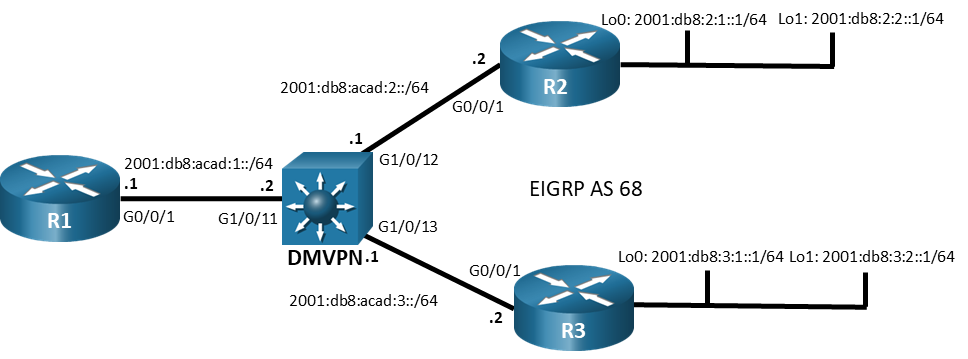
Lab - Implement an IPv6 DMVPN Phase 3 Spoke-to-Spoke Topology

# Topology



# Addressing Table

| **Device** | **Interface** | **IPv6 Address** | **Link Local** |
| --- | --- | --- | --- |
| R1 | G0/0/0 | 2001.db8:acad:1::1/64 | fe80::1 |
| R1 | Tunnel 1 | 2001:db8:cafe:100::1/64 | fe80::2001 |
| R2 | G0/0/0 | 2001:db8:acad:2::2/64 | fe80::2 |
| R2 | Loopback 0 | 2001:db8:2:1::1/64 | fe80::2 |
| R2 | Loopback 1 | 2001:db8:2:2::1/64 | fe80::2 |
| R2 | Tunnel 1 | 2001:db8:cafe:100::2/64 | fe80::2002 |
| R3 | G0/0/0 | 2001:db8:acad:3::2/64 | fe80::3 |
| R3 | Loopback 0 | 2001:db8:3:1::1/64 | fe80::3 |
| R3 | Loopback 1 | 2001:db8:3:2::1/64 | fe80::3 |
| R3 | Tunnel 1 | 2001:db8:cafe:100::3/64 | fe80::2003 |

# Objectives

In this lab, you will create a Dynamic Multipoint Virtual Private Network (DMVPN) that consists of a hub router with two spoke routers. You will implement a DMVPN Phase 3 spoke-to-spoke topology using IPv6.

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Implement IPv6 DMVPN Phase 3

Part 3: Configure EIGRP for IPv6

# Background / Scenario

In this lab you will configure IPv6 DMVPN Phase 3, which is very similar to the configuration with IPv4. Most of the tunnel and NHRP commands have direct parallels in IPv6. In addition, the configuration process and the differences between hub and spoke configuration is also similar. You will dynamically route overlay and transport networks over EIGRP for IPv6.

IPv6 DMVPN can be implemented in three different address type scenarios:

* **IPv4 over IPv6 -** IPv4 is the protocol that is used on the tunnel and IPv6 is used in the physical transport network.
* **IPv6 over IPv4 -** IPv6 is the tunnel protocol and IPv4 is the protocol that is used in the physical transport network.
* **IPv6 over IPv6 -** Both the transport and tunnel networks use IPv6.

In this lab, you will configure the IPv6 over IPv6 scenario.

**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 routers and switches have been erased and have no startup configurations. If you are unsure, please contact your instructor.

# 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

## Build the Network and Configure Basic Device Settings

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

### Cable the network as shown in the topology.

Connect the devices as shown in the topology diagram.

### Configure initial settings for each router and the Layer 3 switch.

* + - 1. 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

ipv6 unicast-routing

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

ipv6 route ::/0 2001:db8:acad:1::2

interface g0/0/1

ipv6 address 2001:db8:acad:1::1/64

ipv6 address fe80::1 link-local

no shutdown

end

Spoke Router R2

hostname R2

ipv6 unicast-routing

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

ipv6 route ::/0 2001:db8:acad:2::1

interface g0/0/1

ipv6 address 2001:db8:acad:2::2/64

ipv6 address fe80::2 link-local

no shutdown

exit

interface loopback 0

ipv6 address 2001:db8:2:1::1/64

ipv6 address fe80::2 link-local

no shutdown

exit

interface loopback 1

ipv6 address 2001:db8:2:2::1/64

ipv6 address fe80::2 link-local

no shutdown

exit

Spoke Router R3

hostname R3

ipv6 unicast-routing

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

ipv6 route ::/0 2001:db8:acad:3::1

interface g0/0/1

ipv6 address 2001:db8:acad:3::2/64

ipv6 address fe80::3 link-local

no shutdown

exit

interface loopback 0

ipv6 address 2001:db8:3:1::1/64

ipv6 address fe80::3 link-local

exit

interface loopback 1

ipv6 address 2001:db8:3:2::1/64

ipv6 address fe80::3 link-local

exit

end

DMVPN Layer 3 Switch

hostname DMVPN

ipv6 unicast-routing

ip routing

no ip domain lookup

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

ipv6 address 2001:db8:acad:1::2/64

ipv6 address fe80::4 link-local

no shutdown

exit

interface g1/0/12

no switchport

ipv6 address 2001:db8:acad:2::1/64

ipv6 address fe80::4 link-local

no shutdown

exit

interface g1/0/13

no switchport

ipv6 address 2001:db8:acad:3::1/64

ipv6 address fe80::4 link-local

no shutdown

exit

ipv6 route 2001:db8:2:1::/64 2001:db8:acad:2::2

ipv6 route 2001:db8:2:2::/64 2001:db8:acad:2::2

ipv6 route 2001:db8:3:1::/64 2001:db8:acad:3::2

ipv6 route 2001:db8:3:2::/64 2001:db8:acad:3::2

end

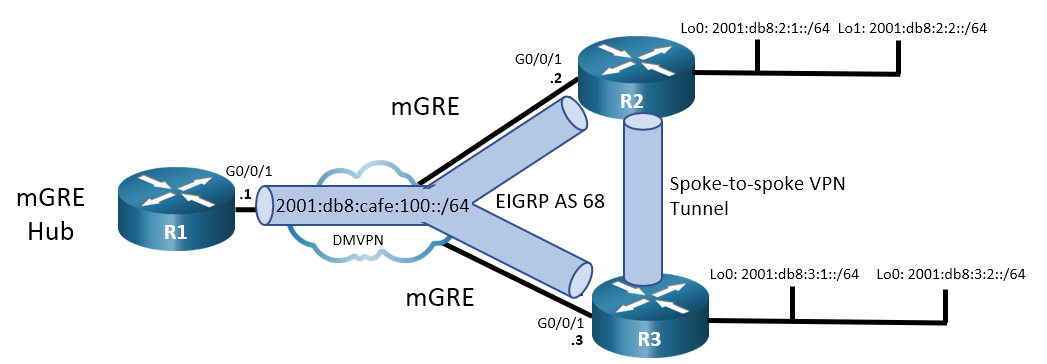
* + - 1. Set the clock on each device to UTC time.
      2. Save the running configuration to the startup configuration.

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

## Implement IPv6 DMVPN Phase 3

In this part of the lab, you will configure IPv6 DMVPN Phase 3 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 3 DMVPN, dynamic IPv6 spoke-to-spoke tunnels will be created between spoke routers after the initiating spoke router sends initial traffic to the hub.



### Verify connectivity in the underlay network.

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

Open configuration window

R1# **ping 2001:db8:2:1::1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:DB8:2:1::1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R1# **ping 2001:db8:3:1::1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:DB8:3:1::1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

### Configure the tunnel interface on the hub router.

As you know, DMVPN requires configuration of tunnel interfaces like GRE. Unlike GRE tunnels, DMVPN Phase 3 uses multipoint GRE (mGRE) mode tunnels. When configuring tunnel interfaces, care must be taken to use unique IPv6 link local addresses on all tunnel interfaces. The tunnel interfaces do not require a tunnel destination because the tunnel interfaces are multipoint.

* + - 1. On R1, create the tunnel interface, set the tunnel mode to mGRE, and establish the tunnel source as Loopback 0. A tunnel key is also required when multiple tunnels will be established from a single interface. Finally, address the interface. The overlay network will use the same IPv6 network for all tunnel interfaces of the DMVPN.

R1(config)# **interface tunnel 1**

R1(config-if)# **tunnel mode gre multipoint ipv6**

R1(config-if)# **tunnel source GigabitEthernet0/0/1**

R1(config-if)# **tunnel key 999**

R1(config-if)# **ipv6 address 2001:db8:cafe:100::1/64**

R1(config-if)# **ipv6 address fe80::2001 link-local**

* + - 1. Configure the hub router as a NHRP server (NHS). Spoke routers require the services of the NHS to establish dynamic tunnels.

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 NHS 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.

The **ipv6 nhrp redirec**t command is required to enable the hub router to support DMVPN Phase 3.

R1(config-if)# **ipv6 nhrp network-id 1**

R1(config-if)# **ipv6 nhrp authentication NHRPauth**

R1(config-if)# **ipv6 nhrp map multicast dynamic**

R1(config-if)# **ipv6 nhrp redirect**

* + - 1. 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)# **ipv6 mtu 1380**

R1(config-if)# **ipv6 tcp adjust-mss 1360**

* + - 1. Verify the tunnel interface configuration with the **show interface tunnel 1** and **show ipv6 interface tunnel 1** commands.

R1# **show interface tunnel 1**

Tunnel1 is up, line protocol is up

Hardware is Tunnel

MTU 1452 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 2001:DB8:ACAD:1::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/IPv6

Key 0x3E7, sequencing disabled

Checksumming of packets disabled

Tunnel TTL 255

Path MTU Discovery, ager 10 mins, min MTU 1280

Tunnel transport MTU 1452 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 00:02:45

Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 20

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

R1# **show ipv6 interface tunnel 1**

Tunnel1 is up, line protocol is up

IPv6 is enabled, link-local address is FE80::2001

No Virtual link-local address(es):

Global unicast address(es):

2001:DB8:CAFE:100::1, subnet is 2001:DB8:CAFE:100::/64

Joined group address(es):

FF02::1

FF02::2

FF02::1:FF00:1

FF02::1:FF00:2001

MTU is 1380 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachables are sent

Input features: IPv6 TCP Adjust MSS

Output features: IPv6 TCP Adjust MSS

ND DAD is not supported

ND reachable time is 30000 milliseconds (using 30000)

ND advertised reachable time is 0 (unspecified)

ND advertised retransmit interval is 0 (unspecified)

ND router advertisements live for 1800 seconds

ND advertised default router preference is Medium

ND RAs are suppressed (periodic)

Hosts use stateless autoconfig for addresses.

Close configuration window

### Configure the R2 and R3 spoke router tunnel interfaces.

In DMVPN Phase 3, the NHRP client (NHC) tunnel interfaces use mGRE as does the NHS hub router. Much of the interface configuration is the same as for the NHS tunnel interface. However, instead of the interfaces being configured to send NHRP redirect messages, the interfaces are configured to create shortcuts, or spoke-to-spoke tunnels.

* + - 1. On R2, create the tunnel interface and configure the mGRE tunnel parameters. 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. Configure the overlay network IPv6 addresses for the tunnel interface. Note that no static tunnel destination is configured, because these are multipoint interfaces.

Open configuration window

R2(config)# **interface tunnel 1**

R2(config-if)# **tunnel mode gre multipoint ipv6**

R2(config-if)# **tunnel source loopback 0**

R2(config-if)# **tunnel key 999**

R2(config-if)# **ipv6 address 2001:db8:cafe:100::2/64**

R2(config-if)# **ipv6 address fe80::2002 link-local**

* + - 1. 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)# **ipv6 nhrp network-id 1**

R2(config-if)# **ipv6 nhrp authentication NHRPauth**

R2(config-if)# **ipv6 nhrp nhs 2001:db8:cafe:100::1 nbma 2001:db8:acad:1::1 multicast**

R2(config-if)# **ipv6 nhrp map multicast dynamic**

R2(config-if)# **ipv6 nhrp shortcut**

* + - 1. Adjust settings on the interface to accommodate the GRE packet overhead.

R2(config-if)# **bandwidth 4000**

R2(config-if)# **ipv6 mtu 1380**

R2(config-if)# **ipv6 tcp adjust-mss 1360**

Close configuration window

* + - 1. Repeat this configuration on router R3 using the commands above and information from the addressing table.

Open configuration window

Close configuration window

* + - 1. 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 from each router.
      2. Go to R1 and view the status of DMVPN with the **show dmvpn** and **show dmvpn detail** commands. Become familiar with the output of each.

Open configuration window

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 2001:DB8:CAFE:100::1, VRF ""

Tunnel Src./Dest. addr: 2001:DB8:ACAD:1::1/Multipoint, Tunnel VRF ""

Protocol/Transport: "multi-GRE/IPv6", Protect ""

Interface State Control: Disabled

nhrp event-publisher : Disabled

Type:Hub, Total NBMA Peers (v4/v6): 2

1.Peer NBMA Address: 2001:DB8:2:1::1

Tunnel IPv6 Address: 2001:DB8:CAFE:100::2

IPv6 Target Network: 2001:DB8:CAFE:100::2/128

# Ent: 2, Status: UP, UpDn Time: 00:12:54, Cache Attrib: D

2.Peer NBMA Address: 2001:DB8:2:1::1

Tunnel IPv6 Address: 2001:DB8:CAFE:100::2

IPv6 Target Network: FE80::2002/128

# Ent: 0, Status: UP, UpDn Time: 00:12:54, Cache Attrib: D

3.Peer NBMA Address: 2001:DB8:3:1::1

Tunnel IPv6 Address: 2001:DB8:CAFE:100::3

IPv6 Target Network: 2001:DB8:CAFE:100::3/128

# Ent: 2, Status: UP, UpDn Time: 00:06:32, Cache Attrib: D

4.Peer NBMA Address: 2001:DB8:3:1::1

Tunnel IPv6 Address: 2001:DB8:CAFE:100::3

IPv6 Target Network: FE80::2003/128

# Ent: 0, Status: UP, UpDn Time: 00:06:32, Cache Attrib: D

Crypto Session Details:

-----------------------------------------------------------------------------

Pending DMVPN Sessions:

Close configuration window

The output shows the status of the tunnel, the tunnel address and the tunnel source address. The list of peers shows the NBMA (underlay) addresses of the DMVPN peers that were learned by NHRP. These addresses come from the tunnel source Loopback 0 addresses. Although there are only two peers known (R2 and R3), there are two entries for each. The first entry shows the tunnel target network interface address, and the second gives the link local address. The status of the entries in the table must be UP for data to travel on the tunnels. The attribute D indicates the tunnels are dynamic. 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.

* + - 1. Verify the status of NHRP by viewing the contents of the NHRP cache with the **show ipv6 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.

Open configuration window

R1# **show ipv6 nhrp detail**

2001:DB8:CAFE:100::2/128 via 2001:DB8:CAFE:100::2

Tunnel1 created 00:27:29, expire 00:07:21

Type: dynamic, Flags: registered nhop

NBMA address: 2001:DB8:2:1::1

Preference: 255

2001:DB8:CAFE:100::3/128 via 2001:DB8:CAFE:100::3

Tunnel1 created 00:21:07, expire 00:08:52

Type: dynamic, Flags: registered nhop

NBMA address: 2001:DB8:3:1::1

Preference: 255

FE80::2002/128 via 2001:DB8:CAFE:100::2

Tunnel1 created 00:27:29, expire 00:07:21

Type: dynamic, Flags: registered

NBMA address: 2001:DB8:2:1::1

Preference: 255

FE80::2003/128 via 2001:DB8:CAFE:100::3

Tunnel1 created 00:21:07, expire 00:08:52

Type: dynamic, Flags: registered

NBMA address: 2001:DB8:3:1::1

Preference: 255

Close configuration window

This output provides details about the tunnel endpoints that are known to NHRP. This incudes the overlay and transport interface addresses for the known peers.

## Configure EIGRP for IPv6

In this scenario, you will create two EIGRP for IPv6 routing processes for two different ASs. AS 68 will route the tunnel network and the LANs to be accessed across the tunnels. AS 168 will route the transport network in order to ensure connectivity between the underlay networks that the tunnel network relies upon.

Initially, static routes were configured in the topology to enable initial testing of network connectivity after the topology was set up for the lab. You no longer need these static routes and will replace them with EIGRPv6.

### Remove static routes.

* + - 1. Remove the preconfigured static routes from the three routers by pasting the commands below into the console of the appropriate devices.

Open configuration window

R1

**no ipv6 route ::/0 2001:db8:acad:1::2**

R2

**no ipv6 route ::/0 2001:db8:acad:2::1**

R3

**no ipv6 route ::/0 2001:db8:acad:3::1**

DMVPN

**no ipv6 route 2001:db8:2:1::/64 2001:db8:acad:2::2**

**no ipv6 route 2001:db8:2:2::/64 2001:db8:acad:2::2**

**no ipv6 route 2001:db8:3:1::/64 2001:db8:acad:3::2**

**no ipv6 route 2001:db8:3:2::/64 2001:db8:acad:3::2**

Close configuration window

**Note**: Normally devices in the DMVPN cloud would require no intervention from enterprise networking staff. However, for the purposes of this lab, some configuration of the DMVPN Layer 3 switch is required.

* + - 1. Create classic mode IPv6 EIGRP processes with AS **68**. This process and AS will route the overlay network. 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 and spoke router tunnel interfaces. Also note that the two spoke routers are configured as stub routers. Configure the three routers as follows:

Open configuration window

R1(config)# **ipv6** **router eigrp 68**

R1(config-router)# **eigrp router-id 1.1.1.1**

R1(config-router)# **interface tunnel 1**

R1(config-if)# **ipv6 eigrp 68**

R1(config-if)# **no ipv6 split-horizon eigrp 68**

Close configuration window

Open configuration window

R2(config)# **ipv6 router eigrp 68**

R2(config-router)# **eigrp router-id 2.2.2.2**

R2(config-router)# **interface tunnel 1**

R2(config-if)# **ipv6 eigrp 68**

R2(config-if)# **no ipv6 split-horizon eigrp 68**

R2(config-if)# **interface loopback 1**

R2(config-if)# **ipv6 eigrp 68**

Close configuration window

Open configuration window

R3(config)# **ipv6 router eigrp 68**

R3(config-router)# **eigrp router-id 3.3.3.3**

R3(config-router)# **interface tunnel 1**

R3(config-if)# **ipv6 eigrp 68**

R3(config-if)# **no ipv6 split-horizon eigrp 68**

R3(config-if)# **interface loopback 1**

R3(config-if)# **ipv6 eigrp 68**

Close configuration window

### Configure dynamic routing for the underlay network.

* + - 1. Create new classic mode EIGRP processes for 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. Split horizon does not need to be disabled for this AS because the underlay network is a point-to-point network.

Open configuration window

R1(config)# **ipv6** **router eigrp 168**

R1(config-router)# **eigrp router-id 10.1.1.1**

R1(config-router)# **interface GigabitEthernet 0/0/1**

R1(config-if)# **ipv6 eigrp 168**

Close configuration window

Open configuration window

R2(config)# **ipv6** **router eigrp 168**

R2(config-router)# **eigrp router-id 20.2.2.2**

R2(config-router)# **interface GigabitEthernet 0/0/1**

R2(config-if)# **ipv6 eigrp 168**

R2(config-if)# **interface loopback 0**

R2(config-if)# **ipv6 eigrp 168**

Close configuration window

Open configuration window

R3(config)# **ipv6** **router eigrp 168**

R3(config-router)# **eigrp router-id 30.3.3.3**

R3(config-router)# **interface GigabitEthernet 0/0/1**

R3(config-if)# **ipv6 eigrp 168**

R3(config-if)# **interface loopback 0**

R3(config-if)# **ipv6 eigrp 168**

Close configuration window

Open configuration window

DMVPN(config)# **ipv6 router eigrp 168**

DMVPN(config-router)# **eigrp router-id 40.4.4.4**

DMVPN(config-router)# **interface GigabitEthernet 1/0/11**

DMVPN(config-if)# **ipv6 eigrp 168**

DMVPN(config-router)# **interface GigabitEthernet 1/0/12**

DMVPN(config-if)# **ipv6 eigrp 168**

DMVPN(config-router)# **interface GigabitEthernet 1/0/13**

DMVPN(config-if)# **ipv6 eigrp 168**

Close configuration window

**Note**: Normally devices in the DMVPN cloud would require no intervention from enterprise networking staff. However, for the purposes of this lab, some configuration of the DMVPN Layer 3 switch is required.

* + - 1. Verify dynamic routing on all three routers by using the **show ipv6 route eigrp** command. Do this on all three routers to verify that the underlay and overlay networks appear in the routing tables. Output is shown for the hub router.

Open configuration window

R1# **show ipv6 route eigrp**

<output omitted>

D 2001:DB8:2:1::/64 [90/131072]

via FE80::4, GigabitEthernet0/0/1

D 2001:DB8:2:2::/64 [90/2048000]

via FE80::2002, Tunnel1

D 2001:DB8:3:1::/64 [90/131072]

via FE80::4, GigabitEthernet0/0/1

D 2001:DB8:3:2::/64 [90/2048000]

via FE80::2003, Tunnel1

D 2001:DB8:ACAD:2::/64 [90/3072]

via FE80::4, GigabitEthernet0/0/1

D 2001:DB8:ACAD:3::/64 [90/3072]

via FE80::4, GigabitEthernet0/0/1

Close configuration window

### Verify DMVPN Phase 3 operation.

You have completed configuration of DMVPN Phase 3. Verify communication as follows:

* + - 1. 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.

Open configuration window

R1# **traceroute 2001:db8:2:2::1**

Type escape sequence to abort.

Tracing the route to 2001:DB8:2:2::1

1 2001:DB8:CAFE:100::2 2 msec 1 msec 1 msec

R1# **traceroute 2001:db8:3:2::1**

Type escape sequence to abort.

Tracing the route to 2001:DB8:3:2::1

1 2001:DB8:CAFE:100::3 1 msec 1 msec 1 msec

Close configuration window

* + - 1. 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.

Open configuration window

R1# **traceroute 2001:db8:2:1::1**

Type escape sequence to abort.

Tracing the route to 2001:DB8:2:1::1

1 2001:DB8:ACAD:1::2 2 msec 1 msec 2 msec

2 2001:DB8:ACAD:2::2 1 msec 0 msec 0 msec

R1# **traceroute 2001:db8:3:1::1**

Type escape sequence to abort.

Tracing the route to 2001:DB8:3:1::1

1 2001:DB8:ACAD:1::2 2 msec 2 msec 1 msec

2 2001:DB8:ACAD:3::2 1 msec 1 msec 1 msec

Close configuration window

* + - 1. Repeat the traceroute commands between R2 and R3.

### Observe dynamic tunnel creation.

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

Open configuration window

R2# **traceroute 2001:db8:3:2::1**

Type escape sequence to abort.

Tracing the route to 2001:DB8:3:2::1

1 2001:DB8:CAFE:100::1 1 msec 1 msec 1 msec

2 2001:DB8:CAFE:100::3 2 msec 1 msec

Close configuration window

* + - 1. Issue the **traceroute** command again. You will now see that DMVPN hub, R1, has enabled direct spoke-to-spoke communication between R2 and R3. R1 is no longer in the path, instead, the path is directly to R3. This tunnel will expire after ten minutes by default. The tunnel dynamically reopens after data is sent to the spoke router again.

Open configuration window

R2# **traceroute 2001:db8:3:2::1**

Type escape sequence to abort.

Tracing the route to 2001:DB8:3:2::1

1 2001:DB8:CAFE:100::3 1 msec 1 msec 1 msec

Close configuration window

* + - 1. You have successfully configured a DMVPN Phase 3 network. Feel free to explore the IPv6 versions of the DMVPN Phase 3 verification commands you used for IPv4 DMVPN.

# 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) |
| 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.

*End of document*