



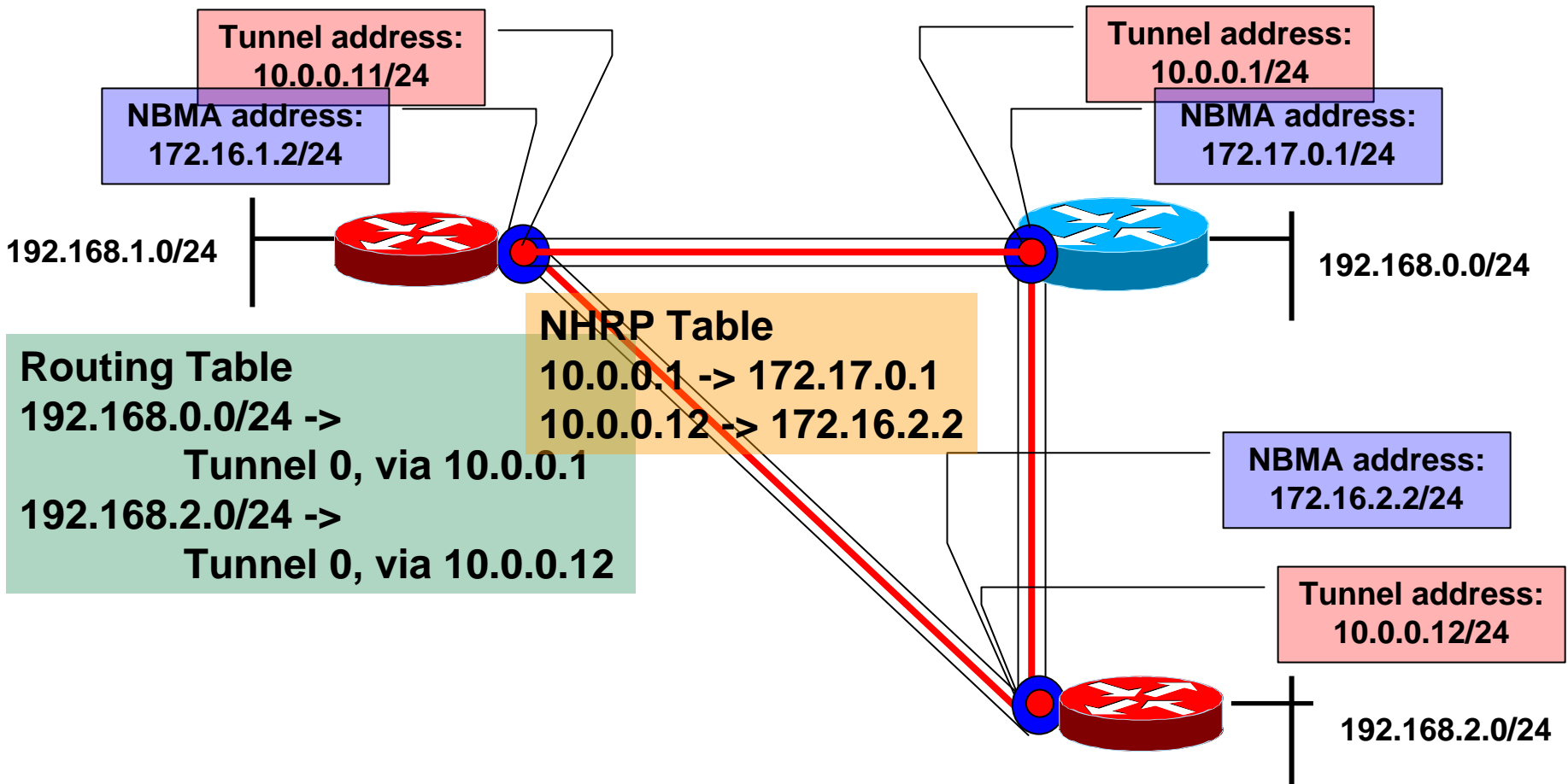
DYNAMIC MULTIPOINT VPN SPOKE TO SPOKE DIRECT TUNNELING

NOVEMBER 2004

Direct Spoke To Spoke Tunnels

- Initially, spoke to spoke traffic can only travel via the hub
- In DMVPN, spokes **can** send packets directly to another spoke, if the routing table and NHRP table are available
- This does not change the principle so far

Routes and NHRP Between Two Spokes



Learning process

- In order to create a spoke to spoke tunnel, a spoke must
 - Learn a routing entry to the destination network
 - The next hop must be the remote spoke tunnel IP address
 - The spoke must learn the NBMA address of this next hop
- The IPsec tunnel is only built after that

Route Learning

- The routing protocol is **only between the hub and the spokes**
- In order for spoke to spoke to work, the **hub must preserve and advertise the private networks next hop as advertised by the spokes themselves**

Route Learning (cont'd.)

- **RIP** keeps the next-hop information by **default**
This can not be disabled
- The next-hop preservation in **EIGRP** is **not a default**
It is turned on with the interface command
`no ip next-hop-self eigrp <as>`
- Next hop preservation in **BGP** is **a default**
It can be disabled with the BGP command
`neighbor <n> next-hop-self`
- In **OSPF**, next-hop preservation happens **naturally** except in point-to-multipoint mode

NHRP Learning

- A spoke will **send an NHRP resolution request to its NHS** to learn an NBMA address
- The queried address **can** be a network address
- Ideally, the **queried address should be a next-hop address**
- **The NHS will respond with an NBMA address from its cache**

The spoke will populate its cache with the answer

NHRP Learning (cont.)

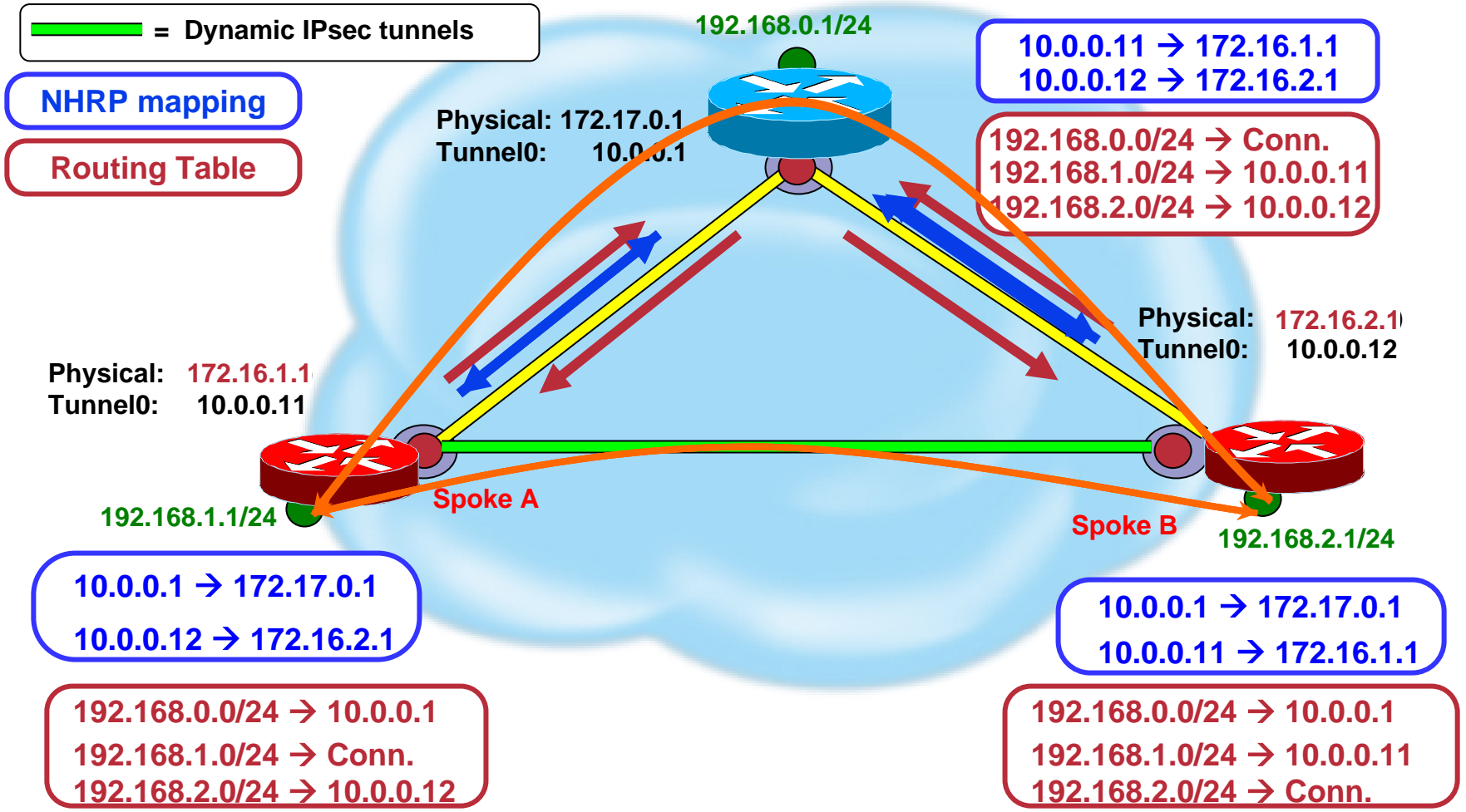
- The resolution reply will have a lifetime set to the **remaining lifetime in the hub cache**
- If the NHS does not have the entry in its cache, it returns an **error** and the spoke will install an incomplete entry and forward packets to the NHS
- During the learning process, the spoke will forward **all the packets to its NHS**

This occurs in process switching

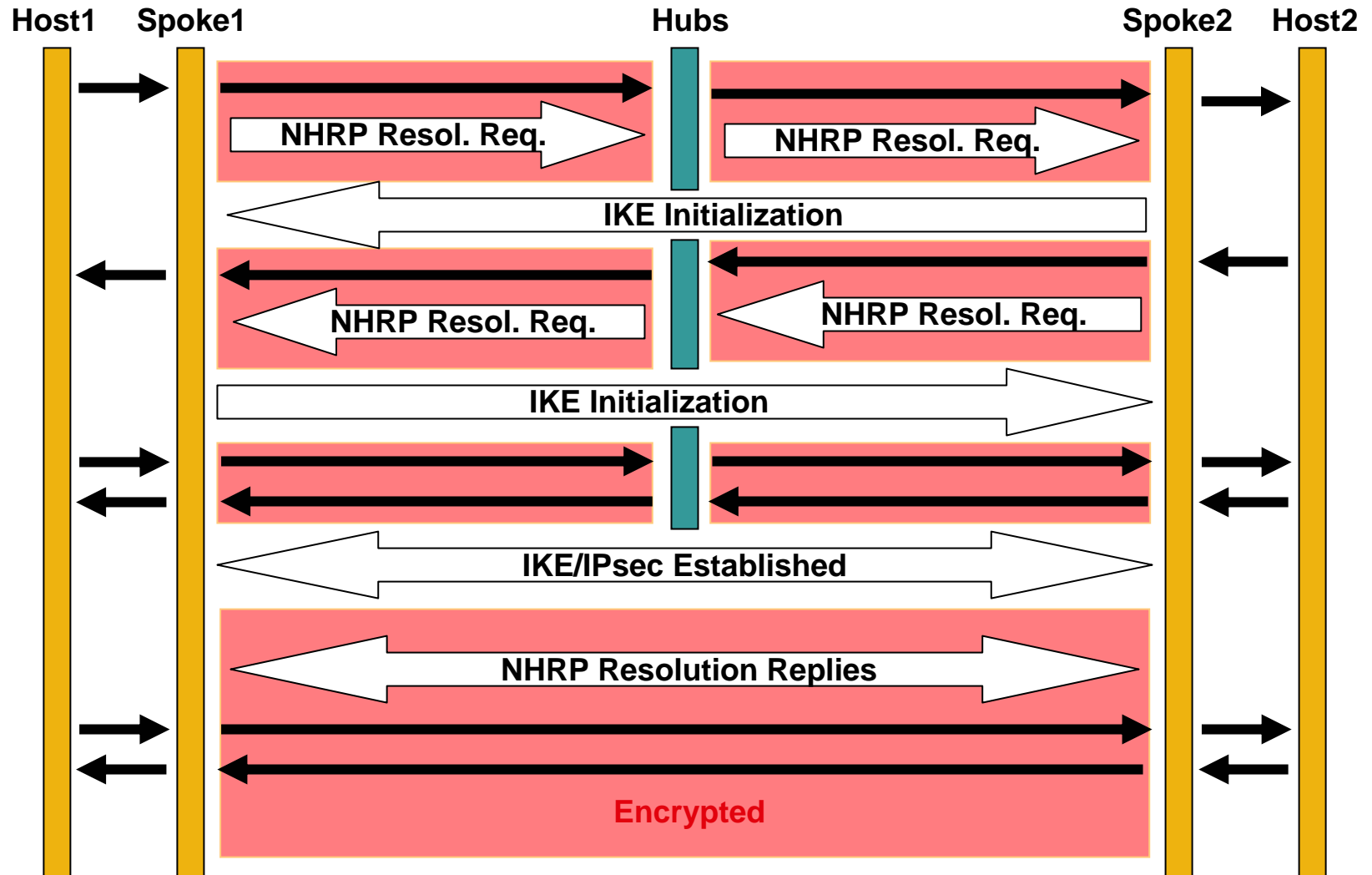
Tunnel Buildup

- As soon as the NHRP entry is created but **NOT** inserted in the cache, an IPsec tunnel will be initiated
- The NHRP entry will **be inserted in the cache and used** when the IPsec tunnel is actually ready
- The IPsec tunnel will disappear when the NHRP entry times out

NHRP Registration Dynamically Addressed Spokes



Building Spoke-to-Spoke Tunnels



IKE Call Access Control

- IKE Call Access Control (CAC) was introduced in Release 12.3(8)T
- This feature allows Cisco IOS® Software to **limit** the number of IKE/IPsec connections
- It **prevents** small platforms from opening dozens of spoke to spoke tunnels (e.g. worm attack)

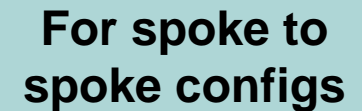
```
crypto call admission limit ike sa <number>
```

DMVPN Hub Configuration

```
crypto ca trustpoint CA
  enrollment terminal
  crl optional
  rsakeypair hub1
crypto ca certificate chain CA
  certificate 2368DB55000000000B4E
  certificate ca 1244325DE0369880465F977A18F61CA8
!
crypto isakmp policy 1
  encryption 3des
!
crypto ipsec transform-set ts esp-3des esp-sha-hmac
!
crypto ipsec profile prof
  set transform-set ts
!
interface Ethernet0/0
  ip address 192.168.0.1 255.255.255.0
!
interface Serial1/0
  ip address 172.17.0.1 255.255.255.252
```

DMVPN Hub Configuration (Cont'd.)

```
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1416
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 3600
  no ip split-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 prof
!
router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.0.0
  no auto-summary
```




For spoke to
spoke configs

DMVPN Spoke Configuration

```
crypto ca trustpoint CA
  enrollment terminal
  crl optional
  rsakeypair spokel
crypto ca certificate chain CA
  certificate 236FD380000000000B4F
  certificate ca 1244325DE0369880465F977A18F61CA8
!
crypto isakmp policy 1
  encryption 3des
!
crypto ipsec transform-set ts esp-3des esp-sha-hmac
!
crypto ipsec profile prof
  set transform-set ts
!
interface Ethernet0/0
  ip address 192.168.1.1 255.255.255.0
!
interface Serial1/0
  ip address 172.16.1.1 255.255.255.252
```

DMVPN Spoke Configuration (Cont'd.)

```
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.11 255.255.255.0
  ip mtu 1416
  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 3600
  ip nhrp nhs 10.0.0.1
  ip nhrp server-only
  delay 1000
  tunnel source Serial1/0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile prof
!
router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.1.0
  no auto-summary
```



For pure hub and spoke

Recommendation

- The use of wildcard pre-shared keys is strongly **discouraged**
- With such topologies, it is recommended to use a **Public Key Infrastructure (PKI)** to authenticate nodes

CISCO SYSTEMS

