
LET'S
BUILD
TOMORROW
TODAY

DMVPN for R&S CCIE Candidates

Johnny Bass

CCIE #6458

BRKCCIE-3003

@CCIE6458

Cisco live!

About the Presenter

- Johnny Bass
- Networking industry since the late 1980s
- CCIE R&S #6458
- CCSI 97168
- Cisco 360 R&S Master Instructor
- Course director for several programs, including Cisco 360 Route Switch, for Global Knowledge

Why Are We Here?

- Show of hands, how many of you are currently supporting DMVPN?
- Show of hands, how many of you actually have configured DMVPN on a router?
- Show of hands, how many of you heard of DMVPN before it was on the v5.0 Blueprint?

DMVPN and the CCIE R&S Exam (V5.0)

4.1.4	Implement and Troubleshoot DMVPN (single hub)
4.1.4 a	NHRP
4.1.4 b	DMVPN with IPsec using preshared key
4.1.4 c	QoS Profile
4.1.4 d	Pre-classify

Agenda

- **Dynamic Multipoint VPN Review**
- How to Configure DMVPN without & with IPSec
- Support for IPv6 with DMVPN
- DMVPN advanced topics (CCIE twists)
- Troubleshooting
- Q&A

DMVPN History

- 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

DMVPN: Major Features

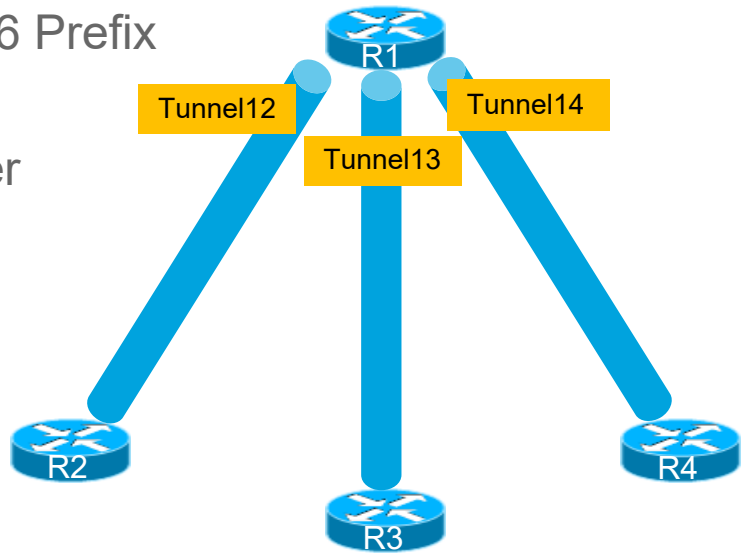
- Offers configuration reduction and no-touch deployment
- Supports IPv4/IPv6 Unicast, Multicast, and dynamic routing protocols
- Supports remote peers with dynamically assigned addresses
- Supports spoke routers behind dynamic NAT and hub routers behind static NAT
- Dynamic spoke-to-spoke tunnels for scaling partial- or
- full-mesh VPNs
- Usable with or without IPsec encryption

Configuration Reduction

- 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

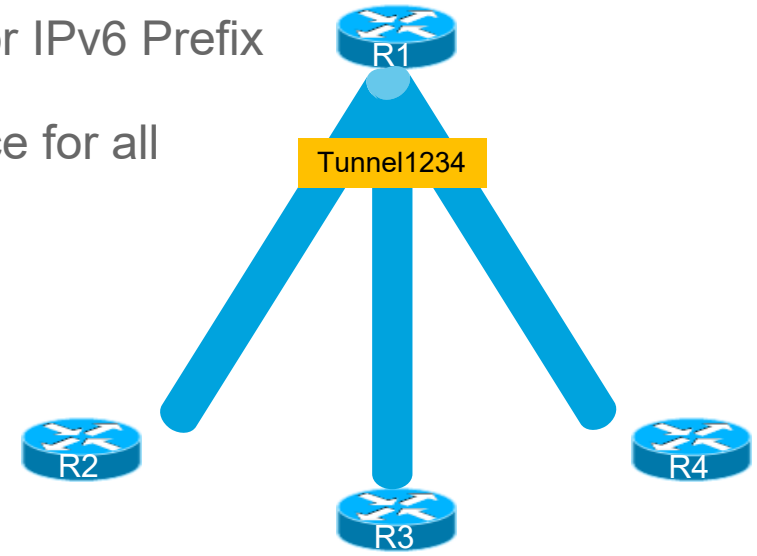
DMVPN Basics – GRE Tunnels

- IPv4 Subnet or IPv6 Prefix per spoke link
- Tunnel interface per spoke on the hub



DMVPN Basics – mGRE Tunnels

- One IPv4 Subnet or IPv6 Prefix for all spokes
  One tunnel interface for all spokes on the hub



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

Dynamic Addressing

- Spokes have a persistent dynamic 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.

DMVPN Components: NHRP

- NHRP is a layer two resolution protocol and cache like ARP or Inverse ARP (Frame Relay)
- It is used in DMVPN to map a tunnel IP address to an NBMA address
- NHRP registration
  - Spoke dynamically registers its mapping with NHRP Server (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

DMVPN Phase 1

- DMVPN Phase 1 network, tunnel interfaces are not symmetrically configured
- All communications are going via the hub router.
- Spoke routers cannot communicate directly to each other.

DMVPN Phase 2

- DMVPN Phase 2 network, tunnel interfaces are symmetrically configured
- mGRE tunnels on spoke routers opens up the capability to allow direct spoke-to-spoke communications.
- Hub cannot summarize spoke routes and cannot send default to spokes

DMVPN Phase 3

- DMVPN Phase 3 network, tunnel interfaces are symmetrically configured
- Hub routers announce their own IP address as the next-hop value when forwarding routing information to spoke routers.
- NHRP Shortcut Switching. This feature allows the spokes to discover shorter paths to a destination network after receiving an NHRP Redirect message from the hub.

Benefits of DMVPN Phase 3

- Because DMVPN Phase 3 does not require the hub to preserve next-hop values in routing updates, summarization of routing protocol updates from hub to spokes is allowed.
- You can even configure the hub router to advertise only a default route to its spoke routers.
- The spokes don't need to have an individual route with an IP next hop of the tunnel IP address of the remote spoke for the networks behind all the other spokes.
- The spokes can use summarized routes with an IP next hop of the tunnel IP address of the hub and still be able to build spoke-to-spoke tunnels.
- This summarization possibility significantly improves network scalability.
- In a DMVPN Phase 3 network, separate regional DMVPN networks can be connected into a single hierarchical DMVPN network.

Agenda

- Dynamic Multipoint VPN Review
- **How to Configure DMVPN without & with IPSec**
- Support for IPv6 with DMVPN
- DMVPN advanced topics (CCIE twists)
- Troubleshooting
- Q&A

Basic NHRP Configuration

- In order to configure an mGRE interface to use NHRP, the following command is necessary:
  - `ip nhrp network-id <id>`
- Where <id> is a unique number (same on hub and all spokes)
- The network ID defines an NHRP domain
- Several domains can co-exist on the same router

Initial NHRP Caches

- Initially, the hub has an empty cache
- The spoke has one static entry mapping the hub's tunnel address to the hub's NBMA address:
  - `ip nhrp map 172.110.123.1 10.1.1.1`
  - Multicast traffic must be sent to the hub
  - `ip nhrp map multicast 10.1.1.1`

  - Tunnel Interface IP subnet is 172.110.123.0/24
  - Tunnel Source 10.1.1.1

The Spokes Must Register To The Hub

- In order for the spokes to register themselves to the hub, the hub must be declared as a Next Hop Server (NHS):
  - `ip nhrp nhs 172.110.123.1`
  - `ip nhrp holdtime 3600` `(optional)`
    - NHRP registrations are sent from NHCs to their configured NHSs every one-third of the NHRP holdtime. Default is 2400 seconds (40 minutes)
  - `ip nhrp registration no-unique` `(optional)`
- Spokes control the cache on the hub

- Tunnel Interface IP subnet is 172.110.123.0/24

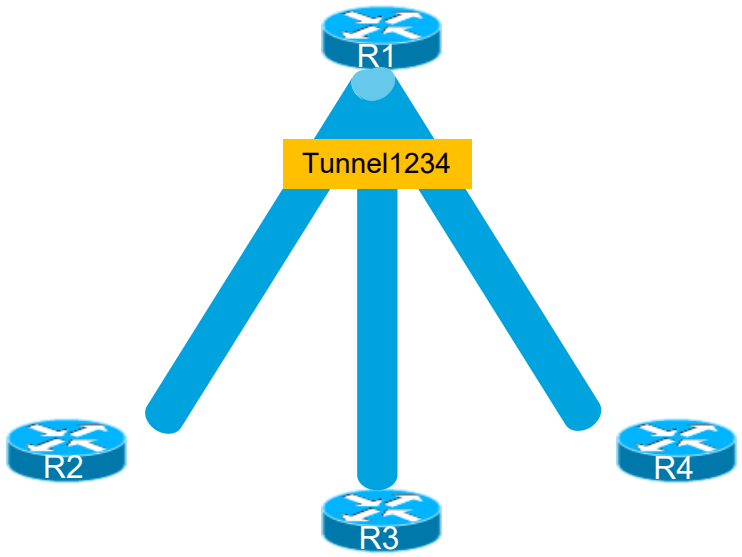
Registration Process

- The spokes send Registration-requests to the hub
- The request contains the spoke's Tunnel and NBMA addresses as well as the hold time and some flags
- The hub creates an entry in its NHRP cache
- The entry will be valid for the duration of the hold time defined in the registration
- The NHS returns a registration reply (acknowledgement)

Multicast Packets from the Hub

- The hub must also send multicast traffic to all the spokes that registered to it
- This must be done dynamically (possible since Release 12.2(13)T)
- This is not the default
  - `ip nhrp map multicast dynamic`

DMVPN Basics - Configuration



Basic DMVPN Configuration Example

```
hostname R1 ! Hub
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface Tunnel123
 ip address 172.110.123.1 255.255.255.0
 no ip redirects
 ip nhrp network-id 1
 ip ospf network non-broadcast
 tunnel source 10.1.1.1
 tunnel mode gre multipoint
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
!
router ospf 2
 network 1.1.1.1 0.0.0.0 area 1
 network 172.110.123.0 0.0.0.255 area 0
 neighbor 172.110.123.2
 neighbor 172.110.123.3
```

```
hostname R2 ! Spoke
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!
interface Tunnel123
 ip address 172.110.123..2 255.255.255.0
 ip nhrp map 172.110.123.1 10.1.1.1
 ip nhrp map multicast 10.1.1.1
 ip nhrp network-id 1
 ip nhrp nhs 172.110.123.1
 ip ospf network non-broadcast
 ip ospf priority 0
 tunnel source 10.1.1.2
 tunnel mode gre multipoint
!
interface FastEthernet0/0
 ip address 10.1.1.2 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
!
router ospf 2
 network 2.2.2.2 0.0.0.0 area 2
 network 172.110.123.0 0.0.0.255 area 0
```

IPsec Protection

- GRE/NHRP can build a fully functional overlay network
- GRE is insecure; ideally, it must be protected
- The good old crypto map configuration is rather cumbersome; DMVPN introduced tunnel protection (which can also be used with VTI)
- Still need to define an IPsec security level

The IPsec Security Policy

- Phase I has to be defined:
  - `crypto isakmp policy 10`
    - `authentication pre-share`
  - `crypto isakmp key CISCO address 0.0.0.0`
- A transform set must be defined:
  - `crypto ipsec transform-set MyTS esp-sha-hmacesp-3des`
  - `mode transport`
- An IPsec profile replaces the crypto map:
  - `crypto ipsec profile MyProfile`
  - `set transform-set MyTS`
  - The IPsec profile is like a crypto map without “set peer” and “match address”

Protecting the tunnel

- The profile must be applied on the tunnel
  - `tunnel protection ipsec profile MyProfile`
- Internally Cisco IOS® Software will treat this as a dynamic crypto map and it derives the local-address, set peer and match address parameters from the tunnel parameters and the NHRP cache
- •This must be configured on the hub and spoke tunnels along with a tunnel key

DMVPN with IPSec Configuration Example

```
hostname R1 ! Hub
!
crypto isakmp policy 10
 encryption aes 256
 hash sha512
 authentication pre-share
crypto isakmp key CISCO address 0.0.0.0
crypto isakmp diagnose error
!
crypto ipsec transform-set MyTS esp-sha256-hmac esp-aes
 mode transport
!
crypto ipsec profile MyProfile
 set transform-set MyTS
!
interface Tunnel123
 ip address 172.110.123.1 255.255.255.0
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip ospf network non-broadcast
 tunnel source 10.1.1.1
 tunnel mode gre multipoint
 tunnel key 1
 tunnel protection ipsec profile MyProfile
```

```
hostname R2 ! Spoke
!
crypto isakmp policy 10
 encryption aes 256
 hash sha512
 authentication pre-share
crypto isakmp key CISCO address 0.0.0.0
crypto isakmp diagnose error
!
crypto ipsec transform-set MyTS esp-sha256-hmac esp-aes
 mode transport
!
crypto ipsec profile MyProfile
 set transform-set MyTS
!
interface Tunnel123
 ip address 172.110.123.2 255.255.255.0
 ip nhrp map 127.110.123.1 10.1.1.1
 ip nhrp map multicast 10.1.1.1
 ip nhrp network-id 1
 ip nhrp nhs 172.110.123.1
 ip ospf network non-broadcast
 ip ospf priority 0
 tunnel source 10.1.1.2
 tunnel mode gre multipoint
 tunnel key 1
 tunnel protection ipsec profile MyProfile
```

Agenda

- Dynamic Multipoint VPN Review
- How to Configure DMVPN without & with IPSec
- **Support for IPv6 with DMVPN**
- DMVPN advanced topics (CCIE twists)
- Troubleshooting
- Q&A

IPv6 NHRP Configuration

- In order to configure an mGRE interface to use NHRP for IPv6, the following command is necessary:
  - `ipv6 nhrp network-id <id>`
- Where <id> is a unique number (same on hub and all spokes)
- The network ID defines an NHRP domain
- Several domains can co-exist on the same router

Initial NHRP Caches

- Initially, the hub has an empty cache
- The spoke has one static entry mapping the hub's tunnel address to the hub's NBMA address:
  - `ipv6 nhrp map 2005:dead:beef:99::1/128 10.1.1.1`
- Multicast traffic must be sent to the hub
  - `ipv6 nhrp map multicast 10.1.1.1`

  - Tunnel Interface IPv6 is 2005:DEAD:BEEF:99::/64
  - Tunnel Source 10.1.1.1

The Spokes Must Register To The Hub

- In order for the spokes to register themselves to the hub, the hub must be declared as a Next Hop Server (NHS):
  - `ipv6 nhrp nhs 2005:dead:beef:99::1`
  - `ipv6 nhrp holdtime 3600 (optional)`
  - `ipv6 nhrp registration no-unique (optional)`
- Spokes control the cache on the hub

Multicast Packets from the Hub

- The hub must also send multicast traffic to all the spokes that registered to it
- This is not the default
  - `ipv6 nhrp map multicast dynamic`

DMVPN IPv6 Configuration Example

```
hostname R1 ! Hub
!
interface Tunnel123
 no ip address
 no ip redirects
 ipv6 address FE80::1 link-local
 ipv6 address 2005:DEAD:BEEF:99::1/64
 ipv6 nhrp map multicast dynamic
 ipv6 nhrp network-id 1
 ipv6 ospf 2 area 0
 ipv6 ospf neighbor FE80::2
 ipv6 ospf network non-broadcast
 tunnel source 10.1.1.1
 tunnel mode gre multipoint
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 ipv6 ospf 1 area 0
!
```

```
hostname R2 ! Spoke
!
interface Tunnel123
 no ip address
 no ip redirects
 ipv6 address FE80::2 link-local
 ipv6 address 2005:DEAD:BEEF:99::2/64
 ipv6 nhrp map multicast 10.1.1.1
 ipv6 nhrp map FE80::1/128 10.1.1.1
 ipv6 nhrp map 2005:DEAD:BEEF:99::1/128
10.1.1.1
 ipv6 nhrp network-id 1
 ipv6 nhrp nhs 2005:DEAD:BEEF:99::1
 ipv6 ospf 2 area 0
 ipv6 ospf network non-broadcast
 ipv6 ospf priority 0
 tunnel source 10.1.1.2
 tunnel mode gre multipoint
!
interface FastEthernet0/0
 ip address 10.1.1.2 255.255.255.0
!
```

DMVPN over IPv6

- In Cisco IOS Release 15.2(1)T, IPv6 support on DMVPN was extended to the public network
- The spoke has one static entry mapping the hub's tunnel address to the hub's NBMA address:
  - `ipv6 nhrp map 2005:dead:beef:99::1/128 2001:1:1::1`
- Multicast traffic must be sent to the hub
  - `ipv6 nhrp map multicast 2001:1:1::1`
- Tunnel mode has to be set to:
  - `tunnel mode gre multipoint ipv6`
    - Tunnel Interface (private) 2005:DEAD:BEEF:99::/64
    - Tunnel Source (public) 2001:1:1::1

DMVPN IPv6 Configuration over IPv6 Example

```
hostname R1 ! Hub
!
interface Tunnel123
 no ip address
 no ip redirects
 ipv6 address FE80::1 link-local
 ipv6 address 2005:DEAD:BEEF:99::1/64
 ipv6 nhrp map multicast dynamic
 ipv6 nhrp network-id 1
 ipv6 ospf 2 area 0
 ipv6 ospf neighbor FE80::2
 ipv6 ospf network non-broadcast
 tunnel source 2001:1:1::1
 tunnel mode gre multipoint ipv6
!
interface FastEthernet0/0
 ipv6 address 2001:1:1::1/64
 ipv6 ospf 1 area 0
!
```

```
hostname R2 ! Spoke
!
interface Tunnel123
 no ip address
 no ip redirects
 ipv6 address FE80::2 link-local
 ipv6 address 2005:DEAD:BEEF:99::2/64
 ipv6 nhrp map multicast 2001:1:1::1
 ipv6 nhrp map FE80::1/128 2001:1:1::1
 ipv6 nhrp map 2005:DEAD:BEEF:99::1/128
10.1.1.1
 ipv6 nhrp network-id 1
 ipv6 nhrp nhs 2005:DEAD:BEEF:99::1
 ipv6 ospf 2 area 0
 ipv6 ospf network non-broadcast
 ipv6 ospf priority 0
 tunnel source 2001:1:1::2
 tunnel mode gre multipoint ipv6
!
interface FastEthernet0/0
 ipv6 address 2001:1:1::2/64
!
```

Agenda

- Dynamic Multipoint VPN Review
- How to Configure DMVPN without & with IPSec
- Support for IPv6 with DMVPN
- **DMVPN advanced topics (CCIE twists)**
- Troubleshooting
- Q&A

Dynamic verses Static Spokes

- Dynamic
  - Spoke to spoke dynamic tunnels
  - Passes through hub, but hub does not decrement TTL due to traffic hidden from via the dynamic tunnel
  - Spoke tunnel mode:
    - `tunnel mode gre multipoint`
- Static
  - Spoke to hub only
  - Traffic can be routed through the hub, therefore the TTL is decremented
  - Spoke tunnel mode:
    - `No tunnel mode`
    - `Tunnel destination "hub address"`

Routing Issues with DMVPN

- Dynamic Spokes:
  - OSPF and EIGRP can neighbor spoke to without issue (no TTL concerns)
  - eBGP can form peering relationships with modifying TTL
- Static Spokes:
  - OSPF can only neighbor to Hub
  - EIGRP can neighbor with static neighbor statements
  - eBGP can form peering relationships by using either ebgp-multihop ot TTL security

OSPF over DMVPN

- Default OSPF network type is Point to Point
- Watch out if multicast is to be supported or not on the tunnel interface

QoS with DMVPN

- Pre-classify
  - Copies payload TOS or Traffic Class field to Tunnel Header

```
R1(config)# interface tunnel123
R1(config-if)# qos preclassify
```

- QoS Per Tunnel
  - Spoke has a NHRP Group referenced under its tunnel interface
  - Hub has policy map and is referenced on the tunnel interface and the NHRP group name from spoke

Per Tunnel Qos

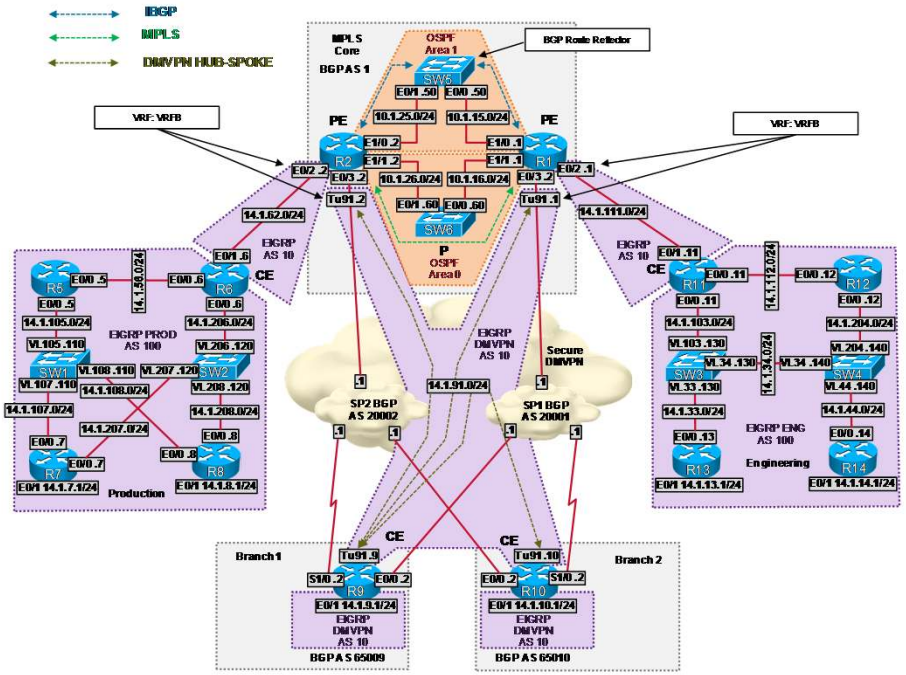
- Spoke

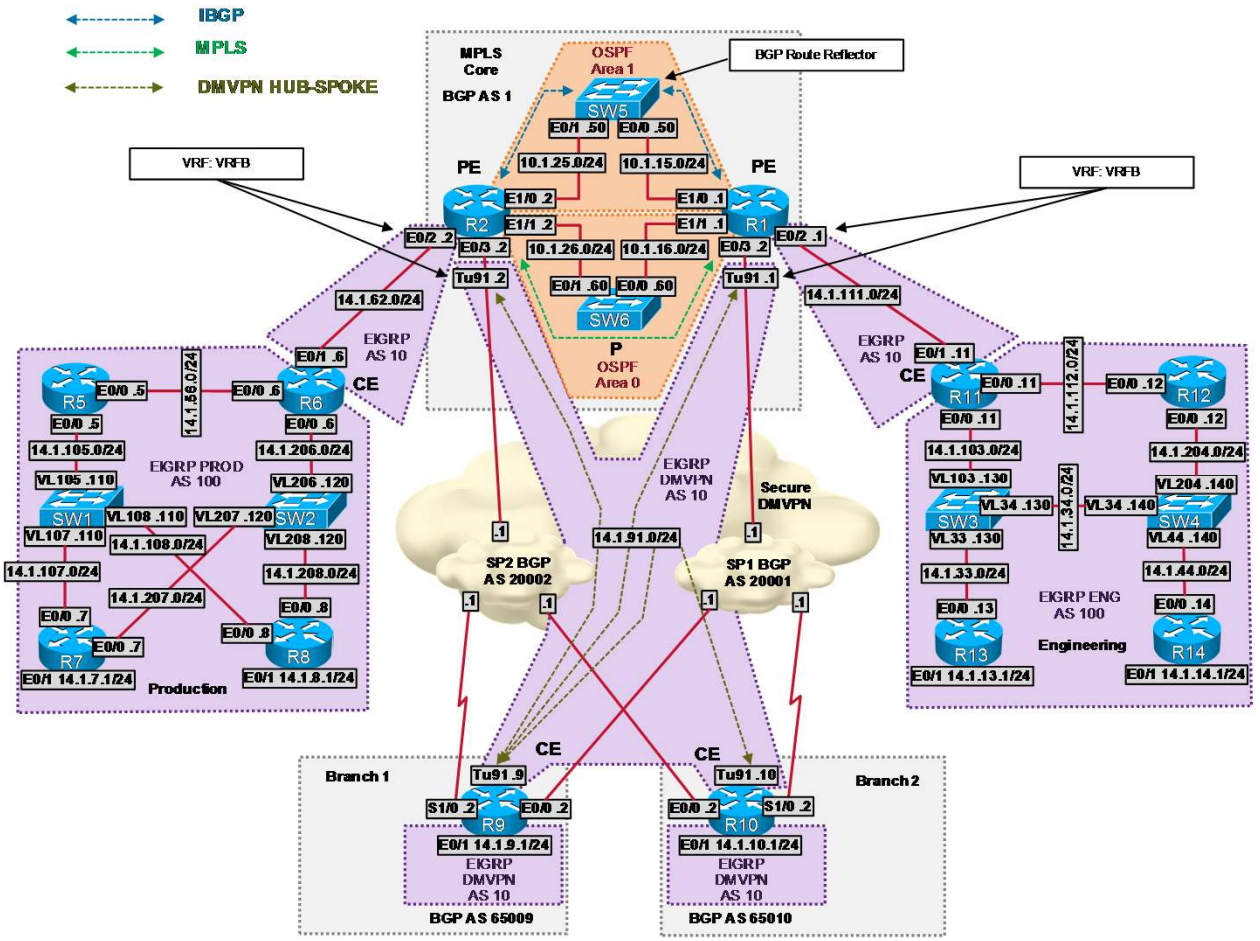
```
Interface tunnel 123
 ip nhrp group spoke1
```

- Hub

```
Class-map Voice
 match access-group 100
!
Policy-map VoIP
 class Voice
  priority percent 30
!
Interface tunnel 123
 ip nhrp map group spoke1 service-policy output
VoIP
```

CCIE DMVPN Example





CCIE DMVPN Example

- **3.5. VRFB DMVPN (4 points)**
- Configure the mGRE Tunnel91 interfaces on R1, R2, R9, and R10.
- Use the Loopback0 interfaces for the Tunnel91 interface source.
- Supply IPv4 addresses for all required tunnel interfaces according to the “MP-BGP MPLS VRFB Topology” diagram.
- Configure R9 as the IPv4 NHRP NHS for the DMVPN spokes R1, R2, and R10.
- Supply the NHRP NHS mapping for unicast IPv4 on R1, R2, and R10. Do not configure any NHRP mapping for unicast IPv4 traffic on R9.
- NHRP communications must be authenticated with the string **eigrp**.
- Provide static mapping for the IPv4 multicast and broadcast traffic on R1, R2, and R10.
- Set the MTU size on the tunnel interfaces to 1400 bytes.
- Place the Tunnel91 interfaces on R1 and R2 in the VRFB.
- Enable direct communications between the DMVPN spoke networks.

3.5. VRFB DMVPN R1 and R2

R1:

```
interface Tunnel91
ip vrf forwarding VRFB
ip address 14.1.91.1 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication eigrp
ip nhrp map 14.1.91.9 14.14.1.9
ip nhrp map multicast 14.14.1.9
ip nhrp network-id 1
ip nhrp nhs 14.1.91.9
ip nhrp shortcut
tunnel source Loopback0
tunnel mode gre multipoint
tunnel key 10
```

R2:

```
interface Tunnel91
ip vrf forwarding VRFB
ip address 14.1.91.2 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication eigrp
ip nhrp map 14.1.91.9 14.14.1.9
ip nhrp map multicast 14.14.1.9
ip nhrp network-id 1
ip nhrp nhs 14.1.91.9
ip nhrp shortcut
tunnel source Loopback0
tunnel mode gre multipoint
tunnel key 10
```

3.5. VRFB DMVPN R9 and R10

R9:

```
interface Tunnel91
ip address 14.1.91.9 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication eigrp
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip nhrp redirect
tunnel source Loopback0
tunnel mode gre multipoint
tunnel key 10
```

R10:

```
interface Tunnel91
ip address 14.1.91.10 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication eigrp
ip nhrp map 14.1.91.9 14.14.1.9
ip nhrp map multicast 14.14.1.9
ip nhrp network-id 1
ip nhrp nhs 14.1.91.9
ip nhrp shortcut
tunnel source Loopback0
tunnel mode gre multipoint
tunnel key 10
```

CCIE DMVPN Example

- **4.1. DMVPN Security (2 points)**
- Configure the IPsec ISAKMP policy on R1, R2, R9, and R10 according to the following specifications:

Parameter	Value
pre-shared key	CCIE
encryption	aes 256 bit
IPsec transform name	TRANSFORM
IPsec transform algorithm	esp-aes esp-sha256-hmac
IPsec mode	transport
IPsec profile name	PROFILE

- Apply the IPsec profile on the Tunnel91 interfaces on R1, R2, R9, and R10.
- The traffic that is forwarded on the Tunnel91 interfaces must be encrypted.

Configuration examples on R1, R2, R9, and R10

```
crypto isakmp policy 10
encr aes 256
authentication pre-share
crypto isakmp key CCIE  address 0.0.0.0
!
crypto ipsec transform-set TRANSFORM esp-aes
esp-sha256-hmac
 mode transport
!
crypto ipsec profile PROFILE
set transform-set TRANSFORM
!
interface Tunnel91
tunnel protection ipsec profile PROFILE
!
```

Agenda

- Dynamic Multipoint VPN Review
- How to Configure DMVPN without & with IPSec
- Support for IPv6 with DMVPN
- DMVPN advanced topics (CCIE twists)
- **Troubleshooting**
- Q&A

Troubleshooting – Show Commands

- **show dmvpn**
  - Display DMVPN session related information
- **show dmvpn detail**
  - display detailed information about all (IPv4/IPv6) networks
- **show ip/ipv6 nhrp**
- **debug dmvpn**
- **debug ip nhrp**

Agenda

- Dynamic Multipoint VPN Review
- How to Configure DMVPN without & with IPSec
- Support for IPv6 with DMVPN
- DMVPN advanced topics (CCIE twists)
- Troubleshooting
- **Q&A**

Q&A

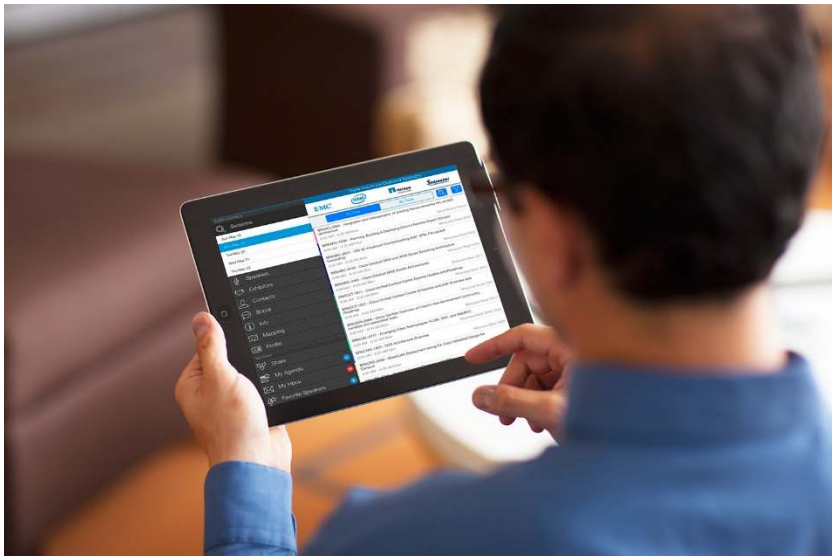
Participate in the “My Favorite Speaker” Contest

Promote Your Favorite Speaker and You Could be a Winner

- Promote your favorite speaker through Twitter and you could win $200 of Cisco Press products (@CiscoPress)
- Send a tweet and include
  - Your favorite speaker’s Twitter handle <CCIE6458>
  - Two hashtags: #CLUS #MyFavoriteSpeaker
- You can submit an entry for more than one of your “favorite” speakers
- Don’t forget to follow @CiscoLive and @CiscoPress
- View the official rules at http://bit.ly/CLUSwin

Complete Your Online Session Evaluation

- Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 Amazon gift card.
- Complete your session surveys though the Cisco Live mobile app or your computer on Cisco Live Connect.



Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online


CISCO
TOMORROW starts here.