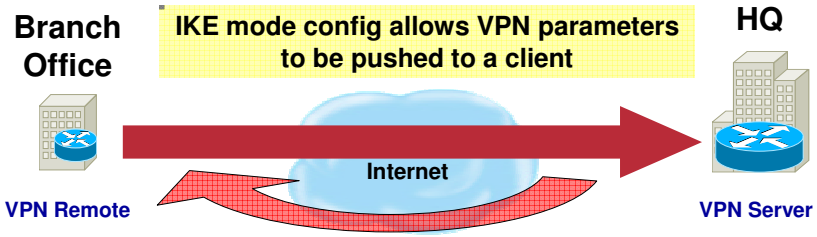


Advance Load Balancing Design



- SLB will load each hub smoothly.
- SLB is fine tunable.
- Dynamic GRE w/ NHRP
- Dynamic routing on a hub with OSPF
- Dynamic routing to core with BGP

Scalability with Cisco Easy VPN



Dynamically updated:

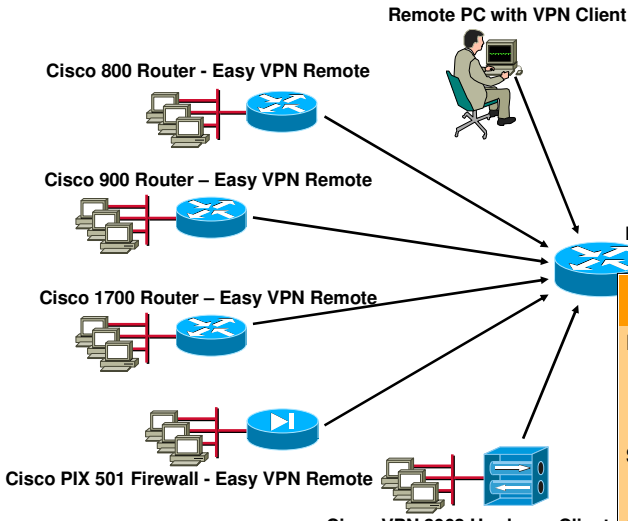
- Central services and security policy
- Offload VPN function from local devices
- Client and Network Extension mode

- Internal IP Address
- Internal Network Mask
- Internal DNS Server
- Internal WINS Server
- Split tunneling
- IPsec Transforms

Centralized control:

- Configuration and security policy pushed at the time of the VPN tunnel establishment

Easy VPN Remote platforms



CISCO Easy VPN Servers

Routers:
- 83x/1700 Series
- 2600 Series
- 3600 Series
- 7100/7200 Series

Security Appliances:
- PIX Firewall Series v6.x
- CVPN 3000 Series v3.x

Cat6K VPNSM [12.2(14)SY]

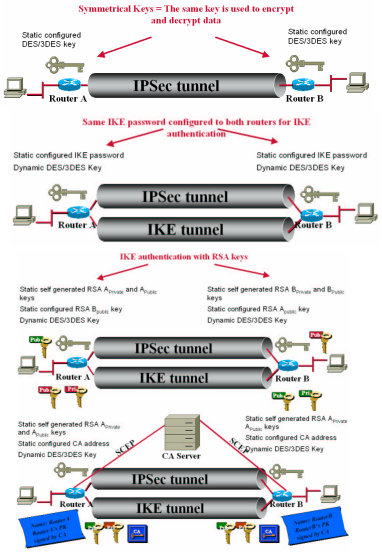
Agenda

- Introduction
- Topologies
- Resiliency and performance
- Scalable authentication
- Q&A

Scalable Authentication

IPsec node authentication types

- IPsec tunnel
  - Static encryption keys
  - IKE with pre-shared secrets
  - IKE with manual RSA keys
  - IKE with certs = PKI



PKI and Cisco

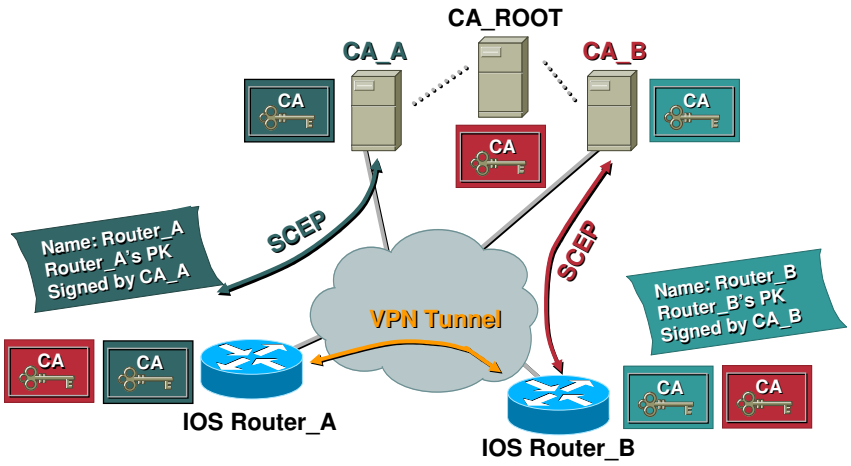
- Build open PKI aligned with PKIX

  www.ietf.org/internet-drafts/draft-nourse-scep-08.txt
- Support of leading CA vendors
  - ✓ Verisign summer 98
  - ✓ Entrust summer 98
  - ✓ Netscape CMS 3.1 end 99
  - ✓ Microsoft Windows 2000 February 00 *requires Windows Resource Kit*
  - – Baltimore Technologies 00
  - – RSA Keon, XCert,…

PKI Feature: 2-Tiered Cert Chaining

Cisco.com

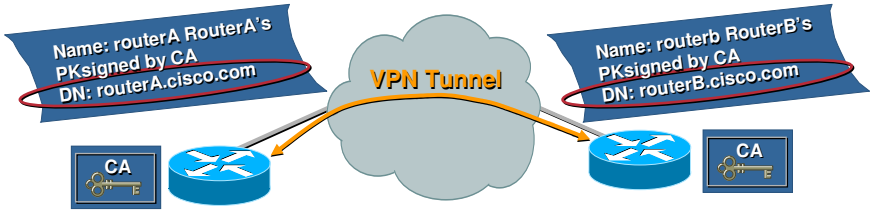
12.1(5)T 2-Tiered Certificate Chaining



PKI Feature: DN Crypto Maps

Cisco.com

12.2(4)T Distinguished Name Crypto Maps



- Customer wants to restrict access to selected encrypted interfaces to peers with specific certificates, and in particular, certificates with particular DNs

PKI Feature: Attribute-Based Access Control

Cisco.com

12.2(15)T Certificate Security Attribute Based Access Control

- Allow applications within IOS to perform authorization based on the fields in the certificate. In this way from a user's view a certificate is used for both authentication and authorization.

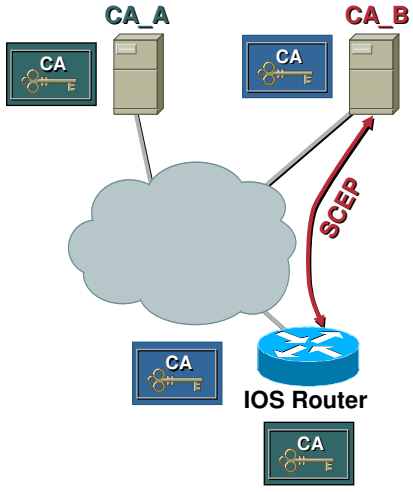
```
crypto ca certificate map Group 10
       issuer-name co Cisco Systems
       subject-name co DIAL
!
crypto ca certificate map Group 20
       issuer-name co Cisco Systems
        subject-name co WAN
!
crypto ca trustpoint Access2
       match certificate Group
```

subject-name
issuer-name
unstructured-subject-name
alt-subject-name
name
valid-start
expires-on

Eq - equal
Ne - not equal
Co - contains
Nc - does not contain
Lt - less than
Ge - greater than or equal

PKI Feature: Certificate Auto-Enrollment

Cisco.com




```
crypto ca trustpoint lab.cisco.com
enrollment mode ra
enrollment url
http://CA1/certsrv/mscep/mscep.dll
password 7 104D000A0618
subject-name OU=Lab1
auto-enroll 90 regenerate
```

At start and when certificate lifetime % expires router starts SCEP to re-enroll aautomatically

12.2(8)T Cert Auto-Enrollment

PKI Feature: New Certificate Enrollment modes

Cisco.com

12.2(12)T TFTP, Cut&Paste Cert Enrollment

- Send enrollment request via tftp
- Retrieve CA certificate via tftp
- Retrieve router's certificate via tftp
- Cut-and-Paste enrollment

PKI Feature: External Certificate Storage

Cisco.com

12.2(15)T Exporting/Importing RSA Keys Support

- Enables export of Key-Pairs from Router
- Can be Protected by Passphrase
- Initial support for SSH format, probable PKCS#12 support to follow.
- Mark Keys as exportable during Generation
- Keys can be marked as Un-Exportable
- Can use any mechanism supported by IOS FS, TFTP, SCP, FTP, NVRAM, etc

PKI Feature: Online Certificate Status Protocol

Cisco.com

12.3(2)T OCSP Support

- Cisco IOS Online Certificate Status Protocol (OCSP)
  - Alternative to certificate revocation lists (CRLs) for checking certificate status
  - Unlike CRLs, which provide only periodic certificate status, OCSP can provide timely information regarding the status of a certificate
  - Cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gt_ocsp.htm

PKI Feature: IOS Built-In Certificate Server

Cisco.com

12.3(4)T - IOS build-in Certificate Server

- Available on all platforms in 12.3(4)T
- CS for the easy cert based VPN deployment
- SCEP is used to talk to clients
- Can be in automatic mode (always grant a certificate to all requests) or manual
- Storage of certs & crl is either flash, or (T)FTP server

Configuring IOS Certificate Server (IOS CS)

Cisco.com

```
crypto pki server MY_SCEP
 database level names
 database url disk0:
 issuer-name cn=eric vyncke,o=cisco,c=be
 grant auto
% This will cause all certificate requests to be
automatically granted.

Are you sure you want to do this? [yes/no]: yes
 cdp-url http://192.168.0.3/disk0/MY_SCEP.crl
 no shutdown
```


Configuring IOS CS (cont.)

Cisco.com

NTP or clock must be configured
HTTP server must be enabled
If CRL Distribution Point is the router, direct flash access must be enabled

```
ntp server 192.168.0.47
ip http server
ip http path disk0:
```

Storage media contains:

```
Directory of disk0:/

    6  -rw-          53   Jun 30 2003 06:38:34  1.cnm
    7  -rw-           2   Jun 30 2003 10:46:28  MY_SCEP.ser
    8  -rw-         294   Jun 30 2003 07:29:48  MY_SCEP.crl
    9  -rw-          51   Jun 30 2003 06:44:56  2.cnm
```


IOS CS - example manual grant

Cisco.com

```
#crypto pki server MY_SCEP info requests
Enrollment Request Database:
ReqID  State      Fingerprint                      SubjectName
--------------------------------------------------------------------
10     pending    E5F7D1B235542F9EC7868D9512352CB4 serialNumber=C10ADCA9+ipaddress=
192.168.0.11+hostname=c2651b.cisco.com,cn=2651c,o=cisco,c=be

#crypto pki server MY_SCEP grant 10
```


Agenda

Cisco.com

- Introduction
- Topologies
- Resiliency and performance
- Scalable authentication
- Q&A

Questions?

Thank you!

Deploying Large IPsec VPNs

fmajstor@cisco.com

NETWORKERS 2003

THE POWER TO TRANSFORM BUSINESS. now.

Please Complete Your Evaluation Form

Session SEC-2001

CISCO SYSTEMS

CISCO SYSTEMS