



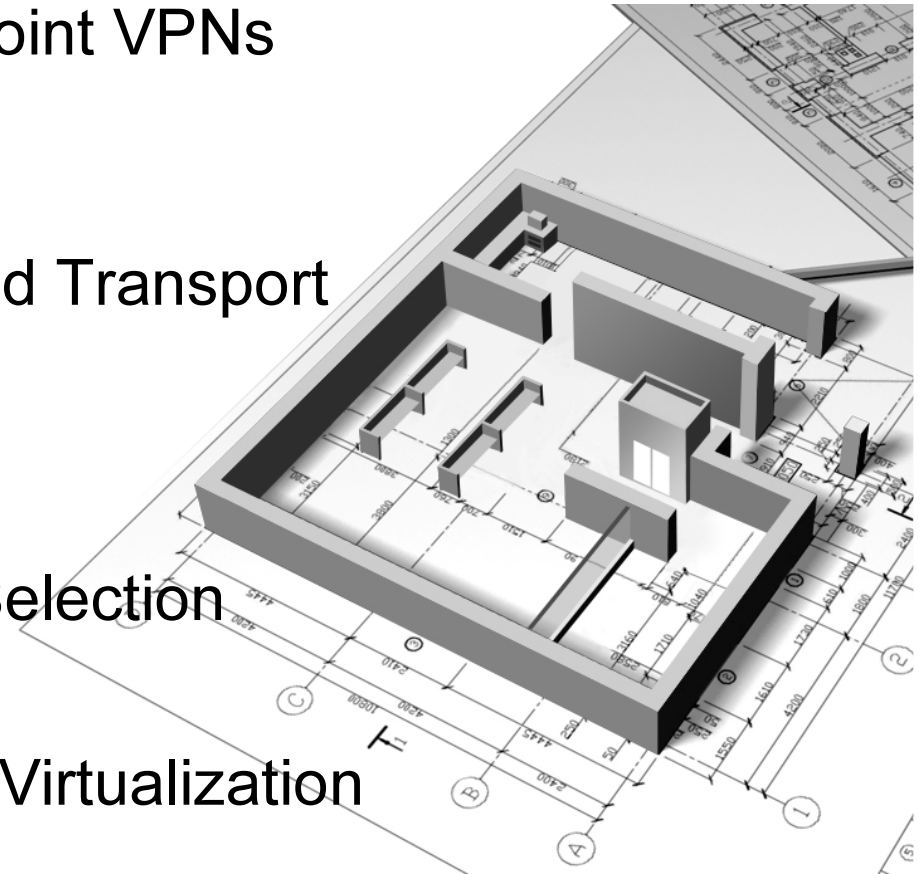
# DMVPN/GET VPN Design & Case Study



**Stephen Lynn**  
**Consulting Systems Engineer**  
**CCIE 5507**

# Agenda

- Overview of Dynamic Multipoint VPNs (DMVPN)
- Overview of Group Encrypted Transport VPNs (GET VPN)
- DMVPN/GET VPN Design Selection
- DMVPN/GET VPN Network Virtualization Case Study



# Session Objectives

At the end of the session, the participants should be able to:

- Understand DMVPN and GETVPN technology and describe the differences
- Understand solution positioning and select the best technology based on business requirements
- Design a network using DMVPN or GET VPN to provide network virtualization and separation

# DMVPN Overview



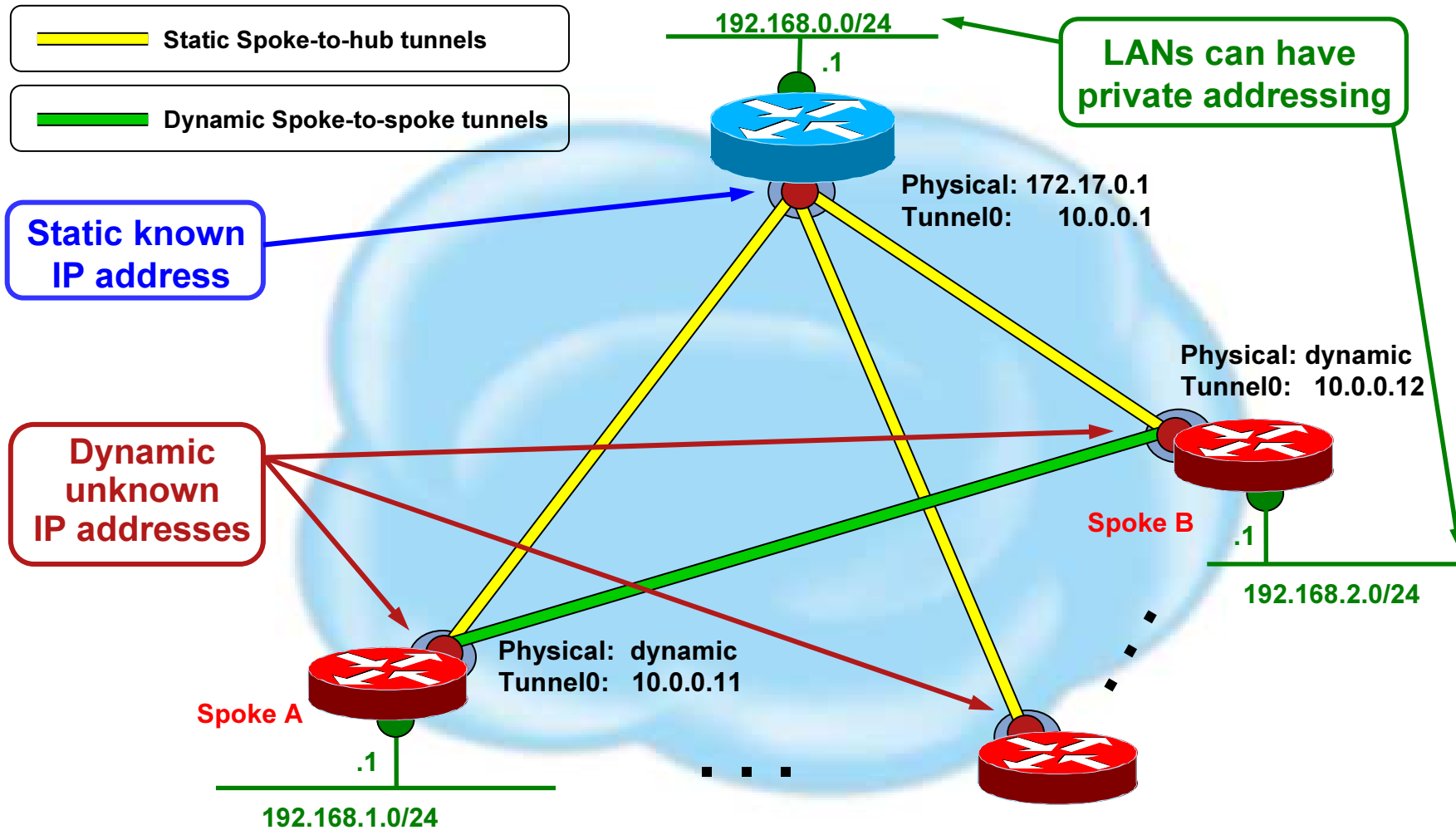
# What is Dynamic Multipoint VPN ?

- 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 (NHRP) mapping database of all the spoke's tunnel to real (public interface) addresses
  - Multipoint GRE Tunnel Interface
    - Single GRE interface to support multiple GRE/IPsec tunnels
    - Simplifies size and complexity of configuration

## DMVPN – How it works

- 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 Multipoint VPN—Example

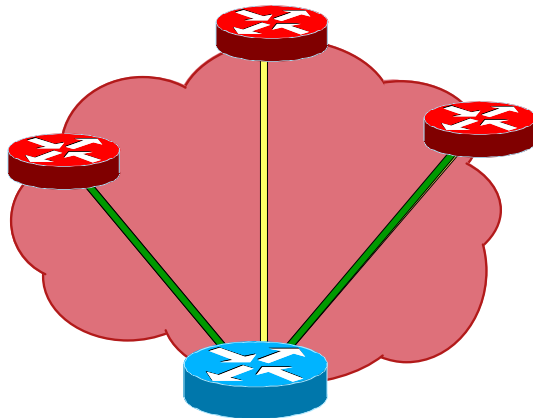


# Dynamic Multipoint VPN (DMVPN)

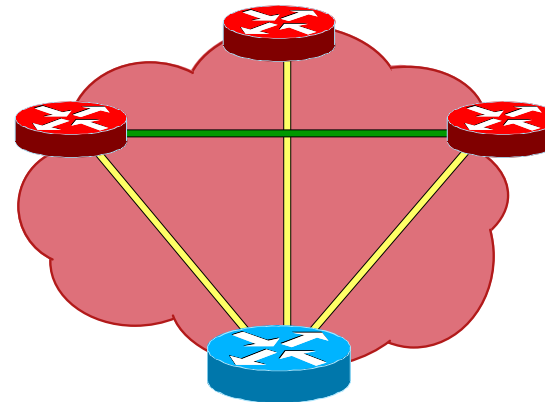
## Major Features

- Configuration reduction and no-touch deployment
- IP unicast, IP multicast and dynamic routing protocols
- Spokes with dynamically assigned addresses
- NAT – 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
- VRFs – GRE tunnels and/or data packets in VRFs
- 2547oDMVPN – MPLS switching over tunnels
- QoS – Aggregate; Static/Manual per-tunnel
- Transparent to most data packet level features
- Wide variety of network designs and options

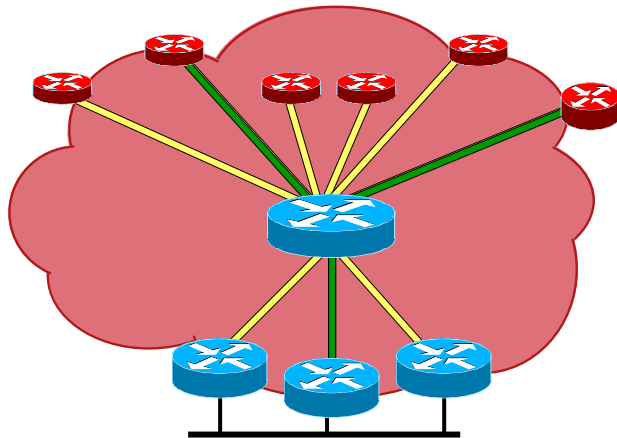
# Network Designs



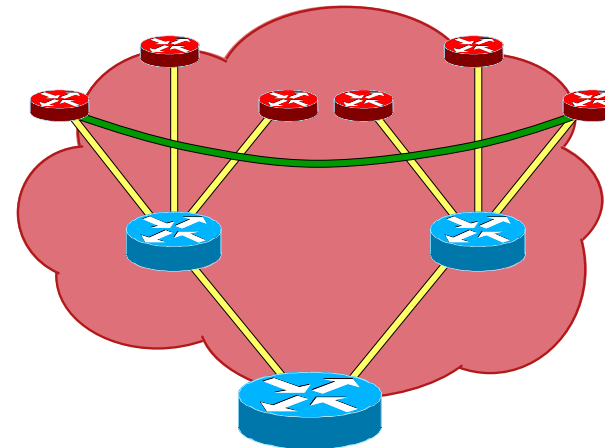
**Hub-and-spoke**



**Spoke-to-spoke (Phase 2)**



**Server Load Balancing**



**Hierarchical (Phase 3)**

# DMVPN Network Designs

- Hub-and-spoke

Spoke-to-spoke traffic via hub, Tunnels =  $O(n)$

**Phase 1:** Hub bandwidth and CPU limit VPN

**SLB:** Many “identical” hubs increase CPU power

- Spoke-to-spoke – Dynamic spoke-to-spoke tunnels

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

**Phase 2:** Single Hub-and-Spoke layer

**Phase 3:** Hierarchical Hub-and-Spoke layers

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.

Number of tunnels  $> O(n)$ ,  $\ll O(n^2)$  (full-mesh)

# Network Designs

## Common Requirements

- **Small/Medium Business**

  - DMVPN Phase 3 single layer design

  - Dial backup and VRF for non-split-tunneling

  - Up to 1000 spokes, with dynamic spoke-spoke tunnels.

- **Larger Business**

  - DMVPN Phase 3 hierarchical layer design

  - Dial backup, multiple ISP connections, VRF for non-split-tunneling and group separation.

  - 1000-2000 spokes, with dynamic spoke-spoke tunnels.

- **Home Office - Work Access**

  - ECT (Enterprise Class Teleworker) designs

  - DMVPN Phase 3 single layer design

  - 1000s of spokes

# Network Designs

## Common Requirements (cont.)

- Point-of-Sale / ATM

  - Server Load Balancing (SLB) designs – Super Hub

  - No spoke-spoke (designs now available to enable spoke-spoke)

  - 4000 – 20000+ spokes.

- Extranet

  - DMVPN Phase 1 Hub-and-spoke design

  - No spoke-spoke not even via the Hub – (using ACLs)

  - Probably <1000 spokes.

- ISP

  - DMVPN Phase 3 or SMB designs, MPLS (2547oDMVPN), VRFs

  - Hub-and-spoke and spoke-spoke networks.

  - Different size networks (# of spokes), but also supporting many DMVPN networks on the same set of hub routers.

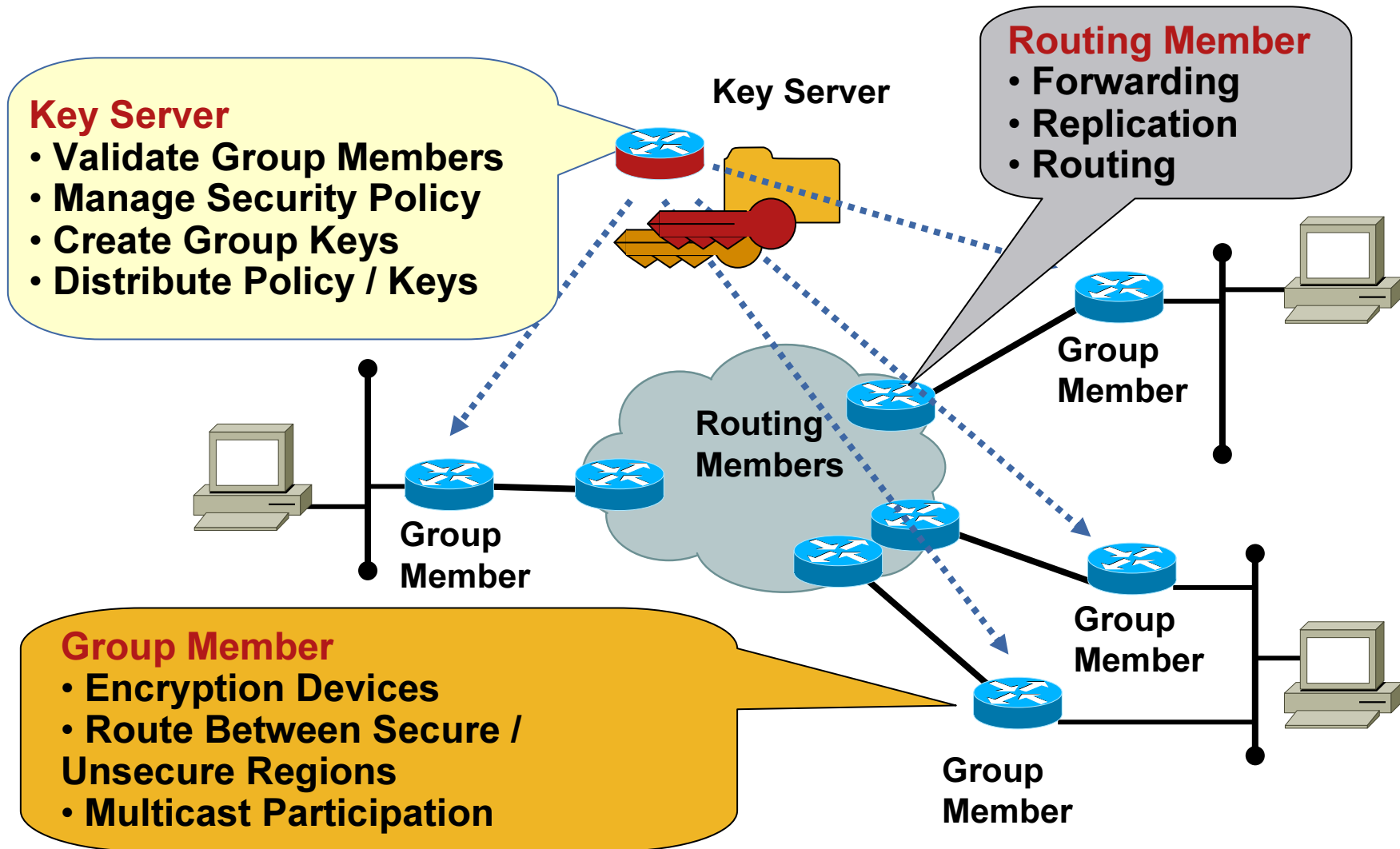
# GET VPN Overview



# What is Group Encrypted Transport VPN ? (GET VPN)

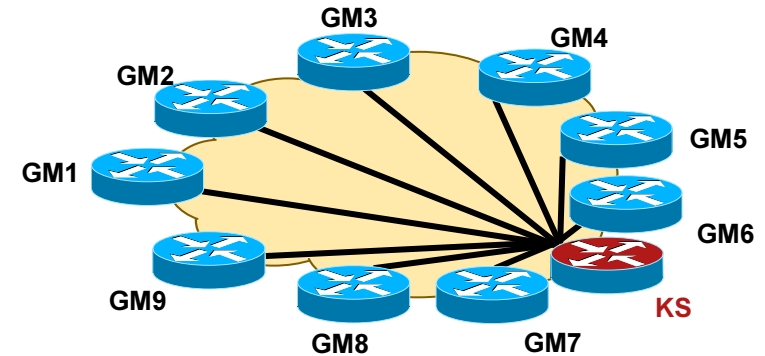
- GET VPN is a group key based tunnel-less VPN solution for the enterprise network using private MPLS/IP core
- Enables secure end-to-end fully meshed network, for Data, Voice, Video, IP Multicast and other applications, without the use of point-to-point VPN tunnels.
- Relies on Open standard technologies
  - Group Domain Of Interpretation (GDOI)
    - RFC 3547
    - Provides cryptographic keys and policies to a group of VPN gateway that share the same security policies
  - IPSec encryptions
    - Supports 3DES, AES128/192/256 algorithms

# GET VPN Components

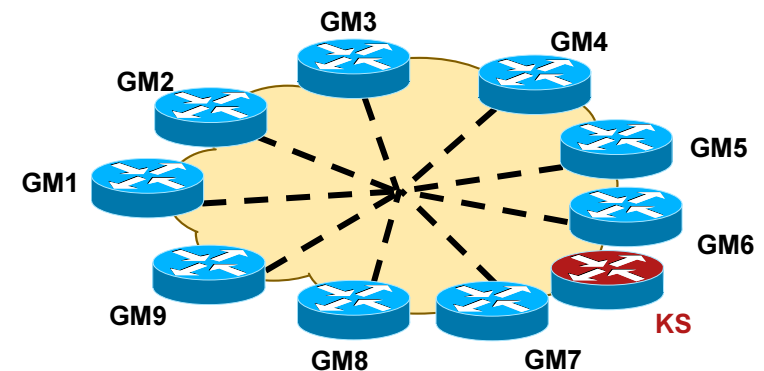


# GETVPN - How Does it Work

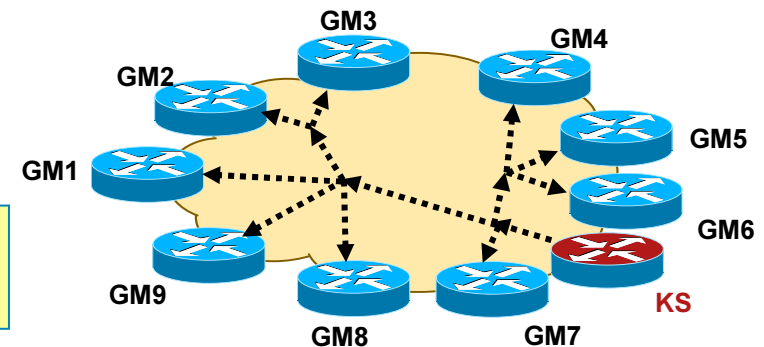
- **Step 1:** Group Members (GM) “register” via GDOI (**IKE**) with the Key Server (KS)  
KS authenticates & authorizes the GM  
KS returns a set of IPsec SAs for the GM to use



- **Step 2:** Data Plane Encryption  
GM exchange encrypted traffic using the group keys  
The traffic uses **IPSEC** Tunnel Mode with “address preservation”



- **Step 3:** Periodic Rekey of Keys  
KS pushes out replacement IPsec keys before current IPsec keys expire. This is called a “rekey”



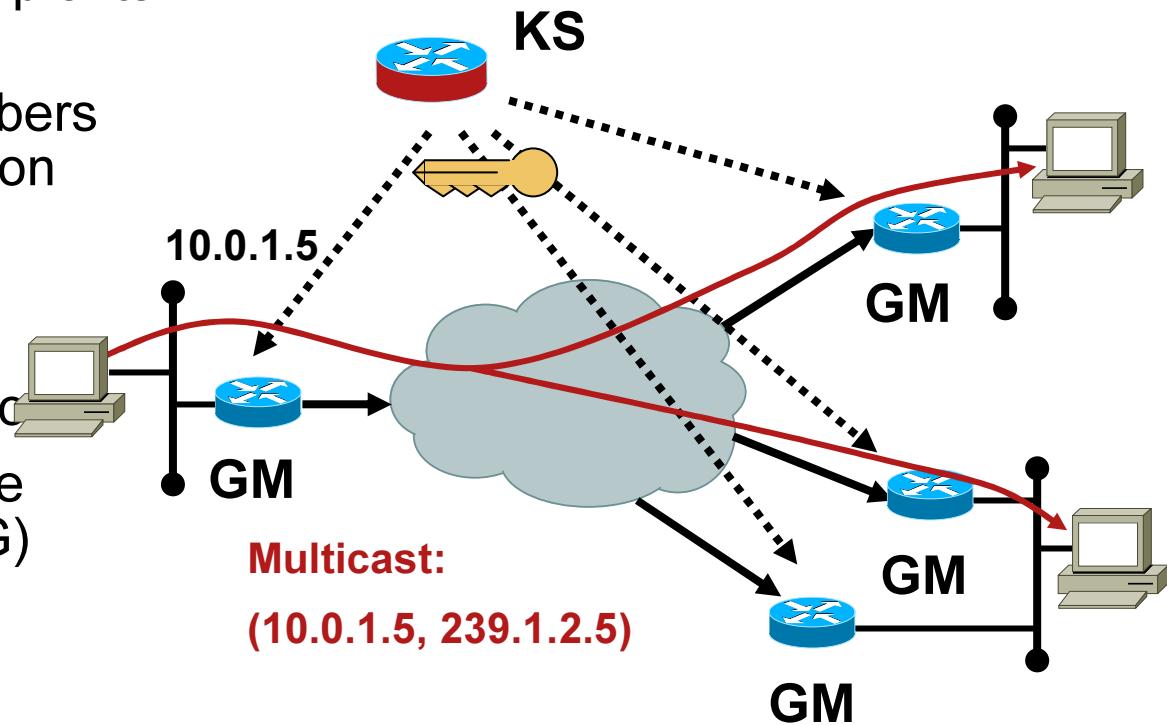
Once you have been admitted to the group, you can communicate freely with any/all group members.

# Group Security Association

- Group Members share a security association
  - Security association is not to a specific group member
  - Security association is with a set of group members
- Safe when VPN gateways are working together to protect the same traffic
  - The VPN gateways are trusted in the same way
  - Traffic can flow between any of the VPN gateways
- Each group supports up to 100 ACL permit entries that define interesting traffic for encryption
  - Each permit entries results in a pair of Security Associations
  - Maximum IPsec SAs in a group cannot exceeds 200

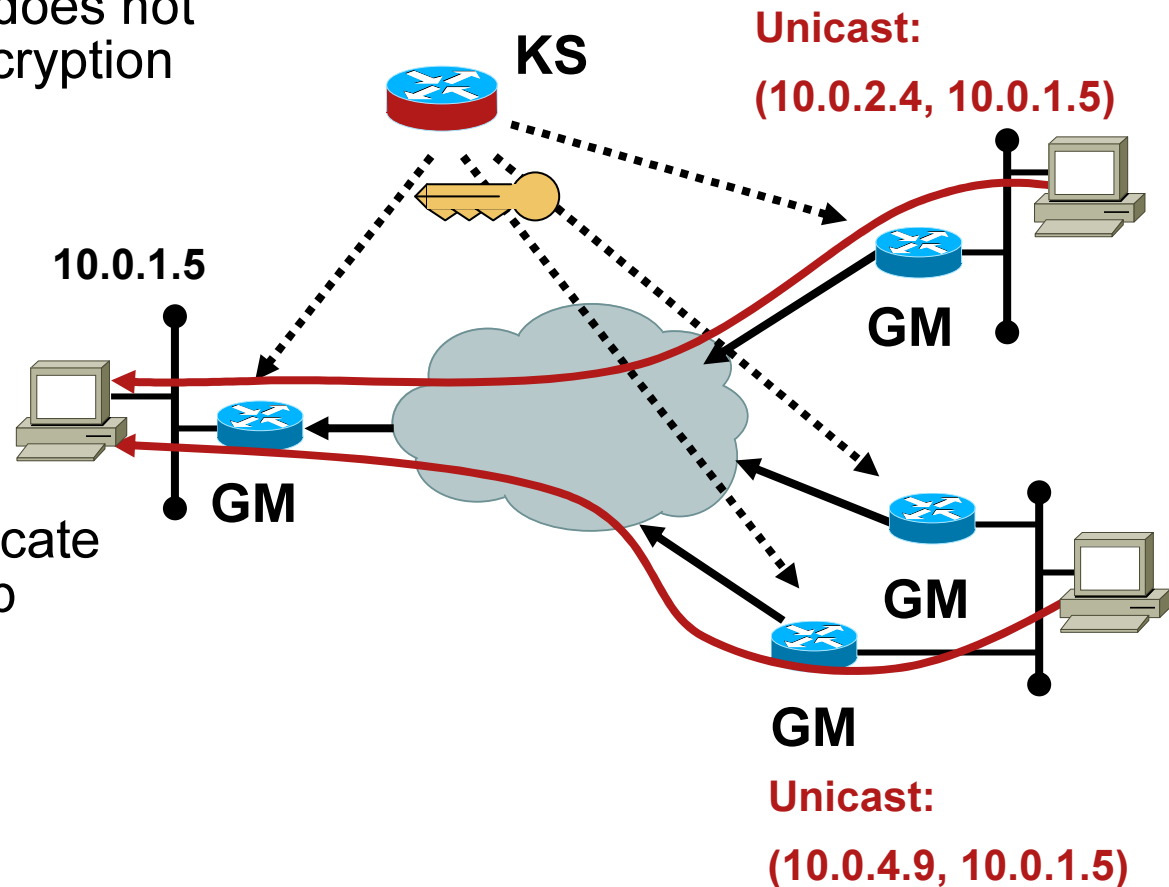
# Secure Data Plane Multicast

- **Premise:** Sender does not know the potential recipients
- Sender assumes that legitimate group members obtain Traffic Encryption Key from key server for the group
- Encrypt Multicast with IP Address Preservation
- Replication In the Core based on original (S,G)

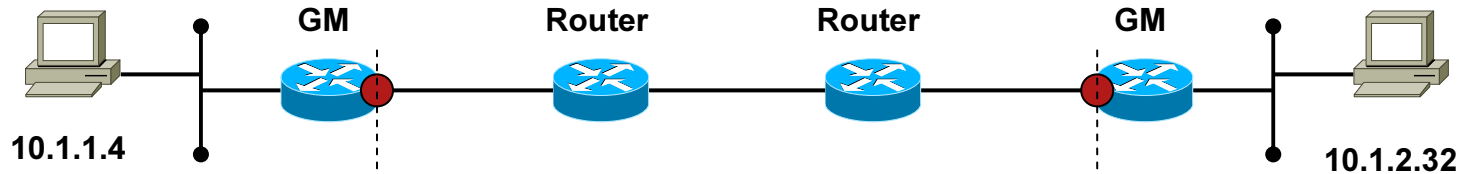


# Corollary: Secure Data Plane Unicast

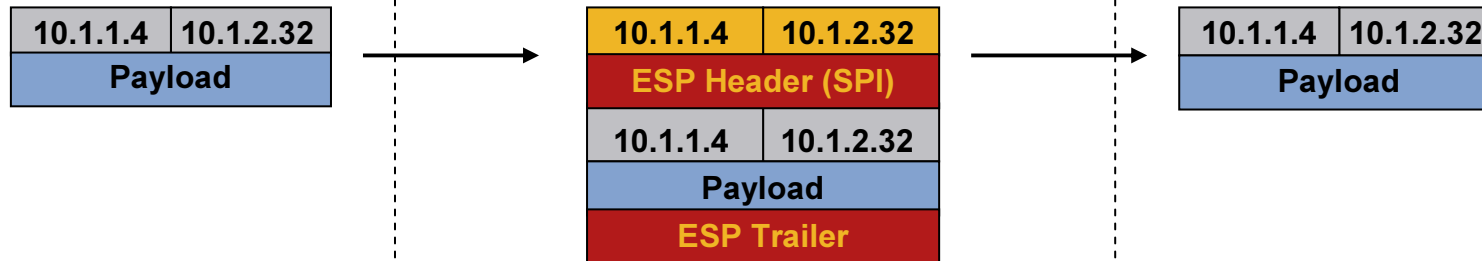
- **Premise:** Receiver advertises destination prefix but does not know the potential encryption sources
- Receiver assumes that legitimate group members obtain Traffic Encryption Key from key server for the group
- Receiver can authenticate the group membership



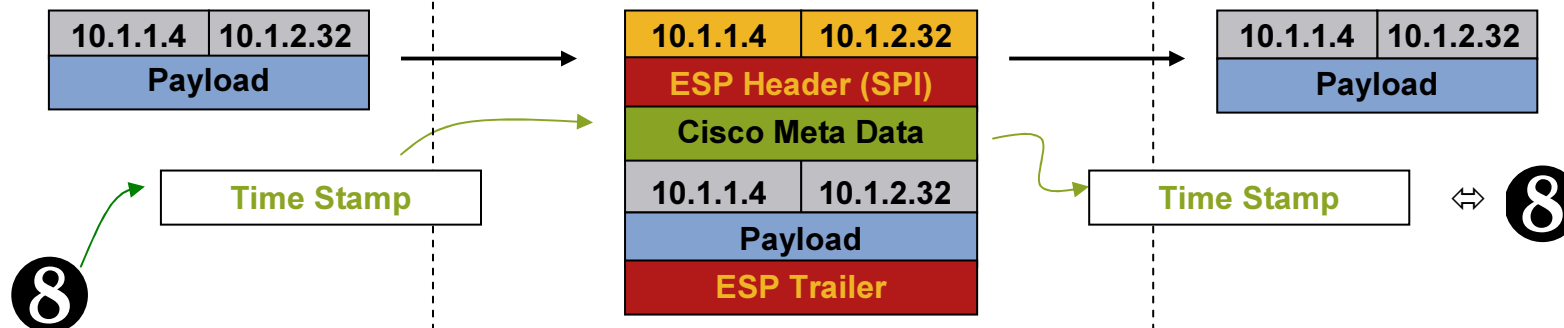
# Group Encrypted Transport (Data Plane)



## Encapsulation without Time-Based Anti-Replay



## Encapsulation with Time-based Anti-Replay



# Group Policy Distribution

- Group Keys

  - Key Encryption Keys (Default Lifetime of 24 hours)

  - Traffic Encryption Keys (Default Lifetime of 1 hour)

- Key Distribution Methods

  - Unicast

    - Infrastructure Capable of Unicast Only

    - Requirement for Rekey Acknowledgement

    - Requirement for per GM rekey control

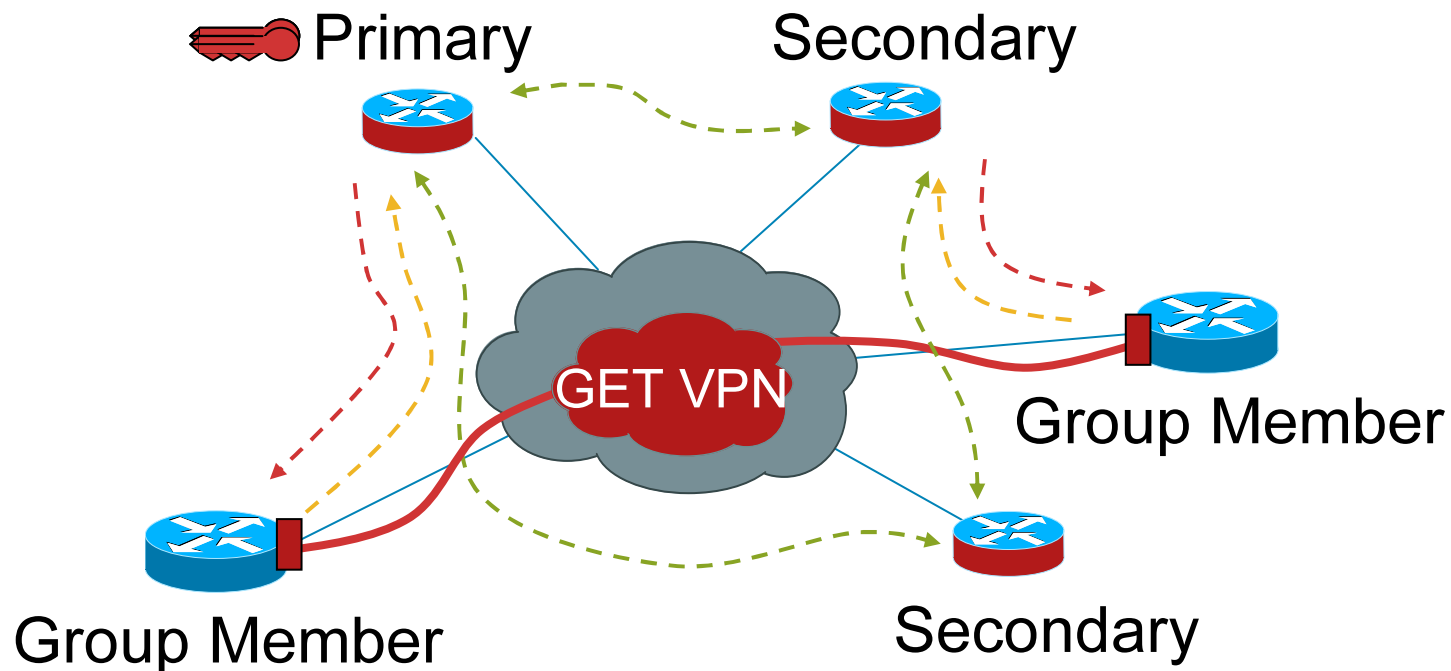
  - Multicast

    - Infrastructure Capable of Multicast

    - Requirement for more Scalable Key and Policy Distribution

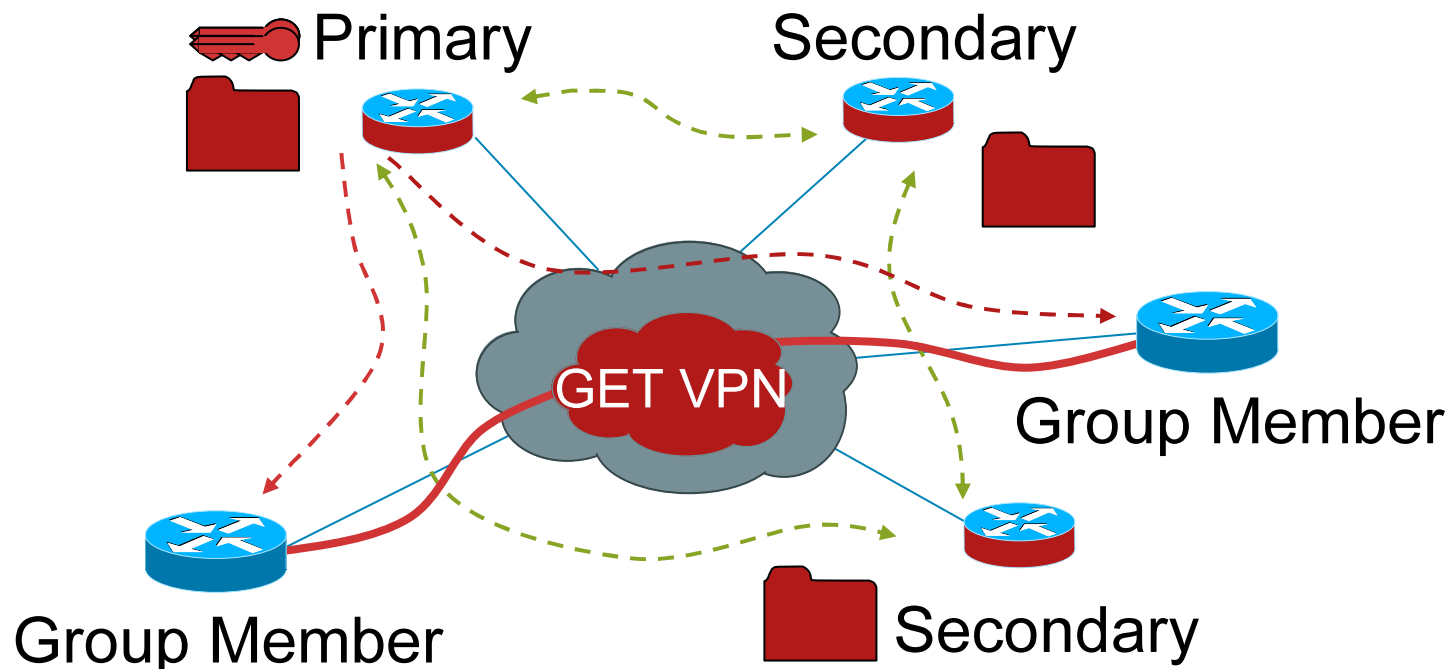
# Cooperative Key Server: Roles

- A Key Server is Elected Primary, Creates Keys, and Distributes Keys
- Group Members Complete Registration to an available Key Server and Receive Policy and Keys



# Cooperative Key Server: Primary Processes

- Primary Key Server Generates new Keys on a Periodic Basis
- Primary Checks Consistency of Policies and Coordinates Group Member List with Secondary KS
- Primary Distributes Keys to Secondary KS and Group Members
- Primary Notifies Secondary of Primary Presence



# Benefits of GET VPN

Previous Limitations	New Feature and Associated Benefits
<p>Multicast traffic encryption was supported through IPsec tunnels:</p> <ul style="list-style-type: none"><li>– Not scalable</li><li>– Difficult to troubleshoot</li></ul>	<p>Encryption supported for Native Multicast and Unicast traffic with Group Security Association</p> <ul style="list-style-type: none"><li>– Allows higher scalability</li><li>– Simplifies Troubleshooting</li><li>– Extensible standards-based framework</li></ul>
<p>Overlay VPN Network</p> <ul style="list-style-type: none"><li>– Overlay Routing</li><li>– Sub-optimal Multicast replication</li><li>– Lack of Virtualized QoS</li><li>– Peer Mesh of IPsec States</li></ul>	<p>No Overlay</p> <ul style="list-style-type: none"><li>– Leverages Core network for Multicast replication via IP Header Preservation</li><li>– Optimal Routing introduced in VPN</li><li>– Standard QoS for encrypted traffic</li><li>– Global Distributed IPsec State</li></ul>
<p>Full Mesh Connectivity</p> <ul style="list-style-type: none"><li>– H and S primary support</li><li>– S to S not scalable</li></ul>	<p>Any to Any Instant Enterprise Connectivity</p> <ul style="list-style-type: none"><li>– Leverages core for instant communication</li><li>– Optimal for Voice over VPN deployments</li></ul>

# Design Selection



# Design Selection Challenge

**Wide variety of platforms and encryption modules to choose for the Hub**

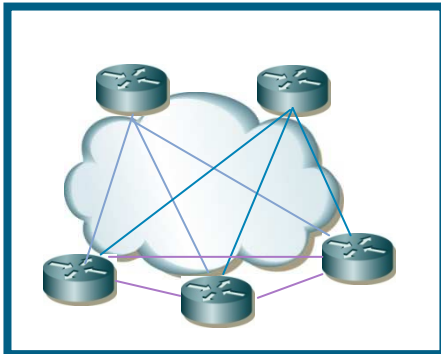
**Certain platforms or IOS trains do not support all the features**

**Routing protocol characteristics and scalability is different**

**More than one design can satisfy a given set of requirements**

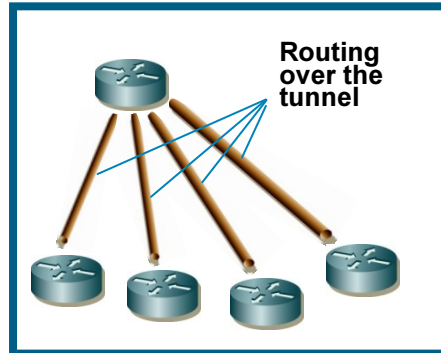
**Addition of certain features change the design or topology e.g. multicast**

# DMVPN Solution – Common Design Selection Criterion



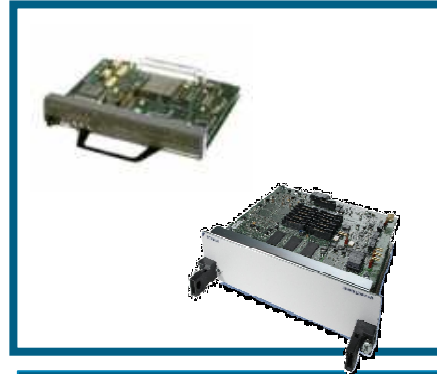
## Topology?

Hub & Spoke or  
Spoke to Spoke



## Routing Protocol choice?

EIGRP, OSPF,  
BGP, RIP



## Encryption Throughput?

VAM2+, VSA,  
SPA



## Fine tune

Modify design  
based on  
platform and IOS

**Step 1:** Select  
topology based on  
requirement

**Step 2:** Select RP  
based on scalability  
requirements OR  
scale design based  
on selected RP

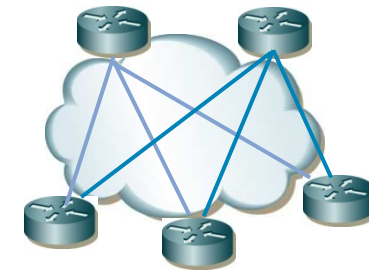
**Step 3:** Select  
platform and/or  
encryption card based  
on throughput  
requirements

**Step 4:** Adjust DMVPN  
phase or topology  
based on IOS,  
platform or traffic  
requirements

# Step 1 – Select Topology

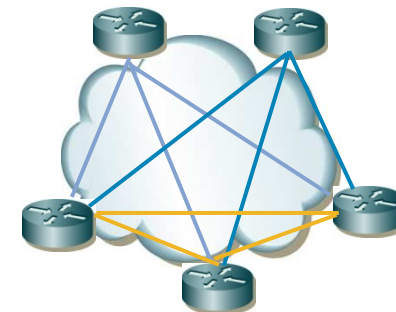
## Resilient Hub and Spoke

All the features of basic hub and spoke design apply  
Spokes connect to two or more hubs for resiliency  
Based on routing, traffic can be distributed to both hubs OR  
can always be sent to a primary hub

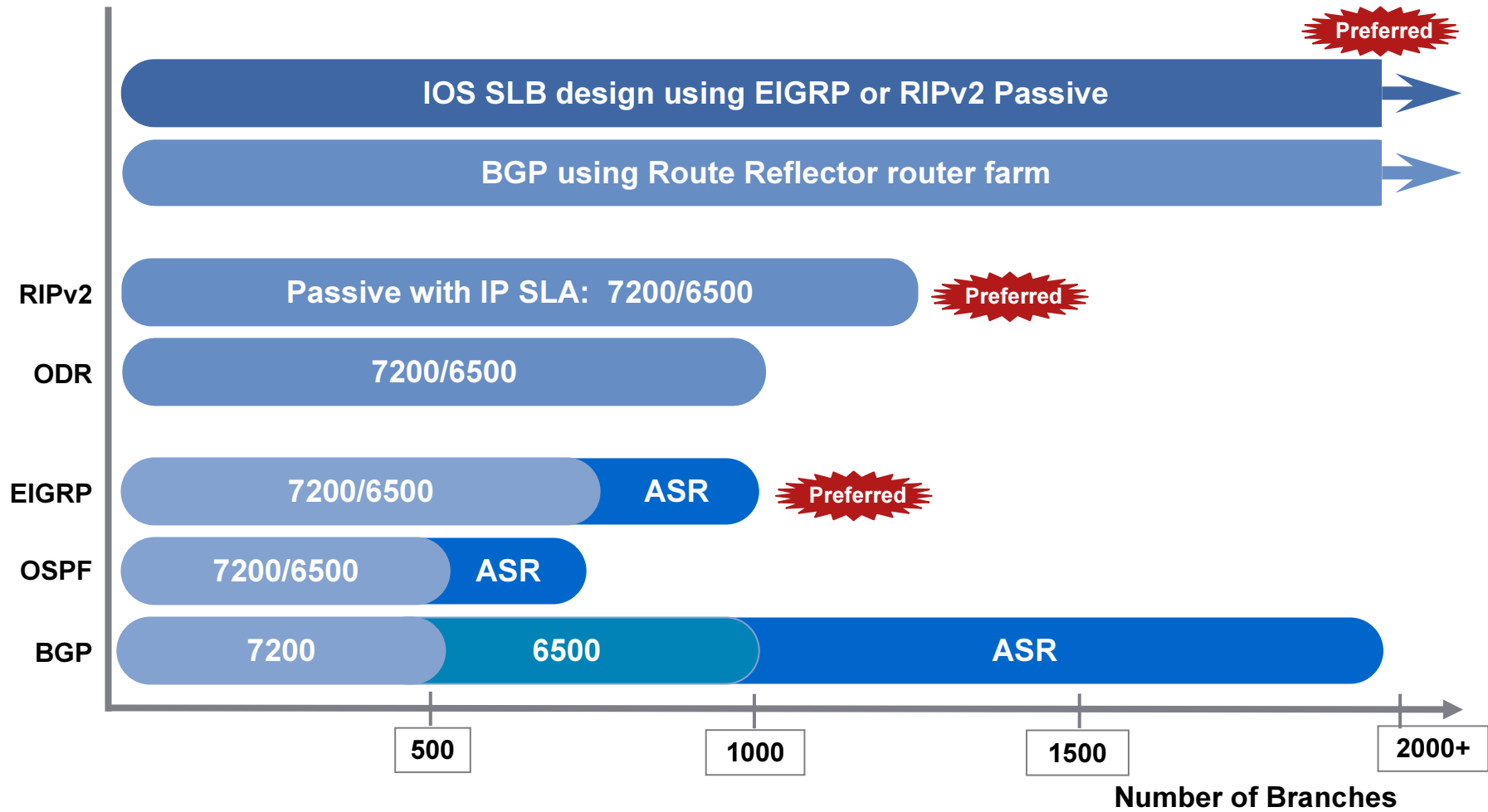


## Resilient Spoke to Spoke

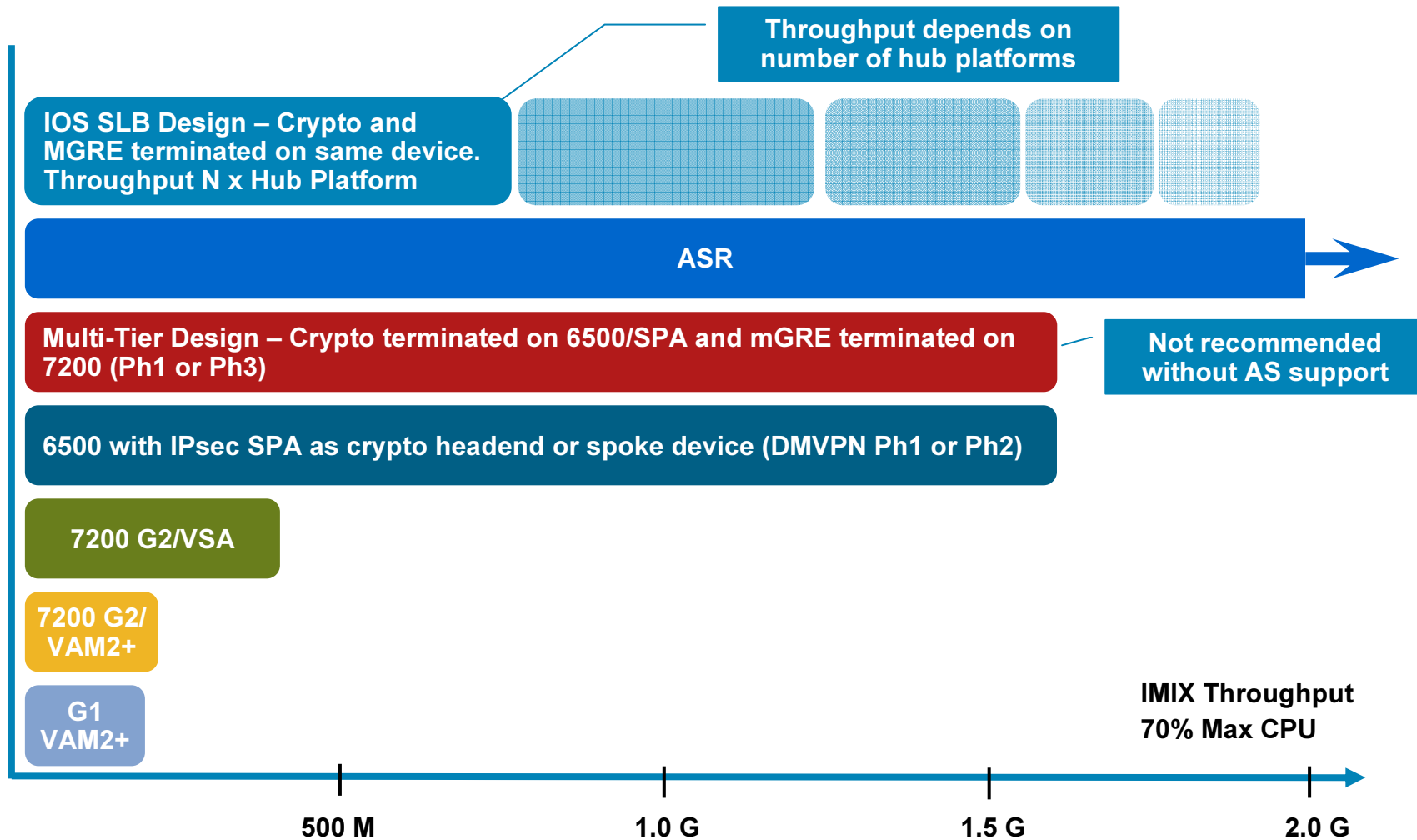
All the features of basic spoke to spoke design apply  
Spokes connect to two or more hubs for resiliency  
Based on routing and/or NHRP configurations, traffic can be  
distributed over both hubs



# Step 2 – Select a Routing Protocol based on Scalability requirements



# Step 3 – Select Platform and Encryption Module



# Step 4 – Final Design Adjustment

Hub and Spoke design works the same in mainline or T train. Select a stable well tested release. Spoke to spoke traffic (if allowed) will traverse the hub

Spoke to spoke design works differently depending on train and platform

12.4 M, pre 12.4(6)T, 12.2(33)SXH, ASR (Rel. 2) or later  
7200/ISR, 6500, ASR1000 as a hub or spoke

## DMVPN Phase 2

Hubs need to be daisy chained

Can not summarize routes

Next hop must be unchanged

OSPF can not support more than two hubs

12.4(6)T or later

7200/ISR (or 6500 use for crypto offloading device)

## DMVPN Phase 3

No daisy chain required

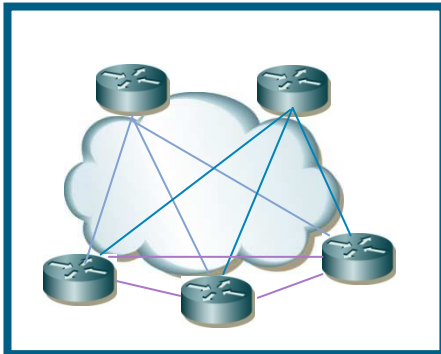
Route summarization possible

NHRP Redirect and shortcut

Hierarchical designs for better scalability

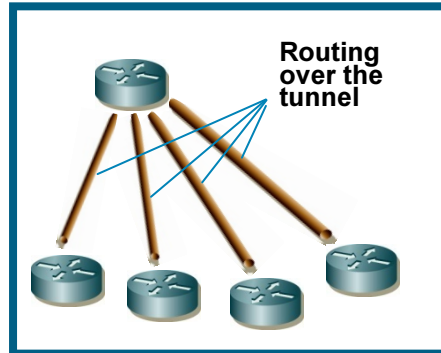
**Preferred**

# GETVPN Solution – Common Design Selection Criterion



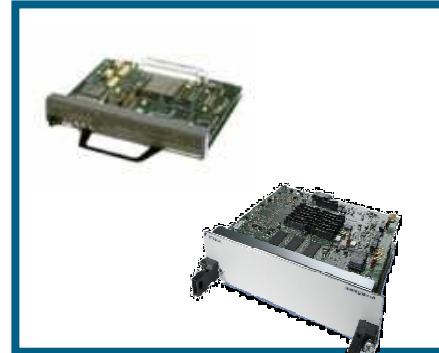
## Policy?

Inclusive or Exclusive



## Scalability?

Rekey Method, KS Architecture



## Encryption Throughput?

VAM2+, VSA, SPA



## Fine tune

Policy Management and Reliability

**Step 1:** Determine the security policy of traffic that needs encryption and scope of the VPN

**Step 2:** Based on scale requirements, select KS platform, KS architecture for control plane

**Step 3:** Select GM platform and/or encryption card based on throughput requirements

**Step 4:** Adjust policy for control and management plane. Optimize timers for convergence

# Step 1 – Select Policy Model and Scope

## Inclusive

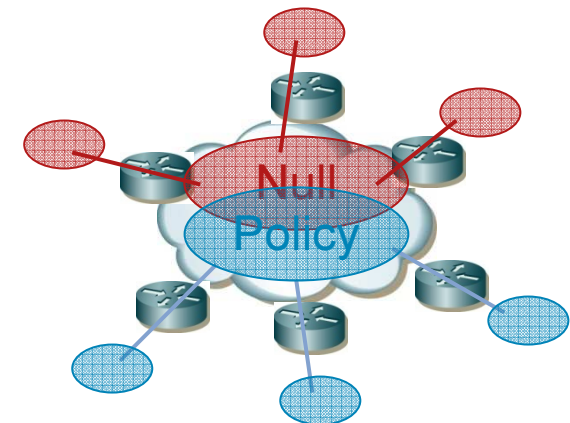
Preferred

- Policy encrypts all traffic by default
- Exceptions defined for control plane and management
- Exceptions defined out-of-scope VPN segments
- Transition plan defined for eliminating exceptions



## Exclusive

- Policy encrypts specific ranges of subnets
- Exceptions defined for specific applications and subnets
- Transition plan defined for in-scope VPN segment inclusion



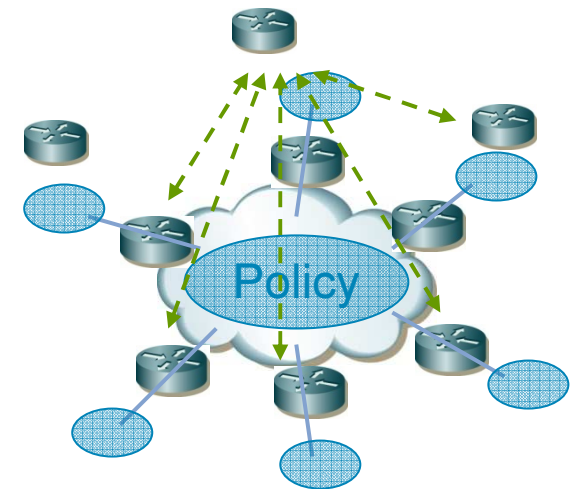
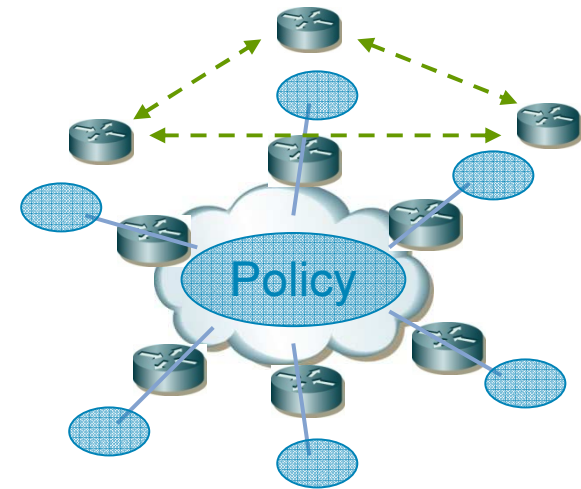
# Step 2 – System Scalability

## Key Server Rekey Management

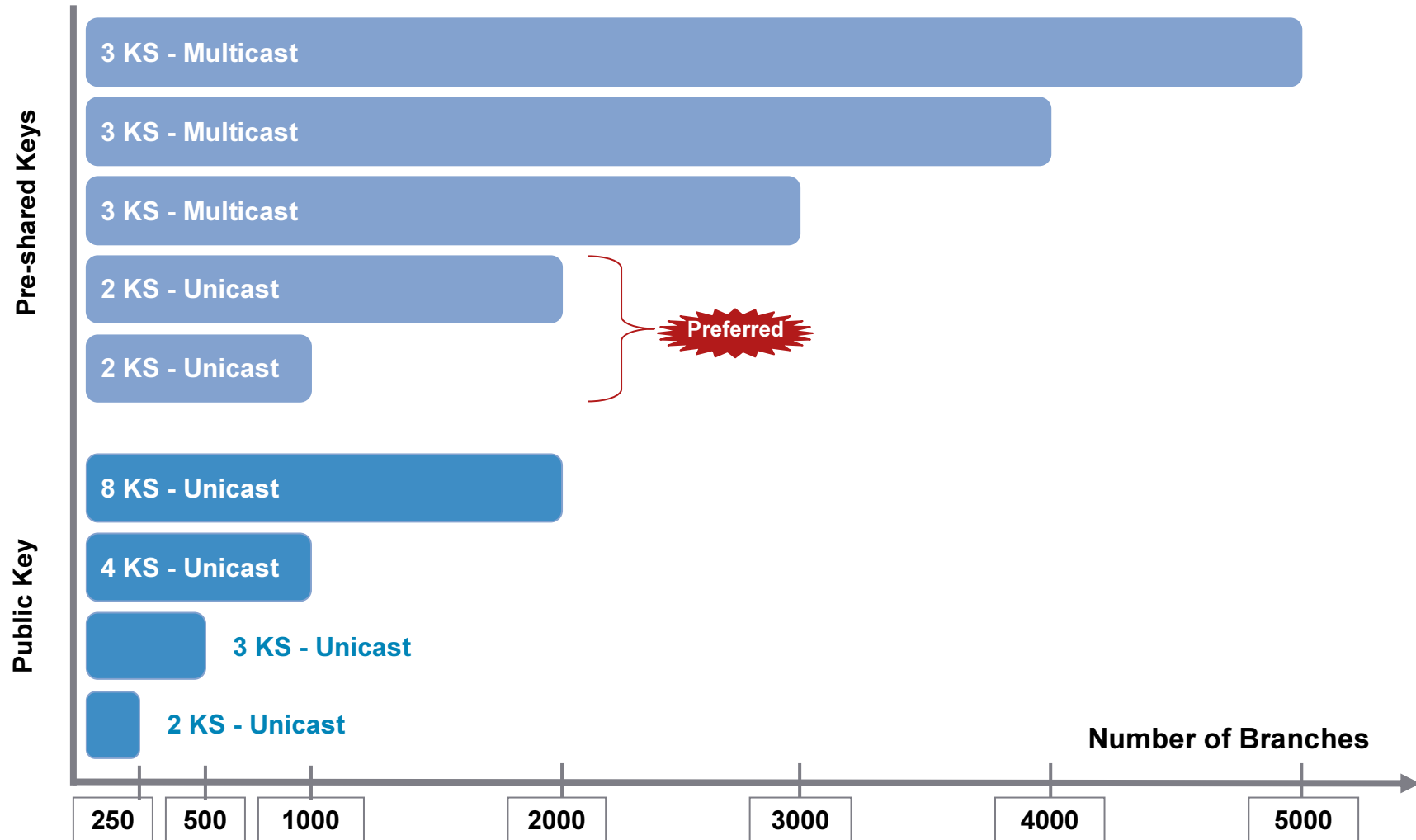
- Determine if multicast rekey is required (> 2000 GM)
- Determine if VPN has multicast enabled
- Assess routing convergence intervals

## Key Server Architecture

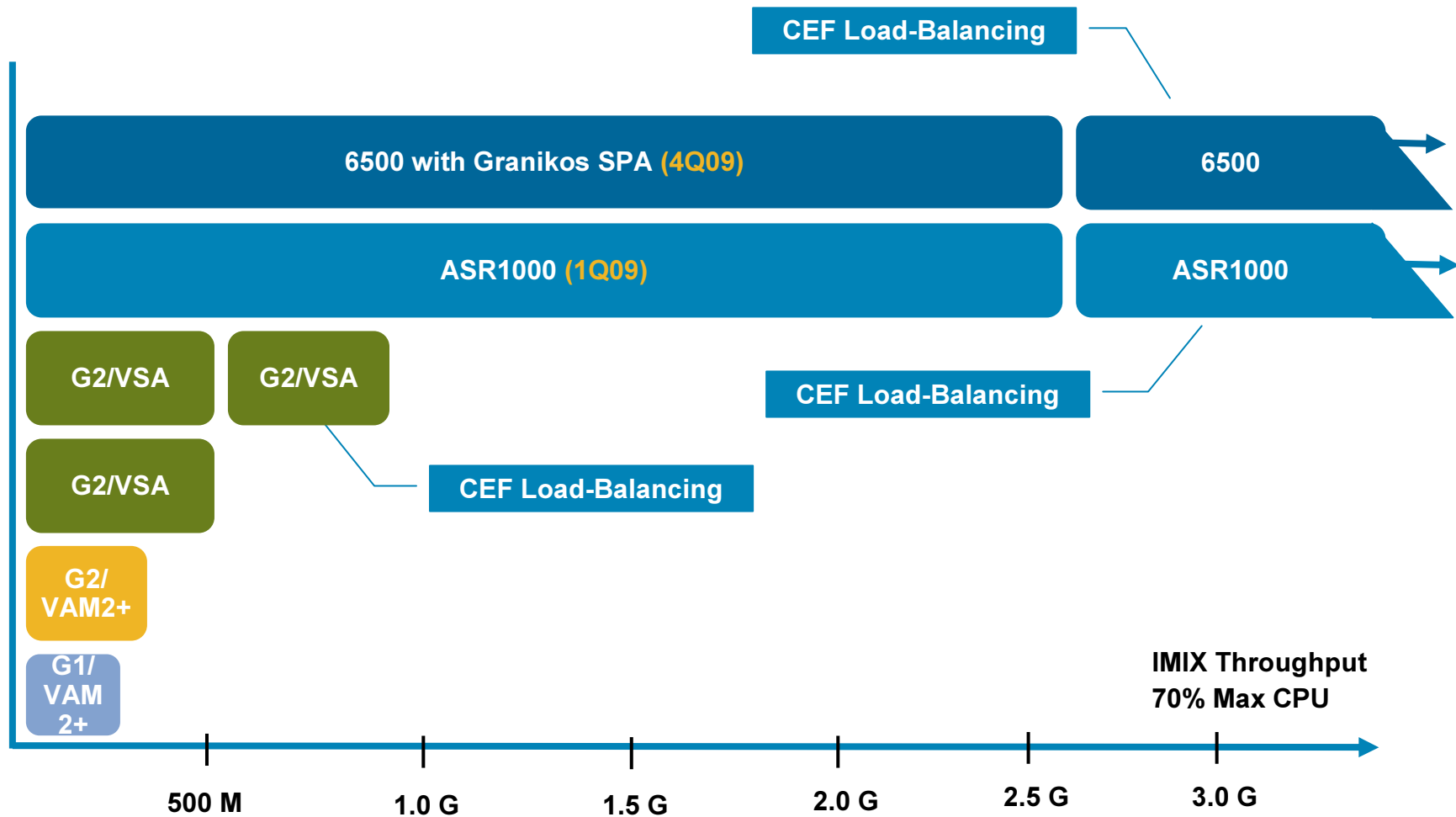
- Determine number of KS require based on GM number
- Determine control plane topology (PIM-SM, -Anycast, -SSM)
- Determine policy exceptions for KS control plane



## Step 2 – System Scalability (Example 7200)



# Step 3 – Select Platform and Encryption Module



# Step 4 – Final Design Adjustment

## -Adjust Policy to facilitate:

- Management plane access (HTTPS, TFTP, SNMP, SSH, TACACS, etc.)
- Sustain control plane (BGP/IGP, PIM, GDOI, IKE, etc.)

## Adjust timers to optimize availability:

- COOP Protocol for KS Convergence
- Rekey Timers for Routing Convergence

**IOS Current Release: 12.4(22)T**

### **GET VPN**

- Phase 1.0 - Originally released in 12.4(11)T
- Phase 1.2 – Planned release in pi12

**ION and XE Planned Releases**

### **GET VPN**

- 6500 Projected release in ION Arrowhead  
-Phase 1.2 (GM Only)
- ASR Projected release in IOS XE RLS 3  
-Phase 1.2 (GM Only)

# DMVPN/GET VPN Network Virtualization Case Study



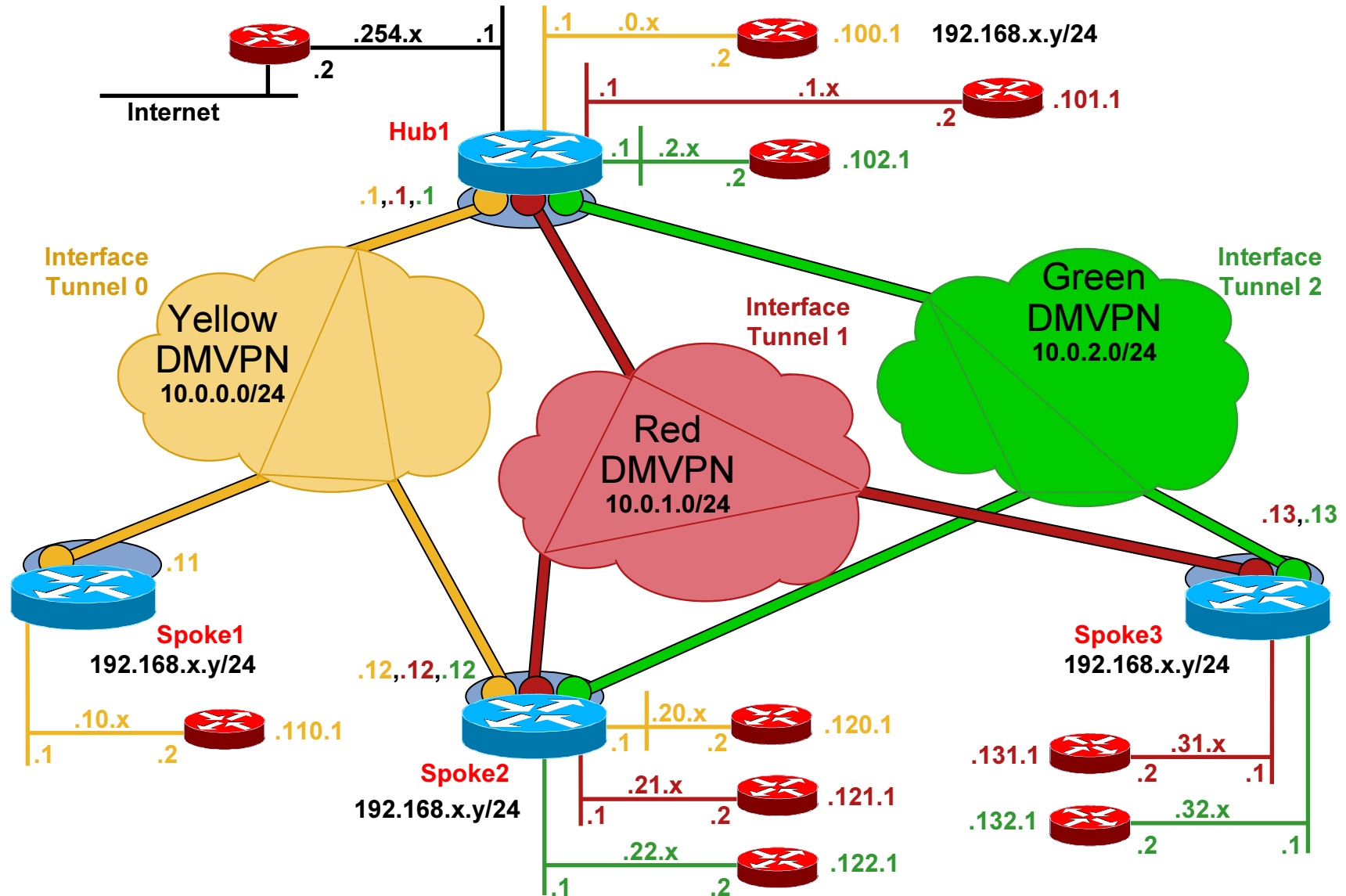
# Business Requirements

- Three Business Units (BU)
  - Sites have one or more BUs
- No security policy within business unit
- Security polices will be applied to inter-BU traffic
- Data must be encrypted when passing through SP network
- Hub access must have high availability
  - Hub services all BUs
- **Optional, multicast traffic over the VPN network**
- **Optional, no disclosure of local addresses to SP**

## 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

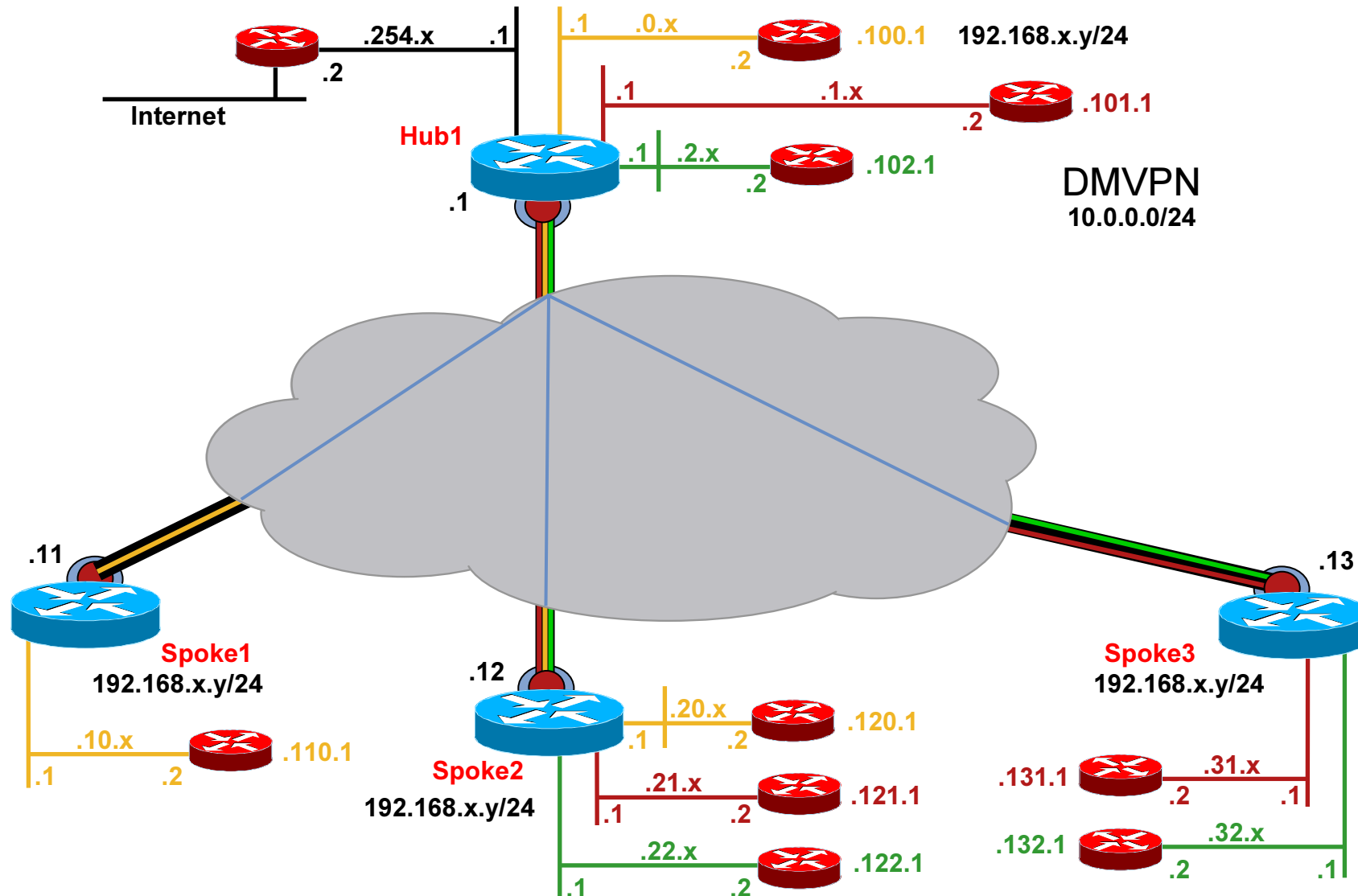


# MPLS over DMVPN – 2547oDMVPN

- 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



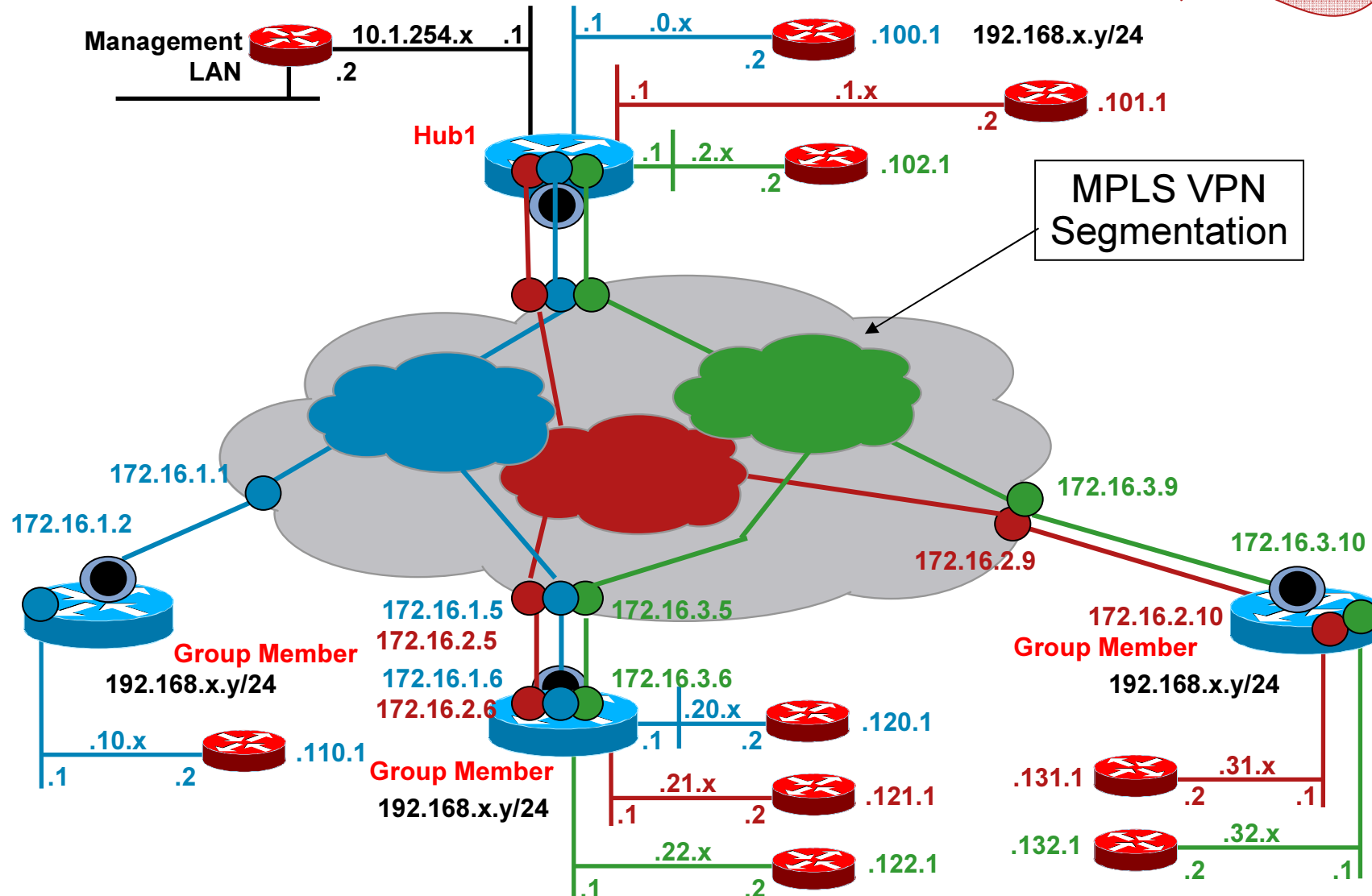
# GET VPN Fundamentals

- Departmental Segmentation Requires:
  - Route Segmentation (aka VRF)
  - Data Plane Segmentation (e.g. Tunnel, Circuit, Switched Path)
  - Control Plane Segmentation (e.g. virtual routing adjacency)
- GET VPN Does Not Create the VPN – it secures the VPN
  - Departmental Segmentation must be accomplished using tunnels (e.g. GRE, L2TPv3, LSP, etc.)
  - GET does not tunnel traffic; therefore, the addresses are exposed
- GET VPN can secure a departmental segment
  - GET can encrypt IP tunnels
  - GET can encrypt traffic forwarded into tunnels

# GETVPN

## Segmented Encrypted Traffic

Option 1A



# Virtualization Decision Matrix: Selection of DMVPN or GETVPN

	Any-to-any Persistence	Secure VPN Partitioning	Mask VPN IP Addresses	Segment Creation By Customer	Scalability Of Routing Adjacency	Efficient Multicast Distribution
Separate DMVPN Clouds	Yellow	Green	Green	Green	Red	Yellow
MPLS VPN Over DMVPN	Red	Green	Green	Green	Yellow	Red
MPLS VPN Segments	Green	Green	Red	Red	Green	Green
Policy Segmented Shared MPLS VPN	Green	Yellow	Red	Yellow	Green	Green
MPLS VPN Over GET Encrypted GRE Tunnels	Yellow	Green	Green	Yellow	Yellow	Yellow
Tunneled GET Encrypted VPN Segments	Red	Green	Green	Yellow	Red	Yellow

# Key Takeaways

The Key Takeaways of this presentation are:

- Positioning

  - DMVPN generally recommended for over Public Networks

  - GET VPN Generally recommended for over Private Networks

- Models

  - DMVPN creates a VPN and secures the VPN

  - GET VPN secures an existing VPN

- Virtualization

  - DMVPN uses multiple overlays or single overlay with MPLS VPN

  - GET VPN uses distinct polices or multiple overlays

# Additional Resources

- **GETVPN Design & Implementation Guide**

[http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6525/ps9370/ps7180/GETVPN\\_DIG\\_version\\_1\\_0\\_External.pdf](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6525/ps9370/ps7180/GETVPN_DIG_version_1_0_External.pdf)

- **DMVPN Design & Implementation Guide**

[http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN\\_and\\_MAN/DMVPNbk.pdf](http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/DMVPNbk.pdf)

