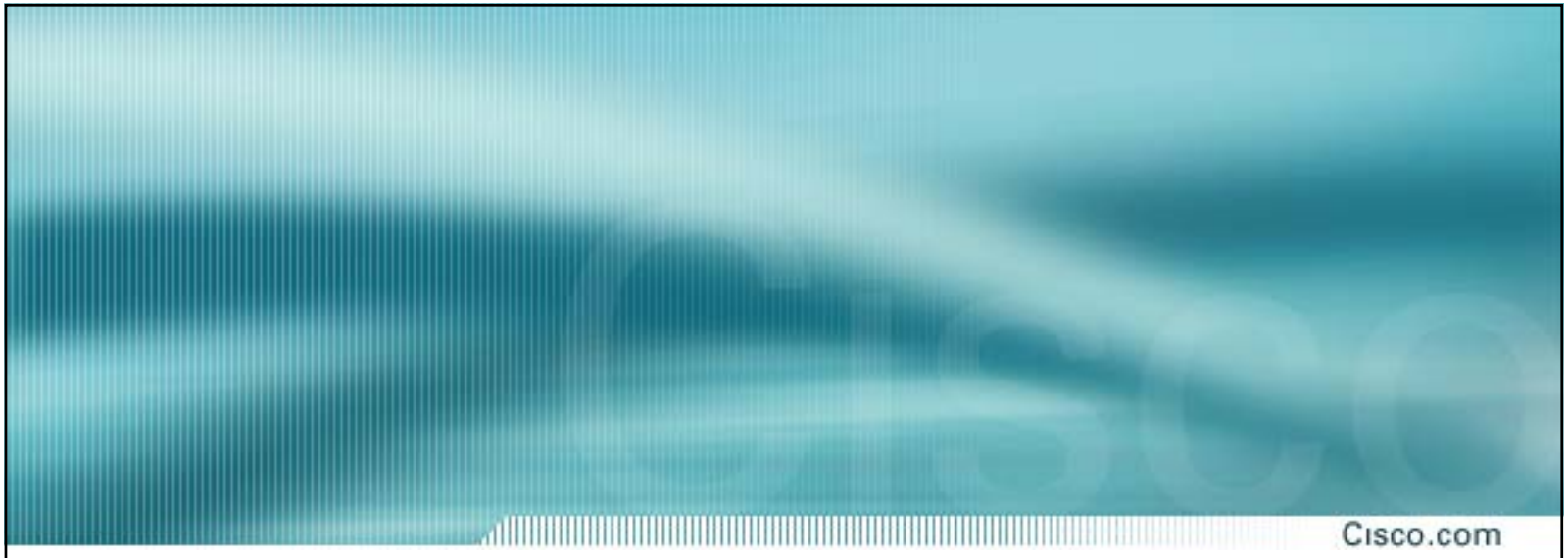


Dynamic Multipoint VPN

James Wu CCIE#5514

Technical Consultant

Asia Pac SP Operation

jawu@cisco.com

IPSec-based VPNs – Current Deployment Options

- **Hub and Spoke**
  - + All traffic must go via hub
  - + Easy to deploy
  - × Two encrypts/decrypts
  - × Can result in wasted bandwidth and hub resources
  - × Can result in unwieldy hub configuration files
- **Full Mesh**
  - + Direct spoke to spoke tunnels
  - × Smaller spoke CPE can't support large numbers of connections (big configurations and lots of resources)
  - × Adding a node = lots of provisioning
  - × Basically a scaling and support headache, therefore most production networks use hub and spoke.

What's Needed?

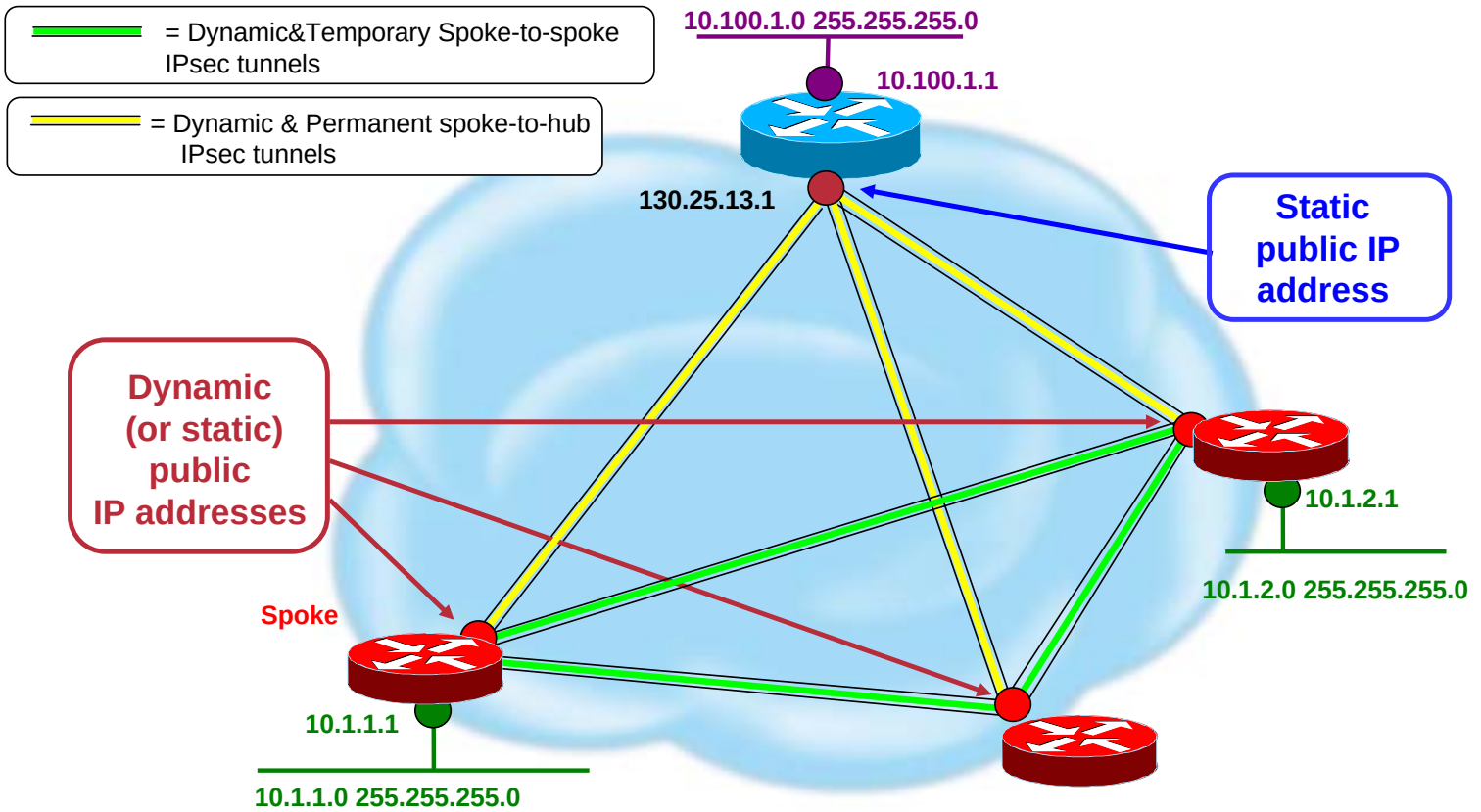
Create the spoke to spoke tunnels dynamically based on traffic requirements!

Advantages:

- ✓**Dynamic mesh: number of active tunnels is much lower on each spoke.**
- ✓**Configuration scales better: no need for static definitions for each spoke in the hub configuration.**
- ✓**Easy to add a node: no need to configure the new spoke on all the other nodes.**

✓***This is the basis of Cisco's Dynamic Multipoint VPN***

Dynamic Multipoint VPN - DMVPN



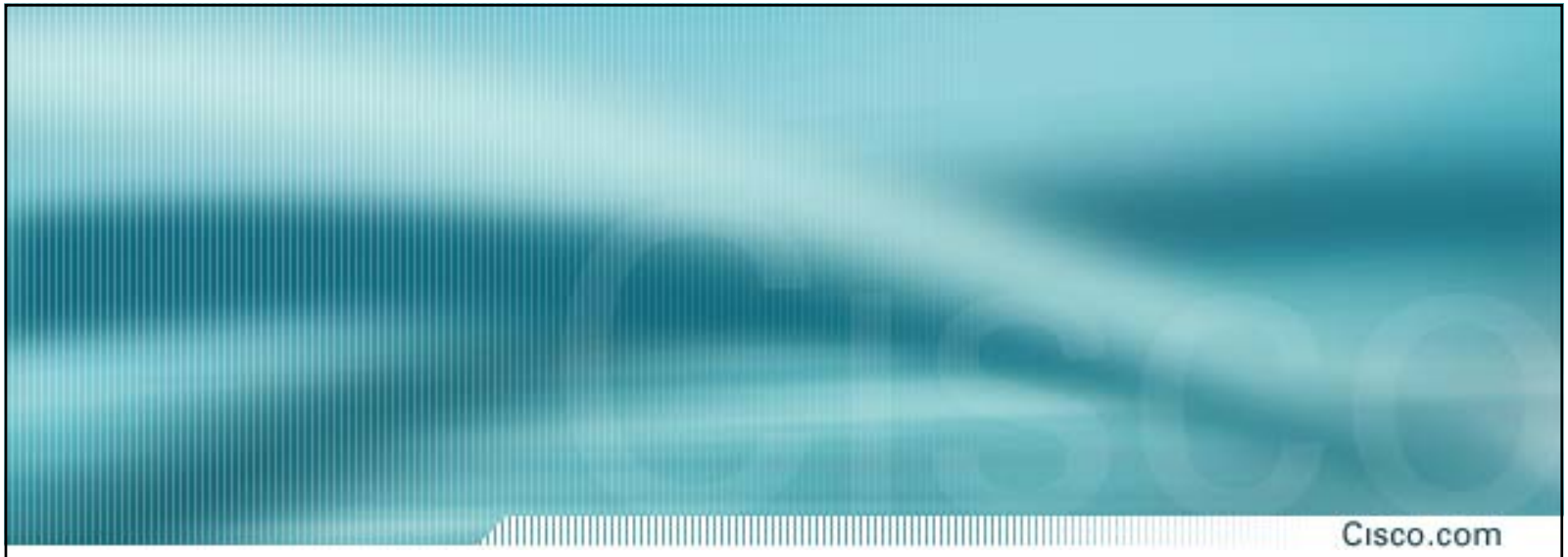
DMVPN – How it works

Cisco.com

- **Relies on two proven Cisco technologies**
  - **NHRP – Next Hop Resolution Protocol**
    - **Client/server protocol: hub is server; spokes are clients**
    - **Hub maintains a (NHRP) database of all the spoke's real (public interface) addresses**
      - **Each spoke registers its real address when it boots**
      - **Spokes query NHRP database for real addresses of destination spokes to build direct tunnels**
  - **Multipoint GRE Tunnel Interface**
    - **Allows single GRE interface to support multiple IPSec tunnels.**
    - **Simplifies size and complexity of configuration**

DMVPN – How it works

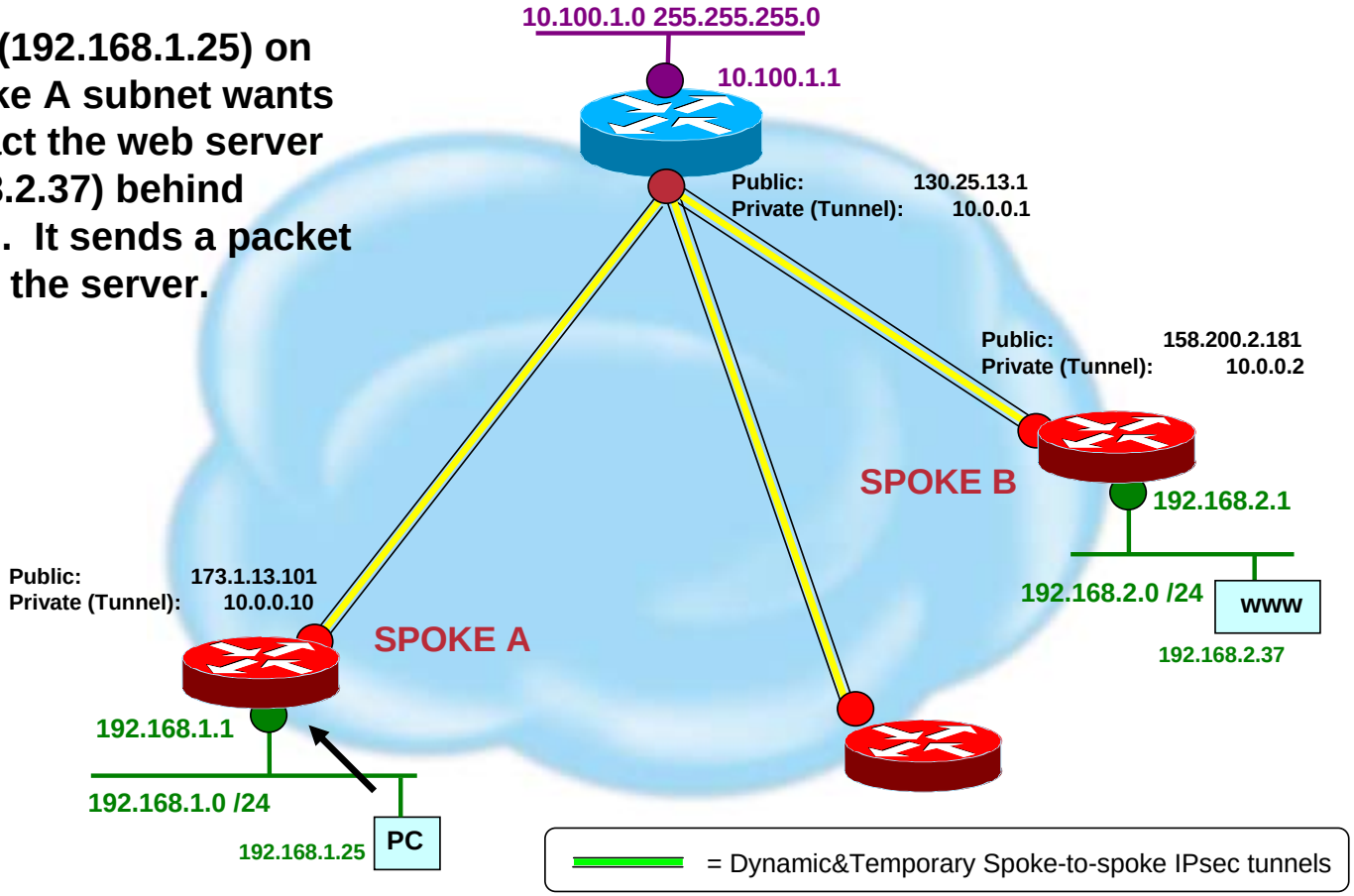
- Spokes have a permanent IPSec tunnel to the hub, but not to the spokes. They register as clients of the NHRP server
- When a spoke needs to send a packet to a destination (private) subnet on another spoke, he queries the NHRP server for the real (outside) address of the destination spoke
- Now the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



Dynamic Multipoint VPN Example

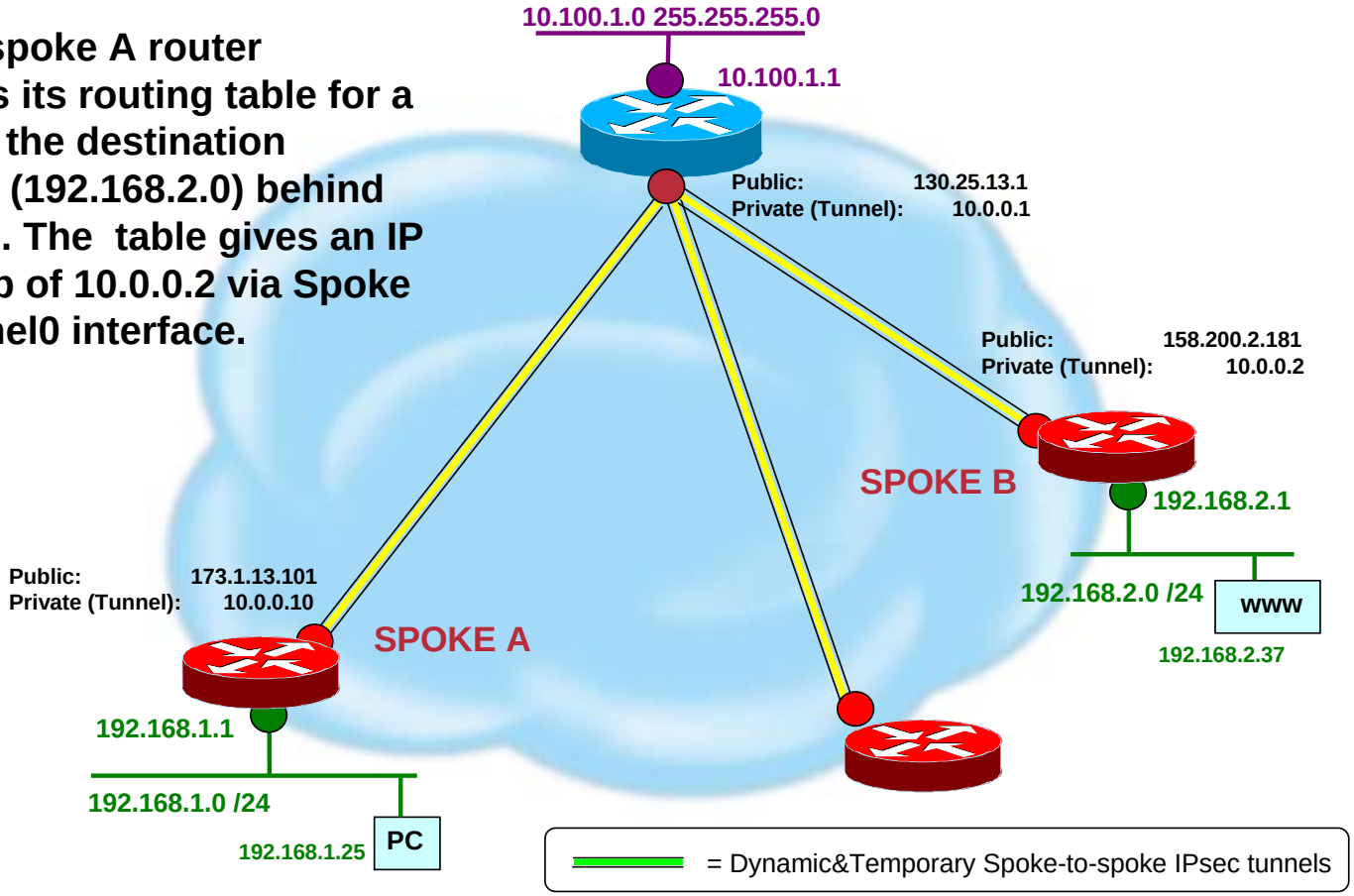
Dynamic Multipoint VPN - Example

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.



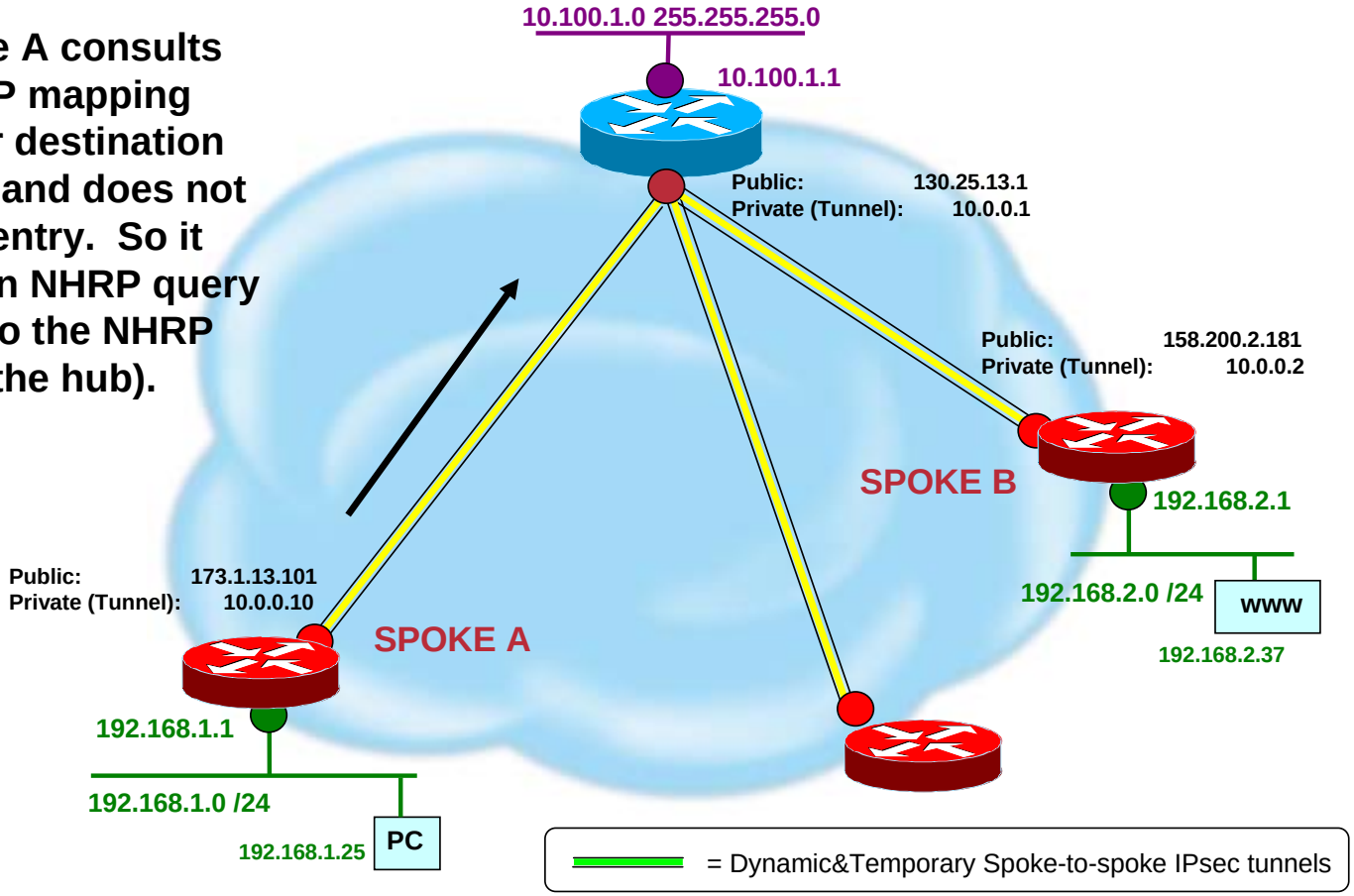
Dynamic Multipoint VPN - Example

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 10.0.0.2 via Spoke A's tunnel0 interface.



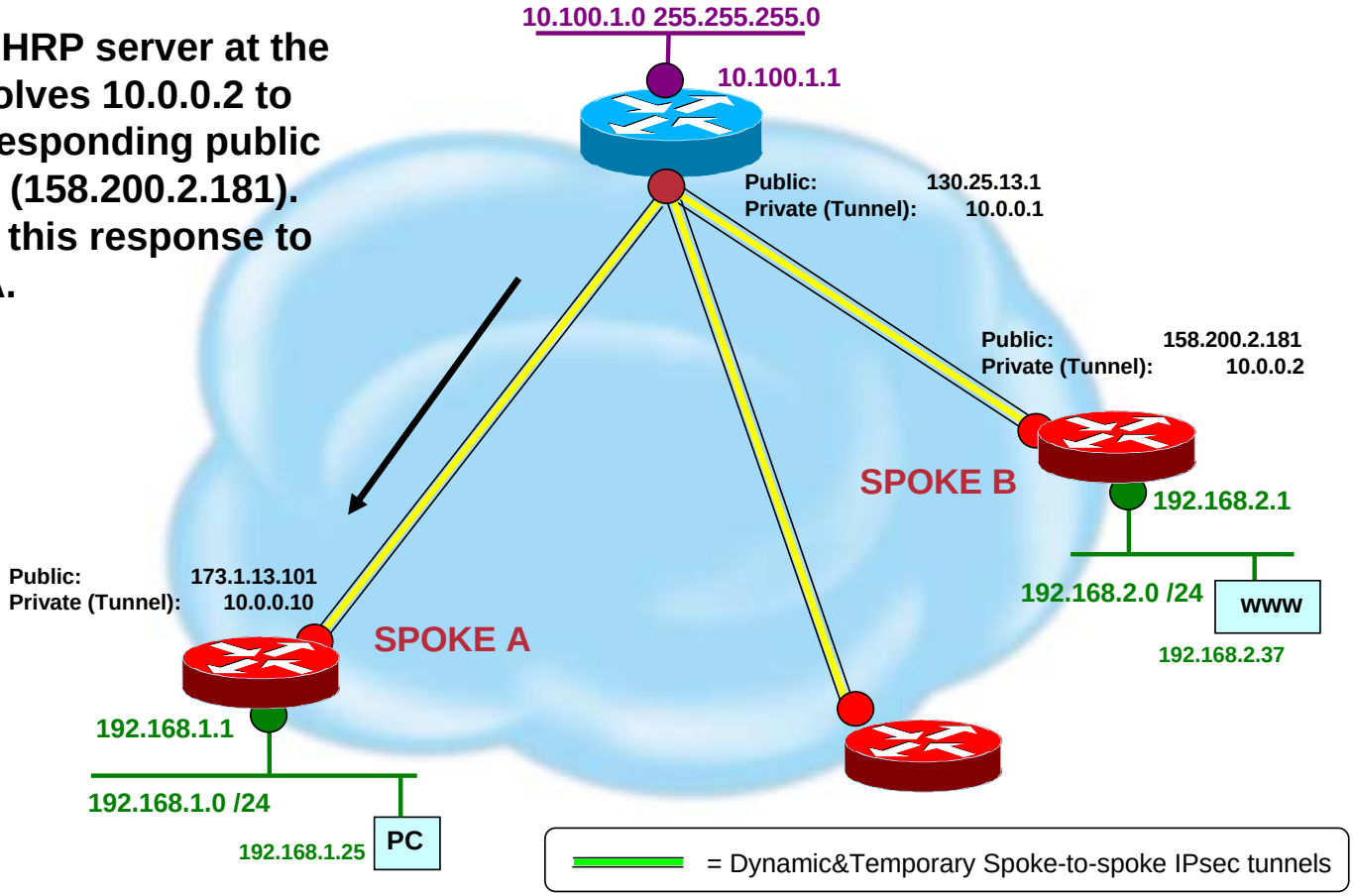
Dynamic Multipoint VPN - Example

3. Spoke A consults its NHRP mapping table for destination 10.0.0.2 and does not find an entry. So it sends an NHRP query packet to the NHRP server (the hub).



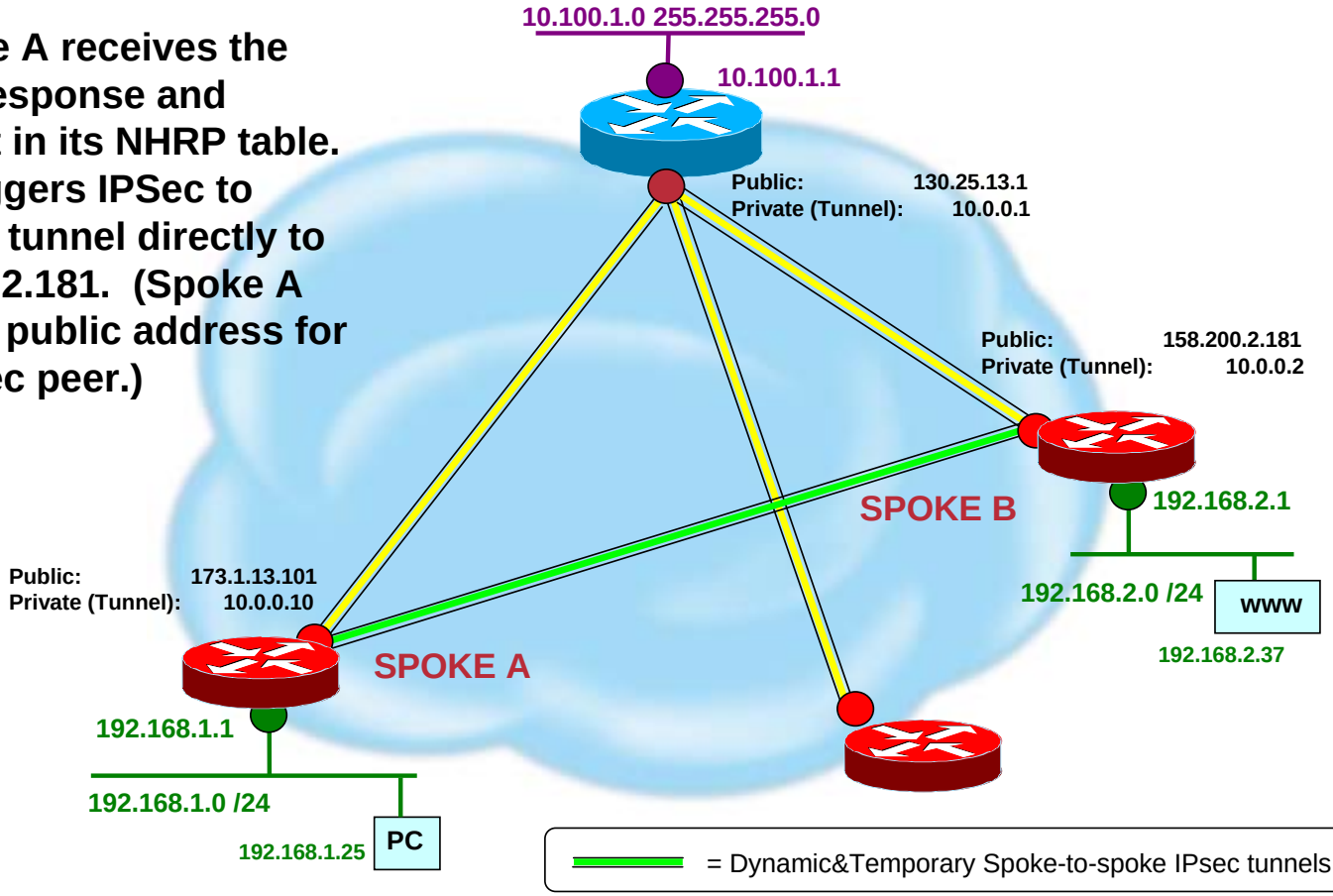
Dynamic Multipoint VPN - Example

4. The NHRP server at the hub resolves 10.0.0.2 to the corresponding public address (158.200.2.181). It sends this response to Spoke A.



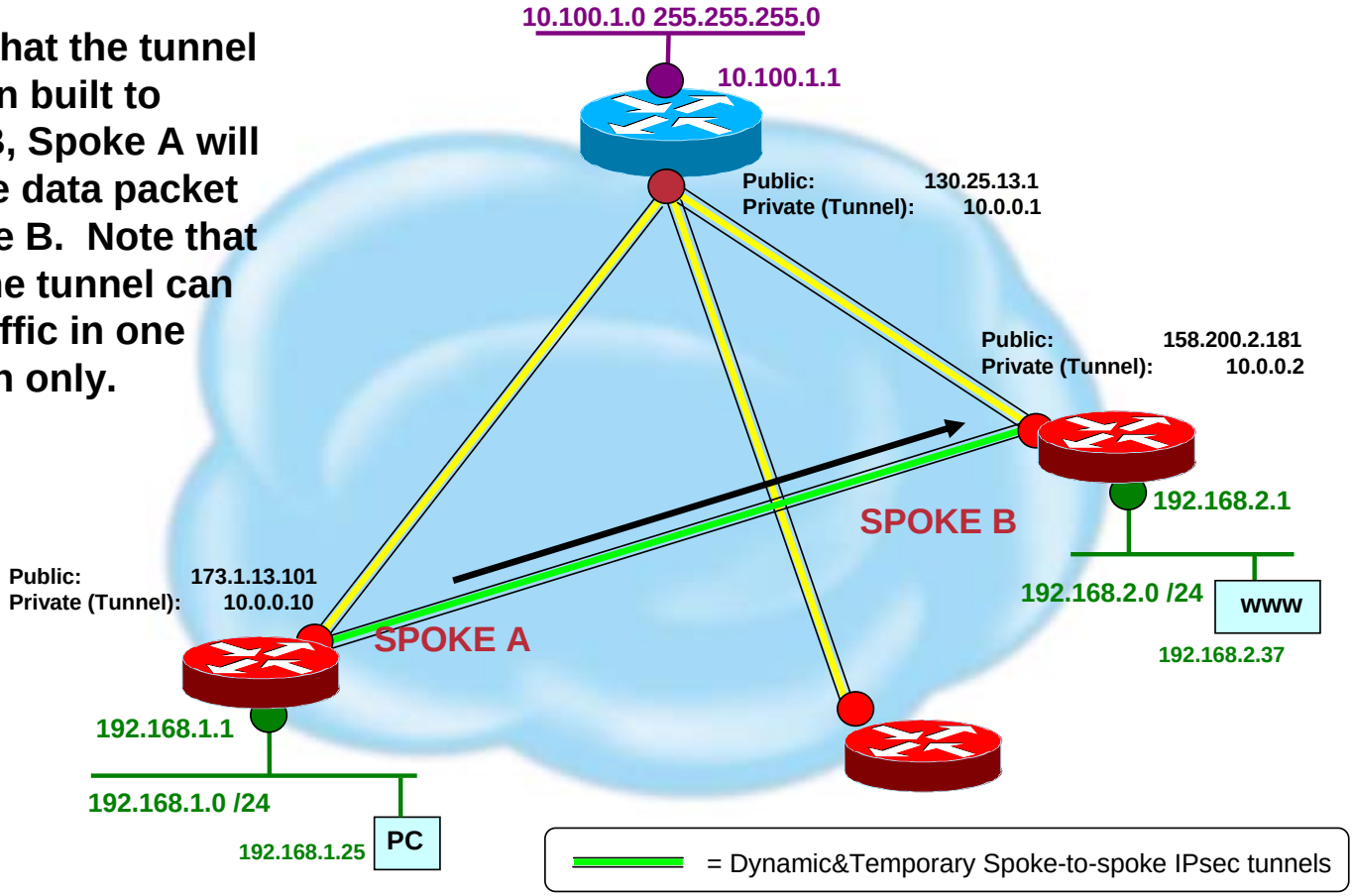
Dynamic Multipoint VPN - Example

5. Spoke A receives the NHRP response and enters it in its NHRP table. This triggers IPSec to create a tunnel directly to 158.200.2.181. (Spoke A uses its public address for the IPSec peer.)



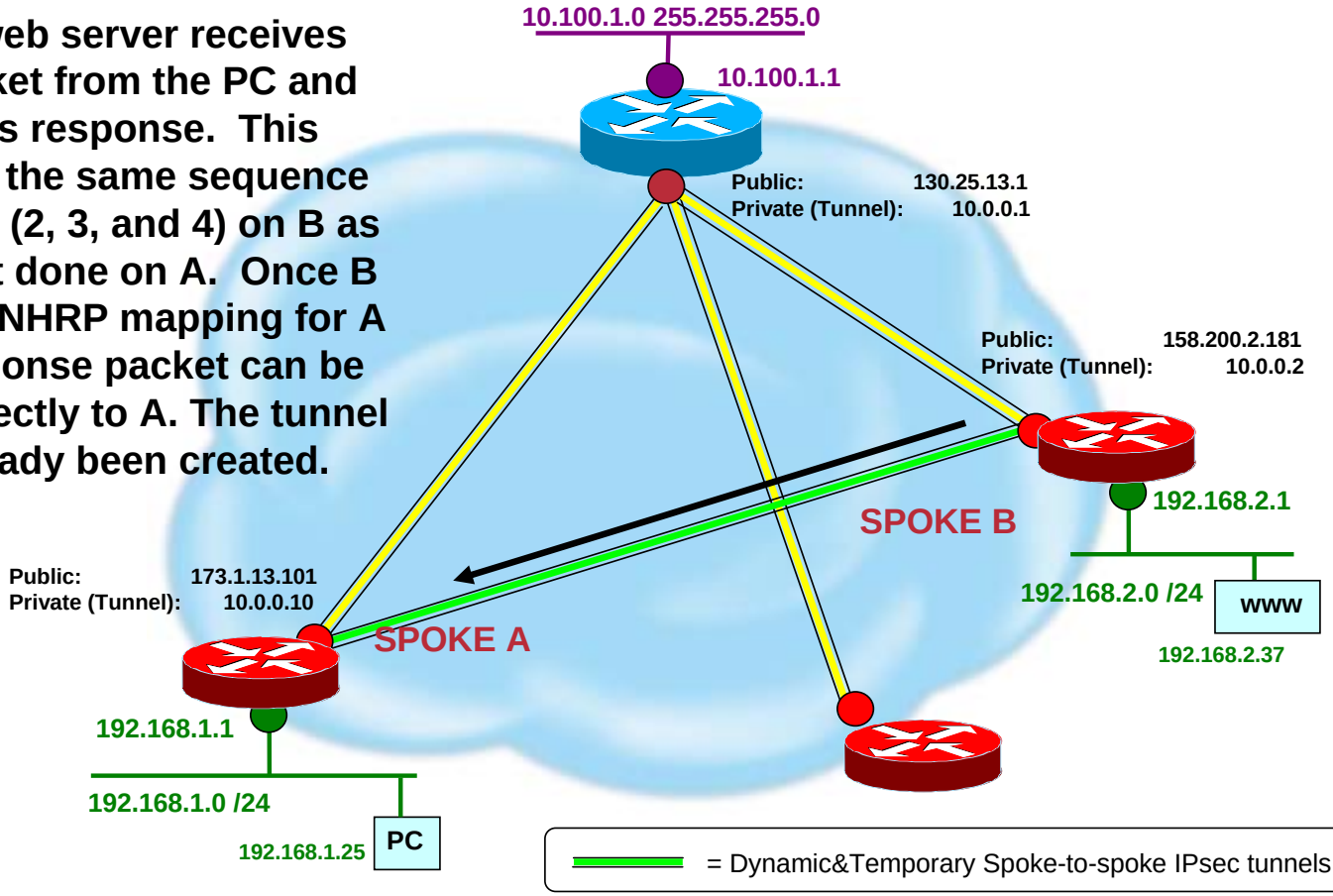
Dynamic Multipoint VPN - Example

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



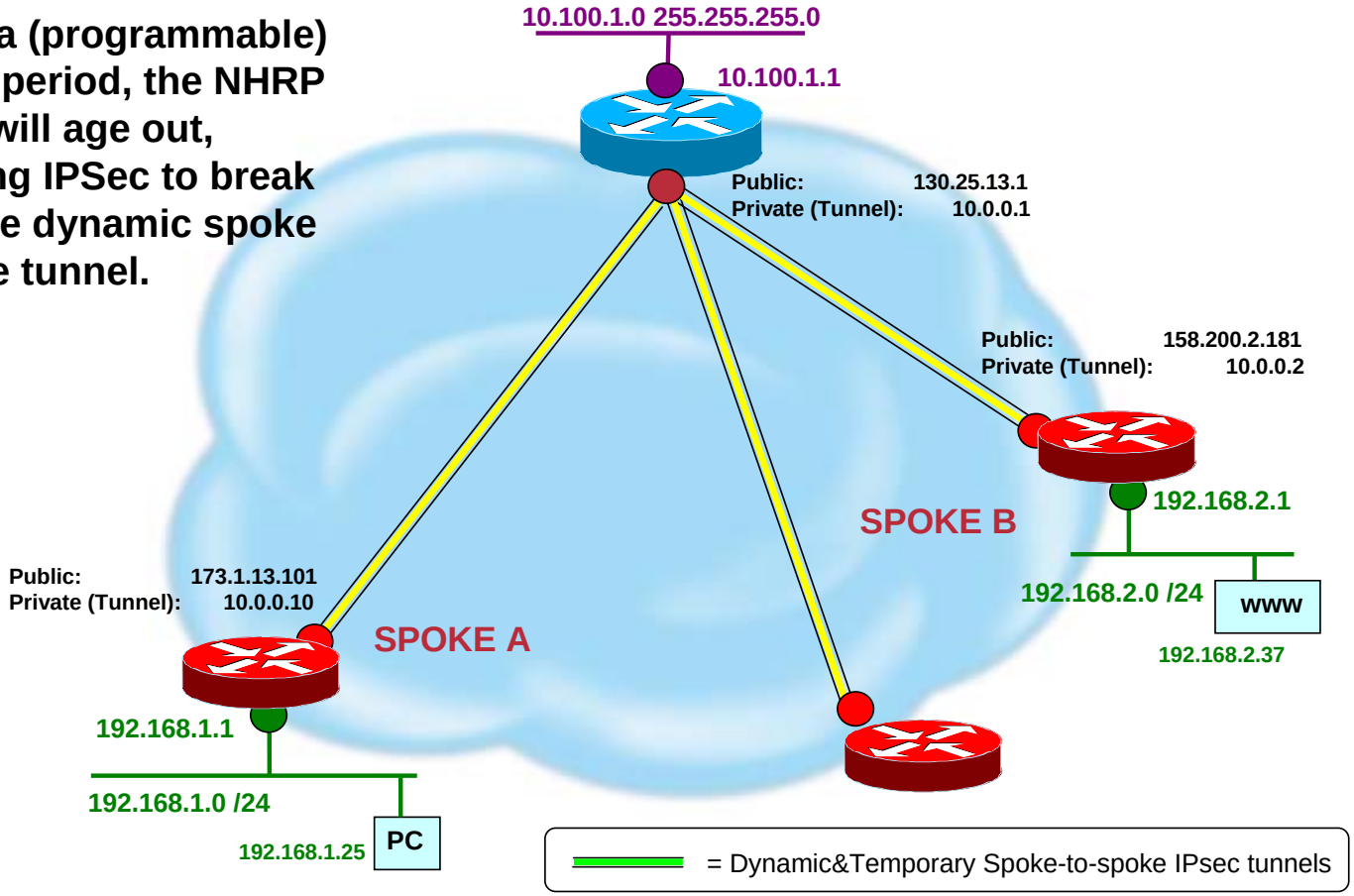
Dynamic Multipoint VPN - Example

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

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



Routing

- Dynamic routing is required over hub-to-spoke tunnels.
- Spoke learns of all private networks on the other spokes and the hub via routing updates sent via the hub.
- IP next-hop for a spoke network is the tunnel interface for that spoke.
- Possible routing protocols are EIGRP, OSPF, BGP, RIP. EIGRP is expected to scale the best of these.

Configuration Examples – Hub


```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto IPsec transform-set trans2 esp-des esp-md5-hmac
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
```

Configuration Examples – Hub – Cont.

Cisco.com

```
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1416
 ip nhrp authentication donttell
 ip nhrp map multicast dynamic
 ip nhrp network-id 99
 ip nhrp holdtime 300
 no ip split-horizon eigrp 1
 no ip next-hop-self eigrp 1
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
```

Configuration Examples – Hub – Cont.


```
interface Ethernet0
 ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.0.255 area 0
!
```

Key point – no explicit configuration lines for each spoke!!!

Configuration Examples – Spoke


```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto IPsec transform-set trans2 esp-des esp-md5-hmac
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
```

Configuration Examples – Spoke – Cont.

Cisco.com

```
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.3 255.255.255.0
 ip mtu 1416
 ip nhrp authentication donttell
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 99
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
```

Configuration Examples – Spoke – Cont.


```
!
interface Ethernet0
 ip address dhcp hostname Spoke1
!
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
```

Key point – all spokes will be configured the same except for tunnel and local interface addresses.

Configuration Size Reduction – Hub Router in 300-Spoke Network

- **Typical Hub Configuration Size**

  13 lines per spoke = 3,900

- **DMVPN Hub Configuration Size**

  16 lines

➢ **Savings: 3,884 lines!**

(This is the configuration related to the spokes, not the entire configuration.)

Adding a Spoke With the DMVPN Solution

Cisco.com

- **Create spoke configuration – easy!**

  Spoke configs are identical except for definition of private network(s), and public IP address (if static).

- **No reconfiguration needed on hub or any other spoke**
- **Burden on provisioning management system is much reduced.**
- **Also note that dynamically addressed CPE (i.e. public interface address obtained via DHCP) are supported by DMVPN.**

IOS Code & Platform Support

- **12.2(13)T**

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftgreips.htm

- **7204/6, 37xx, 26xx, 17xx**

Summary

- **Dynamic Multipoint VPNs take IPSec VPNs *to the next level* by…**
  - ✓ **Enabling dynamic tunnels**
  - ✓ **Eliminating the hassle of adding a node**
  - ✓ **Drastically reducing configuration size**
  - ✓ **All while supporting dynamically addressed CPE, multicast, and split tunneling!**
- **Bottom line is great scalability with less administration!**