Advanced Concepts of Dynamic Multipoint VPN (DMVPN)

BRKSEC-4012

Agenda

For Your Reference

- DMVPN Overview
- NHRP Details
  - NHRP Overview
  - NHRP Registrations
  - NHRP Resolutions/Redirects
    - Phase 2
    - Phase 3
- Network Virtualization
  - VRF-lite
  - 2547oDMVPN
- Interaction with other Features
  - NAT, IPv6, Per-tunnel QoS

DMVPN Overview

What is Dynamic Multipoint VPN?

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

DMVPN: Major Features

- Configuration reduction and no-touch deployment
- Supports:

  IP unicast, IP multicast and dynamic Routing Protocols.

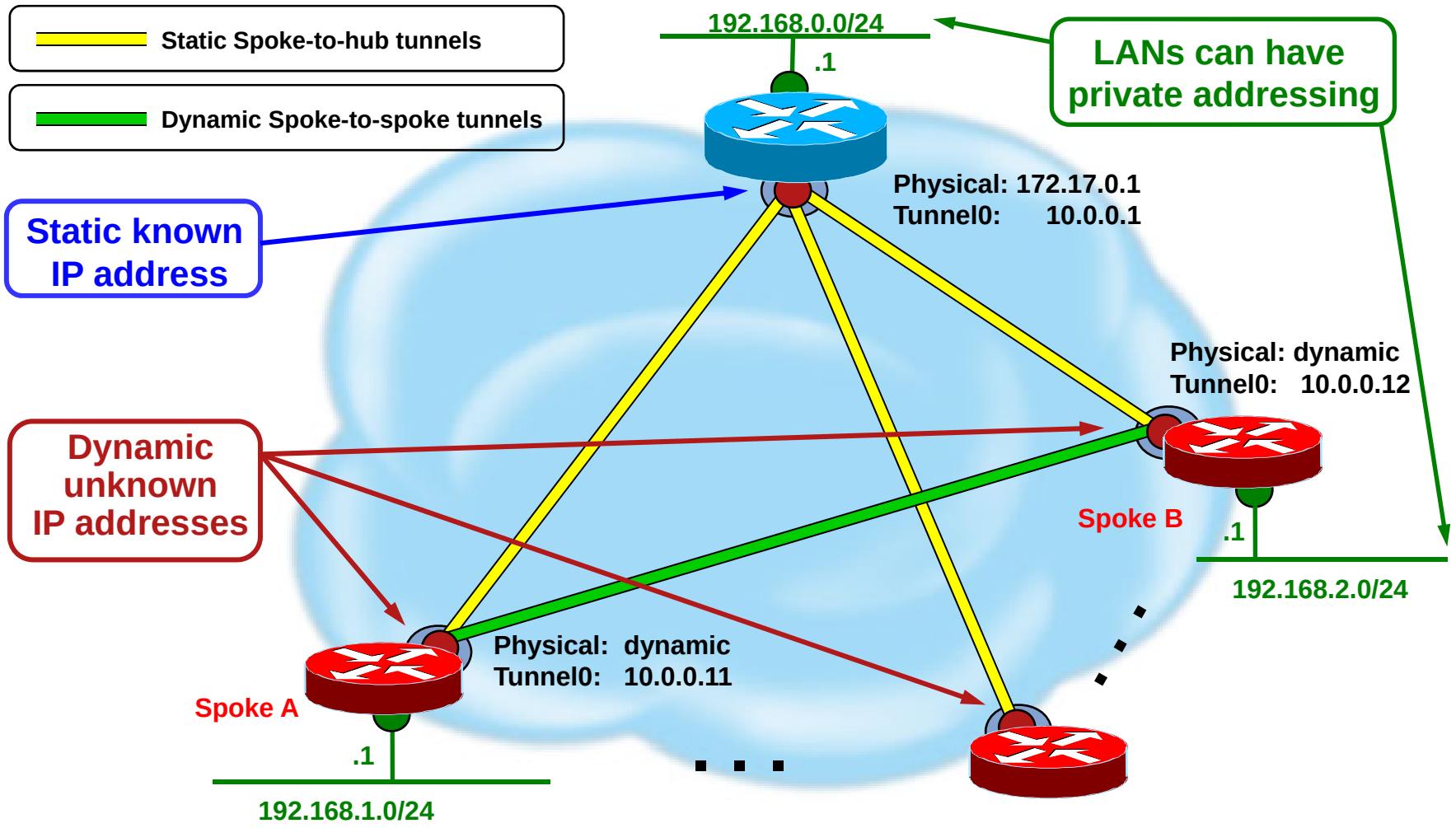
  Remote peers with dynamically assigned addresses.

  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
- Works with MPLS; GRE tunnels and/or data packets in VRFs and MPLS switching over the tunnels.
- Wide variety of network designs and options.

DMVPN: How it works

- Spokes build a dynamic permanent GRE/IPsec tunnel to the hub, but not to other spokes. They register as clients of the NHRP server (hub).
- When a spoke needs to send a packet to a destination (private) subnet behind another spoke, it queries via NHRP 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 dynamic spoke-to-spoke tunnel is built over the mGRE interface.
- When traffic ceases then the spoke-to-spoke tunnel is removed.

DMVPN: Example



NHRP Main Functionality

- NHRP Registrations

  Spoke (NHC) dynamically register its VPN to NBMA address mapping with hub (NHS).

    Static NHRP mappings on spokes for Hub (NHS)

    Needed to “start the game”

    Builds hub-and-spoke control plane network

- NHRP Resolutions

  Dynamically resolve spoke to spoke VPN to NBMA mapping to build spoke-spoke tunnels.

  Single instead of multiple tunnel hops across NBMA network

  NHRP Resolution requests/replies sent via hub-and-spoke control plane path

DMVPN and IPsec

- IPsec integrated with DMVPN, but not required
- Packets Encapsulated in GRE, then Encrypted with IPsec
- NHRP controls the tunnels, IPsec does encryption
- Bringing up a tunnel
  - NHRP signals IPsec to setup encryption
  - ISAKMP authenticates peer, generates SAs
  - IPsec responds to NHRP and the tunnel is activated
  - All NHRP and data traffic is Encrypted
- Bringing down a tunnel
  - NHRP signals IPsec to tear down tunnel
  - IPsec can signal NHRP if encryption is cleared or lost
- ISAKMP Keepalives monitor state of spoke-spoke tunnels

Routing

- Spokes are only routing neighbors with hubs, not with other spokes
  - Spokes advertise local network to hubs
- Hubs are routing neighbors with spokes
  - Collect spoke network routes from spokes
  - Advertise spoke and local networks to all spokes
  - All Phases:
    - Turn off split-horizon (EIGRP, RIP)
    - Single area and no summarization when using OSPF
  - Phase 1 & 3:
    - Hubs can not preserve original IP next-hop; Can Summarize
      - EIGRP, BGP (next-hop-self); RIP, ODR (default)
      - OSPF (network point-multipoint); # hubs not limited
  - Phase 2:
    - Hubs must preserve original IP next-hop; Cannot summarize
      - EIGRP (no ip next-hop-self); BGP (default)
      - OSPF (network broadcast); Only 2 hubs
- Hubs are routing neighbors with other hubs and local network
  - Phase1 & 3: Can use different routing protocol than hub-spoke tunnels
  - Phase 2: Must use same routing protocol as hub-spoke tunnels

Routing Table Example (Spoke)

Phase 1 & 3
(with summarization)

```
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
```

Phase 1 & 3
(without summarization)

```
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 [90/297372416] via 10.0.0.1, 00:02:36, Tunnel0
C   192.168.1.0/24 is directly connected, Ethernet0/0
D    192.168.2.0/24 [90/297321216] via 10.0.0.1, 00:02:36, Tunnel0
D    192.168.3.0/24 [90/297321216] via 10.0.0.1, 00:02:36, Tunnel0
. . .
S*   0.0.0.0/0 [1/0] via 172.16.1.1
```

Phase 2
(no summarization)

```
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 [90/297372416] via 10.0.0.1, 00:42:34, Tunnel0
C   192.168.1.0/24 is directly connected, Ethernet0/0
D    192.168.2.0/24 [90/297321216] via 10.0.0.12, 00:42:34, Tunnel0
D    192.168.3.0/24 [90/297321216] via 10.0.0.13, 00:42:34. Tunnel0
. . .
S*   0.0.0.0/0 [1/0] via 172.16.1.1
```

Redundancy

- Active-active redundancy model – two or more hubs per spoke
  - All configured hubs are active and are routing neighbors with spoke
  - Routing protocol routes are used to determine traffic forwarding
    - Single route: one tunnel (hub) at a time – primary/backup mode
    - Multiple routes: both tunnels (hubs) – load-balancing mode
- ISAKMP/IPsec
  - Cannot use IPsec Stateful failover (NHRP isn't supported)
  - ISAKMP invalid SPI recovery is not useful with DMVPN
  - ISAKMP keepalives on spokes for timely hub recovery
    - crypto isakmp keepalives *initial retry*
- Can use single or multiple DMVPNs for redundancy
  - Each mGRE interface is a separate DMVPN network using different tunnel key, NHRP network-id and IP subnet
  - Can "glue" mGRE interfaces into same DMVPN network(*) same tunnel source, NHRP network-id and authentication; no tunnel key and different IP subnet (Phase 3 only)
  - If using same tunnel source (must use tunnel key)
    - tunnel protection ipsec profile *name* shared

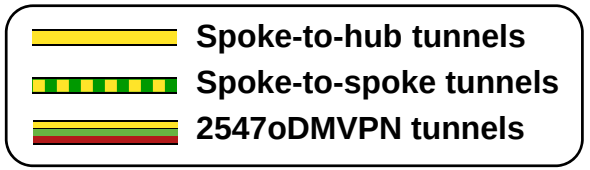
Redundancy (cont)

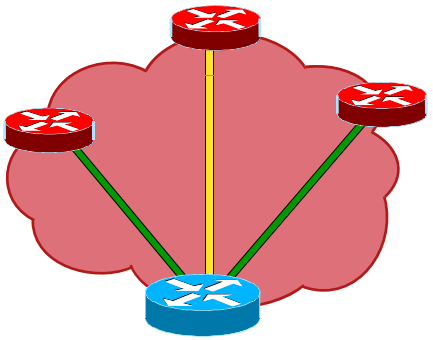
- Spokes – at least two hubs (NHSs)
  - Phase 1: (Hub-and-spoke)
    - p-pGRE interfaces → two DMVPN networks, one hub on each
  - Phase 1, 2 or 3: (Hub-and-spoke or Dynamic Mesh)
    - mGRE interface → one DMVPN network, two hubs
- Hubs – interconnect and routing
  - Phase 1: (Hub and spoke only)
    - Interconnect hubs directly over physical link, p-pGRE or mGRE
    - Hubs can exchange routing through any of these paths
  - Phase 2: (Dynamic Mesh)
    - Hubs must exchange routing over DMVPN network
    - Hubs point to other hubs as NHSs in a daisy-chain
  - Phase 3: (Dynamic Mesh)
    - Interconnect hubs over same or different mGRE (same DMVPN)
    - Hubs must exchange routing over DMVPN network

Network Designs

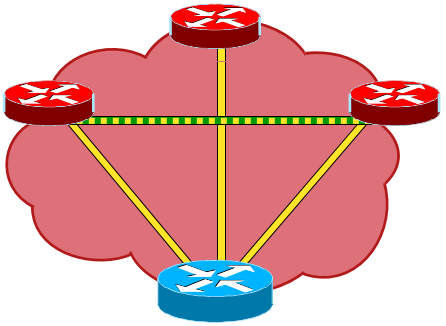
- Hub-and-spoke – Order(n)
  - Spoke-to-spoke traffic via hub
    - Phase 1: Hub bandwidth and CPU limit VPN
    - SLB: Many “identical” hubs increase CPU limit
- Spoke-to-spoke – Order(n) « Order(n^2)
  - Control traffic — Hub and spoke; Hub to hub
    - Phase 2: (single)
    - Phase 3: (hierarchical)
  - Unicast Data traffic — Dynamic mesh
    - Spoke routers support spoke-hub and spoke-spoke tunnels currently in use.
    - Hub supports spoke-hub traffic and overflow from spoke-spoke traffic.
- Network Virtualization
  - VRF-lite – Multiple DMVPNs
  - MPLS over DMVPN (2547oDMVPN) – Single DMVPN

Network Designs

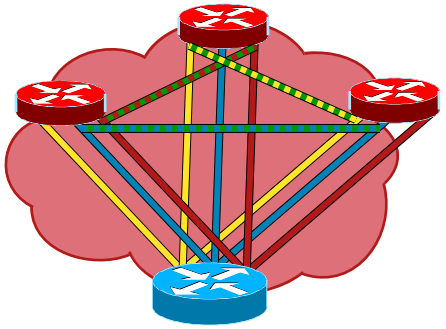




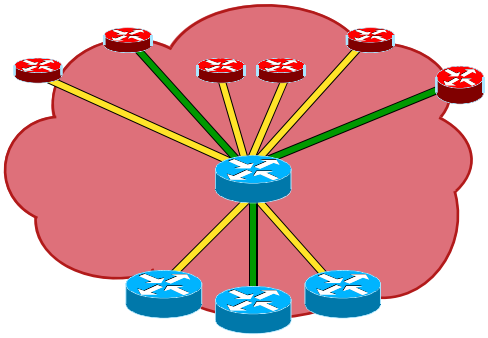
Hub and spoke (Phase 1)



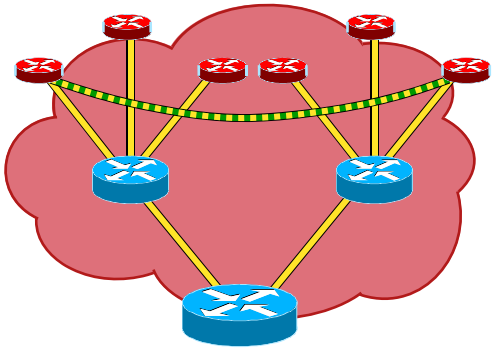
Spoke-to-spoke (Phase 2)



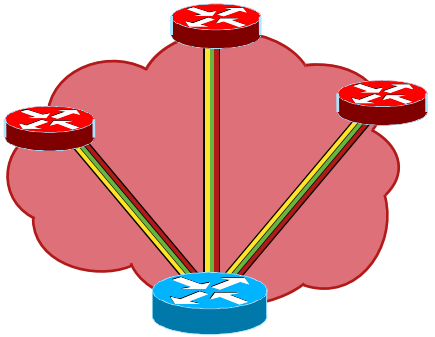
VRF-lite



Server Load Balancing



Hierarchical (Phase 3)



2547oDMVPN

Hub-and-Spoke
Functionality

- GRE, NHRP and IPsec configuration
  - p-pGRE or mGRE on spokes; mGRE on hubs
  - ISAKMP Authentication (PKI, PSK, wildcard PSK)
- NHRP Registration
  - Static NHRP mapping for Hub on Spoke
  - Dynamically learn NHRP mapping for Spoke on Hub
    - Dynamically addressed spokes (DHCP, NAT , …)
  - NAT detection support

Dynamic Mesh (Spoke-Spoke Tunnels) Functionality

- mGRE/NHRP+IPsec configuration
  - On both hub and spokes
  - ISAKMP authentication information
    - Certificates, wildcard pre-shared keys (not secure)
- Spoke-spoke data traffic direct
  - Reduced load on hub
  - Reduced latency
    - Single IPsec encrypt/decrypt
  - NAT support
- NHRP Resolutions (Phase 2)
- NHRP Redirect and Resolutions (Phase 3)

Dynamic Mesh (Spoke-Spoke Tunnels) Considerations

- Resiliency
  - No monitoring of spoke-spoke tunnel (use ISAKMP keepalives)
    - crypto isakmp keepalives *initial retry*
- Path Selection
  - NHRP will always build spoke-spoke tunnel
  - No latency or performance measurement of spoke-spoke vs spoke-hub-spoke paths
- Overloading spoke routers
  - CPU or memory → IKE Call Admission Control (CAC)
    - crypto call admission limit ike {sa | in-negotiation } *max-SAs*
    - call admission limit *percent*
    - show crypto call admission statistics
  - Bandwidth → Design for expected traffic
    - Hub-spoke versus Spoke-spoke
    - Spoke-spoke availability is best effort

NHRP Details

Agenda

- DMVPN Overview
- NHRP Details
  - NHRP Overview
  - NHRP Registrations
  - NHRP Resolutions/Redirects
    - Phase 2
    - Phase 3
- Network Virtualization
  - VRF-lite
  - 2547oDMVPN
- Interaction with other Features
  - NAT, IPv6, Per-tunnel QoS

NHRP Message Types

- Registration

  Build base (hierarchical – Phase 3) hub-and-spoke network for control traffic, also used for data traffic

- Resolution

  Get mapping to build dynamic spoke-spoke tunnels

- Traffic Indication (Redirect) – New for Phase 3

  Trigger resolution requests at previous GRE tunnel hop

- Purge

  Clear out stale dynamic NHRP mappings

- Error

  Signal error conditions

NHRP Message Extension Types

- Responder Address Extension:

  Address mapping for Responding node (Reply messages)

- Forward Transit NHS Record Extension:

  List NHSs that NHRP request message traversed
  – copied to reply message

- Reverse Transit NHS Record Extension:

  List of NHSs that NHRP reply message traversed

- Authentication Extension:

  NHRP Authentication

- NAT Address Extension: (new)

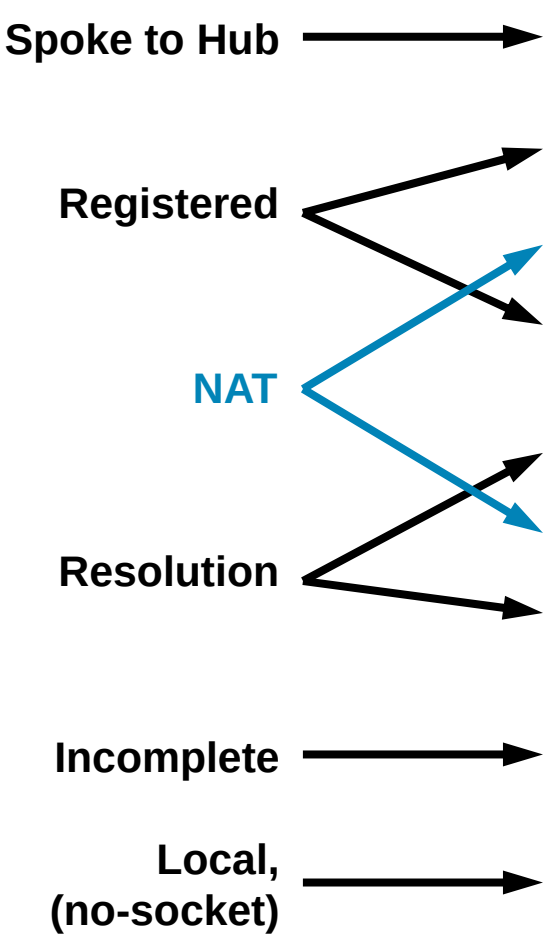
  Address mapping for peer (Registration message)

  Address mapping for self (Resolution request/reply)

NHRP Mapping Entries

- **Static**
  - Both host (/32) and network (/<x>) mappings
- **Dynamic**
  - **Registered**
    - From NHRP Registration (/32)
    - NAT – record both inside and outside NAT address
  - **Learned**
    - From NHRP Resolution (/32 or /<x>)
    - NAT – record both inside and outside NAT address
- **Incomplete**
  - When sending NHRP resolutions
  - Host mapping entry
- **Local**
  - Mapping for local network sent in an NHRP Resolution Reply
  - Record which nodes were sent this mapping
- **(no socket)**
  - Not used to forward data packets
  - Do not trigger IPsec encryption

NHRP Mapping Entries




```
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:20:10, never expire
  Type: static, Flags: used
  NBMA address: 172.17.0.9

10.0.0.18/32 via 10.0.0.18, Tunnel0 created 00:16:09, expire 00:05:50
  Type: dynamic, Flags: unique registered used
  NBMA address: 172.18.0.2
    (Claimed NBMA address: 172.16.2.1)

10.0.0.19/32 via 10.0.0.19, Tunnel0 created 01:20:08, expire 00:05:51
  Type: dynamic, Flags: unique registered used
  NBMA address: 172.16.3.1

10.0.0.18/32 via 10.0.0.18, Tunnel0 created 00:09:04, expire 00:00:22
  Type: dynamic, Flags: router implicit
  NBMA address: 172.18.0.2
    (Claimed NBMA address: 172.16.2.1)

192.168.23.0/24 via 10.0.0.19, Tunnel0 created 00:00:11, expire 00:05:48
  Type: dynamic, Flags: router used
  NBMA address: 172.16.3.1

10.0.0.45/32, Tunnel0 created 00:00:21, expire 00:02:43
  Type: incomplete, Flags: negative
  Cache hits: 2

192.168.15.0/24 via 10.0.0.11, Tunnel0 created 00:05:39, expire 00:05:50
  Type: dynamic, Flags: router unique local
  NBMA address: 172.16.1.1
    (no-socket)
```

NHRP Mapping flags

- **unique**
  Mapping (VPN IP → NBMA IP) is unique, don't allow overwrite with new NBMA
- **registered**
  Mapping entry from an NHRP registration
- **authoritative**
  Mapping entry can be used to answer NHRP resolution requests
- **used**
  Mapping entry was used in last 60 seconds to forward data traffic
- **router**
  Mapping entry for remote router
- **implicit**
  Mapping entry from source information in NHRP packet
- **local**
  Mapping entry for a local network, record remote requester
- **nat** **(new as of 12.4(6)T, not shown after 12.4(15)T)**
  Remote peer supports the new NHRP NAT extention

NHRP Purge Messages

- Used to clear invalid NHRP mapping information from the network
- NHRP “local” mapping entries
  - Created when sending an NHRP resolution reply
  - Copy of mapping information sent in reply
  - Entry tied to corresponding entry in routing table
  - Keeps list of nodes where resolution reply was sent
- If routing table changes so that local mapping entry is no longer valid
  - Purge message is sent to each NHRP node in list
  - NHRP nodes clear that mapping from their table
  - Purge messages forwarded over direct tunnel if available, otherwise sent via routed path

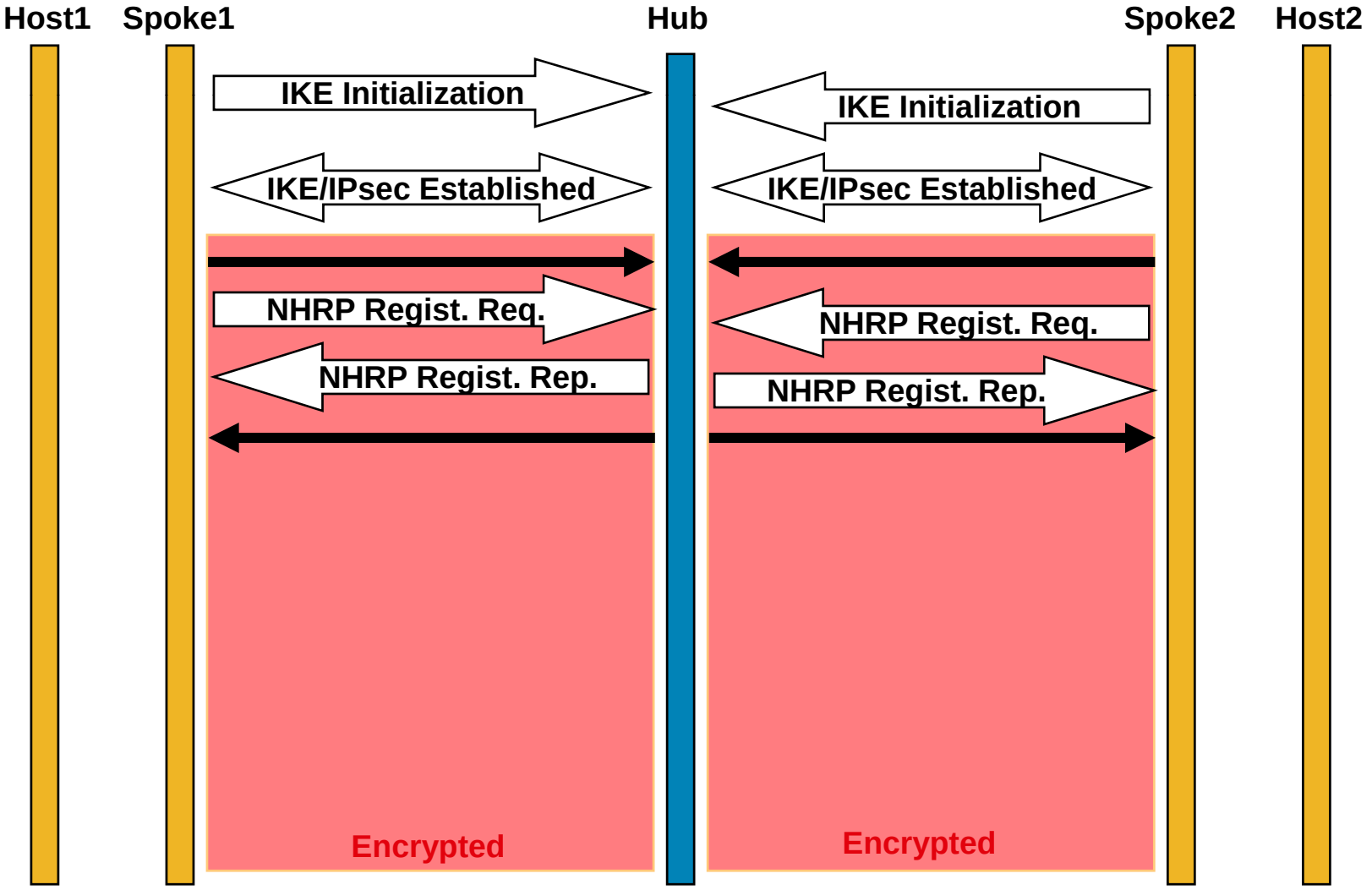
Agenda

- DMVPN Overview
- NHRP Details
  - NHRP Overview
  - NHRP Registrations
  - NHRP Resolutions/Redirects
    - Phase 2
    - Phase 3
- Network Virtualization
  - VRF-lite
  - 2547oDMVPN
- Interaction with other Features
  - NAT, IPv6, Per-tunnel QoS

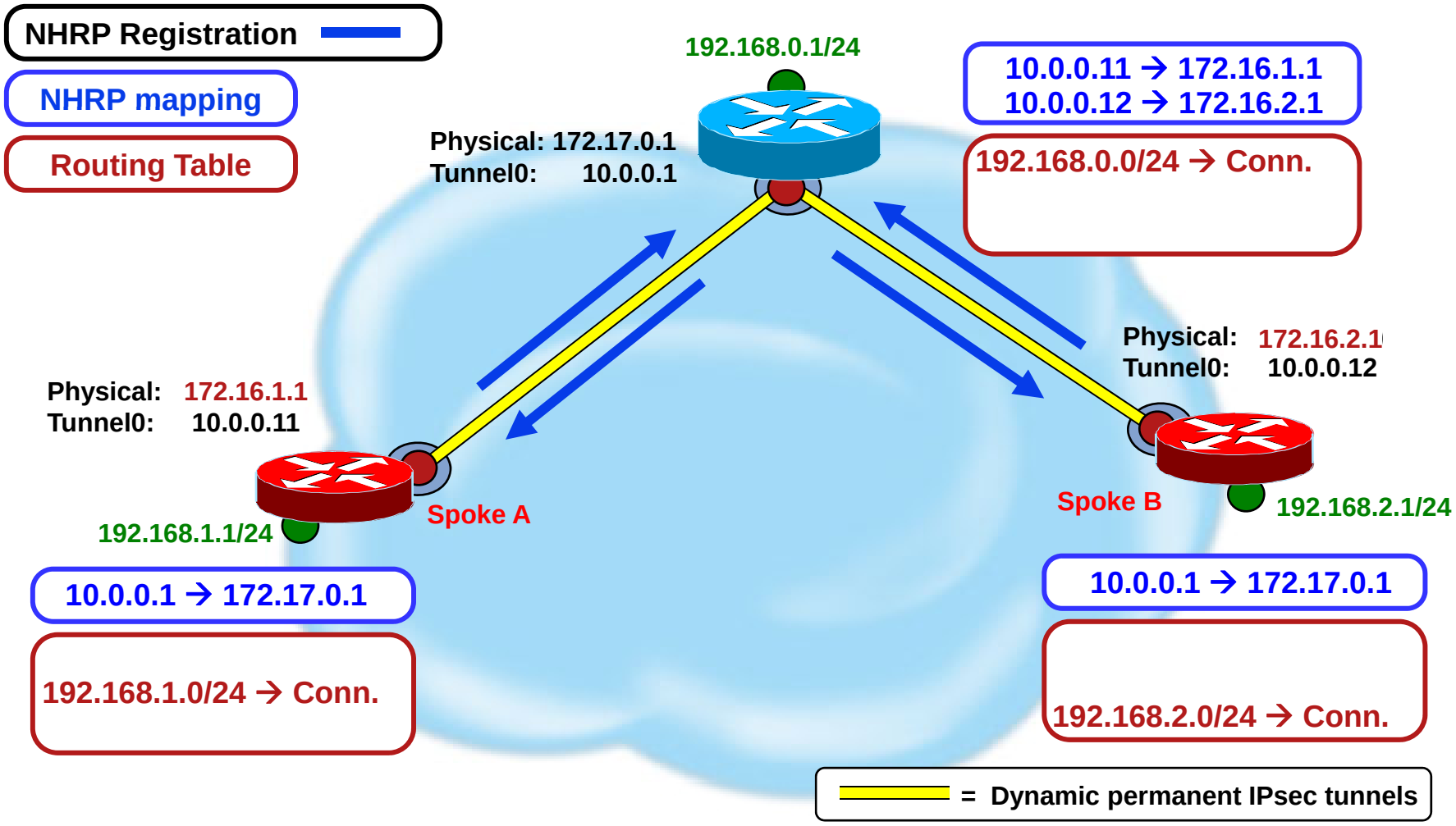
NHRP Registration

- Builds base hub-and-spoke network
  - Hub-and-spoke data traffic
  - Control traffic; NHRP, Routing protocol, IP multicast
  - Phase 2 – Single level hub-and-spoke
  - Phase 3 – Hierarchical hub-and-spoke (tree).
- Next Hop Client (NHC) has static mapping for Next Hop Servers (NHSs)
- NHC dynamically registers own mapping with NHS
  - Supports spokes with dynamic NBMA addresses or NAT
- NHS registration reply gives liveliness of NHS
  - Supplies outside NAT address of spoke

NHRP Registration
Building Spoke-Hub Tunnels



NHRP Registration
Building Spoke-Hub Tunnels



NHRP Registration Request

- Spoke to hub
  - Every ⅓ 'ip nhrp holdtime' or 'ip nhrp registration timeout'
    - If no reply, retransmit after 1, 2, 4, 8, 16, 32, 64, 64 ,… sec., mark Hub down after 3rd retransmit
- Contains Spoke's VPN to NBMA mapping
  - Extension headers
    - Responder Address, Forward and Reverse Transit NHS, Authentication, NAT

NHRP: Send Registration Request via Tunnel0 vrf 0, src: 10.0.0.11, 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", src NBMA: 172.16.1.1, src protocol: 10.0.0.11, dst protocol: 10.0.0.1
(C-1) code: no error(0), prefix: 255, mtu: 1514, hd_time: 360
Responder Address Extension(3):
Forward Transit NHS Record Extension(4):
Reverse Transit NHS Record Extension(5):
Authentication Extension(7): type:Cleartext(1), data:test
NAT Address Extension(9): (C-1) prefix: 32, client NBMA: 172.17.0.1, client protocol: 10.0.0.1

NHRP Registration Reply

- Hub to spoke
  - Liveliness of Hub
- Contains
  - Spoke's VPN to NBMA mapping
  - Hub's VPN to NBMA mapping as responder
  - Extension headers
    - Responder Address, Forward and Reverse Transit NHS, Authentication,NAT

```
NHRP: Send Registration Reply via Tunnel0 vrf 0, 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", src NBMA: 172.16.1.1, src protocol: 10.0.0.11, dst protocol: 10.0.0.1
  (C-1) code: no error(0), prefix: 255, mtu: 1514, hd_time: 360
Responder Address Extension(3):
  (C) prefix: 0, client NBMA: 172.17.0.1, client protocol: 10.0.0.1
Forward Transit NHS Record Extension(4):
Reverse Transit NHS Record Extension(5):
Authentication Extension(7): type:Cleartext(1), data:test
NAT Address Extension(9): (C-1) prefix: 32, client NBMA: 172.17.0.1, client protocol: 10.0.0.1
```

NHRP Mapping Tables
After Registration

Hub

```
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 00:11:03, expire 00:04:52
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 172.16.1.1

10.0.0.12/32 via 10.0.0.12, Tunnel0 created 01:03:31, expire 00:05:46
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 172.16.2.1
. . .
```

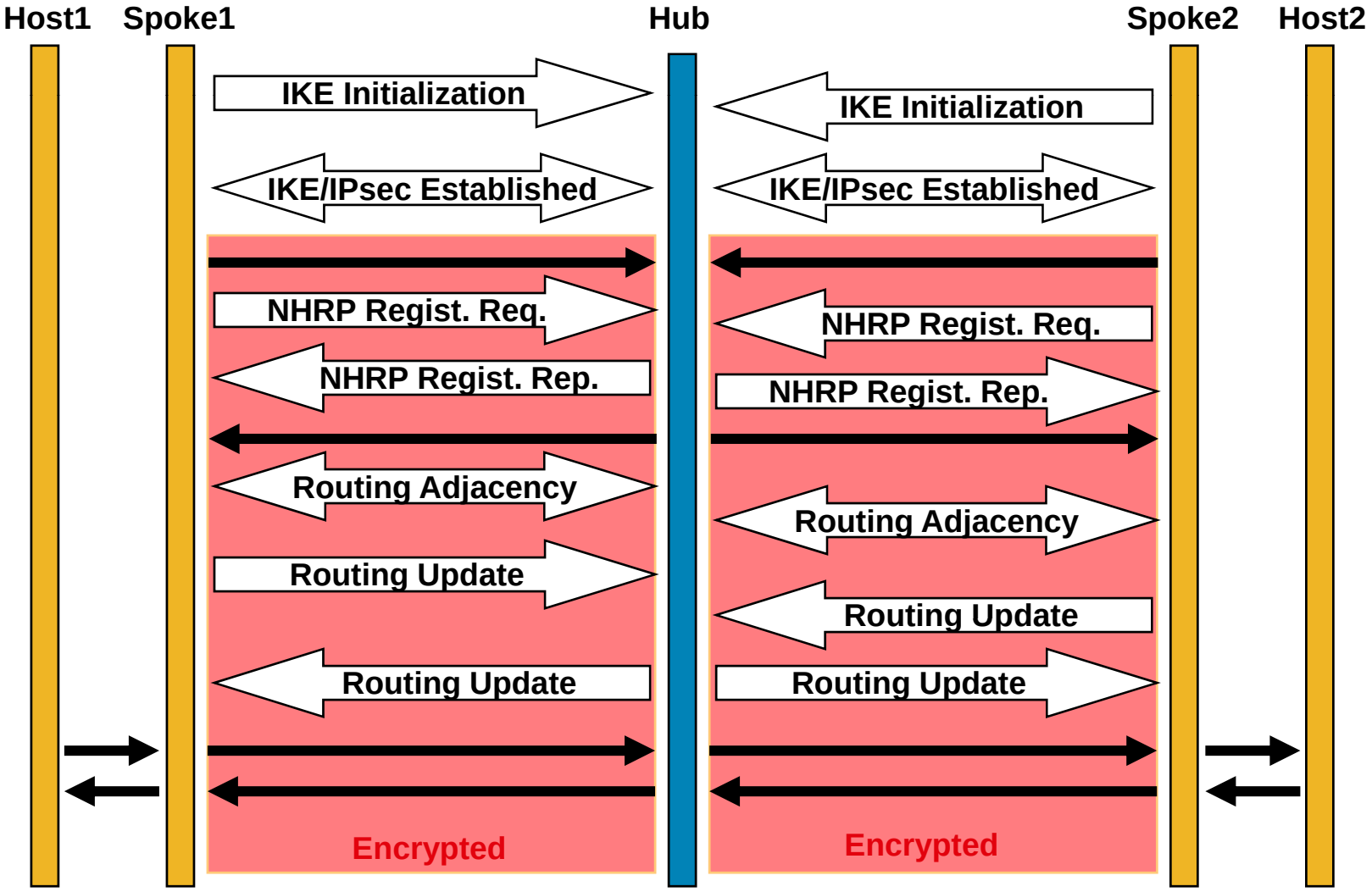
Spoke A

```
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:03:37, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
```

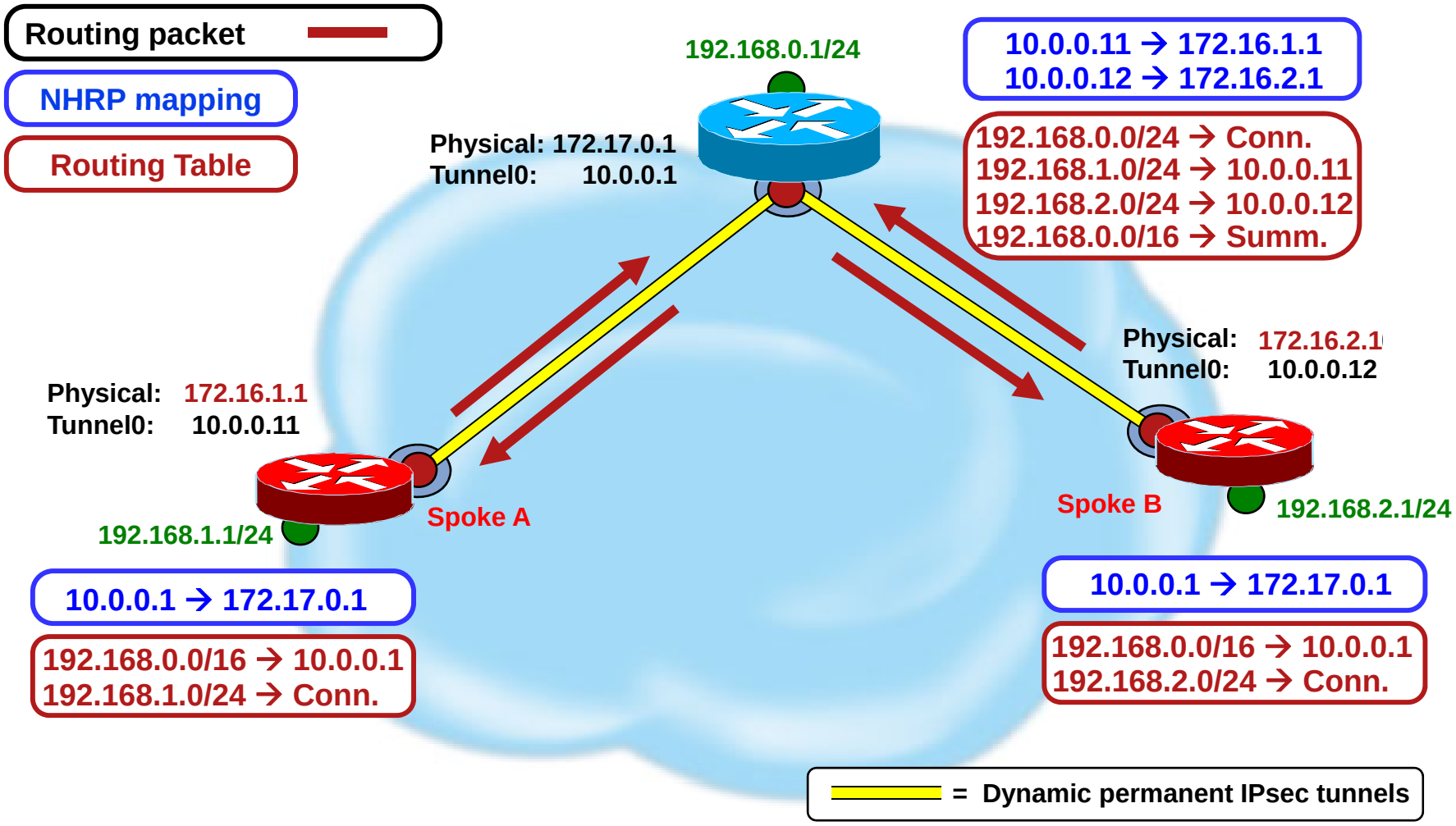
Spoke B

```
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:02:21, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
```

NHRP Registration (cont)
Routing Adjacency



NHRP Registration (cont)
Routing Adjacency



Hub-and-Spoke
Data Packet Forwarding

- Process-switching
  - Routing table selects outgoing interface and IP next-hop
  - NHRP looks up packet IP destination to select IP next-hop, overriding IP next-hop from routing table.
    - Could attempt to trigger spoke-spoke tunnel
      - 'tunnel destination …' → Can only send to hub
      - 'ip nhrp server-only' → Don't send NHRP resolution request
  - If no matching NHRP mapping then send to NHS (hub)
- CEF switching
  - IP Next-hop from FIB table (Routing table)
    - IP Next-hop → Hub ➔ data packets send to Hub
  - Adjacency will be complete so CEF switch packet to hub
    - NHRP not involved

Agenda

- DMVPN Overview
- NHRP Details
  - NHRP Overview
  - NHRP Registrations
  - NHRP Resolutions/Redirects
    - Phase 2
    - Phase 3
- Network Virtualization
  - VRF-lite
  - 2547oDMVPN
- Interaction with other Features
  - NAT, IPv6, Per-tunnel QoS

Phase 2
Building Spoke-spoke Tunnels

- IP Data packet is forwarded out tunnel interface to IP next-hop from routing table
- NHRP looks in mapping table for IP destination
  - If (socket) Entry Found
    - Forward to NBMA from mapping table – overriding IP next-hop
  - If (no socket) Entry Found
    - If arriving interface is not tunnel interface – convert entry to (socket)
    - Trigger IPsec to bring up crypto socket
    - Forward to IP next-hop (if in NHRP table) otherwise to NHS
  - If No Entry Found
    - Forward to IP next-hop (if in NHRP table) otherwise to NHS
    - If arriving interface was not tunnel interface
      - Initiate NHRP Resolution Request for IP destination

Phase 2
Sending NHRP Resolutions

- CEF FIB table has IP next-hop of tunnel IP address of remote spoke for network behind remote spoke
- Triggered by IP next-hop from FIB pointing to glean or incomplete adjacency entry (no valid adjacency entry)
- Send resolution request for IP next-hop (tunnel IP address) of remote Spoke
- Resolution request forwarded via NHS path
- Phase 2 (old) – see appendix

  Resolution request answered by last NHS in path

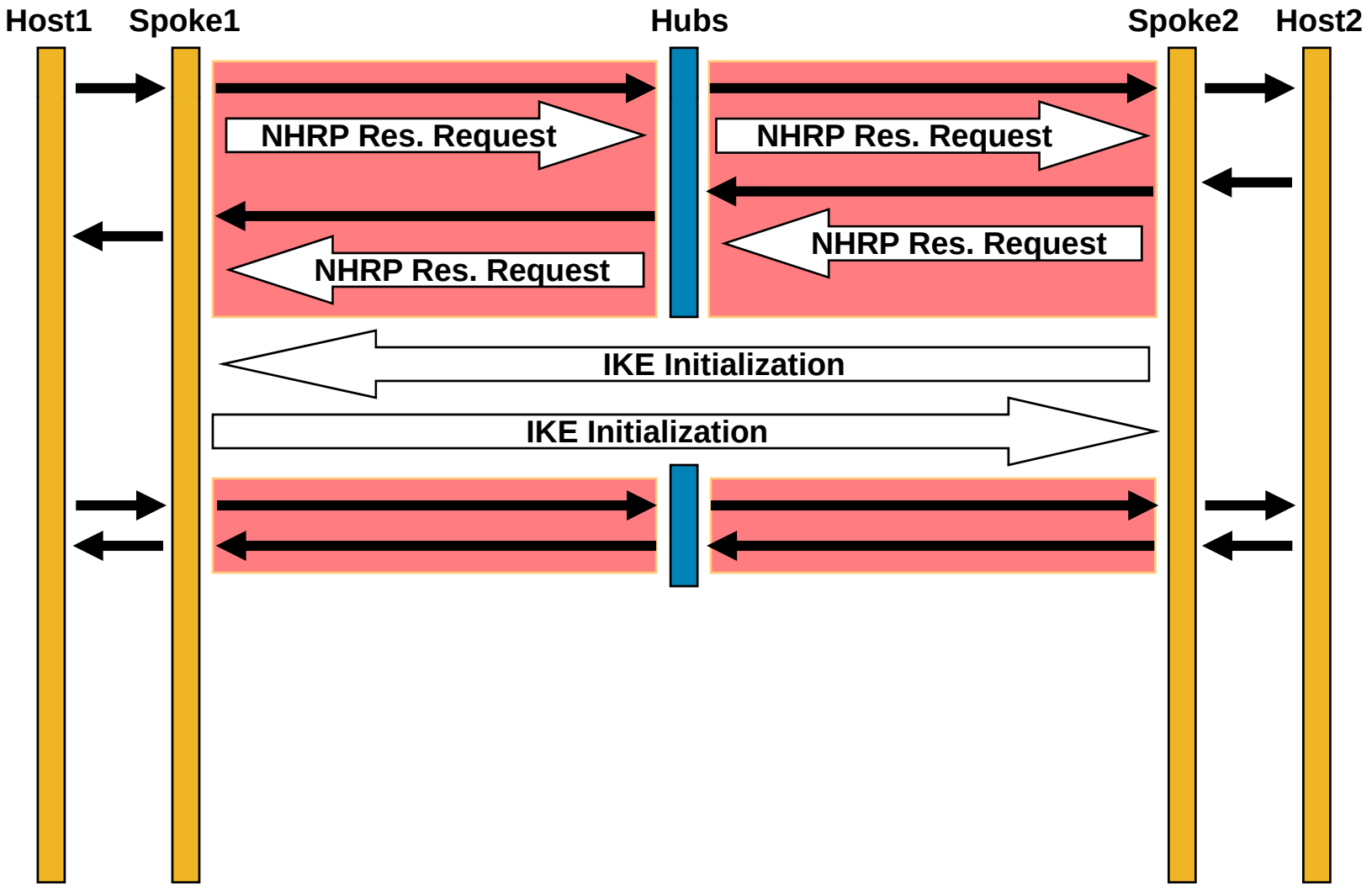
  Resolution reply forwarded back via NHS path

  Data packets forwarded (process-switched) on NHS path until last tunnel hop then CEF switched while bringing up spoke-spoke tunnel

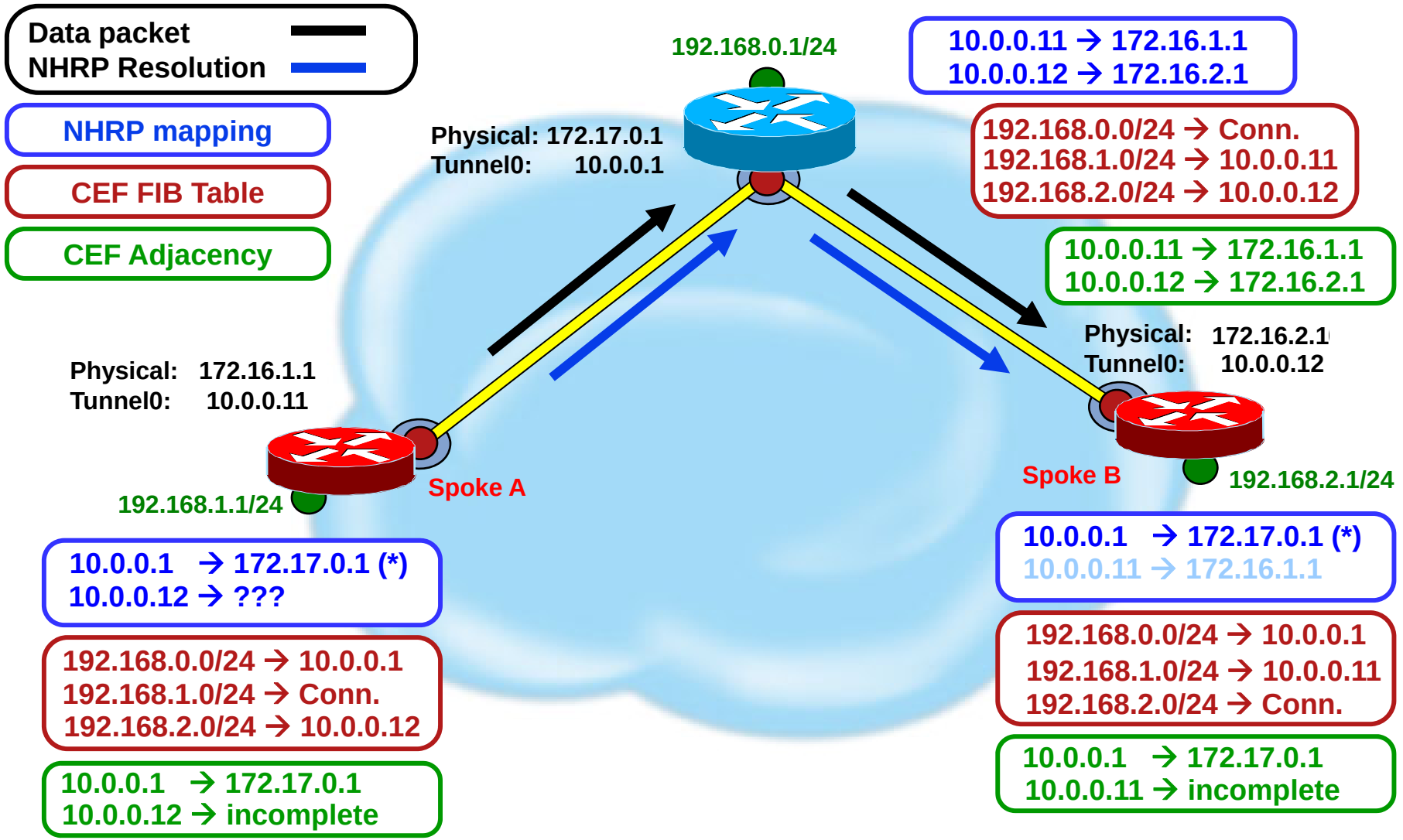
Phase 2 (new)
NHRP Resolution process changes

- When:
  - 12.4(6)T, 12.4(5a), 12.4(7) and later (not on 6500/7600 yet)
- Why:
  - To Support spoke-spoke tunnels when spokes are behind NAT
- How:
  - Registered NHRP mappings on hub are **not** marked Authoritative
- Effect:
  - Resolution request will be forwarded via NHS path **all** the way to the remote spoke
  - Resolution request is answered by the remote spoke
  - Spoke-spoke tunnel is built
  - Resolution reply forwarded back via spoke-spoke tunnel

Phase 2
NHRP Resolution Request



Phase 2
NHRP Resolution Request



Phase 2
NHRP Resolutions Request Message

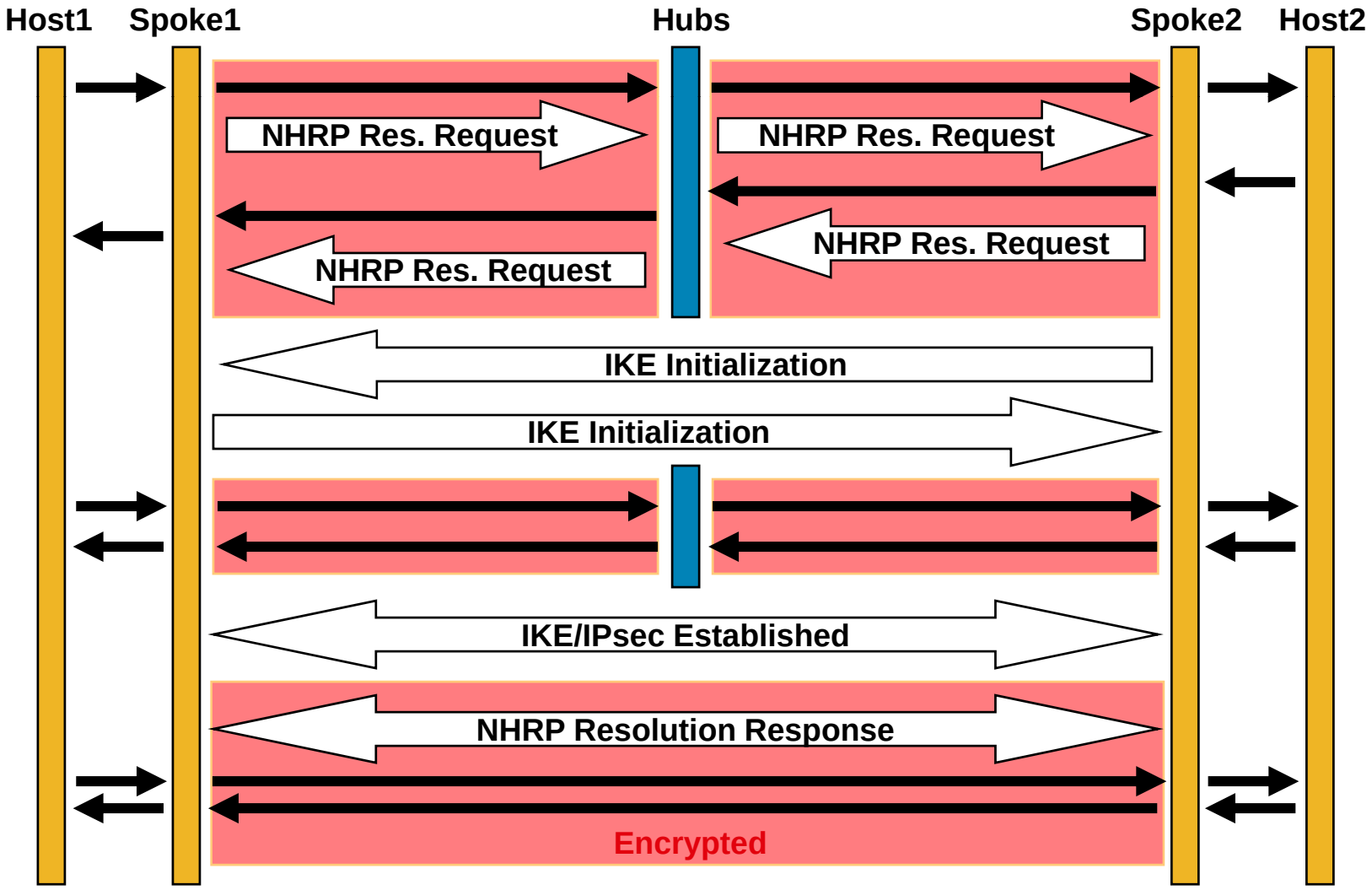
NHRP: Send Resolution Request via Tunnel0 vrf 0, packet size: 84, **src: 10.0.0.11, dst: 10.0.0.1**
(F) afn: IPv4(1), type: IP(800), **hop: 255**, ver: 1, shtl: 4(NSAP), sstl: 0(NSAP)
(M) flags: "router auth src-stable nat ", reqid: 164
src NBMA: 172.16.1.1, src protocol: 10.0.0.11, dst protocol: 10.0.0.12
(C-1) code: no error(0) prefix: 0, mtu: 1514, hd_time: 360
Responder Address Extension(3):
Forward Transit NHS Record Extension(4):
Reverse Transit NHS Record Extension(5):
Authentication Extension(7): type:Cleartext(1), data:test
NAT address Extension(9):

As Sent

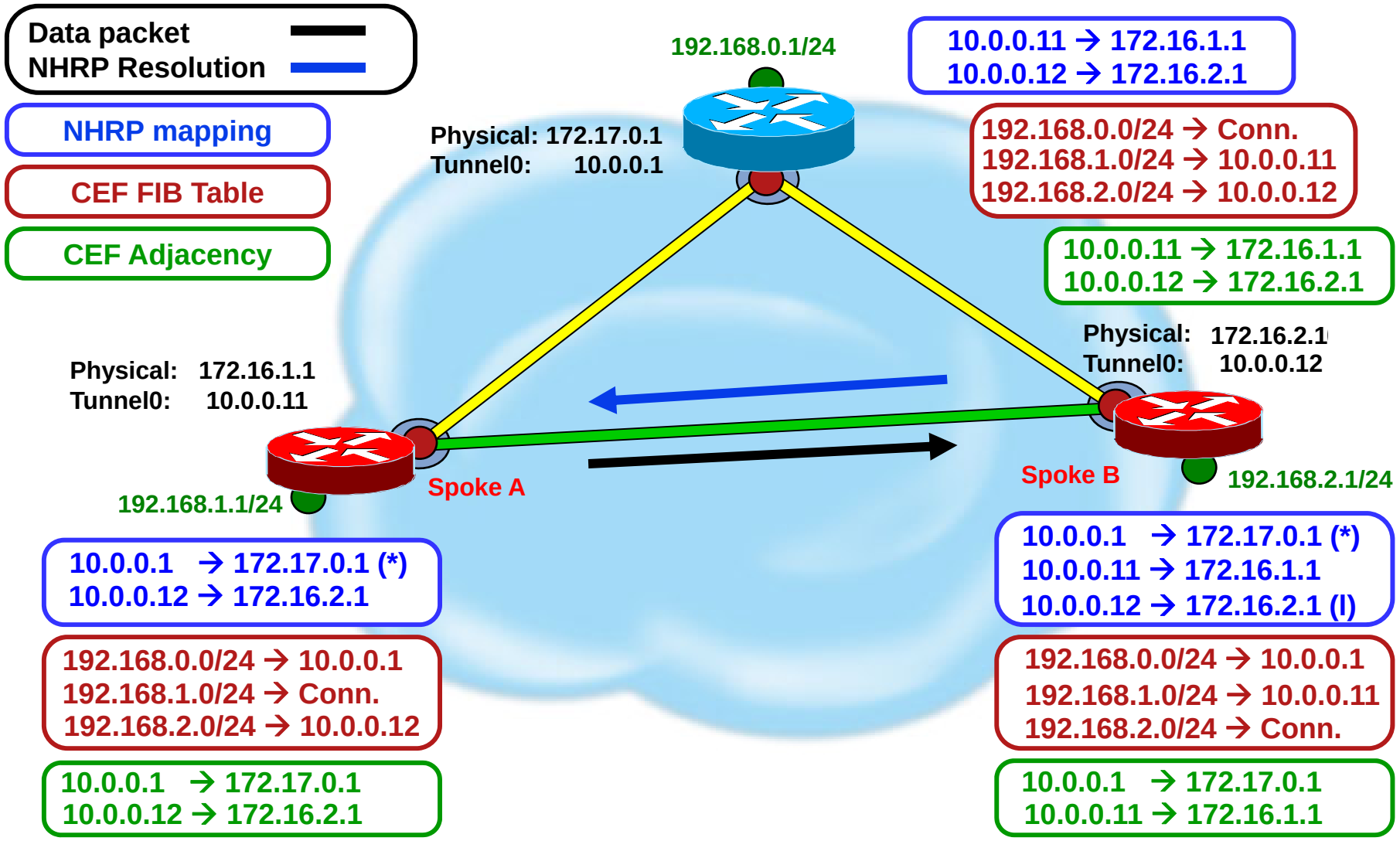
NHRP: Receive Resolution Request via Tunnel0 vrf 0, packet size: 104
(F) afn: IPv4(1), type: IP(800), **hop: 254**, ver: 1, shtl: 4(NSAP), sstl: 0(NSAP)
(M) flags: "router auth src-stable nat ", reqid: 164
src NBMA: 172.16.1.1, src protocol: 10.0.0.11, dst protocol: 10.0.0.12
(C-1) code: no error(0), prefix: 0, mtu: 1514, hd_time: 360
Responder Address Extension(3):
Forward Transit NHS Record Extension(4): client NBMA: 172.17.0.1, client protocol: 10.0.0.1
Reverse Transit NHS Record Extension(5):
Authentication Extension(7): type:Cleartext(1), data:test
NAT address Extension(9):

As Rcvd

Phase 2
NHRP Resolution Reply



Phase 2
NHRP Resolution Reply



Phase 2
NHRP Resolution Reply Message

- Lookup protocol destination in routing table → directly connected
- Create NHRP local mapping entry for protocol destination address with mask-length of 32 to NBMA address
- Create NHRP Resolution Response with protocol destination, NBMA address and mask-length of 32
- Delay Resolution response to send via direct spoke-spoke tunnel

```
NHRP: Send Resolution Reply via Tunnel0 vrf 0, packet size: 152, src: 10.0.0.12, dst: 10.0.0.11
 (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1, shtl: 4(NSAP), sstl: 0(NSAP)
 (M) flags: "router auth dst-stable unique src-stable nat ", reqid: 164
     src NBMA: 172.16.1.1, src protocol: 10.0.0.11, dst protocol: 10.0.0.12
 (C-1) code: no error(0), prefix: 32, mtu: 1514, hd_time: 360,
    client NBMA: 172.16.2.1, client protocol: 10.0.0.12
Responder Address Extension(3):
 (C) code: no error(0), prefix: 0, mtu: 1514, hd_time: 360
    client NBMA: 172.16.2.1, client protocol: 10.0.0.12
Forward Transit NHS Record Extension(4): client NBMA: 172.17.0.1, client protocol: 10.0.0.1
Reverse Transit NHS Record Extension(5):
Authentication Extension(7): type:Cleartext(1), data:test
NAT address Extension(9):
```

Phase 2
NHRP Resolution Response Processing

- Receive NHRP Resolution reply

  If using IPsec (tunnel protection …) then

    Trigger IPsec to setup ISAKMP and IPsec SAs for tunnel

    Data packets still forwarded via spoke-hub-…-hub-spoke path

    IPsec triggers back to NHRP when done

- Install new mapping in NHRP mapping table
- Send trigger to CEF to complete corresponding CEF adjacency

  Data packets now forwarded via direct spoke-spoke tunnel by CEF, NHRP no longer involved

Phase 2
NHRP Mapping Tables

Hub1

```
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 01:03:38, expire 00:04:18
  Type: dynamic, Flags: unique nat registered
  NBMA address: 172.16.1.1
10.0.0.12/32 via 10.0.0.12, Tunnel0 created 01:02:15, expire 00:05:44
  Type: dynamic, Flags: unique nat registered
  NBMA address: 172.16.2.1
```

Spoke A

```
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:53:25, never expire
  Type: static, Flags: nat used
  NBMA address: 172.17.0.1
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 00:00:10, expire 00:05:50
  Type: dynamic, Flags: router unique nat local
  NBMA address: 172.16.1.1  (no-socket)
10.0.0.12/32 via 10.0.0.12, Tunnel0 created 00:00:10, expire 00:05:49
  Type: dynamic, Flags: router nat used
  NBMA address: 172.16.2.1
```

Spoke B

```
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:56:12, never expire
  Type: static, Flags: nat used
  NBMA address: 172.17.0.1
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 00:00:11, expire 00:05:49
  Type: dynamic, Flags: router nat used
  NBMA address: 172.16.1.1
10.0.0.12/32 via 10.0.0.12, Tunnel0 created 00:00:11, expire 00:05:48
  Type: dynamic, Flags: router unique nat local
  NBMA address: 172.16.2.1 (no-socket)
```

Phase 2: Dynamic mappings
Refresh or Remove

- Dynamic NHRP mapping entries have finite lifetime
  - Controlled by 'ip nhrp holdtime …' on source of mapping (spoke)
- Background process checks mapping entry every 60 seconds
  - Process-switching
    - Used flag set each time mapping entry is used
    - If used flag is set and expire time < 120 seconds, then refresh entry, otherwise clear used flag
  - CEF-switching
    - If expire time < 120 seconds, CEF Adjacency entry marked "stale"
    - If CEF Adjacency entry is used, signal to NHRP to refresh entry
- Another resolution request is sent to refresh entry
  - Resolution request via NHS path; reply via direct tunnel
- If entry expires it is removed
  - If using IPsec → Trigger IPsec to remove IPsec/ISAKMP SAs

Phase 2: CEF Switching
Data Packet Forwarding

- IP Data packet is forwarded out tunnel interface to IP next-hop from CEF FIB table
- If adjacency is of type Valid

  Packet is encapsulated and forwarded by CEF out tunnel interface – NHRP is not involved
- If adjacency is of type Glean or Incomplete

  Punt packet to process switching

  If original arriving interface was not this tunnel interface

    Initiate NHRP Resolution Request for IP next-hop

    Resolution reply is used to create NHRP mapping and to complete the Adjacency

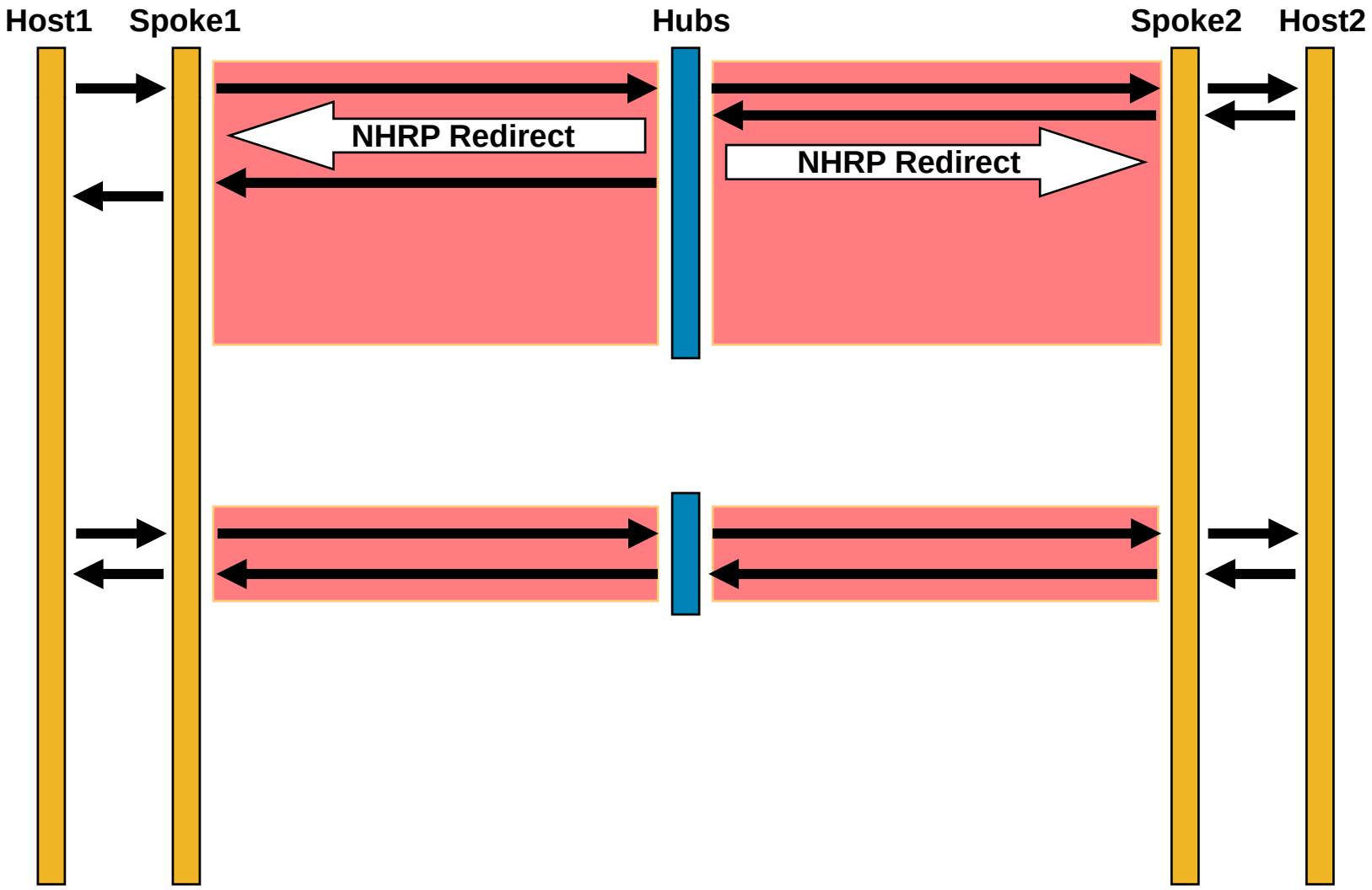
Agenda

- DMVPN Overview
- NHRP Details
  - NHRP Overview
  - NHRP Registrations
  - NHRP Resolutions/Redirects
    - Phase 2
    - Phase 3
- Network Virtualization
  - VRF-lite
  - 2547oDMVPN
- Interaction with other Features
  - NAT, IPv6, Per-tunnel QoS

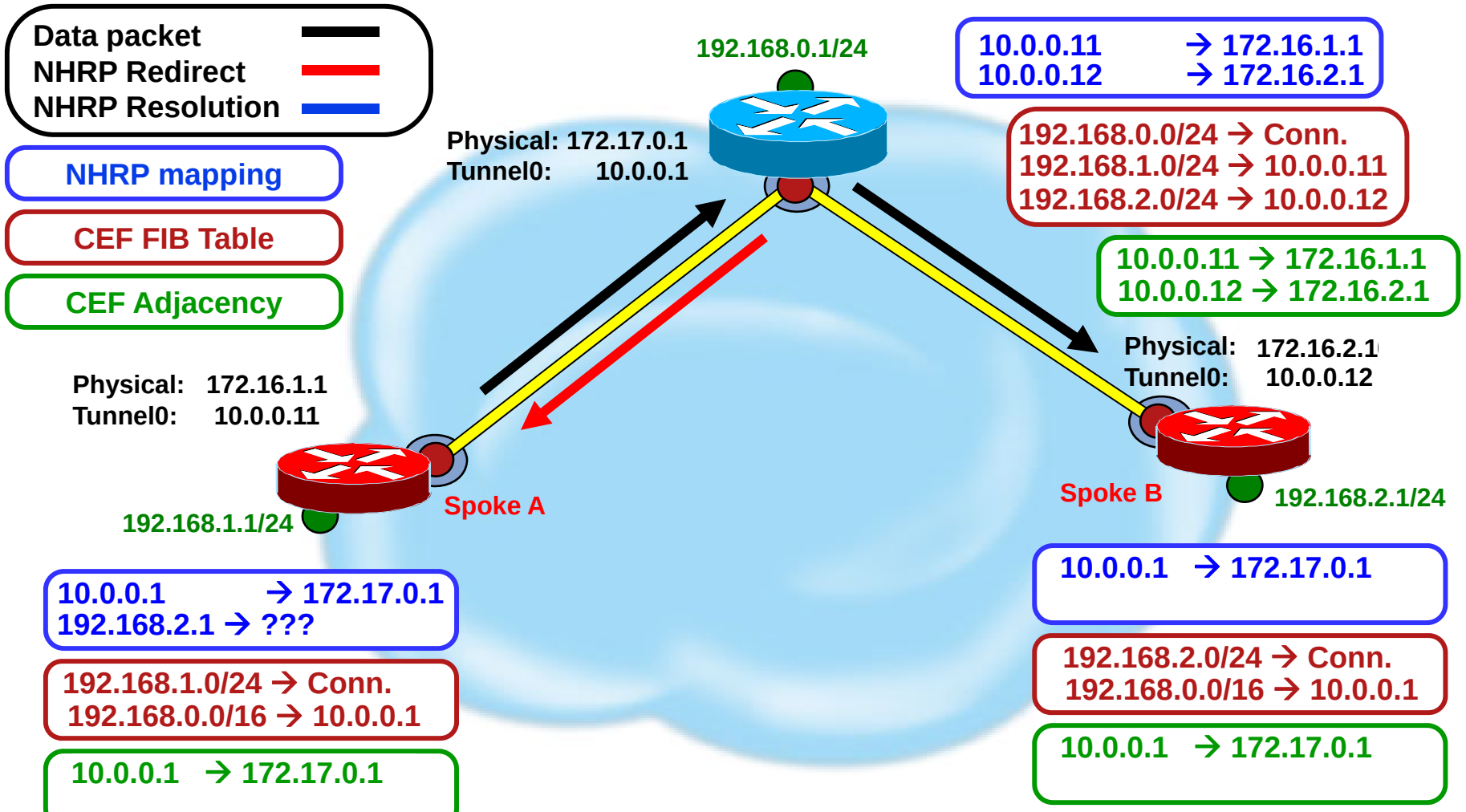
Phase 3
Building Spoke-spoke Tunnels

- Originating spoke
  - IP Data packet is forwarded out tunnel interface to destination via Hub (NHS)
- Hub (NHS)
  - Receives and forwards data packet on same tunnel interface.
  - Sends NHRP Redirect message to originating spoke.
- Originating spoke
  - Receives NHRP redirect message
  - Sends NHRP Resolution Request for Data IP packet destination via NHS
- Destination spoke
  - Receives NHRP Resolution Request
  - Builds spoke-spoke tunnel
  - Sends NHRP Resolution Reply over spoke-spoke tunnel

Phase 3
NHRP Redirects



Phase 3
NHRP Redirects



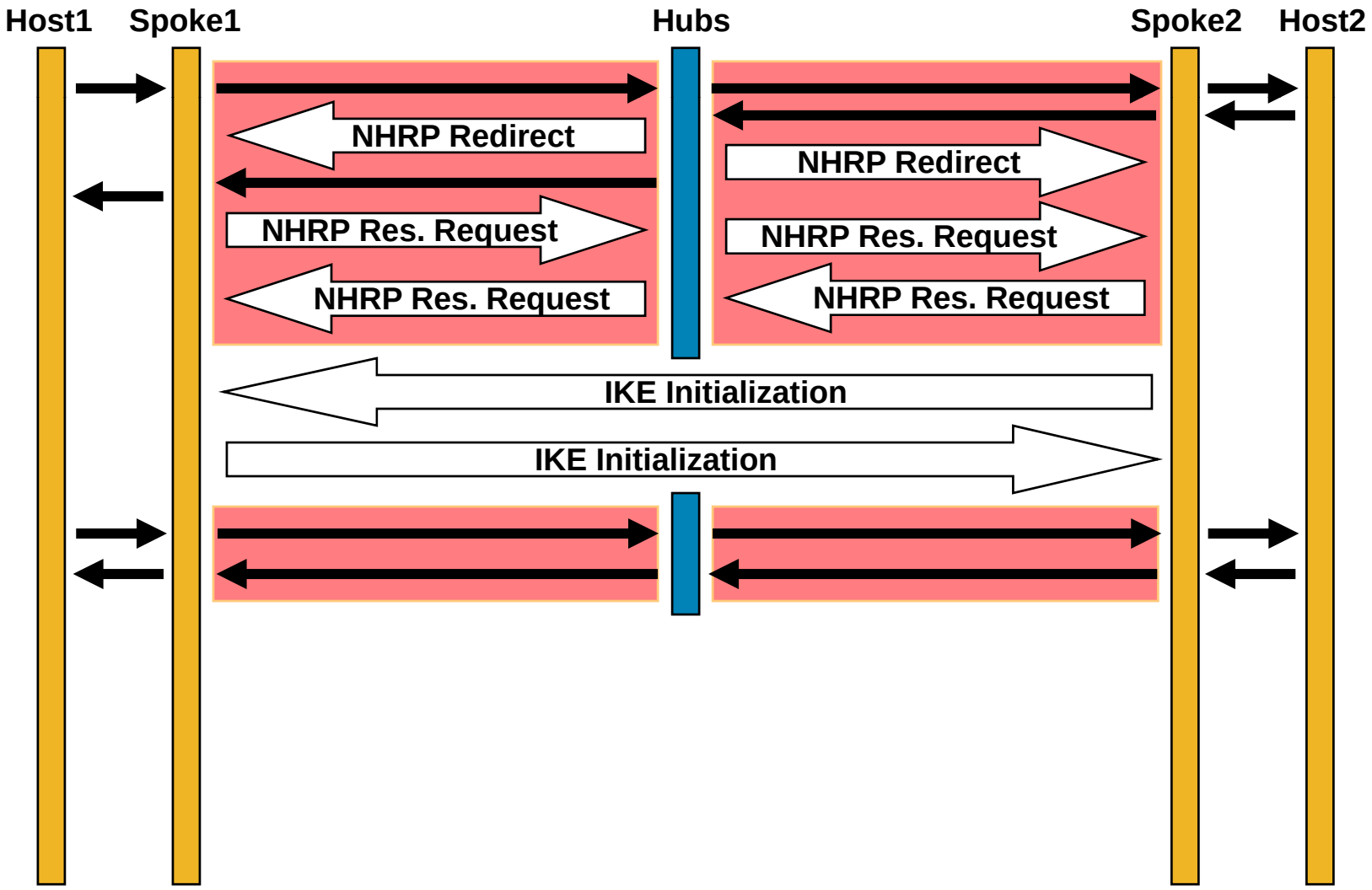
Phase 3
NHRP Redirect Message

```
NHRP: inserting (172.16.1.1/192.168.2.1) in redirect table
NHRP: Attempting to send packet via DEST 192.168.1.1
NHRP: Encapsulation succeeded.  Tunnel IP addr 172.16.1.1
NHRP: Send Traffic Indication via Tunnel0 vrf 0, packet size: 96, src: 10.0.0.1, dst: 192.168.1.1
  (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1, shtl: 4(NSAP), sstl: 0(NSAP)
  (M) traffic code: redirect(0)
      src NBMA: 172.17.0.1, src protocol: 10.0.0.1, dst protocol: 192.168.1.1
      Contents of nhrp traffic indication packet:
        45 00 00 64 00 19 00 00 FD 01 25 2D C0 A8 01 01 C0 A8 02 01 08 00 A8 E3 0B 78 0C
 Forward Transit NHS Record Extension(4):
 Reverse Transit NHS Record Extension(5):
 Authentication Extension(7):   type:Cleartext(1), data:test
NAT Address Extension(9):
```

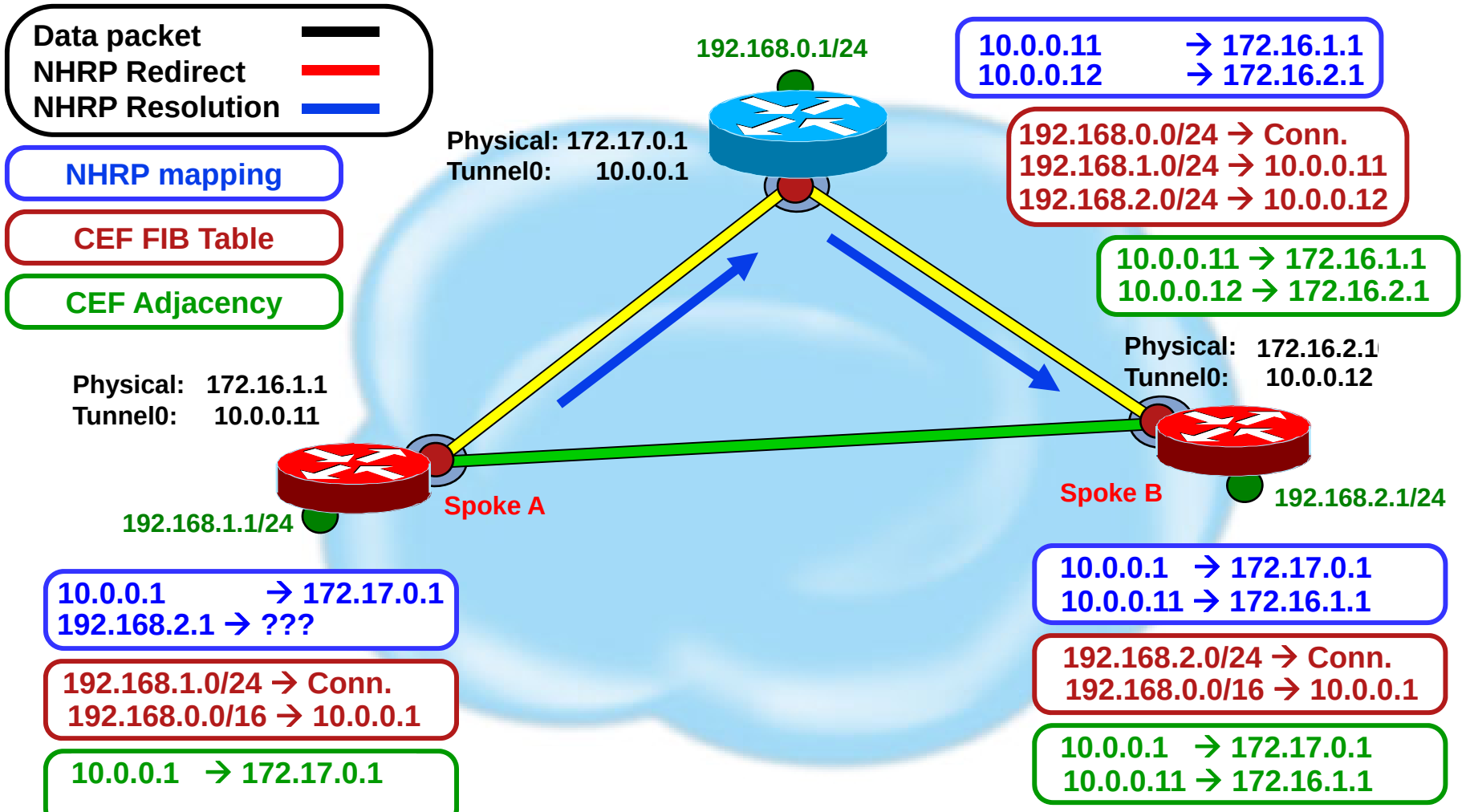
Phase 3
NHRP Redirect Processing

- Sender
  - Insert (GRE IP header source, packet destination IP address) in NHRP redirect table – used to rate-limit NHRP redirect messages
  - Check packet destination IP address against NHRP redirect ACL if denied then stop processing – Don't trigger spoke-spoke tunnel *
  - Send NHRP redirect to GRE/IP header source
  - Time out rate-limit entries from the NHRP redirect table
- Receiver
  - Check data IP source address from data IP header in redirect
    - If routing to the IP source is out:
      - The same GRE tunnel interface then drop redirect
      - Another interface, the IP destination is permitted by 'ip nhrp interest *ACL*' and 'ip nhrp shortcut' is configured
        - Trigger an NHRP resolution request to IP destination
      - Otherwise drop redirect

Phase 3
NHRP Resolution Request



Phase 3
NHRP Resolution Request



Phase 3
NHRP Resolution Request Message

```
NHRP: Send Resolution Request via Tunnel0 vrf 0, packet size: 84,
    src: 10.0.0.11, dst: 192.168.2.1
  (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1, shtl: 4(NSAP), sstl: 0(NSAP)
  (M) flags: "router auth src-stable nat ", reqid: 10599
      src NBMA: 172.16.1.1, src protocol: 10.0.0.11, dst protocol: 192.168.2.1
  (C-1) code: no error(0) prefix: 0, mtu: 1514, hd_time: 360
Responder Address Extension(3):
Forward Transit NHS Record Extension(4):
Reverse Transit NHS Record Extension(5):
Authentication Extension(7):  type:Cleartext(1), data:test
NAT address Extension(9):
```

As Sent

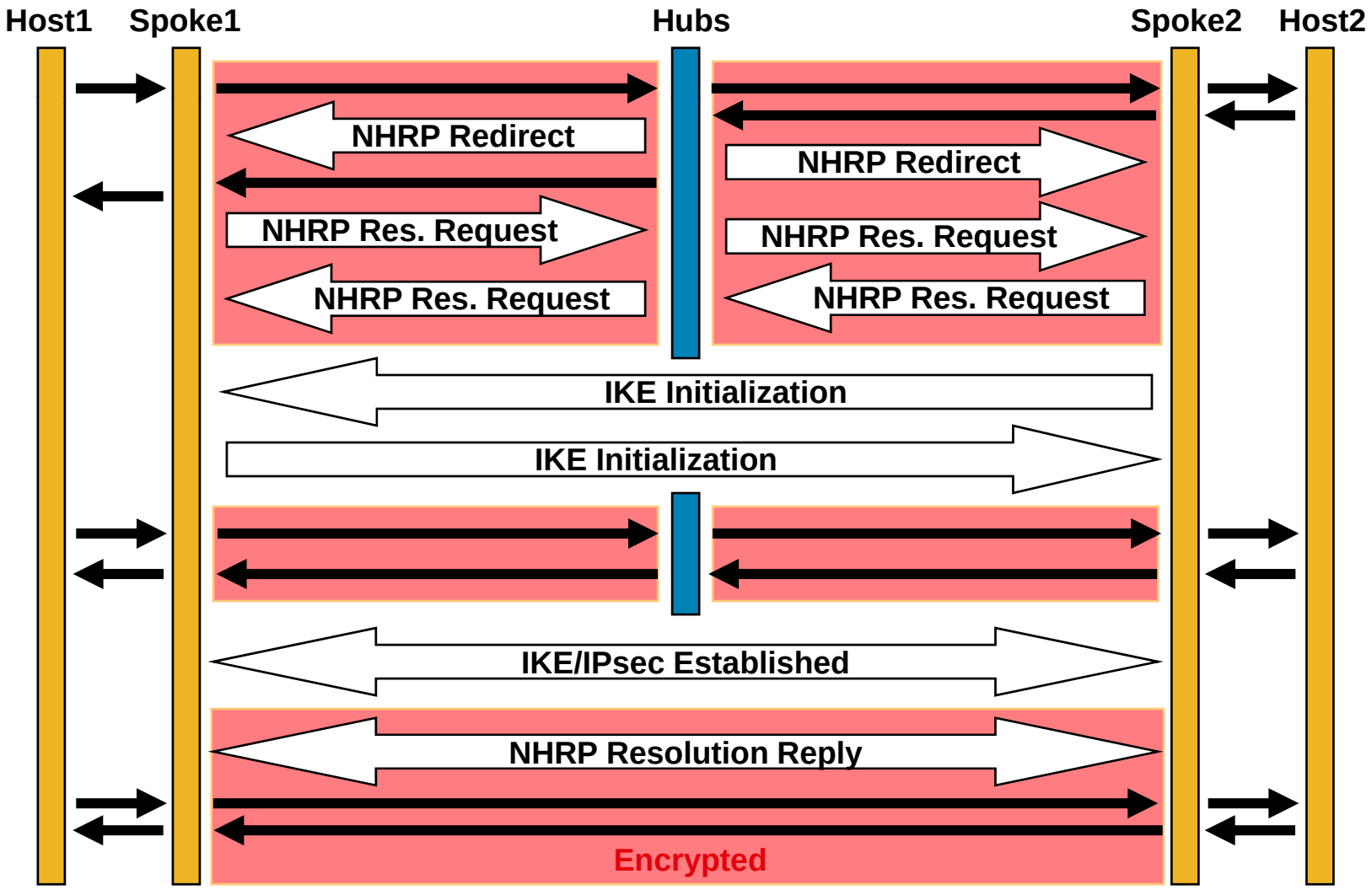
```
NHRP: Receive Resolution Request via Tunnel0 vrf 0, packet size: 104
  (F) afn: IPv4(1), type: IP(800), hop: 254, ver: 1, shtl: 4(NSAP), sstl: 0(NSAP)
  (M) flags: "router auth src-stable nat ", reqid: 10599
      src NBMA: 172.16.1.1, src protocol: 10.0.0.11, dst protocol: 192.168.2.1
  (C-1) code: no error(0), prefix: 0, mtu: 1514, hd_time: 360
Responder Address Extension(3):
Forward Transit NHS Record Extension(4): client NBMA: 172.17.0.1, client protocol: 10.0.0.1
Reverse Transit NHS Record Extension(5):
Authentication Extension(7): type:Cleartext(1), data:test
NAT address Extension(9):
```

As Rcvd

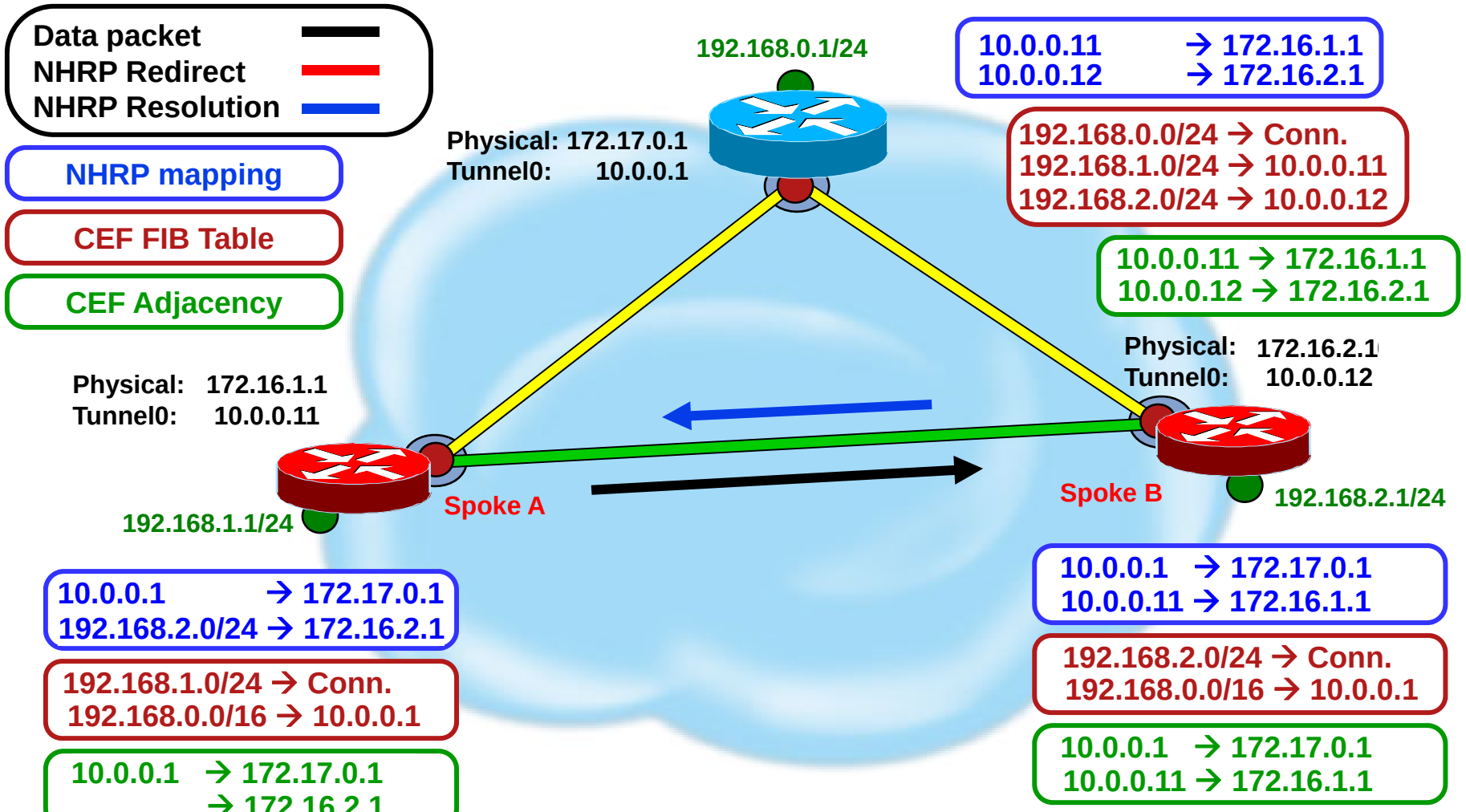
Phase 3
NHRP Resolution Processing

- Spoke (NHC) routing table has Hub (NHS) as IP next-hop for networks behind remote Spoke
  - Note, if routing table has IP next-hop of remote spoke then process as in Phase 2
- Data packets are forwarded (CEF-switched) via routed path
  - Redirect message sent by next tunnel hop on routed path
  - Redirect for data packet triggers resolution request
- Send resolution request for IP destination from data packet header in redirect message
- Resolution requests forwarded via routed path
- Resolution replies forwarded over direct tunnel
  - Direct tunnel initiated from remote → local spoke
- NHRP forwards data packets over direct tunnel when set up

Phase 3
NHRP Resolution Reply



Phase 3
NHRP Resolution Reply



Phase 3
NHRP Resolution Reply Message

- Lookup protocol destination in routing table for matching network, subnet mask and IP next-hop.
- Create NHRP local mapping entry for protocol destination network with mask-length to NBMA address
- Create NHRP Resolution Response with protocol destination, NBMA address and mask-length
- Delay Resolution response to send via direct spoke-spoke tunnel

```
NHRP: Send Resolution Reply via Tunnel0 vrf 0, packet size: 132, src: 10.0.0.12, dst: 10.0.0.11
 (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1, shtl: 4(NSAP), sstl: 0(NSAP)
 (M) flags: "router auth dst-stable unique src-stable nat ", reqid: 10599
     src NBMA: 172.16.1.1, src protocol: 10.0.0.11, dst protocol: 192.168.2.1
 (C-1) code: no error(0), prefix: 24, mtu: 1514, hd_time: 360,
     client NBMA: 172.16.2.1, client protocol: 10.0.0.12
Responder Address Extension(3):
 (C) code: no error(0), prefix: 0, mtu: 1514, hd_time: 360
     client NBMA: 172.16.2.1, client protocol: 10.0.0.12
Forward Transit NHS Record Extension(4): client NBMA: 172.17.0.1, client protocol: 10.0.0.1
Reverse Transit NHS Record Extension(5):
Authentication Extension(7): type:Cleartext(1), data:test
NAT address Extension(9):
```

Phase 3
NHRP Mapping Tables

Spoke A

```
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:03:37, never expire
  Type: static, Flags: nat used
  NBMA address: 172.17.0.1
10.0.0.12/32 via 10.0.0.12, Tunnel0 created 00:00:06, expire 00:05:54
  Type: dynamic, Flags: router nat implicit used
  NBMA address: 172.16.2.1
192.168.1.0/24 via 10.0.0.11, Tunnel0 created 00:00:06, expire 00:05:54
  Type: dynamic, Flags: router unique nat local
  NBMA address: 172.16.1.1  (no-socket)
192.168.2.0/24 via 10.0.0.12, Tunnel0 created 00:00:06, expire 00:05:53
  Type: dynamic, Flags: router nat
  NBMA address: 172.16.2.1
```

Spoke B

```
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:04:46, never expire
  Type: static, Flags: nat used
  NBMA address: 172.17.0.1
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 00:00:13, expire 00:05:46
  Type: dynamic, Flags: router nat implicit used
  NBMA address: 172.16.1.1
192.168.1.0/24 via 10.0.0.11, Tunnel0 created 00:00:11, expire 00:05:48
  Type: dynamic, Flags: router nat
  NBMA address: 172.16.1.1
192.168.2.0/24 via 10.0.0.12, Tunnel0 created 00:00:13, expire 00:05:46
  Type: dynamic, Flags: router unique nat local
  NBMA address: 172.16.2.1   (no-socket)
```

Phase 3: Dynamic Mappings
Refresh or Remove

- Dynamic NHRP mapping entries have finite lifetime
  - Controlled by 'ip nhrp holdtime …' on source of mapping (spoke)
  - Two types of mapping entries
    - Master entry – Remote Spoke Tunnel IP address
    - Child entries – Remote Network address(es)
- Background process checks mapping entries every 60 seconds
  - Child entry: Marked used and timing out → refresh Child entry
  - Master entry: Timing out → mark CEF adjacency stale
    - If CEF adjacency is used → refresh Master entry
- Refreshing entries
  - Send another Resolution request and reply
    - Resolution request/reply sent over direct tunnel
- If entry expires it is removed
  - If using IPsec and last entry using NBMA address
    - Trigger IPsec to remove IPsec and ISAKMP SAs

Phase 3: CEF Switching
Data Packet Forwarding

- IP Data packet is forwarded out tunnel interface
  1. IP next-hop from CEF FIB mapped to Adjacency
     If adjacency is:
     Glean or Incomplete → Punt to process switching
     Valid → Select adjacency for the packet
  2. NHRP in CEF Feature path
     Look up packet IP destination in NHRP mapping table
     Matching entry
     – reselect adjacency → use direct spoke-spoke tunnel
     No matching entry
     – leave CEF adjacency → packet goes to hub
- If packet arrived on and is forwarded out the same tunnel interface
  Forward data packet
  If 'ip nhrp redirect' is on inbound tunnel then send NHRP redirect
- Packet is encapsulated, encrypted and forwarded

Network Virtualization with DMVPN

Network Overview

- Business Unit (BU) traffic separated throughout network
  - VRF-lite → DMVPN per BU
    - Dynamic spoke-spoke tunnels
  - MPLS → single DMVPN (2547oDMVPN)
    - Hub-and-spoke Only
  - Can be mixed on “Internet” router behind hub
- Routing
  - EIGRP
    - Outside of DMVPN for routing with the rest of the network
    - One address-family per BU
    - VRF-lite → Transport routes over DMVPN
  - BGP
    - Inside of DMVPN; import/export routes between VRFs
    - One address-family one per BU
    - VRF-lite → On hub only
    - 2547oDMVPN → On hub and spokes; transport routes over MPLS

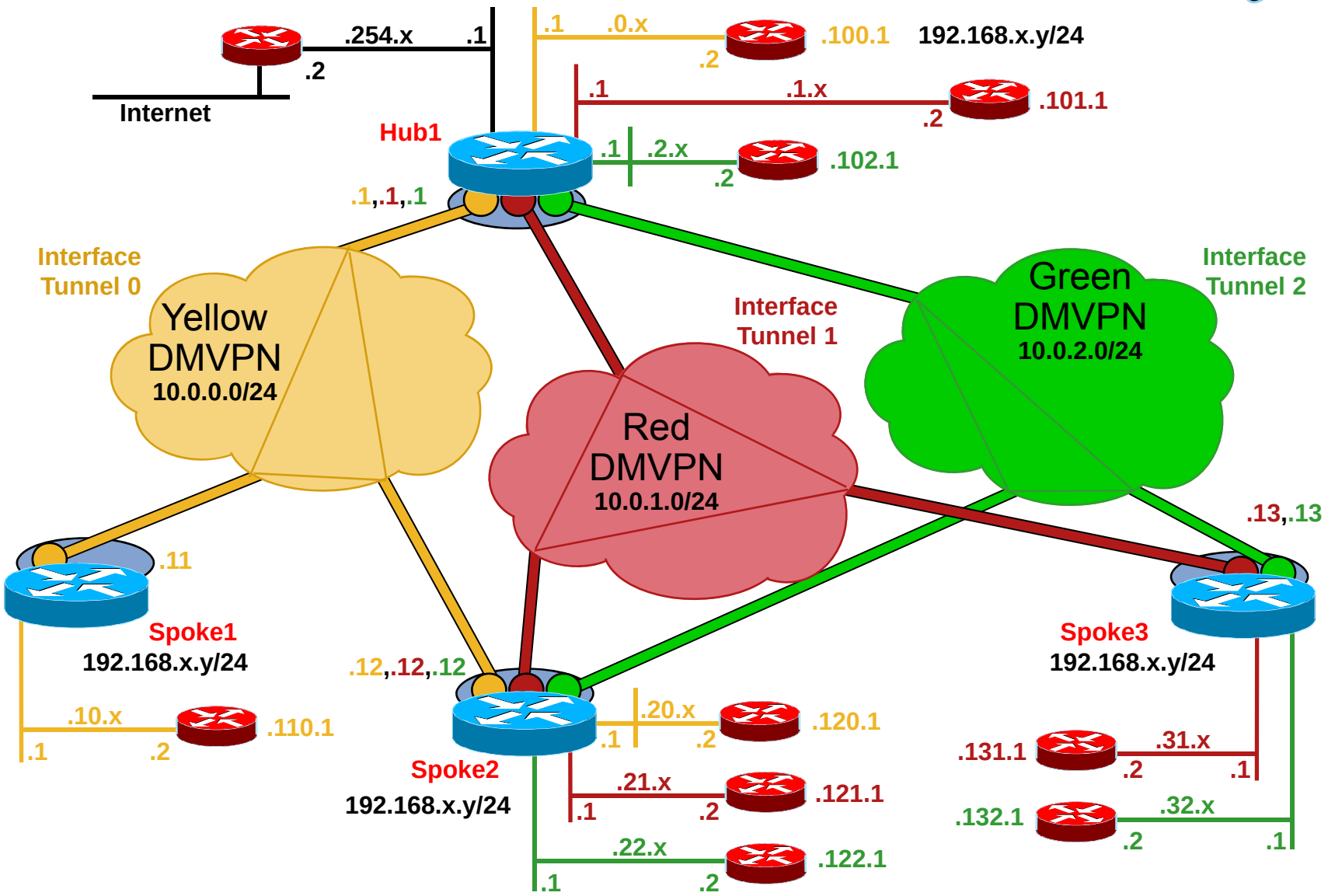
Agenda

- DMVPN Overview
- NHRP Details
  - NHRP Overview
  - NHRP Registrations
  - NHRP Resolutions/Redirects
    - Phase 2
    - Phase 3
- Network Virtualization
  - VRF-lite
  - 2547oDMVPN
- Interaction with other Features
  - NAT, IPv6, Per-tunnel QoS

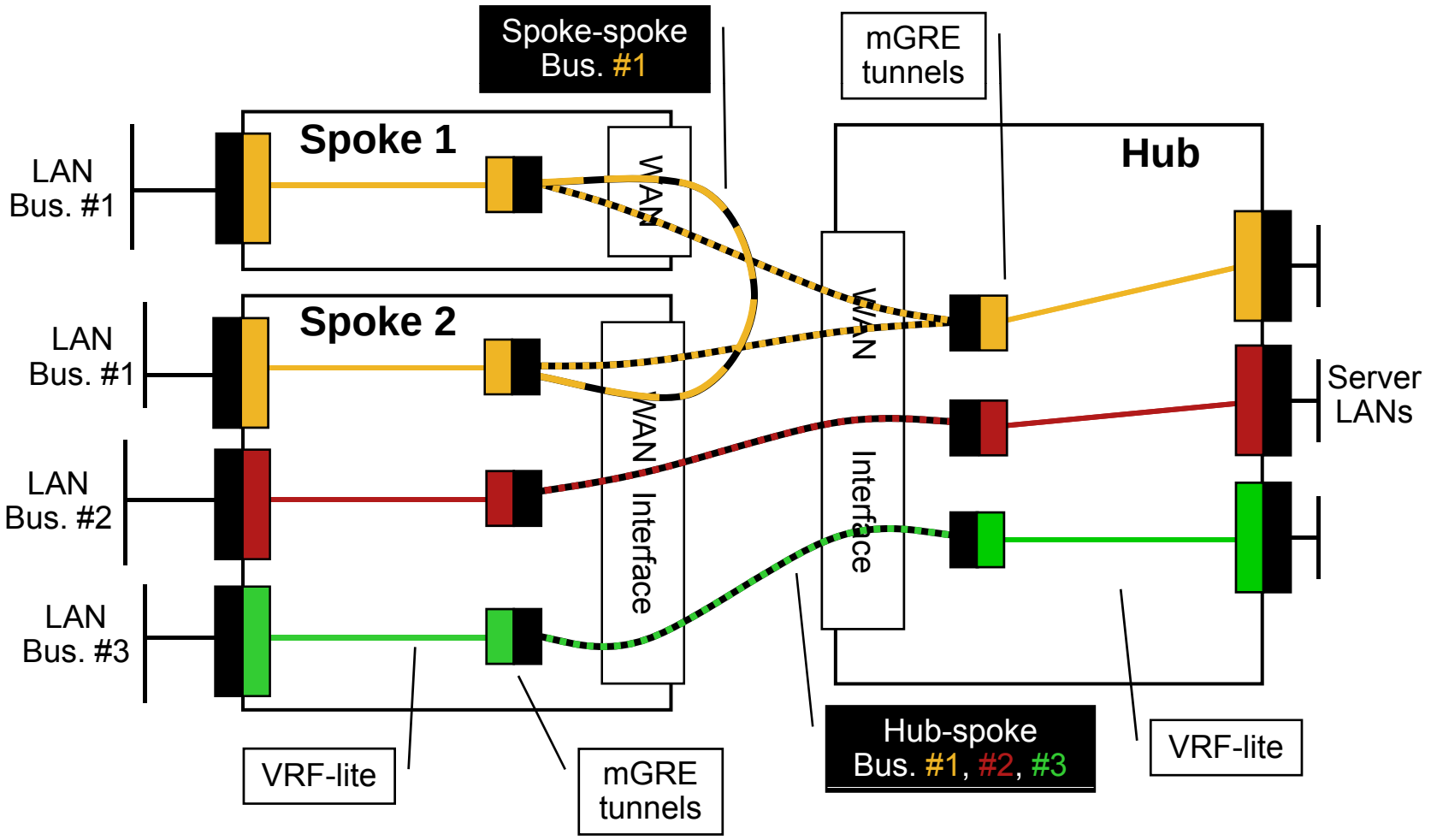
Separate DMVPNs – VRF-lite

- Separate mGRE tunnel per BU
- Hub routers handle all BU DMVPNs
- Multiple Hub routers for redundancy and load
  - All Hub routers configured similar to each other
  - Either manually map spokes to Hub routers
    - Need (2n) Hub routers for redundancy
  - Or use IOS SLB to dynamically map spokes to Hub routers
    - Need (n+1) Hub routers for redundancy and 2 IOS SLB routers
- EIGRP used for routing protocol outside of and over DMVPNs
- BGP used only on the hub
  - For import/export of routes between VRFs

Separate DMVPNs VRF-lite
Logical Topology



Separate DMVPNs – VRF-lite



Configuration
Crypto and Physical Interfaces

```
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto isakmp policy 1
      encryption 3des
crypto isakmp keepalive 15
!
crypto ipsec fragmentation after-encryption
crypto ipsec transform-set T2 esp-3des esp-md5-hmac
      mode transport
!
crypto ipsec profile vpnprof
      set transform-set T1
!
interface Ethernet<y>/0  ! <inside LAN/VRF interface(s)>
      ip vrf forwarding <vrf-name>
      ip address 192.168.<xy>.1 255.255.255.0
!
interface Ethernet3/0  ! <Internet access, on hub only>
      ip vrf forwarding Internet
      ip address 192.168.254.1 255.255.255.0
!
interface Serial<#>/0  ! <outside (public) interface>
      ip address 172.<16|17>.<x>.1 255.255.255.252
!
ip route 0.0.0.0 0.0.0.0 172.<16|17>.<x>.2
```

vrf-name = Yellow, Red, Green

x = Hub, Spoke# (0,1,2,3)
y = BU# (Yellow = 0, Red = 1, Green = 2)

Configuration
Basic VRF and Tunnel

```
ip vrf <vrf-name>     ! <spokes and hub>
     rd <x>:<x>
     route-target export <x>:<x>
     route-target import <x>:<x>
!
...
!
ip vrf Internet                                   ! <hub only>
     rd 10:10
     route-target export 10:10
     route-target import 10:10
     route-target import 1:1
     route-target import 2:2              ! <import routes into Internet VRF>
     route-target import 3:3
!
interface Tunnel<y>
     bandwidth 1000
     ip address 10.0.<y>.1 255.255.255.0
     ip mtu 1400                                  ! <VRF-lite solution only>
     ip nhrp authentication <vrf-name> or test
     ip nhrp map multicast dynamic                ! <hub only>
     ip nhrp network-id 10000<y>
     ip nhrp holdtime 360
     ip tcp adjust-mss 1360                       ! <VRF-lite solution only>
     tunnel source Serial<#>/0
     tunnel mode gre multipoint
     tunnel key 10000<y>
     tunnel protection ipsec profile vpnprof shared
```

x = rd# (Yellow = 1, Red = 2, Green = 3)

vrf-name = Yellow, Red, Green

y = BU# (Yellow = 0, Red = 1, Green = 2)

Configuration
EIGRP and BGP

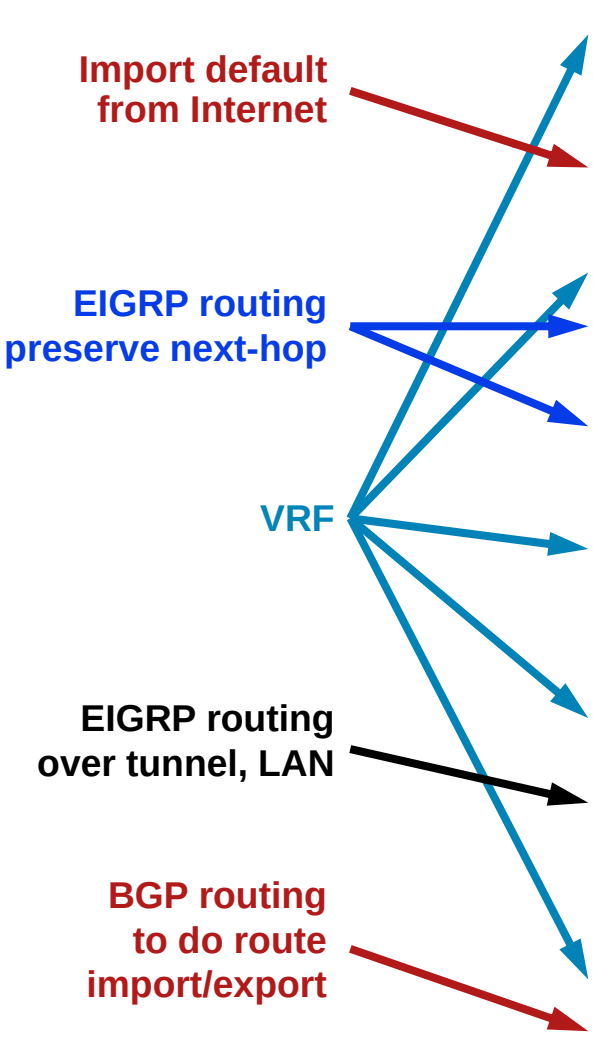
```
router eigrp 1
    no auto-summary
    !
    address-family ipv4 vrf <vrf-name>
        redistribute bgp 1
        network <tunnel-network>
        network <LAN-network>
        default-metric 1000 100 255 1 1500
        no auto-summary
        autonomous-system 1
    exit-address-family
    !
    ...
!
router bgp 1
    no synchronization
    bgp log-neighbor-changes
    no auto-summary
    !
    address-family ipv4 vrf <vrf-name>, <or Internet>
        redistribute connected
        redistribute eigrp 1
        no synchronization
    exit-address-family
    !
```

vrf-name = Yellow, Red, Green

Separate DMVPNs – VRF-lite
Configuration concepts

- On Spokes and Hubs
  - Per BU (VRF) configuration
    - EIGRP Address Family
    - DMVPN Tunnel mGRE interface
    - LAN interface
  - EIGRP used for routing protocol on LANs and over DMVPNs
- Only on Hubs
  - BGP
    - Redistribute between EIGRP and BGP for import/export of routes between BU VRFs and Internet VRF

Separate DMVPNs – VRF-lite
Hub Configuration – BU VRFs




```
ip vrf Yellow
     rd 1:1
     route-target
     route-target
     route-target
!
interface Tunne
     ip vrf forwar
     ip address 1
     no ip next-h
     ip nhrp netw
     ip nhrp auth
     no ip split-h
     tunnel key 1
!
interface Etherr
     ip vrf forwar
     ip address 1
!
router eigrp 1
     !
     address-fam
        redistribut
        network 1
        network 1
     exit-address
!
router bgp 1
     !
     address-fam
        redistribut
        redistribut
     exit-address
```

```
ip vrf Red
     rd 2:2
     route-target
     route-target
     route-target
!
interface Tunne
     ip vrf forwar
     ip address 1
     no ip next-h
     ip nhrp netw
     ip nhrp auth
     no ip split-h
     tunnel key 1
!
interface Ether
     ip vrf forwar
     ip address 1
!
router eigrp 1
     !
     address-fam
        redistribu
        network 1
        network 1
     exit-address
!
router bgp 1
     !
     address-fam
        redistribu
        redistribu
     exit-address
```

```
ip vrf Green
     rd 3:3
     route-target export 3:3
     route-target import 3:3
     route-target import 10:10
!
interface Tunnel2
     ip vrf forwarding Green
     ip address 10.0.2.1 255.255.255.0
     no ip next-hop-self eigrp 1
     ip nhrp network-id 100002
     ip nhrp authentication Green
     no ip split-horizon eigrp 1
     tunnel key 100002
!
interface Ethernet2/0
     ip vrf forwarding Green
     ip address 192.168.2.1 255.255.255.0
!
router eigrp 1
     !
     address-family ipv4 vrf Green
        redistribute bgp 1
        network 10.0.2.0 0.0.0.255
        network 192.168.2.0
     exit-address-family
!
router bgp 1
     !
     address-family ipv4 vrf Green
        redistribute connected
        redistribute eigrp 1
     exit-address-family
```

Separate DMVPNs – VRF-lite
Spoke 2 – Configuration

VRF config

EIGRP routing over DMVPN

No BGP config

```
ip vrf Yellow
     rd 1:1
     route-target export
     route-target import
!
interface Tunnel0
     ip vrf forwarding Ye
     ip address 10.0.0.12
     ip nhrp authenticati
     ip nhrp map multica
     ip nhrp map 10.0.0.
     ip nhrp network-id 1
     ip nhrp nhs 10.0.0.1
     tunnel key 100000
!
router eigrp 1
     no auto-summary
     !
     address-family ipv4
          network 10.0.0.0
          network 192.168
          no auto-summar
          autonomous-sys
     exit-address-family
!
interface Ethernet0/0
     ip vrf forwarding Ye
     ip address 192.168.
```

```
ip vrf Red
     rd 2:2
     route-target export
     route-target import
!
interface Tunnel1
     ip vrf forwarding Re
     ip address 10.0.1.12
     ip nhrp authenticati
     ip nhrp map multica
     ip nhrp map 10.0.1.
     ip nhrp network-id 1
     ip nhrp nhs 10.0.1.1
     tunnel key 100001
!
router eigrp 1
     no auto-summary
     !
     address-family ipv4
          network 10.0.1.0
          network 192.168
          no auto-summar
          autonomous-sys
     exit-address-family
!
interface Ethernet1/0
     ip vrf forwarding Re
     ip address 192.168.
```

```
ip vrf Green
     rd 3:3
     route-target export 3:3
     route-target import 3:3
!
interface Tunnel2
     ip vrf forwarding Green
     ip address 10.0.2.12 255.255.255.0
     ip nhrp authentication Green
     ip nhrp map multicast 172.17.0.1
     ip nhrp map 10.0.2.1 172.17.0.1
     ip nhrp network-id 100002
     ip nhrp nhs 10.0.2.1
     tunnel key 100002
!
router eigrp 1
     no auto-summary
     !
     address-family ipv4 vrf Green
          network 10.0.2.0 0.0.0.255
          network 192.168.22.0
          no auto-summary
          autonomous-system 1
     exit-address-family
!
interface Ethernet2/0
     ip vrf forwarding Green
     ip address 192.168.22.1 255.255.255.0
```

Separate DMVPNs – VRF-lite
Routing Tables – Hub

Global

```
     172.17.0.0/30 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, Serial4/0
S*  0.0.0.0/0 [1/0] via 172.17.0.2
```

Internet

```
B    192.168.10.0/24 [20/15385600] via 10.0.0.11 (Yellow), 00:11:37, Tunnel0
B    192.168.20.0/24 [20/15385600] via 10.0.0.12 (Yellow), 00:11:51, Tunnel0
B    192.168.110.0/24 [20/15411200] via 10.0.0.11 (Yellow), 00:11:37, Tunnel0
B    192.168.120.0/24 [20/15411200] via 10.0.0.12 (Yellow), 00:11:51, Tunnel0

B    192.168.21.0/24 [20/15385600] via 10.0.1.12 (Red), 00:11:51, Tunnel1
B    192.168.31.0/24 [20/15385600] via 10.0.1.13 (Red), 00:11:51, Tunnel1
B    192.168.121.0/24 [20/15411200] via 10.0.1.12 (Red), 00:11:51, Tunnel1
B    192.168.131.0/24 [20/15411200] via 10.0.1.13 (Red), 00:11:51, Tunnel1

B    192.168.22.0/24 [20/15385600] via 10.0.2.12 (Green), 00:11:51, Tunnel2
B    192.168.32.0/24 [20/15385600] via 10.0.2.13 (Green), 00:12:06, Tunnel2
B    192.168.122.0/24 [20/15411200] via 10.0.2.12 (Green), 00:11:51, Tunnel2
B    192.168.132.0/24 [20/15411200] via 10.0.2.13 (Green), 00:12:06, Tunnel2

B       10.0.0.0 is directly connected, 00:12:06, Tunnel0
B       10.0.1.0 is directly connected, 00:12:06, Tunnel1
B       10.0.2.0 is directly connected, 00:12:06, Tunnel2

B    192.168.0.0/24 is directly connected, 00:12:06, Ethernet0/0
B    192.168.1.0/24 is directly connected, 00:12:06, Ethernet1/0
B    192.168.2.0/24 is directly connected, 00:12:06, Ethernet2/0

C    192.168.254.0/24 is directly connected, Ethernet3/0
D*EX 0.0.0.0/0 [170/281600] via 192.168.254.2, 00:05:41, Ethernet3/0
```

Separate DMVPNs – VRF-lite
Routing Tables – Hub (VRFs)

Yellow

```
D    192.168.10.0/24 [90/15385600] via 10.0.0.11, 00:11:52, Tunnel0
D    192.168.20.0/24 [90/15385600] via 10.0.0.12, 00:11:54, Tunnel0
D    192.168.110.0/24 [90/15411200] via 10.0.0.11, 00:11:52, Tunnel0
D    192.168.120.0/24 [90/15411200] via 10.0.0.12, 00:11:54, Tunnel0

C       10.0.0.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, Ethernet0/0

B    192.168.254.0/24 is directly connected, 00:12:08, Ethernet3/0
B*   0.0.0.0/0 [20/281600] via 192.168.254.2 (Internet), 00:04:23, Ethernet3/0
```

Red

```
D    192.168.21.0/24 [90/15385600] via 10.0.1.12, 00:11:53, Tunnel1
D    192.168.31.0/24 [90/15385600] via 10.0.1.13, 00:12:07, Tunnel1
D    192.168.121.0/24 [90/15411200] via 10.0.1.12, 00:11:53, Tunnel1
D    192.168.131.0/24 [90/15411200] via 10.0.1.13, 00:12:07, Tunnel1

C       10.0.1.0 is directly connected, Tunnel1
C    192.168.1.0/24 is directly connected, Ethernet1/0

B    192.168.254.0/24 is directly connected, 00:12:07, Ethernet3/0
B*   0.0.0.0/0 [20/281600] via 192.168.254.2 (Internet), 00:04:22, Ethernet3/0
```

Green

```
D    192.168.22.0/24 [90/15385600] via 10.0.2.12, 00:11:53, Tunnel2
D    192.168.32.0/24 [90/15385600] via 10.0.2.13, 00:12:06, Tunnel2
D    192.168.122.0/24 [90/15411200] via 10.0.2.12, 00:11:53, Tunnel2
D    192.168.132.0/24 [90/15411200] via 10.0.2.13, 00:12:06, Tunnel2

C       10.0.2.0 is directly connected, Tunnel2
C    192.168.2.0/24 is directly connected, Ethernet2/0

B    192.168.254.0/24 is directly connected, 00:12:06, Ethernet3/0
B*   0.0.0.0/0 [20/281600] via 192.168.254.2 (Internet), 00:04:20, Ethernet3/0
```

Separate DMVPNs – VRF-lite
Routing Tables – Spoke2

Spoke2: Yellow

```
D    192.168.10.0/24 [90/15641600] via 10.0.0.11, 00:18:22, Tunnel0
C    192.168.20.0/24 is directly connected, Ethernet0/0
D    192.168.110.0/24 [90/15667200] via 10.0.0.11, 00:18:22, Tunnel0
D    192.168.120.0/24 [90/307200] via 192.168.20.2, 00:18:24, Ethernet0/0

C       10.0.0.0 is directly connected, Tunnel0
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:18:24, Tunnel0
D    192.168.254.0/24 [90/2841600] via 10.0.0.1, 00:11:08, Tunnel0
D*EX 0.0.0.0/0 [170/2841600] via 10.0.0.1, 00:10:53, Tunnel0
```

Red

```
C    192.168.21.0/24 is directly connected, Ethernet1/0
D    192.168.31.0/24 [90/15641600] via 10.0.1.13, 00:18:25, Tunnel1
D    192.168.121.0/24 [90/307200] via 192.168.21.2, 00:18:25, Ethernet1/0
D    192.168.131.0/24 [90/15667200] via 10.0.1.13, 00:18:25, Tunnel1

C       10.0.1.0 is directly connected, Tunnel1
D    192.168.1.0/24 [90/2841600] via 10.0.1.1, 00:18:25, Tunnel1
D    192.168.254.0/24 [90/2841600] via 10.0.1.1, 00:11:09, Tunnel1
D*EX 0.0.0.0/0 [170/2841600] via 10.0.1.1, 00:10:54, Tunnel1
```

Green

```
C    192.168.22.0/24 is directly connected, Ethernet2/0
D    192.168.32.0/24 [90/15641600] via 10.0.2.13, 00:18:27, Tunnel2
D    192.168.122.0/24 [90/307200] via 192.168.22.2, 00:18:27, Ethernet2/0
D    192.168.132.0/24 [90/15667200] via 10.0.2.13, 00:18:27, Tunnel2

C       10.0.2.0 is directly connected, Tunnel2
D    192.168.2.0/24 [90/2841600] via 10.0.2.1, 00:18:27, Tunnel2
D    192.168.254.0/24 [90/2841600] via 10.0.2.1, 00:11:09, Tunnel2
D*EX 0.0.0.0/0 [170/2841600] via 10.0.2.1, 00:10:54, Tunnel2
```

Separate DMVPNs – VRF-lite
Routing Tables – Spoke 1 and 3

Spoke1: Yellow

```
C    192.168.10.0/24 is directly connected, Ethernet0/0
D    192.168.110.0/24 [90/307200] via 192.168.10.2, 1d03h, Ethernet0/0

D    192.168.20.0/24 [90/15641600] via 10.0.0.12, 1d03h, Tunnel0
D    192.168.120.0/24 [90/15667200] via 10.0.0.12, 18:20:09, Tunnel0

C       10.0.0.0 is directly connected, Tunnel0
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 1d03h, Tunnel0
D EX 192.168.254.0/24 [170/2841600] via 10.0.0.1, 1d03h, Tunnel0
D*EX 0.0.0.0/0 [170/2841600] via 10.0.0.1, 1d03h, Tunnel0
```

Spoke3: Red

```
C    192.168.31.0/24 is directly connected, Ethernet1/0
D    192.168.131.0/24 [90/307200] via 192.168.31.2, 00:19:33, Ethernet1/0

D    192.168.21.0/24 [90/15641600] via 10.0.1.12, 00:19:33, Tunnel1
D    192.168.121.0/24 [90/15667200] via 10.0.1.12, 00:19:33, Tunnel1

C       10.0.1.0 is directly connected, Tunnel1
D    192.168.1.0/24 [90/2841600] via 10.0.1.1, 00:19:33, Tunnel1
D    192.168.254.0/24 [90/2841600] via 10.0.1.1, 00:11:09, Tunnel1
D*EX 0.0.0.0/0 [170/2841600] via 10.0.1.1, 00:10:54, Tunnel1
```

Green

```
C    192.168.32.0/24 is directly connected, Ethernet2/0
D    192.168.132.0/24 [90/307200] via 192.168.32.2, 00:19:35, Ethernet2/0

D    192.168.22.0/24 [90/15641600] via 10.0.2.12, 00:19:35, Tunnel2
D    192.168.122.0/24 [90/15667200] via 10.0.2.12, 00:19:35, Tunnel2

C       10.0.2.0 is directly connected, Tunnel2
D    192.168.2.0/24 [90/2841600] via 10.0.2.1, 00:19:35, Tunnel2
D    192.168.254.0/24 [90/2841600] via 10.0.2.1, 00:11:09, Tunnel2
D*EX 0.0.0.0/0 [170/2841600] via 10.0.2.1, 00:10:54, Tunnel2
```

Separate DMVPNs – VRF-lite Summary

- Separate DMVPN mGRE tunnel per BU VRF
- Hub routers handle all DMVPNs
  - Multiple Hub routers for redundancy and load
- EIGRP used for routing protocol outside of and over DMVPNs on Spokes and Hubs
  - Address family per VRF
- BGP used only on the hub
  - Redistribute between EIGRP and BGP for import/export of routes between VRFs
  - “Internet” VRF for Internet access and routing between VRFs
- Global routing table only for routing DMVPN tunnel packets

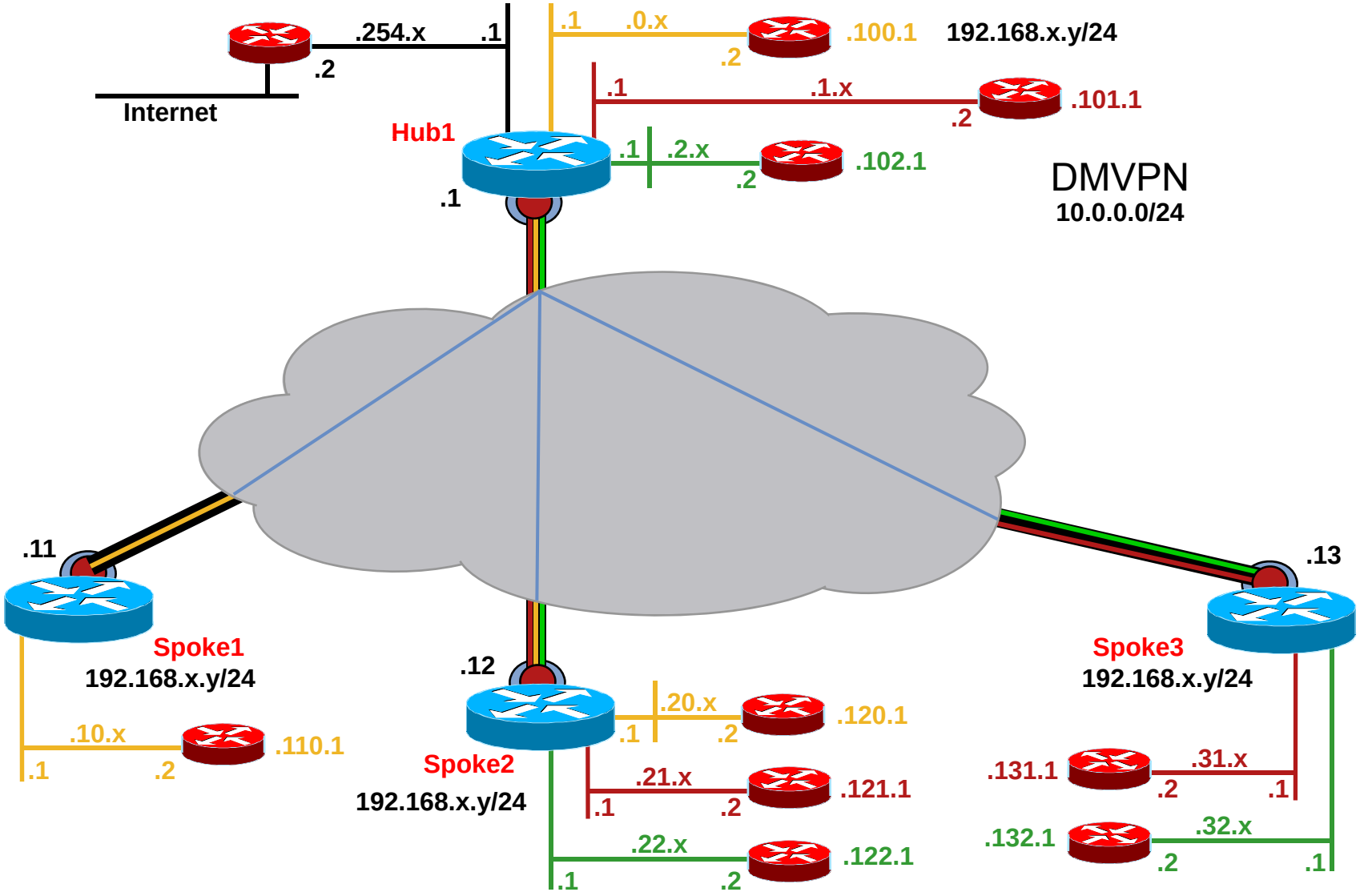
Agenda

- DMVPN Overview
- NHRP Details
  - NHRP Overview
  - NHRP Registrations
  - NHRP Resolutions/Redirects
    - Phase 2
    - Phase 3
- Network Virtualization
  - VRF-lite
  - 2547oDMVPN
- Interaction with other Features
  - NAT, IPv6, Per-tunnel QoS

MPLS over DMVPN – 2547oDMVPN

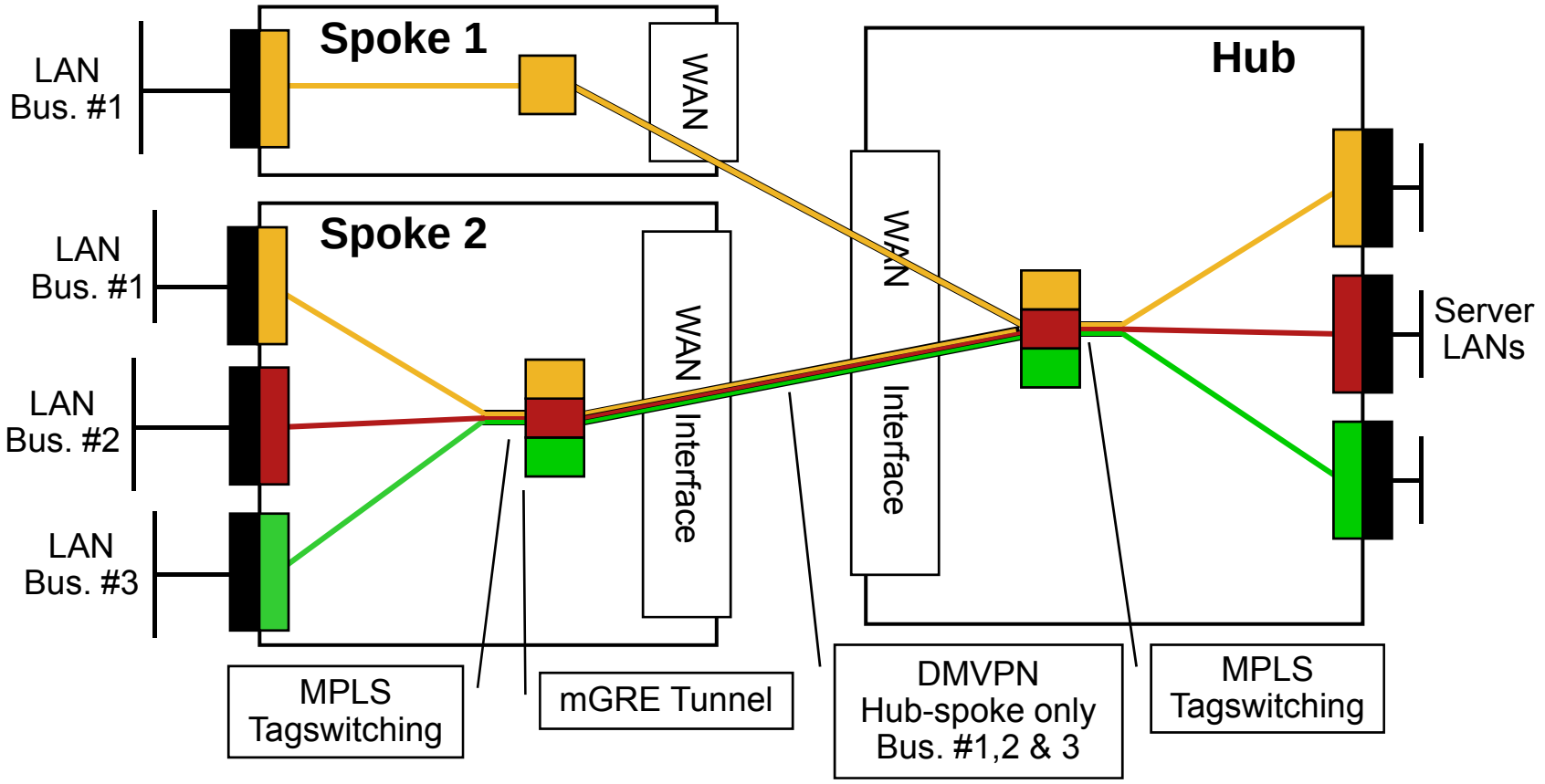
- Single DMVPN
  - MPLS VPN over DMVPN (hub-and-spoke only)
  - Single mGRE tunnel on all routers
- Simplified MPLS configuration
  - Still adds complexity for managing and troubleshooting
- Multiple Hub routers for redundancy and load
  - Hub routers configured similar to each other
  - Manually map spokes to Hub routers
    - Need (2n) Hub routers for redundancy
- EIGRP is used for routing outside the DMVPN network
- BGP must be used for routing protocol over DMVPN
  - Redistribute EIGRP to/from BGP for transport over DMVPN
  - Import/export of routes between VRFs

MPLS over DMVPN – 2547oDMVPN
Logical Topology



MPLS over DMVPN – 2547oDMVPN

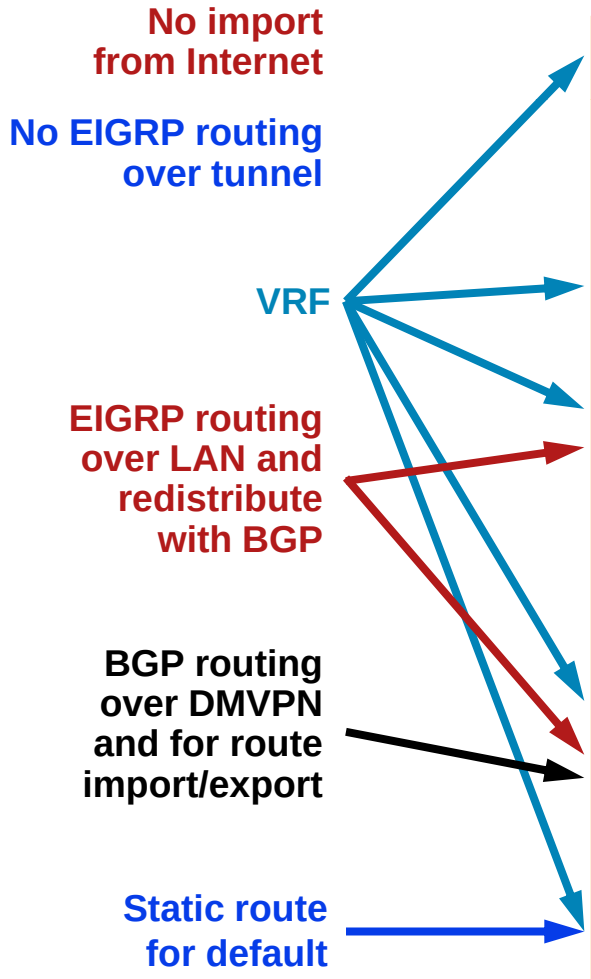
- Map BU traffic to separate LANs/vLANs using VRF-lite
  - May need separate router if BU servers on same LAN



MPLS over DMVPN – 2547oDMVPN
Configuration concepts

- On Spokes and Hubs
  - Single DMVPN Tunnel mGRE interface
  - Per BU (VRF) configuration
    - BGP Address Family
    - EIGRP Address Family
    - LAN interface
  - EIGRP used for routing protocol on LANs
    - Redistribute to/from BGP
  - BGP used for routing protocol on DMVPNs
    - VPNv4 for MPLS VPNs
    - Redistribute to/from EIGRP

MPLS over DMVPN – 2547oDMVPN
Hub Configuration – BU VRFs

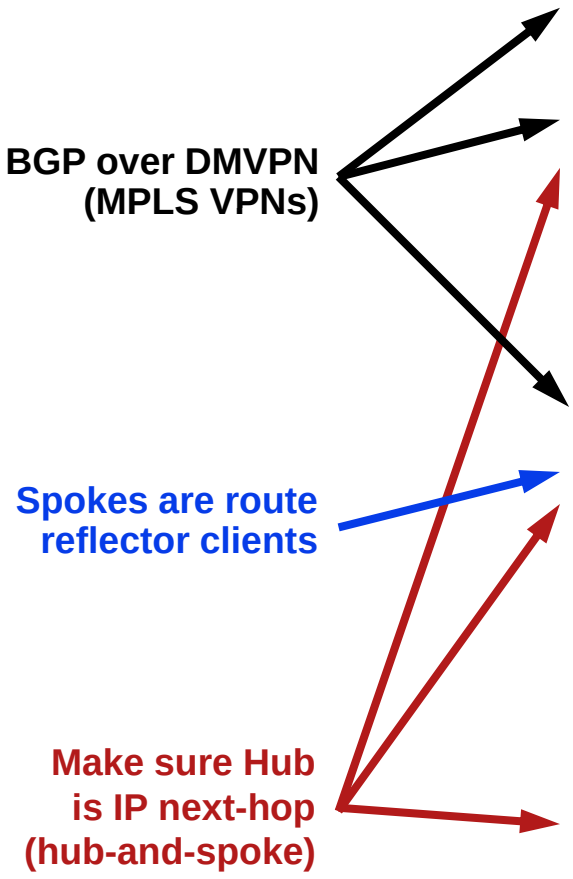



```
ip vrf Yellow
     rd 1:1
     route-target
     route-target
!
interface Etherr
     ip vrf forwar
     ip address 1
     ip tcp adjust
!
router eigrp 1
     !
     address-fam
          redistribu
          network 1
          default-m
          autonom
     exit-address
     !
router bgp 1
     !
     address-fam
          redistribu
          redistribu
          redistribu
          default-in
     exit-address
!
ip route vrf Yell
                Eth
```

```
ip vrf Red
     rd 2:2
     route-target
     route-target
!
interface Ether
     ip vrf forwar
     ip address 1
     ip tcp adjus
!
router eigrp 1
     !
     address-fam
          redistribu
          network
          default-n
          autonom
     exit-address
     !
router bgp 1
     !
     address-fam
          redistribu
          redistribu
          redistribu
          default-ir
     exit-address
!
ip route vrf Red
                Et
```

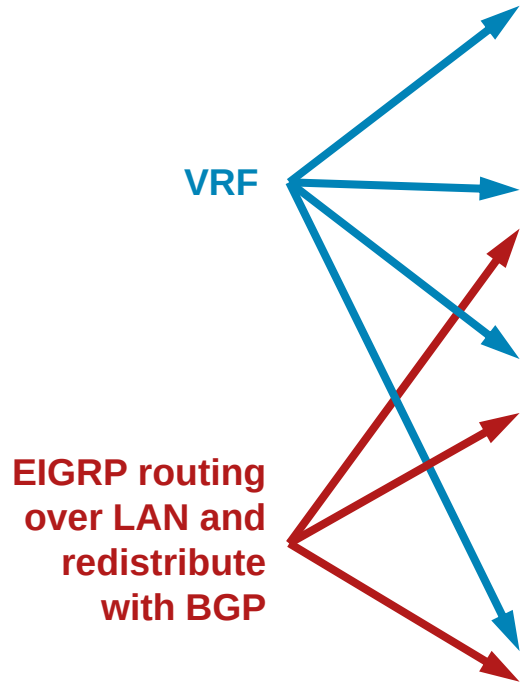
```
ip vrf Green
     rd 3:3
     route-target export 3:3
     route-target import 3:3
!
interface Ethernet0/0
     ip vrf forwarding Green
     ip address 192.168.2.1 255.255.255.0
     ip tcp adjust-mss 1360
!
router eigrp 1
     !
     address-family ipv4 vrf Green
          redistribute bgp 1
          network 192.168.2.0
          default-metric 1000 100 255 1 1500
          autonomous-system 1
     exit-address-family
     !
router bgp 1
     !
     address-family ipv4 vrf Green
          redistribute connected
          redistribute static
          redistribute eigrp 1
          default-information originate
     exit-address-family
!
ip route vrf Green 0.0.0.0 0.0.0.0 –
                Ethernet3/0 192.168.254.2
```

MPLS over DMVPN – 2547oDMVPN
Hub Configuration – BGP over DMVPN




```
interface Tunnel0
    ip address 10.0.0.1 255.255.255.0
    ip nhrp authentication test
    ip nhrp network-id 100000
    mpls ip
    mpls mtu 1404
    tunnel key 100000
!
router bgp 1
    neighbor 10.0.0.11 remote-as 1
    neighbor 10.0.0.11 update-source Tunnel0
    neighbor 10.0.0.12 remote-as 1
    neighbor 10.0.0.12 update-source Tunnel0
    neighbor 10.0.0.13 remote-as 1
    neighbor 10.0.0.13 update-source Tunnel0
    no auto-summary
    !
    address-family vpnv4
        neighbor 10.0.0.11 activate
        neighbor 10.0.0.11 send-community extended
        neighbor 10.0.0.11 route-reflector-client
        neighbor 10.0.0.11 route-map Next-hop-self out
        neighbor 10.0.0.12 activate
        neighbor 10.0.0.12 send-community extended
        neighbor 10.0.0.12 route-reflector-client
        neighbor 10.0.0.12 route-map Next-hop-self out
        neighbor 10.0.0.13 activate
        neighbor 10.0.0.13 send-community extended
        neighbor 10.0.0.13 route-reflector-client
        neighbor 10.0.0.13 route-map Next-hop-self out
    exit-address-family
!
access-list 10 permit any
!
route-map Next-hop-self permit 10
    match ip address 10
    set ip next-hop 10.0.0.1
```

MPLS over DMVPN – 2547oDMVPN
Spoke 2 – Configuration

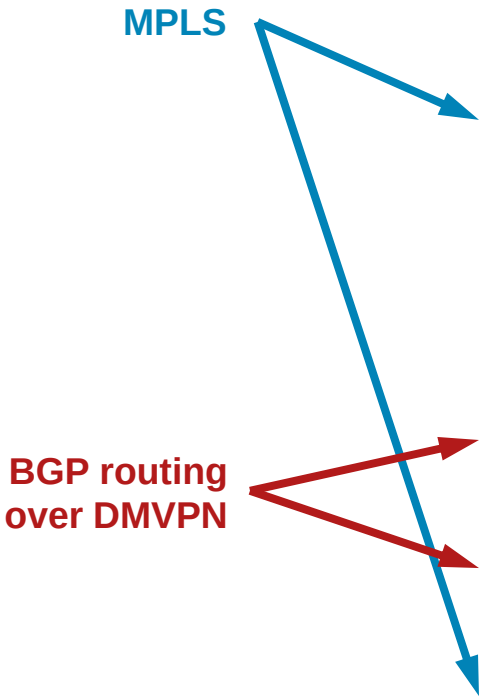



```
ip vrf Yellow
      rd 1:1
      route-target
      route-target
!
interface Etherne
      ip vrf forwar
      ip address 1
      ip tcp adjust
!
router eigrp 1
      !
      address-fam
            redistribu
            network
            default-n
            autonom
      exit-address
!
router bgp 1
      !
      address-fam
            redistribu
            no synch
      exit-address
```

```
ip vrf Red
      rd 2:2
      route-target
      route-target
!
interface Ethern
      ip vrf forwa
      ip address 1
      ip tcp adjus
!
router eigrp 1
      !
      address-fan
            redistrib
            network
            default-
            autonor
      exit-addres
!
router bgp 1
      !
      address-fan
            redistrib
            no sync
      exit-addres
```

```
ip vrf Green
      rd 3:3
      route-target export 3:3
      route-target import 3:3
!
interface Ethernet0/0
      ip vrf forwarding Green
      ip address 192.168.22.1 255.255.255.0
      ip tcp adjust-mss 1360
!
router eigrp 1
      !
      address-family ipv4 vrf Green
            redistribute bgp 1
            network 192.168.22.0
            default-metric 1000 100 255 1 1500
            autonomous-system 1
      exit-address-family
!
router bgp 1
      !
      address-family ipv4 vrf Green
            redistribute eigrp 1
            no synchronization
      exit-address-family
```

MPLS over DMVPN – 2547oDMVPN
Spoke 2 – Configuration (BGP over DMVPN)




```
interface Tunnel0
      ip address 10.0.0.12 255.255.255.0
      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
      mpls ip
      mpls mtu 1404
      tunnel source Serial2/0
      tunnel mode gre multipoint
      tunnel key 100000
      tunnel protection ipsec profile vpnprof
!
!
router bgp 1
      bgp router-id 10.0.0.12
      neighbor 10.0.0.1 remote-as 1
      neighbor 10.0.0.1 update-source Tunnel0
      !
      address-family vpnv4
            neighbor 10.0.0.1 activate
            neighbor 10.0.0.1 send-community extended
      exit-address-family
!
mpls ldp router-id Tunnel0
```

MPLS over DMVPN – 2547oDMVPN
Routing Tables – Hub (Global, VRF)

Global

```
     172.17.0.0/30 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, Serial4/0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Tunnel0
S*   0.0.0.0/0 [1/0] via 172.17.0.2
```

Yellow

```
B    192.168.10.0/24 [200/0] via 10.0.0.11, 03:26:56
B    192.168.20.0/24 [200/0] via 10.0.0.12, 03:26:56
B    192.168.110.0/24 [200/307200] via 10.0.0.11, 03:26:56
B    192.168.120.0/24 [200/307200] via 10.0.0.12, 03:26:56

C    192.168.0.0/24 is directly connected, Ethernet0/0
D    192.168.100.0/24 [90/307200] via 192.168.0.2, 03:27:24, Ethernet0/0
```

Red

```
B    192.168.21.0/24 [200/0] via 10.0.0.12, 03:26:54
B    192.168.31.0/24 [200/0] via 10.0.0.13, 03:26:54
B    192.168.121.0/24 [200/307200] via 10.0.0.12, 03:26:54
B    192.168.131.0/24 [200/307200] via 10.0.0.13, 03:26:54

C    192.168.1.0/24 is directly connected, Ethernet1/0
D    192.168.101.0/24 [90/307200] via 192.168.1.2, 03:27:22, Ethernet1/0
```

Green

```
B    192.168.22.0/24 [200/0] via 10.0.0.12, 03:26:53
B    192.168.32.0/24 [200/0] via 10.0.0.13, 03:26:53
B    192.168.132.0/24 [200/307200] via 10.0.0.13, 03:26:53
B    192.168.122.0/24 [200/307200] via 10.0.0.12, 03:26:53

C    192.168.2.0/24 is directly connected, Ethernet2/0
D    192.168.102.0/24 [90/307200] via 192.168.2.2, 03:27:18, Ethernet2/0
```

MPLS over DMVPN – 2547oDMVPN
MPLS Tables – Hub

Hub1#show mpls forwarding

Lcl tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
16	Untagged	192.168.100.0/24[V]	0	Et0/0	192.168.0.2
17	Untagged	192.168.101.0/24[V]	0	Et1/0	192.168.1.2
18	Untagged	192.168.102.0/24[V]	0	Et2/0	192.168.2.2
20	Aggregate	192.168.254.0/24[V]	0		
21	21	192.168.20.0/24[V]	0	Tu0	10.0.0.12
22	17	192.168.10.0/24[V]	660	Tu0	10.0.0.11
23	16	192.168.120.0/24[V]	1944	Tu0	10.0.0.12
24	16	192.168.110.0/24[V]	2300	Tu0	10.0.0.11
25	19	192.168.31.0/24[V]	0	Tu0	10.0.0.13
26	20	192.168.21.0/24[V]	0	Tu0	10.0.0.12
27	16	192.168.131.0/24[V]	0	Tu0	10.0.0.13
28	17	192.168.121.0/24[V]	0	Tu0	10.0.0.12
29	18	192.168.32.0/24[V]	0	Tu0	10.0.0.13
30	19	192.168.22.0/24[V]	0	Tu0	10.0.0.12
31	17	192.168.132.0/24[V]	0	Tu0	10.0.0.13
32	18	192.168.122.0/24[V]	0	Tu0	10.0.0.12
33	Aggregate	192.168.2.0/24[V]	0		
34	Aggregate	192.168.1.0/24[V]	0		
35	Aggregate	192.168.0.0/24[V]	0		

MPLS over DMVPN – 2547oDMVPN
Routing Tables – Spoke2

Spoke2: Yellow

```
B    192.168.10.0/24 [200/0] via 10.0.0.1, 03:49:48
B    192.168.110.0/24 [200/307200] via 10.0.0.1, 03:49:48
C    192.168.20.0/24 is directly connected, Ethernet0/0
D    192.168.120.0/24 [90/307200] via 192.168.20.2, 05:36:34, Ethernet0/0
B    192.168.0.0/24 [200/0] via 10.0.0.1, 03:49:17
B    192.168.100.0/24 [200/307200] via 10.0.0.1, 03:49:48
```

Red

```
C    192.168.21.0/24 is directly connected, Ethernet1/0
D    192.168.121.0/24 [90/307200] via 192.168.21.2, 05:36:34, Ethernet1/0
B    192.168.31.0/24 [200/0] via 10.0.0.1, 03:49:47
B    192.168.131.0/24 [200/307200] via 10.0.0.1, 03:49:47
B    192.168.1.0/24 [200/0] via 10.0.0.1, 03:49:17
B    192.168.101.0/24 [200/307200] via 10.0.0.1, 03:49:47
```

Green

```
C    192.168.22.0/24 is directly connected, Ethernet2/0
D    192.168.122.0/24 [90/307200] via 192.168.22.2, 05:36:33, Ethernet2/0
B    192.168.32.0/24 [200/0] via 10.0.0.1, 03:49:46
B    192.168.132.0/24 [200/307200] via 10.0.0.1, 03:49:46
B    192.168.2.0/24 [200/0] via 10.0.0.1, 03:49:16
B    192.168.102.0/24 [200/307200] via 10.0.0.1, 03:49:46
```

MPLS over DMVPN – 2547oDMVPN
Routing Tables – Spoke 1 and 3

Spoke1: Yellow

```
C    192.168.10.0/24 is directly connected, Ethernet0/0
D    192.168.110.0/24 [90/307200] via 192.168.10.2, 05:26:34, Ethernet0/0
B    192.168.20.0/24 [200/0] via 10.0.0.1, 03:39:47
B    192.168.120.0/24 [200/307200] via 10.0.0.1, 03:39:47

B    192.168.0.0/24 [200/0] via 10.0.0.1, 03:39:16
B    192.168.100.0/24 [200/307200] via 10.0.0.1, 03:39:47
B*   0.0.0.0/0 [200/0] via 10.0.0.1, 01:48:54
```

Spoke3: Red

```
B    192.168.21.0/24 [200/0] via 10.0.0.1, 03:48:36
B    192.168.121.0/24 [200/307200] via 10.0.0.1, 03:48:36
C    192.168.31.0/24 is directly connected, Ethernet1/0
D    192.168.131.0/24 [90/307200] via 192.168.31.2, 05:35:23, Ethernet1/0

B    192.168.1.0/24 [200/0] via 10.0.0.1, 03:48:06
B    192.168.101.0/24 [200/307200] via 10.0.0.1, 03:48:36
B*   0.0.0.0/0 [200/0] via 10.0.0.1, 01:57:42
```

Green

```
B    192.168.22.0/24 [200/0] via 10.0.0.1, 03:48:35
B    192.168.122.0/24 [200/307200] via 10.0.0.1, 03:48:35
C    192.168.32.0/24 is directly connected, Ethernet2/0
D    192.168.132.0/24 [90/307200] via 192.168.32.2, 05:35:22, Ethernet2/0

B    192.168.2.0/24 [200/0] via 10.0.0.1, 03:48:05
B    192.168.102.0/24 [200/307200] via 10.0.0.1, 03:48:35
B*   0.0.0.0/0 [200/0] via 10.0.0.1, 01:56:12
```

MPLS over DMVPN – 2547oDMVPN
Summary

- Single DMVPN (Hub-and-spoke Only)
  - MPLS VPN over DMVPN
  - Single mGRE tunnel on all routers
- MPLS configuration
  - Hub and Spoke routers are MPLS PEs
- Multiple Hub routers for redundancy and load
- EIGRP is used for routing outside of DMVPN network
- BGP used for routing protocol over DMVPN
  - Redistribute between EIGRP and BGP for transport over DMVPN
  - Import/export of routes between BU VRFs and Internet VRF
  - “Internet” VRF for Internet access and routing between BU VRFs
- Global routing table only for routing DMVPN tunnel packets

Interaction with Other Technologies

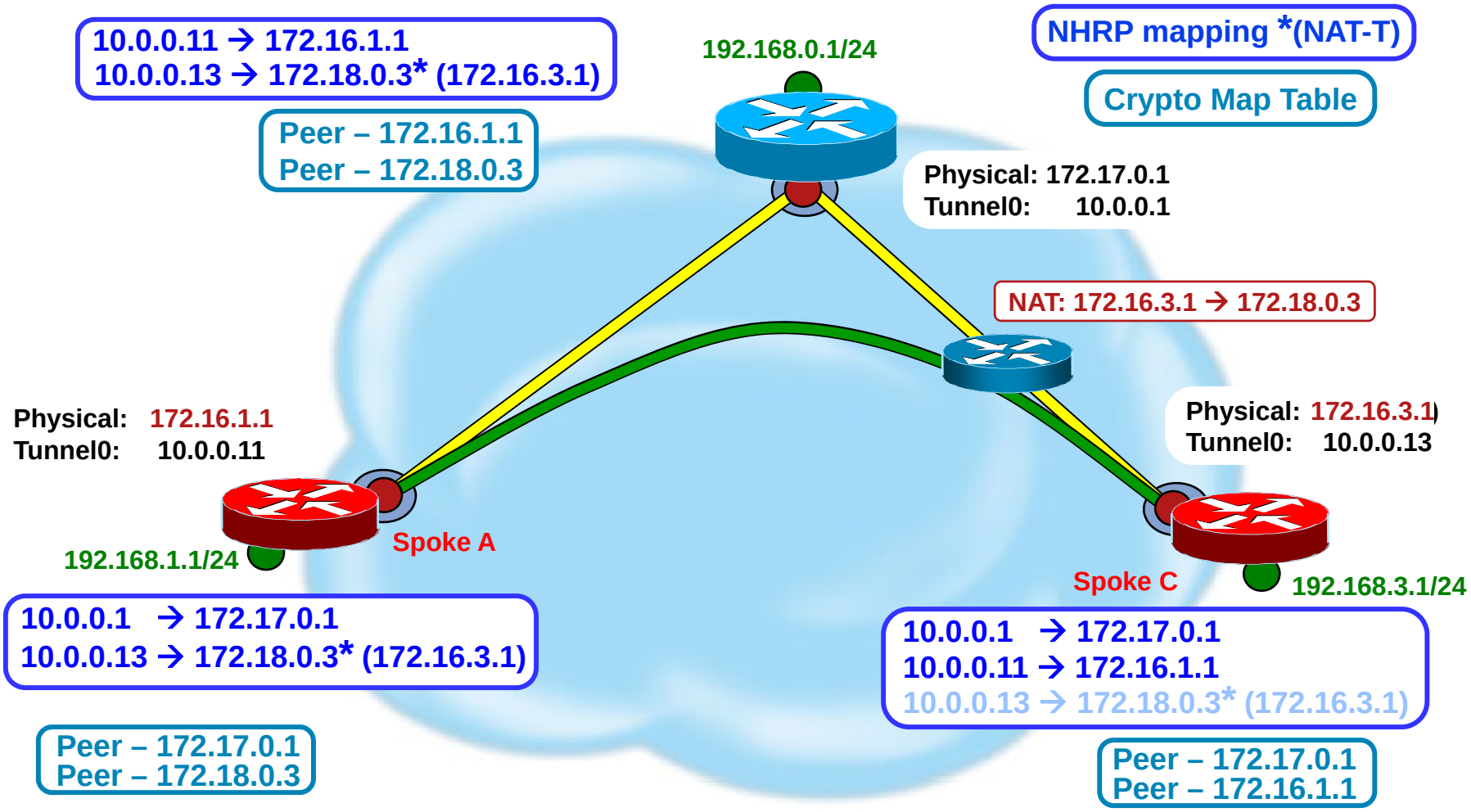
Agenda

- DMVPN Overview
- NHRP Details
  - NHRP Overview
  - NHRP Registrations
  - NHRP Resolutions/Redirects
    - Phase 2
    - Phase 3
- Network Virtualization
  - VRF-lite
  - 2547oDMVPN
- Interaction with other Features
  - NAT, IPv6, Per-tunnel QoS

DMVPN and NAT-T Spoke-Spoke
Phase 2 & 3 (12.4(6)T)

- Spoke-spoke dynamic tunnels are now supported to/from NAT translated spokes
  - Hub reports spoke's outside NAT IP address back to spoke in NHRP registration reply.
- Spoke's outside NAT IP address passed in NHRP resolution request and reply packets
- Spokes use remote spoke's outside NAT IP address to build spoke-to-spoke tunnel.
- Two spokes behind the same NAT node
  - Must be NAT translated to unique outside NAT IP address
  - NAT node must support spokes using outside IP NAT address for each other—traffic loops through NAT node
- If spoke-spoke tunnel will not come up, traffic will continue to be forwarded via the hub.

DMVPN and NAT-T



DMVPN and NAT-T
Registrations

```
NHRP: Send Registration Request via Tunnel0 vrf 0, src: 10.0.0.13, 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", src NBMA: 172.16.3.1, src protocol: 10.0.0.13, dst protocol: 10.0.0.1
  (C-1) code: no error(0), prefix: 255, mtu: 1514, hd_time: 360
Responder Address Extension(3):
Forward Transit NHS Record Extension(4):
Reverse Transit NHS Record Extension(5):
Authentication Extension(7): type:Cleartext(1), data:test
NAT Address Extension (9): (C-1) prefix: 32, client NBMA: 172.17.0.1, client protocol: 10.0.0.1
```

```
NHRP: Send Registration Reply via Tunnel0 vrf 0, src: 10.0.0.1, dst: 10.0.0.13
  (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1, shtl: 4(NSAP), sstl: 0(NSAP)
  (M) flags: "unique nat", src NBMA: 172.16.3.1, src protocol: 10.0.0.13, dst protocol: 10.0.0.1
  (C-1) code: no error(0), prefix: 255, mtu: 1514, hd_time: 360
Responder Address Extension(3):
  (C) prefix: 0, client NBMA: 172.17.0.1, client protocol: 10.0.0.1
Forward Transit NHS Record Extension(4):
Reverse Transit NHS Record Extension(5):
Authentication Extension(7): type:Cleartext(1), data:test
NAT Address Extension(9): (C-1) prefix: 32, client NBMA: 172.17.0.1, client protocol: 10.0.0.1
                          (C-2) prefix: 32, client NBMA: 172.18.0.3, client protocol: 10.0.0.13
```

DMVPN and NAT-T
Phase 3 – Resolutions

```
NHRP: Send Resolution Request via Tunnel0 vrf 0, packet size: 84, src: 10.0.0.11, dst: 10.0.0.1
  (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1, shtl: 4(NSAP), sstl: 0(NSAP)
  (M) flags: "router auth src-stable nat ", reqid: 164
      src NBMA: 172.16.1.1, src protocol: 10.0.0.11, dst protocol: 10.0.0.13
  (C-1) code: no error(0) prefix: 0, mtu: 1514, hd_time: 360
Responder Address Extension(3):
Forward Transit NHS Record Extension(4):
Reverse Transit NHS Record Extension(5):
Authentication Extension(7):  type:Cleartext(1), data:test
NAT address Extension(9):
```

```
NHRP: Send Resolution Reply via Tunnel0 vrf 0, packet size: 152, src: 10.0.0.13, dst: 10.0.0.11
  (F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1, shtl: 4(NSAP), sstl: 0(NSAP)
  (M) flags: "router auth dst-stable unique src-stable nat ", reqid: 164
      src NBMA: 172.16.1.1, src protocol: 10.0.0.11, dst protocol: 10.0.0.13
  (C-1) code: no error(0), prefix: 32, mtu: 1514, hd_time: 360,
     client NBMA: 172.16.3.1 client protocol: 10.0.0.13
 Responder Address Extension(3):
  (C) code: no error(0), prefix: 0, mtu: 1514, hd_time: 360
      client NBMA: 172.16.3.1, client protocol: 10.0.0.13
 Forward Transit NHS Record Extension(4): client NBMA: 172.17.0.1, client protocol: 10.0.0.1
 Reverse Transit NHS Record Extension(5):
 Authentication Extension(7): type:Cleartext(1), data:test
 NAT Address Extension (9): (C-1) prefix: 32, client NBMA: 172.18.0.3, client protocol: 10.0.0.13
```

IPv6 Phase 1

- IPv6 packets over DMVPN IPv4 tunnels
  - In IOS release 12.4(20)T (July 2008)
  - IPv4 infrastructure network
  - IPv6 and/or IPv4 data packets over same IPv4 GRE tunnel
- Configure IPv6 just like on other interfaces
  - Complete set of NHRP commands
    - network-id, holdtime, authentication, map, etc.
  - NHRP registers two addresses
    - Link-local for routing protocol (Automatic or Manual)*
    - Unicast Global for packet forwarding (Mandatory)

IPv6 Phase 1 Configuration

Hub

```
ipv6 unicast-routing
ipv6 cef
…
interface Tunnel0
   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 tcp adjust-mss 1360
   no ip split-horizon eigrp 1
   ipv6 address 2001:DB8:0:100::1/64
   ipv6 mtu 1400
   ipv6 eigrp 1
   no ipv6 split-horizon eigrp 1
   ipv6 nhrp authentication testv6
   ipv6 nhrp map multicast dynamic
   ipv6 nhrp network-id 100006
   ipv6 nhrp holdtime 300
   ipv6 nhrp redirect
   tunnel source Serial2/0
   tunnel mode gre multipoint
   tunnel protection ipsec profile vpnprof
!
interface Ethernet0/0
   ip address 192.168.0.1 255.255.255.0
   ipv6 address 2001:DB8::1/64
   ipv6 eigrp 1
!
interface Serial2/0
   ip address 172.17.0.1 255.255.255.252
!
ipv6 router eigrp 1
   no shutdown
```

Spoke

```
ipv6 unicast-routing
ipv6 cef
…
interface Tunnel0
   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 10.0.0.1 172.17.0.1
   ip nhrp network-id 100000
   ip nhrp holdtime 360
   ip nhrp nhs 10.0.0.1
   ip nhrp shortcut
   ip tcp adjust-mss 1360
   ipv6 address 2001:DB8:0:100::B/64
   ipv6 mtu 1400
   ipv6 eigrp 1
   ipv6 nhrp authentication testv6
   ipv6 nhrp map multicast 172.17.0.1
   ipv6 nhrp map 2001:DB8:0:100::1/128 172.17.0.1
   ipv6 nhrp network-id 100006
   ipv6 nhrp holdtime 300
   ipv6 nhrp nhs 2001:DB8:0:100::1
   ipv6 nhrp shortcut
   tunnel source Serial1/0
   tunnel mode gre multipoint
   tunnel protection ipsec profile vpnprof
!
interface Ethernet0/0
   ip address 192.168.1.1 255.255.255.0
   ipv6 address 2001:DB8:0:1::1/64
   ipv6 eigrp 1
!
interface Serial1/0
   ip address 172.16.1.1 255.255.255.252
!
ipv6 router eigrp 1
   no shutdown
```

IPv6 Phase 1
‘show ipv6 nhrp’

Hub

```
2001:DB8:0:100::B/128 via 2001:DB8:0:100::B
   Tunnel0 created 1d16h, expire 00:04:58
   Type: dynamic, Flags: unique registered used
   NBMA address: 172.16.1.1
FE80::A8BB:CCFF:FE00:C800/128 via 2001:DB8:0:100::B
   Tunnel0 created 1d16h, expire 00:04:58
   Type: dynamic, Flags: unique registered
   NBMA address: 172.16.1.1
```

Spoke

```
2001:DB8:0:100::1/128 via 2001:DB8:0:100::1
   Tunnel0 created 1d16h, never expire
   Type: static, Flags: used
   NBMA address: 172.17.0.1
FE80::A8BB:CCFF:FE00:6400/128 via FE80::A8BB:CCFF:FE00:6400
   Tunnel0 created 1d16h, expire 00:04:59
   Type: dynamic, Flags:
   NBMA address: 172.17.0.1
```

Per-tunnel QoS – 12.4(22)T

- QoS per tunnel (spoke) on hub
  - Dynamically selected Hierarchical (parent/child) QoS Policy
    - **Spoke:** Configure NHRP group name
    - **Hub:** NHRP group name mapped to QoS template policy
  - Multiple spokes with same NHRP group mapped to individual instances of same QoS template policy
- QoS policy applied at outbound physical interface
  - Classification done before GRE encapsulation by tunnel
    - ACL match against Data IP packet
    - 'qos pre-classify' not configured on tunnel interface
  - Shaping/policing done on physical after IPsec encryption
  - Can't have separate aggregate QoS policy on physical

Per-tunnel QoS Configurations

Hub

```
class-map match-all typeA_voice
  match access-group 100
class-map match-all typeB_voice
  match access-group 100
class-map match-all typeA_Routing
  match ip precedence 6
class-map match-all typeB_Routing
  match ip precedence 6

policy-map typeA
  class typeA_voice
    priority 1000
  class typeA_Routing
    bandwidth percent 20

policy-map typeB
  class typeB_voice
    priority percent 20
  class typeB_Routing
    bandwidth percent 10

policy-map typeA_parent
  class class-default
    shape average 3000000
    service-policy typeA

policy-map typeB_parent
  class class-default
    shape average 2000000
    service-policy typeB
```

Hub (cont)

```
interface Tunnel0
  ip address 10.0.0.1 255.255.255.0
  …
  ip nhrp map group typeA service-policy output typeA_parent
  ip nhrp map group typeB service-policy output typeB_parent
  …
  ip nhrp redirect
  no ip split-horizon eigrp 100
  ip summary-address eigrp 100 192.168.0.0 255.255.192.0 5
  …
```

Spoke1

```
interface Tunnel0
  ip address 10.0.0.11 255.255.255.0
  …
  ip nhrp group typeA
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp nhs 10.0.0.1
  …
```

Spoke2

```
interface Tunnel0
  ip address 10.0.0.12 255.255.255.0
  …
  ip nhrp group typeB
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp nhs 10.0.0.1
  …
```

Spoke3

```
interface Tunnel0
  ip address 10.0.0.13 255.255.255.0
  …
  ip nhrp group typeA
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp nhs 10.0.0.1
  …
```

Per-tunnel QoS
QoS Output

Hub#show ip nhrp

```
10.0.0.11/32 via 10.0.0.11
   Tunnel0 created 21:24:03, expire 00:04:01
   Type: dynamic, Flags: unique registered
   NBMA address: 172.16.1.1
   Group: typeA
10.0.0.12/32 via 10.0.0.12
   Tunnel0 created 21:22:33, expire 00:05:30
   Type: dynamic, Flags: unique registered
   NBMA address: 172.16.2.1
   Group: typeB
10.0.0.13/32 via 10.0.0.13
   Tunnel0 created 00:09:04, expire 00:04:05
   Type: dynamic, Flags: unique registered
   NBMA address: 172.16.3.1
   Group: typeA
```

Hub#show ip nhrp group-map

```
Interface: Tunnel0
   NHRP group: typeA
      QoS policy: typeA_parent
      Tunnels using the QoS policy:
      Tunnel destination overlay/transport address
      10.0.0.11/172.16.1.1
      10.0.0.13/172.16.3.1
   NHRP group: typeB
      QoS policy: typeB_parent
      Tunnels using the QoS policy:
      Tunnel destination overlay/transport address
      10.0.0.12/172.16.2.1
```

Hub#show policy-map multipoint tunnel 0 <spoke> output

```
Interface Tunnel0 ↔ 172.16.1.1

  Service-policy output: typeA_parent
    Class-map: class-default (match-any)
      19734 packets, 6667163 bytes
      shape (average) cir 3000000, bc 12000, be 12000

      Service-policy : typeA
        Class-map: typeA_voice (match-all)      3737 packets, 4274636 bytes
        Class-map: typeA_Routing (match-all) 14424 packets, 1269312 bytes
        Class-map: class-default (match-any)   1573 packets, 1123215 bytes

Interface Tunnel0 ↔ 172.16.2.1

  Service-policy output: typeB_parent
    Class-map: class-default (match-any)
      11420 packets, 1076898 bytes
      shape (average) cir 2000000, bc 8000, be 8000

      Service-policy : typeB
        Class-map: typeB_voice (match-all)      1005 packets, 128640 bytes
        Class-map: typeB_Routing (match-all) 10001 packets, 880088 bytes
        Class-map: class-default (match-any)   414 packets, 68170 bytes

Interface Tunnel0 ↔ 172.16.3.1

  Service-policy output: typeA_parent
    Class-map: class-default (match-any)
      5458 packets, 4783903 bytes
      shape (average) cir 3000000, bc 12000, be 12000

      Service-policy : typeA
        Class-map: typeA_voice (match-all)      4914 packets, 4734392 bytes
        Class-map: typeA_Routing (match-all) 523 packets, 46004 bytes
        Class-map: class-default (match-any)   21 packets, 14995 bytes
```

Per-tunnel QoS
Scaling – 7200 NPE-G1/VAM2+

Stable	CPU Utilization			
Tunnels/Active	No traffic	28 Mbps	38 Mbps	47.6 Mbps
500/150	9%	41%	52%	64%
600/180	12%	49%	62%	75%
700/210	14%	53%	73%	85%

Unstable	CPU Utilization			
Tunnels/Active	N/A	28 Mbps	38 Mbps	47.6 Mbps
500/150		43%	52%	64%
600/180		51%	68%(99%)	78%(99%)
700/210		53%(99%)	76%(99%)	99%(flapping)

- **Key**
  1) **Tunnels/Active = Number of tunnels versus number of active shapers**
  2) **"Unstable" corresponds to detaching and re-attaching service policy on the tunnels**
  3) **All CPU values are observed steady state values (99%) within braces means CPU was 99% for a while before stabilization.**
  4) **Original EC = 700/210 @ 47.6 Mbps <= 80% CPU under unstable conditions (presumably)**
  5) **For 7200 NPE-G2/VSA low scale numbers, CSCsu73714 filed.**

DMVPN Futures

- Hardware support
  - Phase 3 on 6500 and ASR (Release 5)
  - Multicast switching over DMVPN on 6500
- Tunnel Health Monitoring
  - Extention NHRP MIB
  - Backup NHS
  - Tunnel interface up/down state change
- Routing Protocol Scalability/Convergence
- DHCP over DMVPN
  - Spoke tunnel IP address and LAN IP address/pool
- IPv6 – Second Phase
  - Phase 2: IPv6 over IPv6 GRE encrypted tunnel

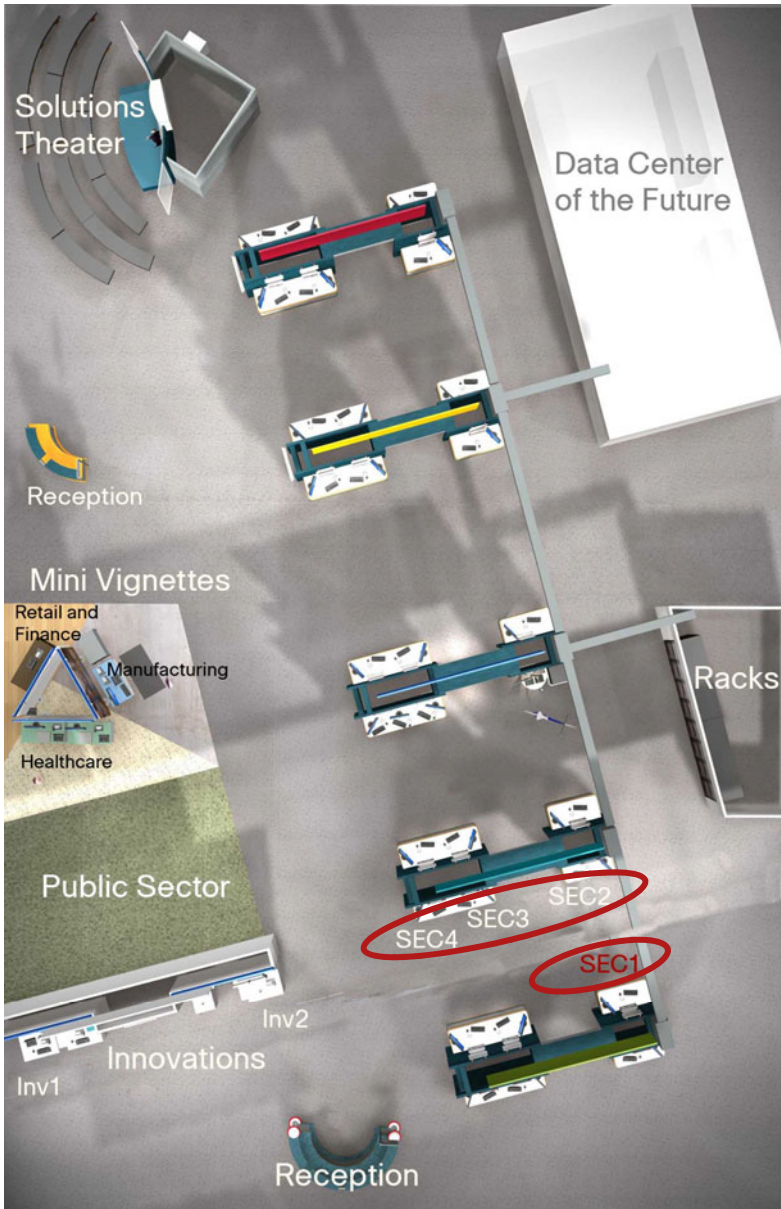
Q and A


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

Please Visit the Cisco Booth in the World of Solutions

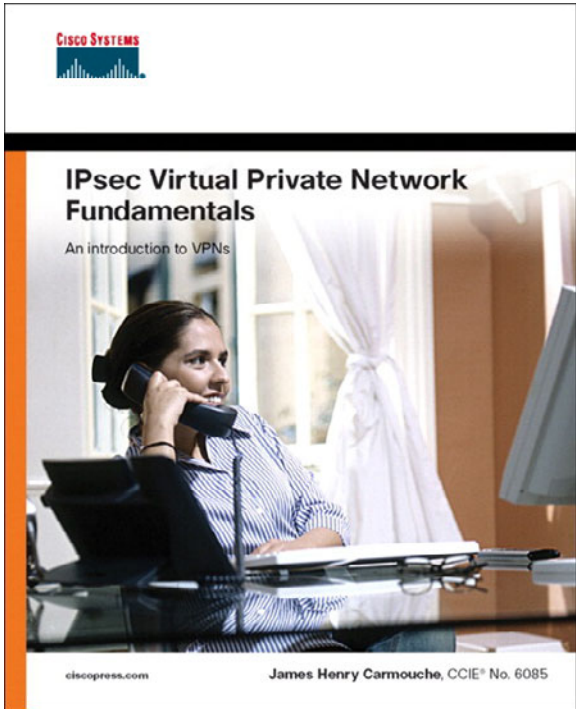
See the technology in action

- 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



Recommended Reading

- IPsec Virtual Private Network Fundamentals, ISBN: 1-58705-207-5
- IPSec VPN Design, ISBN: 1-58705-111-7
- MPLS and VPN Architectures, Second Edition, ISBN: 1-58705-002-1



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.

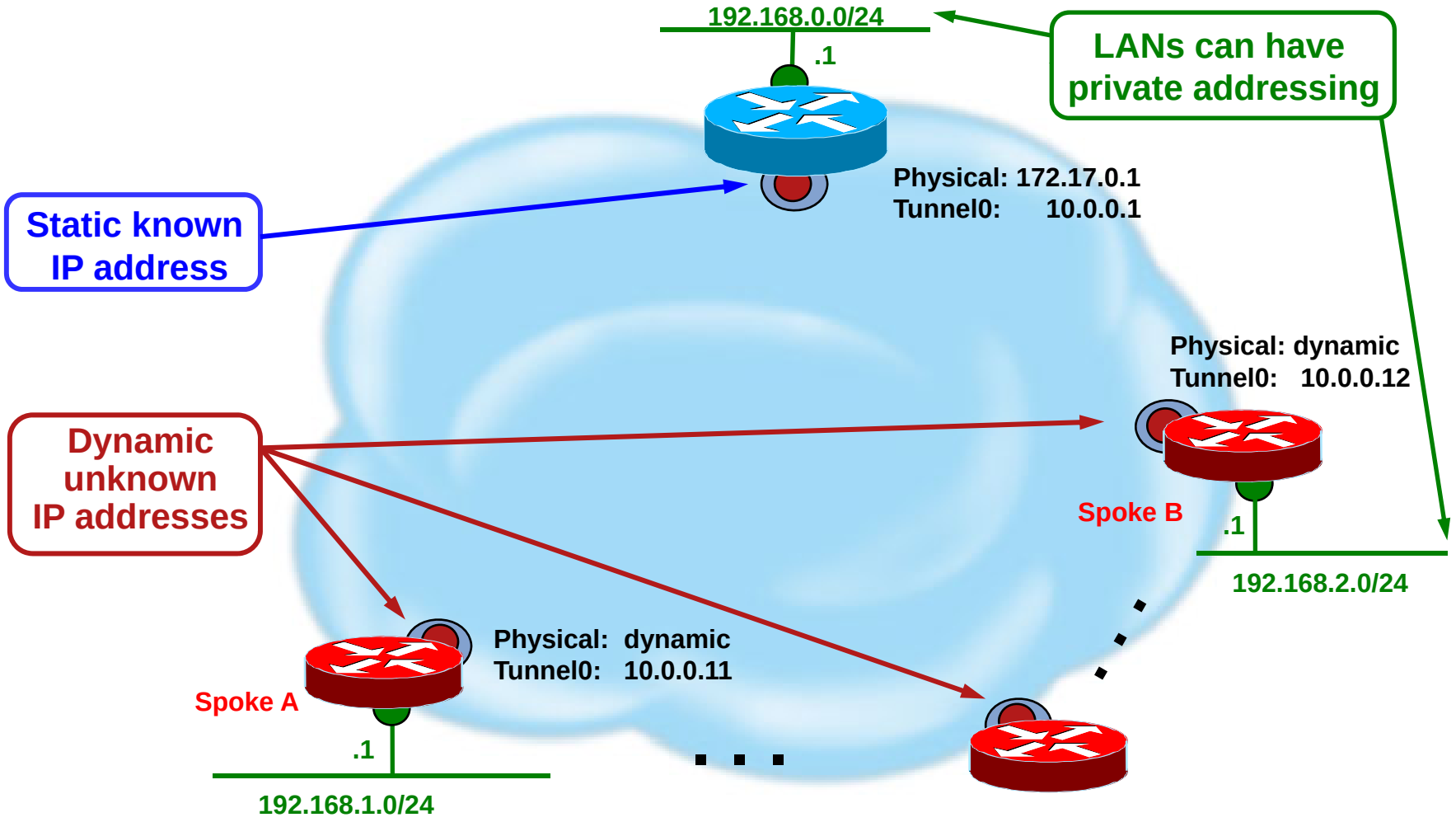
Appendix


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

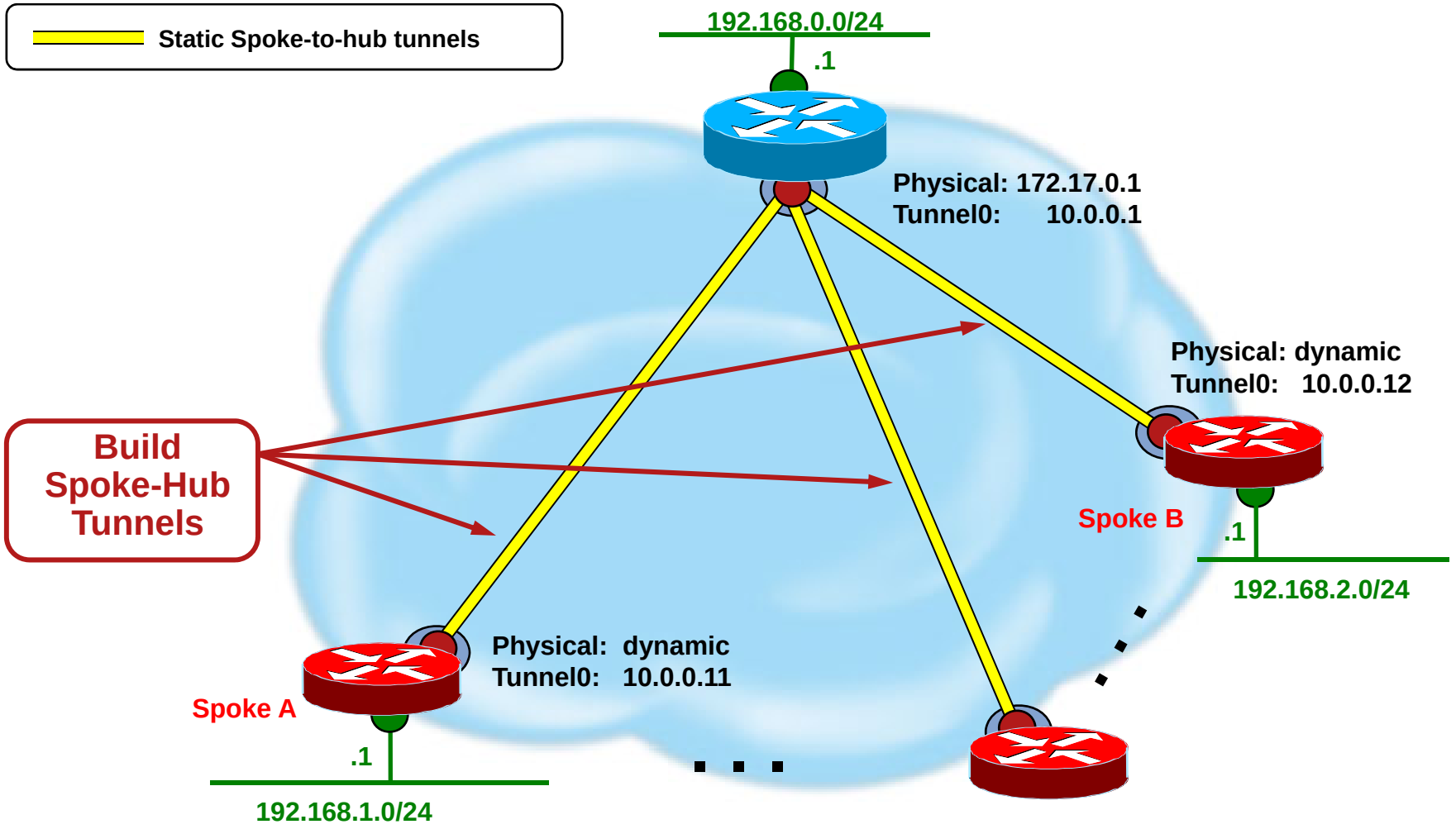
Appendix

- DMVPN Overview
- NHRP Details
  - NHRP Overview
  - NHRP Registrations
  - NHRP Resolutions/Redirects
    - Phase 2
    - Phase 3
- Network Virtualization
  - VRF-lite
  - 2547oDMVPN

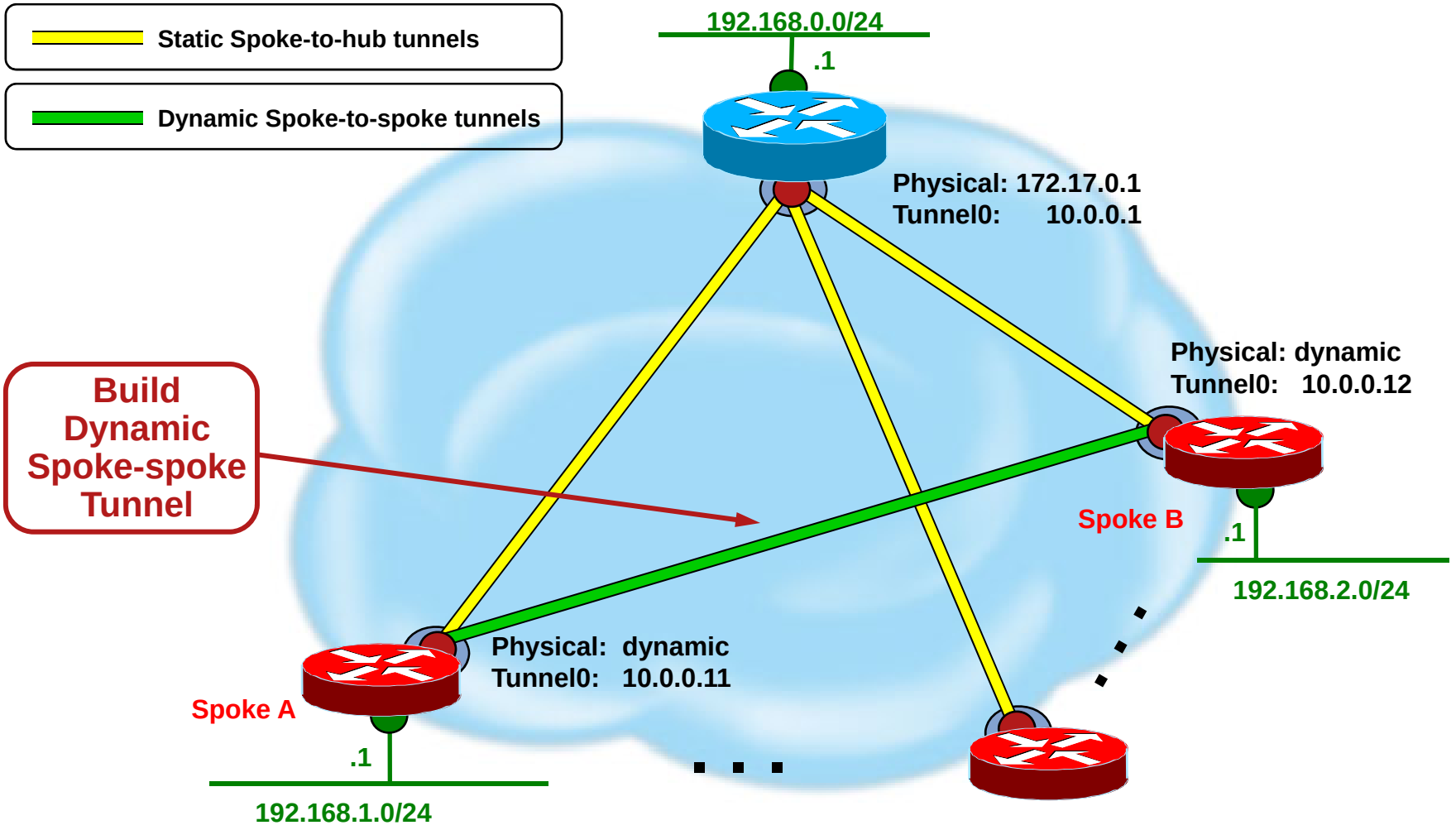
Dynamic Multipoint VPN—Example



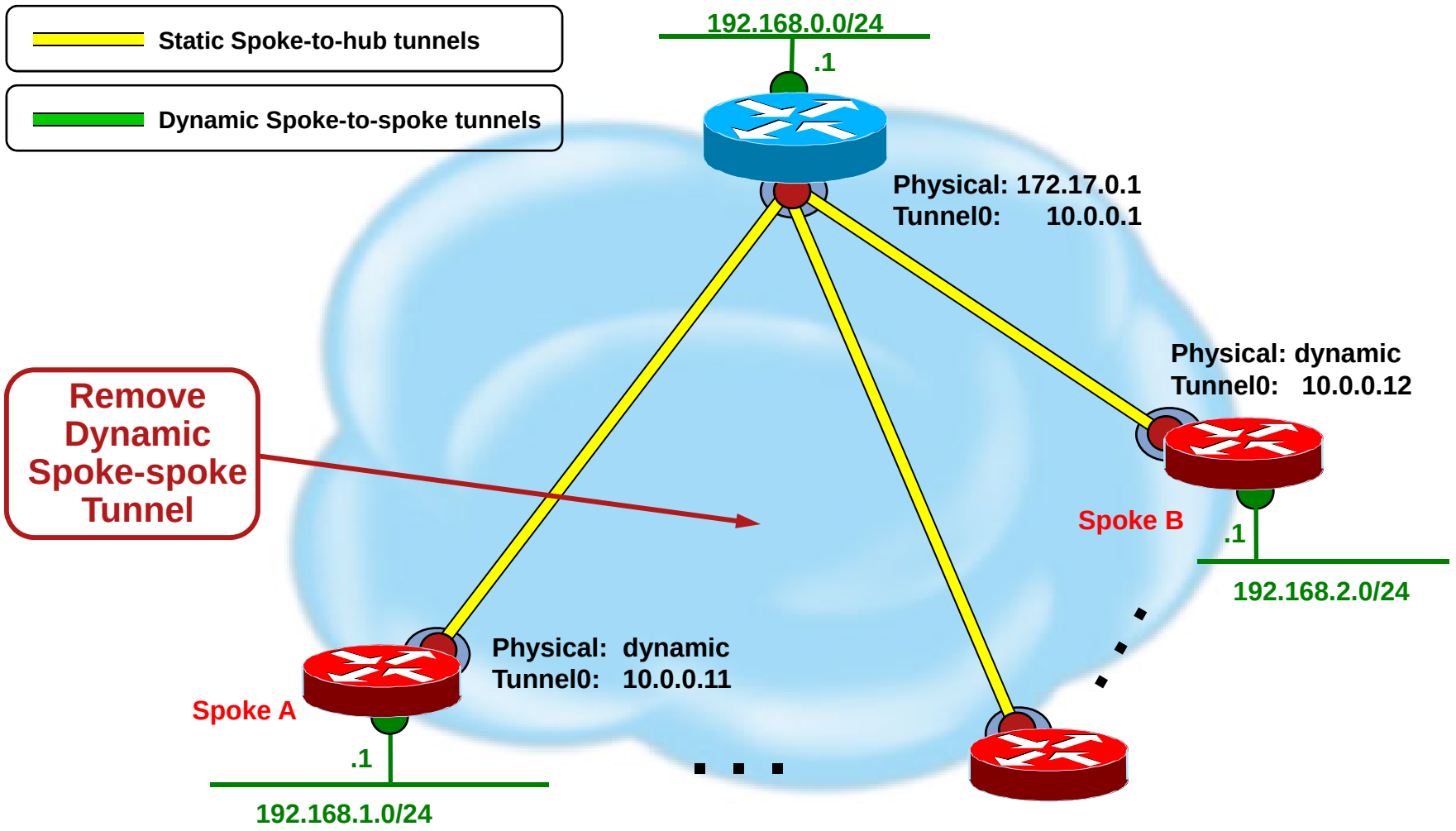
Dynamic Multipoint VPN—Example (Step 1)



Dynamic Multipoint VPN—Example (Step 2)



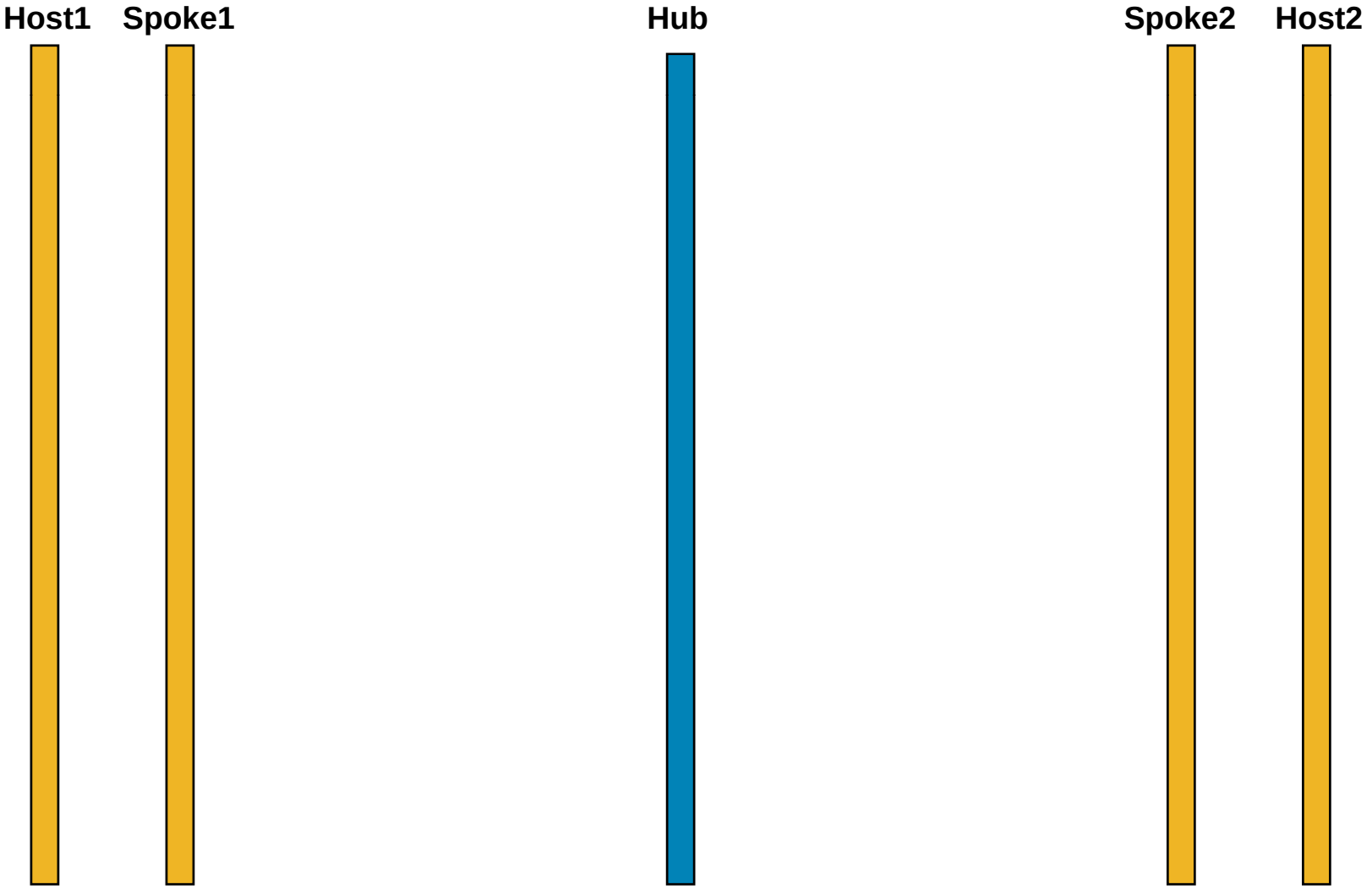
Dynamic Multipoint VPN—Example (Step 3)



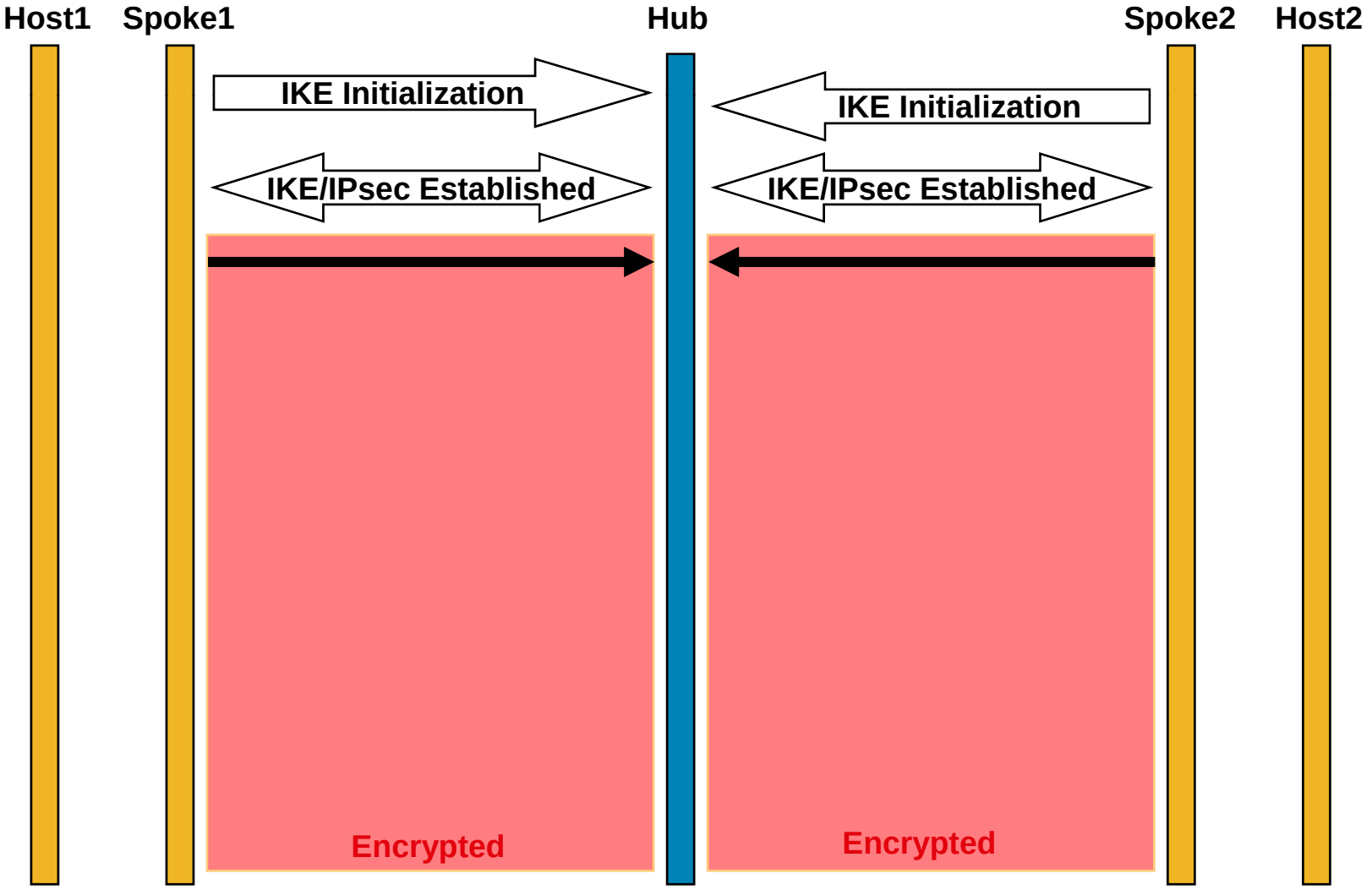
Appendix

- DMVPN Overview
- NHRP Details
  - NHRP Overview
  - NHRP Registrations
  - NHRP Resolutions/Redirects
    - Phase 2
    - Phase 3
- Network Virtualization
  - VRF-lite
  - 2547oDMVPN

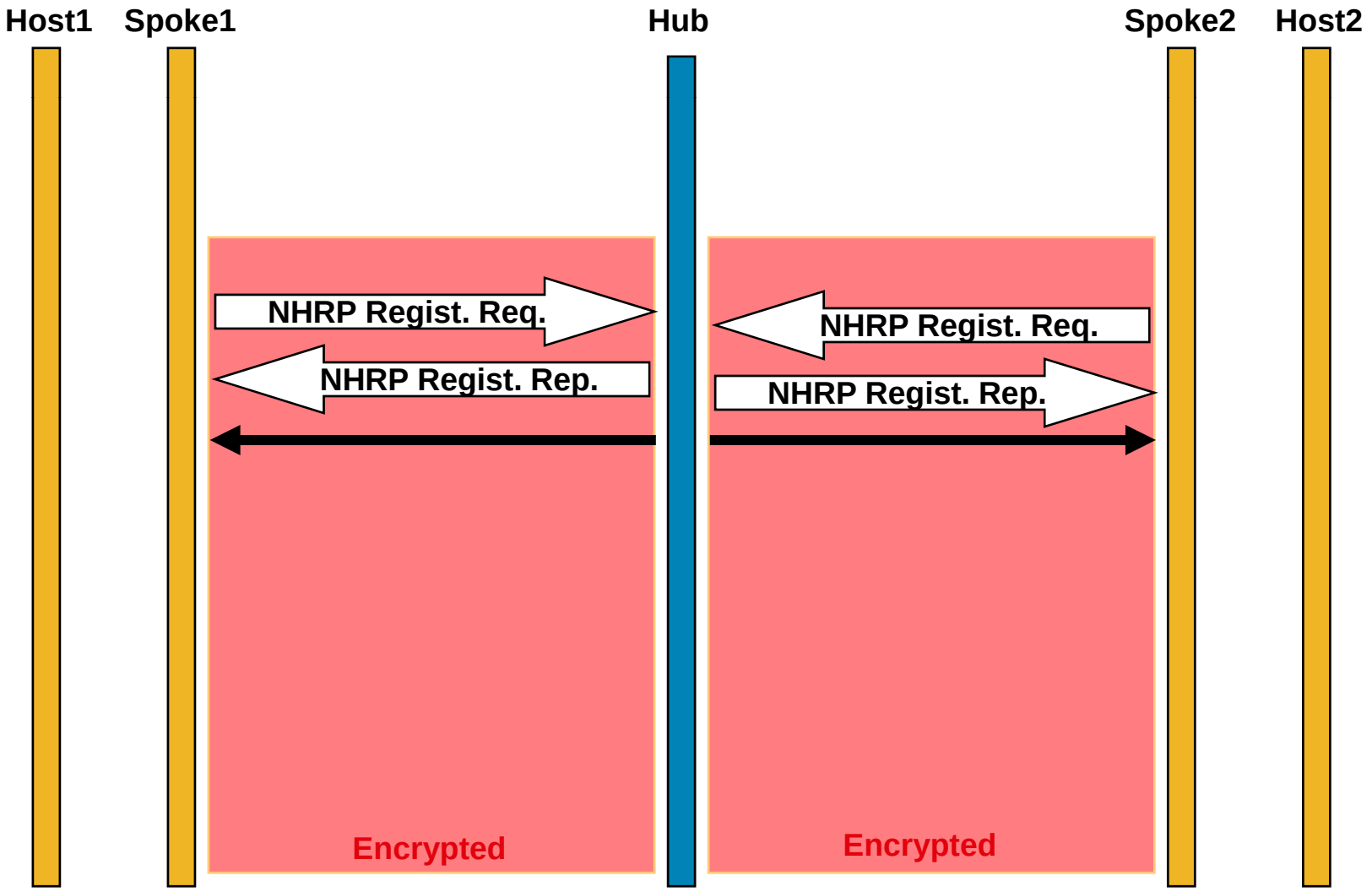
NHRP Registration
Building Hub-and-Spoke Tunnels



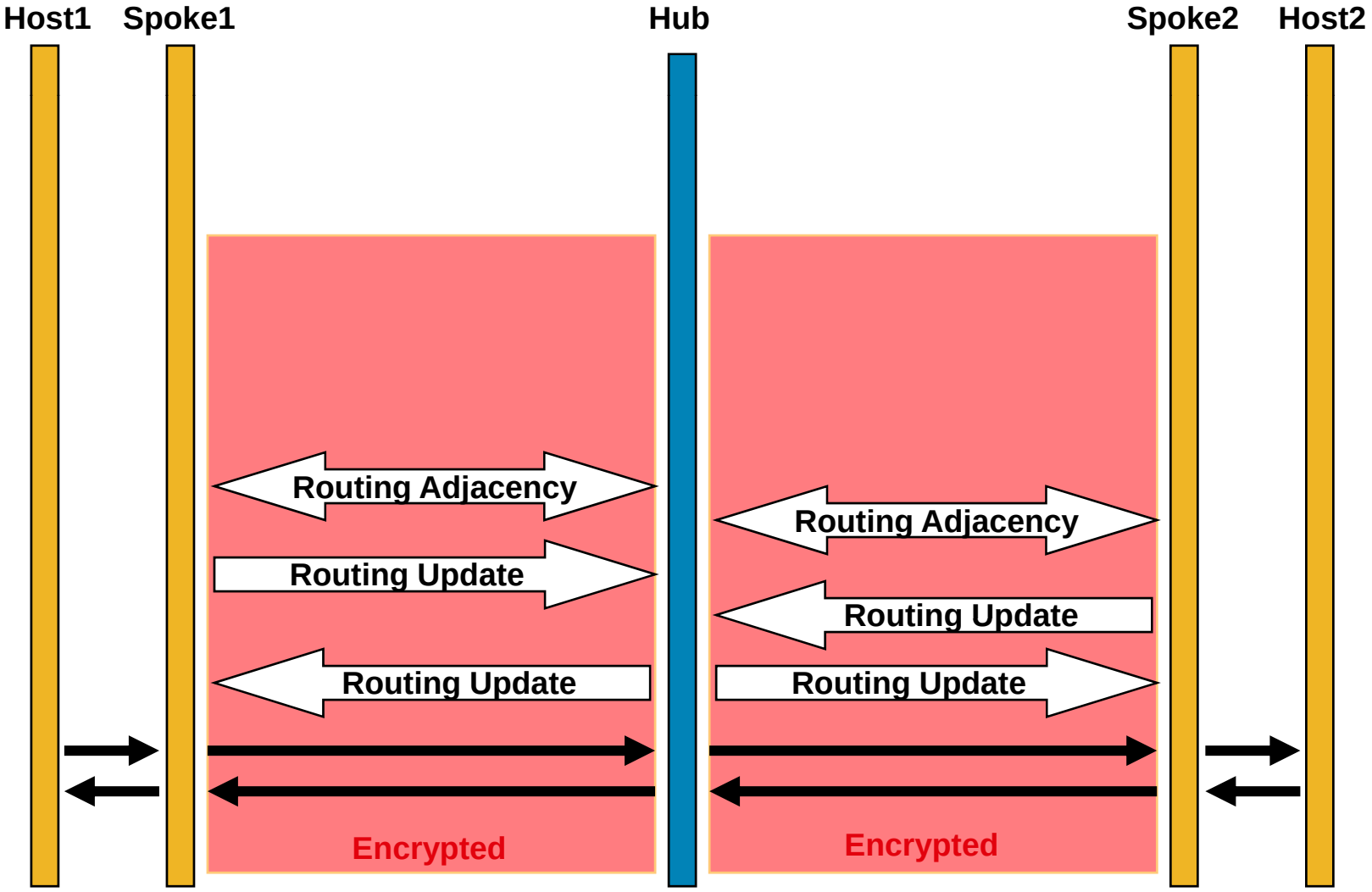
NHRP Registration
Building Hub-and-Spoke Tunnels (Step 1)



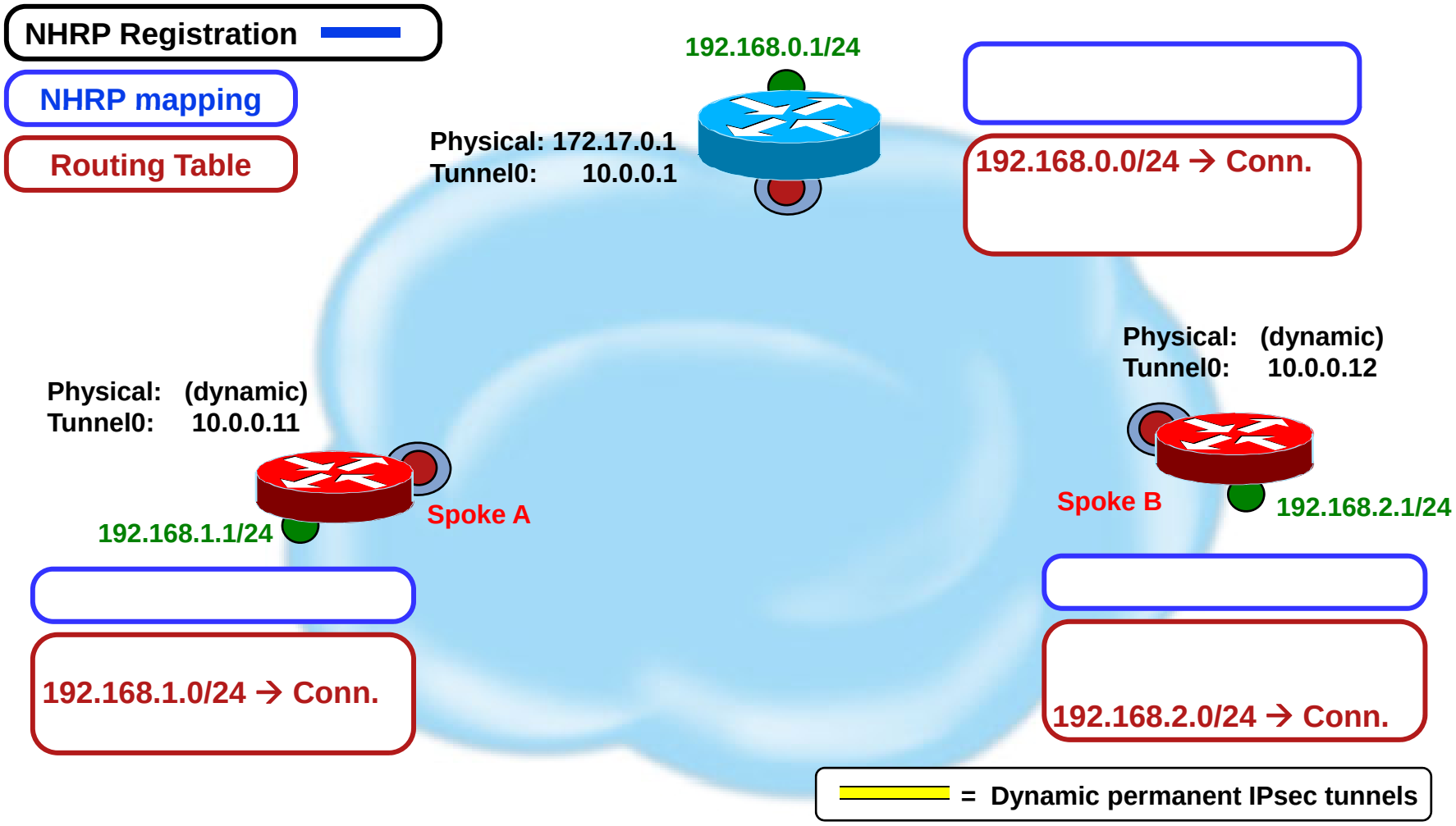
NHRP Registration
Building Hub-and-Spoke Tunnels (Step 2)



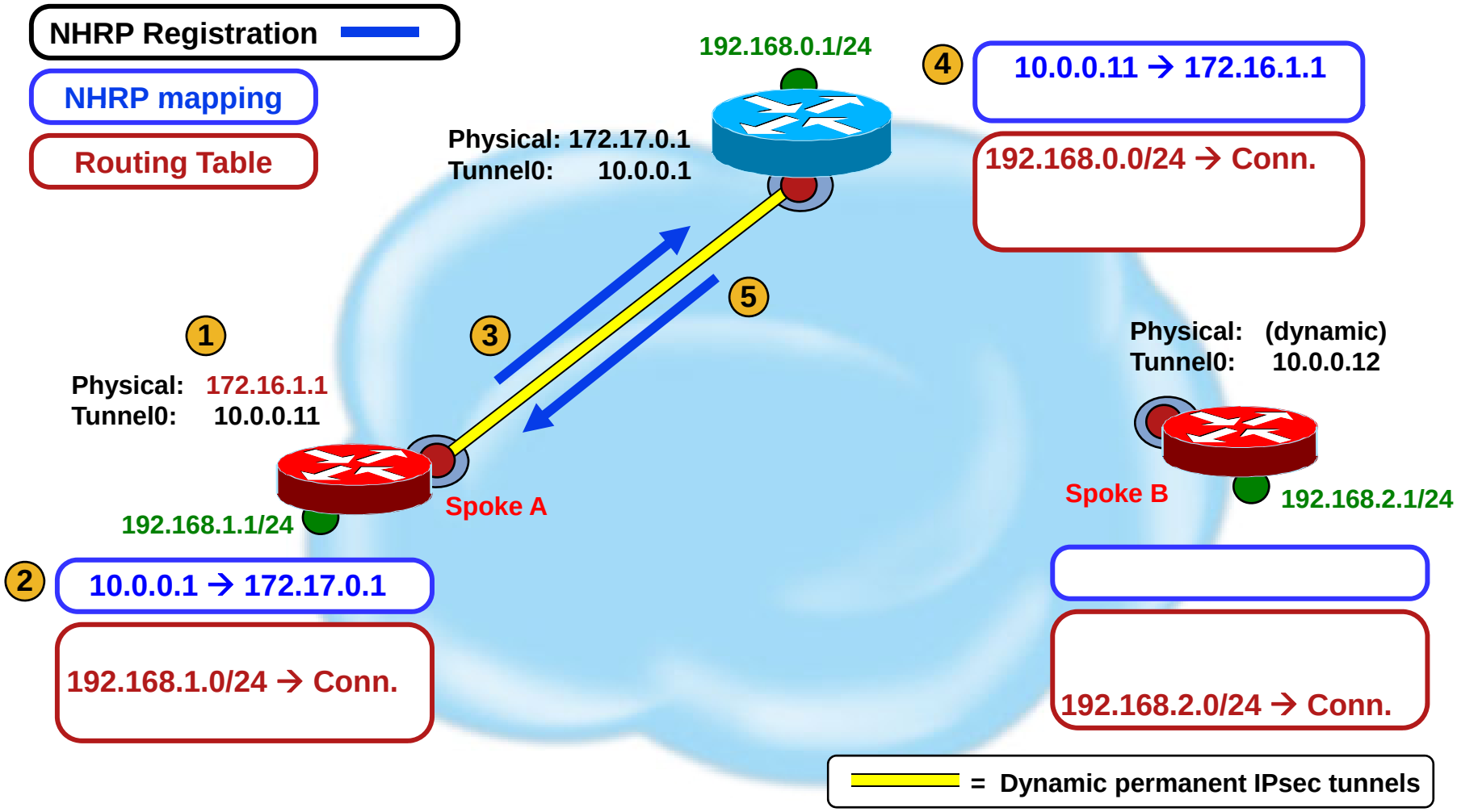
NHRP Registration
Routing Adjacency (Step 3)



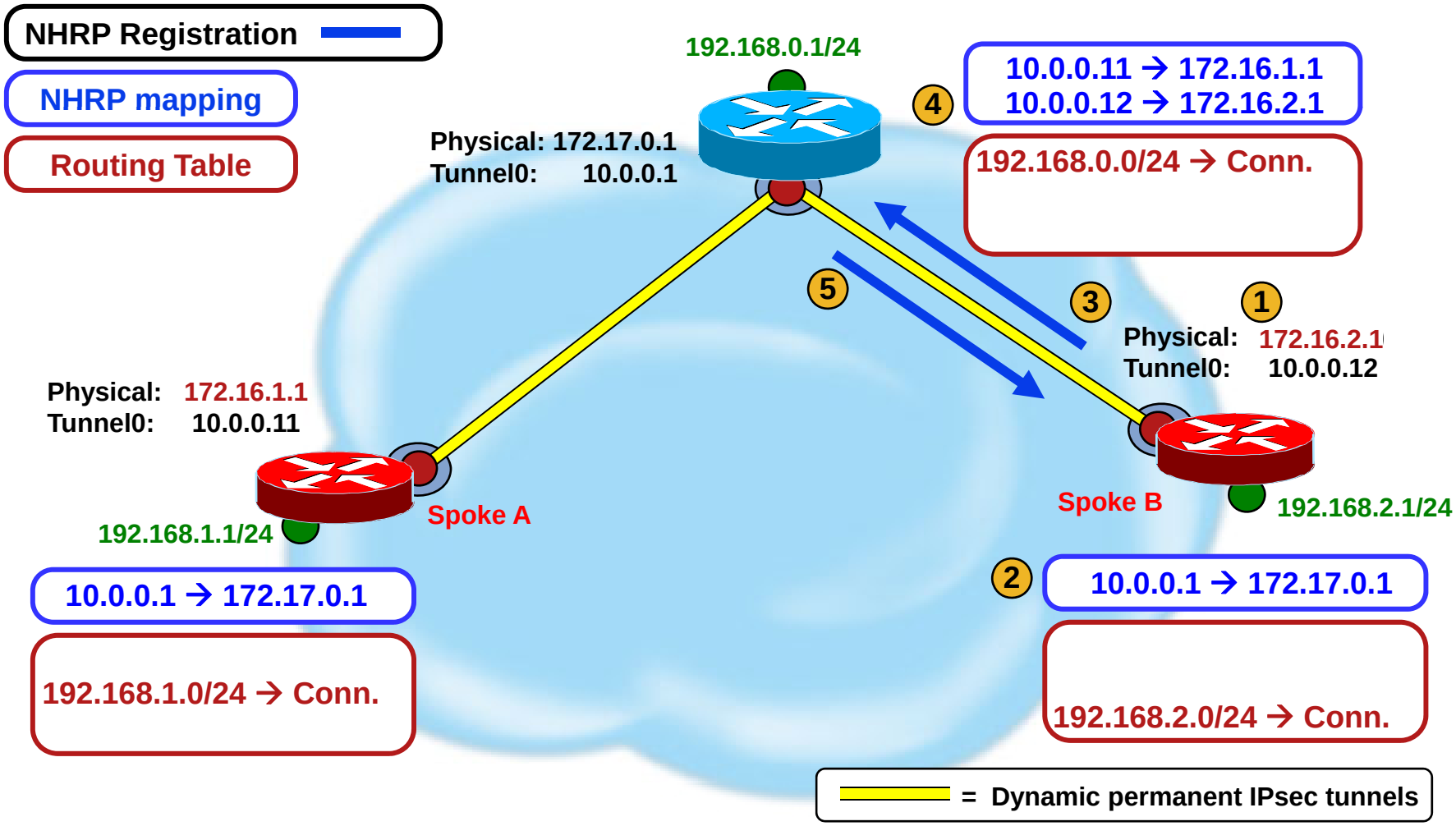
NHRP Registration
Building Hub-and-Spoke Tunnels



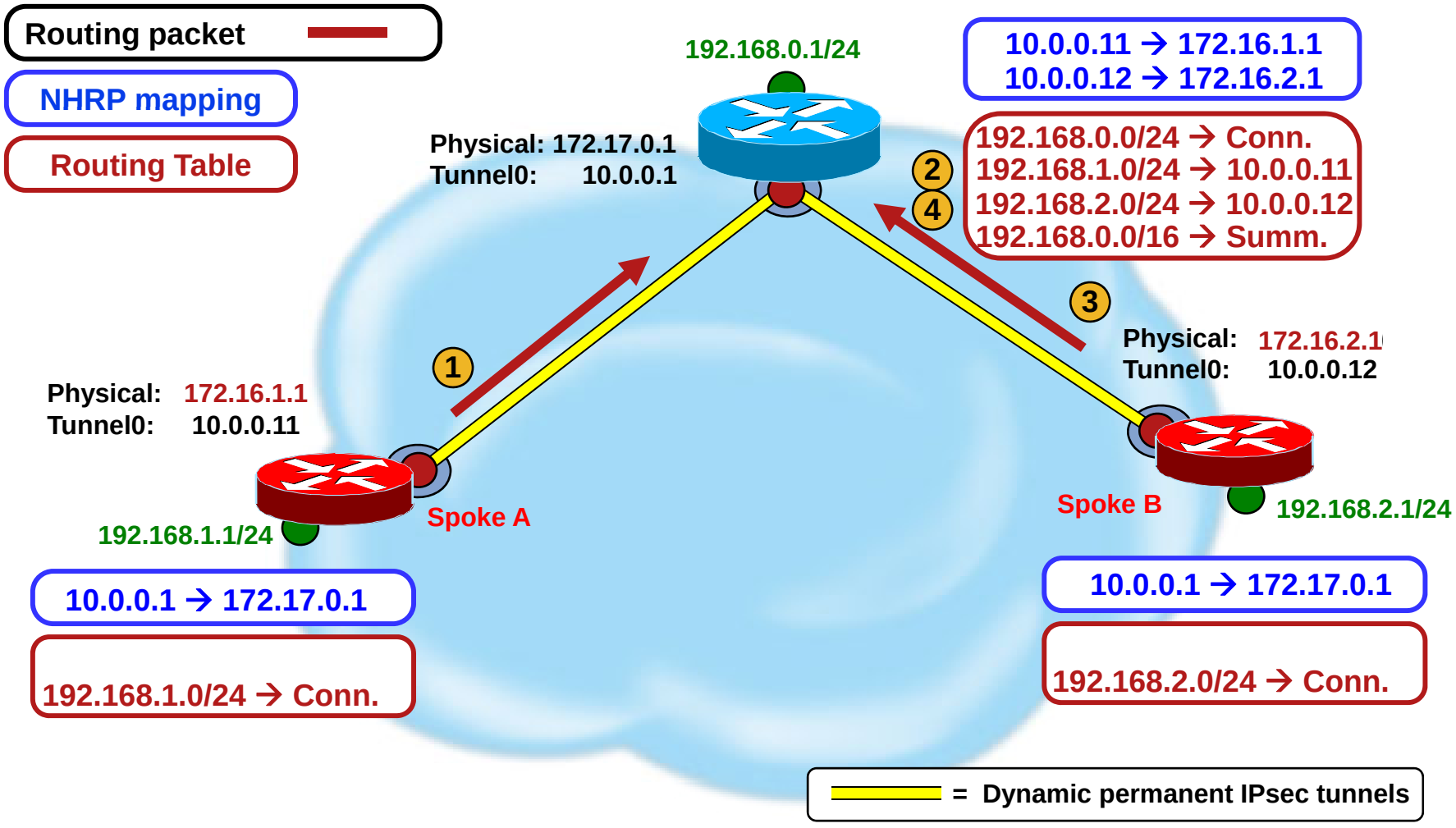
NHRP Registration
Building Hub-and-Spoke Tunnels (Step 1&2)



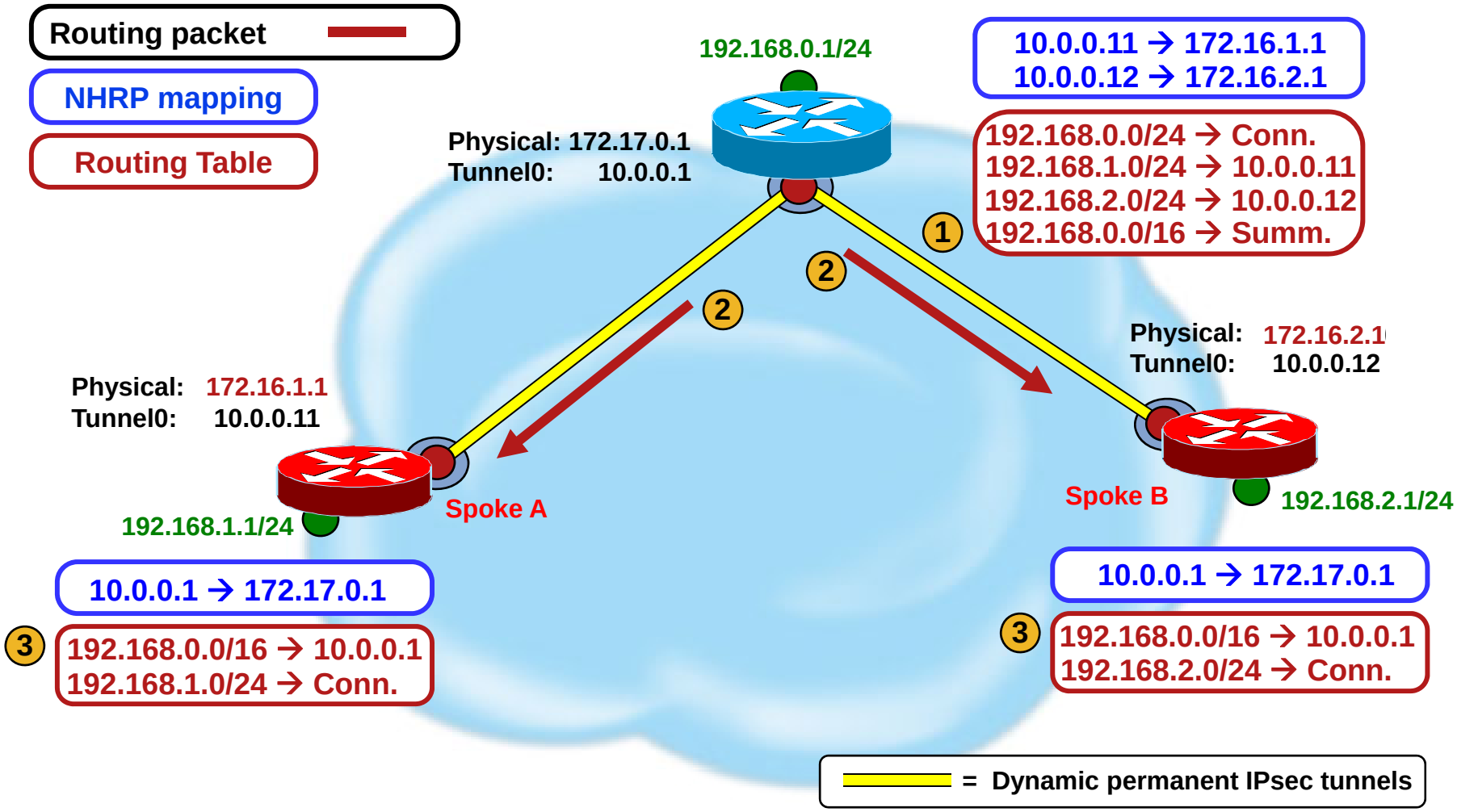
NHRP Registration
Building Hub-and-Spoke Tunnels (Step 1&2)



NHRP Registration
Routing Adjacency (Step 3a)



NHRP Registration
Routing Adjacency (Step 3b)



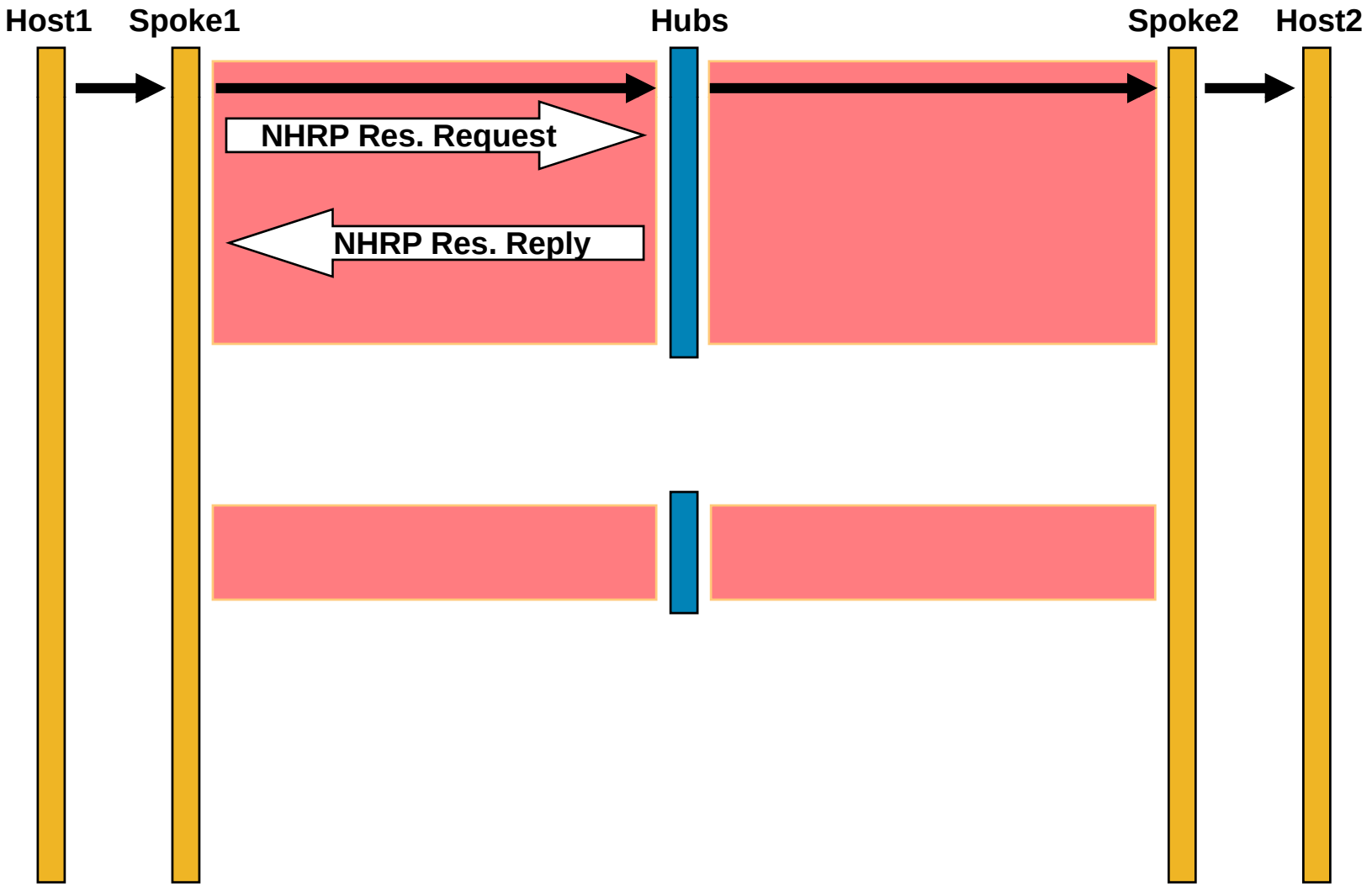
Appendix

- DMVPN Overview
- NHRP Details
  - NHRP Overview
  - NHRP Registrations
  - NHRP Resolutions/Redirects
    - Phase 2 (old)
    - Phase 2
    - Phase 3
- Network Virtualization
  - VRF-lite
  - 2547oDMVPN

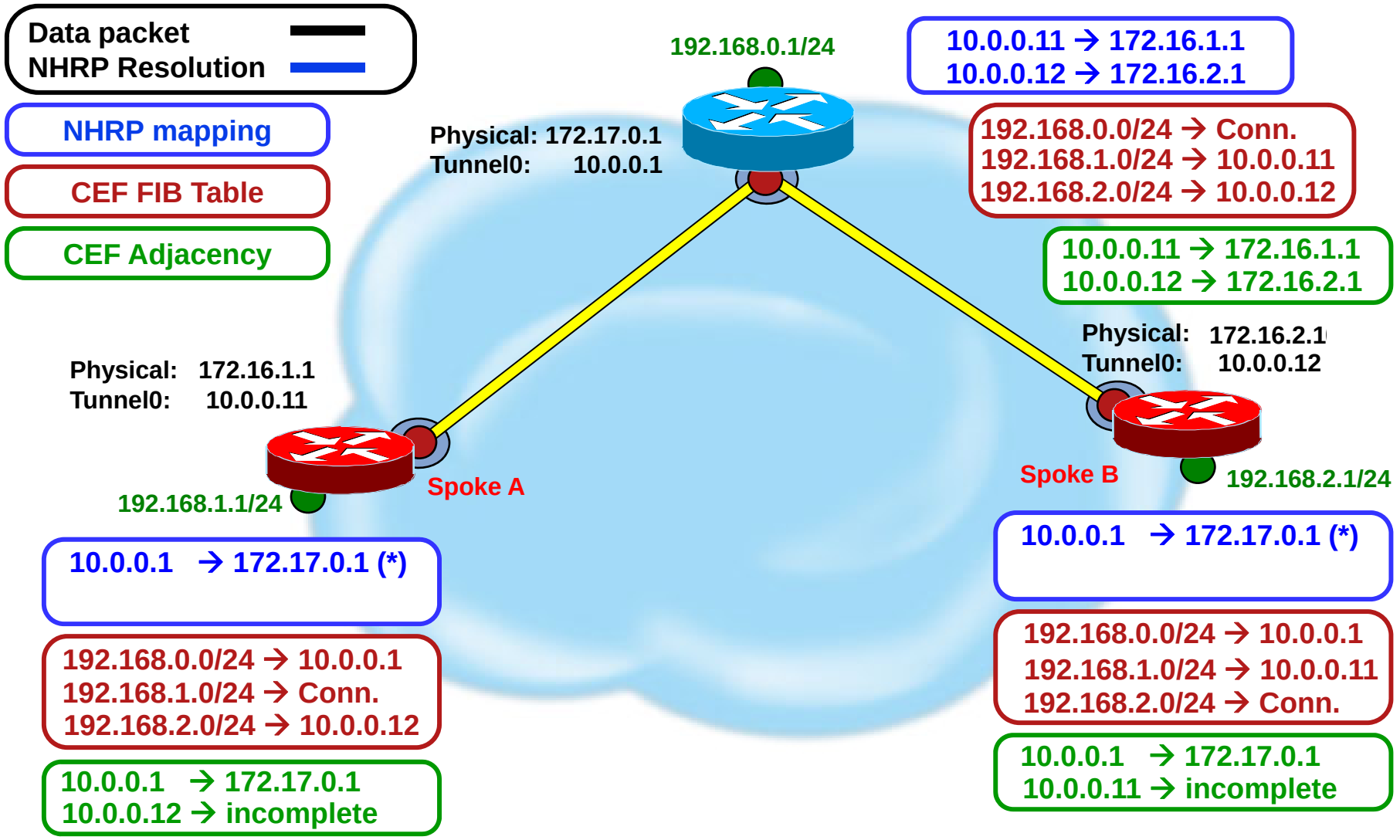
Phase 2 (old)
Sending NHRP Resolutions

- CEF FIB table has IP next-hop of tunnel IP address of remote spoke for network behind remote spoke
- Triggered by IP next-hop from FIB pointing to glean or incomplete adjacency entry (no valid adjacency entry)
- Send resolution request for IP next-hop (tunnel IP address) of remote Spoke
- Resolution request forwarded via NHS path
- Resolution request answered by last NHS in path
- Resolution reply forwarded back via NHS path
- Data packets forwarded (process-switched) on NHS path until last tunnel hop

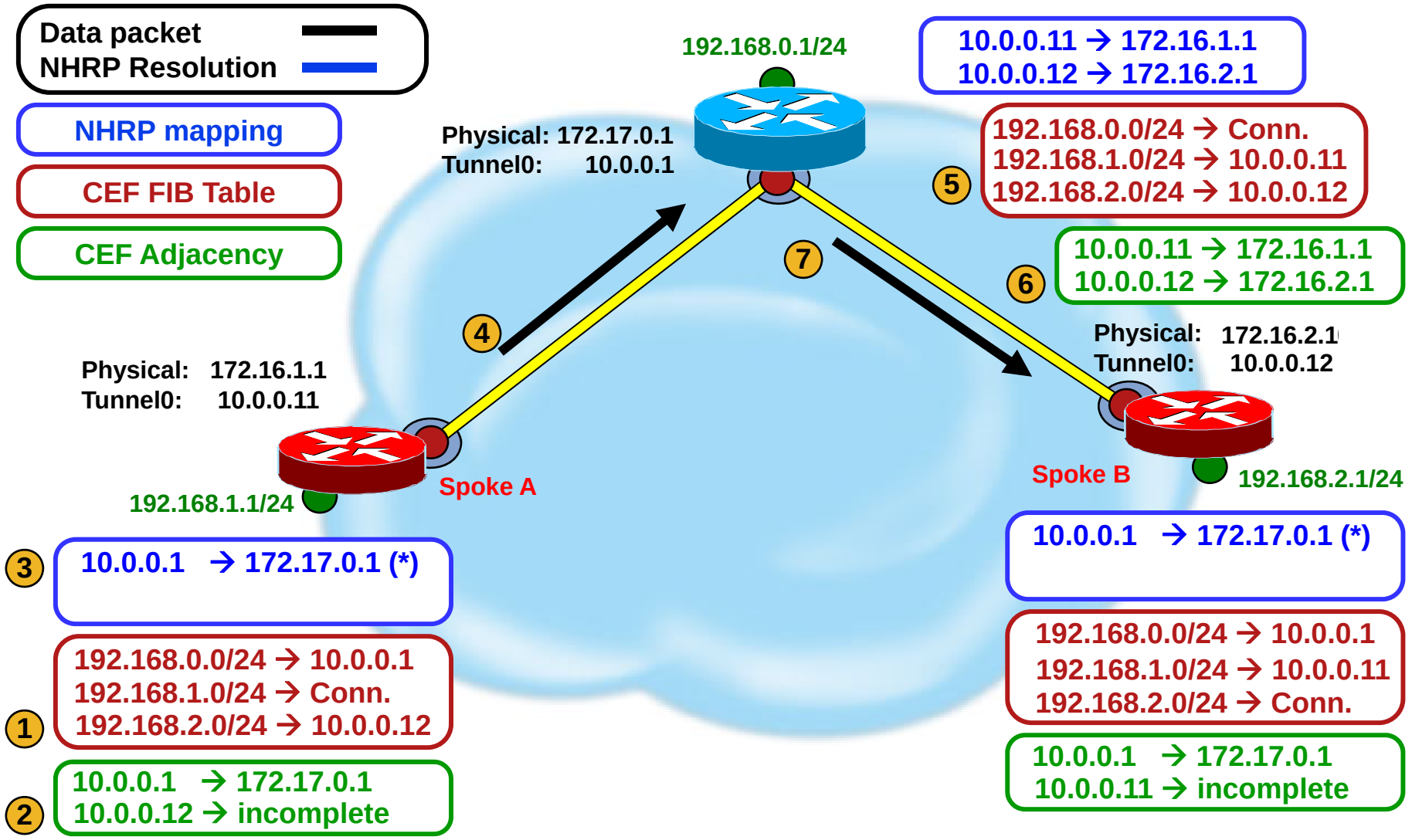
Phase 2 (old)
NHRP Resolution Request/Reply (Step 1)



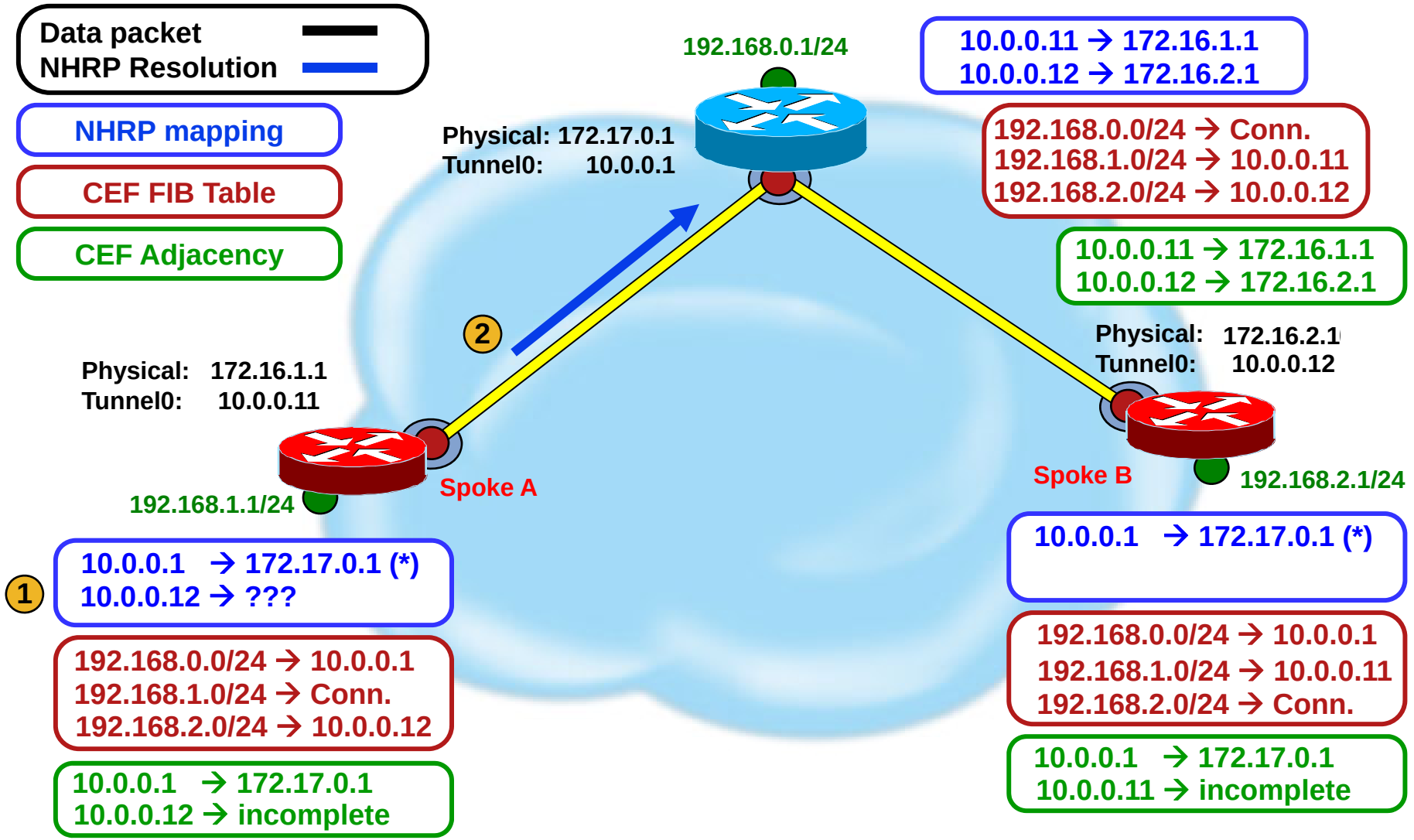
Phase 2 (old)
NHRP Resolution Request (starting state)



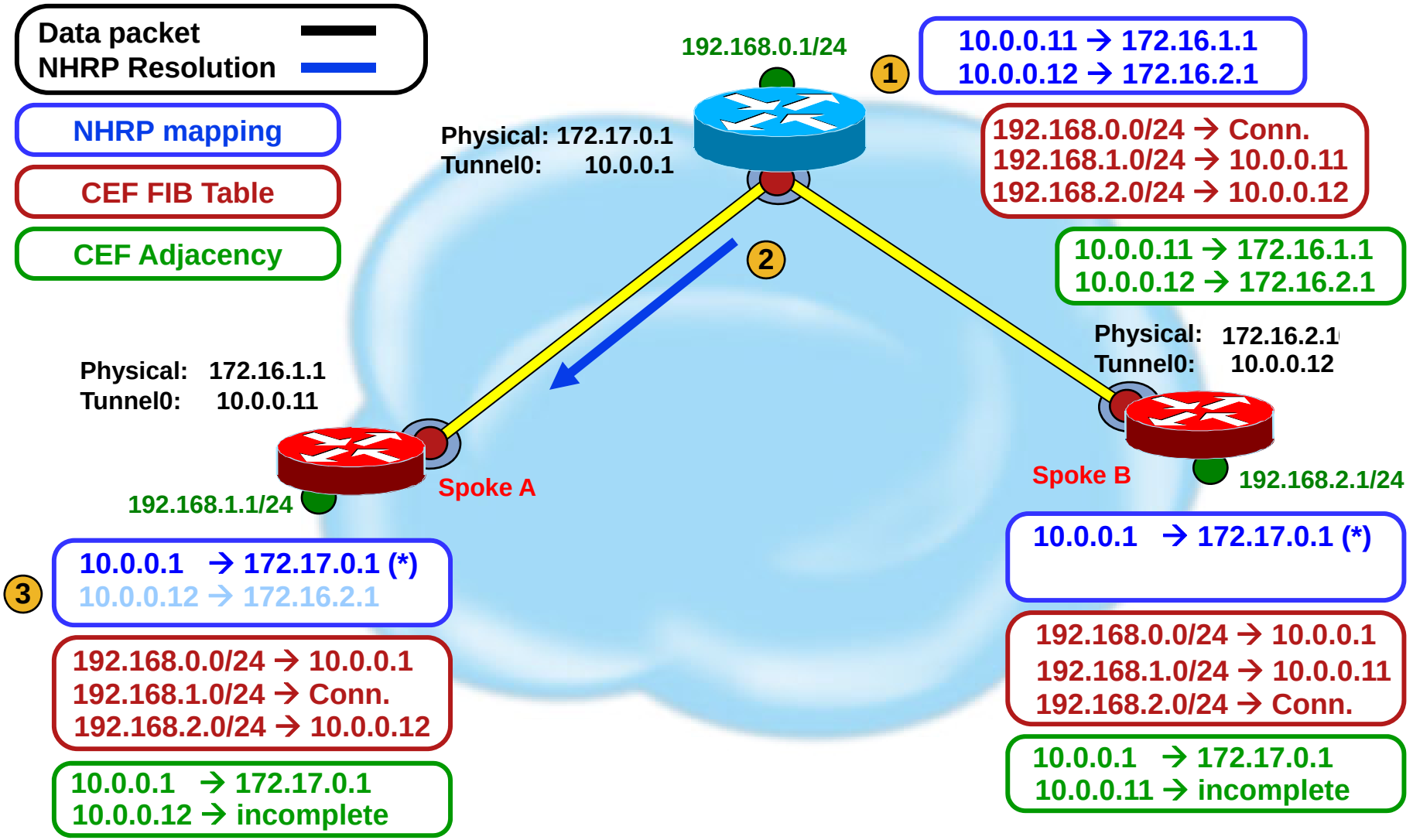
Phase 2 (old)
NHRP Resolution Request (Step 1a)



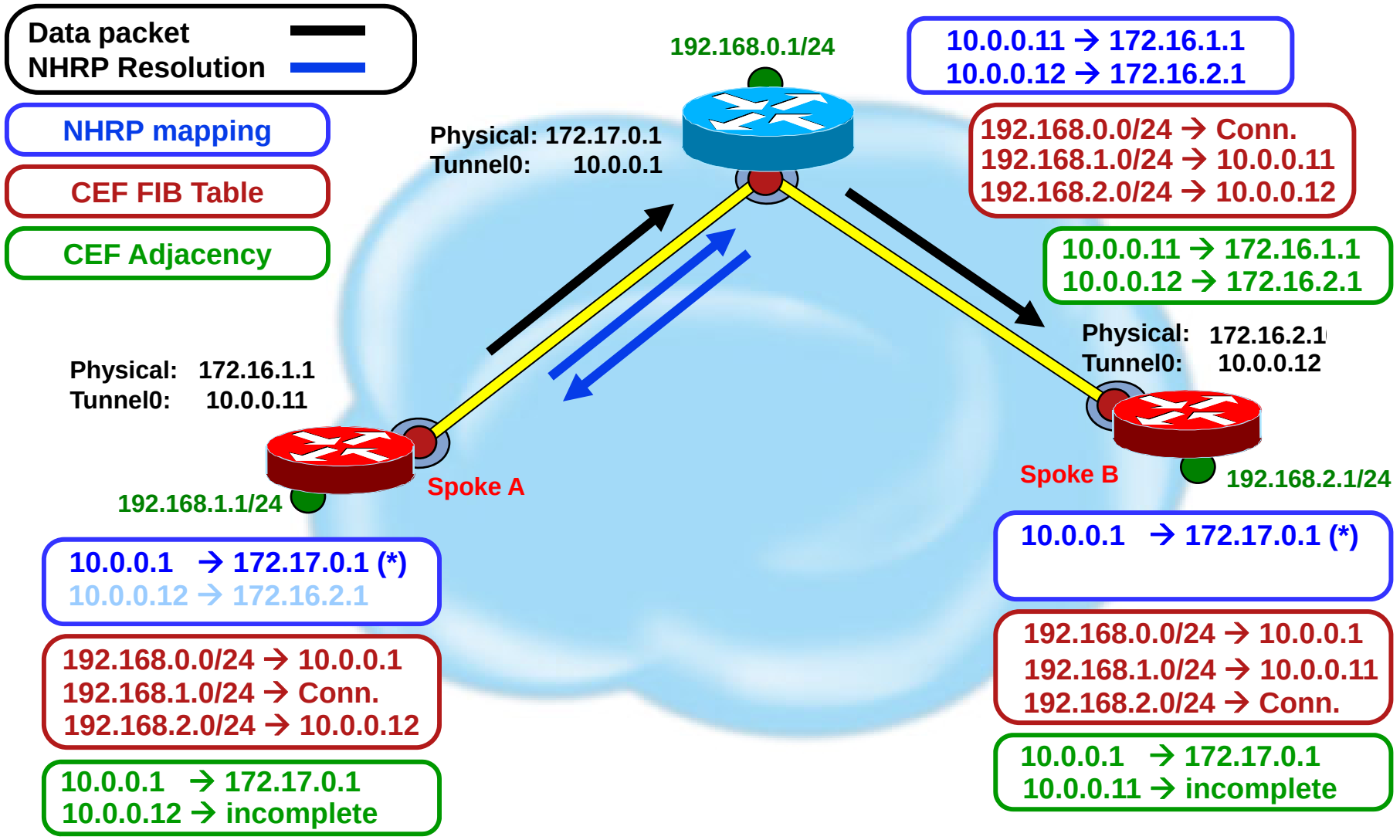
Phase 2 (old)
NHRP Resolution Request (Step 1b)



Phase 2 (old)
NHRP Resolution Reply (Step 1c)



Phase 2 (old)
NHRP Resolution Request/Reply



Phase 2 (old)
Receiving NHRP Resolution Request

- Insert protocol source to NBMA source address mapping, from request into mapping table (no socket) if not already there
- Look up protocol destination in mapping table
  - If found (authoritative) – Answer Request
- Look up protocol destination in routing table
  - If Outbound interface is not the tunnel
    - This node is the exit point – Answer Request
- Look up protocol destination IP next-hop
  - Found Entry (socket)
    - Forward to NBMA from mapping table
  - Not found or Found Entry (no socket)
    - Forward to NHS

Phase 2 (old)
NHRP Resolution Reply

- Lookup protocol destination in routing table for matching network, subnet mask and IP next-hop.
- Create NHRP local mapping entry for protocol destination network with mask-length to NBMA address
- Create NHRP Resolution Response with protocol destination, NBMA address and mask-length
- Resolution Response Forwarding

Look up protocol source in mapping table

Found Entry (socket)

Forward to NBMA from mapping table

Not found or Found Entry (no socket)

Forward to IP next-hop (if in table) otherwise to NHS

Phase 2 (old)
NHRP Resolution Request/Reply

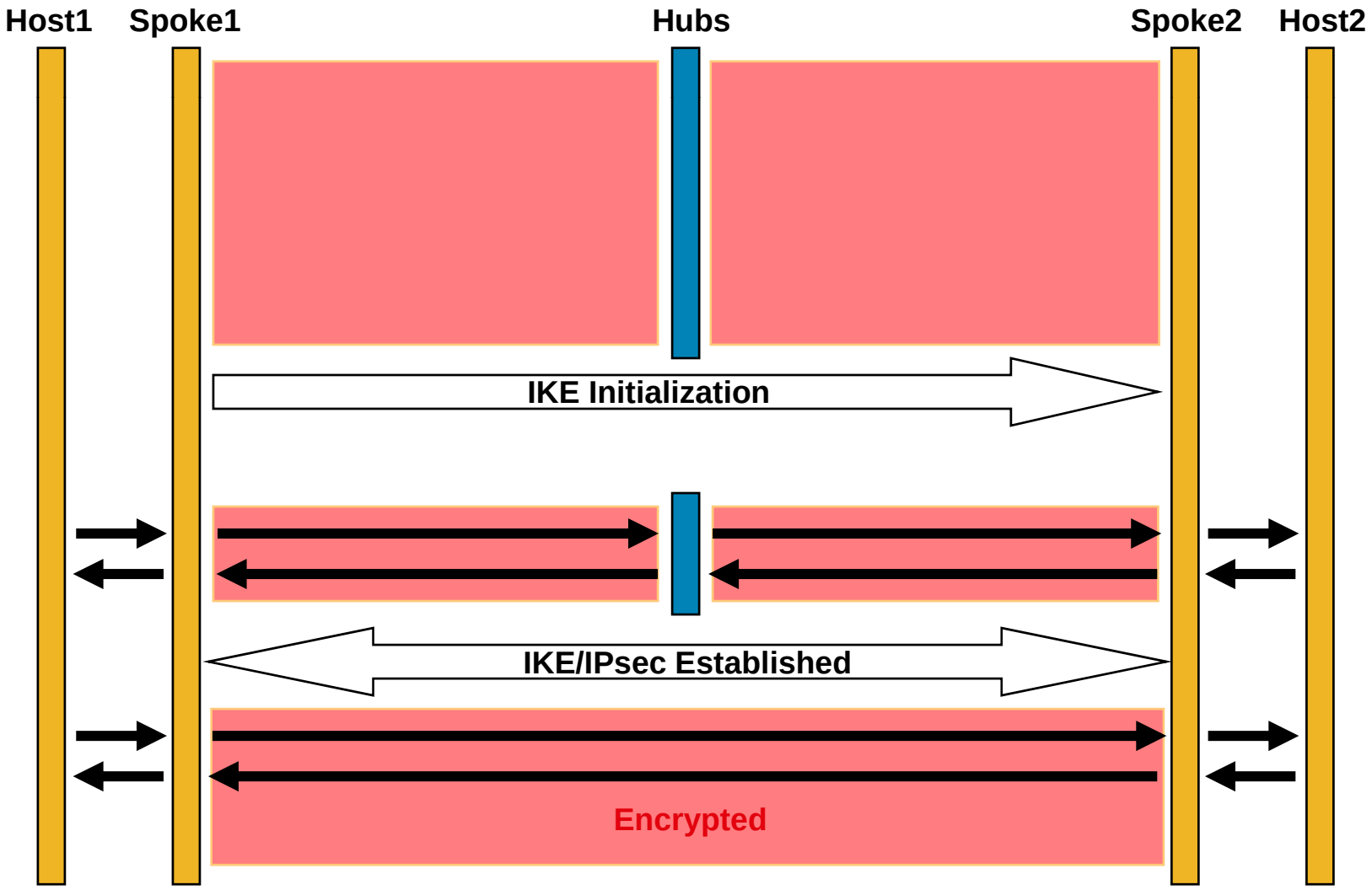
NHRP: Send Resolution Request via Tunnel1 vrf 0, packet size: 80, src: 10.0.0.11, dst: 10.0.0.1
(F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1, shtl: 4(NSAP), sstl: 0(NSAP)
(M) flags: "router auth src-stable", reqid: 10,
src NBMA: 172.16.1.1, src protocol: 10.0.0.11, dst protocol: 10.0.0.12
(C-1) code: no error(0) prefix: 0, mtu: 1514, hd_time: 360
Responder Address Extension(3):
Forward Transit NHS Record Extension(4):
Reverse Transit NHS Record Extension(5):
Authentication Extension(7): type:Cleartext(1), data:test

Request

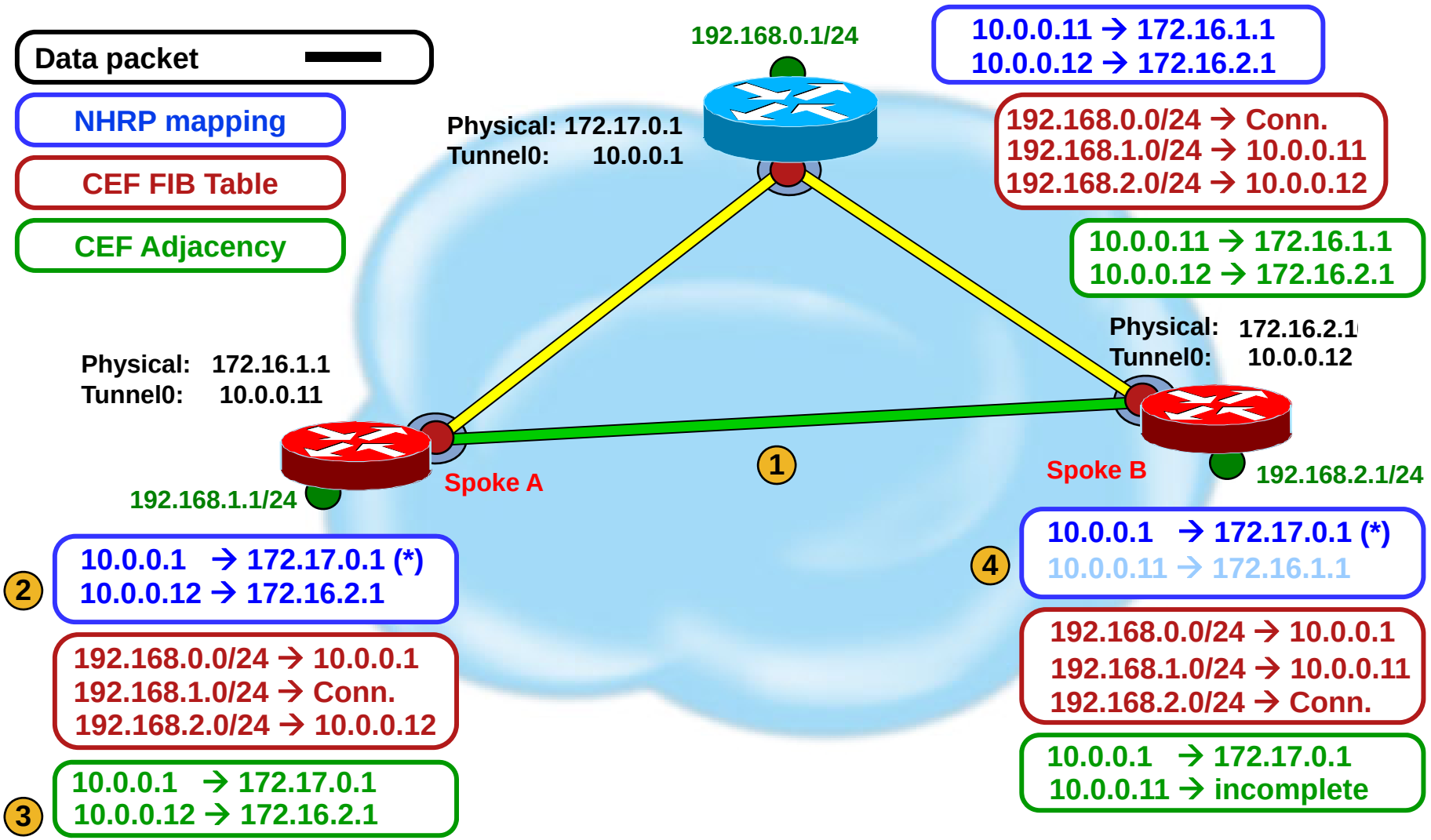
NHRP: Receive Resolution Reply via Tunnel1 vrf 0, packet size: 108
(F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1, shtl: 4(NSAP), sstl: 0(NSAP)
(M) flags: "router auth dst-stable src-stable", reqid: 10
src NBMA: 172.16.1.1, src protocol: 10.0.0.11, dst protocol: 10.0.0.12
(C-1) code: no error(0) prefix: 32, mtu: 1514, hd_time: 360
client NBMA: 172.16.2.1, client protocol: 10.0.0.12
Responder Address Extension(3):
(C) code: no error(0), prefix: 0, mtu: 1514, hd_time: 360
client NBMA: 172.17.0.1, client protocol: 10.0.0.1
Forward Transit NHS Record Extension(4):
Reverse Transit NHS Record Extension(5):
Authentication Extension(7): type:Cleartext(1), data:test

Reply

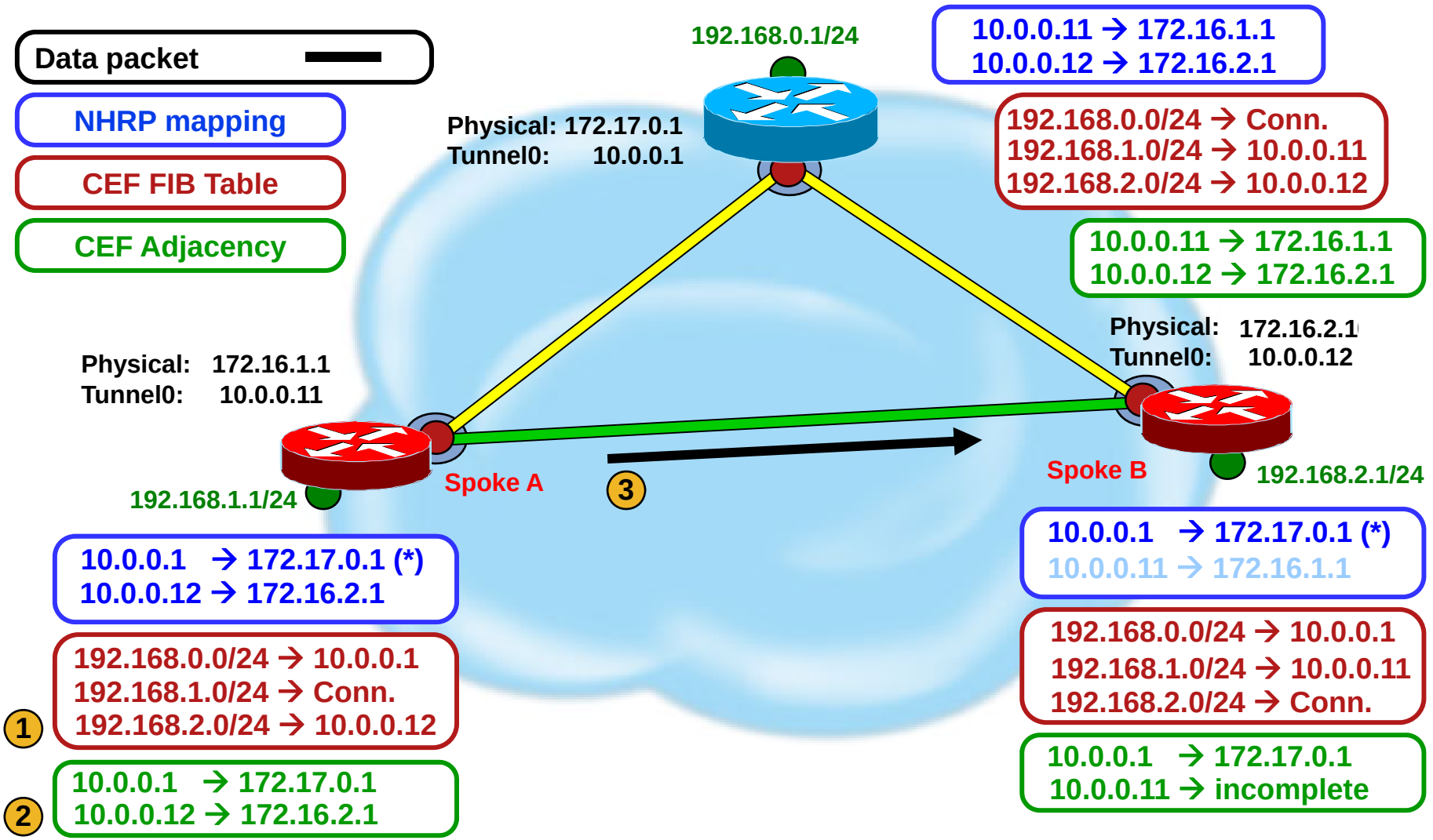
Phase 2 (old)
NHRP Resolution Shortcut Tunnel (Step 2)



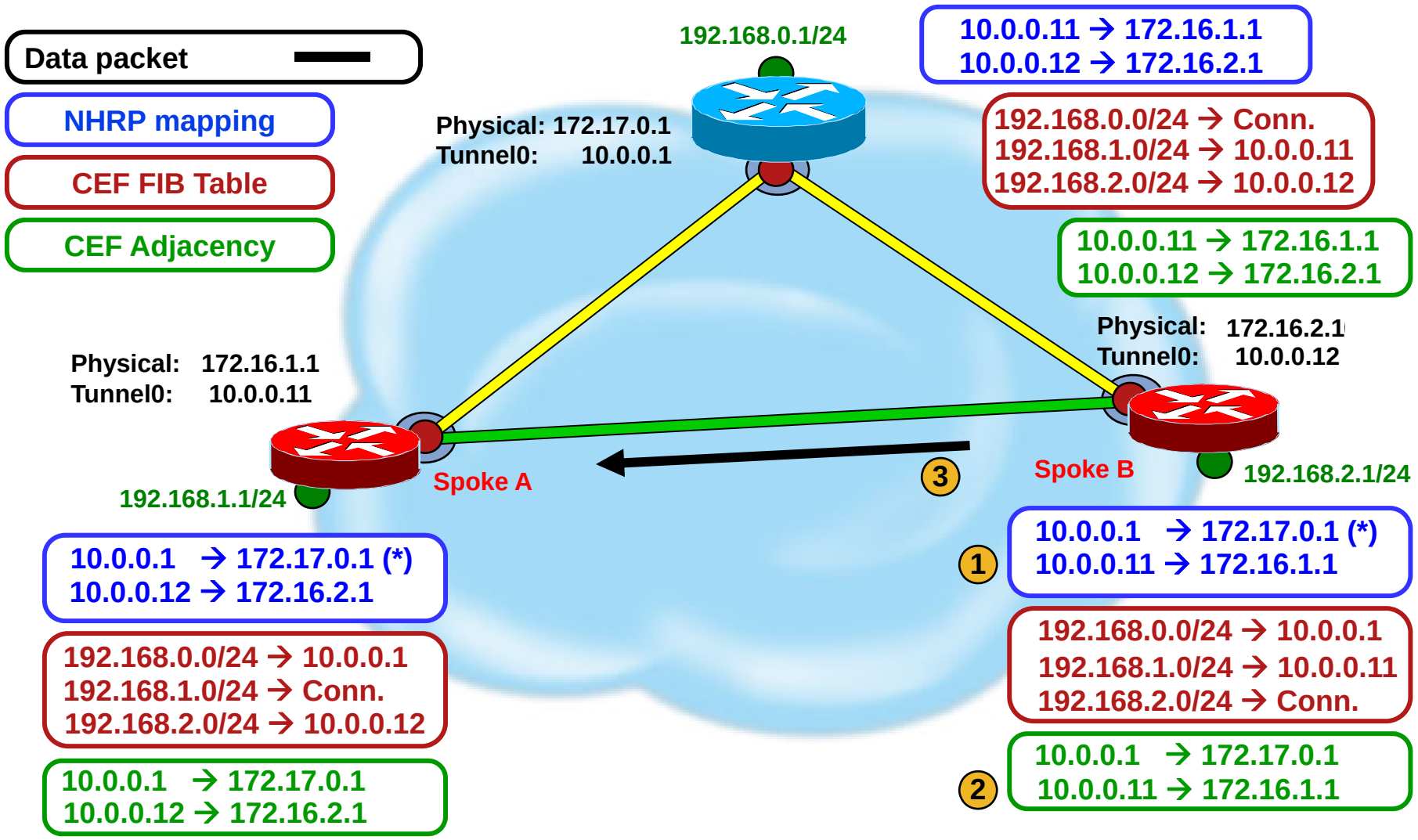
Phase 2 (old)
NHRP Resolution Shortcut Tunnel (Step 2a)



Phase 2 (old)
NHRP Resolution Shortcut Tunnel (Step 2b)



Phase 2 (old)
NHRP Resolution Shortcut Tunnel (Step 2c)



Phase 2 (old)
NHRP Mapping Tables

Hub1

```
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 01:03:38, expire 00:05:18
  Type: dynamic, Flags: authoritative unique registered used
  NBMA address: 172.16.1.1
10.0.0.12/32 via 10.0.0.12, Tunnel0 created 01:02:15, expire 00:05:23
  Type: dynamic, Flags: authoritative unique registered used
  NBMA address: 172.16.2.1
```

Spoke A

```
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:53:25, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
10.0.0.12/32 via 10.0.0.12, Tunnel0 created 00:00:06, expire 00:05:31
  Type: dynamic, Flags: router
  NBMA address: 172.16.2.1
```

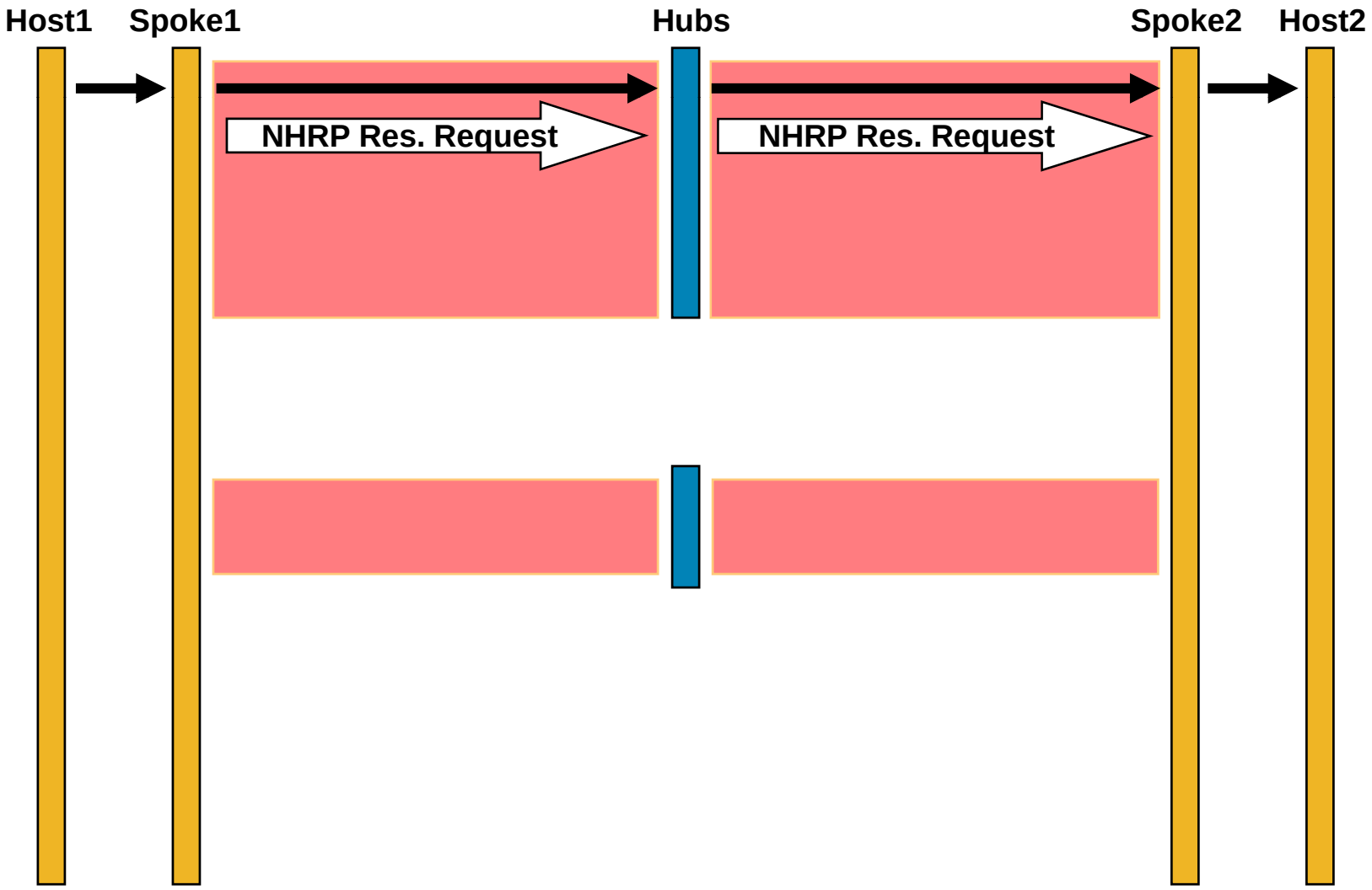
Spoke B

```
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:56:12, never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 00:00:10, expire 00:05:22
  Type: dynamic, Flags: router
  NBMA address: 172.16.1.1
```

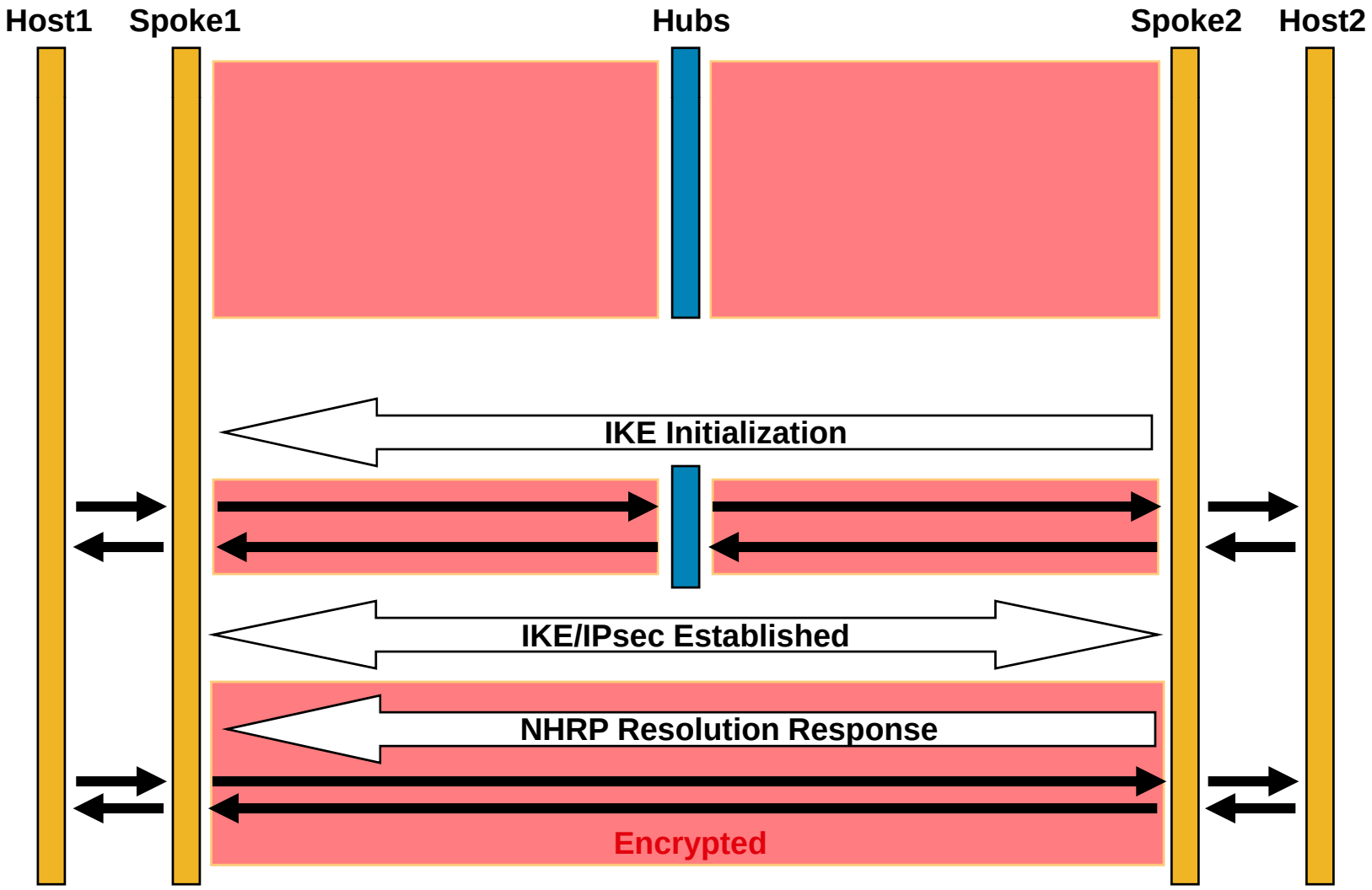
Appendix

- DMVPN Overview
- NHRP Details
  - NHRP Overview
  - NHRP Registrations
  - NHRP Resolutions/Redirects
    - Phase 2 (old)
    - Phase 2 (new)
    - Phase 3
- Network Virtualization
  - VRF-lite
  - 2547oDMVPN

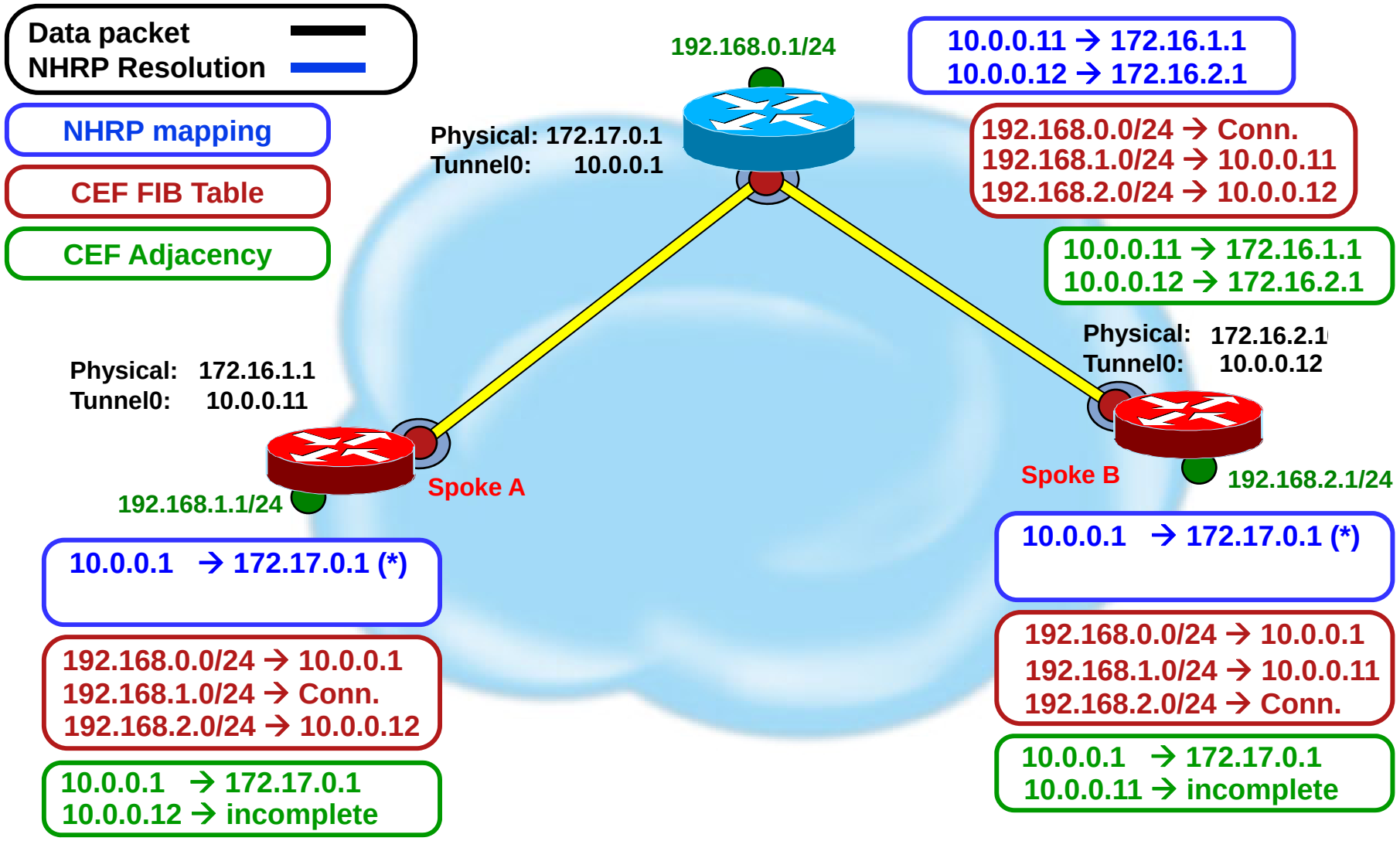
Phase 2 (new)
NHRP Resolution Request (Step 1)



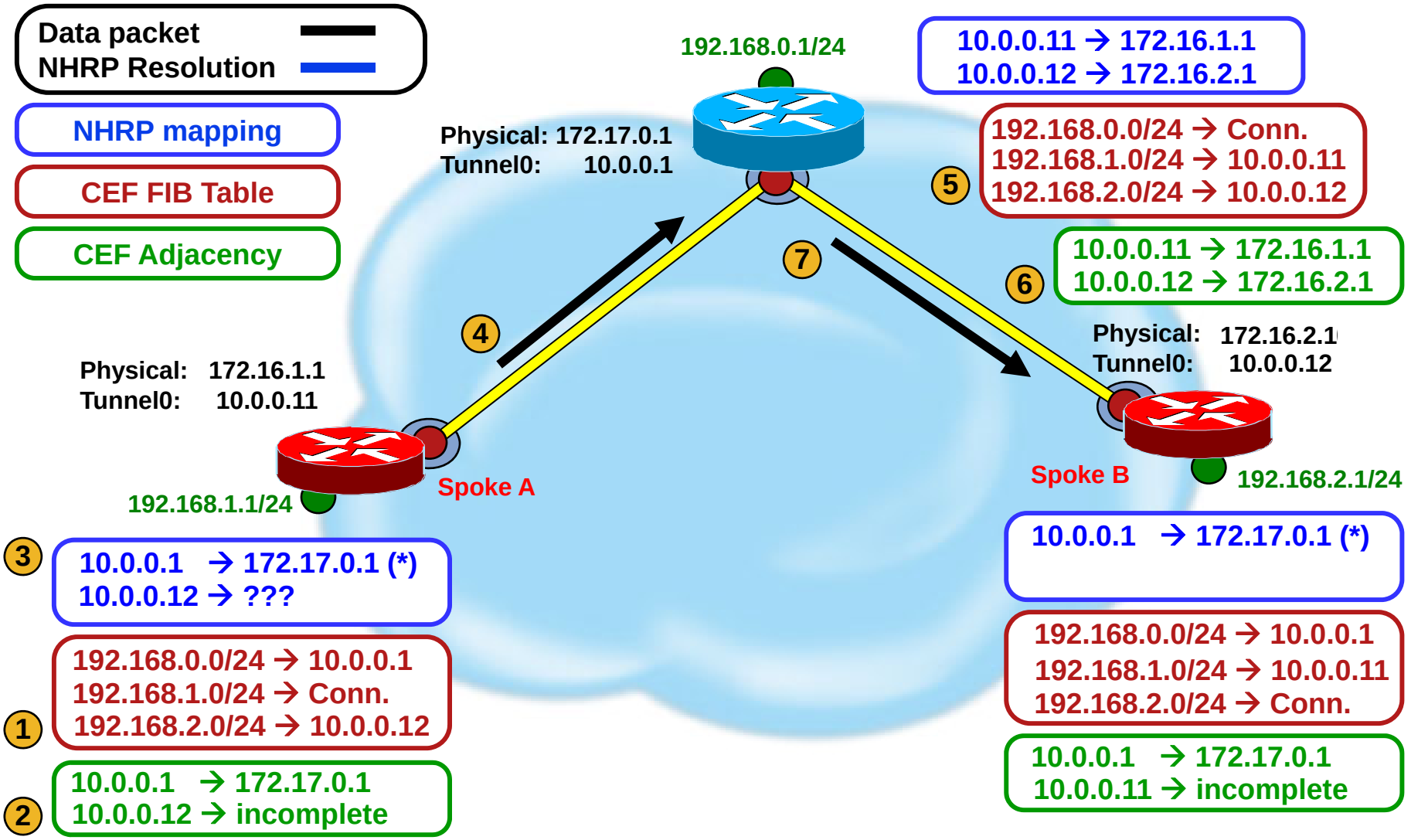
Phase 2 (new)
NHRP Resolution Reply (Step 2)



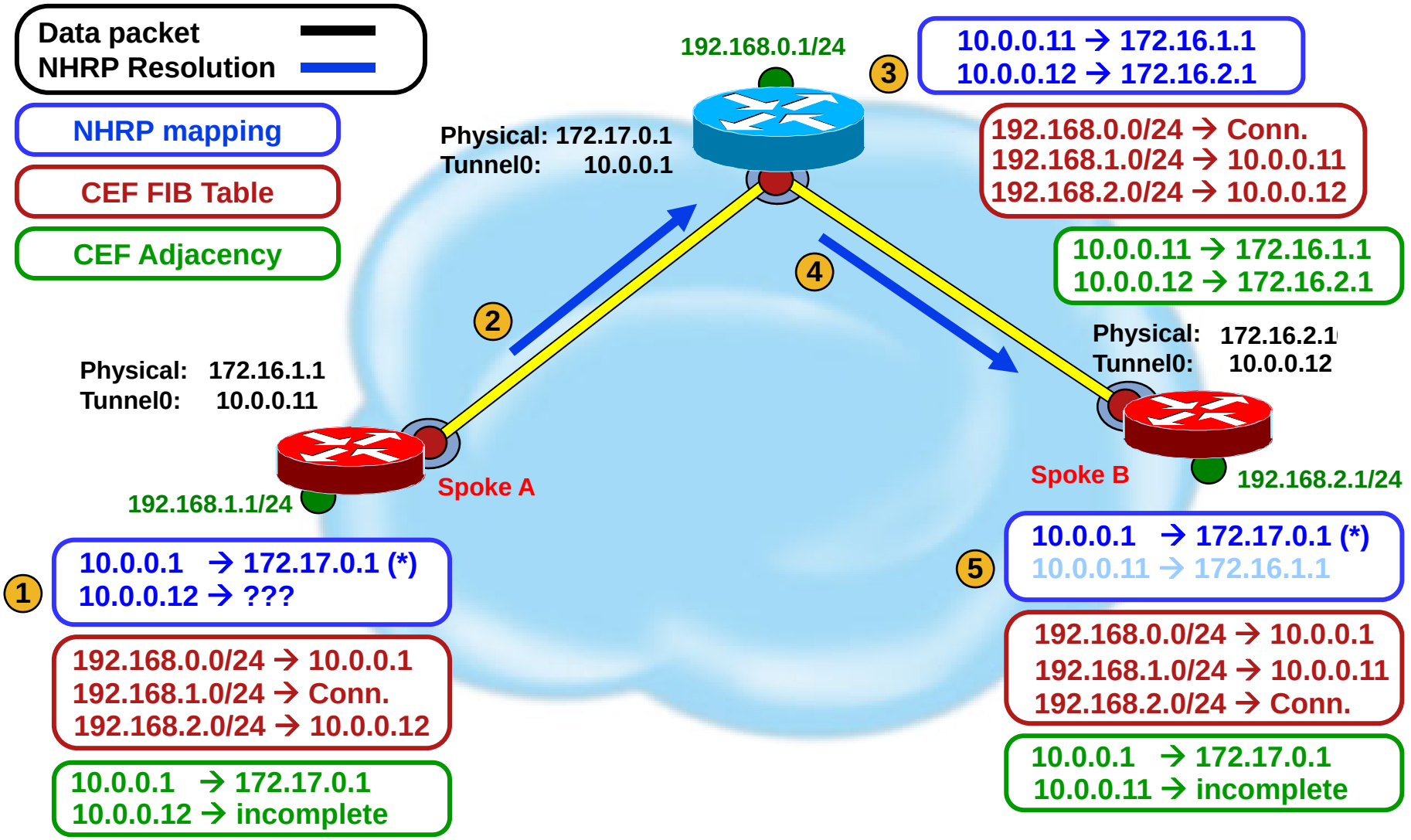
Phase 2 (new)
NHRP Resolution Request



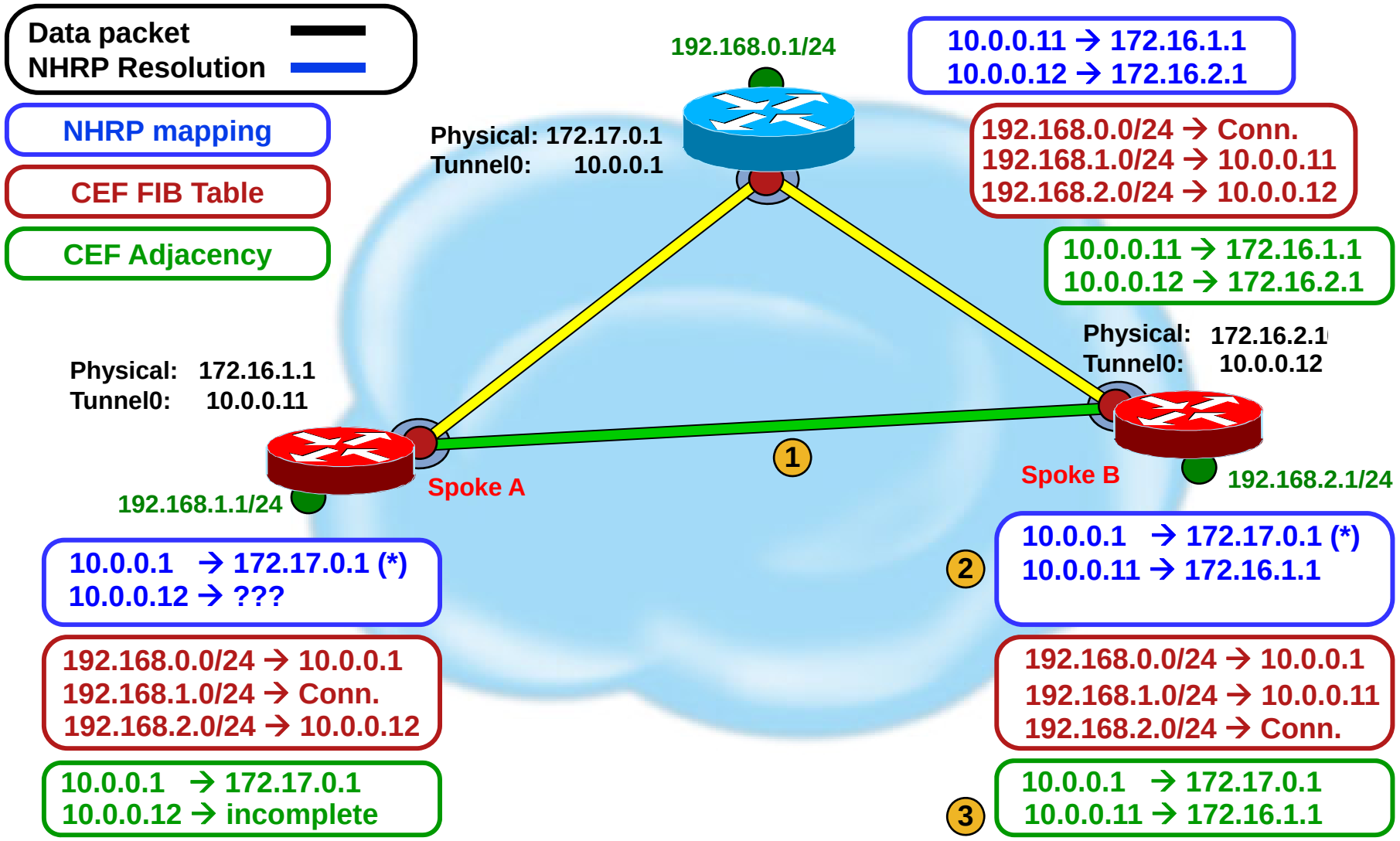
Phase 2 (new)
NHRP Resolution Request (Step 1a)



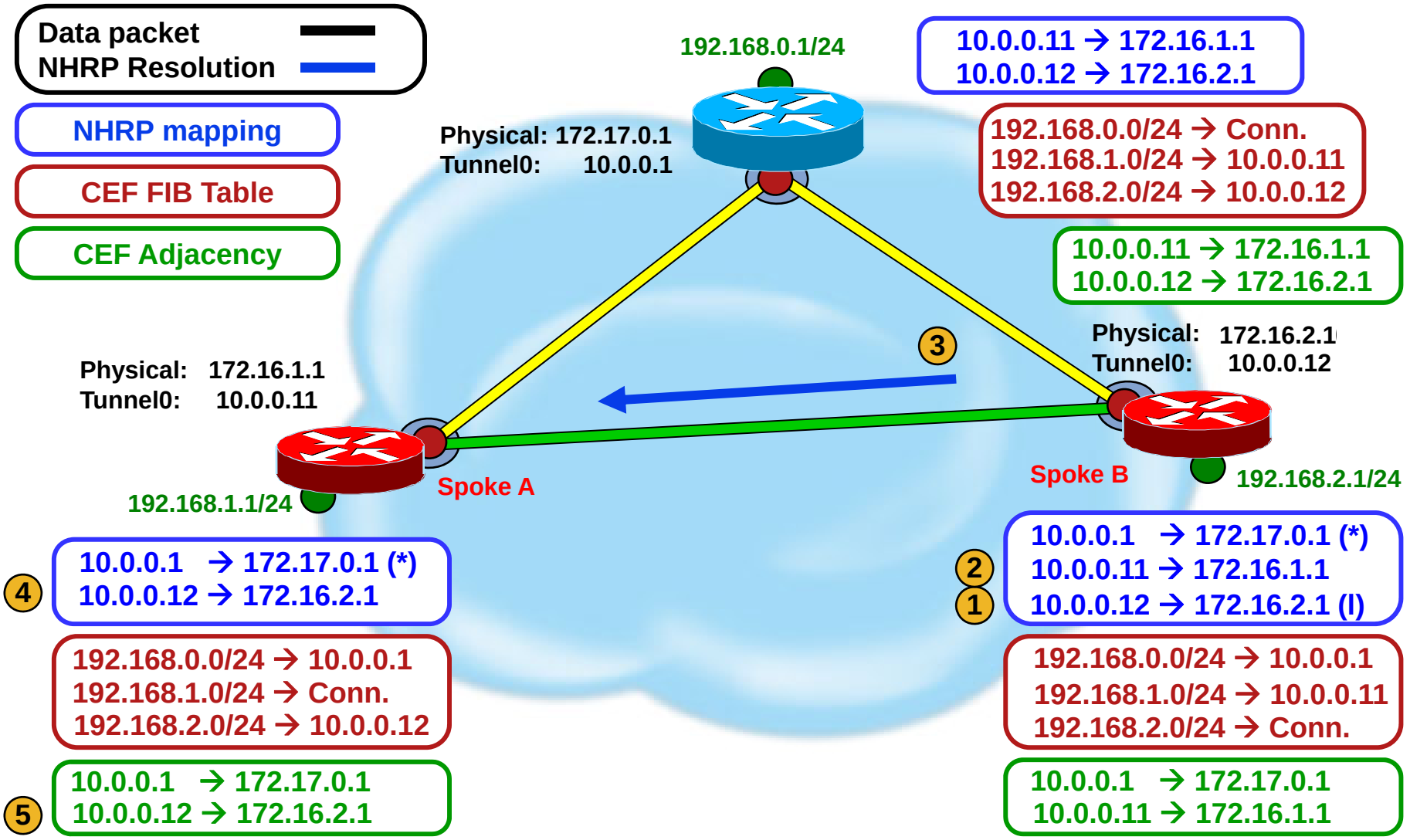
Phase 2 (new)
NHRP Resolution Request (Step 1b)



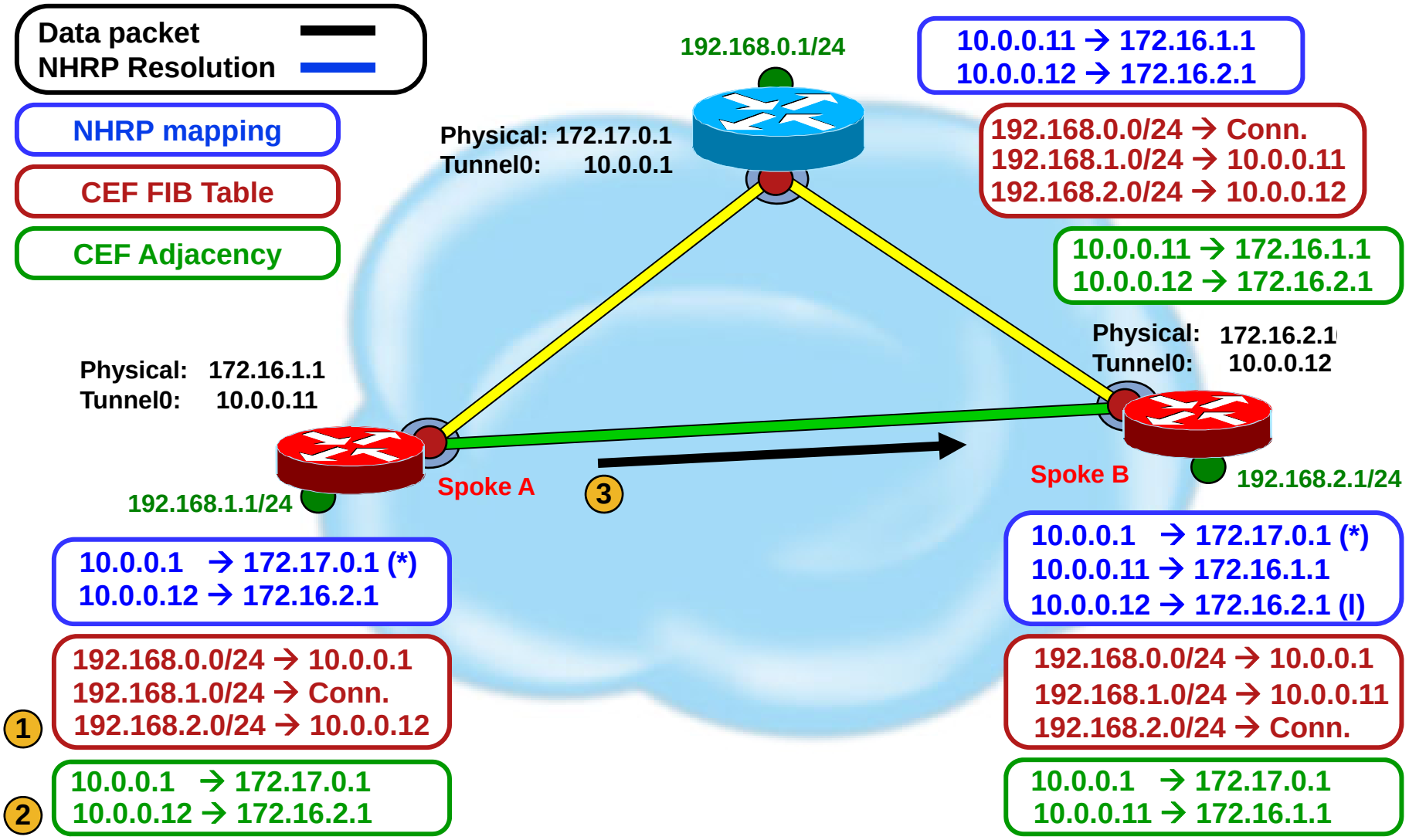
Phase 2 (new)
NHRP Resolution Reply (Step 2a)



Phase 2 (new)
NHRP Resolution Reply (Step 2b)



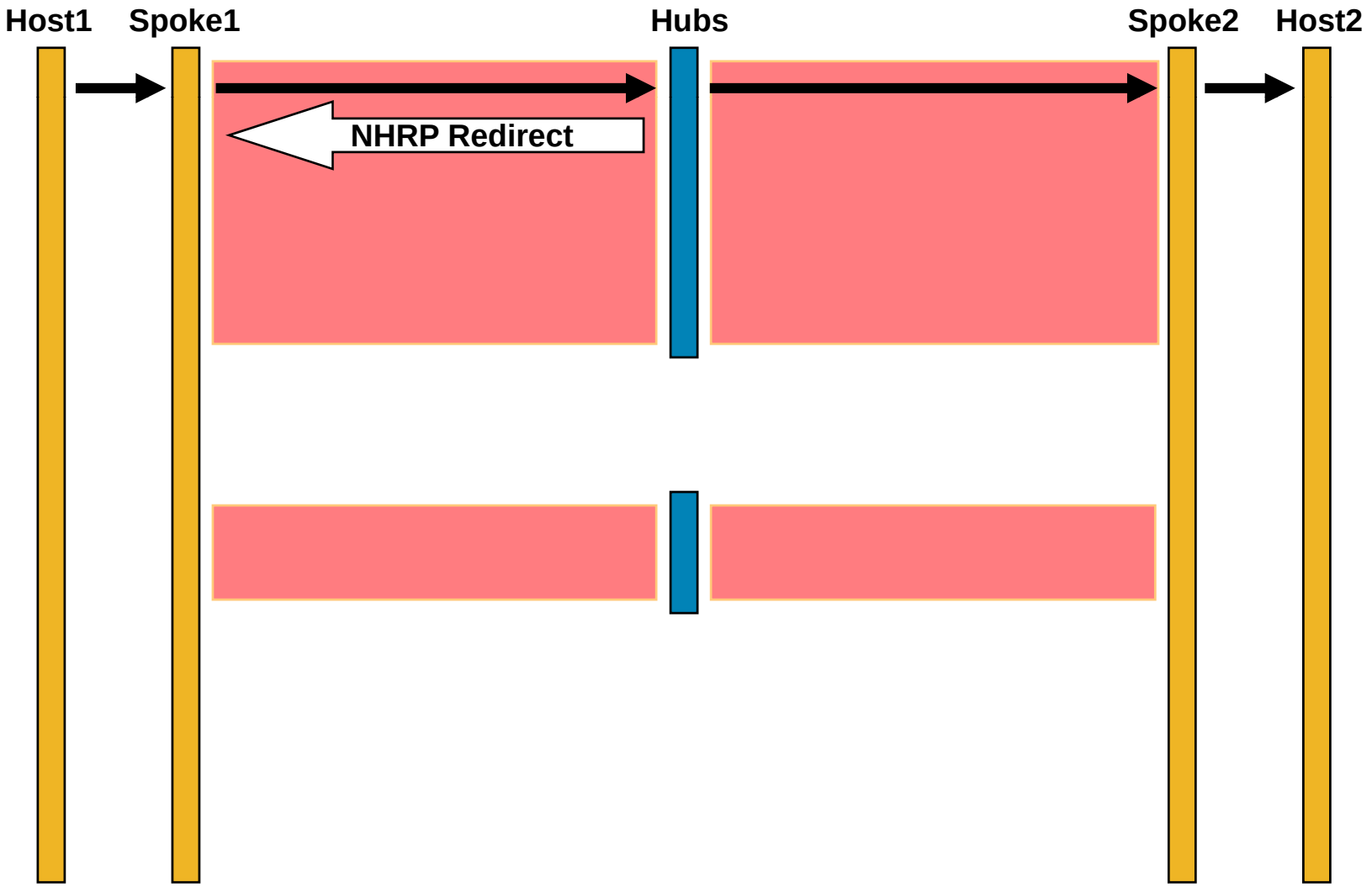
Phase 2 (new)
NHRP Resolution Reply (Step 2c)



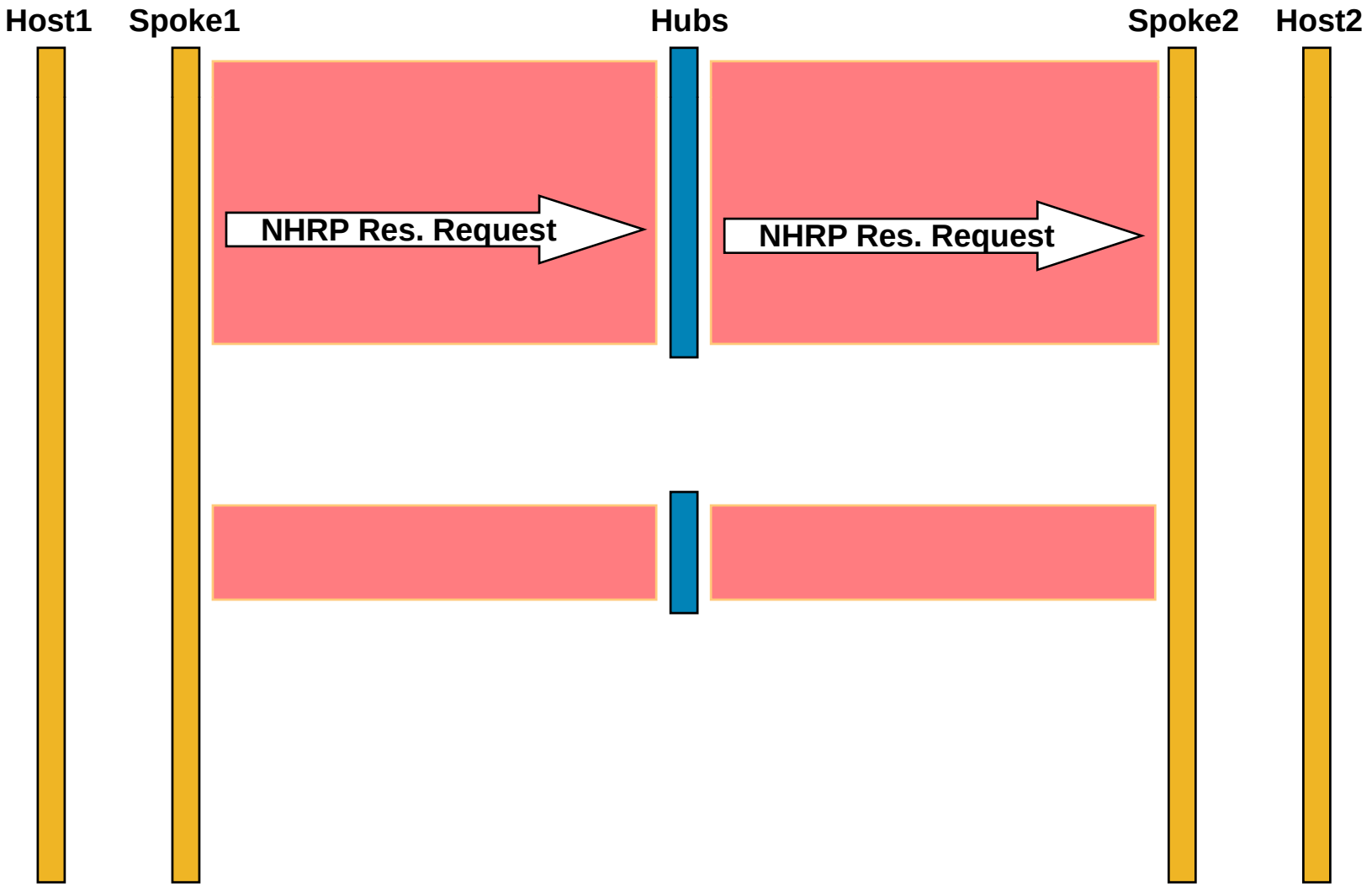
Appendix

- DMVPN Overview
- NHRP Details
  - NHRP Overview
  - NHRP Registrations
  - NHRP Resolutions/Redirects
    - Phase 2 (old)
    - Phase 2 (new)
    - Phase 3
- Network Virtualization
  - VRF-lite
  - 2547oDMVPN

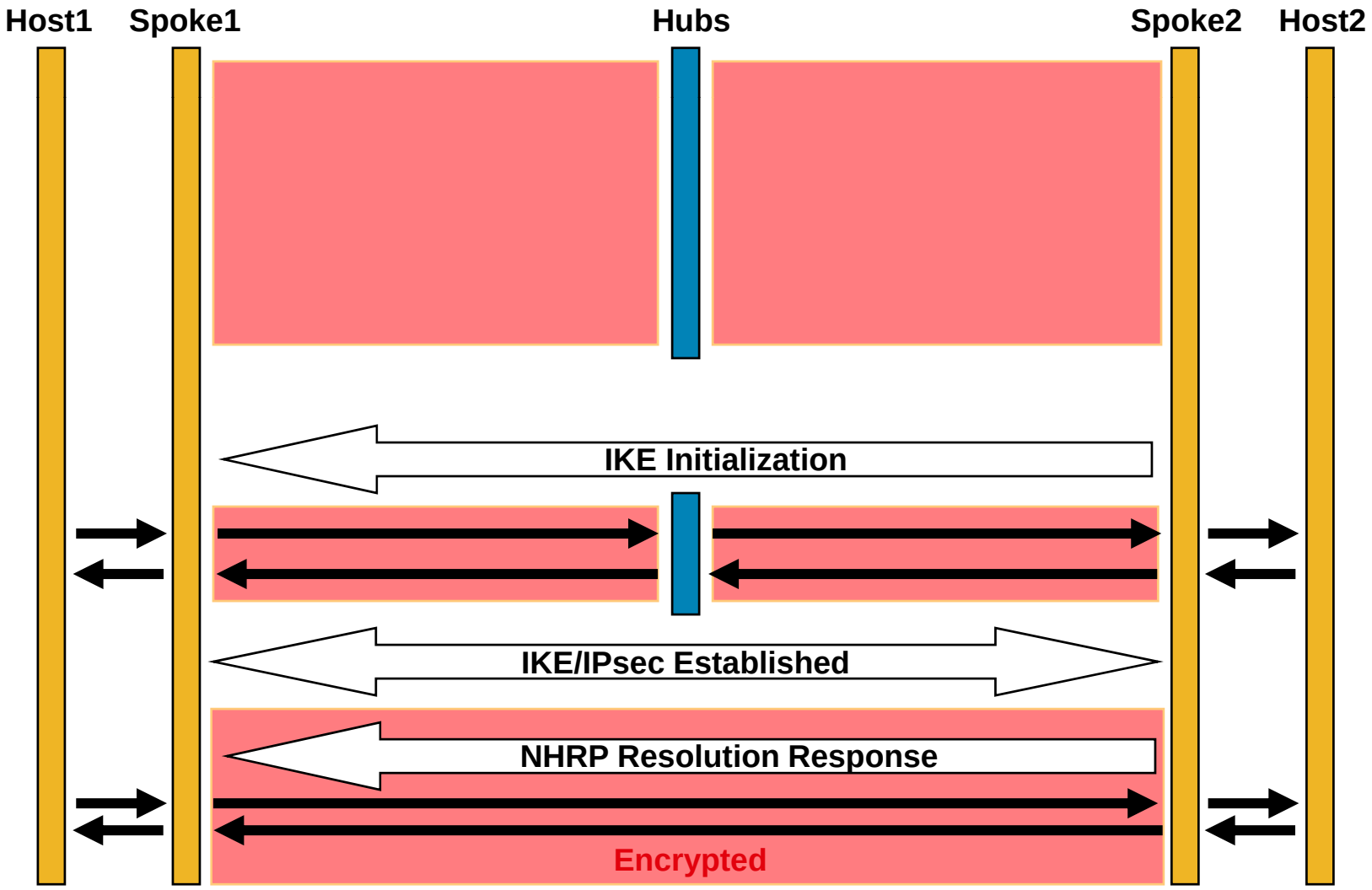
Phase 3
NHRP Redirect (Step 1)



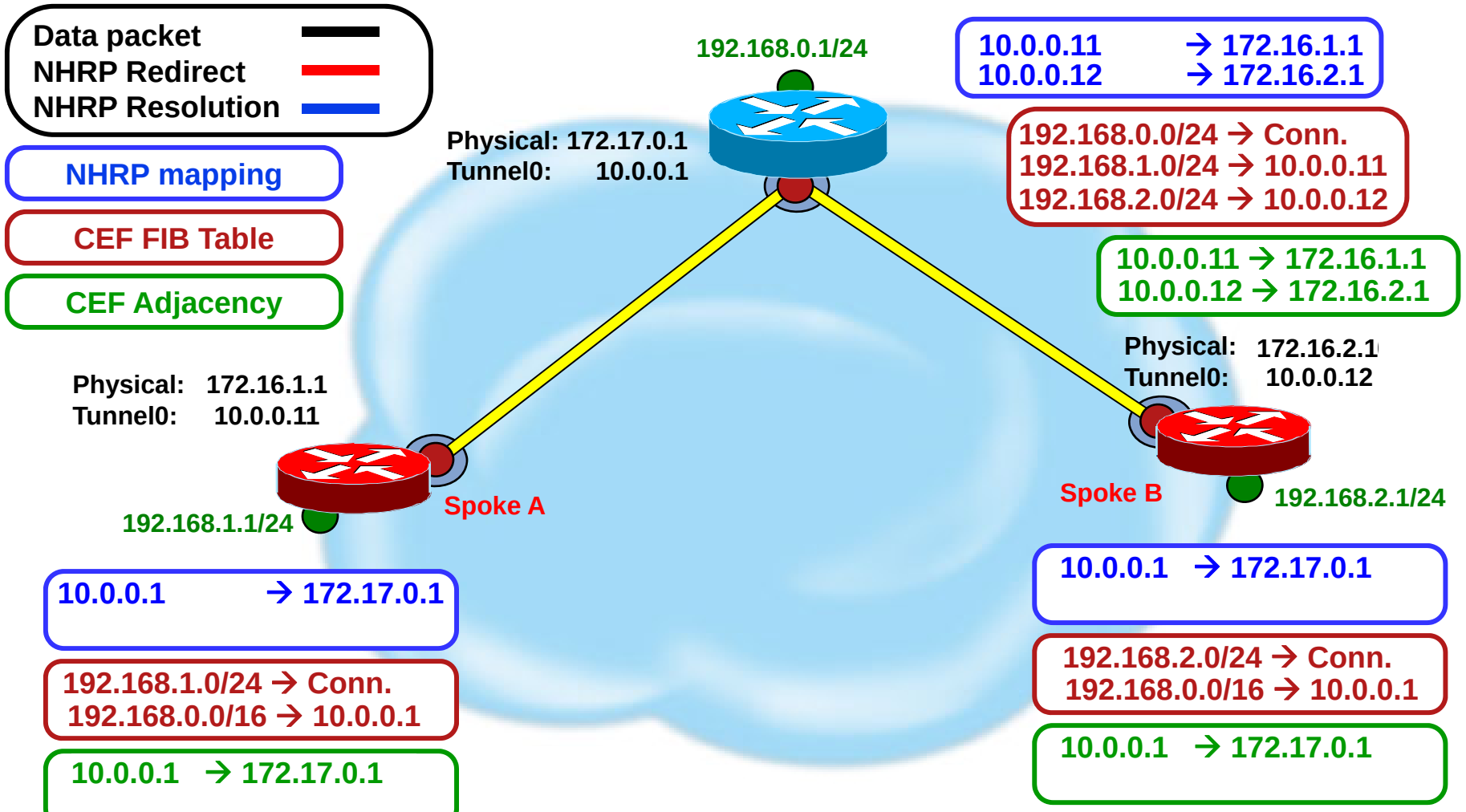
Phase 3
NHRP Resolution Request (Step 2)



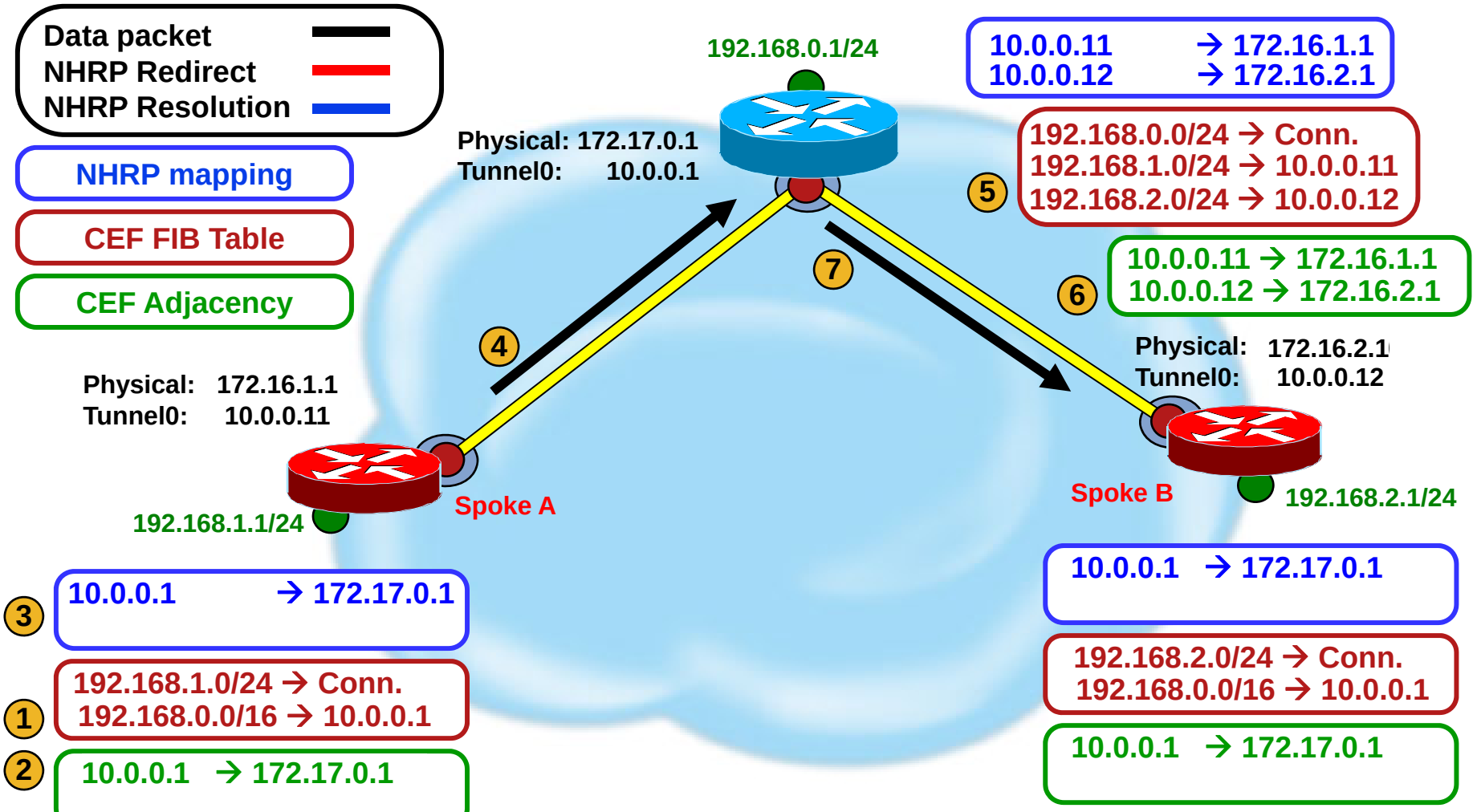
Phase 3
NHRP Resolution Reply (Step 3)



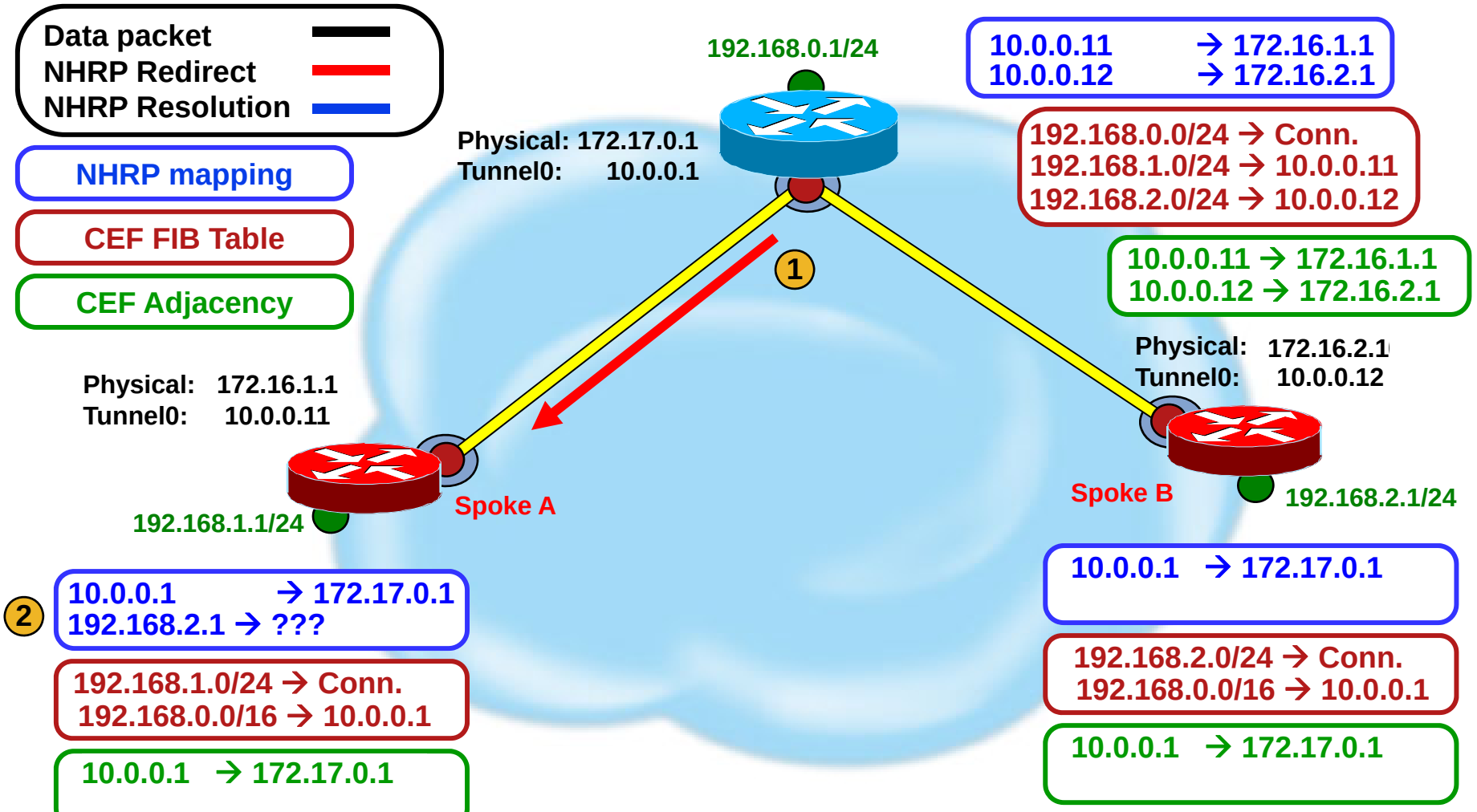
Phase 3
NHRP Resolution Redirect



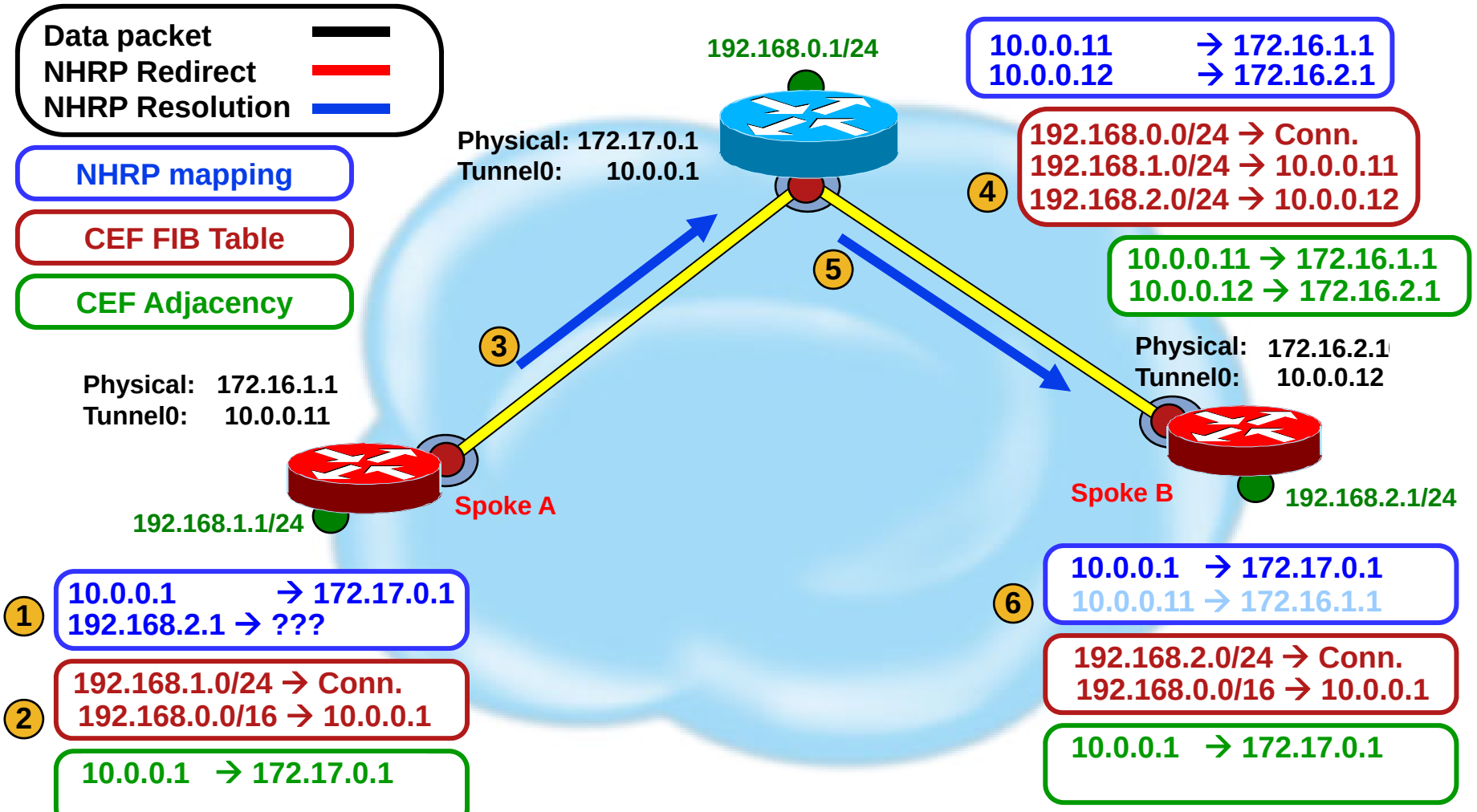
Phase 3
NHRP Resolution Redirect (Step 1a)



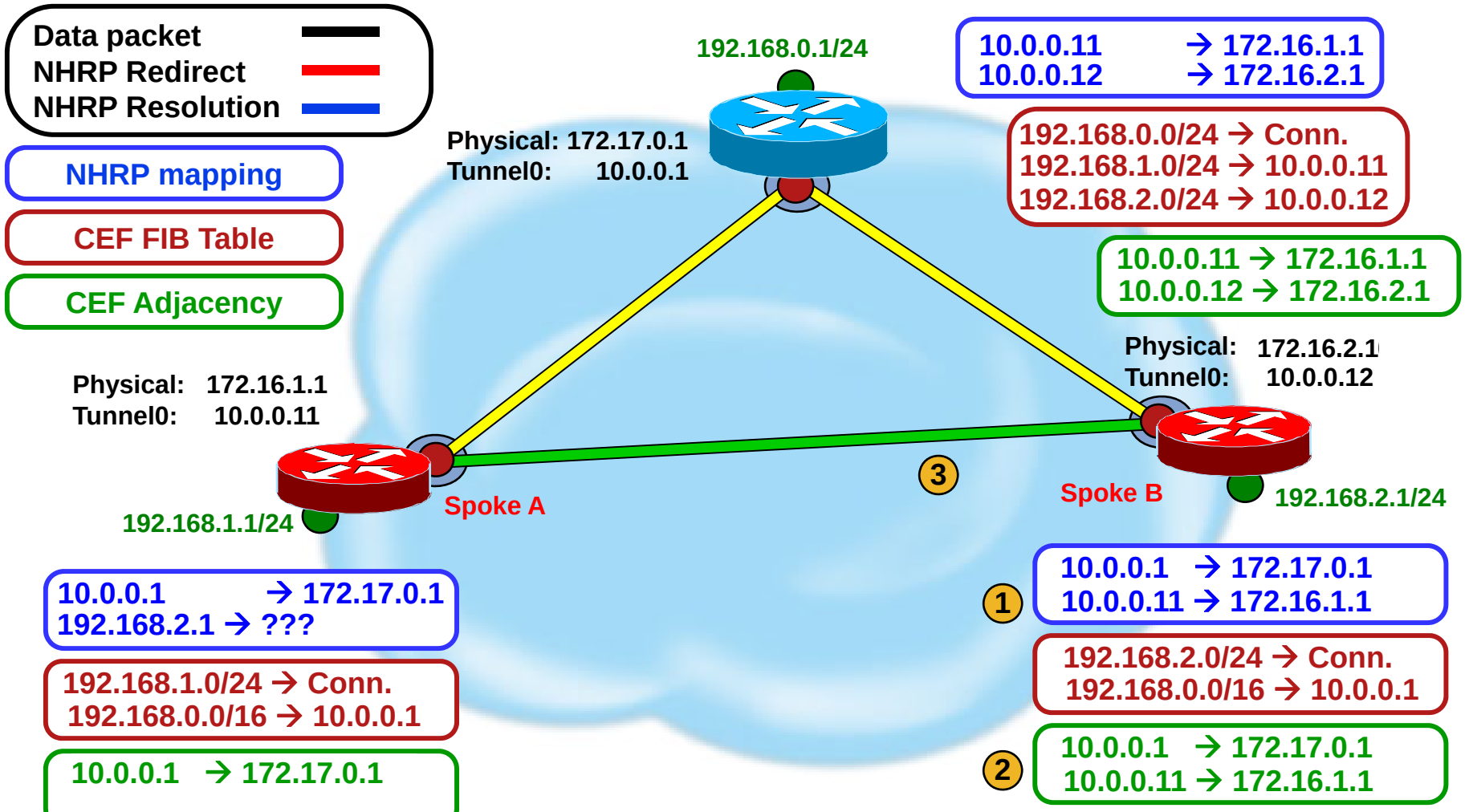
Phase 3
NHRP Resolution Redirect (Step 1b)



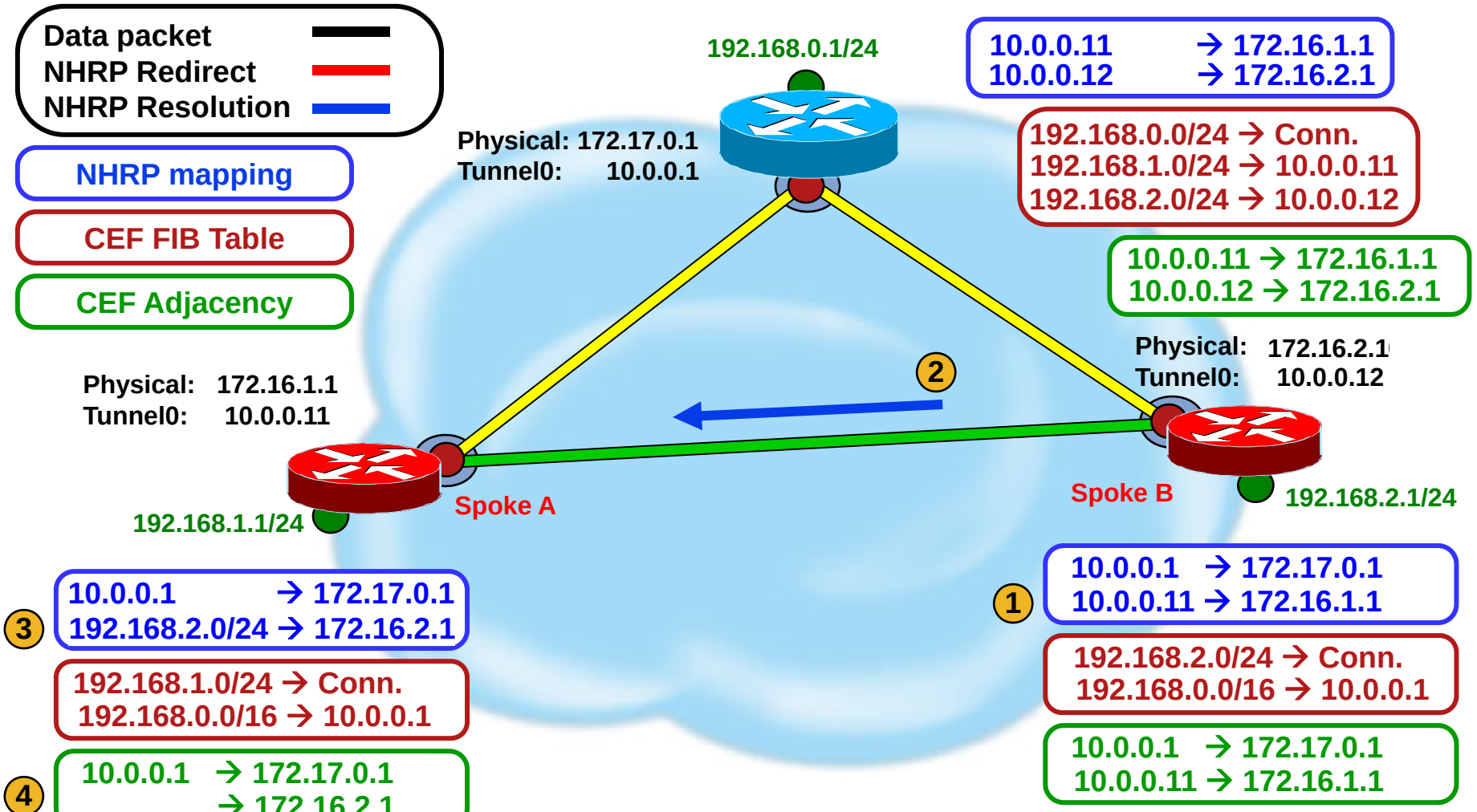
Phase 3
NHRP Resolution Request (Step 2)



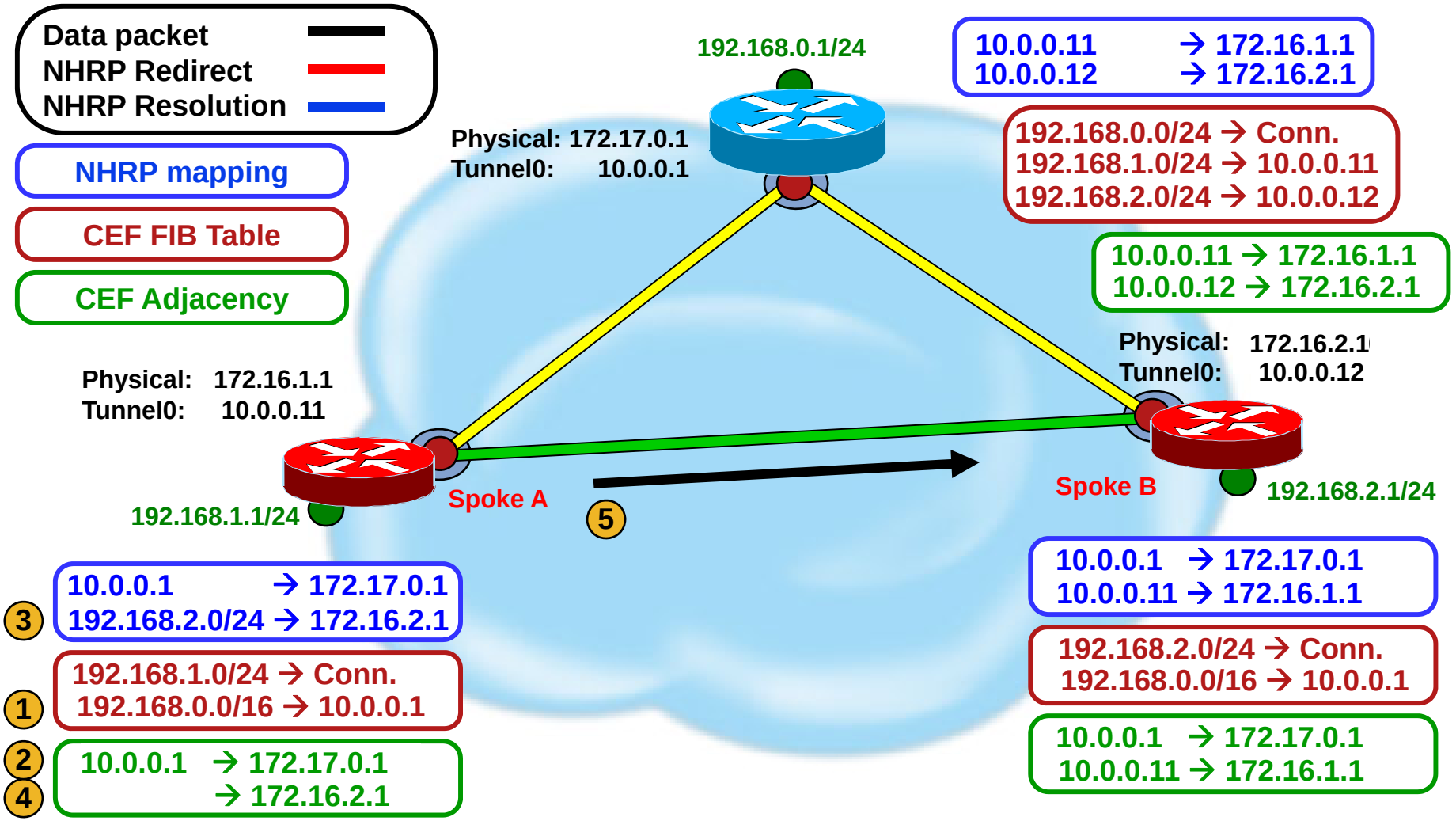
Phase 3
NHRP Resolution Reply (Step 3a)



Phase 3
NHRP Resolution Reply (Step 3b)



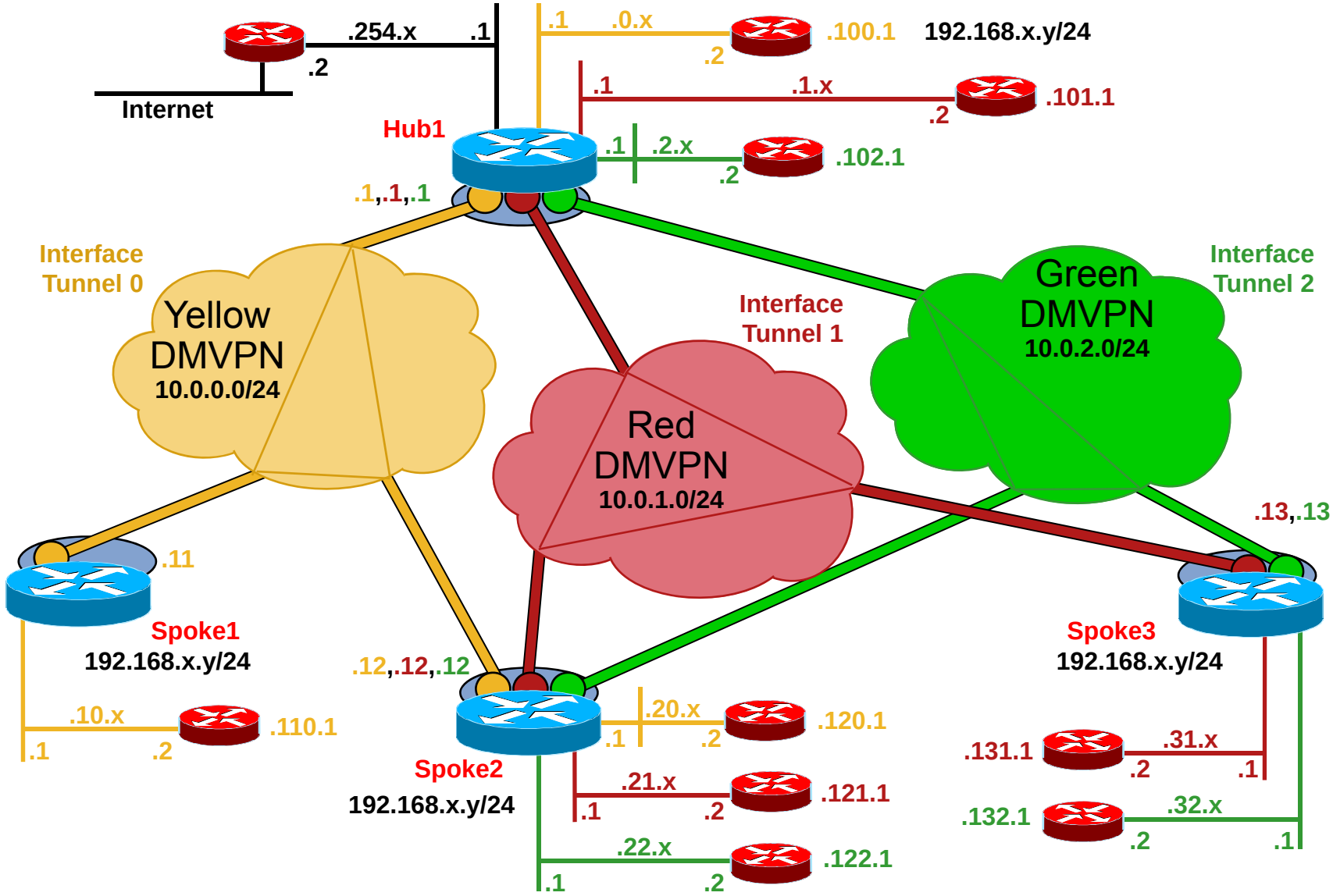
Phase 3
NHRP Resolution Reply (Step 3c)



Appendix

- DMVPN Overview
- NHRP Details
  - NHRP Overview
  - NHRP Registrations
  - NHRP Resolutions/Redirects
    - Phase 2 (old)
    - Phase 2 (new)
    - Phase 3
- Network Virtualization
  - VRF-lite
  - 2547oDMVPN

Separate DMVPNs VRF-lite
Logical Topology



Separate DMVPNs – VRF-lite
Hub Configuration

```
version 12.4
!
hostname Hub1
!
ip cef
!
ip vrf Green
   rd 3:3
   route-target export 3:3
   route-target import 3:3
   route-target import 10:10
!
ip vrf Internet
   rd 10:10
   route-target export 10:10
   route-target import 10:10
   route-target import 1:1
   route-target import 2:2
   route-target import 3:3
!
ip vrf Red
   rd 2:2
   route-target export 2:2
   route-target import 2:2
   route-target import 10:10
!
ip vrf Yellow
   rd 1:1
   route-target export 1:1
   route-target import 1:1
   route-target import 10:10
```

```
crypto isakmp policy 2
   authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set t2 esp-des esp-md5-hmac
   mode transport
!
crypto ipsec profile vpnprof
   set transform-set t2
!
interface Tunnel0
   bandwidth 1000
   ip vrf forwarding Yellow
   ip address 10.0.0.1 255.255.255.0
   ip mtu 1400
   no ip next-hop-self eigrp 1
   ip nhrp authentication Yellow
   ip nhrp map multicast dynamic
   ip nhrp network-id 100000
   ip nhrp holdtime 360
   ip tcp adjust-mss 1360
   no ip split-horizon eigrp 1
   tunnel source Serial4/0
   tunnel mode gre multipoint
   tunnel key 100000
   tunnel protection ipsec profile vpnprof shared
!
```

Separate DMVPNs – VRF-lite
Hub Configuration (cont)

```
interface Tunnel1
   bandwidth 1000
   ip vrf forwarding Red
   ip address 10.0.1.1 255.255.255.0
   ip mtu 1400
   no ip next-hop-self eigrp 1
   ip nhrp authentication Red
   ip nhrp map multicast dynamic
   ip nhrp network-id 100001
   ip nhrp holdtime 360
   ip tcp adjust-mss 1360
   no ip split-horizon eigrp 1
   tunnel source Serial4/0
   tunnel mode gre multipoint
   tunnel key 100001
   tunnel protection ipsec profile vpnprof shared
!
interface Tunnel2
   bandwidth 1000
   ip vrf forwarding Green
   ip address 10.0.2.1 255.255.255.0
   ip mtu 1400
   no ip next-hop-self eigrp 1
   ip nhrp authentication Green
   ip nhrp map multicast dynamic
   ip nhrp network-id 100002
   ip nhrp holdtime 360
   ip tcp adjust-mss 1360
   no ip split-horizon eigrp 1
   tunnel source Serial4/0
   tunnel mode gre multipoint
   tunnel key 100002
   tunnel protection ipsec profile vpnprof shared
```

```
interface Ethernet0/0
   ip vrf forwarding Yellow
   ip address 192.168.0.1 255.255.255.0
!
interface Ethernet1/0
   ip vrf forwarding Red
   ip address 192.168.1.1 255.255.255.0
!
interface Ethernet2/0
   ip vrf forwarding Green
   ip address 192.168.2.1 255.255.255.0
!
interface Ethernet3/0
   ip vrf forwarding Internet
   ip address 192.168.254.1 255.255.255.0
!
interface Serial4/0
   ip address 172.17.0.1 255.255.255.252
!
router eigrp 1
   no auto-summary
   !
      address-family ipv4 vrf Yellow
      redistribute bgp 1
      network 10.0.0.0 0.0.0.255
      network 192.168.0.0
      default-metric 1000 100 255 1 1500
      no auto-summary
      autonomous-system 1
   exit-address-family
   !
```

Separate DMVPNs – VRF-lite
Hub Configuration (cont)

```
router eigrp 1
   no auto-summary
   !
      address-family ipv4 vrf Red
      redistribute bgp 1
      network 10.0.1.0 0.0.0.255
      network 192.168.1.0
      default-metric 1000 100 255 1 1500
      no auto-summary
      autonomous-system 1
   exit-address-family
   !
   address-family ipv4 vrf Internet
      redistribute bgp 1
      network 192.168.254.0
      default-metric 1000 100 255 1 1500
      no auto-summary
      autonomous-system 1
   exit-address-family
   !
   address-family ipv4 vrf Green
      redistribute bgp 1
      network 10.0.2.0 0.0.0.255
      network 192.168.2.0
      default-metric 1000 100 255 1 1500
      no auto-summary
      autonomous-system 1
   exit-address-family
!
```

```
router bgp 1
   no synchronization
   bgp log-neighbor-changes
   no auto-summary
   !
   address-family ipv4 vrf Yellow
      redistribute connected
      redistribute eigrp 1
      no synchronization
   exit-address-family
   !
   address-family ipv4 vrf Red
      redistribute connected
      redistribute eigrp 1
      no synchronization
   exit-address-family
   !
   address-family ipv4 vrf Internet
      redistribute connected
      redistribute eigrp 1
      default-information originate
      no synchronization
   exit-address-family
   !
   address-family ipv4 vrf Green
      redistribute connected
      redistribute eigrp 1
      no synchronization
   exit-address-family
!
ip route 0.0.0.0 0.0.0.0 172.17.0.2
```

Separate DMVPNs – VRF-lite
Spoke1 Configuration

```
version 12.4
!
hostname Spoke1
!
ip cef
!
ip vrf Yellow
   rd 1:1
   route-target export 1:1
   route-target import 1:1
!
crypto isakmp policy 2
   authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set t2 esp-des esp-md5-hmac
   mode transport
!
crypto ipsec profile vpnprof
   set transform-set t2
!
router eigrp 1
   no auto-summary
   !
   address-family ipv4 vrf Yellow
      network 10.0.0.0 0.0.0.255
      network 192.168.10.0
      no auto-summary
      autonomous-system 1
   exit-address-family
!
ip route 0.0.0.0 0.0.0.0 172.16.1.2
```

```
interface Tunnel0
   bandwidth 1000
   ip vrf forwarding Yellow
   ip address 10.0.0.11 255.255.255.0
   no ip redirects
   ip mtu 1400
   ip nhrp authentication Yellow
   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
   ip tcp adjust-mss 1360
   delay 1000
   tunnel source Serial2/0
   tunnel mode gre multipoint
   tunnel key 100000
   tunnel protection ipsec profile vpnprof
!
interface Ethernet0/0
   ip vrf forwarding Yellow
   ip address 192.168.10.1 255.255.255.0
!
interface Serial2/0
   ip address 172.16.1.1 255.255.255.252
!
```

Separate DMVPNs – VRF-lite
Spoke2 Configuration

```
version 12.4
!
hostname Spoke2
!
ip cef
!
ip vrf Green
   rd 3:3
   route-target export 3:3
   route-target import 3:3
!
ip vrf Red
   rd 2:2
   route-target export 2:2
   route-target import 2:2
!
ip vrf Yellow
   rd 1:1
   route-target export 1:1
   route-target import 1:1
!
crypto isakmp policy 2
   authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set t2 esp-des esp-md5-hmac
   mode transport
!
crypto ipsec profile vpnprof
   set transform-set t2
!
```

```
interface Tunnel0
   bandwidth 1000
   ip vrf forwarding Yellow
   ip address 10.0.0.12 255.255.255.0
   ip mtu 1400
   ip nhrp authentication Yellow
   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
   ip tcp adjust-mss 1360
   delay 1000
   tunnel source Serial4/0
   tunnel mode gre multipoint
   tunnel key 100000
   tunnel protection ipsec profile vpnprof shared
!
interface Tunnel1
   bandwidth 1000
   ip vrf forwarding Red
   ip address 10.0.1.12 255.255.255.0
   ip mtu 1400
   ip nhrp authentication Red
   ip nhrp map 10.0.1.1 172.17.0.1
   ip nhrp map multicast 172.17.0.1
   ip nhrp network-id 100001
   ip nhrp holdtime 360
   ip nhrp nhs 10.0.1.1
   ip tcp adjust-mss 1360
   delay 1000
   tunnel source Serial4/0
   tunnel mode gre multipoint
   tunnel key 100001
   tunnel protection ipsec profile vpnprof shared
```

Separate DMVPNs – VRF-lite
Spoke2 Configuration (cont)

```
interface Tunnel2
   bandwidth 1000
   ip vrf forwarding Green
   ip address 10.0.2.12 255.255.255.0
   ip mtu 1400
   ip nhrp authentication Green
   ip nhrp map 10.0.2.1 172.17.0.1
   ip nhrp map multicast 172.17.0.1
   ip nhrp network-id 100002
   ip nhrp holdtime 360
   ip nhrp nhs 10.0.2.1
   ip tcp adjust-mss 1360
   delay 1000
   tunnel source Serial4/0
   tunnel mode gre multipoint
   tunnel key 100002
   tunnel protection ipsec profile vpnprof shared
!
interface Ethernet0/0
   ip vrf forwarding Yellow
   ip address 192.168.20.1 255.255.255.0
!
interface Ethernet1/0
   ip vrf forwarding Red
   ip address 192.168.21.1 255.255.255.0
!
interface Ethernet2/0
   ip vrf forwarding Green
   ip address 192.168.22.1 255.255.255.0
!
interface Serial4/0
   ip address 172.16.2.1 255.255.255.252
```

```
router eigrp 1
   no auto-summary
   !
   address-family ipv4 vrf Yellow
      network 10.0.0.0 0.0.0.255
      network 192.168.20.0
      no auto-summary
      autonomous-system 1
   exit-address-family
   !
   address-family ipv4 vrf Red
      network 10.0.1.0 0.0.0.255
      network 192.168.21.0
      no auto-summary
      autonomous-system 1
   exit-address-family
   !
   address-family ipv4 vrf Green
      network 10.0.2.0 0.0.0.255
      network 192.168.22.0
      no auto-summary
      autonomous-system 1
   exit-address-family
!
ip route 0.0.0.0 0.0.0.0 172.16.2.2
```

Separate DMVPNs – VRF-lite
Spoke3 Configuration

```
version 12.4
!
hostname Spoke3
!
ip cef
!
ip vrf Green
   rd 3:3
   route-target export 3:3
   route-target import 3:3
!
ip vrf Red
   rd 2:2
   route-target export 2:2
   route-target import 2:2
!
crypto isakmp policy 2
   authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set t2 esp-des esp-md5-hmac
   mode transport
!
crypto ipsec profile vpnprof
   set transform-set t2
!
```

```
interface Tunnel1
   bandwidth 1000
   ip vrf forwarding Red
   ip address 10.0.1.13 255.255.255.0
   ip mtu 1400
   ip nhrp authentication Red
   ip nhrp map 10.0.1.1 172.17.0.1
   ip nhrp map multicast 172.17.0.1
   ip nhrp network-id 100001
   ip nhrp holdtime 360
   ip nhrp nhs 10.0.1.1
   ip tcp adjust-mss 1360
   delay 1000
   tunnel source Serial3/0
   tunnel mode gre multipoint
   tunnel key 100001
   tunnel protection ipsec profile vpnprof shared
!
interface Tunnel2
   bandwidth 1000
   ip vrf forwarding Green
   ip address 10.0.2.13 255.255.255.0
   ip mtu 1400
   ip nhrp authentication Green
   ip nhrp map 10.0.2.1 172.17.0.1
   ip nhrp map multicast 172.17.0.1
   ip nhrp network-id 100002
   ip nhrp holdtime 360
   ip nhrp nhs 10.0.2.1
   ip tcp adjust-mss 1360
   delay 1000
   tunnel source Serial3/0
   tunnel mode gre multipoint
   tunnel key 100002
   tunnel protection ipsec profile vpnprof shared
```

Separate DMVPNs – VRF-lite
Spoke3 Configuration (cont)

```
interface Ethernet1/0
   ip vrf forwarding Red
   ip address 192.168.31.1 255.255.255.0
!
interface Ethernet2/0
   ip vrf forwarding Green
   ip address 192.168.32.1 255.255.255.0
!
interface Serial3/0
   ip address 172.16.3.1 255.255.255.252
!
router eigrp 1
   no auto-summary
   !
   address-family ipv4 vrf Red
      network 10.0.1.0 0.0.0.255
      network 192.168.31.0
      no auto-summary
      autonomous-system 1
   exit-address-family
   !
   address-family ipv4 vrf Green
      network 10.0.2.0 0.0.0.255
      network 192.168.32.0
      no auto-summary
      autonomous-system 1
   exit-address-family
!
ip route 0.0.0.0 0.0.0.0 172.16.3.2
```

Separate DMVPNs – VRF-lite
Ping to Internet from behind Spoke1

Ping and Traceroute

```
RS1#ping 192.168.254.2

Sending 5, 100-byte ICMP Echos to 192.168.254.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/48/52 ms

RS1#traceroute 192.168.254.2

Tracing the route to 192.168.254.2

  1 192.168.10.1    20 msec 20 msec 20 msec
  2 10.0.0.1        28 msec 32 msec 28 msec
  3 192.168.254.2   52 msec *  52 msec
```

NHRP

```
Spoke1#show ip nhrp

10.0.0.1/32 via 10.0.0.1, Tunnel0 created 1d04h, never expire
  Type: static, used
  NBMA address: 172.17.0.1
```

Separate DMVPNs – VRF-lite
Ping within VRF from behind Spoke1

Ping and Traceroute

```
RS1# ping 192.168.120.1 source 192.168.110.1

Sending 5, 100-byte ICMP Echos to 192.168.120.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.110.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/77/128 ms

RS1# traceroute ip 192.168.120.1 source 192.168.110.1

Tracing the route to 192.168.120.1
  1 192.168.10.1    20 msec 20 msec 20 msec
  2 10.0.0.12       28 msec 32 msec 28 msec
  3 192.168.20.2    40 msec *  40 msec
```

NHRP

```
Spoke1#show ip nhrp

10.0.0.1/32 via 10.0.0.1, Tunnel0 created 1d04h, never expire
  Type: static, used
  NBMA address: 172.17.0.1
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 00:00:51, expire 00:05:09
  Type: dynamic, router, unique, local
  NBMA address: 172.16.1.1    (no-socket)
10.0.0.12/32 via 10.0.0.12, Tunnel0 created 00:00:52, expire 00:05:08
  Type: dynamic, router
  NBMA address: 172.16.2.1
```

Separate DMVPNs – VRF-lite
Ping between VRFs from behind Spoke2

Ping and Traceroute

```
RS2# ping 192.168.110.1 source 192.168.121.1

Sending 5, 100-byte ICMP Echos to 192.168.110.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.121.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/89/100 ms

RS2# traceroute ip 192.168.110.1 source 192.168.121.1

Tracing the route to 192.168.110.1
  1  192.168.21.1     20 msec 20 msec 20 msec
  2  10.0.1.1         32 msec 28 msec 32 msec
  3  192.168.254.2    48 msec 52 msec 48 msec
  4  192.168.254.1    52 msec 48 msec 52 msec
  5  10.0.0.11        80 msec 80 msec 80 msec
  6  192.168.10.2     80 msec *  108 msec
```

NHRP

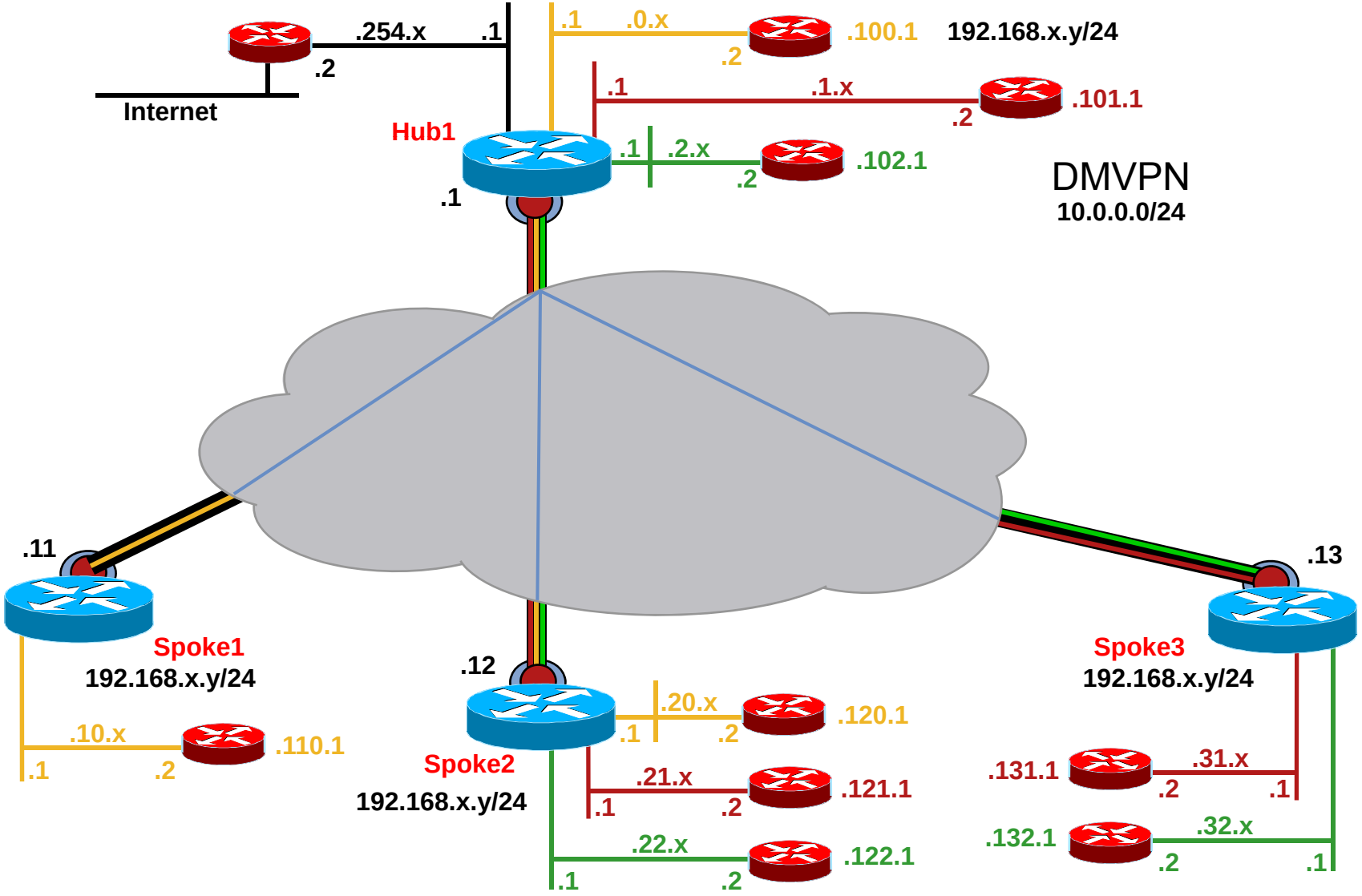
```
Spoke2# show ip nhrp

10.0.1.1/32 via 10.0.1.1, Tunnel1 created 00:19:45, never expire
  Type: static, Flags: used
  NBMA address: 172.17.0.1
10.0.2.1/32 via 10.0.2.1, Tunnel2 created 00:19:42, never expire
  Type: static, Flags: used
  NBMA address: 172.17.0.1
```

Appendix

- DMVPN Overview
- NHRP Details
  - NHRP Overview
  - NHRP Registrations
  - NHRP Resolutions/Redirects
    - Phase 2 (old)
    - Phase 2 (new)
    - Phase 3
- Network Virtualization
  - VRF-lite
  - 2547oDMVPN

MPLS over DMVPN – 2547oDMVPN
Logical Topology



MPLS over DMVPN – 2547oDMVPN
Hub Configuration

```
version 12.4
!
hostname Hub1
!
ip cef
!
ip vrf Green
   rd 3:3
   route-target export 3:3
   route-target import 3:3
!
ip vrf Internet
   rd 10:10
   import map No-Default
   route-target export 10:10
   route-target import 10:10
   route-target import 1:1
   route-target import 2:2
   route-target import 3:3
!
ip vrf Red
   rd 2:2
   route-target export 2:2
   route-target import 2:2
!
ip vrf Yellow
   rd 1:1
   route-target export 1:1
   route-target import 1:1
!
crypto isakmp policy 2
   authentication pre-share
```

```
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set t2 esp-des esp-md5-hmac
   mode transport
crypto ipsec profile vpnprof
   set transform-set t2
!
interface Tunnel0
   bandwidth 1000
   ip address 10.0.0.1 255.255.255.0
   ip nhrp authentication test
   ip nhrp map multicast dynamic
   ip nhrp network-id 100000
   ip nhrp holdtime 360
   mpls ip
   mpls mtu 1404
   tunnel source Serial4/0
   tunnel mode gre multipoint
   tunnel key 100000
   tunnel protection ipsec profile vpnprof
!
interface Ethernet0/0
   ip vrf forwarding Yellow
   ip address 192.168.0.1 255.255.255.0
   ip tcp adjust-mss 1360
!
interface Ethernet1/0
   ip vrf forwarding Red
   ip address 192.168.1.1 255.255.255.0
   ip tcp adjust-mss 1360
!
interface Ethernet2/0
   ip vrf forwarding Green
   ip address 192.168.2.1 255.255.255.0
   ip tcp adjust-mss 1360
```

MPLS over DMVPN – 2547oDMVPN
Hub Configuration (cont)

```
interface Ethernet3/0
   ip vrf forwarding Internet
   ip address 192.168.254.1 255.255.255.0
   ip tcp adjust-mss 1360
!
interface Serial4/0
   ip address 172.17.0.1 255.255.255.252
!
router eigrp 1
   no auto-summary
   !
   address-family ipv4 vrf Yellow
      redistribute bgp 1
      network 192.168.0.0
      default-metric 1000 100 255 1 1500
      no auto-summary
      autonomous-system 1
   exit-address-family
   !
   address-family ipv4 vrf Red
      redistribute bgp 1
      network 192.168.1.0
      default-metric 1000 100 255 1 1500
      no auto-summary
      autonomous-system 1
   exit-address-family
   !
   address-family ipv4 vrf Internet
      redistribute bgp 1
      network 192.168.254.0
      default-metric 1000 100 255 1 1500
      no auto-summary
      autonomous-system 1
   exit-address-family
   address-family ipv4 vrf Green
      redistribute bgp 1
      network 192.168.2.0
      default-metric 1000 100 255 1 1500
      no auto-summary
      autonomous-system 1
   exit-address-family
!
router bgp 1
   no synchronization
   bgp router-id 10.0.0.1
   bgp log-neighbor-changes
   neighbor 10.0.0.11 remote-as 1
   neighbor 10.0.0.11 update-source Tunnel0
   neighbor 10.0.0.12 remote-as 1
   neighbor 10.0.0.12 update-source Tunnel0
   neighbor 10.0.0.13 remote-as 1
   neighbor 10.0.0.13 update-source Tunnel0
   no auto-summary
   !
   address-family vpnv4
   neighbor 10.0.0.11 activate
      neighbor 10.0.0.11 send-community extended
      neighbor 10.0.0.11 route-reflector-client
      neighbor 10.0.0.11 route-map Next-hop-self out
      neighbor 10.0.0.12 activate
      neighbor 10.0.0.12 send-community extended
      neighbor 10.0.0.12 route-reflector-client
      neighbor 10.0.0.12 route-map Next-hop-self out
      neighbor 10.0.0.13 activate
      neighbor 10.0.0.13 send-community extended
      neighbor 10.0.0.13 route-reflector-client
      neighbor 10.0.0.13 route-map Next-hop-self out
   exit-address-family
```

MPLS over DMVPN – 2547oDMVPN
Hub Configuration (cont)

```
router bgp 1
   no synchronization
   !
   address-family ipv4 vrf Yellow
      redistribute connected
      redistribute static
      redistribute eigrp 1
      default-information originate
      no synchronization
   exit-address-family
   !
   address-family ipv4 vrf Red
      redistribute connected
      redistribute static
      redistribute eigrp 1
      default-information originate
      no synchronization
   exit-address-family
   !
   address-family ipv4 vrf Internet
      redistribute connected
      redistribute eigrp 1
      no synchronization
   exit-address-family
   !
   address-family ipv4 vrf Green
      redistribute connected
      redistribute static
      redistribute eigrp 1
      default-information originate
      no synchronization
   exit-address-family
```

```
!
ip route 0.0.0.0 0.0.0.0 172.17.0.2
ip route vrf Green 0.0.0.0 0.0.0.0 Ethernet3/0 192.168.254.2
ip route vrf Red 0.0.0.0 0.0.0.0 Ethernet3/0 192.168.254.2
ip route vrf Yellow 0.0.0.0 0.0.0.0 Ethernet3/0 192.168.254.2
!
access-list 10 permit any
access-list 20 deny host 0.0.0.0
access-list 20 permit any
!
route-map Next-hop-self permit 10
   match ip address 10
   set ip next-hop 10.0.0.1
!
route-map No-Default permit 10
   match ip address 20
!
mpls ldp router-id Tunnel0
```

MPLS over DMVPN – 2547oDMVPN
Spoke1 Configuration

```
version 12.4
!
hostname Spoke1
!
ip cef
!
ip vrf Yellow
   rd 1:1
   route-target export 1:1
   route-target import 1:1
!
crypto isakmp policy 2
   authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set t2 esp-des esp-md5-hmac
   mode transport
!
crypto ipsec profile vpnprof
   set transform-set t2
!
```

```
interface Tunnel0
   bandwidth 1000
   ip address 10.0.0.11 255.255.255.0
   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
   mpls ip
   mpls mtu 1404
   tunnel source Serial2/0
   tunnel mode gre multipoint
   tunnel key 100000
   tunnel protection ipsec profile vpnprof
!
interface Ethernet0/0
   ip vrf forwarding Yellow
   ip address 192.168.10.1 255.255.255.0
   ip tcp adjust-mss 1360
!
interface Serial2/0
   ip address 172.16.1.1 255.255.255.252
```

MPLS over DMVPN – 2547oDMVPN
Spoke1 Configuration (cont)

```
router eigrp 1
   no auto-summary
   !
   address-family ipv4 vrf Yellow
      redistribute bgp 1
      network 192.168.10.0
      default-metric 1000 100 255 1 1500
      no auto-summary
      autonomous-system 1
   exit-address-family
!
router bgp 1
   no synchronization
   bgp router-id 10.0.0.11
   bgp log-neighbor-changes
   neighbor 10.0.0.1 remote-as 1
   neighbor 10.0.0.1 update-source Tunnel0
   no auto-summary
   !
   address-family vpnv4
      neighbor 10.0.0.1 activate
      neighbor 10.0.0.1 send-community extended
   exit-address-family
   !
   address-family ipv4 vrf Yellow
      redistribute eigrp 1
      no synchronization
   exit-address-family
!
ip route 0.0.0.0 0.0.0.0 172.16.1.2
!
mpls ldp router-id Tunnel0
```

MPLS over DMVPN – 2547oDMVPN
Spoke2 Configuration

```
version 12.4
!
hostname Spoke2
!
ip cef
!
ip vrf Green
   rd 3:3
   route-target export 3:3
   route-target import 3:3
!
ip vrf Red
   rd 2:2
   route-target export 2:2
   route-target import 2:2
!
ip vrf Yellow
   rd 1:1
   route-target export 1:1
   route-target import 1:1
!
crypto isakmp policy 2
   authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set t2 esp-des esp-md5-hmac
   mode transport
!
crypto ipsec profile vpnprof
   set transform-set t2
!
```

```
interface Tunnel0
   bandwidth 1000
   ip address 10.0.0.12 255.255.255.0
   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
   mpls ip
   mpls mtu 1404
   tunnel source Serial4/0
   tunnel mode gre multipoint
   tunnel key 100000
   tunnel protection ipsec profile vpnprof
!
interface Ethernet0/0
   ip vrf forwarding Yellow
   ip address 192.168.20.1 255.255.255.0
   ip tcp adjust-mss 1360
!
interface Ethernet1/0
   ip vrf forwarding Red
   ip address 192.168.21.1 255.255.255.0
   ip tcp adjust-mss 1360
!
interface Ethernet2/0
   ip vrf forwarding Green
   ip address 192.168.22.1 255.255.255.0
   ip tcp adjust-mss 1360
!
interface Serial4/0
   ip address 172.16.2.1 255.255.255.252
```

MPLS over DMVPN – 2547oDMVPN
Spoke2 Configuration (cont)

```
router eigrp 1
   no auto-summary
   !
   address-family ipv4 vrf Yellow
      redistribute bgp 1
      network 192.168.20.0
      default-metric 1000 100 255 1 1500
      no auto-summary
      autonomous-system 1
   exit-address-family
   !
   address-family ipv4 vrf Red
      redistribute bgp 1
      network 192.168.21.0
      default-metric 1000 100 255 1 1500
      no auto-summary
      autonomous-system 1
   exit-address-family
   !
   address-family ipv4 vrf Green
      redistribute bgp 1
      network 192.168.22.0
      default-metric 1000 100 255 1 1500
      no auto-summary
      autonomous-system 1
   exit-address-family
!
```

```
router bgp 1
   no synchronization
   bgp router-id 10.0.0.12
   bgp log-neighbor-changes
   neighbor 10.0.0.1 remote-as 1
   neighbor 10.0.0.1 update-source Tunnel0
   no auto-summary
   !
   address-family vpnv4
      neighbor 10.0.0.1 activate
      neighbor 10.0.0.1 send-community extended
   exit-address-family
   !
   address-family ipv4 vrf Yellow
      redistribute eigrp 1
      no synchronization
   exit-address-family
   !
   address-family ipv4 vrf Red
      redistribute eigrp 1
      no synchronization
   exit-address-family
   !
   address-family ipv4 vrf Green
      redistribute eigrp 1
      no synchronization
   exit-address-family
!
ip route 0.0.0.0 0.0.0.0 172.16.2.2
!
mpls ldp router-id Tunnel0
```

MPLS over DMVPN – 2547oDMVPN
Spoke3 Configuration

```
version 12.4
!
hostname Spoke3
!
ip cef
!
ip vrf Green
   rd 3:3
   route-target export 3:3
   route-target import 3:3
!
ip vrf Red
   rd 2:2
   route-target export 2:2
   route-target import 2:2
!
crypto isakmp policy 2
   authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set t2 esp-des esp-md5-hmac
   mode transport
!
crypto ipsec profile vpnprof
   set transform-set t2
!
```

```
interface Tunnel0
   bandwidth 1000
   ip address 10.0.0.13 255.255.255.0
   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 240
   ip nhrp nhs 10.0.0.1
   delay 1000
   mpls ip
   mpls mtu 1404
   tunnel source Serial3/0
   tunnel mode gre multipoint
   tunnel key 100000
   tunnel protection ipsec profile vpnprof
!
interface Ethernet1/0
   ip vrf forwarding Red
   ip address 192.168.31.1 255.255.255.0
   ip tcp adjust-mss 1360
!
interface Ethernet2/0
   ip vrf forwarding Green
   ip address 192.168.32.1 255.255.255.0
   ip tcp adjust-mss 1360
!
interface Serial3/0
   ip address 172.16.3.1 255.255.255.252
!
```

MPLS over DMVPN – 2547oDMVPN
Spoke3 Configuration (cont)

```
router eigrp 1
   no auto-summary
   !
   address-family ipv4 vrf Red
      redistribute bgp 1
      network 192.168.31.0
      default-metric 1000 100 255 1 1500
      no auto-summary
      autonomous-system 1
   exit-address-family
   !
   address-family ipv4 vrf Green
      redistribute bgp 1
      network 192.168.32.0
      default-metric 1000 100 255 1 1500
      no auto-summary
      autonomous-system 1
   exit-address-family
!
```

```
router bgp 1
   no synchronization
   bgp router-id 10.0.0.13
   bgp log-neighbor-changes
   neighbor 10.0.0.1 remote-as 1
   neighbor 10.0.0.1 update-source Tunnel0
   no auto-summary
   !
   address-family vpnv4
      neighbor 10.0.0.1 activate
      neighbor 10.0.0.1 send-community extended
   exit-address-family
   !
   address-family ipv4 vrf Red
      redistribute eigrp 1
      no synchronization
   exit-address-family
   !
   address-family ipv4 vrf Green
      redistribute eigrp 1
      no synchronization
   exit-address-family
!
ip route 0.0.0.0 0.0.0.0 172.16.3.2
!
mpls ldp router-id Tunnel0
```

MPLS over DMVPN – 2547oDMVPN
Ping to Internet from behind Spoke1

Ping and Traceroute

```
RS1#ping 192.168.254.2

Sending 5, 100-byte ICMP Echos to 192.168.254.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/48/60 ms

RS1#traceroute 192.168.254.2

Tracing the route to 192.168.254.2

  1 192.168.10.1 32 msec 24 msec 20 msec
  2 192.168.254.1 [MPLS: Label 19 Exp 0] 28 msec 32 msec 28 msec
  3 192.168.254.2 52 msec *  60 msec
```

MPLS

```
Hub1#show mpls forwarding

Lcl   Outgoing    Prefix          Bytes tag   Outgoing    Next Hop
tag   tag or VC   or Tunnel Id    switched    interface
19    Untagged    0.0.0.0/0[V]      696       Et3/0       192.168.254.2
```

MPLS over DMVPN – 2547oDMVPN
Ping within VRF from behind Spoke1

Ping and Traceroute

```
RS1# ping 192.168.120.1 source 192.168.110.1

Sending 5, 100-byte ICMP Echos to 192.168.120.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.110.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/72/108 ms

RS1# traceroute ip  192.168.120.1 source 192.168.110.1
Tracing the route to 192.168.120.1

  1 192.168.10.1 20 msec 20 msec 20 msec
  2 10.0.0.1 [MPLS: Label 23 Exp 0] 60 msec 80 msec 60 msec
  3 192.168.20.1 [MPLS: Label 16 Exp 0] 44 msec 52 msec 48 msec
  4 192.168.20.2 80 msec *  60 msec
```

MPLS

```
Hub1# show mpls forwarding

Lcl   Outgoing    Prefix           Bytes tag   Outgoing    Next Hop
tag   tag or VC   or Tunnel Id     switched    interface
23    16          192.168.120.0/24[V]  1944    Tu0         10.0.0.12

Spoke2# show mpls forwarding

Lcl   Outgoing    Prefix           Bytes tag   Outgoing    Next Hop
tag   tag or VC   or Tunnel Id     switched    interface
16    Untagged    192.168.120.0/24[V]  3282    Et0/0       192.168.20.2
```

MPLS over DMVPN – 2547oDMVPN
Ping between VRFs from behind Spoke2

Ping and Traceroute

```
RS2# ping 192.168.110.1 source 192.168.121.1

Sending 5, 100-byte ICMP Echos to 192.168.110.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.121.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 88/98/112 ms

RS2# traceroute ip 192.168.110.1 source 192.168.121.1

  1 192.168.21.1 20 msec 24 msec 24 msec
  2 192.168.254.1 [MPLS: Label 36 Exp 0] 40 msec 28 msec 32 msec
  3 192.168.254.2 48 msec 48 msec 52 msec
  4 192.168.254.1 52 msec 48 msec 48 msec
  5 192.168.10.1 [MPLS: Label 16 Exp 0] 80 msec 80 msec 88 msec
  6 192.168.10.2 104 msec *  112 msec
```

MPLS

```
Hub1# show mpls forwarding
Lcl   Outgoing    Prefix           Bytes tag   Outgoing    Next Hop
tag   tag or VC   or Tunnel Id     switched    interface
36    Untagged    0.0.0.0/0[V]     0           Et3/0       192.168.254.2

Spoke2# show mpls forwarding
Lcl   Outgoing    Prefix           Bytes tag   Outgoing    Next Hop
tag   tag or VC   or Tunnel Id     switched    interface
16    Untagged    192.168.110.0/24[V]  2030    Et0/0       192.168.10.2
```

DMVPN and VRF (lite)

- Tunnel Packets in VRF

  GRE tunnel packets use VRF routing table

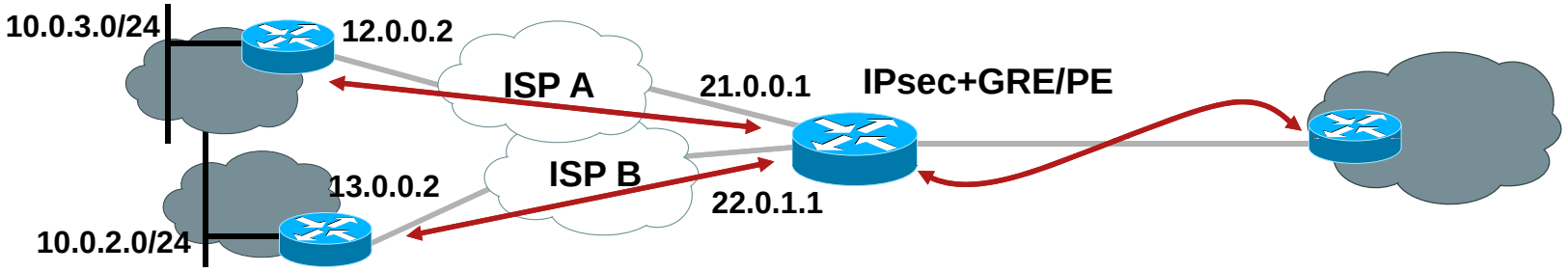
  Data, Routing and NHRP packets use global routing table
- Dual tunnel interfaces
- Single WAN interface, select VRF by ISAKMP profile
- Dual WAN interface, select VRF by WAN interface
- Single LAN interface

- Data packets in VRF

  GRE tunnel packets use global routing table

  Data, Routing and NHRP packets use VRF routing table
- Dual tunnel interfaces
- Dual LAN interface
- Single WAN Interface

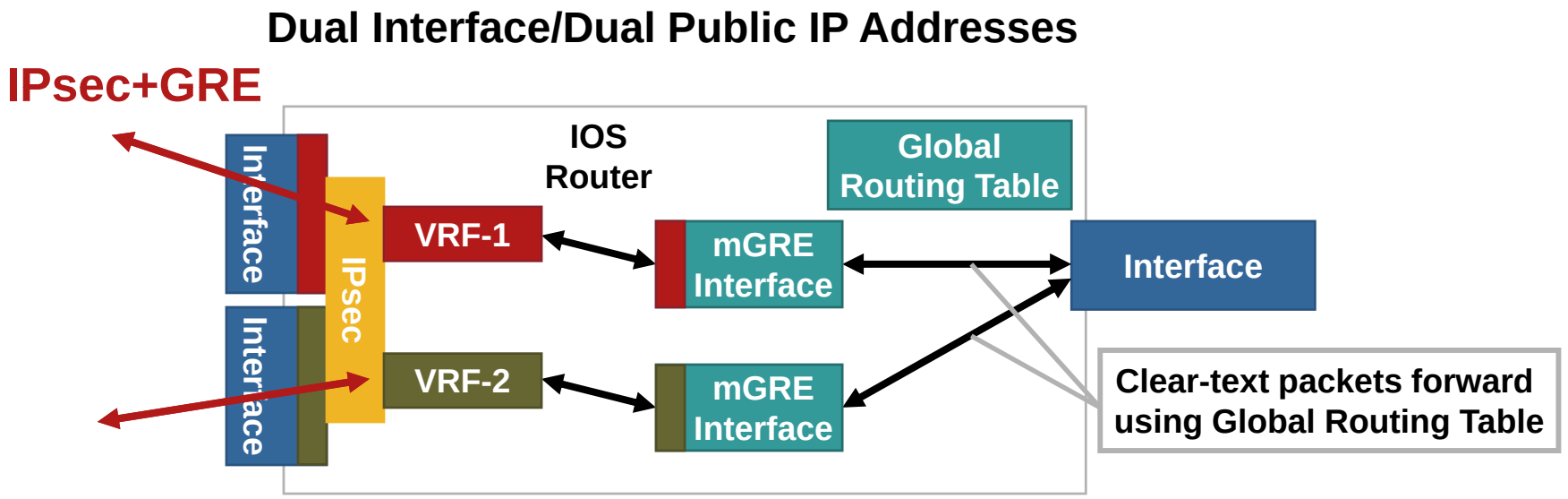
DMVPN and VRF: GRE Tunnel in VRF
Dual WAN Interface—Configuration




```
ip vrf ISPA
     rd 1:101
!
ip vrf ISPB
     rd 2:202
!
crypto keyring ISPA vrf ISPA
     pre-shared-key address 12.0.0.2 key ISPA-123
!
crypto keyring ISPB vrf ISPB
     pre-shared-key address 13.0.0.2 key ISPB-123
!
crypto isakmp policy 1
     authentication pre-share
!
crypto ipsec transform-set test esp-3des esp-md5-hmac
!
crypto ipsec profile vpnprof
     set transform-set tset
```

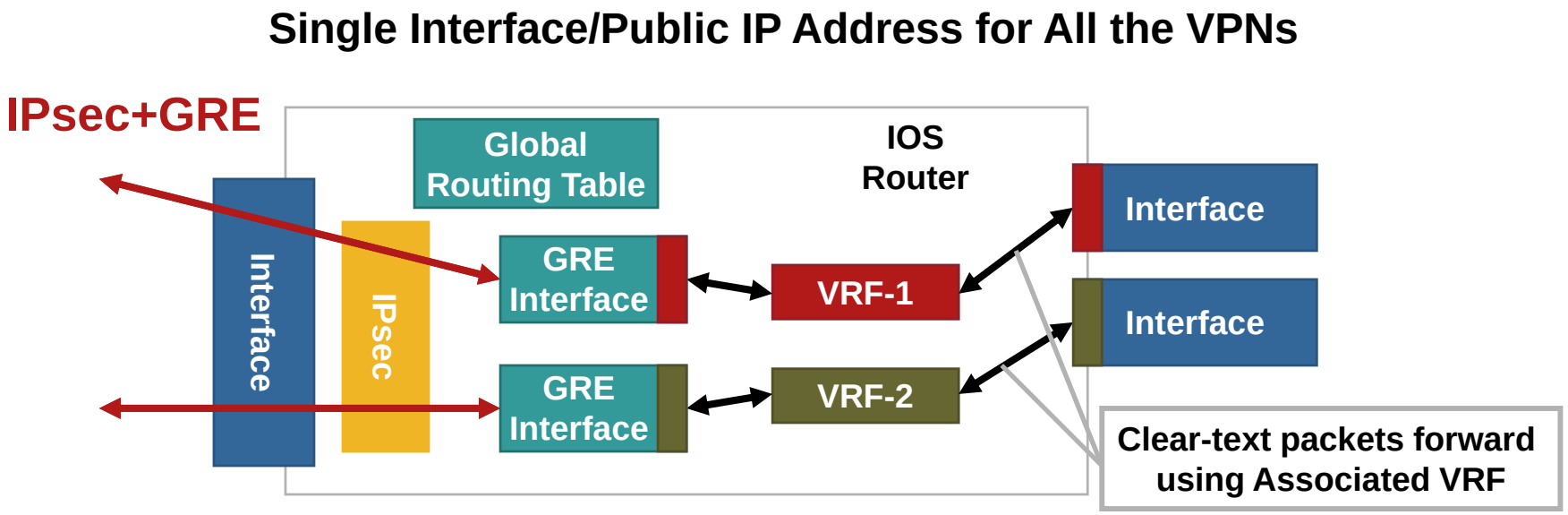
```
interface tunnel0
     ip address 10.0.1.1 255.255.255.252
     . . .
     tunnel vrf ISPA
     tunnel source Fastethernet4/0
     tunnel mode gre multipoint
     tunnel protection ipsec profile vpnprof
!
interface tunnel1
     ip address 10.0.2.1 255.255.255.252
     . . .
     tunnel vrf ISPB
     tunnel source Fastethernet4/1
     tunnel mode gre multipoint
     tunnel protection ipsec profile vpnprof
!
interface FastEthernet4/0
     ip address 21.0.0.1 255.255.255.0
     ip vrf-forwarding ISPA
!
interface FastEthernet4/1
     ip address 22.0.1.1 255.255.255.0
     ip vrf-forwarding ISPB
!
ip route vrf ISPA 0.0.0.0 0.0.0.0 21.0.0.2
ip route vrf ISPB 0.0.0.0 0.0.0.0 22.0.1.2
```

DMVPN and VRF: GRE Tunnel in VRF
Dual WAN interface—Packet Flow



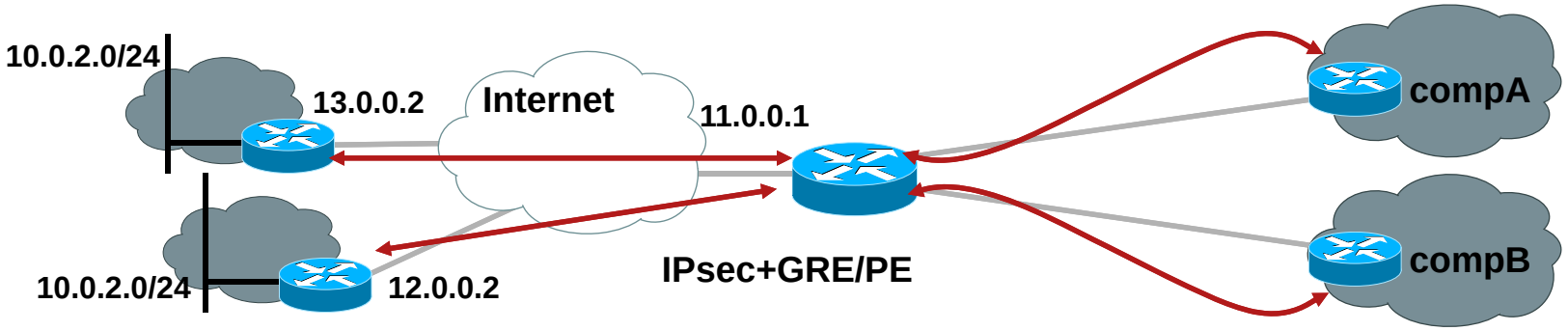
- Based on incoming interface, the IPsec packet is directly associated with VRF
- After decryption the GRE packet is assigned to GRE tunnel in the VRF
- GRE decapsulated clear-text packets forwarded using Global Routing table

DMVPN and VRF
Data Packets in VRF—Packet Flow



- IPsec packets are forwarded using global routing table
- After decryption the GRE packet is assigned to GRE tunnel using global routing table
- GRE decapsulated clear-text packets forwarded using associated VRF

DMVPN and VRF
Data Packets in VRF—Configuration




```
ip vrf compA
     rd 1:101
!
ip vrf compB
     rd 2:202
!
crypto ipsec profile vpnprof
     set transform-set tset
!
interface FastEthernet2/0
     ip address 10.0.11.1 255.255.255.0
     ip vrf-forwarding compA
!
interface FastEthernet3/0
     ip address 10.0.12.1 255.255.255.0
     ip vrf-forwarding compB
!
interface FastEthernet4/0
     ip address 11.0.0.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 11.0.0.2
```

```
interface tunnel0
     ip address 10.0.1.1 255.255.255.0
     . . .
     ip vrf forwarding compA
     tunnel source FastEthernet4/0
     tunnel mode gre multipoint
     tunnel  protection ipsec profile vpnprof shared
!
interface tunnel1
     ip address 10.0.2.1 255.255.255.0
     . . .
     ip vrf forwarding compB
     tunnel source FastEthernet4/0
     tunnel mode gre multipoint
     tunnel  protection ipsec profile vpnprof shared
!
router eigrp 1
     address-family ipv4 vrf compA
     network 10.0.0.0
     no auto-summary
     autonomous-system 1
     exit-address-family
!
     address-family ipv4 vrf compB
     network 10.0.0.0
     no auto-summary
     autonomous-system 1
     exit-address-family
```