



# **INTRODUCTION TO DYNAMIC MULTIPOINT VPN**

**SECURITY TECHNOLOGY GROUP  
NOVEMBER 2004**

# DYNAMIC MULTIPOINT VPN (DMVPN) FUNDAMENTALS



# DMVPN – How it Works

- **DMVPN is a Cisco IOS Software solution for building IPsec+GRE VPNs in an easy and scalable manner**
- **Relies on two proven Cisco technologies**

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

**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 does not alter the standards-based IPsec VPN tunnels, but it changes their configuration**

# DMVPN – How it works (Cont.)

- **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**

# Routing with DMVPN

- **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:**
  - Enhanced Interior Gateway Routing Protocol (EIGRP), which scales reasonably well**
  - Open Shortest Path First (OSPF)**
  - Border Gateway Protocol (BGP)**
  - Routing Information Protocol (RIP)**

# DMVPN Phases

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

# IPsec+GRE versus DMVPN Phase 1 Hub-to-Spoke

Feature	IPsec+GRE	DMVPN
All traffic must go via the hub		
Easy to deploy		
Small hub configuration files		
No hub provisioning for new spokes		
Easy Configuration of dynamically addressed CPE		

## DMVPN Phase 1 Benefits

- Simplified and Smaller Configs for Hub and Spoke
- Zero touch provisioning for adding spokes to the VPN
- Easily supports dynamically addressed CPEs

# IPsec+GRE versus DMVPN Phase 2

## Static Full Mesh versus Virtual Full Mesh

Feature	IPsec+GRE	DMVPN
Direct spoke-to-spoke tunnels		
Connections to all nodes with smaller spoke CPE		
Provisioning for adding a new node		
Scaling and support of a full mesh		

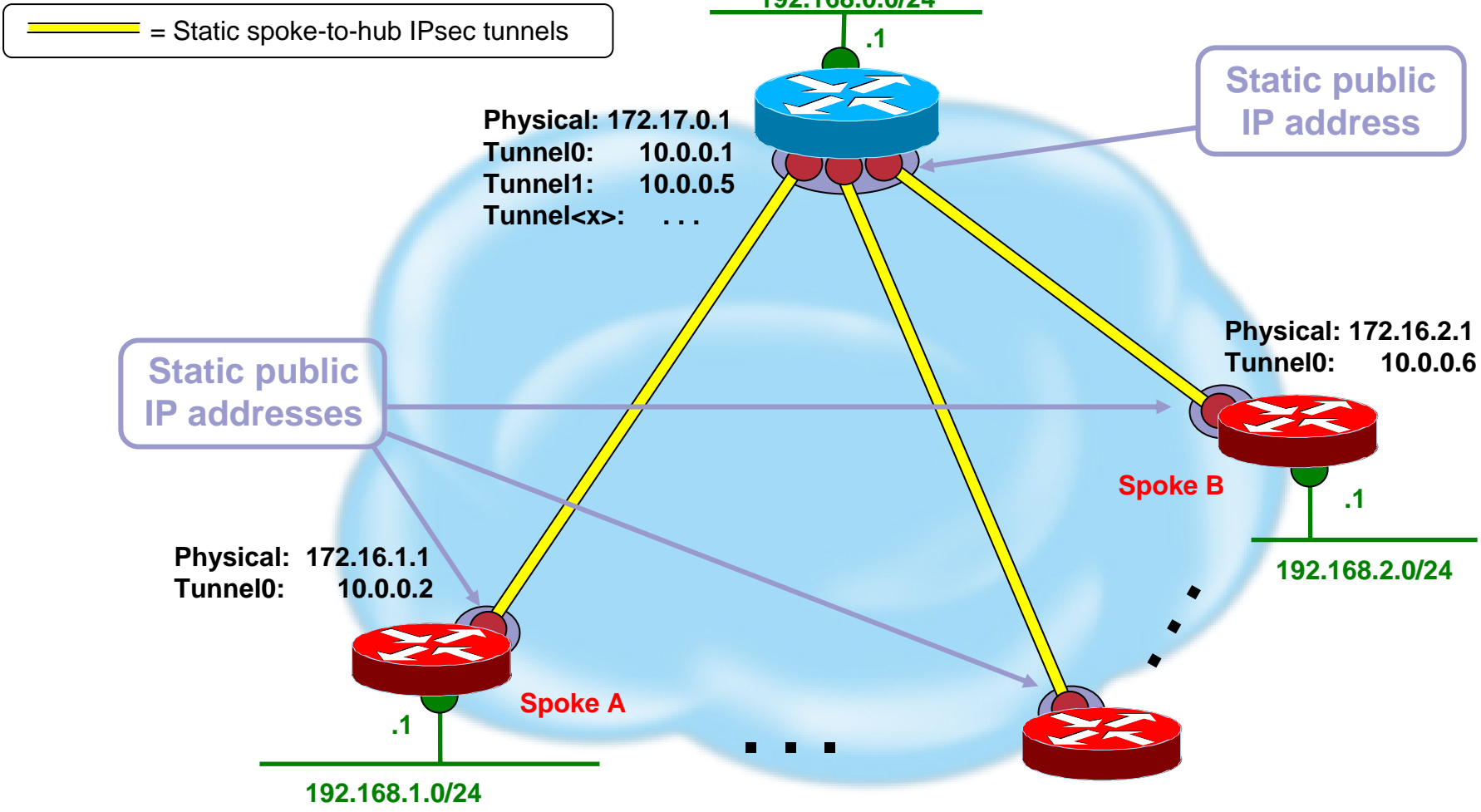
### DMVPN Phase 2 Benefits – Future Functionality

- On-demand spoke-to-spoke tunnels – avoids dual encrypts/decrypts
- Smaller spoke CPE can participate in the virtual full mesh

# CONFIGURATION SIMPLICITY



# How Does the Configuration Change – IPsec + GRE



# IPsec+GRE Hub and Spoke Hub Configuration


Cisco.com

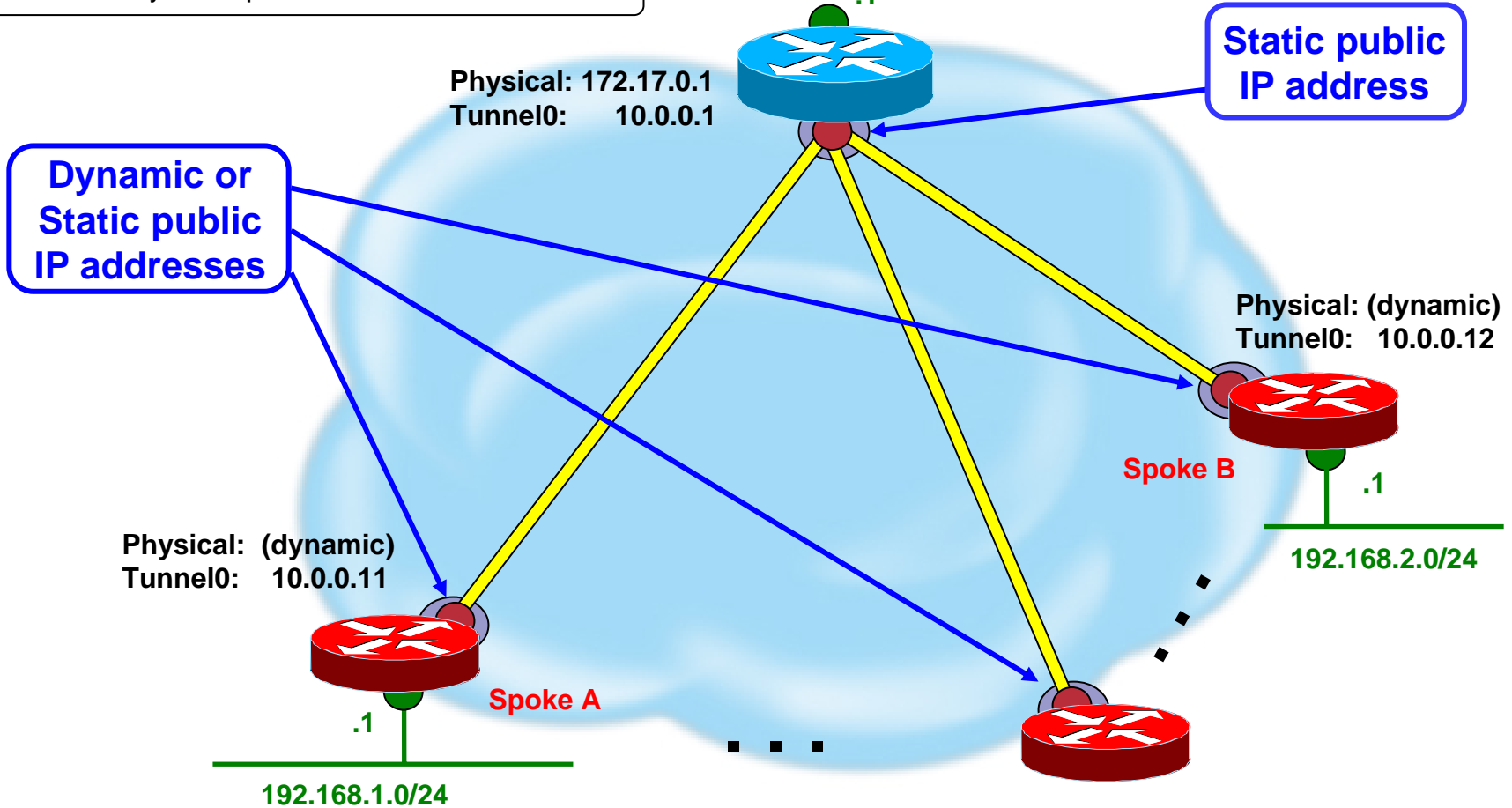
```
crypto ca trustpoint msca-root
  enrollment terminal
  crl optional
  rsakeypair hub1
crypto ca certificate chain msca-root
  certificate 2368DB5500000000B4E
  certificate ca 1244325DE0369880465F977A18F61CA8
!
crypto isakmp policy 1
  encryption 3des
!
crypto ipsec transform-set t1 esp-3des esp-md5-hmac
!
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
```

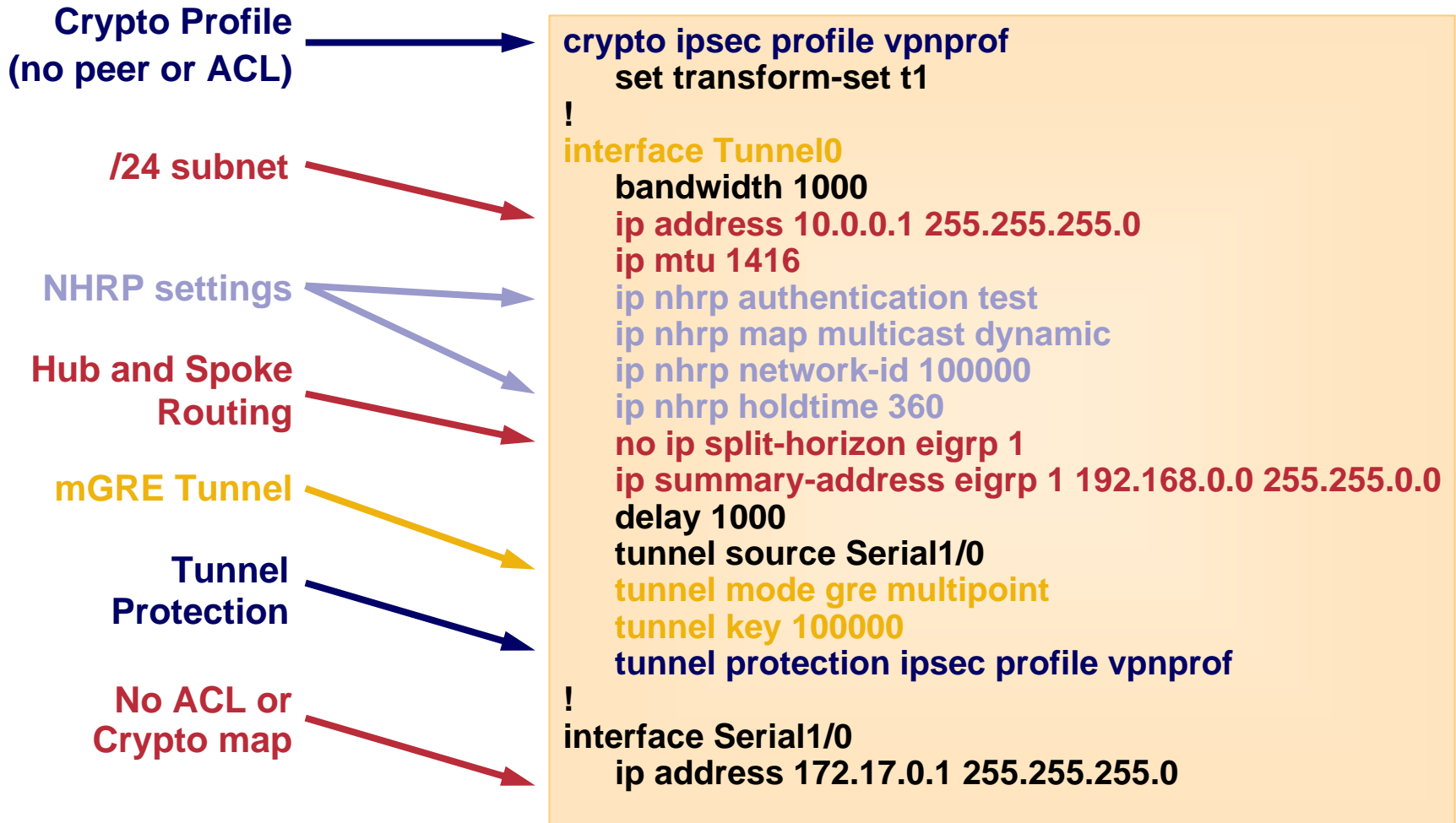
**One tunnel interface & crypto map(optional) for each spoke  
Hub config 13 lines per spoke so 300 spokes=3900 lines**

# Dynamic Multipoint VPN Phase 1 Hub-and-Spoke

 = Dynamic permanent IPsec+GRE tunnels

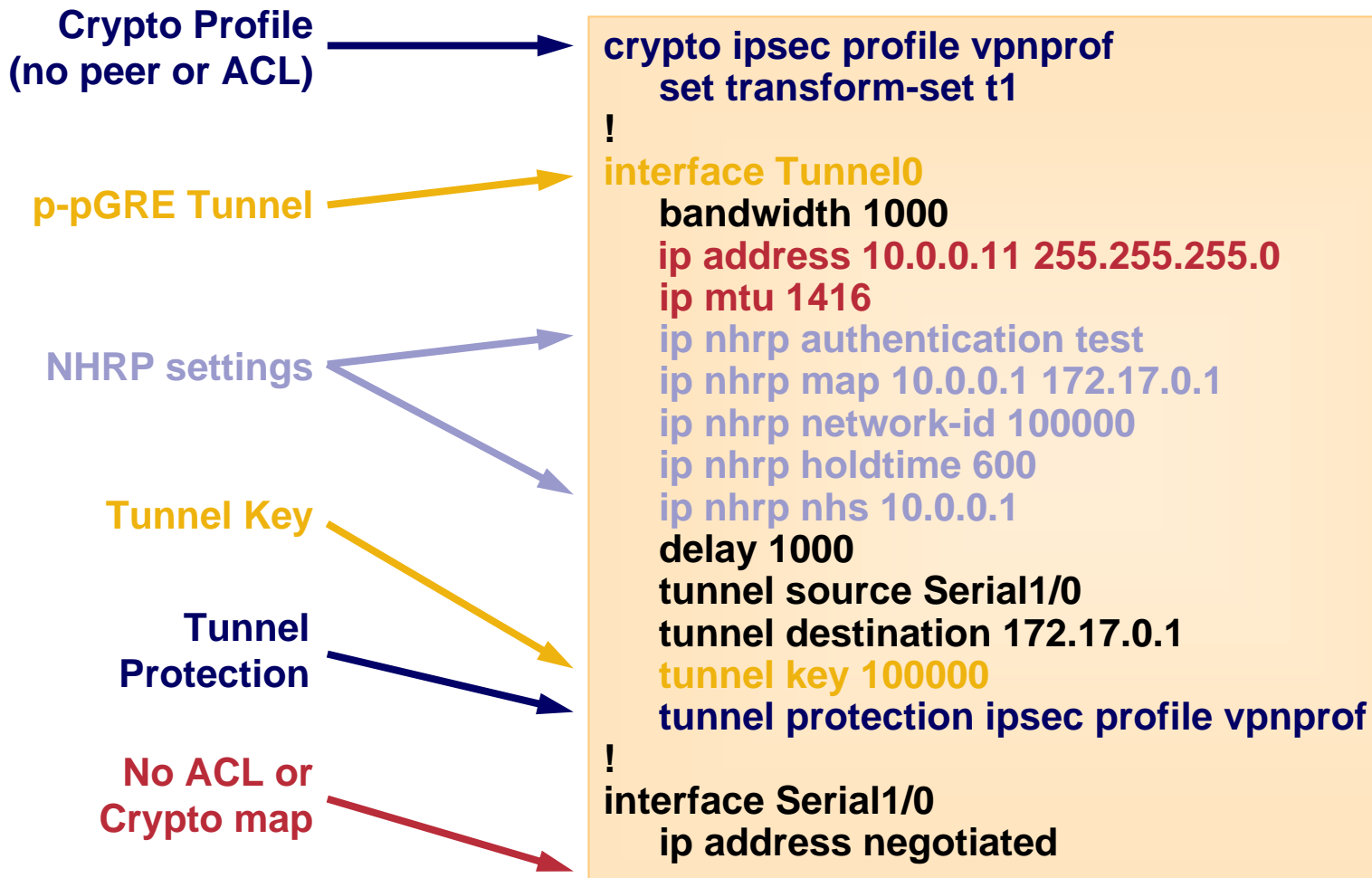


# DMVPN Phase 1 - Hub and Spoke Configuration Changes – Hub



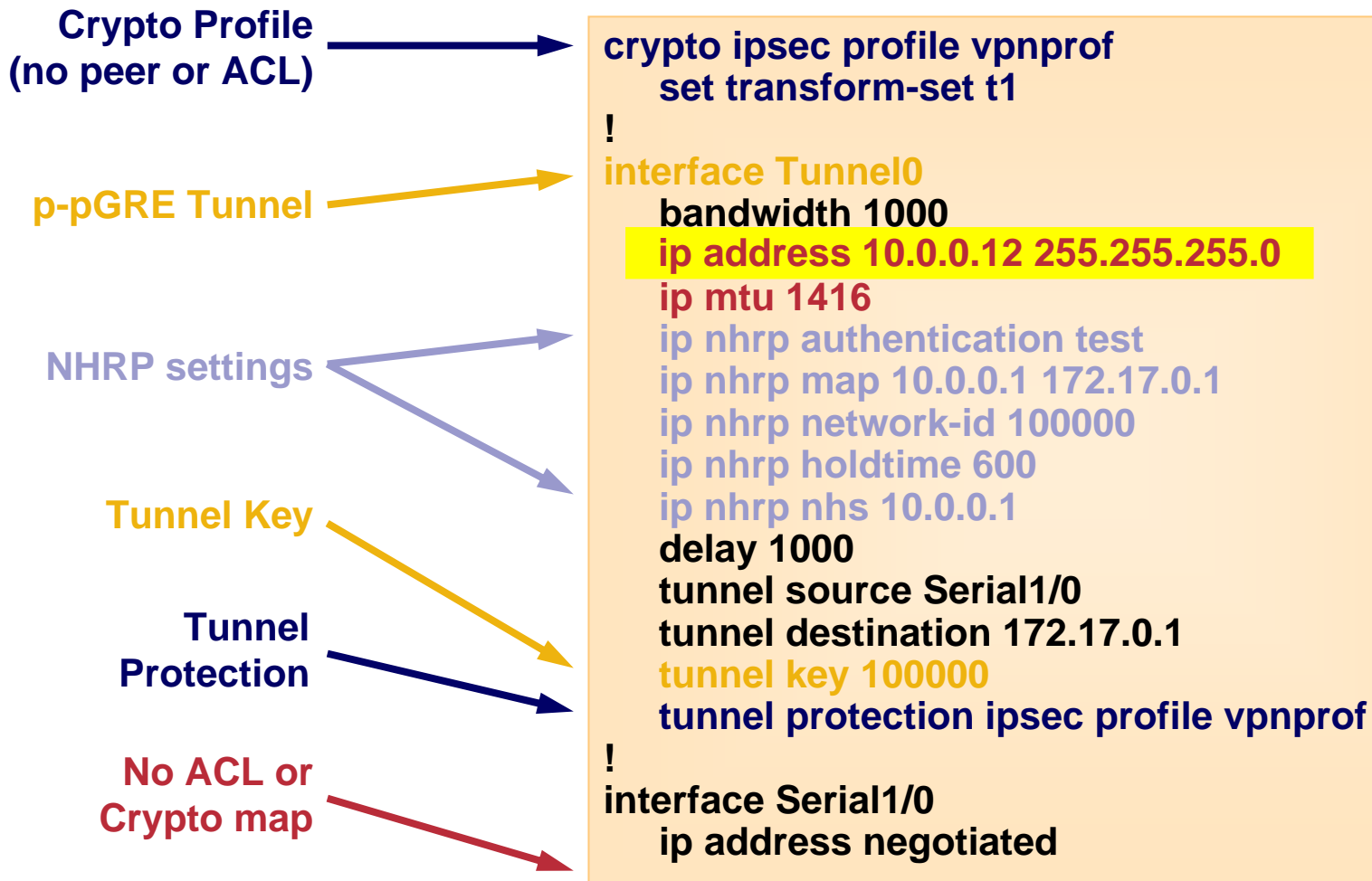
**No explicit configuration lines for each spoke.  
Hub configuration size = 13 lines 300 spokes = 13 lines**

# DMVPN Phase 1 - Hub and Spoke Configuration Changes – Spoke A



**Uniform spoke configuration in the VPN**

# DMVPN Phase 1 - Hub and Spoke Configuration Changes – Spoke B



**Spoke B does not change much**

# Recap: IPsec+GRE versus DMVPN

- **Hub configuration**

1 interface/spoke → 300 spokes = **300 interfaces**

4 IP addresses/spoke → 300 spokes = **1200 addresses**

13 lines/spoke → 300 spokes = **3900 lines**

- **Hub Configuration**

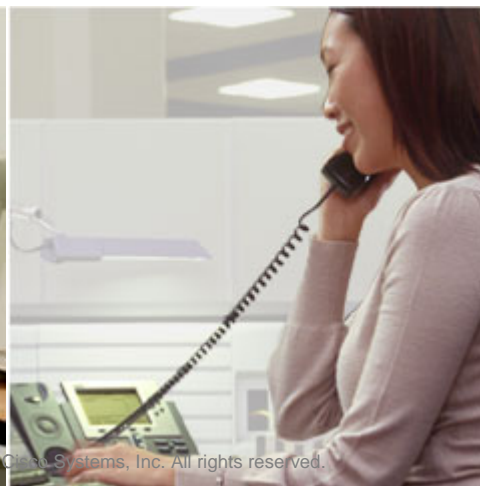
1 interface → 300 spokes = **1 interface**

1 IP address/spoke → 300 spokes = **300 addresses**

13 lines → 300 spokes = **13 lines** -> 1000 spokes = **13 lines**

**“ Provisioning a new branch office requires config changes to our central hub connecting over 20 banks. If there is an error in configuration, we have had downtimes exceeding 13 hours. I cannot afford to bring down my network for 13 hours. This is the most appealing part of DMVPN to me.”**

CUSTOMER INTERVIEW,  
AMEX BANKS



# DMVPN Solution Roadmap

Cisco.com

## Q1CY'04 – Phase 1

- Cisco 1700, 2600, 3700, and 7200 Series Routers

### Network Features Requirements

- Network integration with DMVPN
- Tunnel to Physical address mapping with NHRP
- Route propagation with EIGRP & OSPF
- Interoperability with NAT (spokes running NAT and/or behind NAT boxes)
- Multicast support in VPN.
- VPN failover and load balancing
- QoS functionality for spoke-to-hub
- VRF support-extend MPLS VPN with DMVPN
- Functionality in all switching paths (Cisco Express Forwarding and process paths)

### Management

- ISC 3.x management and monitoring
- VMS management and monitoring

## Q2CY'04 – Phase 2

- Cisco 800, 1700, 2600, 3700, and 7200 Series Routers
- VPNSM (6500/7600) DMVPN Phase 1.0 support

### Network Feature Requirements

- DMVPN spoke-to-spoke communication
- Tunnel to Physical addr mapping with NHRP
- Route propagation with EIGRP & OSPF
- Interoperability with NAT and Multicast support for spoke-to-spoke
- Spoke-to-spoke Communication independent Of single Hub Failures in redundant Multihub configurations
- Application of QoS policies for every spoke-to-spoke Tunnel Interface
- Complete V3PN Interoperability for spoke-to-spoke
- Dynamic limiting of spoke-to-spoke tunnels based on CPU usage
- Functionality in all switching paths (Cisco Express Forwarding/process)

### Management

- ISC 3.x management and monitoring
- VMS management and monitoring

## Q3CY'04 – Phase 3

### Targeted support

- Cisco 800, 1700, 2600, 3700, and 7200 Series Routers

### Network Features Requirements

- EIGRP/OSPF scaling with Route summarization
- Traffic shaping at hub interfaces on a per spoke / spoke group basis
- Exploration of an alternate routing protocol like BGP for scaling.
- Functionality in Cisco Express Forwarding and Process Paths
- Timeouts for removal of idle spoke-to-spoke tunnels
- Default QoS policies downloaded from hub to spoke based on spoke type

### Management

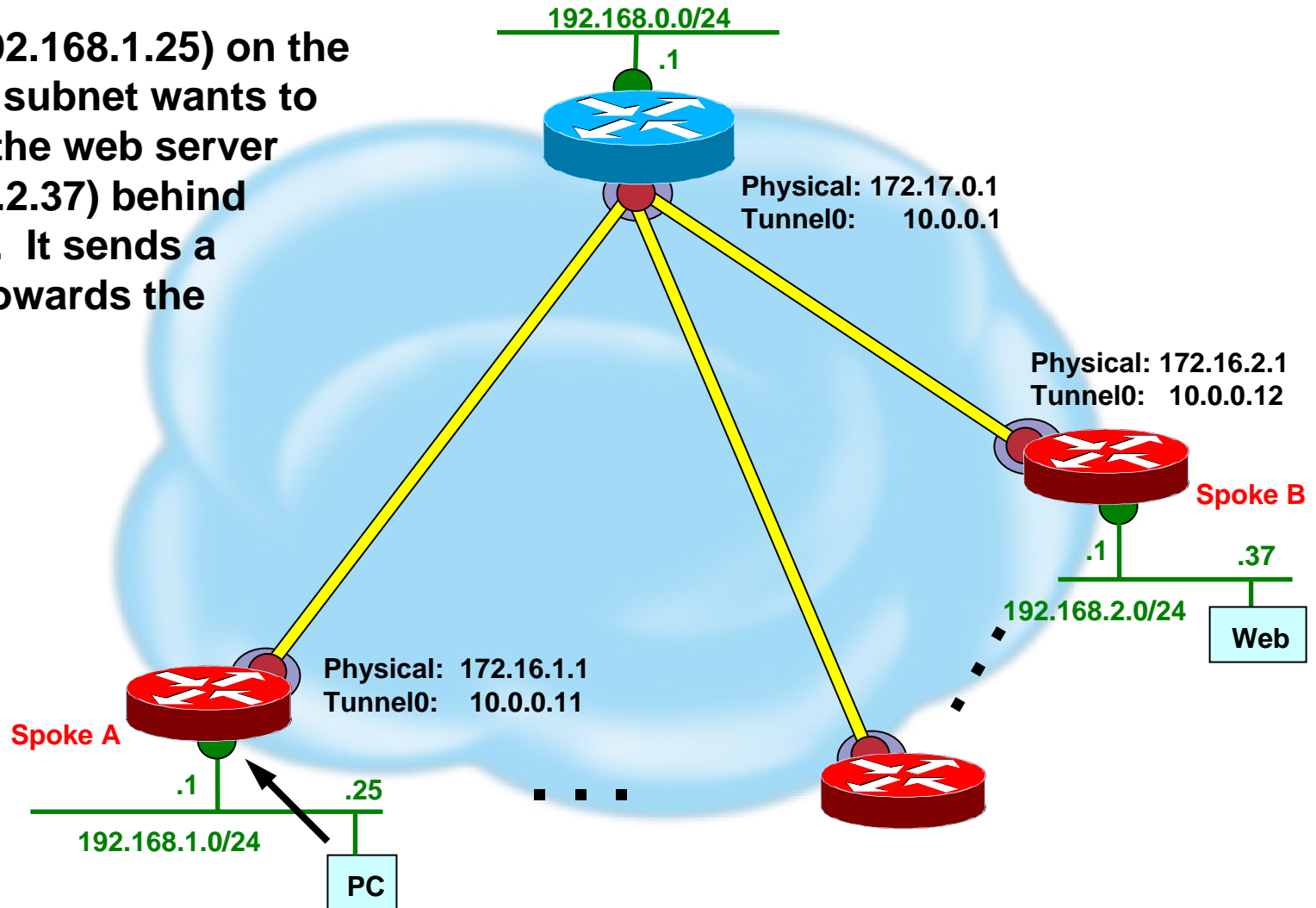
- ISC 3.x management and monitoring
- VMS management and monitoring

# DMVPN TRACE



# Dynamic Multipoint VPN—Example

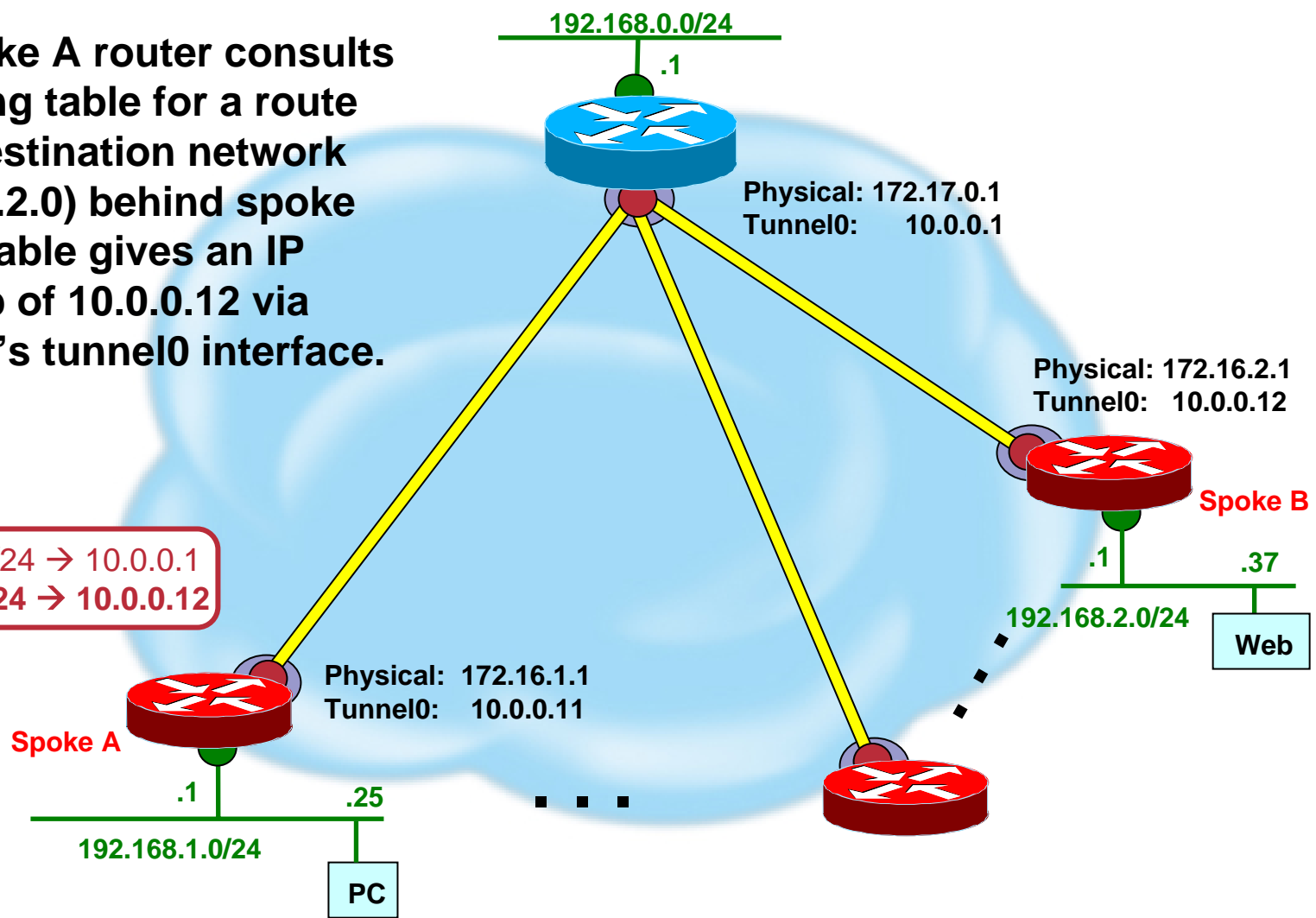
1. A PC (192.168.1.25) on the spoke A subnet wants to contact the web server (192.168.2.37) behind spoke B. It sends a packet towards the server.



# Dynamic Multipoint VPN—Example

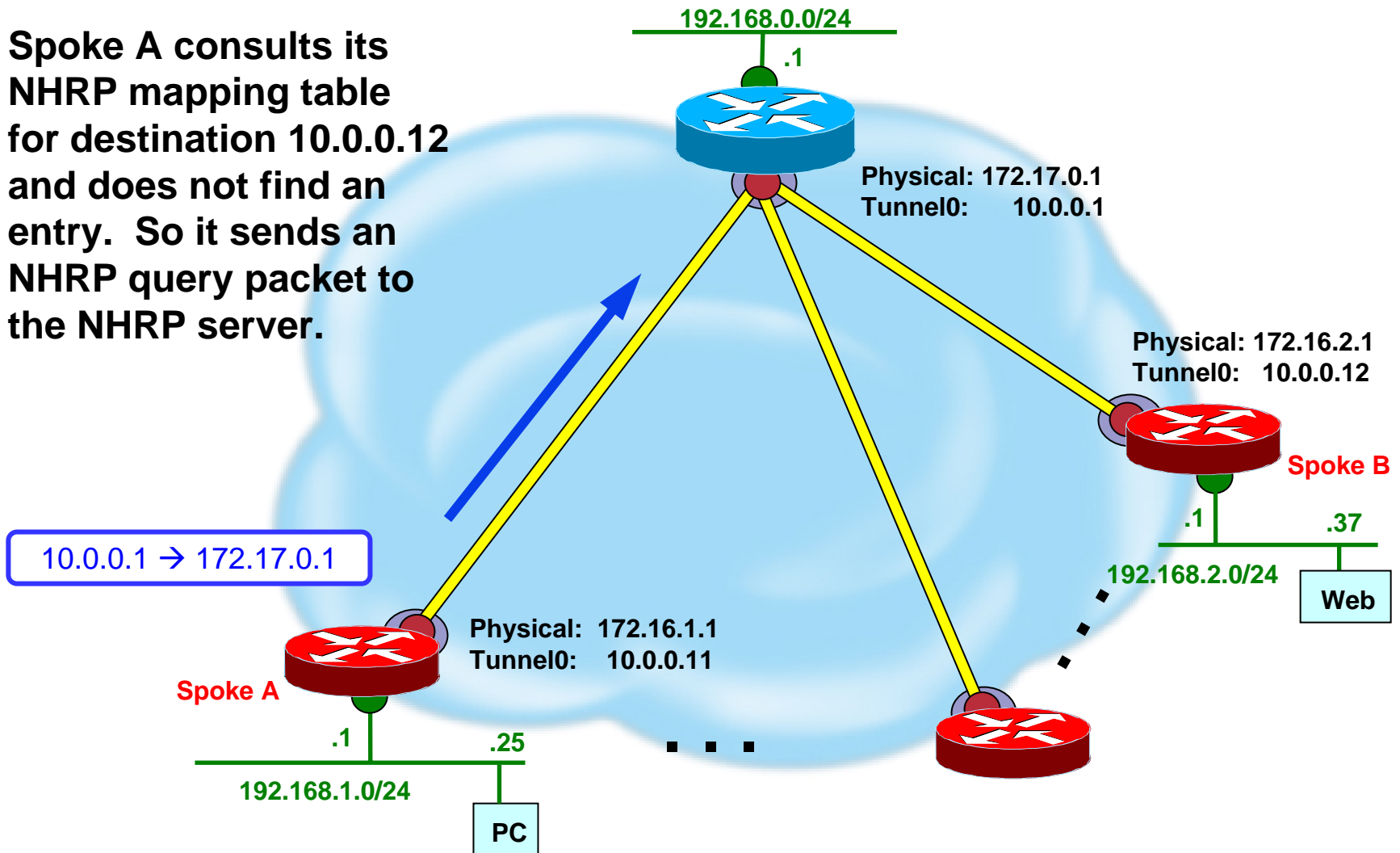
2. The spoke A router consults its routing table for a route to the destination network (192.168.2.0) behind spoke B. The table gives an IP next-hop of 10.0.0.12 via Spoke A's tunnel0 interface.

192.168.0.0/24 → 10.0.0.1  
192.168.2.0/24 → 10.0.0.12



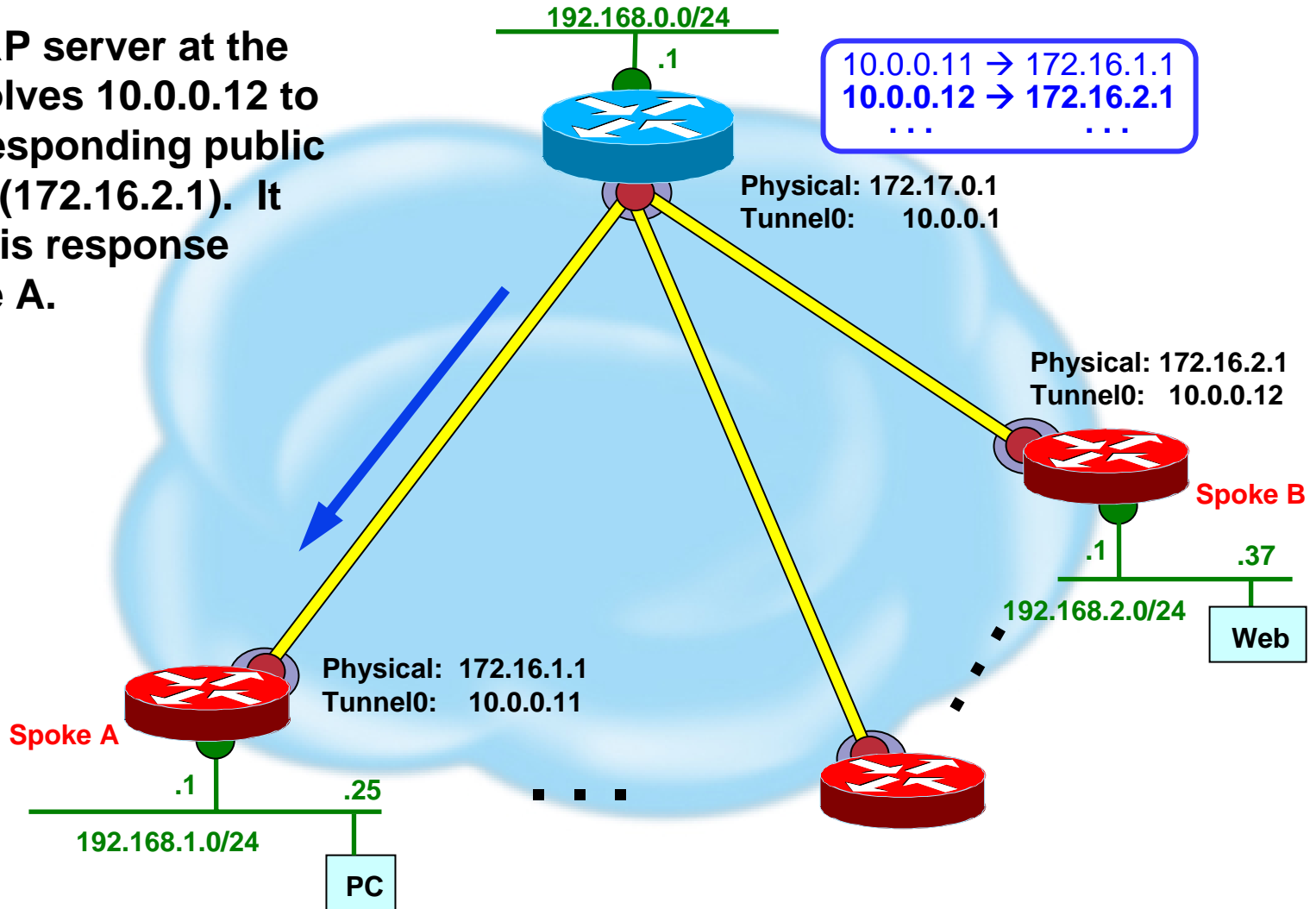
# Dynamic Multipoint VPN—Example

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.



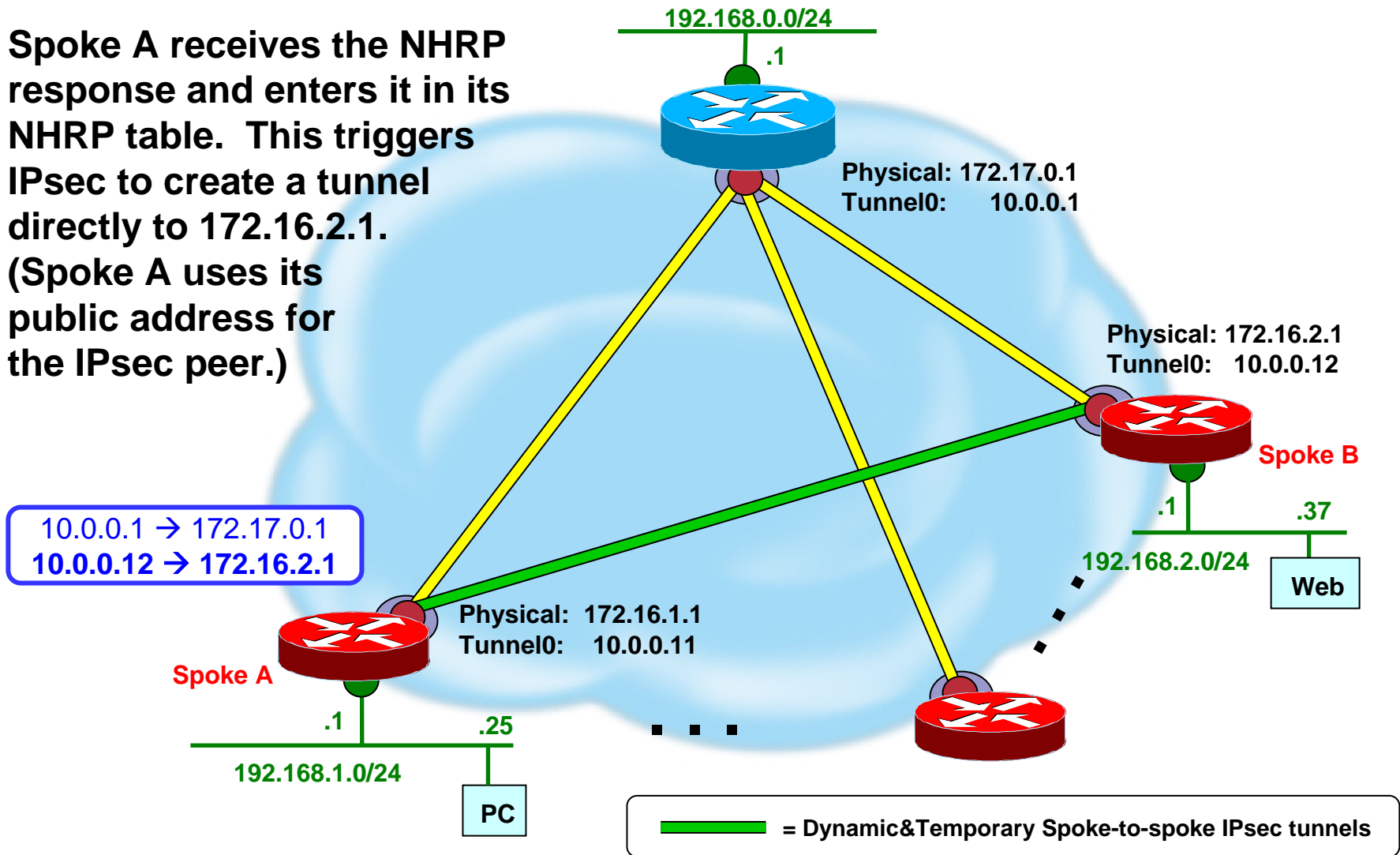
# Dynamic Multipoint VPN—Example

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.



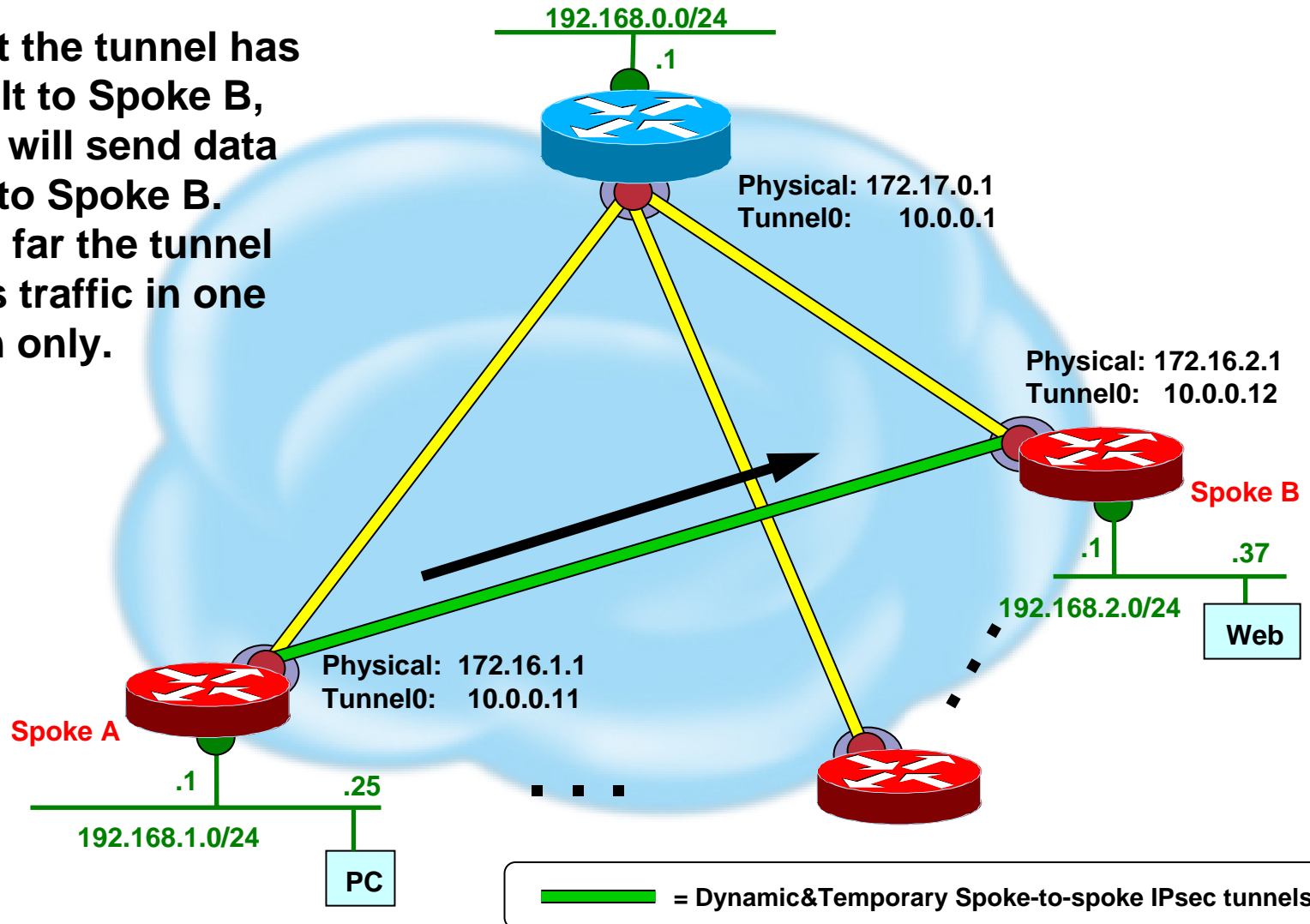
# Dynamic Multipoint VPN—Example

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.)



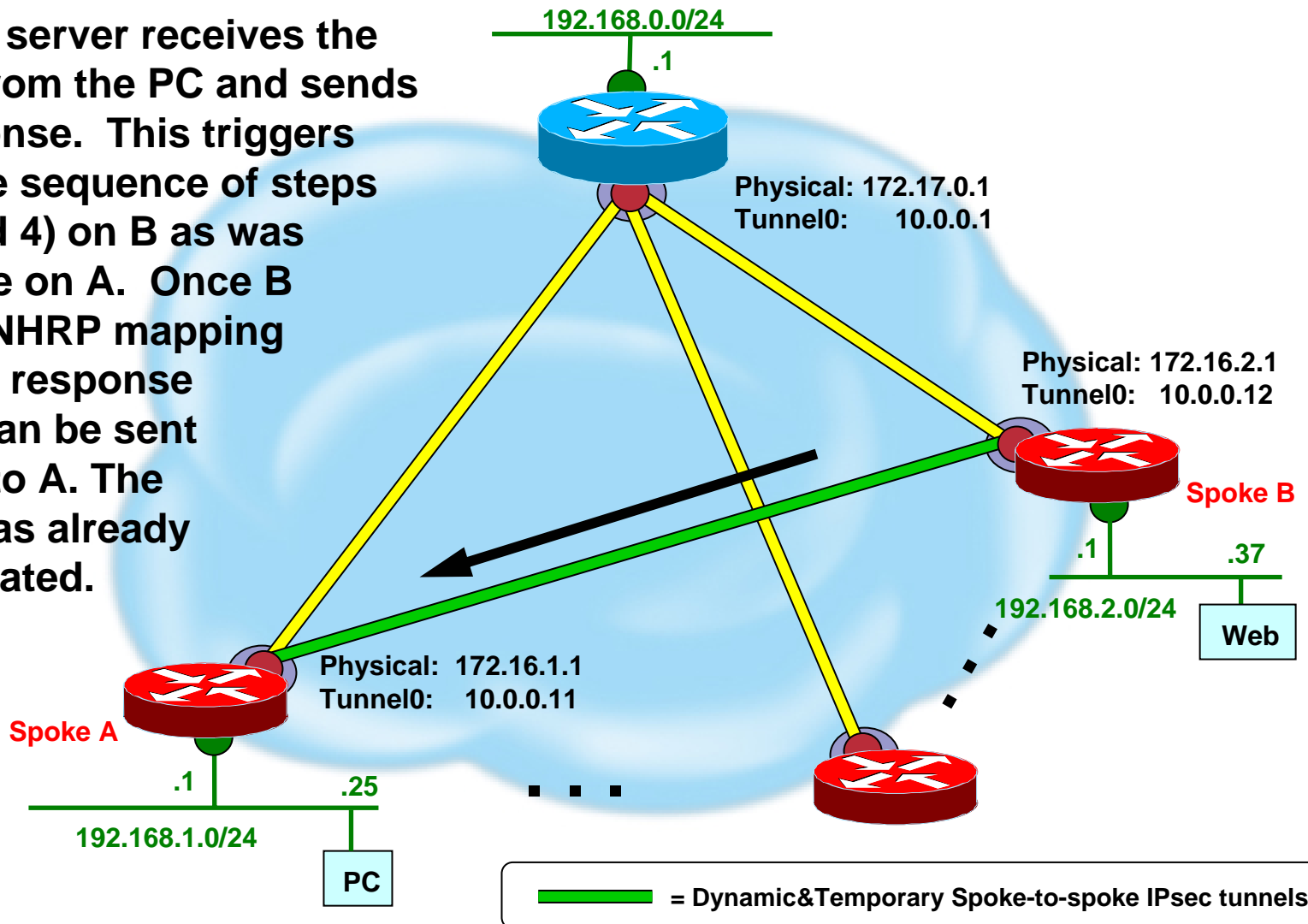
# Dynamic Multipoint VPN—Example

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.



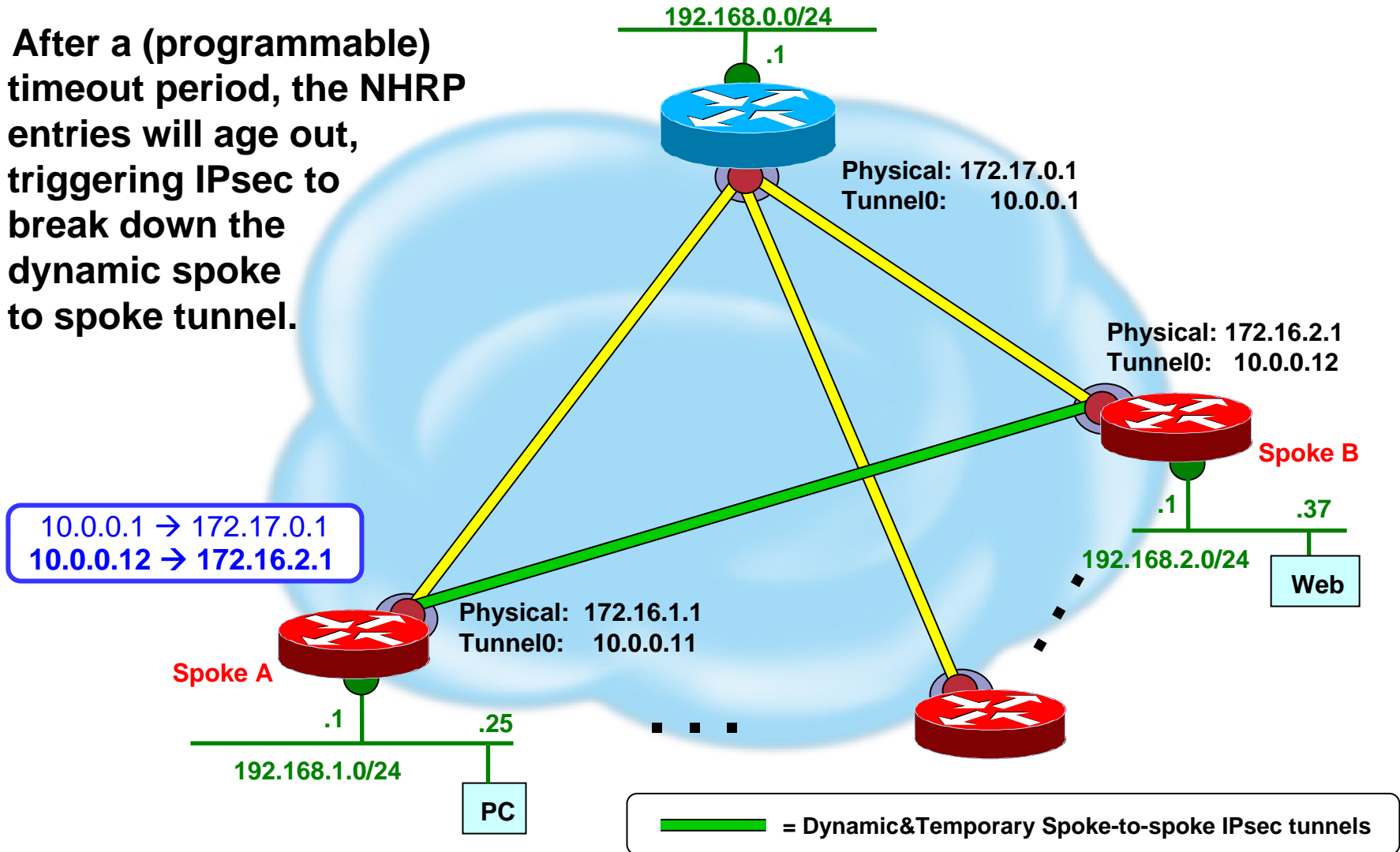
# Dynamic Multipoint VPN—Example

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.



# QUESTIONS



# CISCO SYSTEMS

