Cisco IOS DMVPN Overview

February 2008

Cisco.com/go/dmvpn

Cisco IOS Software Secure Connectivity Overview

Industry-Leading VPN Solutions

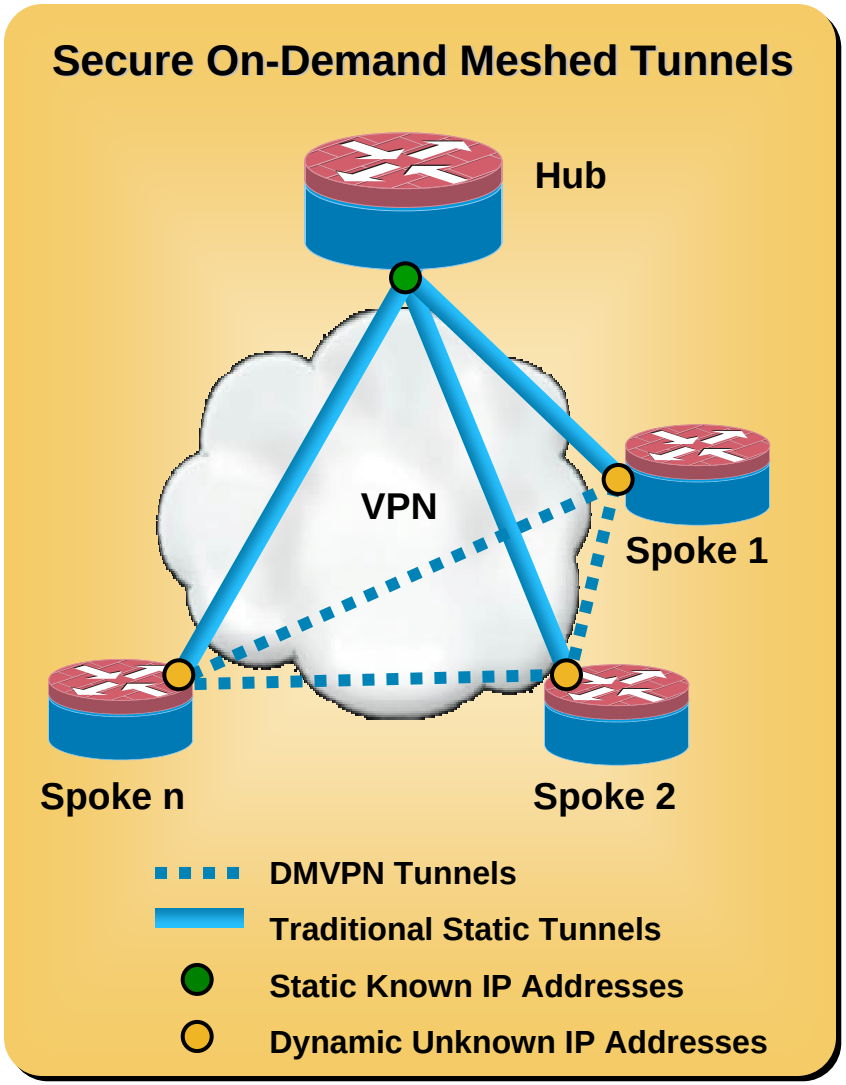
Solution	Critical Technologies
Standard IPsec	▪ Full standards compliance for interoperability with other vendors
Advanced site-to-site VPN	▪ Hub-and-spoke VPN: Enhanced Easy VPN: Dynamic Virtual Tunnel Interfaces, Reverse Route Injection, dynamic policy push, and high scalability Routed IPsec + GRE or DMVPN with dynamic routing ▪ Spoke-to-spoke VPN: Dynamic Multipoint VPN (DMVPN) – On-demand VPNs (partial mesh) ▪ Any-to-any VPN: Group Encrypted Transport (GET) VPN – No point-to-point tunnels
Advanced remote-access VPN	▪ Easy VPN (IPsec): Cisco® Dynamic Policy Push and *free* VPN clients for Windows, Linux, Solaris, and Mac platforms ▪ SSL VPN: No client preinstallation required; provides endpoint security through Cisco Secure Desktop

Cisco IOS VPN Primary Differentiators

First to market	**Cisco® is the first to support innovative VPN solutions such as Easy VPN, DMVPN, and GETVPN on an integrated services access router.**
Platform support	**Cisco has comprehensive VPN platform offerings, including support for VSA, VAM2+, VPN-SPA, and integrated services routers.**
Integration	**Cisco VPN solutions have advanced network integration capabilities, such as QoS, IP Multicast, voice, and video.**
Feature performance	**Cisco VPN solutions offer rich integration of VPN with several routing protocols such as OSPF, EIGRP, BGP, and RIPv2 without degrading performance to enable scalable services.**
Enhanced management	**Cisco has a comprehensive management suite for provisioning and maintenance of VPN networks.**

Dynamic Multipoint VPN

- Provides full meshed connectivity with simple configuration of hub and spoke
- Supports dynamically addressed spokes
- Facilitates zero-touch configuration for addition of new spokes
- Features automatic IPsec triggering for building an IPsec tunnel



What Is Dynamic Multipoint VPN?

- DMVPN is a Cisco IOS® Software solution for building IPsec + GRE VPNs in an easy, dynamic, and scalable manner.
- DMVPN relies on two proven technologies:

  Next Hop Resolution Protocol (NHRP): Creates a distributed (NHRP) mapping database of all the spoke tunnels to real (public interface) addresses

  Multipoint GRE Tunnel Interface: Single GRE interface to support multiple GRE and IPsec tunnels; simplifies size and complexity of configuration

Enterprise Network Designs

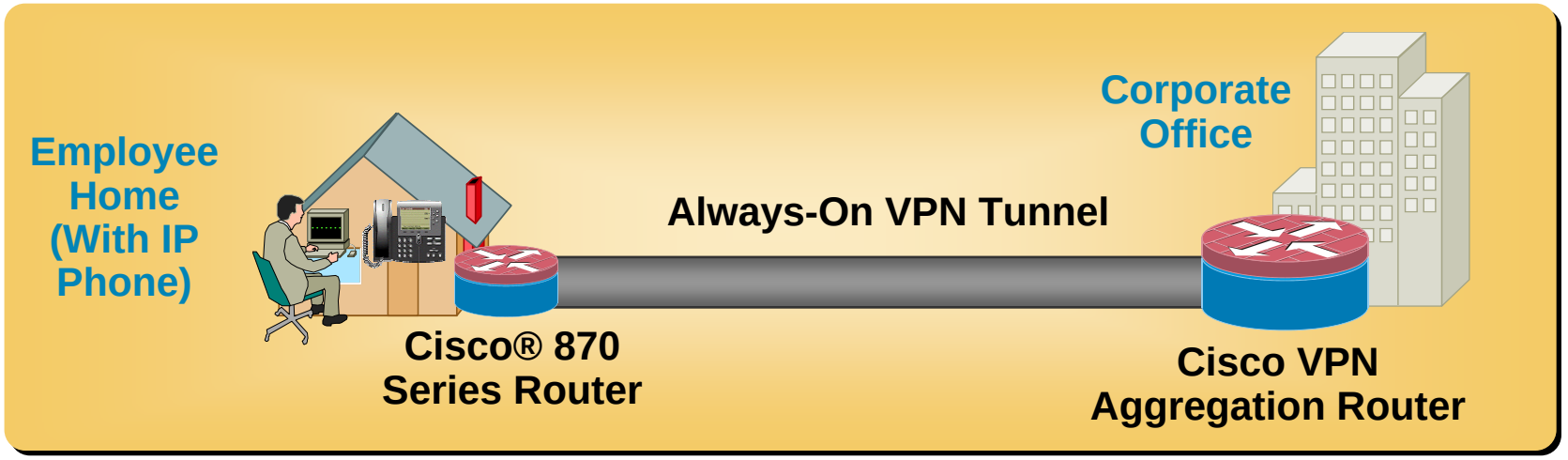
Point of Sale

- Typical examples include Bank ATM or retail credit and debit card networks
- Requirement is to terminate a very large number (up to 20,000+) of low-bandwidth spokes
- Routing protocol scalability very important

- Server-load-balancing (SLB) designs for super hub
- No spoke-to-spoke functions required immediately, but under consideration for future

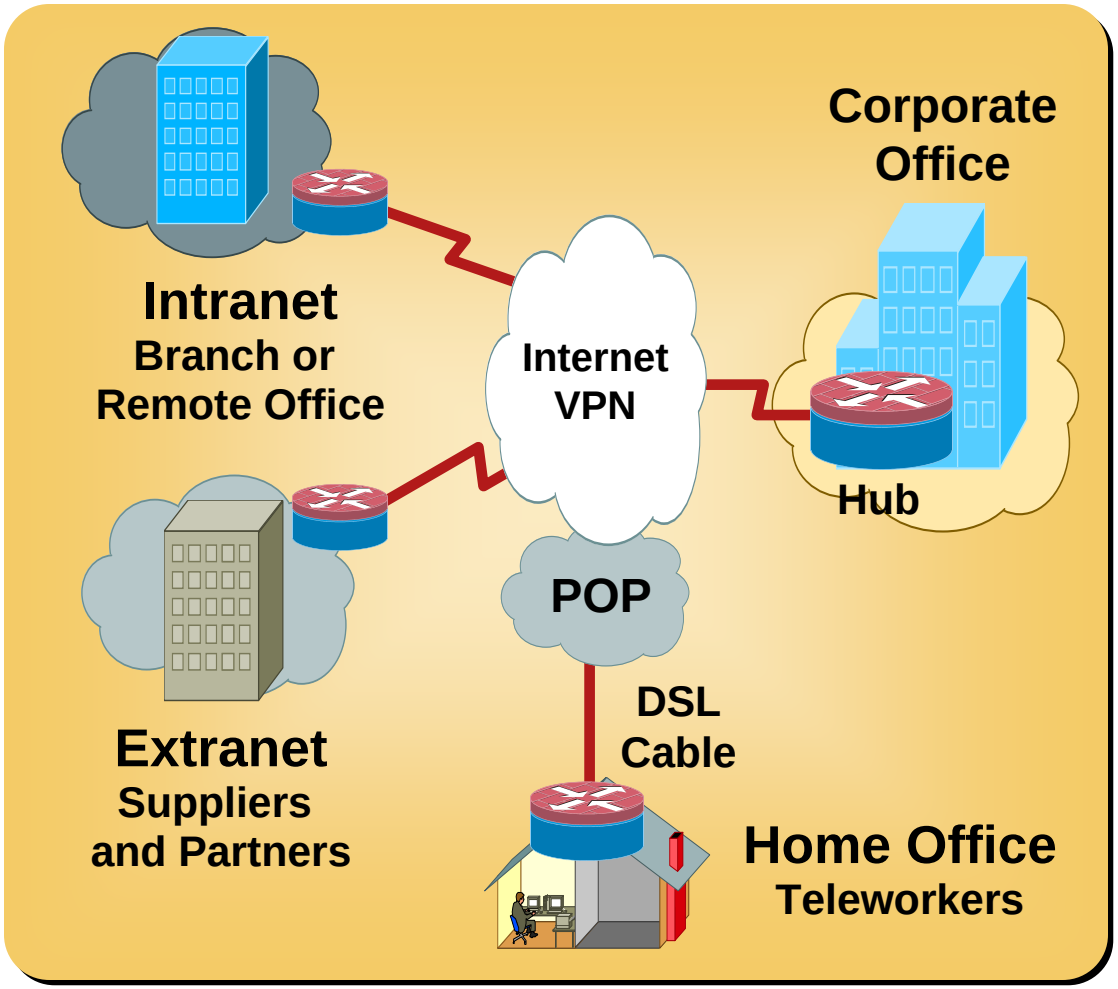
Enterprise Network Designs

Small Office or Home Office



- Single-layer small DMVPN network
- Used to provide work access from home or offsite locations
- Enterprise Class Teleworker (ECT) designs
- NAT support needed on most of the spokes
- Thousands of spokes
- Typical requirement is to support voice and data to and from the head-office (hub) location with occasional spoke-to-spoke voice

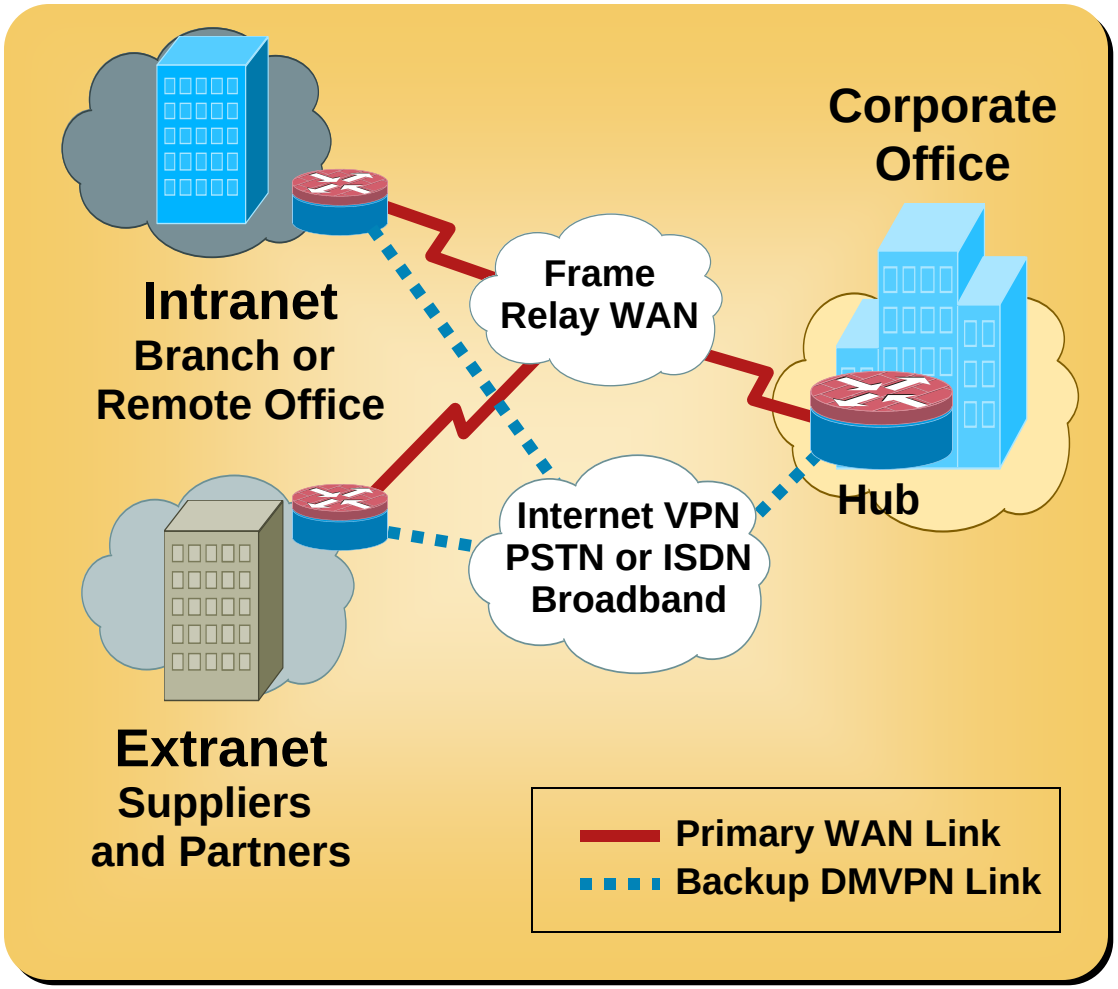
Enterprise Network Designs
Extranet



- DMVPN hub-and-spoke design
- No spoke-spoke allowed, not even through the hub (using ACLs)
- Typically less than 1000 spokes
- Hub choice depends on amount of traffic each spoke transmits and receives

Enterprise Network Designs

DMVPN Backup for Layer 2 MPLS WAN



- Single-layer DMVPN design (mostly)
- Hub-and-spoke and spoke-to-spoke networks
- Different size networks (number of spokes), but also supporting many DMVPN networks on the same set of hub routers

Service Provider Network Designs

Internet Service Provider

- Single-layer DMVPN design (mostly)
- VRF-aware DMVPN on the hubs to segregate customer traffic
- MPLS (2547oDMVPN); connecting provider edge devices over an IP network (current support only for hub and spoke)
- Hub-and-spoke and spoke-to-spoke networks
- Different size networks (number of spokes), but also supporting many DMVPN networks on the same set of hub routers

DMVPN Overview

DMVPN: Major Features

- Offers configuration reduction and no-touch deployment
- Supports IP Unicast, IP Multicast, and dynamic routing protocols
- Supports remote peers with dynamically assigned addresses
- Supports spoke routers behind dynamic NAT and hub routers behind static NAT
- Dynamic spoke-to-spoke tunnels for scaling partial- or full-mesh VPNs
- Usable with or without IPsec encryption

Configuration Reduction

Before DMVPN: p-pGRE + IPsec

- Single GRE interface for each spoke
- All tunnels need to be predefined
  - Uses static tunnel destination
  - Requires static addresses for spokes
  - Supports dynamic routing protocols
- Large hub configuration
  - 1 interface/spoke ➔ 250 spokes = 250 interfaces
  - 7 lines/spoke ➔ 250 spokes = 1750 lines
  - 4 IP addresses/spoke ➔ 250 spokes = 1000 addresses
- Addition of spokes requires changes on the hub
- Spoke-to-spoke traffic through the hub

Configuration Reduction

With DMVPN: mGRE + IPsec

- One mGRE interface supports ALL spokes
  - Multiple mGRE interfaces allowed: each is in a separate DMVPN
- Dynamic Tunnel Destination simplifies support for dynamically addressed spokes
  - NHRP registration and dynamic routing protocols
- Smaller hub configuration
  - One interface for all spokes e.g. 250 spokes → 1 interface
  - Configuration including NHRP e.g. 250 spokes → 15 lines
  - All spokes in the same subnet e.g. 250 spokes → 250 addresses
- No need to touch the hub for new spokes
- Spoke to spoke traffic via the hub or direct

Dynamic Routing Protocols

	Network Type	Route Control	Converge	CPU	Scaling	Notes
EIGRP	Hub-spoke Spoke-spoke	Good	Faster	High	Lower	
OSPF	Hub-spoke Spoke-spoke	Fair	Faster	High	Lower	Single area
BGP	Hub-spoke Spoke-spoke	Good	Slower	Medium	Medium*	Static neighbor
RIPv2	Hub-spoke**	Poor	Slower	Low	High	Passive mode needs IP SLA
ODR	Hub-spoke**	None	Slower	Low	High	Default route only

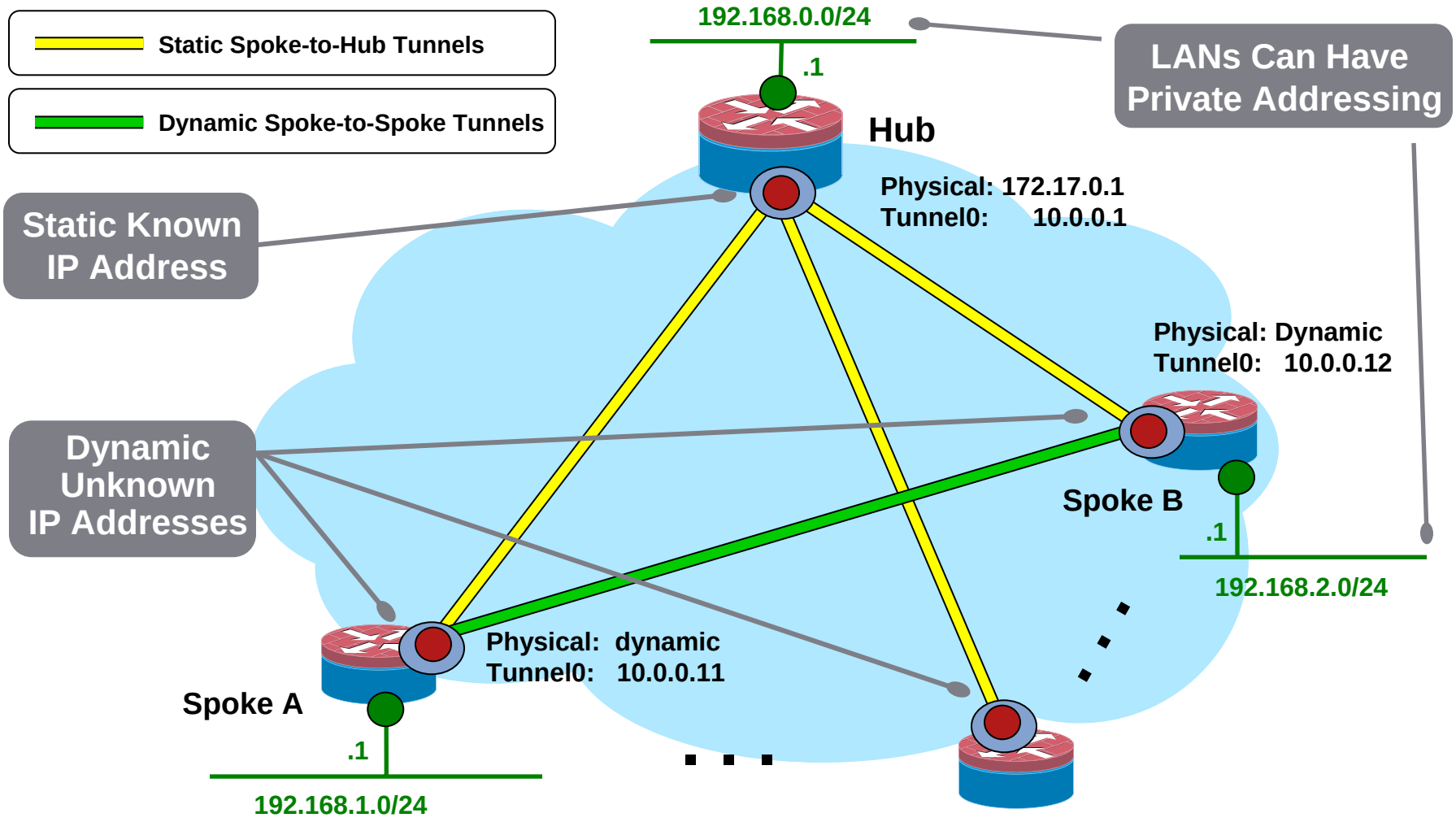
*** Scaling can be increased by using a BGP Route Reflector model; i.e., terminating BGP session at the hub location on a number of BGP route reflectors—hub is a route reflector client**

**** Can be used for spoke-to-spoke**

Dynamic Addressing

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

Dynamic Tunnels: Example



DMVPN Uses: With or Without IPsec

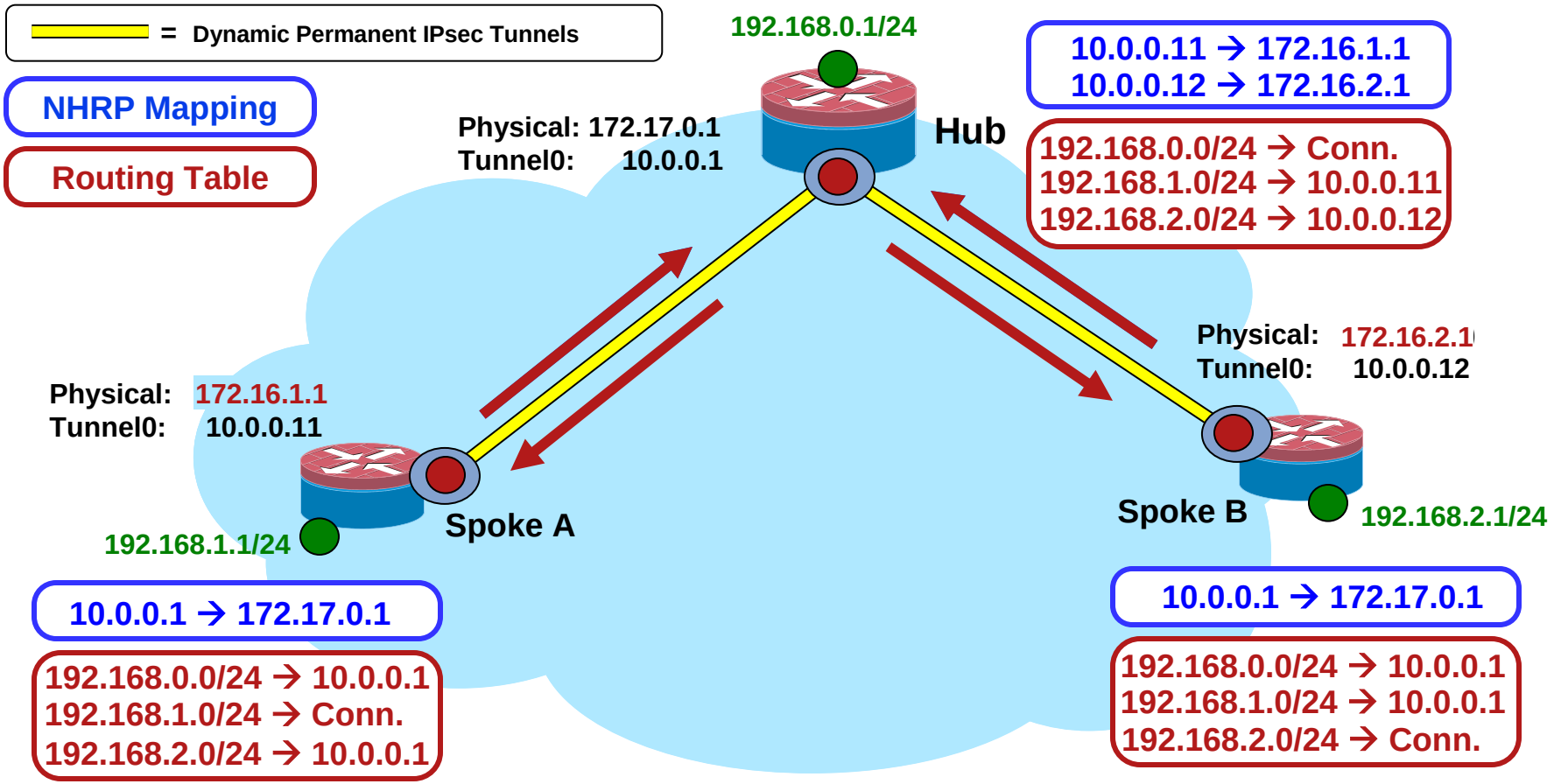
- DMVPN builds out a dynamic tunnel overlay network.
- DMVPN can run without encryption.
- IPsec is triggered through "tunnel protection".
  - NHRP triggers IPsec before installing new mappings.
  - IPsec notifies NHRP when encryption is ready.
  - NHRP installs mappings, and sends registration if needed.
  - NHRP and IPsec notify each other when a mapping or service assurance is cleared.

DMVPN Details

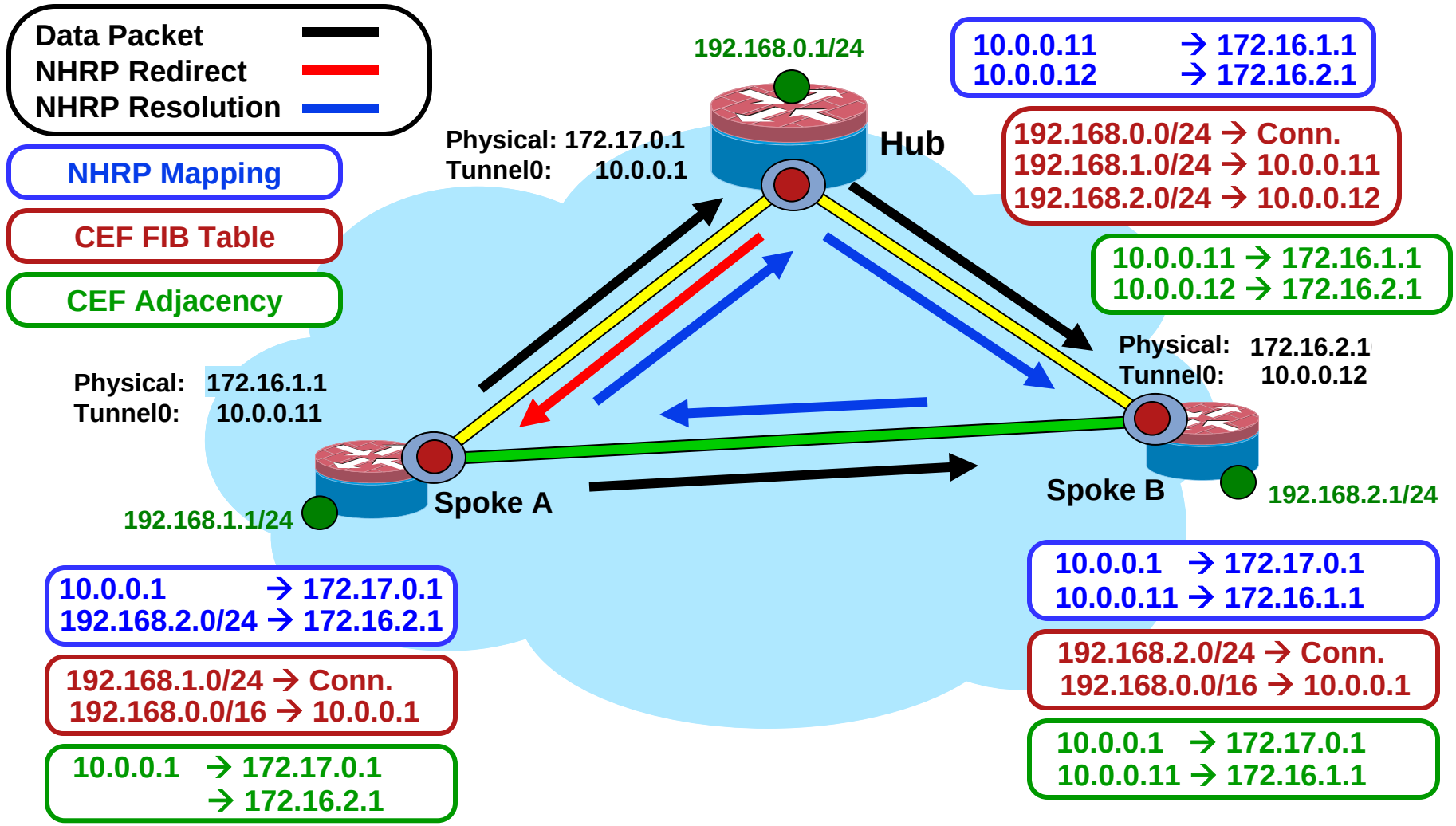
DMVPN Components: NHRP

- NHRP registration
  - Spoke dynamically registers its mapping with NHS
  - Supports spokes with dynamic NBMA addresses or NAT
- NHRP resolutions and redirects
  - Supports building dynamic spoke-to-spoke tunnels
  - Control and IP Multicast traffic still through hub
  - Unicast data traffic direct; reduced load on hub routers

NHRP Registration Example
Dynamically Addressed Spokes



NHRP Resolutions and Redirects



DMVPN Components
Multipoint GRE Tunnels

- Single tunnel interface (multipoint)
  - Non-Broadcast Multi-Access (NBMA) network
  - Smaller hub configuration
  - Multicast and broadcast support
- Dynamic tunnel destination
  - Next Hop Resolution Protocol (NHRP)
  - VPN IP-to-NBMA IP address mapping
  - Short-cut forwarding
  - Direct support for dynamic addresses and NAT

DMVPN
Design Overview

Network Designs

- Hub-and-spoke

  Spoke-to-spoke traffic through hub; requires about the same number of tunnels as spokes

  - Hub bandwidth and CPU limit VPN
  - Server Load Balancing: Many “identical” hubs increase CPU power; spoke-to-spoke design under consideration

- Spoke-to-spoke: Dynamic spoke-to-spoke tunnels

  Control traffic: Hub-and-spoke; hub to hub

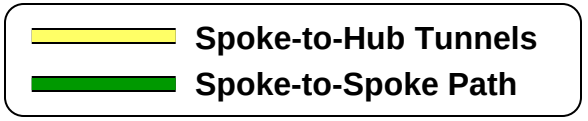
  - Hub-and-spoke single-layer
  - Hierarchical hub-and-spoke layers

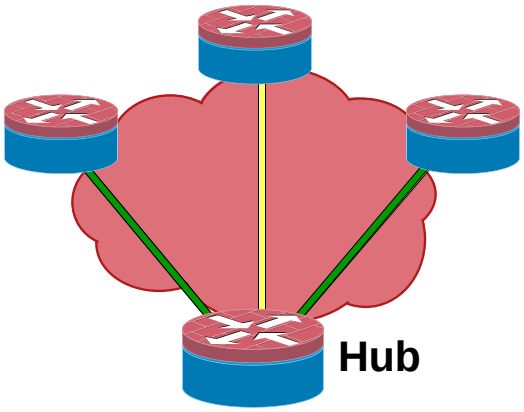
  Unicast data traffic: Dynamic mesh

  - Spoke routers support spoke-to-hub and spoke-to-spoke tunnels

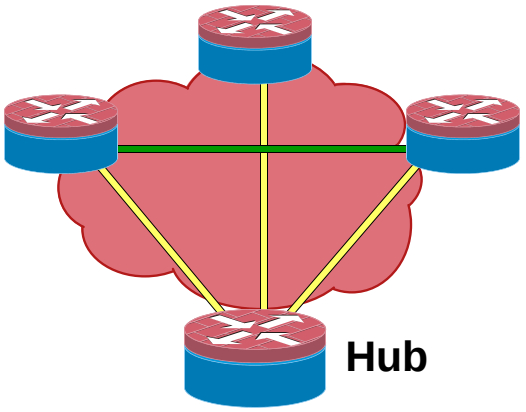
  Number of tunnels falls between the number of spokes n and n^2 where n is the number of spokes (full-mesh)

Network Designs

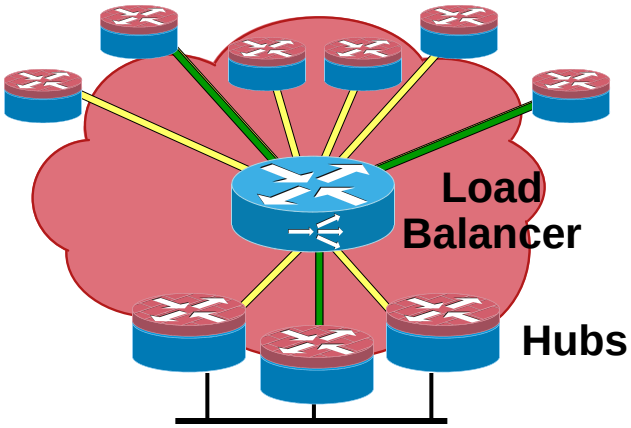




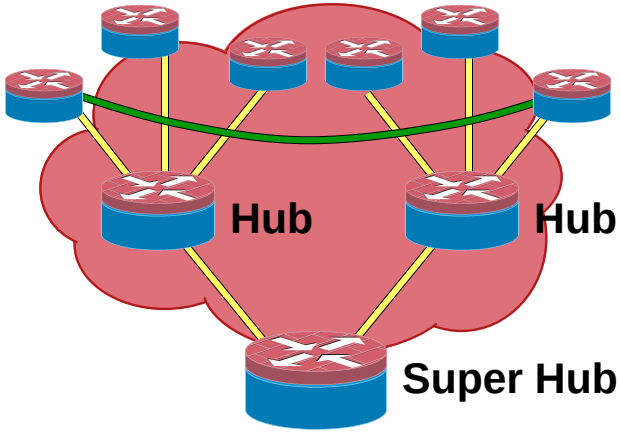
Hub-and-Spoke



Spoke-to-Spoke



Hub-and-Spoke with Server Load Balancing



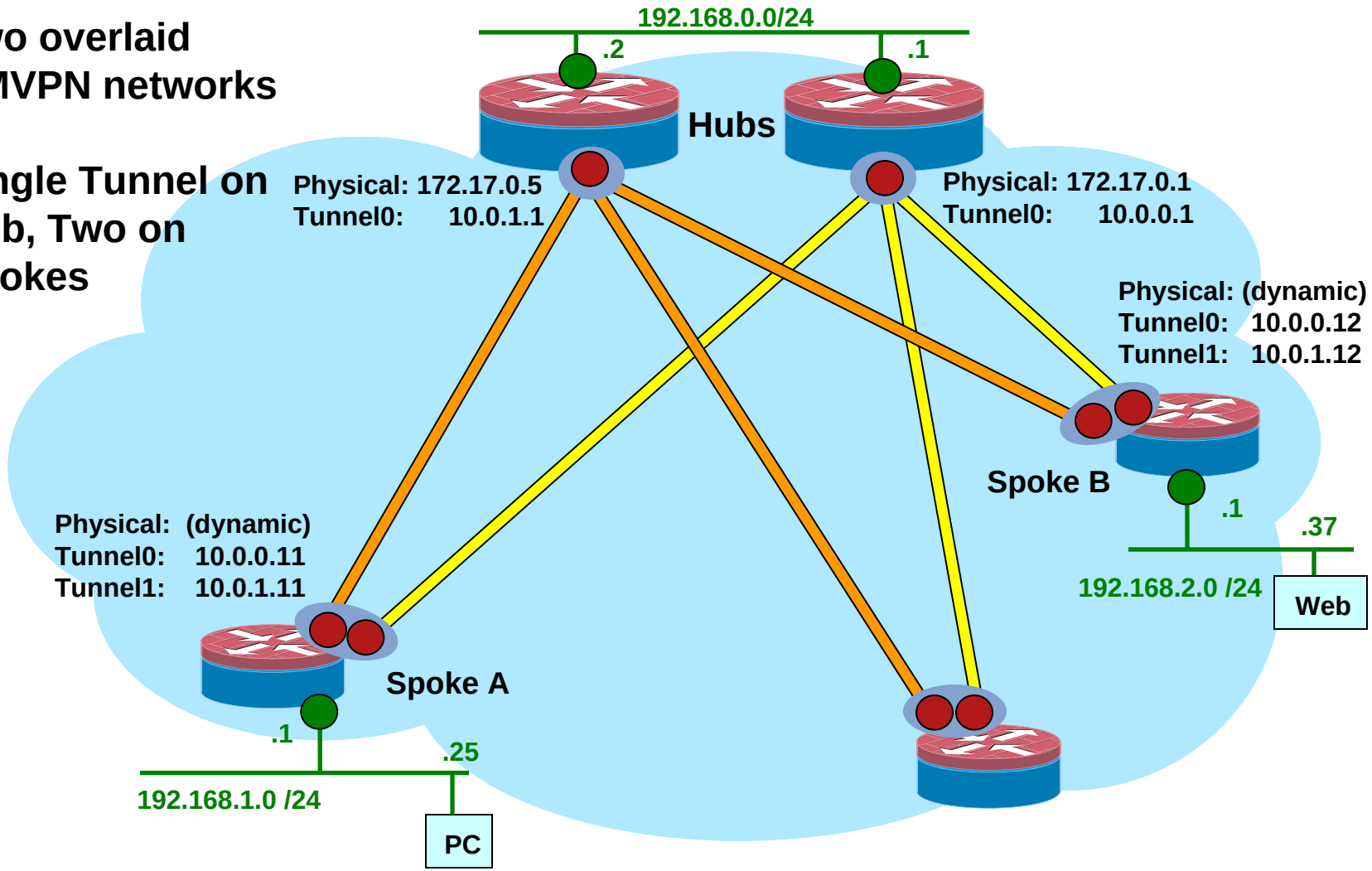
Hierarchical Spoke-to-Spoke

DMVPN Hub-and-Spoke Designs

DMVPN Dual Hub

Two overlaid DMVPN networks

Single Tunnel on Hub, Two on Spokes



Large Scale Deployment
Server Load Balancing Features

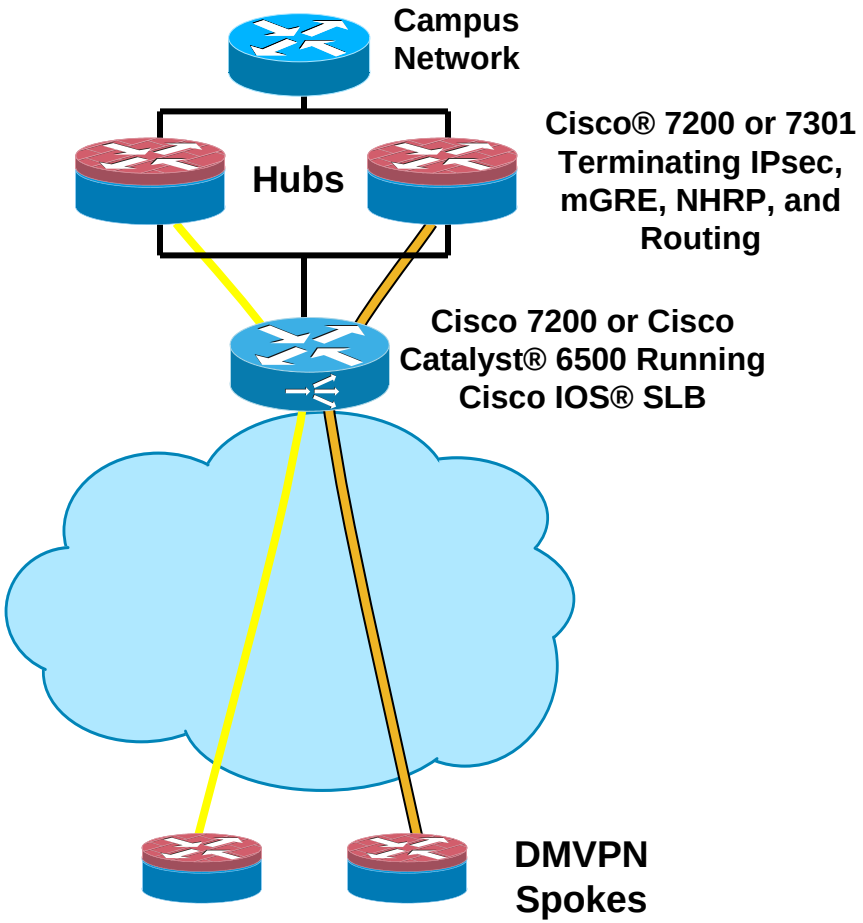
- Scales to very large DMVPN hub-and-spoke network
  - Supports thousands of spokes
  - Spoke-to-spoke through the hub is allowed
  - Direct spoke-to-spoke tunnels are being explored
  - Keep all features of DMVPN hub-and-spoke networks
- Automates load management
  - Tunnels load balanced over available hubs
    - mGRE tunnels only or both IPsec + mGRE tunnels
  - N + 1 Hub redundancy
- Allows incremental performance by adding hubs
  - Tunnel creation rate, throughput, and maximum number of tunnels

Large Scale Deployment
Server Load Balancing Benefits

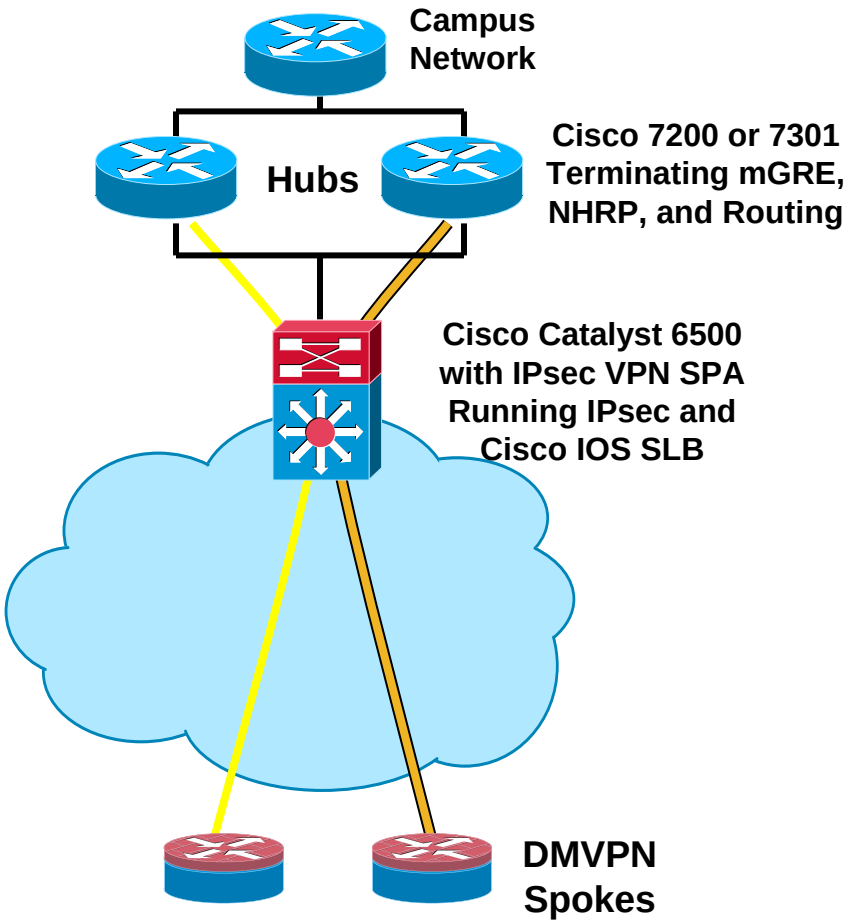
- Very easy to configure and maintain
- The Spoke-to-Spoke links are established on demand whenever there is traffic between the spokes.
  - The following packets are then able to bypass the Hub and use the Spoke-to-Spoke tunnel
  - After a pre-configured period of inactivity on the Spoke-to-Spoke tunnels, the router tears down these tunnels in order to save resources (IPsec SAs)
- In this way, even the low end routers (e.g. Cisco 1800) can participate in large IPsec VPNs with thousands of nodes, as they do not need to have large numbers of simultaneous Spoke-to-Spoke tunnels

Server Load Balancing Deployment Models

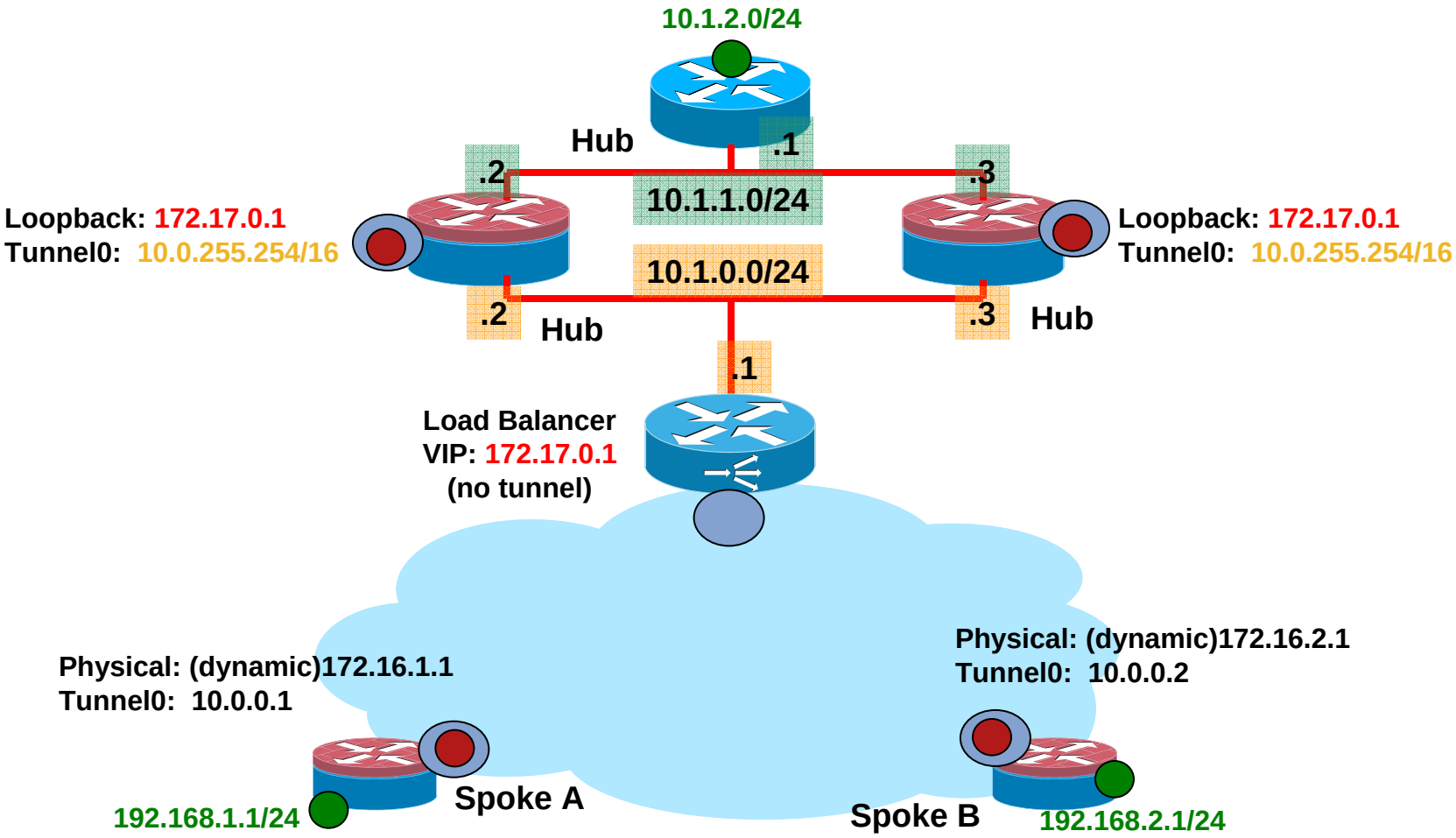
Distributed Encryption with Server Load Balancing (SLB)



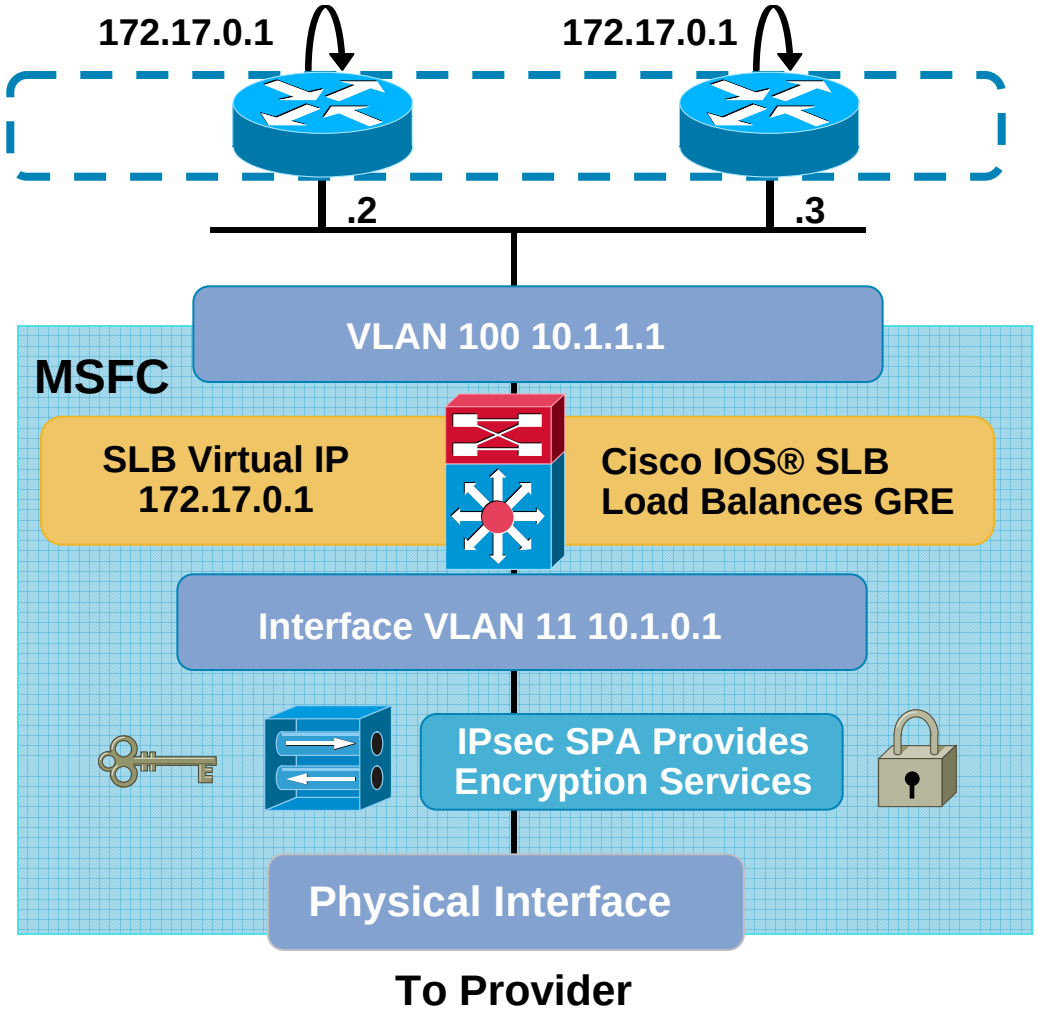
Integrated Encryption with Server Load Balancing



Distributed Encryption with SLB



Integrated Encryption with SLB



Cisco® 7201 or 7301 Routers

Cisco Catalyst® 6500

Integrated Encryption with SLB

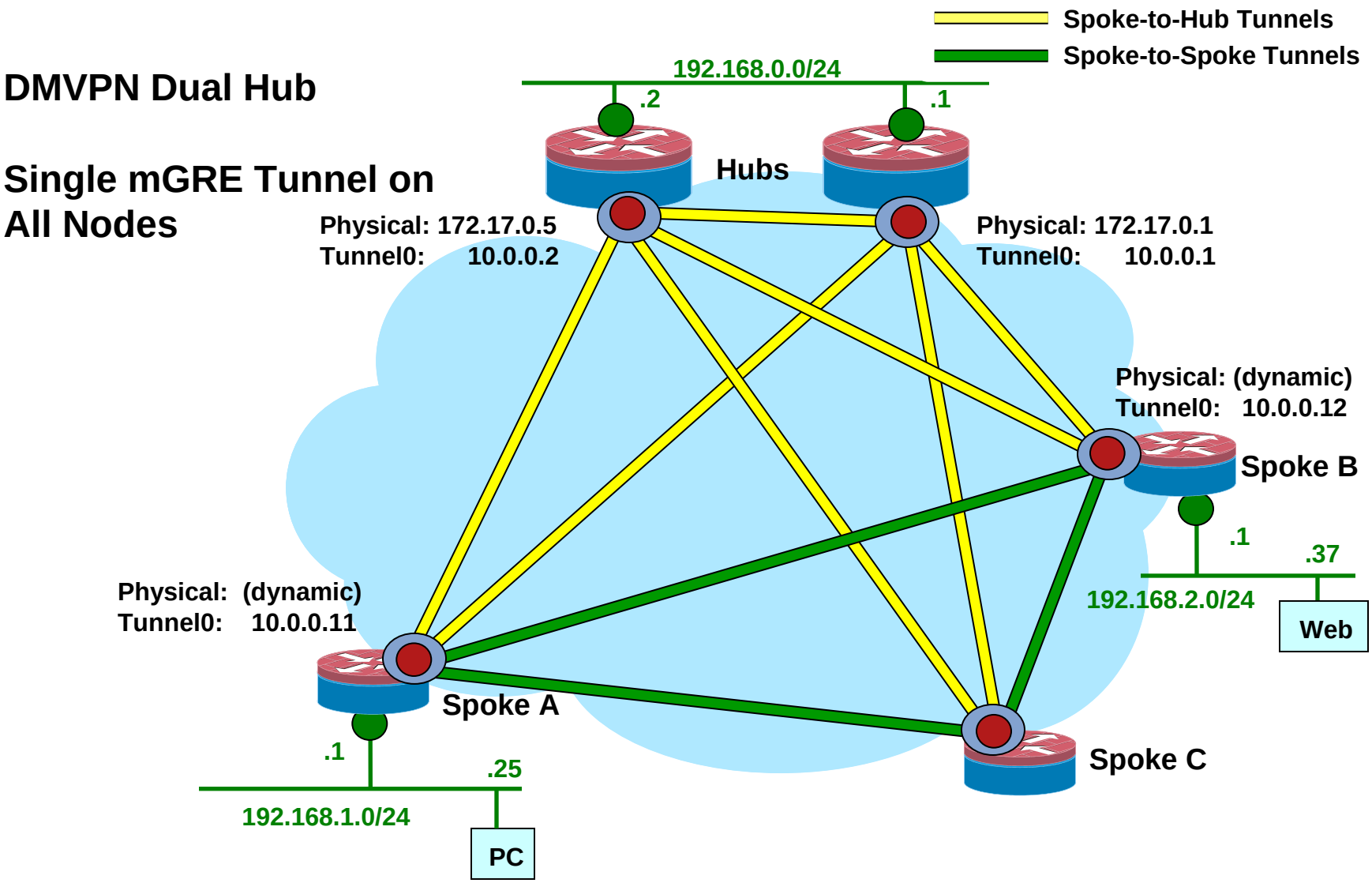
- High-concentration hub aggregates thousands of high-bandwidth DMVPN spokes
  - Hub-and-spoke model with one tunnel per spoke
- Cisco® Catalyst® 6500 with Supervisor Engine 2, MSFC, and IPsec VPN SPA acts as front-end for Router farm made up of 1RU Cisco 7201 or 7301s
  - IPsec VPN SPA performs encryption
  - Cisco IOS Server Load Balancing (SLB) on MSFC load balances mGRE tunnels on Cisco 7200 or 7301 Router farm
  - In the event a Cisco 7200 or 7301 Router goes down, SLB redistributes tunnels
- Cisco 7200 or 7301 Router farm processes mGRE, NHRP, and routing protocols
  - EIGRP between hub (Cisco 7200 or 7301 Routers) and spokes
  - BGP between hubs

DMVPN Spoke-to-Spoke Designs

Spoke-to-Spoke DMVPN Features

- Single mGRE interface with "tunnel protection …"
  - On hubs and spokes
- Data traffic flows directly from spoke to spoke
  - Reduced load on hub
  - Reduced latency: Single IPsec encryption and decryption
- Routing protocols follow hub-and-spoke
  - Hub summarizes spoke routes
  - Routes on spokes must have IP next hop of remote spoke

DMVPN Dual Hub Spoke-to-Spoke



DMVPN Dual Hub Spoke-to-Spoke

- One DMVPN network

  Each spoke has single mGRE tunnel.

  – NHRP mappings for two hubs (NHSs)

  Each hub has single mGRE tunnel interface.

  – Member of same DMVPN network

  Hubs and spokes can be members of more then one DMVPN network for more complex network designs.

- Control of routing and forwarding

  Single interface on spoke makes it harder to modify routing metric to prefer one hub over the other.

- Spoke-to-hub and hub-to-spoke paths can be asymmetric

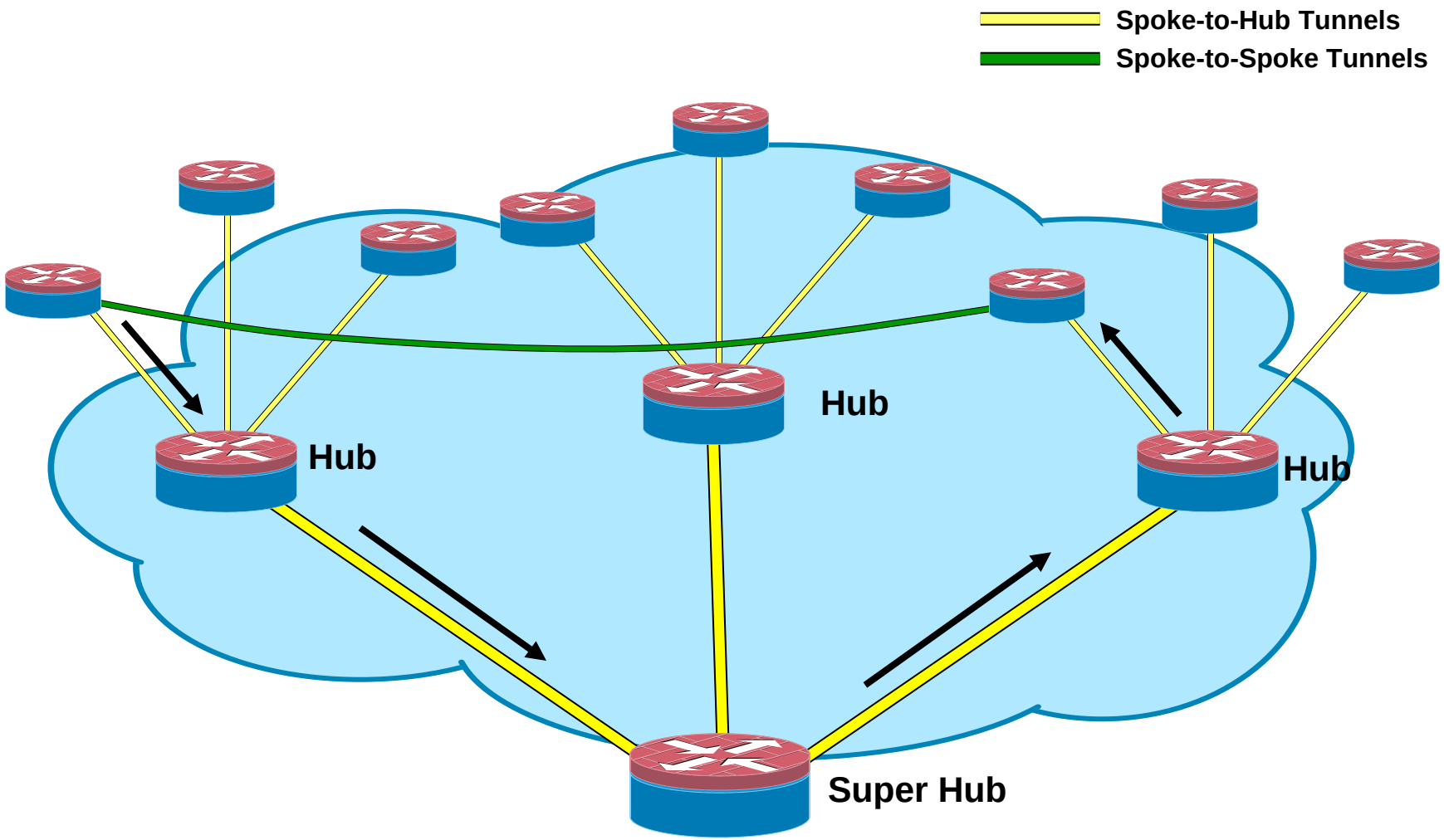
Large Scale DMVPN Features

- Used to increase scale of DMVPN networks
  - Increased number of spokes, with same spoke-to-hub ratio
  - Distribution hubs offload central hub
    - Manage local spoke-to-spoke tunnels
    - Support IP Multicast and routing protocols
- No hub daisy chain
  - Uses routing and Cisco® Express Forwarding switching to forward data and NHRP packets optimally through hubs
  - Reduces complexity and load for routing protocol
- OSPF routing protocol not limited to 2 hubs
  - Network point-to-multipoint mode
  - Still single OSPF area

Large Scale DMVPN Features (Cont.)

- Spokes do not need full routing tables
  - Can summarize routes at the hub
  - Reduced space and load on small spokes
  - Reduced routing protocol load on hub
    - 1000 spokes; 1 route per spoke
    - Hub advertises 1 route to 1000 spokes →1000 advertisements
- Not available on Cisco® Catalyst® 6500 or Cisco 7600
- Cannot mix older DMVPN implementations with latest
  - Migrate spokes to latest DMVPN implementation

DMVPN Hierarchical Network Phase 3



DMVPN Manageability

Cisco Security Manager 3.1

- Supports DMVPN hub-and-spoke and spoke-to-spoke configurations
- Supports DMVPN server-load-balancer model
- Supports high-concentration hub design
- Supports VRF-aware DMVPN
- Supports all the common routing protocols: EIGRP, OSPF, RIPv2, and ODR
- Supports wide variety of Cisco® platforms (Cisco 800 Series, Cisco 7000 Series, etc.)

Debug and Show Commands Introduced in Cisco IOS Software Release12.4(9)T

- Show

  show dmvpn
  [peer {{{ nbma | tunnel } ***ip_address*** } |
  { network ***ip_address mask*** } | { interface ***tunnel#*** } |
  { vrf ***vrf_name*** }}]
  [detail] [static]

- Debug

  debug dmvpn [{ error | event | detail | packet | all }
  { nhrp | crypto | tunnel | socket | all }]
  debug dmvpn condition [peer
  {{{ nbma | tunnel } ***ip_address*** } | { network ***ip_address mask*** } |
  { interface ***tunnel#*** } | { vrf ***vrf_name*** }}]

- Logging

  logging dmvpn { <cr> | rate-limit < ***0-3600*** > }

Summary

- Industry-leading integration of VPN and networking

  Tunnel-less IPsec, dynamic IPsec tunnels, QoS, and IP Multicast

- Excellent application support

  Voice, video, multicast, and non-IP application support

- Ease of deployment and management

  DMVPN: Large-scale scalable and secure connectivity

  Low-touch, highly scalable deployment options, such as Secure Device Provisioning, Cisco® Configuration Engine, and Cisco Configuration Express

  IP SLA: VPN performance and SLA conformance monitoring

www.cisco.com/go/routersecurity