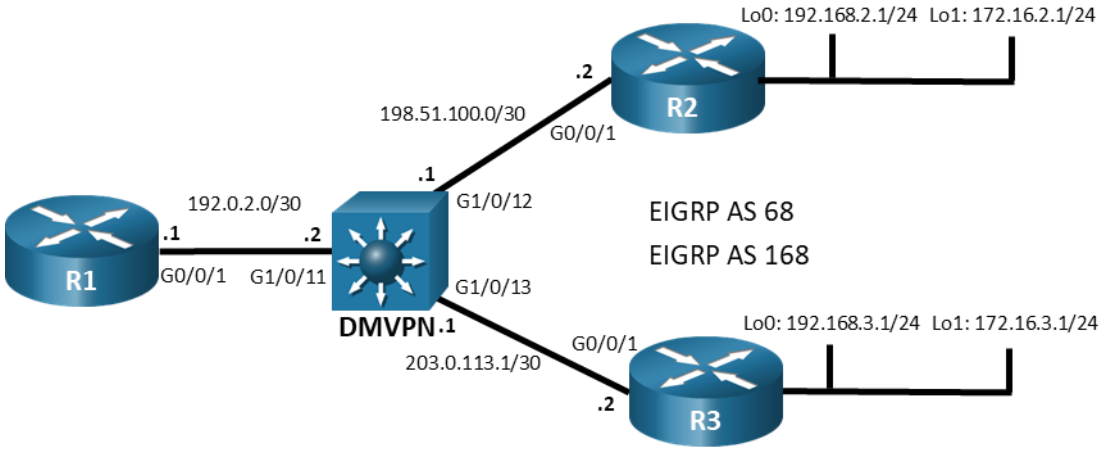
Lab - Configure Secure DMVPN Tunnels (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Answers: 20.1.2 Lab - Configure Secure DMVPN Tunnels

Topology



Addressing Table

Device	Interface	IPv4 Address
R1	G0/0/1	192.0.2.1/24
	Tunnel 1	100.100.100.1/29
R2	G0/0/1	198.51.100.2/24
	Loopback 0	192.168.1.1/24
	Loopback 1	172.16.1.1/24
	Tunnel 1	100.100.100.2/29
R3	G0/0/1	203.0.113.2/24
	Loopback 0	192.168.3.1/24
	Loopback 1	172.16.3.1/24
	Tunnel 1	100.100.100.3/29

Objectives

Part 1: Build the Network and Verify DMVPN Phase 3 Operation

Part 2: Secure DMVPN Phase 3 Tunnels

Background / Scenario

In previous labs, you have configured DMVPN Phase 1 and Phase 3 networks, including configuration of DMVPN Phase 3 with IPv6. However, in those labs, IPsec was not used to encrypt and protect data travelling on the tunnels. IPsec functionality is essential to DMVPN implementation. In this lab, you will work with the DMVPN Phase 3 implementation from the Implement a DMVPN Phase 3 Spoke-to-Spoke Topology lab. You will start with a working configuration and then apply IPsec to the spoke-to-hub and spoke-to-spoke tunnels. Finally, you will verify the operation of the secured tunnels.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switch used is a Cisco Catalyst 3650 with Cisco IOS XE Release 16.9.4 (universalk9 image). Other routers, Layer 3 switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Required Resources

- 3 Routers (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 1 Switch (Cisco 3560 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 1 PC (Choice of operating system with a terminal emulation program installed)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Initial Configurations

Students will use the answer configurations from the lab Implement a DMVPN Phase 3 Spoke-to-Spoke Topology. If they do not have the preconfigured devices, they could benefit by practicing configuration of DMVPN Phase 3 from that lab. Otherwise, they could paste the initial configurations into the devices. Initial configurations are provided here.

R1 hub router

```
hostname R1
no ip domain lookup
banner motd # R1, Implement DMVPN Hub #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 logging synchronous
 login
 exit
interface g0/0/1
 ip address 192.0.2.1 255.255.255.252
 no shutdown
 exit
interface tunnel 1
 tunnel mode gre multipoint
```

```
 tunnel source g0/0/1
 tunnel key 999
 ip address 100.100.100.1 255.255.255.248
 ip nhrp network-id 1
 ip nhrp authentication NHRPauth
 ip nhrp map multicast dynamic
 ip nhrp redirect
 bandwidth 4000
 ip mtu 1400
 ip tcp adjust-mss 1360
 exit
router eigrp DMVPN_TUNNEL_NET
 address-family ipv4 unicast autonomous-system 68
 eigrp router-id 1.1.1.1
 network 100.100.100.0 255.255.255.248
 af-interface tunnel 1
  no split-horizon
router eigrp DMVPN_TRANS_NET
 address-family ipv4 unicast autonomous-system 168
 eigrp router-id 10.1.1.1
 network 192.0.2.0 255.255.255.252
end
```

R2 spoke router 1

```
hostname R2
no ip domain lookup
banner motd # R2, Implement DMVPN Spoke 1 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 logging synchronous
 login
 exit
interface g0/0/1
 ip address 198.51.100.2 255.255.255.252
 no shutdown
 exit
interface loopback 0
 ip address 192.168.2.1 255.255.255.0
 no shutdown
 exit
interface loopback 1
```

```
 ip address 172.16.2.1 255.255.255.0
 no shutdown
 exit
interface tunnel 1
 tunnel mode gre multipoint
 tunnel source loopback 0
 no tunnel destination
 tunnel key 999
 ip address 100.100.100.2 255.255.255.248
 ip nhrp network-id 1
 ip nhrp authentication NHRPauth
 ip nhrp nhs 100.100.100.1
 ip nhrp map multicast 192.0.2.1
 ip nhrp map 100.100.100.1 192.0.2.1
 ip nhrp shortcut
 ip mtu 1400
 ip tcp adjust-mss 1360
router eigrp DMVPN_TUNNEL_NET
 address-family ipv4 unicast autonomous-system 68
 eigrp router-id 2.2.2.2
 network 100.100.100.0 255.255.255.248
 network 172.16.2.0 255.255.255.0
 eigrp stub connected
router eigrp DMVPN_TRANS_NET
 address-family ipv4 unicast autonomous-system 168
 eigrp router-id 20.2.2.2
 network 198.51.100.0 255.255.255.252
 network 192.168.2.0 255.255.255.0
end
```

Router R3 spoke 2

```
hostname R3
no ip domain lookup
banner motd # R3, Implement DMVPN Spoke 2 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 logging synchronous
 login
 exit
interface g0/0/1
```

```
 ip address 203.0.113.2 255.255.255.252
 no shutdown
 exit
interface loopback 0
 ip address 192.168.3.1 255.255.255.0
 no shutdown
 exit
interface loopback 1
 ip address 172.16.3.1 255.255.255.0
 no shutdown
 exit
interface tunnel 1
 tunnel mode gre multipoint
 tunnel source loopback 0
 no tunnel destination
 tunnel key 999
 ip address 100.100.100.3 255.255.255.248
 ip nhrp network-id 1
 ip nhrp authentication NHRPauth
 ip nhrp nhs 100.100.100.1
 ip nhrp map multicast 192.0.2.1
 ip nhrp map 100.100.100.1 192.0.2.1
 ip nhrp shortcut
 ip mtu 1400
 ip tcp adjust-mss 1360
router eigrp DMVPN_TUNNEL_NET
 address-family ipv4 unicast autonomous-system 68
 eigrp router-id 3.3.3.3
 network 100.100.100.0 255.255.255.248
 network 172.16.3.0 255.255.255.0
 eigrp stub connected
router eigrp DMVPN_TRANS_NET
 address-family ipv4 unicast autonomous-system 168
 eigrp router-id 30.3.3.3
 network 203.0.113.0 255.255.255.252
 network 192.168.3.0 255.255.255.0
 eigrp stub connected
end
```

Layer 3 Switch DMVPN

```
hostname DMVPN
no ip domain lookup
ip routing
banner motd # DMVPN, DMVPN cloud switch #
line con 0
 exec-timeout 0 0
```

```
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 logging synchronous
 login
interface g1/0/11
 no switchport
 ip address 192.0.2.2 255.255.255.252
 no shutdown
 exit
interface g1/0/12
 no switchport
 ip address 198.51.100.1 255.255.255.252
 no shutdown
 exit
interface g1/0/13
 no switchport
 ip address 203.0.113.1 255.255.255.252
 no shutdown
 exit
router eigrp DMVPN_TRANS_NET
 address-family ipv4 unicast autonomous-system 168
 eigrp router-id 40.4.4.4
 network 192.0.2.0 255.255.255.252
 network 198.51.100.0 255.255.255.252
 network 203.0.113.0 255.255.255.252
end
```

Instructions

Part 1: Build the Network and Verify DMVPN Phase 3 Operation

In Part 1, you will set up the network topology and configure basic settings if the network is not already configured. This lab uses the same topology and final configurations from the **Implement a DMVPN Phase 3 Spoke-to-Spoke Topology** lab.

Step 1: Cable the network as shown in the topology.

Connect the devices as shown in the topology diagram.

Step 2: Configure initial settings for each router and the Layer 3 switch.

Console into each device, enter global configuration mode, and apply the initial settings for the lab if the devices are not already configured.

Step 3: Verify connectivity in the network.

a. From R1, **ping** the loopback interfaces of R2 and R3. All pings should be successful. This verifies that full connectivity exists in the underlay, or transport, network.

```
R1# ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R1# ping 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Step 4: Verify DMVPN Phase 3 operation.

a. Return to R2. Initiate a **traceroute** to the simulated LAN interface on R3. The path will pass through R1 as it does in a DMVPN Phase 1 network.

Note: The first trace may fail if the DMVPN switch CAM table is empty.

```
R2# traceroute 172.16.3.1
Type escape sequence to abort.
Tracing the route to 172.16.3.1
VRF info: (vrf in name/id, vrf out name/id)
  1 100.100.100.1 1 msec 1 msec 1 msec
  2 100.100.100.3 1 msec *  2 msec
```

b. Issue the **traceroute** command again. You will now see that R1 has enabled direct spoke-to-spoke communication between R2 and R3. This tunnel will expire and close dynamically. The tunnel reopens after data for the spoke router is sent again.

```
R2# traceroute 172.16.3.1
Type escape sequence to abort.
Tracing the route to 172.16.3.1
VRF info: (vrf in name/id, vrf out name/id)
  1 100.100.100.3 1 msec *  1 msec
```

Part 2: Secure DMVPN Phase 3 Tunnels

Now that the tunnels have been configured and DMVPN connectivity has been verified, the tunnels can be secured with IPsec.

Step 1: Create the IKE policy.

Create an IKE policy that defines the hash algorithm, encryption type, key exchange method, Diffie-Hellman group, and the authentication method.

```
R1(config)# crypto isakmp policy 99
R1(config-isakmp)# hash sha384
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# group 14
R1(config-isakmp)# authentication pre-share
```

```
R1(config-isakmp)# exit
```

Step 2: Configure the ISAKMP key.

Configure the pre-shared key and peer address. Use 0.0.0.0 to match multiple peer addresses. Use a key of **DMVPN@key#**.

```
R1(config)# crypto isakmp key DMVPN@key# address 0.0.0.0
```

Step 3: Create and configure the IPsec transform set.

Configure the IPsec transform set. Use **DMVPN_TRANS** as the transform set name. Specify **esp-aes** with a 256-bit key as the encryption transform and **esp-sha384-hmac** as the authentication transform. Configure the transform set to use IPsec **transport** mode for the tunnels.

```
R1(config)# crypto ipsec transform-set DMVPN_TRANS esp-aes 256 esp-sha384-hmac
R1(cfg-crypto-trans)# mode transport
R1(cfg-crypto-trans)# exit
```

Step 4: Create the IPsec profile.

Create an IPsec profile with the name **DMVPN_PROFILE**. Associate the **DMVPN_TRANS** transform set with the profile.

```
R1(config)# crypto ipsec profile DMVPN_PROFILE
R1(ipsec-profile)# set transform-set DMVPN_TRANS
R1(ipsec-profile)# exit
```

Step 5: Apply the IPsec profile to the tunnel interface.

Finally, apply the IPsec profile to the tunnel interface. After you apply the profile, you will see the that IPsec is now active and you will lose adjacency with R2 and R3 until their respective ends of the tunnel are configured.

```
R1(config)# interface tunnel 1
R1(config-if)# tunnel protection ipsec profile DMVPN_PROFILE
R1(config-if)# exit
*Mar 30 07:39:32.398: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config)#
*Mar 30 07:39:32.963: %IOSXE-3-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:001
TS:00000000594132950499 %IPSEC-3-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC
packet, dest_addr= 192.0.2.1, src_addr= 192.168.2.1, prot= 47
*Mar 30 07:39:43.664: %DUAL-5-NBRCHANGE: EIGRP-IPv4 68: Neighbor 100.100.100.2
(Tunnel1) is down: holding time expired
*Mar 30 07:39:44.235: %DUAL-5-NBRCHANGE: EIGRP-IPv4 68: Neighbor 100.100.100.3
(Tunnel1) is down: holding time expired
R1(config)#
```

Step 6: Configure R2 and R3 with IPsec.

Repeat this configuration on the R2 and R3 routers.

```
R2(config)# crypto isakmp policy 99
R2(config-isakmp)# hash sha384
R2(config-isakmp)# encryption aes 256
R2(config-isakmp)# group 14
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# exit
R2(config)# crypto isakmp key DMVPN@key# address 0.0.0.0
```

```
R2(config)# crypto ipsec transform-set DMVPN_TRANS esp-aes 256 esp-sha384-hmac
R2(cfg-crypto-trans)# mode transport
R2(cfg-crypto-trans)# exit
R2(config)# crypto ipsec profile DMVPN_PROFILE
R2(ipsec-profile)# set transform-set DMVPN_TRANS
R2(ipsec-profile)# exit
R2(config)# interface tunnel 1
R2(config-if)# tunnel protection ipsec profile DMVPN_PROFILE
R2(config-if)# exit

R3(config)# crypto isakmp policy 99
R3(config-isakmp)# hash sha384
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# group 14
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# exit
R3(config)# crypto isakmp key DMVPN@key# address 0.0.0.0
R3(config)# crypto ipsec transform-set DMVPN_TRANS esp-aes 256 esp-sha384-hmac
R3(cfg-crypto-trans)# mode transport
R3(cfg-crypto-trans)# exit
R3(config)# crypto ipsec profile DMVPN_PROFILE
R3(ipsec-profile)# set transform-set DMVPN_TRANS
R3(ipsec-profile)# exit
R3(config)# interface tunnel 1
R3(config-if)# tunnel protection ipsec profile DMVPN_PROFILE
R3(config-if)# exit
```

Step 7: Verify DMVPN Phase 3 operation.

a. As was done previously, test the operation of the spoke-to-spoke DMVPN. Return to R2. Initiate a **traceroute** to the simulated LAN interface on R3. The path will pass through R1 as it does in a DMVPN Phase 1 network.

```
R2# traceroute 172.16.3.1
Type escape sequence to abort.
Tracing the route to 172.16.3.1
VRF info: (vrf in name/id, vrf out name/id)
  1 100.100.100.1 1 msec 1 msec 1 msec
  2 100.100.100.3 1 msec *  2 msec
```

b. Issue the **traceroute** command again. You will now see that R1 has enabled direct spoke-to-spoke communication between R2 and R3. This tunnel will expire and close dynamically. The tunnel reopens after data for the spoke router is sent again.

```
R2# traceroute 172.16.3.1
Type escape sequence to abort.
Tracing the route to 172.16.3.1
VRF info: (vrf in name/id, vrf out name/id)
  1 100.100.100.3 1 msec *  1 msec
```

Step 8: Verify IPsec configuration.

Note: Shut down a tunnel interface to clear its IPsec socket if you wish to explore the outputs before and after spoke-to-spoke tunnel establishment.

a. To show information about the IPsec profiles that are configured on a device, issue the **show crypto ipsec profile** command. Note that the profile that was previously configured is shown along with a default profile.

```
R2# show crypto ipsec profile
IPSEC profile DMVPN_PROFILE
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                DMVPN_TRANS:  { esp-256-aes esp-sha384-hmac  } ,
        }

IPSEC profile default
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                default:  { esp-aes esp-sha-hmac  } ,
        }
```

b. It is very important to verify that tunnel traffic will be encrypted. On R1, issue the **show dmvpn detail** command. As the hub router, R1 should see the spoke peers. The first part of the output shows the tunnel interface status and the peer table. Both peers should be shown with their transport and overlay interface addresses, as you have seen previously.

The Crypto Session Details portion of the output should contain information about the status of the encrypted tunnels. Both of the spoke routers should appear in this output also. Note that the transform set that you configured is also displayed in the Crypto Session output.

```
R1# show dmvpn detail
<output omitted>
Interface Tunnel1 is up/up, Addr. is 100.100.100.1, VRF ""
   Tunnel Src./Dest. addr: 192.0.2.1/Multipoint, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "DMVPN_PROFILE"
   Interface State Control: Disabled
   nhrp event-publisher : Disabled
Type:Hub, Total NBMA Peers (v4/v6): 2

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1 192.168.2.1       100.100.100.2    UP 00:04:25     D   100.100.100.2/32
    1 192.168.3.1       100.100.100.3    UP 00:04:59     D   100.100.100.3/32


Crypto Session Details:
--------------------------------------------------------------------------------
```

```
Interface: Tunnel1
Session: [0x7F6E17B867D0]
  Session ID: 0
  IKEv1 SA: local 192.0.2.1/500 remote 192.168.2.1/500 Active
          Capabilities:(none) connid:1001 lifetime:23:59:19
  Session ID: 0
  IKEv1 SA: local 192.0.2.1/500 remote 192.168.2.1/500 Active
          Capabilities:(none) connid:1002 lifetime:23:59:28
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 192.168.2.1
  IPSEC FLOW: permit 47 host 192.0.2.1 host 192.168.2.1
        Active SAs: 4, origin: crypto map
        Inbound:  #pkts dec'ed 17 drop 0 life (KB/Sec) 4607998/3568
        Outbound: #pkts enc'ed 16 drop 0 life (KB/Sec) 4607999/3568
   Outbound SPI : 0xD2E76488, transform : esp-256-aes esp-sha384-hmac
    Socket State: Open

Interface: Tunnel1
Session: [0x7F6E17B86950]
  Session ID: 0
  IKEv1 SA: local 192.0.2.1/500 remote 192.168.3.1/500 Active
          Capabilities:(none) connid:1004 lifetime:23:59:48
  Session ID: 0
  IKEv1 SA: local 192.0.2.1/500 remote 192.168.3.1/500 Active
          Capabilities:(none) connid:1003 lifetime:23:59:40
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 192.168.3.1
  IPSEC FLOW: permit 47 host 192.0.2.1 host 192.168.3.1
        Active SAs: 6, origin: crypto map
        Inbound:  #pkts dec'ed 11 drop 0 life (KB/Sec) 4607999/3588
        Outbound: #pkts enc'ed 10 drop 0 life (KB/Sec) 4607999/3588
   Outbound SPI : 0xCB3D3313, transform : esp-256-aes esp-sha384-hmac
    Socket State: Open

Pending DMVPN Sessions:
```

c. Issue the **show crypto ipsec sa** command on R2 to display the security associations (sa) that have been made by R2. This output is for the spoke-to-hub tunnel between R1 and R2 prior to the establishment of the spoke-to-spoke tunnel. This command provides additional details regarding the IPsec status of the tunnel, encrypted and decrypted packet statistics, and other details regarding characteristics of the encrypted tunnel.

```
R2# show crypto ipsec sa

interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 192.168.2.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.0.2.1/255.255.255.255/47/0)
```

```
   current_peer 192.0.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 125, #pkts encrypt: 125, #pkts digest: 125
    #pkts decaps: 126, #pkts decrypt: 126, #pkts verify: 126
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.2.1, remote crypto endpt.: 192.0.2.1
     plaintext mtu 1458, path mtu 1514, ip mtu 1514, ip mtu idb Loopback0
     current outbound spi: 0x97C1D18A(2546061706)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xD2E76488(3538379912)
        transform: esp-256-aes esp-sha384-hmac ,
        in use settings ={Transport, }
        conn id: 2003, flow_id: ESG:3, sibling_flags FFFFFFFF80000008, crypto map:
Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4607984/3047)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x97C1D18A(2546061706)
        transform: esp-256-aes esp-sha384-hmac ,
        in use settings ={Transport, }
        conn id: 2004, flow_id: ESG:4, sibling_flags FFFFFFFF80000008, crypto map:
Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4607990/3047)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

The output below is for the same command after the spoke-to-spoke tunnel is open. Entries exist for both the tunnel to R1 and the spoke-to-spoke tunnel between R2 and R3.

```
R2# show crypto ipsec sa

interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 192.168.2.1
```

```
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.3.1/255.255.255.255/47/0)
   current_peer 192.168.3.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.2.1, remote crypto endpt.: 192.168.3.1
     plaintext mtu 1458, path mtu 1514, ip mtu 1514, ip mtu idb Loopback0
     current outbound spi: 0x658E8CF5(1703841013)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xFA8FC9F2(4203727346)
        transform: esp-256-aes esp-sha384-hmac ,
        in use settings ={Transport, }
        conn id: 2005, flow_id: ESG:5, sibling_flags FFFFFFFF80000008, crypto map:
Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4608000/3316)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
      spi: 0x59C41A42(1506024002)
        transform: esp-256-aes esp-sha384-hmac ,
        in use settings ={Transport, }
        conn id: 2007, flow_id: ESG:7, sibling_flags FFFFFFFF80004008, crypto map:
Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4608000/3326)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x60CC6F77(1624010615)
        transform: esp-256-aes esp-sha384-hmac ,
        in use settings ={Transport, }
        conn id: 2006, flow_id: ESG:6, sibling_flags FFFFFFFF80000008, crypto map:
Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4608000/3316)
        IV size: 16 bytes
```

```
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
       spi: 0x658E8CF5(1703841013)
        transform: esp-256-aes esp-sha384-hmac ,
        in use settings ={Transport, }
        conn id: 2008, flow_id: ESG:8, sibling_flags FFFFFFFF80004008, crypto map:
Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4608000/3326)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.0.2.1/255.255.255.255/47/0)
   current_peer 192.0.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 67, #pkts encrypt: 67, #pkts digest: 67
    #pkts decaps: 67, #pkts decrypt: 67, #pkts verify: 67
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.2.1, remote crypto endpt.: 192.0.2.1
     plaintext mtu 1458, path mtu 1514, ip mtu 1514, ip mtu idb Loopback0
     current outbound spi: 0x97C1D18A(2546061706)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xD2E76488(3538379912)
        transform: esp-256-aes esp-sha384-hmac ,
        in use settings ={Transport, }
        conn id: 2003, flow_id: ESG:3, sibling_flags FFFFFFFF80000008, crypto map:
Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4607991/3305)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x97C1D18A(2546061706)
```

```
        transform: esp-256-aes esp-sha384-hmac ,
        in use settings ={Transport, }
        conn id: 2004, flow_id: ESG:4, sibling_flags FFFFFFFF80000008, crypto map:
Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4607995/3305)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

d. On R2 issue the **show crypto isakmp sa** command to view the Internet Security Association Management Protocol (ISAKMP) SAs between the peers. Before the formation of the spoke-to-spoke tunnel, SAs have been made between R2 and R3, but no further negotiations have occurred, as indicated by the MM_NO_STATE state of the two SAs between the routers.

```
R2# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.0.2.1       192.168.2.1     QM_IDLE           1001 ACTIVE
192.168.2.1     192.0.2.1       QM_IDLE           1002 ACTIVE
192.168.3.1     192.168.2.1     MM_NO_STATE       1004 ACTIVE (deleted)
192.168.2.1     192.168.3.1     MM_NO_STATE       1003 ACTIVE (deleted)

IPv6 Crypto ISAKMP SA
```

After traffic has established the spoke-to-spoke tunnel, the SAs all show the QM_IDLE state. The SAs have been fully negotiated and are available for further ISAKMP quick mode exchanges.

Note: ISAKMP modes are outside the scope of this course.

```
R2# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.0.2.1       192.168.2.1     QM_IDLE           1001 ACTIVE
192.168.2.1     192.0.2.1       QM_IDLE           1002 ACTIVE
192.168.3.1     192.168.2.1     QM_IDLE           1004 ACTIVE
192.168.2.1     192.168.3.1     QM_IDLE           1003 ACTIVE

IPv6 Crypto ISAKMP SA
```

e. You have successfully configured and verified IPsec on DMVPN Phase 3 tunnels.

Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Device Configs – Final

Routers R1, R2, and R3

```
enable
configure terminal
enable
conf t
crypto isakmp policy 99
 hash sha384
 encryption aes 256
 group 14
 authentication pre-share
 exit
crypto isakmp key DMVPN@key# address 0.0.0.0
crypto ipsec transform-set DMVPN_TRANS esp-aes 256 esp-sha384-hmac
 mode transport
 exit
crypto ipsec profile DMVPN_PROFILE
 set transform-set DMVPN_TRANS
 exit
interface tunnel1
 tunnel protection ipsec profile DMVPN_PROFILE
 exit
```