

## <u>Tasks</u> BGP

- 1. Configure R1 and R10 in AS 1, R2 in AS 2, and R3 in AS 33
- 2. Configure EBGP peerings between the SP router which is in AS 100.100 for the IPv4 unicast AFI/SAFI. Note that R3's connected route to the SP is in the INTERNET VRF
- 3. The SP has incorrectly configured the **remote-as** setting to R3 as AS 3 rather than AS 33. Configure only R3 to fix this issue.
- 4. Configure the SP to advertise a default route.

## **DMVPN**

- 1. Configure tunnel100 as the DMVPN tunnel using NHRP network ID 123.
- 2. R1 is the spoke (behind R10 who is performing NAT overload); R2 and R3 are spokes
- 3. Configure the Tunnel to support DMVPN Phase 3

## **DMVPN Security**

- 1. Configure ISAKMP as follows
- 1. AES 192, SHA512, Group 14, Pre-share authentication
- 2. Configure the pre-shared key between the DMVPN routers as "CCIE"
- 3. Configure a transform set called TS which supports AES 128 encyrption and SHA256 HMAC authentication

## **DMVPN Routing**

- 1. Configure named EIGRP (called CCIE) in AS 234
- 2. Configure the strongest authentication possible for all current and future interfaces that are in this EIGRP process
- 3. Configure EIGRP on all interfaces in the 10.0.0.0/8 network
- 4. Test connectivity between the PC and the server using the hostname rather than the IP address (i.e. ping SERVER)