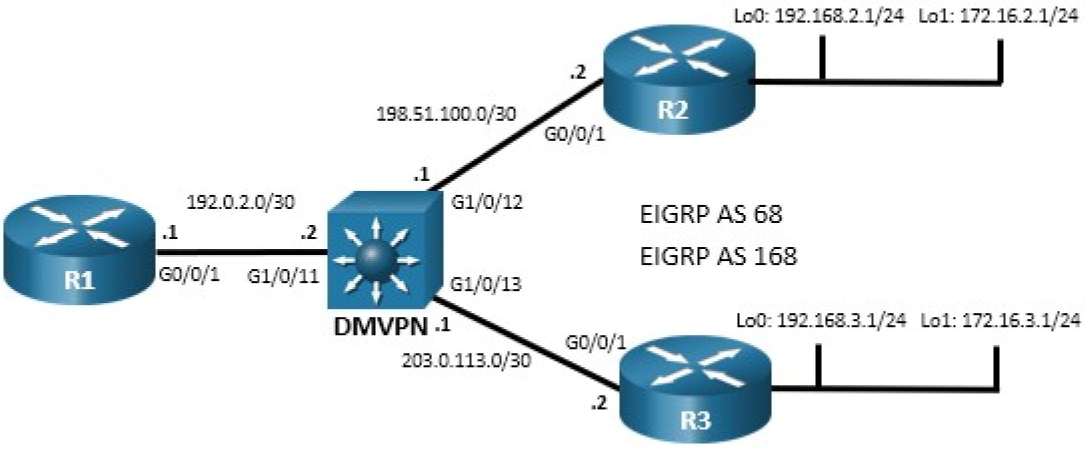
Lab - Implement a DMVPN Phase 1 Hub-to-Spoke Topology (Instructor Version)

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

Topology



Addressing Table

Device	Interface	IPv4 Address
R1	G0/0/1	192.0.2.1/30
	Tunnel 1	100.100.100.1/29
R2	G0/0/1	198.51.100.2/30
	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	203.0.113.2/30
	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 Configure Basic Device Settings

Part 2: Configure and Verify DMVPN Phase 1

Part 3: Configure EIGRP Routing for the Tunnel Networks

Background / Scenario

In this lab you will create a Dynamic Multipoint Virtual Private Network (DMVPN) that consists of a hub router with two spokes. You will implement a DMVPN Phase 1 hub-to-spoke topology.

DMVPN is a Cisco IOS Software solution for building scalable IPsec Virtual Private Networks (VPNs). Cisco DMVPN uses a centralized architecture to provide easier implementation and management for deployments that require granular access controls for diverse user communities, including mobile workers, telecommuters, and extranet users. The centralized architecture involves designating one or more routers as multipoint GRE hub routers that are used to connect spoke, or branch, routers to VPN services.

Cisco DMVPN allows branch locations to communicate directly with each other over the public WAN or internet, such as when using voice over IP (VoIP) between two branch offices, But it does not require a permanent VPN connection between sites. It enables dynamic deployment of IPsec VPNs and improves network performance by reducing latency and jitter, while optimizing head office bandwidth utilization.

DMVPN combines GRE tunnels, IPsec encryption, and Next Hop Resolution Protocol (NHRP) routing. The use of multipoint GRE (mGRE) enables a single physical interface on the hub router to support tunnel connections from multiple spoke routers, thus providing the scalability required to connect many locations over VPN to a single hub, such as at a headquarters site. Securing the VPN with crypto profiles makes it unnecessary to define static crypto maps. This enables dynamic discovery of tunnel endpoints. In addition, DMVPN enables the dynamic establishment and teardown of spoke-to-spoke tunnels when they are required. This feature will be covered in a subsequent lab.

DMVPN was released in phases that provide different capabilities to the DMVPN network.

Phase 1: This phase provides mechanisms (NHRP, mGRE) for creating the spoke-to-hub DMVPN topology. Spoke routers that are configured with NHRP register with the hub router which then dynamically creates spoke-to-hub tunnels over a single physical interface. In this phase, mGRE is only configured on the hub router, with the spoke router establishing GRE tunnels to connect to the hub. Phase 1 supported only spoke-to-hub communication, meaning that all inter-spoke tunnel traffic had to pass through the hub router and essentially traverse two tunnels.

Phase 2: This phase enabled dynamic establishment and teardown of spoke-to-spoke tunnels as required by network traffic. Spoke-to-spoke communication requires multiple tunnels to be connected on a single spoke router physical interface. To accomplish this, the spoke routers are configured with mGRE like the hub router. The hub router orchestrates the dynamic establishment of the spoke-to-spoke tunnels.

Phase 3: This phase improved upon Phase 2 by using a different mechanism for the establishment of spoke-to-spoke tunnels. In this case, instead of the hub forwarding NHRP resolution messages between the spoke endpoints, the hub creates a NHRP redirection message that is sent to the spoke that is initiating the tunnel. The spoke uses this information to establish the tunnel by forwarding the NHRP resolution request message directly to the spoke router, rather than relying on the hub to do so. This allows the spoke routers to create routing table entries for the spoke-to-spoke networks and also enables the distribution of route summaries from the hub router to the spokes. Finally, Phase 3 enables a hierarchical tree-based VPN architecture in which central hub routers connect other, regional hubs and their spokes. This allows for the establishment of tunnels between routers that are not connected to the same regional hub.

Save your configurations from this lab. You will use them as a starting point for the DMVPN Phase 3 lab that follows.

In this lab, you will configure DMVPN Phase 1.

Note: This lab does not include the configuration of IPSec to secure the tunnels. This essential procedure will be covered in a later lab.

Note: This lab is an exercise in configuring and verifying various implementations of DMVPN topologies and does not reflect networking best practices.

Note: The routers used with CCNP hands-on labs are Cisco 4221s with Cisco IOS XE Release 16.9.4 (universalk9 image). The Layer 3 switch 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.

Note: Make sure that the switches have been erased and have no startup configurations. If you are unsure, please contact your instructor.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 3 Routers (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 1 Layer 3 switch (Cisco 3650 with Cisco IOS 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

Instructions

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings.

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

Attach the devices as shown in the topology diagram, and cable as necessary.

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

a. Console into each device, enter global configuration mode, and apply the initial settings for the lab. Initial configurations for each device are provided below.

Hub Router R1

```
hostname R1
no ip domain lookup
banner motd # R1, Implement a 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
ip route 0.0.0.0 0.0.0.0 g0/0/1
interface g0/0/1
 ip address 192.0.2.1 255.255.255.252
 no shutdown
 exit
end
```

Spoke Router R2

```
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
ip route 0.0.0.0 0.0.0.0 g0/0/1
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
end
```

Spoke Router R3

```
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
ip route 0.0.0.0 0.0.0.0 g0/0/1
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
end
```

DMVPN Layer 3 Switch

```
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
 exit
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
ip route 192.168.2.0 255.255.255.0 g1/0/12
ip route 172.16.2.0 255.255.255.0 g1/0/12
ip route 192.168.3.0 255.255.255.0 g1/0/13
ip route 172.16.3.0 255.255.255.0 g1/0/13
end
```

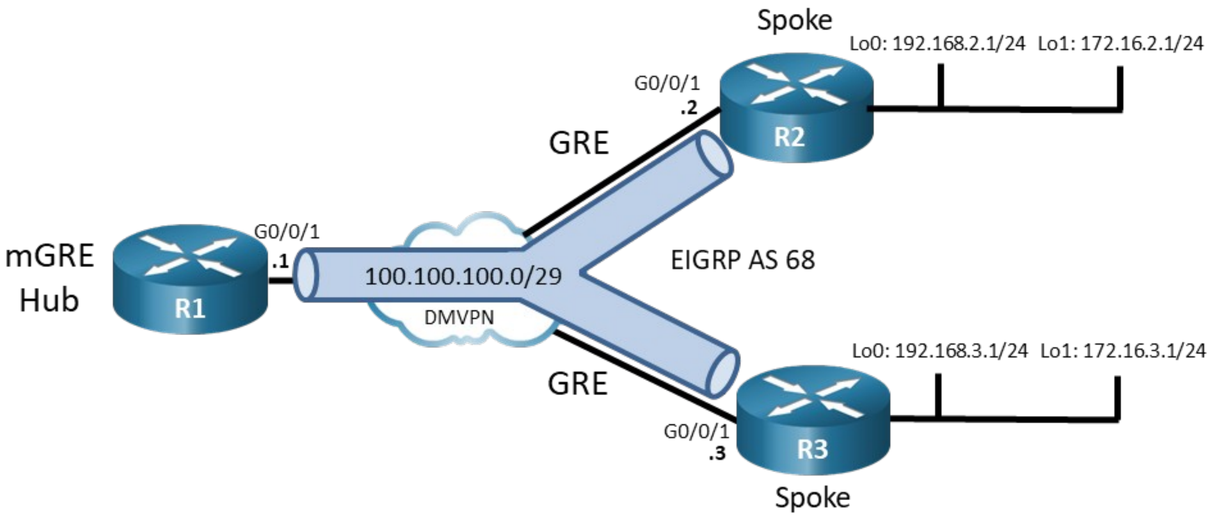
b. Set the clock on each device to UTC time.

c. Save the running configuration to the startup configuration.

Part 2: Configure and Verify DMVPN Phase 1

In this part of the lab, you will configure DMVPN Phase 1 to create DMVPN tunnels between the spoke routers R2 and R3, and the hub router, R1. DMVPN is very flexible and there are many options for implementation beyond what is being done in this lab.

In Phase 1 DMVPN, all spoke router traffic must pass through the hub router as shown in the topology diagram.



Note: In this lab, you will need to change the configuration of the DMVPN Layer 3 switch. Normally, you would not need to configure this device. The DMVPN switch is simulating the ISP transport network.

Step 1: Verify connectivity in the underlay network.

From R1, ping the Loopback 0 interfaces of R2 and R3.

```
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 2: Configure the tunnel interface on the hub router.

DMVPN requires configuration of tunnel interfaces like GRE. In fact, DMVPN Phase 1 uses GRE and mGRE mode tunnels. The hub router tunnel interface will use mGRE. This will enable it to create multiple tunnels on a single interface.

a. On R1, create the tunnel interface, set the tunnel mode to mGRE, and establish the tunnel source as Loopback 0. For DMVPN Phase 1, a tunnel key is also required when multiple tunnels will be established from a single interface. Finally, address the interface on the 100.100.100.0/29 network. The overlay network will use this subnet for all members of the DMVPN network. The hub router interface does not require a tunnel destination because it is a multipoint interface.

```
R1(config)# interface tunnel 1
R1(config-if)# tunnel mode gre multipoint
R1(config-if)# tunnel source GigabitEthernet0/0/1
R1(config-if)# tunnel key 999
R1(config-if)# ip address 100.100.100.1 255.255.255.248
```

b. Configure the hub router as a NHRP server (NHS). NHRP enables DMVPN to dynamically learn the NBMA physical addresses of devices in the network. The NHRP network ID must be consistent between the hub and spokes in the DMVPN network. You configure authentication to add a layer of security. Finally, configure the interface as multicast dynamic, which enables the hub to dynamically add spoke routers to the NHRP table when spokes initiate a tunnel. This enables the use of dynamic routing protocols between the hub and spoke routers.

```
R1(config-if)# ip nhrp network-id 1
R1(config-if)# ip nhrp authentication NHRPauth
R1(config-if)# ip nhrp map multicast dynamic
```

c. Because DMVPN networks add information to packet headers, the interface should be fine-tuned to participate in the DMVPN network. In addition, configure the interface bandwidth so that routing protocols that use bandwidth values will function properly.

```
R1(config-if)# bandwidth 4000
R1(config-if)# ip mtu 1400
R1(config-if)# ip tcp adjust-mss 1360
R1(config-if)# end
```

d. Verify the tunnel interface configuration with the **show interface tunnel 1** command.

```
R1# show interface tunnel 1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 100.100.100.1/29
  MTU 9972 bytes, BW 4000 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 192.0.2.1 (GigabitEthernet0/0/1)
   Tunnel Subblocks:
      src-track:
         Tunnel1 source tracking subblock associated with GigabitEthernet0/0/1
```

```
          Set of tunnels with source GigabitEthernet0/0/1, 1 member (includes
iterators), on interface <OK>
  Tunnel protocol/transport multi-GRE/IP
    Key 0x3E7, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1472 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:02:06
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

Step 3: Configure the R2 and R3 spoke router tunnel interfaces.

In contrast to NHS interfaces, configuration of the NHRP client (NHC) tunnel interfaces uses regular GRE and also requires the configuration of a tunnel destination address.

a. On R2, create the tunnel interface and configure the GRE tunnel parameters. Set the tunnel destination as the address of the GigabitEthernet 0/0/1 interface of the hub router. Configuring the tunnel source as the Loopback 0 interface provides a stable source for the tunnel. The tunnel key must match the key that is configured on the hub router. Finally, configure the overlay network IP address for the tunnel interface.

```
R2(config)# interface tunnel 1
R2(config-if)# tunnel mode gre ip
R2(config-if)# tunnel source loopback 0
R2(config-if)# tunnel destination 192.0.2.1
R2(config-if)# tunnel key 999
R2(config-if)# ip address 100.100.100.2 255.255.255.248
```

b. Configure the tunnel interface as an NHRP client. You will need to designate the underlay address of the NHRP server and map the NHRP server underlay address to its overlay address.

```
R2(config-if)# ip nhrp network-id 1
R2(config-if)# ip nhrp authentication NHRPauth
R2(config-if)# ip nhrp nhs 100.100.100.1
R2(config-if)# ip nhrp map multicast 192.0.2.1
R2(config-if)# ip nhrp map 100.100.100.1 192.0.2.1
```

c. Adjust settings on the interface to accommodate the GRE packet overhead.

```
R2(config-if)# ip mtu 1400
R2(config-if)# ip tcp adjust-mss 1360
```

d. Repeat this configuration on router R3 using the commands above and information from the addressing table.

```
R3(config)# interface tunnel 1
R3(config-if)# tunnel mode gre ip
R3(config-if)# tunnel source loopback 0
R3(config-if)# tunnel destination 192.0.2.1
R3(config-if)# tunnel key 999
R3(config-if)# ip address 100.100.100.3 255.255.255.248
R3(config-if)# ip nhrp network-id 1
R3(config-if)# ip nhrp authentication NHRPauth
R3(config-if)# ip nhrp nhs 100.100.100.1
R3(config-if)# ip nhrp map multicast 192.0.2.1
R3(config-if)# ip nhrp map 100.100.100.1 192.0.2.1
R3(config-if)# ip mtu 1400
R3(config-if)# ip tcp adjust-mss 1360
```

e. Verify your configurations with the **show interface** command. If your configurations are correct, you should be able to successfully ping the interface addresses of the overlay network (100.100.100.0/29) from each router.

f. View the status of DMVPN with the **show dmvpn** and **show dmvpn detail** commands. Become familiar with the output of each. The output from the hub router is shown.

```
R1# show dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

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 ""
   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 00:05:45     D   100.100.100.2/32
    1 192.168.3.1       100.100.100.3    UP 00:06:15     D   100.100.100.3/32
```

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

Pending DMVPN Sessions:
```

The output shows the status of the tunnel, the tunnel address and the tunnel source address. The table shows the NBMA (underlay) addresses of the known DMVPN peers. That address is derived from the tunnel source addresses that you configured on R2 and R3. The tunnel source is the Loopback 0 interface address. The overlay network peer tunnel interface addresses are also shown. The state of the entries in the table must be UP in order for data to travel on the tunnels. If configured, the crypto settings for the tunnel would be shown. You will secure the tunnels in a later lab.

Repeat this command on the spoke routers so that you become familiar with the command output.

g. Verify the status of NHRP by viewing the contents of the NHRP with the **show ip nhrp detail** command. Output is shown for the hub router. Note that it displays information for both of the dynamic tunnels between the spoke routers and the hub.

```
R1# show ip nhrp detail
100.100.100.2/32 via 100.100.100.2
   Tunnel1 created 00:25:06, expire 00:08:13
   Type: dynamic, Flags: registered nhop
   NBMA address: 192.168.2.1
   Preference: 255
100.100.100.3/32 via 100.100.100.3
   Tunnel1 created 00:25:36, expire 00:08:18
   Type: dynamic, Flags: registered nhop
   NBMA address: 192.168.3.1
   Preference: 255
```

Part 3: Configure EIGRP Routing for the Tunnel Networks

Cisco recommends that EIGRP be used to route DMVPN networks. Because the hub router uses a single interface to reach multiple networks, the split horizon rule will affect connectivity. For that reason, split horizon should be disabled on the hub router. Finally, improve network performance by configuring the spoke routers as stubs.

You will configure two separate EIGRP routing processes to route the overlay and underlay networks. Each network will use a different autonomous system number. Care should be taken not to route the underlay interface network using the same routing process as the overlay network. This can disrupt routing protocol operation on the hub router, severely impact performance, and possibly cause the router to crash. This condition is called recursive routing. Cisco IOS should detect recursive routing and provide syslog information regarding this error. In addition, IOS will temporarily disable the tunnel interface until recursive routing has stopped.

Step 1: Configure dynamic routing for the overlay network.

a. Remove the static routes from the three routers and the Layer 3 switch by pasting the commands below into the console of the appropriate devices.

R1, R2, and R3

```
no ip route 0.0.0.0 0.0.0.0 g0/0/1
```

DMVPN switch

```
no ip route 192.168.2.0 255.255.255.0 g1/0/12
no ip route 172.16.2.0 255.255.255.0 g1/0/12
no ip route 192.168.3.0 255.255.255.0 g1/0/13
no ip route 172.16.3.0 255.255.255.0 g1/0/13
```

b. Create a named EIGRP process with the name **DMVPN_TUNNEL_NET**. This process and AS will route the overlay network. Note that the DMVPN switch must also be configured. Add the tunnel interface and Loopback 1 interface networks to the routing process. Loopback 1 simulates a LAN that will be sending traffic through the tunnel. Note that split horizon is disabled on the hub router tunnel interface. Also note that the two hub routers are configured as stub routers. Configure the three routers as follows:

```
R1(config)# router eigrp DMVPN_TUNNEL_NET
R1(config-router)# address-family ipv4 unicast autonomous-system 68
R1(config-router-af)# eigrp router-id 1.1.1.1
R1(config-router-af)# network 100.100.100.0 255.255.255.248
R1(config-router-af)# af-interface tunnel 1
R1(config-router-af-interface)# no split-horizon

R2(config)# router eigrp DMVPN_TUNNEL_NET
R2(config-router)# address-family ipv4 unicast autonomous-system 68
R2(config-router-af)# eigrp router-id 2.2.2.2
R2(config-router-af)# network 100.100.100.0 255.255.255.248
R2(config-router-af)# network 172.16.2.0 255.255.255.0
R2(config-router-af)# eigrp stub connected

R3(config)# router eigrp DMVPN_TUNNEL_NET
R3(config-router)# address-family ipv4 unicast autonomous-system 68
R3(config-router-af)# eigrp router-id 3.3.3.3
R3(config-router-af)# network 100.100.100.0 255.255.255.248
R3(config-router-af)# network 172.16.3.0 255.255.255.0
R3(config-router-af)# eigrp stub connected
```

Step 2: Configure dynamic routing for the underlay network.

a. Create a new named EIGRP process with the name **DMVPN_TRANS_NET** with AS **168**. This process and AS will route the underlay, or transport, network. Note that the DMVPN Layer 3 switch did not need to have routing knowledge for the tunnel network. However, it does need to be configured to route between the point-to-point underlay networks. After configuring the DMVPN Layer 3 switch with EIGRP, you will see EIGRP new adjacency syslog messages on the DMVPN switch for EIGRP AS 168 and on R1, R2, and R3 for EIGRP AS 68 and EIGRP 168.

```
R1(config)# router eigrp DMVPN_TRANS_NET
R1(config-router)# address-family ipv4 unicast autonomous-system 168
R1(config-router-af)# eigrp router-id 10.1.1.1
R1(config-router-af)# network 192.0.2.0 255.255.255.252

R2(config)# router eigrp DMVPN_TRANS_NET
R2(config-router)# address-family ipv4 unicast autonomous-system 168
R2(config-router-af)# eigrp router-id 20.2.2.2
R2(config-router-af)# network 198.51.100.0 255.255.255.252
```

```
R1(config-router-af)# network 192.168.2.0 255.255.255.0
R2(config-router-af)# eigrp stub connected

R3(config)# router eigrp DMVPN_TRANS_NET
R3(config-router)# address-family ipv4 unicast autonomous-system 168
R3(config-router-af)# eigrp router-id 30.3.3.3
R3(config-router-af)# network 203.0.113.0 255.255.255.252
R3(config-router-af)# network 192.168.3.0 255.255.255.0
R3(config-router-af)# eigrp stub connected

DMVPN(config)# router eigrp DMVPN_TRANS_NET
DMVPN(config-router)# address-family ipv4 unicast autonomous-system 168
DMVPN(config-router-af)# eigrp router-id 40.4.4.4
DMVPN(config-router-af)# network 203.0.113.0 255.255.255.252
DMVPN(config-router-af)# network 192.0.2.0 255.255.255.252
DMVPN(config-router-af)# network 198.51.100.0 255.255.255.252
```

b. Verify dynamic routing on all three routers by using the **show ip route eigrp | begin Gateway** and **show ip route eigrp** commands followed by the AS number. Do this on all three routers to verify that the underlay and overlay networks appear in the routing tables for the correct AS. Output is shown for the hub router.

```
R1# show ip route eigrp | begin Gateway
Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 2 subnets
D        172.16.2.0 [90/26880640] via 100.100.100.2, 00:04:09, Tunnel1
D        172.16.3.0 [90/26880640] via 100.100.100.3, 00:04:04, Tunnel1
D     192.168.2.0/24 [90/16000] via 192.0.2.2, 00:04:14, GigabitEthernet0/0/1
D     192.168.3.0/24 [90/16000] via 192.0.2.2, 00:04:14, GigabitEthernet0/0/1
      198.51.100.0/30 is subnetted, 1 subnets
D        198.51.100.0 [90/15360] via 192.0.2.2, 00:04:14, GigabitEthernet0/0/1
      203.0.113.0/30 is subnetted, 1 subnets
D        203.0.113.0 [90/15360] via 192.0.2.2, 00:04:14, GigabitEthernet0/0/1

R1# show ip route eigrp 68 | begin Gateway
Gateway of last resort is not set

Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 2 subnets
D        172.16.2.0 [90/26880640] via 100.100.100.2, 06:04:37, Tunnel1
D        172.16.3.0 [90/26880640] via 100.100.100.3, 06:04:41, Tunnel1

R1# show ip route eigrp 168 | begin Gateway
Gateway of last resort is not set

D     192.168.2.0/24 [90/16000] via 192.0.2.2, 00:16:08, GigabitEthernet0/0/1
D     192.168.3.0/24 [90/16000] via 192.0.2.2, 00:14:55, GigabitEthernet0/0/1
```

```
      198.51.100.0/30 is subnetted, 1 subnets
D        198.51.100.0 [90/15360] via 192.0.2.2, 00:17:48, GigabitEthernet0/0/1
      203.0.113.0/30 is subnetted, 1 subnets
D        203.0.113.0 [90/15360] via 192.0.2.2, 00:17:48, GigabitEthernet0/0/1
```

Step 3: Verify DMVPN Phase 1 operation.

You have completed the configuration of DMVPN Phase 1. Verify communication as follows:

a. On R1 execute a **traceroute** to the Loopback 1 interface IP addresses on R2 and R3. You should see the path use the tunnel network.

```
R1# traceroute 172.16.2.1
Type escape sequence to abort.
Tracing the route to 172.16.2.1
VRF info: (vrf in name/id, vrf out name/id)
  1 100.100.100.2 1 msec *  1 msec
R1# 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
```

b. On R1, execute a **traceroute** to the Loopback 0 interface IP addresses on R2 and R3. You should see the path use the physical point-to-point networks of the underlay transport network.

```
R1# traceroute 192.168.2.1
Type escape sequence to abort.
Tracing the route to 192.168.2.1
VRF info: (vrf in name/id, vrf out name/id)
  1 192.0.2.2 2 msec 4 msec 1 msec
  2 198.51.100.2 1 msec *  1 msec

R1# traceroute 192.168.3.1
Type escape sequence to abort.
Tracing the route to 192.168.3.1
VRF info: (vrf in name/id, vrf out name/id)
  1 192.0.2.2 2 msec 1 msec 1 msec
  2 203.0.113.2 1 msec *  1 msec
```

c. Repeat the **traceroute** commands on R2 and R3.

d. You have successfully configured a DMVPN Phase 1 network. Save your configurations. You will use them as the starting point for the DMVPN Phase 3 lab.

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

Router R1

```
enable
configure terminal
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
 bandwidth 4000
 ip mtu 1400
 ip tcp adjust-mss 1360
 exit
no ip route 0.0.0.0 0.0.0.0 g0/0/1
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
```

Router R2

```
enable
configure terminal
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 ip
 tunnel source loopback 0
 tunnel destination 192.0.2.1
 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 mtu 1400
 ip tcp adjust-mss 1360
no ip route 0.0.0.0 0.0.0.0 g0/0/1
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

```
enable
configure terminal
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 ip
 tunnel source loopback 0
 tunnel destination 192.0.2.1
 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 mtu 1400
 ip tcp adjust-mss 1360
no ip route 0.0.0.0 0.0.0.0 g0/0/1
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

```
enable
configure terminal
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
no ip route 192.0.2.0 255.255.255.252 g1/0/11
no ip route 198.51.100.0 255.255.255.252 g1/0/12
no ip route 192.168.2.0 255.255.255.0 g1/0/12
no ip route 172.16.2.0 255.255.255.0 g1/0/12
no ip route 203.0.113.0 255.255.255.252 g1/0/13
no ip route 192.168.3.0 255.255.255.0 g1/0/13
no ip route 172.16.3.0 255.255.255.0 g1/0/13
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
```