TOMORROW starts here.
DMVPN for R&S CCIE Candidates
Johnny Bass
CCIE #6458
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)

<table>
<thead>
<tr>
<th>4.1.4</th>
<th>Implement and Troubleshoot DMVPN (single hub)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.4 a</td>
<td>NHRP</td>
</tr>
<tr>
<td>4.1.4 b</td>
<td>DMVPN with IPsec using preshared key</td>
</tr>
<tr>
<td>4.1.4 c</td>
<td>QoS Profile</td>
</tr>
<tr>
<td>4.1.4 d</td>
<td>Pre-classify</td>
</tr>
</tbody>
</table>
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

Diagram:
- R1
- R2
- R3
- R4
- Tunnel 1234
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
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 99.1.1.1 10.15.15.1`
- Multicast traffic must be sent to the hub
  - `ip nhrp map multicast 10.15.15.1`

- Tunnel Interface IP is 99.1.1.0/24
- Tunnel Source 10.15.15.1
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 99.1.1.1`
  - `ip nhrp holdtime 3600 (optional)`
  - `ip nhrp registration no-unique (optional)`

• Spokes control the cache on the hub

• Tunnel Interface IP is 99.1.1.0/24
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

### Router R1: Hub

```
hostname R1 ! Hub
! interface Loopback0
  ip address 1.1.1.1 255.255.255.255
! interface Tunnel1234
  ip address 99.1.1.1 255.255.255.0
  ip nhrp map multicast dynamic
  ip nhrp network-id 1
  ip ospf network non-broadcast
  tunnel source 10.15.15.1
  tunnel mode gre multipoint
! interface FastEthernet0/0
  ip address 10.15.15.1 255.255.255.0
! 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 99.0.0.0 0.255.255.255 area 0
  neighbor 99.1.1.4
  neighbor 99.1.1.3
  neighbor 99.1.1.2
```

### Router R2: Spoke

```
hostname R2 ! Spoke
! interface Loopback0
  ip address 2.2.2.2 255.255.255.255
! interface Tunnel1234
  ip address 99.1.1.2 255.255.255.0
  ip nhrp map 99.1.1.1 10.15.15.1
  ip nhrp map multicast 10.15.15.1
  ip nhrp network-id 1
  ip nhrp nhs 99.1.1.1
  ip ospf network non-broadcast
  ip ospf priority 0
  tunnel source 10.25.25.2
  tunnel mode gre multipoint
! interface FastEthernet0/0
  ip address 10.25.25.2 255.255.255.0
! 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 99.0.0.0 0.255.255.255 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 ts esp-sha-hmacesp-3des
  – mode transport

• An IPsec profile replaces the crypto map:
  – crypto ipsec profile prof
  – set transform-set ts
  – 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 prof`

• 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
encr 3des
hash md5
authentication pre-share
crypto isakmp key CISCO address 0.0.0.0
crypto isakmp diagnose error
!
crypto ipsec transform-set ts esp-sha-hmacesp-3des
mode transport
!
crypto ipsec profile prof
set transform-set ts
!
interface Tunnel1234
ip address 99.1.1.1 255.255.255.0
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip ospf network non-broadcast
tunnel source 10.15.15.1
tunnel mode gre multipoint
tunnel protection ipsec profile prof
!
```

```
hostname R2 ! Spoke
!
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
crypto isakmp key CISCO address 0.0.0.0
crypto isakmp diagnose error
!
crypto ipsec transform-set ts esp-sha-hmacesp-3des
mode transport
!
crypto ipsec profile prof
set transform-set ts
!
interface Tunnel1234
ip address 99.1.1.2 255.255.255.0
ip nhrp map 99.1.1.1 10.15.15.1
ip nhrp map multicast 10.15.15.1
ip nhrp network-id 1
ip nhrp nh 99.1.1.1
ip ospf network non-broadcast
ip ospf priority 0
tunnel source 10.25.25.2
tunnel mode gre multipoint
tunnel protection ipsec profile prof
!
```
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 10.15.15.1`
- Multicast traffic must be sent to the hub
  - `ipv6 nhrp map multicast 10.15.15.1`

- Tunnel Interface IPv6 is 2005:DEAD:BEEF:99::/64
- Tunnel Source 10.15.15.1
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 Tunnel1234
   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 10.15.15.1
   tunnel mode gre multipoint

interface FastEthernet0/0
   ip address 10.15.15.1 255.255.255.0
   ipv6 ospf 1 area 0

hostname R2 ! Spoke

interface Tunnel1234
   no ip address
   no ip redirects
   ipv6 address FE80::2 link-local
   ipv6 address 2005:DEAD:BEEF:99::2/64
   ipv6 nhrp map multicast 10.15.15.1
   ipv6 nhrp map FE80::1/128 10.15.15.1
   ipv6 nhrp map 2005:DEAD:BEEF:99::1/128 10.15.15.1
   ipv6 nhrp network-id 1
   ipv6 nhrp nh 2005:DEAD:BEEF:99::1
   ipv6 ospf 2 area 0
   ipv6 ospf network non-broadcast
   ipv6 ospf priority 0
   tunnel source 10.15.15.2
   tunnel mode gre multipoint

interface FastEthernet0/0
   ip address 10.25.25.2 255.255.255.0
```
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:
    * tunnel mode gre
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 tunnel1234
    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 1234
  ip nhrp group spoke1
```

**Hub**

```
class-map Voice
  match access-group 100
!
policy-map VoIP
  class Voice
    priority percent 30
!
interface tunnel 1234
  ip nhrp map group spoke1
  service-policy output VoIP
```
 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
Complete Your Online Session Evaluation

• Give us your feedback and you could win fabulous prizes. Winners announced daily.

• Complete your session evaluation through the Cisco Live mobile app or visit one of the interactive kiosks located throughout the convention center.

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