## Practical 3

Configuring EtherChannels

Suggested Topology

**Aim: Implement EtherChannel** Step 1: Design the Topology.

Step 2: Configure the network.

Examine the default port status and manipulate DTP.

Switch D1:

Switch A1:

Change the administrative mode of interface f0/1 on A1 to Dynamic Desirable with the interface configuration command switchport mode dynamic desirable. Then check the interface switchport status and you will see that it is in trunk mode. The output of show interfaces trunk will show the protocol as desirable. The output of show interfaces trunk on D1 will show auto.

To see this, configure D1 interface g1/0/6 with the switchport mode trunk command. Then you should once again see that A1 has automatically negotiated a trunk, this time between f0/2 and D1 g1/0/6.

Then go to D1 and configure interfaces g1/0/5 and g1/0/6 as trunks with the additional command switchport nonegotiate. Then you re- enable the interfaces at A1, you will see that they do not form trunks with D1.

At each switch, issue the global configuration command default interface range first-int-id last-int-id to reset the interfaces back to their defaults.

Configure Basic Device Settings Switch D1:

Switch D2:

Switch A1:

Step 3: Configure Static EtherChannel.

• Configure and verify trunking between D2 and A1. Verify the trunks have formed.

Configure and verify a static EtherChannel link between D2 and A1.

Add the command channel-group 1 mode on to all the trunk interfaces between D2 and A1.

Verify the EtherChannel has formed by examining the output of the show ether channel summary command. Also check the spanning tree status. You will see that there is a change to the topology because Po1 replaced interfaces F0/3 and F0/4 with a lower cost.

Make a change to the EtherChannel.

On D2 and A1, create VLAN 999 with the name NATIVE\_VLAN.

On D2 and A1, modify interface port-channel 1 so that it uses VLAN 999 as the native VLAN.

Verify the change has been applied by examining the output of show interfaces trunk.

Step 4: Implement EtherChannel Using PAgP.

Configure and verify trunking between D1 and A1. Verify the trunks are still working.

Configure and verify an EtherChannel using PAgP between D1 and A1.

Add the command channel-group 2 mode desirable non-silent to all the trunk interfaces between D1 and A1.

Verify the EtherChannel has formed by examining the output of the show etherchannel summary command.

Make a change to the EtherChannel.

On D1, create VLAN 999 with the name NATIVE\_VLAN.

On D1 and A1, modify interface port-channel 2 so that it uses VLAN 999 as the native VLAN.

Verify the change has been applied by examining the output of show interfaces trunk | iPort|Po3.

Step 5: Implement EtherChannel using LACP.

• Configure and verify trunking between D1 and D2. Verify the trunks are still operational.

Configure and verify an EtherChannel using LACP between D1 and D2.

Add the command channel-group 4 mode active to all the trunk interfaces between D1 and D2.

Make a change to the EtherChannel.

On D1 and D2, modify interface port-channel 4 so that it uses VLAN 999 as the native VLAN.

Verify the change has been applied by examining the output of show interfaces trunk | iPort|Po4.

**Practical 4**

* Configure Secure DMVPN Tunnels
* Implement a DMVPN Phase 1 Hub-to-Spoke Topology
* Implement a DMVPN Phase 3 Spoke-to-Spoke Topology

## A) Configure Secure DMVPN Tunnels

Addressing Table

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

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.

*Close configuration window*

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.

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

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

*Close configuration window*

Part 3: Configure EIGRP Routing for the Tunnel Networks

Step 1: Configure dynamic routing for the overlay network.

Step 2: Configure dynamic routing for the underlay network.

Step 3: Verify DMVPN Phase 1 operation.

## 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) |

## B) Implement a DMVPN Phase 1 Hub-to-Spoke Topology

## Addressing Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** |  | **Interface** | **IPv4 Address** |
| R1  *R1* | G0/0/1 |  | 192.0.2.1/30 |
| Tunnel 1 |  | 100.100.100.1/29 |
| R2  *R2*  *R2*  *R2* | G0/0/1 |  | 198.51.100.2/30 |
| Loopback 0 |  | 192.168.2.1/24 |
| Loopback 1 |  | 172.16.2.1/24 |
| Tunnel 1 |  | 100.100.100.2/29 |
| R3  *R3*  *R3*  *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 |

Part 1: Build the Network and Configure Basic Device Settings

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 **Lab - Implement a DMVPN Phase 1 Hub-to-Spoke Topology**.

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.

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.

Part 2: Configure DMVPN Phase 3

Step 1: Modify the tunnel interfaces on the spoke routers.

Step 2: Modify the configuration on the spoke routers to enable NHRP routing shortcuts.

Step 3: Modify the configuration of hub router to send NHRP redirect messages.

Part 3: Verify DMVPN Phase 3

Step 1: Observe dynamic tunnel creation.

Step 2: View the routing table.

Step 3: Verify the DMVPN

Step 4: View NHRP Mappings

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) |

### C) Implement a DMVPN Phase 3 Spoke-to-Spoke Topology

**Addressing Table**

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** |  | **Interface** | **IPv4 Address** |
| R1  *R1* | G0/0/1 |  | 192.0.2.1/24 |
| Tunnel 1 |  | 100.100.100.1/29 |
| R2  *R2*  *R2*  *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  *R3*  *R3*  *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 |

**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.**

**Lab - Configure Secure DMVPN Tunnels**

**Step 3: Verify connectivity in the network.**

**Step 4: Verify DMVPN Phase 3 operation.**

**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.**

**Step 2: Configure the ISAKMP key.**

**Step 3: Create and configure the IPsec transform set.**

**Step 4: Create the IPsec profile.**

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

**Step 6: Configure R2 and R3 with IPsec.**

**Step 7: Verify DMVPN Phase 3 operation.**

**Step 8: Verify IPsec configuration.**

**Step 9: You have successfully configured and verified IPsec on DMVPN Phase 3 tunnels.**

**Practical 5**

### A) Implement BGP Communities

**Addressing Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IPv4 Address** | **IPv6 Address** | **IPv6 Link-Local** |
| R1  *R1*  *R1*  *R1*  *R1* | G0/0/0 | 10.1.2.1/24 | 2001:db8:acad:1012::1/64 | fe80::1:1 |
| S0/1/0 | 10.1.3.1/25 | 2001:db8:acad:1013::1/64 | fe80::1:2 |
| S0/1/1 | 10.1.3.129/25 | 2001:db8:acad:1014::1/64 | fe80::1:3 |
| Loopback0 | 192.168.1.1/27 | 2001:db8:acad:1000::1/64 | fe80::1:4 |
| Loopback1 | 192.168.1.65/26 | 2001:db8:acad:1001::1/64 | fe80::1:5 |
| R2  *R2*  *R2*  *R2* | G0/0/0 | 10.1.2.2/24 | 2001:db8:acad:1012::2/64 | fe80::2:1 |
| G0/0/1 | 10.2.3.2/24 | 2001:db8:acad:1023::2/64 | fe80::2:2 |
| Loopback0 | 192.168.2.1/27 | 2001:db8:acad:2000::1/64 | fe80::2:3 |
| Loopback1 | 192.168.2.65/26 | 2001:db8:acad:2001::1/64 | fe80::2:4 |
| R3  *R3*  *R3*  *R3*  *R3* | G0/0/0 | 10.2.3.3/24 | 2001:db8:acad:1023::3/64 | fe80::3:1 |
| S0/1/0 | 10.1.3.3/25 | 2001:db8:acad:1013::3/64 | fe80::3:2 |
| S0/1/1 | 10.1.3.130/25 | 2001:db8:acad:1014::3/64 | fe80::3:3 |
| Loopback0 | 192.168.3.1/27 | 2001:db8:acad:3000::1/64 | fe80::3:4 |
| Loopback1 | 192.168.3.65/26 | 2001:db8:acad:3001::1/64 | fe80::3:5 |

**Instructions**

Build the Network and Configure Basic Device Settings and Interface Addressing

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

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

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

Part 2: Configure basic settings for each router.

a. Console into each router, enter global configuration mode, and apply the basic settings and interface addressing. A command list for each router is listed below for initial configuration.

Configure and Verify Multi-Protocol BGP on all Routers

In Part 2, you will configure and verify Multi-Protocol BGP on all routers to achieve full connectivity between the routers. The text below provides you with the complete configuration for R1. You will use this to inform your configuration of R2 and R3. The configuration being used here is not meant to represent best practice, but to assess your ability to complete the required configurations.

Part 1: On R1, create the core BGP configuration.

Part 2: On R1, configure the IPv4 unicast address family.

Part 3: On R1, configure the IPv6 unicast address family.

Part 4: Verify that MP-BGP is operational.

Configure and Verify BGP Communities on all Routers

Part 1: Configure all routers to send community information.

Part 2: Configure and verify the effect of the no-export community.

Part 3: Add private community information to routes advertised by R1.

Part 4: Configure community-based route filtering and manipulation.

### B) Implement BGP Path Manipulation

### Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IPv4 Address** | **IPv6 Address** | **IPv6 Link-Local** |
| R1  *R1*  *R1*  *R1*  *R1* | G0/0/0 | 10.1.2.1/24 | 2001:db8:acad:1012::1/64 | fe80::1:1 |
| S0/1/0 | 10.1.3.1/25 | 2001:db8:acad:1013::1/64 | fe80::1:2 |
| S0/1/1 | 10.1.3.129/25 | 2001:db8:acad:1014::1/64 | fe80::1:3 |
| Loopback0 | 192.168.1.1/27 | 2001:db8:acad:1000::1/64 | fe80::1:4 |
| Loopback1 | 192.168.1.65/26 | 2001:db8:acad:1001::1/64 | fe80::1:5 |
| R2  *R2*  *R2*  *R2* | G0/0/0 | 10.1.2.2/24 | 2001:db8:acad:1012::2/64 | fe80::2:1 |
| G0/0/1 | 10.2.3.2/24 | 2001:db8:acad:1023::2/64 | fe80::2:2 |
| Loopback0 | 192.168.2.1/27 | 2001:db8:acad:2000::1/64 | fe80::2:4 |
| Loopback1 | 192.168.2.65/26 | 2001:db8:acad:2001::1/64 | fe80::2:4 |
| R3  *R3*  *R3*  *R3*  *R3* | G0/0/0 | 10.2.3.3/24 | 2001:db8:acad:1023::3/64 | fe80::3:1 |
| S0/1/0 | 10.1.3.3/25 | 2001:db8:acad:1013::3/64 | fe80::3:2 |
| S0/1/1 | 10.1.3.130/25 | 2001:db8:acad:1014::3/64 | fe80::3:3 |
| Loopback0 | 192.168.3.1/27 | 2001:db8:acad:3000::1/64 | fe80::3:4 |
| Loopback1 | 192.168.3.65/26 | 2001:db8:acad:3001::1/64 | fe80::3:5 |

## Instructions

Part 1: Build the Network and Configure Basic Device Settings and Interface Addressing

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

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 basic settings for each router.

a. Console into each router, enter global configuration mode, and apply the basic settings and interface addressing. A command list for each router is listed below to perform initial configuration.

Part 2: Configure and Verify Multi-Protocol BGP on all Routers

In Part 2, you will configure and verify Multi-Protocol BGP on all routers to achieve full connectivity between the routers. The text below provides you with the complete configuration for R1. You will use this to inform your configuration of R2 and R3. The configuration being used here is not meant to represent best practice, but to assess your ability to complete the required configurations.

Step 1: On R1, create the core BGP configuration.

Step 2: On R1, configure the IPv4 unicast address family.

Step 3: On R1, configure the IPv6 unicast address family.

Step 4: Configure MP-BGP on R2 and R3 as you did in the previous step.

Step 5: Verify that MP-BGP is operational.

Part 3: Configure and Verify BGP Path Manipulation Settings on all Routers

In Part 3, you will configure path manipulation tools for BGP. The way these tools are being used here is not meant to represent best practice, but to assess your ability to complete the required configurations.

Step 1: Configure ACL-based route filtering.

Step 2: Configure prefix-list-based route filtering.

Step 3: Configure an AS-PATH ACL to filter routes being advertised.

Step 4: Configure IPv6 prefix-list-based route filtering.

Step 5: Configure BGP path attribute manipulation to effect routing.

**Practical 6**

### A) Control Routing Updates

Instructions

**Part 1: Build the Network and Configure Basic Device Settings** Step 1: Cable the network as shown in the topology. Step 2: Configure basic settings for each device.

**Part 2: Configure Routing and Redistribution** Step 1: Configure Routing.

Step 2: Verify EIGRP and OSPF routing

Step 3: Configure Redistribution on R2

Step 4: Verify Redistribution

**Part 3: Filter Redistributed Routes using a Distributed List and ACL.**

Step 1: Configure an ACL and distribute list on R2

Step 2: Verify the configuration

**Part 4: Filter Redistributed Routes using a Distribute List and Prefix List** Step 1: Filter redistributed routes using a distributed list and prefix list.

**Part 5: Filter Redistributed Routes using a Route Map.**

Step 1: Filter redistributed routes using a route map.

Step 2: Filter redistributed routes and set attributes using a route map.

### B) Path Control Using PBR

**Instructions**

**Part 1: Build the Network and Configure Basic Device Settings** Step 1: Cable the network as shown in the topology.

Step 2: Configure basic settings for each device.

**Part 2: Configure and Verify Routing** Step 1: Configure Routing.

Step 2: Verify OSPF routing

Step 3: Verify end-to-end connectivity and path taken

**Part 3: Configure PBR to Provide Path Control** Step 1: Configure PBR on R1.

Step 2: Test the policy.

**Part 4: Configure Local PBR to Provide Path Control** Step 1: Configure Local PBR on R1. Step 2: Test Local PBR on R1.

**Practical 7**

### Implement MPLS

Cisco MPLS Configuration

Step 1 – IP addressing of MPLS Core and OSPF

First bring 3 routers into your topology R1, R2, R3 position them as below. We are going to address the routers and configure ospf to ensure loopback to loopback connectivity between R1 and R3

You should now have full ip connectivity between R1, R2, R3 to verify this we need to see if we can ping between the loopbacks of R1 and R3

You could show the routing table here, but the fact that you can ping between the loopbacks is verification enough and it is safe to move on.

Step 2 – Configure LDP on all the interfaces in the MPLS Core

In order to run MPLS you need to enable it, there are two ways to do this.

* At each interface enter the mpls ip command
* Under the ospf process use the mpls ldp autoconfig command

For this tutorial we will be using the second option, so go int the ospf process and enter mpls ldp autoconfig – this will enable mpls label distribution protocol on every interface running ospf under that specific process.

You should see log messages coming up showing the LDP neighbors are up.

To verify the mpls interfaces the command is very simple – sh mpls interface This is done on R2 and you can see that both interfaces are running mpls and using LDP

You can also verify the LDP neighbors with the sh mpls ldp neighbors command.

One more verification to confirm LDP is running ok is to do a trace between R1 and R3 and verify if you get MPLS Labels show up in the trace.

As you can see the trace to R2 used an MPLS Label in the path, as this is a very small MPLS core only one label was used as R3 was the final hop.

So to review we have now configured IP addresses on the MPLS core, enabled OSPF and full IP connectivity between all routers and finally enabled mpls on all the interfaces in the core and have established ldp neighbors between all routers.

The next step is to configure MP-BGP between R1 and R3

This is when you start to see the layer 3 vpn configuration come to life

Step 3 – MPLS BGP Configuration between R1 and R3

We need to establish a MultiProtocol BGP session between R1 and R3 this is done by configuring the vpnv4 address family as below

You should see log messages showing the BGP sessions coming up.

To verify the BGP session between R1 and R3 issue the command sh bgp vpnv4 unicast all summary

You can see here that we do have a bgp vpnv4 peering to R3 – looking at the PfxRcd you can see it says 0 this is because we have not got any routes in BGP. We are now going to add two more routers to the topology. These will be the customer sites connected to R1 and R3. We will then create a VRF on each router and put the interfaces connected to each site router into that VRF.

Step 4 – Add two more routers, create VRFs

We will add two more routers into the topology so it now looks like the final topology

Router 4 will peer OSPF using process number 2 to a VRF configured on R1. It will use the local site addressing of 192.168.1.0/24.

Now at this point we have R4 peering to R1 but in the global routing table of R1 which is not what we want.

We are now going to start using VRF’s What is a VRF in networking?

Virtual routing and forwarding (VRF) is a technology included in IP (Internet Protocol) that allows multiple instances of a routing table to co-exist in a router and work together but not interfere with each other.. This increases functionality by allowing network paths to be segmented without using multiple devices.

As an example if R1 was a PE Provider Edge router of an ISP and it had two customers that were both addressed locally with the 192.168.1.0/24 address space it could accommodate both their routing tables in different VRFs – it distinguishes between the two of them using a Route Distinguisher

So back to the topology – we now need to create a VRF on R1

For this mpls tutorial I will be using VRF RED

The RD and route-target do not need to be the same – and for a full explanation please read this post on Route Distinguishers

Route Distinguisher vs Route Target before proceeding.

So now we have configured the VRF on R1 we need to move the interface F0/1 into that VRF

Now notice what happens when you do that – the IP address is removed

You just need to re-apply it

Now if we view the config on R1 int f0/1 you can see the VRF configured.

Now we can start to look int VRF’s and how they operate – you need to understand now that there are 2 routing tables within R1 The Global Routing Table

The Routing Table for VRF RED

If you issue the command sh ip route this shows the routes in the global table and you will notice that you do not see 192.168.1.0/24

If you now issue the command sh ip route vrf red – this will show the routes in the routing table for VRF

RED

NOTE: The VRF name is case sensitive!

We just need to enable OSPF on this interface and get the loopback address for R4 in the VRF RED routing table before proceeding.

You should see a log message showing the OSPF neighbor come up

If we now check the routes in the VRF RED routing table you should see 4.4.4.4 in there as well.

We now need to repeat this process for R3 & R6

Router 6 will peer OSPF using process number 2 to a VRF configured on R3. It will use the local site addressing of 192.168.2.0/24.

We also need to configure a VRF onto R3 as well.

So now we have configured the VRF on R3 we need to move the interface F0/1 into that VRF

Now notice what happens when you do that – the IP address is removed

You just need to re-apply it

Now if we view the config on R3 int f0/1 you can see the VRF configured.

Finally we just need to enable OSPF on that interface and verify the routes are in the RED routing table.

Check the routes in vrf RED

Ok so we have come a long way now let’s review the current situation. We now have this setup

R1,R2,R3 form the MPLS Core and are running OSPF with all loopbacks running a /32 address and all have full connectivity. R1 and R3 are peering with MP-BGP. LDP is enabled on all the internal interfaces. The external interfaces of the MPLS core have been placed into a VRF called RED and then a site router has been joined to that VRF on each side of the MPLS core – (These represent a small office) The final step to get full connectivity across the MPLS core is to redistribute the routes in OSPF on R1 and R3 into MP-BGP and MP-BGP into OSPF, this is what we are going to do now.

We need to redistribute the OSPF routes from R4 into BGP in the VRF on R1, the OSPF routes from R6 into MP-BGP in the VRF on R3 and then the routes in MP-BGP in R1 and R3 back out to OSPF

Before we start lets do some verifications

Check the routes on R4

As expected we have the local interface and the loopback address.

When we are done we want to see 6.6.6.6 in there so we can ping across the MPLS Check the routes on R1

Remember we have a VRF configured on this router so this command will show routes in the global routing table (the MPLS Core) and it will not show the 192.168.1.0/24 route as that is in VRF RED – to see that we run the following command

Here you can see Routing Table: RED is shown and the routes to R4 are now visible with 4.4.4.4 being in OSPF. So we need to do the following;

* Redistribute OSPF into MP-BGP on R1
* Redistribute MP-BGP into OSPF on R1
* Redistribute OSPF into MP-BGP on R3
* Redistribute MP-BGP into OSPF on R3

Redistribute OSPF into MP-BGP on R1

Redistribute OSPF into MP-BGP on R3

This has enabled redistribution of the OSPF routes into BGP. We can check the routes from R4 and R6 are now showing in the BGP table for their VRF with this command

sh ip bgp vpnv4 vrf RED

Here we can see that 4.4.4.4 is now in the BGP table in VRF RED on R1 with a next hop of 192.168.1.4 (R4) and also 6.6.6.6 is in there as well with a next hop of 3.3.3.3 (which is the loopback of R3 – showing that it is going over the MPLS and R1 is not in the picture)

The same should be true on R3

Which it is! 6.6.6.6 is now in the BGP table in VRF RED on R3 with a next hop of 192.168.2.6 (R6) and also 4.4.4 is in there as well with a next hop of 1.1.1.1 (which is the loopback of R1 – showing that it is going over the MPLS and R2 is not in the picture)

The final step is to get the routes that have come across the MPLS back into OSPF and then we can get end to end connectivity

If all has worked we should be now able to ping 6.6.6.6 from R4

Before we do let’s see what the routing table looks like on R4

Great we have 6.6.6.6 in there

Also check the routing table on R6

Brilliant we have 4.4.4.4 in there so we should be able to ping across the

MPLS

Which we can – to prove this is going over the MPLS and be label switched and not routed, lets do a trace