CCNP LAB GUIDE

ENARSI

Version 1.1

Developed By: Waleed Adlan

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

EIGRP Module

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

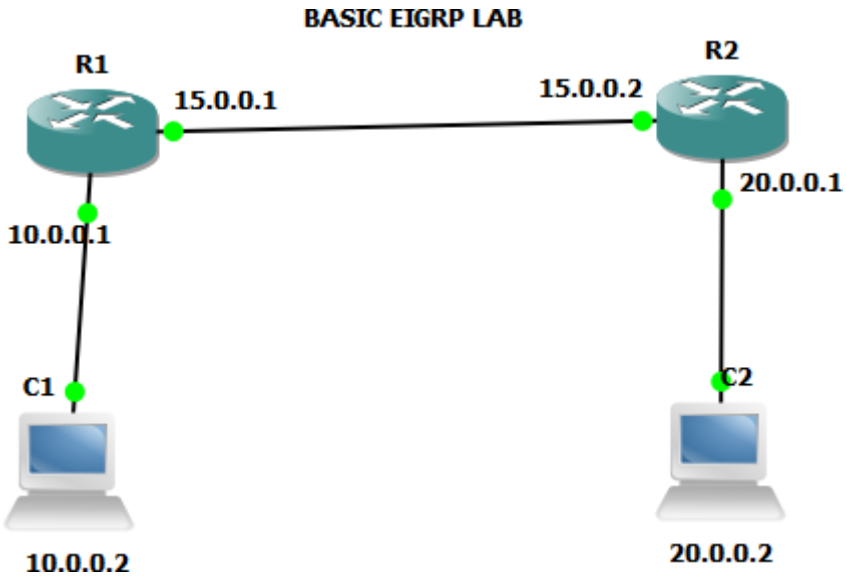
LAB 1

Basic EIGRP Configuration

Objective:

The lab main goal is to configure eigrp between two routers as shown in the below diagram, and ensure basic connectivity between the two hosts.

Diagram:



Preliminary Tasks:

Make the physical connection, and assign the ip addresses as shown in the diagram.

Task 1:

Enable EGIRP on Both Routers, and disable auto-summary

```
!R1
router eigrp 1
 network 10.0.0.0
 network 15.0.0.0
no auto-summary
!R2
router eigrp 1
 network 20.0.0.0
 network 15.0.0.0
 no auto-summary
!
```

Verification:

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   15.0.0.2                Fa0/1           11 00:12:15   67   402  0  5
```

```
R1#show ip route
D    20.0.0.0/8 [90/30720] via 15.0.0.2, 00:13:18, FastEthernet0/1
C    10.0.0.0/8 is directly connected, FastEthernet0/0
C    15.0.0.0/8 is directly connected, FastEthernet0/1
```

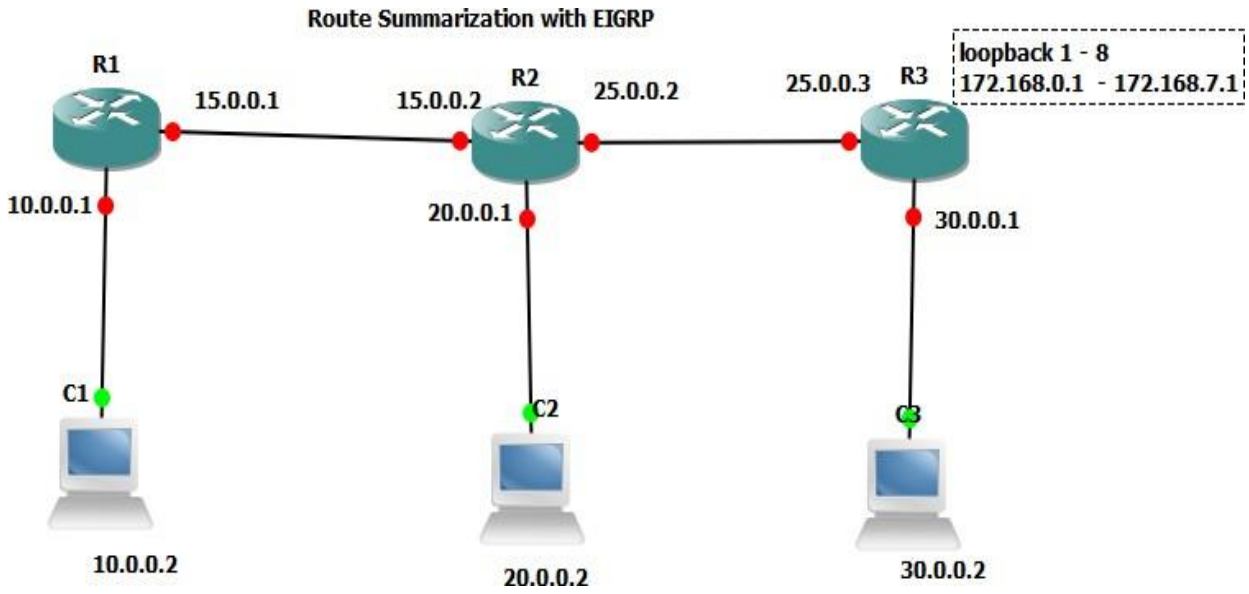
LAB 2

EIGRP WITH ROUTE SUMMARIZATION

Objective:

The main purpose of this lab, is to allow students configure eigrp with manual summarization.

Diagram:



Preliminary Tasks:

Connect the network as shown in the diagram, and assign the ip addresses for all physical interfaces.

Task 1:

Configure eight loopback addresses on R3 as follows:

```
!R3
interface Loopback1
 ip address 172.168.0.1 255.255.255.0
!
interface Loopback2
 ip address 172.168.1.1 255.255.255.0
!
interface Loopback3
 ip address 172.168.2.1 255.255.255.0
!
interface Loopback4
 ip address 172.168.3.1 255.255.255.0
!
interface Loopback5
 ip address 172.168.4.1 255.255.255.0
!
interface Loopback6
 ip address 172.168.5.1 255.255.255.0
!
interface Loopback7
 ip address 172.168.6.1 255.255.255.0
!
interface Loopback8
```

ip address 172.168.7.1 255.255.255.0

!

Task2:

Enable eigrp on all routers and on all interfaces, and disable auto summarization

Task3:

Configure R2 to manual summarize all the loopback networks to R1 as follows:

!R2

interface FastEthernet0/1

ip summary-address eigrp 1 172.168.0.0 255.255.248.0

Verification:

R1#sh ip route

D 20.0.0.0/8 [90/30720] via 15.0.0.2, 00:17:42, FastEthernet0/1

172.168.0.0/21 is subnetted, 1 subnets

D 172.168.0.0 [90/158720] via 15.0.0.2, 00:03:26, FastEthernet0/1

D 25.0.0.0/8 [90/30720] via 15.0.0.2, 00:17:42, FastEthernet0/1

C 10.0.0.0/8 is directly connected, FastEthernet0/0

D 30.0.0.0/8 [90/33280] via 15.0.0.2, 00:11:33, FastEthernet0/1

C 15.0.0.0/8 is directly connected, FastEthernet0/1

R2#sh ip route

C 20.0.0.0/8 is directly connected, FastEthernet0/0

172.168.0.0/16 is variably subnetted, 9 subnets, 2 masks

D 172.168.4.0/24 [90/156160] via 25.0.0.3, 00:11:52, FastEthernet1/0

D 172.168.5.0/24 [90/156160] via 25.0.0.3, 00:11:49, FastEthernet1/0

D 172.168.6.0/24 [90/156160] via 25.0.0.3, 00:11:46, FastEthernet1/0

D 172.168.7.0/24 [90/156160] via 25.0.0.3, 00:11:41, FastEthernet1/0

D 172.168.0.0/24 [90/156160] via 25.0.0.3, 00:12:10, FastEthernet1/0

D 172.168.0.0/21 is a summary, 00:04:33, Null0

D 172.168.1.0/24 [90/156160] via 25.0.0.3, 00:12:05, FastEthernet1/0

D 172.168.2.0/24 [90/156160] via 25.0.0.3, 00:12:01, FastEthernet1/0

D 172.168.3.0/24 [90/156160] via 25.0.0.3, 00:11:57, FastEthernet1/0

C 25.0.0.0/8 is directly connected, FastEthernet1/0

D 10.0.0.0/8 [90/30720] via 15.0.0.1, 00:18:49, FastEthernet0/1

D 30.0.0.0/8 [90/30720] via 25.0.0.3, 00:12:41, FastEthernet1/0

C 15.0.0.0/8 is directly connected, FastEthernet0/1

Ping should be successful between all PCs and the loopback addresses.

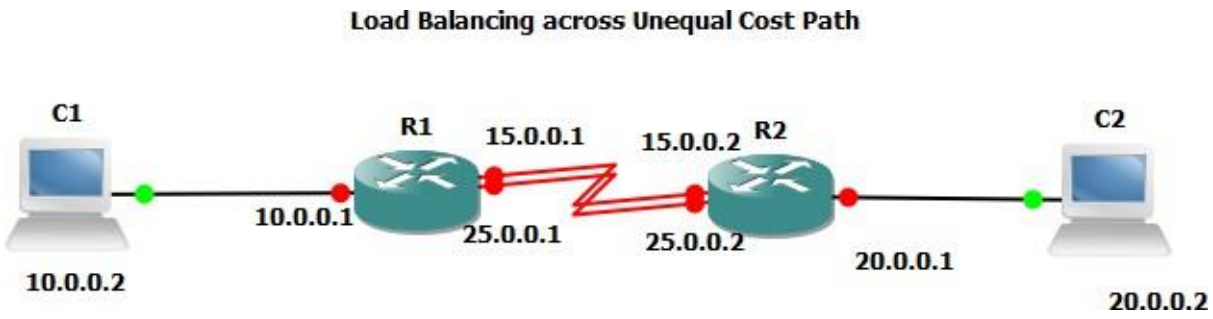
Lab 3

Load Balancing across Unequal Cost Path

Objective:

The main purpose of this lab is to configure load balancing over unequal cost paths.

Diagram:



Preliminary Tasks:

Connect the devices as shown in the diagram, and configure the relevant ip addresses for all physical interfaces.

Task 1:

Enable Eigrp 1 on both routers for all connected networks, and disable auto-summary.

Task2:

Change the bandwidth for Serial1/1 to 800 on R2 as shown next, to make the two links having unequal cost path.

!R2

interface S1/1

bandwidth 800

Task 3:

On R2, configure the variance value to 2, to let eigrp consider the two paths having an equal metric.

!R2

router eigrp 1

variance 2

Verification

R2#sh ip eigrp topology

P 10.0.0.0/8, 1 successors, FD is 2172416

via 25.0.0.1 (2172416/28160), Serial1/0

via 15.0.0.1 (3714560/28160), Serial1/1

P 15.0.0.0/8, 1 successors, FD is 3712000

via Connected, Serial1/1

via 25.0.0.1 (2681856/2169856), Serial1/0

P 20.0.0.0/8, 1 successors, FD is 28160

via Connected, FastEthernet0/0

P 25.0.0.0/8, 1 successors, FD is 2169856

via Connected, Serial1/0

R2#sh ip route

C 20.0.0.0/8 is directly connected, FastEthernet0/0

C 25.0.0.0/8 is directly connected, Serial1/0

D 10.0.0.0/8 [90/2172416] via 25.0.0.1, 00:00:06, Serial1/0

[90/3714560] via 15.0.0.1, 00:00:06, Serial1/1

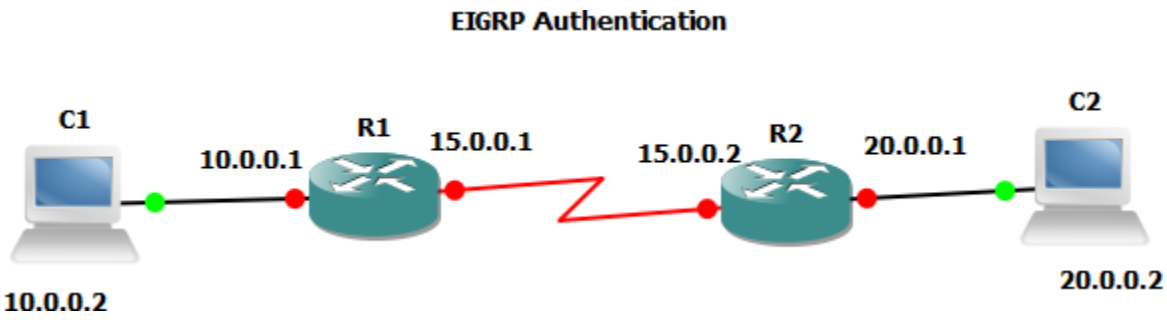
Lab 4

EIGRP Authentication

Objective:

The main target of this lab, is to allow students to configure a secure eigrp neighborhood using md5 authentication.

Diagram:



Preliminary Tasks:

Connect the above network, and configure the relevant ip addresses.

Task1:

Enable Eigrp on Both Devices advertising all networks, and disable auto summary.

Task2:

Configure Eigrp md5 authentication on both routers as follows:

R1

key chain chain1

```
 key 1
   key-string cisco
!
interface Serial1/0
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 chain1

!R2
key chain chain2
 key 1
   key-string cisco
!
interface Serial1/0
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 chain2
```

Verification

```
R1#sh ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   15.0.0.2                Se1/0            13 00:05:53   60   360  0  4

R2#debug eigrp packets
```

EIGRP Packets debugging is on

(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)

R2#

*Sep 13 11:09:49.955: EIGRP: Sending HELLO on FastEthernet0/0

*Sep 13 11:09:49.955: AS 1, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0

*Sep 13 11:09:50.347: EIGRP: Sending HELLO on Serial1/0

*Sep 13 11:09:50.347: AS 1, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0

R2#

*Sep 13 11:09:52.071: EIGRP: received packet with MD5 authentication, key id = 1

*Sep 13 11:09:52.071: EIGRP: Received HELLO on Serial1/0 nbr 15.0.0.1

*Sep 13 11:09:52.071: AS 1, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0

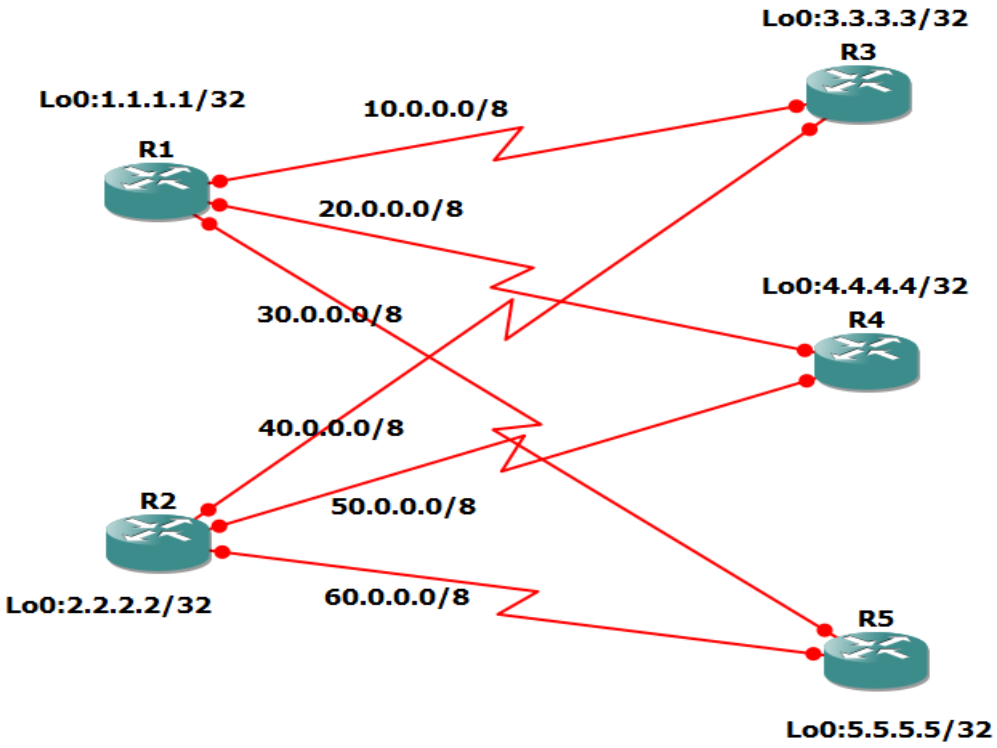
R2#

Ping Should be successful between devices.

Lab 5
EIGRP Stub

Objective

The main target of this lab, is to allow students to configure a EIGRP stub feature



Preliminary Tasks:

Connect the above network, and configure the relevant ip addresses.

Task1:

Enable Eigrp on Both Devices advertising all networks, and disable auto summary.

Task2:

Configure Eigrp on R3,R4 & R5 to enable stub feature

!R3|R4|R5

Router eigrp 100

Eigrp stub

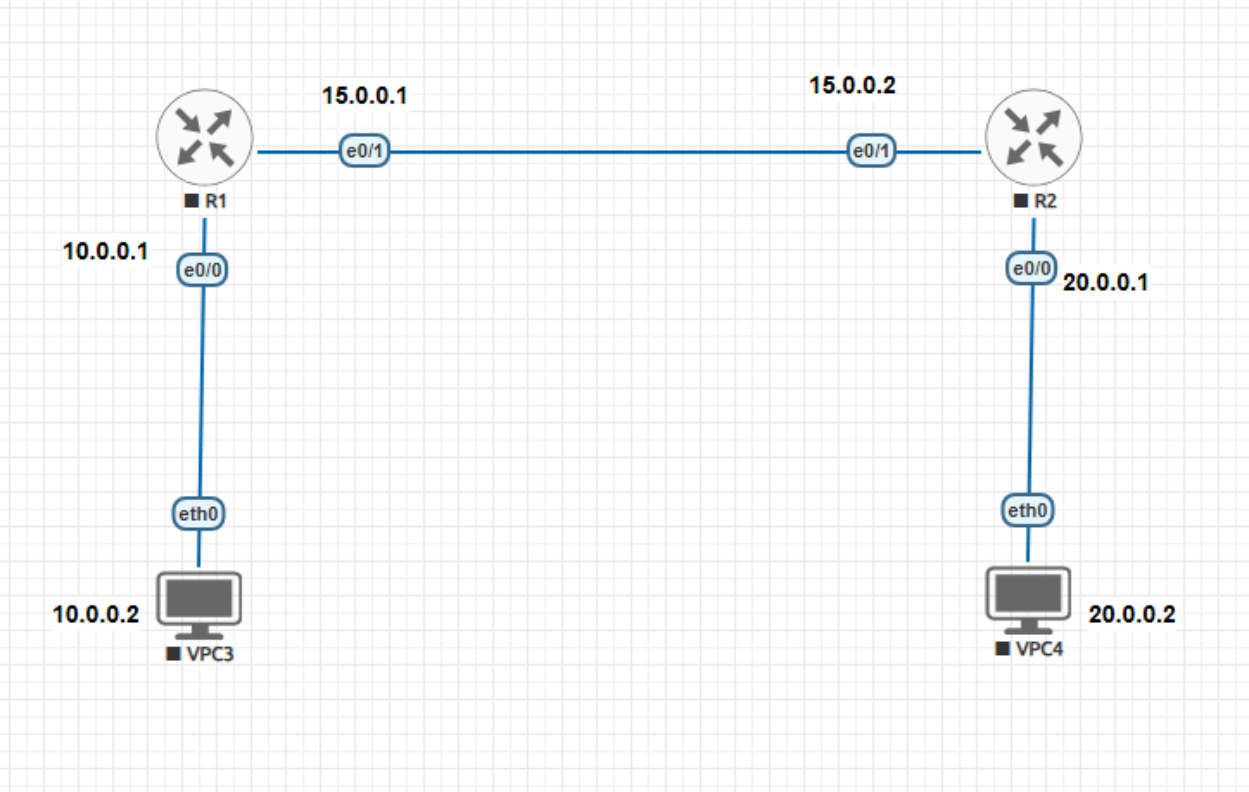
!Verification

The effect will be that R1,R2 will receive only the connected and summary routes (if available) and if R1&R2 lost a connection for a certain network they will not ask R3,R4 & R5 for alternative path, because they declared them as stub routers

Lab 6
EIGRP Named Mode

Objective

The main target of this lab, is to allow students to configure and Practice EIGRP named mode



Preliminary Tasks:

Connect the above network, and configure the relevant ip addresses.

Task1:

Enable EIGRP Named Mode on both routers using AS number as 1 and name as CCNP

!R1

```
router eigrp CCNP
address-family ipv4 autonomous-system 1
network 10.0.0.0
network 15.0.0.0
topology base
no auto-summary


!R2
router eigrp CCNP
address-family ipv4 autonomous-system 1
network 20.0.0.0
network 15.0.0.0
topology base
no auto-summary
```

!**Verification**

Make sure the two routers exchanged routes and the ping is working fine between the two networks

OSPF Module

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

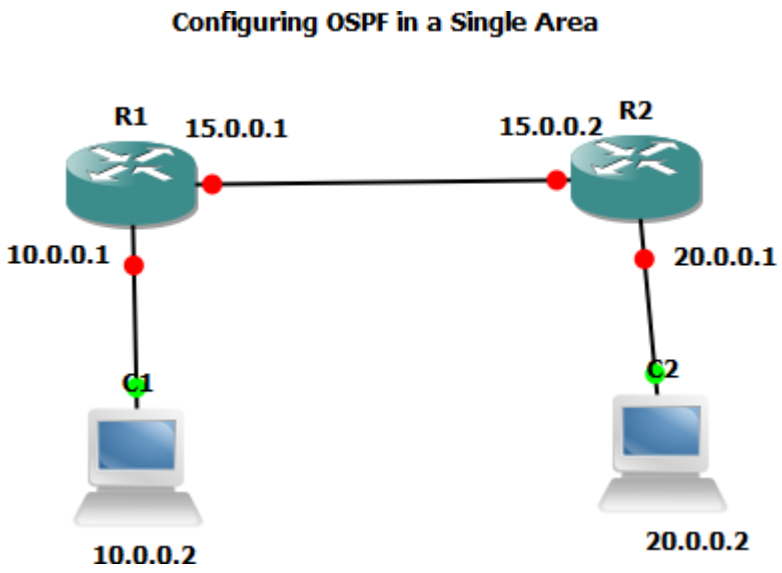
Lab 7

Configuring OSPF In a Single Area

Objective:

The target of this lab is to configure routers on area 0, and verify OSPF adjacency and PCs connectivity.

Diagram:



Preliminary Tasks:

Connect the network as shown in the above diagram, and configure the relevant IP addresses of all the physical interfaces.

Task1:

Configure OSPF in both routers and put all the interfaces in area 0

!R1

router ospf 1

network 15.0.0.0 0.255.255.255 area 0

network 10.0.0.0 0.255.255.255 area 0

!R2

network 15.0.0.0 0.255.255.255 area 0

network 20.0.0.0 0.255.255.255 area 0

Verification

R1#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
20.0.0.1	1	FULL/BDR	00:00:37	15.0.0.2	FastEthernet0/1

R1#sh ip route

O 20.0.0.0/8 [110/2] via 15.0.0.2, 00:02:11, FastEthernet0/1

C 10.0.0.0/8 is directly connected, FastEthernet0/0

C 15.0.0.0/8 is directly connected, FastEthernet0/1

R1#

Ping between PCs should be working fine....

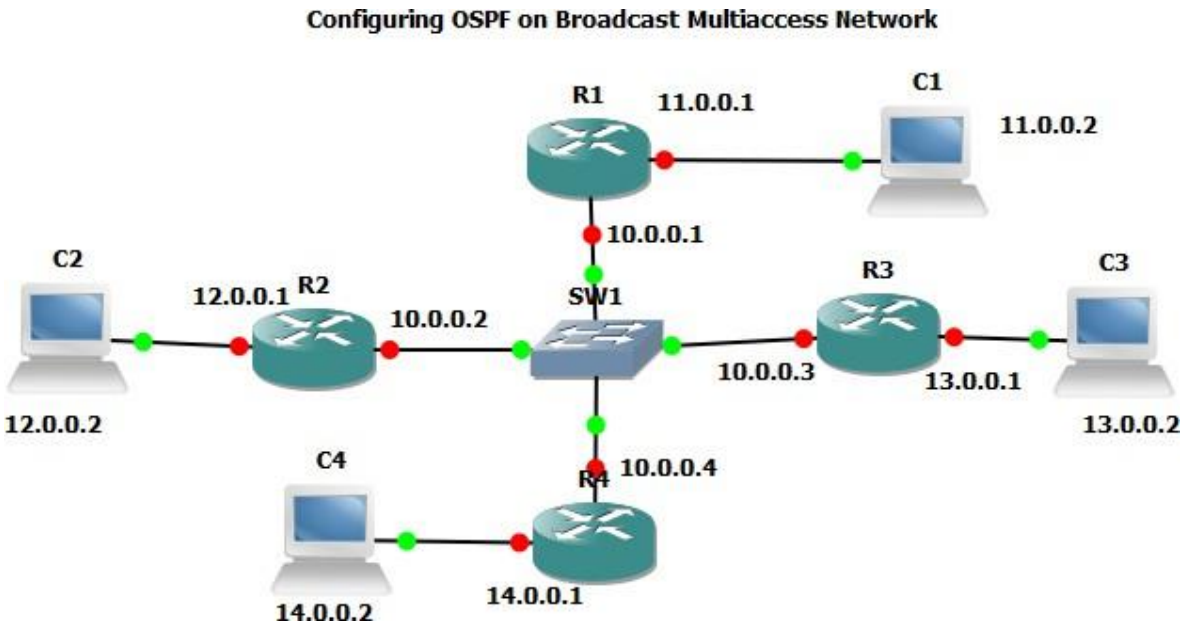
Lab 8

Configuring OSPF on Broadcast Multi-access Network

Objective:

The main goal of this lab is to configure ospf on BMA network, and to check the DR/BDR status of the routers.

Diagram:



Preliminary Task:

Connect the network as shown in the diagram, and assign ip addresses for the physical interfaces.

Task 1:

Configure ospf area 0 in all routers, and check the ospf neighbor table, and figure out who is the DR for the multi-access network

Verification:

!R1

R1#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
12.0.0.1	1	FULL/BDR	00:00:36	10.0.0.2	FastEthernet0/1
13.0.0.1	1	FULL/DROTHER	00:00:35	10.0.0.3	FastEthernet0/1
14.0.0.1	1	FULL/DROTHER	00:00:38	10.0.0.4	FastEthernet0/1

R1#

R3#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
11.0.0.1	1	FULL/DR	00:00:37	10.0.0.1	FastEthernet0/1
12.0.0.1	1	FULL/BDR	00:00:37	10.0.0.2	FastEthernet0/1
14.0.0.1	1	2WAY/DROTHER	00:00:39	10.0.0.4	FastEthernet0/1

R3#

Task 2:

Make sure that one of the DROTHER routers gain the DR status, and all other routers change to DROTHER status.

!R1/R2/R4

interface fa0/1

ip ospf priority 0

Verification:

R3#sh ip ospf interface fa0/1

FastEthernet0/1 is up, line protocol is up

Internet Address 10.0.0.3/8, Area 0

Process ID 1, Router ID 13.0.0.1, Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 13.0.0.1, Interface address 10.0.0.3

No backup designated router on this network

Old designated Router (ID) 14.0.0.1, Interface address 10.0.0.4

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

oob-resync timeout 40

-output omitted-

Note: ping between all PCs should work fine...

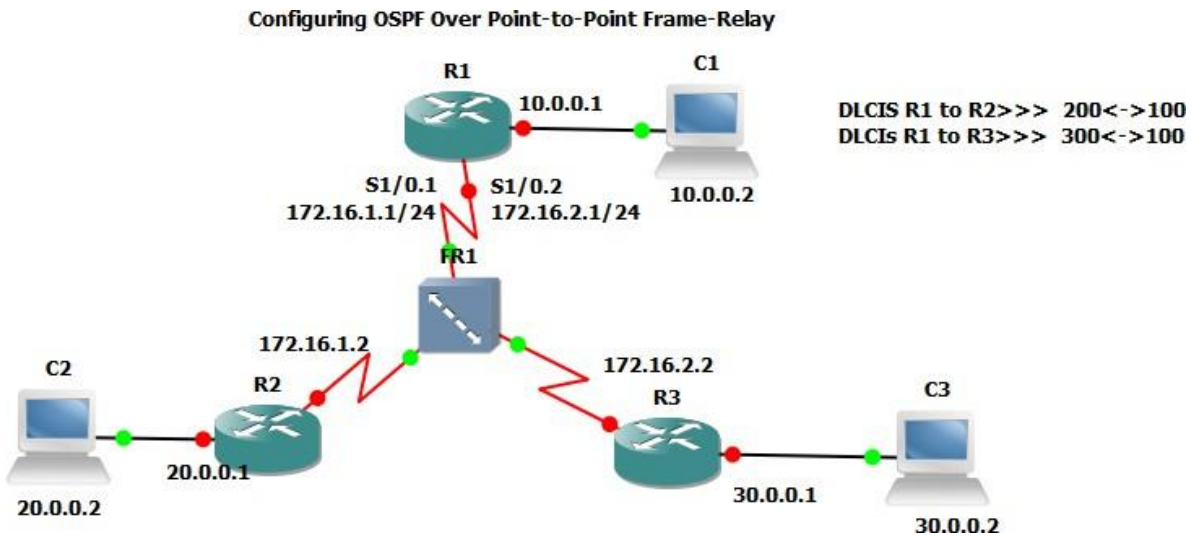
Lab 9

Configuring OSPF over point-to-point Frame-Relay

Objective:

The main target of this lab is to configure ospf on point-to-point frame-relay network.

Diagram:



Preliminary Task:

Connect the network as shown in the diagram, assign the relevant IP addresses. Then configure the frame-relay switch to provide DLCIs 200 & 300 for the interface connected to R1, and DLCI 100 for both interfaces connected to R2 & R3.

Task 1:

Configure frame-relay encapsulation on all router's serial interfaces.

Then Divide R1's serial interfaces into two point-to-point sub-interfaces as shown in the diagram and assign them the relevant IP addresses.

Assign IP addresses for the physical interfaces of R2 & R3

```
!R1
interface Serial1/0
encapsulation frame-relay
!
interface Serial1/0.1 point-to-point
 ip address 172.16.1.1 255.255.255.0
 frame-relay interface-dlci 200
!
interface Serial1/0.2 point-to-point
 ip address 172.16.2.1 255.255.255.0
 frame-relay interface-dlci 300


!R2
interface Serial1/0
 ip address 172.16.1.2 255.255.255.0
 encapsulation frame-relay

!R3
interface Serial1/0
 ip address 172.16.2.2 255.255.255.0
 encapsulation frame-relay
```

Verification:

```
R1#show frame-relay map
Serial1/0.1 (up): point-to-point dlci, dlci 200(0xC8,0x3080), broadcast
        status defined, active
Serial1/0.2 (up): point-to-point dlci, dlci 300(0x12C,0x48C0), broadcast
        status defined, active


R1#ping 172.16.1.2


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/43/92 ms
R1#


R1#ping 172.16.2.2


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/45/116 ms
R1#
```

Task 2:

Configure ospf on all routers and put all interfaces into area 0, and check the neighbor table

!R1

```
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 network 172.16.1.0 0.0.0.255 area 0
 network 172.16.2.0 0.0.0.255 area 0
```

!R2

```
router ospf 1
 log-adjacency-changes
 network 20.0.0.0 0.255.255.255 area 0
 network 172.16.1.0 0.0.0.255 area 0
```

!R3

```
router ospf 1
network 30.0.0.0 0.255.255.255 area 0
 network 172.16.2.0 0.0.0.255 area 0
```

Verification:

R3#sh ip ospf neighbor

Neighborhood didn't get established, because the network type of R2 and R3 (NBMA) is different from R1 sub-interfaces network type (point-to-point), which leads to differences in Hello timer.

R1#sh ip ospf int s1/0.1

Serial1/0.1 is up, line protocol is up

Internet Address 172.16.1.1/24, Area 0

Process ID 1, Router ID 172.16.2.1, Network Type POINT_TO_POINT, Cost: 64

Transmit Delay is 1 sec, State POINT_TO_POINT

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

R2#sh ip ospf int s1/0

Serial1/0 is up, line protocol is up

Internet Address 172.16.1.2/24, Area 0

Process ID 1, Router ID 172.16.1.2, Network Type NON_BROADCAST, Cost: 64

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 172.16.1.2, Interface address 172.16.1.2

No backup designated router on this network

Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5

oob-resync timeout 120

Task 3:

Change the network type on Both R2 & R3 to point-to-point, to allow the neighbor relation get established

!R2/R3

interface s1/0

ip ospf network point-to-point

Verification:

R1#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.16.2.2	0	FULL/ -	00:00:34	172.16.2.2	Serial1/0.2
172.16.1.2	0	FULL/ -	00:00:33	172.16.1.2	Serial1/0.1

R1#sh ip route

O 20.0.0.0/8 [110/65] via 172.16.1.2, 00:00:42, Serial1/0.1

172.16.0.0/24 is subnetted, 2 subnets

C 172.16.1.0 is directly connected, Serial1/0.1

C 172.16.2.0 is directly connected, Serial1/0.2

C 10.0.0.0/8 is directly connected, FastEthernet0/0

O 30.0.0.0/8 [110/65] via 172.16.2.2, 00:00:52, Serial1/0.2

Ping should be working between Pcs....

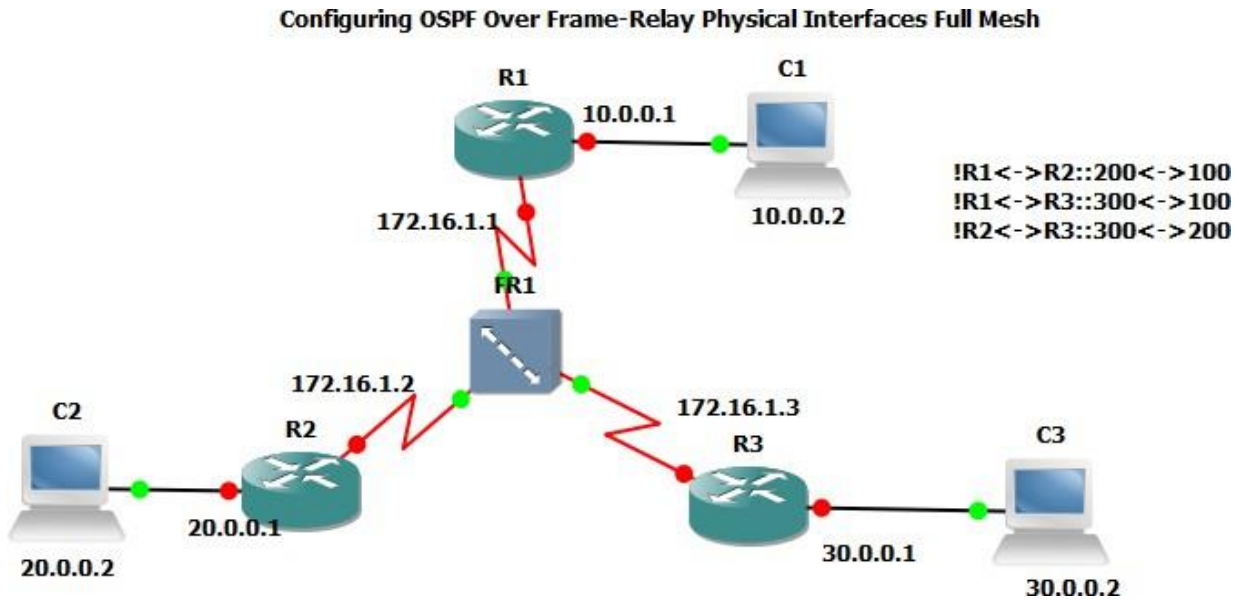
Lab 10

Configuring OSPF on Frame-Relay Physical Interfaces (NBMA Network)

Objective:

The main goal of this lab is configure OSPF over frame-relay physical interfaces full mesh topology, and check the neighbor table and the DR/BDR routers.

Diagram:



Preliminary Task:

Connect the network as above, and configure the IP addresses on all physical interfaces, and configure the frame-relay switch to provide a full mesh network between R1, R2 & R3 according to the DLCI table shown in the diagram.

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

Task 1:

Configure encapsulation frame-relay on all Serial interfaces of the routers, and assign the IP address to the physical serial interfaces.

```
!R1
interface Serial1/0
 ip address 172.16.1.1 255.255.255.0
 encapsulation frame-relay
!R2
interface Serial1/0
 ip address 172.16.1.2 255.255.255.0
 encapsulation frame-relay

!R3
interface Serial1/0
 ip address 172.16.1.3 255.255.255.0
 encapsulation frame-relay
```

Verification:

```
R1#show frame-relay map
Serial1/0 (up): ip 172.16.1.2 dlci 200(0xC8,0x3080), dynamic,
        broadcast,, status defined, active
Serial1/0 (up): ip 172.16.1.3 dlci 300(0x12C,0x48C0), dynamic,
        broadcast,, status defined, active
```

Task 2:

Configure ospf on all routers by putting all interfaces into area 0, and don't forget to configure the neighbor command under OSPF process, as the network is NBMA network which requires neighbor command to be added.

```
!R1
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
network 172.16.1.0 0.0.0.255 area 0
neighbor 172.16.1.2
neighbor 172.16.1.3

!R2
router ospf 1
network 20.0.0.0 0.255.255.255 area 0
network 172.16.1.0 0.0.0.255 area 0
neighbor 172.16.1.3
neighbor 172.16.1.1

!R3
router ospf 1
network 30.0.0.0 0.255.255.255 area 0
```

network 172.16.1.0 0.0.0.255 area 0

neighbor 172.16.1.2

neighbor 172.16.1.1

Verification:

R1#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.16.1.2	1	FULL/DR	00:01:35	172.16.1.2	Serial1/0
172.16.1.3	1	FULL/BDR	00:01:51	172.16.1.3	Serial1/0

R1#sh ip route

O 20.0.0.0/8 [110/65] via 172.16.1.2, 00:01:59, Serial1/0

172.16.0.0/24 is subnetted, 1 subnets

C 172.16.1.0 is directly connected, Serial1/0

C 10.0.0.0/8 is directly connected, FastEthernet0/0

O 30.0.0.0/8 [110/65] via 172.16.1.3, 00:01:15, Serial1/0

R1#

Ping should be working fine between PCs.....

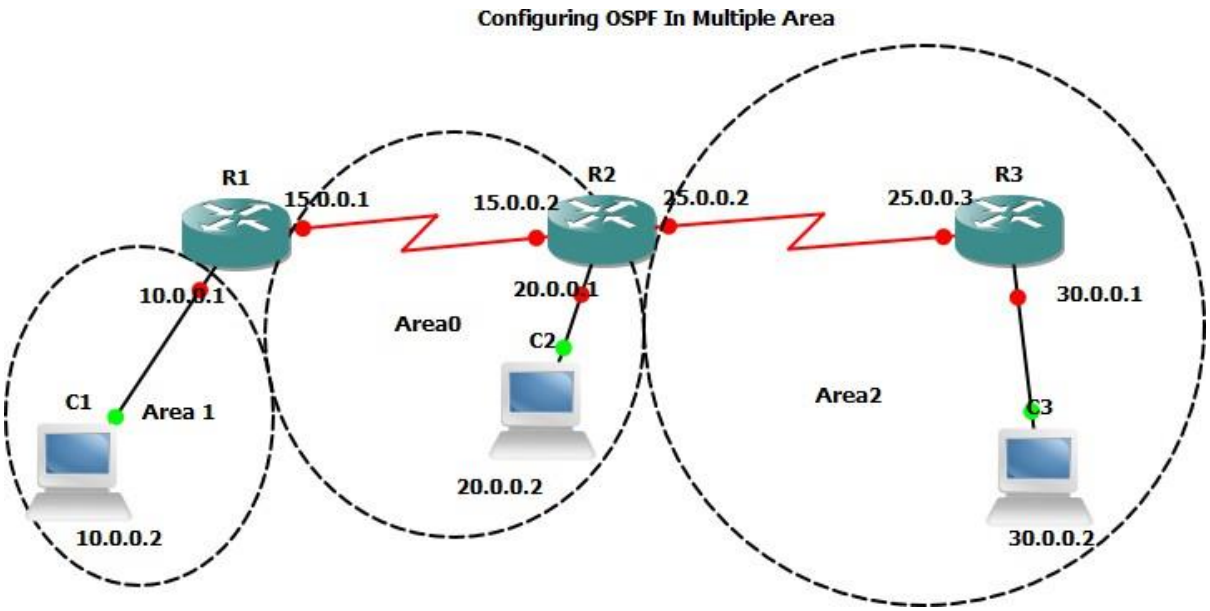
Lab 11

Configuring OSPF In a Multiple Areas

Objective:

The main goal of this lab is to configure multiple areas ospf design.

Diagram:



Preliminary Tasks:

Connect the network as shown in the diagram, and configure all related IP addresses needed.

Task 1:

Configure ospf areas on all routers as shown in the diagram.

!R1

router ospf 1

network 10.0.0.0 0.255.255.255 area 1

network 15.0.0.0 0.255.255.255 area 0

!R2

router ospf 1

 network 15.0.0.0 0.255.255.255 area 0

 network 20.0.0.0 0.255.255.255 area 0

 network 25.0.0.0 0.255.255.255 area 2

!R3

router ospf 1

 network 25.0.0.0 0.255.255.255 area 2

 network 30.0.0.0 0.255.255.255 area 2

!

!Verification:

R1#sh ip route

O   20.0.0.0/8 [110/65] via 15.0.0.2, 00:05:08, Serial1/0

O IA 25.0.0.0/8 [110/128] via 15.0.0.2, 00:04:05, Serial1/0

C   10.0.0.0/8 is directly connected, FastEthernet0/0

O IA 30.0.0.0/8 [110/129] via 15.0.0.2, 00:03:46, Serial1/0

C   15.0.0.0/8 is directly connected, Serial1/0

R1#

R2#sh ip route

C 20.0.0.0/8 is directly connected, FastEthernet0/0

C 25.0.0.0/8 is directly connected, Serial1/1

O IA 10.0.0.0/8 [110/65] via 15.0.0.1, 00:05:07, Serial1/0

O 30.0.0.0/8 [110/65] via 25.0.0.3, 00:04:42, Serial1/1

C 15.0.0.0/8 is directly connected, Serial1/0

R2#

R3#sh ip route

O IA 20.0.0.0/8 [110/65] via 25.0.0.2, 00:05:32, Serial1/0

C 25.0.0.0/8 is directly connected, Serial1/0

O IA 10.0.0.0/8 [110/129] via 25.0.0.2, 00:05:32, Serial1/0

C 30.0.0.0/8 is directly connected, FastEthernet0/0

O IA 15.0.0.0/8 [110/128] via 25.0.0.2, 00:05:32, Serial1/0

R3#

Ping between all PCs should be working.

Task2:

Modify ospf hello interval default value on R1's serial, and check the neighbor status before and after the manipulation.

!R1

int s1/0

ip ospf hello-interval 3

Before hello Manipulation

```
R1#sh ip ospf interface s1/0
Serial1/0 is up, line protocol is up
Internet Address 15.0.0.1/8, Area 0
  Process ID 1, Router ID 15.0.0.1, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:08

R1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
25.0.0.2          0   FULL/  -        00:00:33    15.0.0.2        Serial1/0
R1#
```

After Hello-interval Manipulation

```
R1#sh ip ospf interface s1/0
*Sep 13 14:52:05.107: %SYS-5-CONFIG_I: Configured from console by console
R1#sh ip ospf interface s1/0
Serial1/0 is up, line protocol is up
  Internet Address 15.0.0.1/8, Area 0
```

Process ID 1, Router ID 15.0.0.1, Network Type POINT_TO_POINT, Cost: 64

Transmit Delay is 1 sec, State POINT_TO_POINT

Timer intervals configured, Hello 3, Dead 12, Wait 12, Retransmit 5

R1#sh ip ospf neighbor

R1#

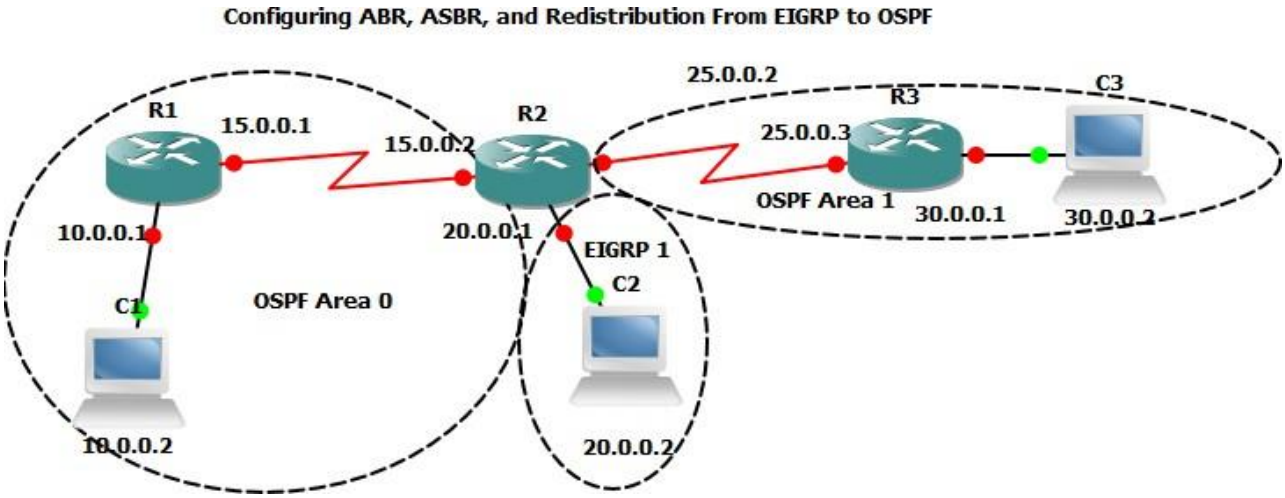
Lab 12

Configuring ABR, ASBR & redistribution From Eigrp to OSPF

Objective:

The objective of this lab is to configure a multiple routing protocol network, and to show the role of the ABR & ASBR in OSPF plus the redistribution mechanism between OSPF and EIGRP.

Diagram:



Preliminary Tasks:

Connect the network as shown in the diagram, and configure the ip addresses of all the physical Interfaces

Task 1:

Configure Ospf and Eigrp as explained in the diagram, and redistribute from eigrp to ospf

!R1

router ospf 1

network 10.0.0.0 0.255.255.255 area 0

```
 network 15.0.0.0 0.255.255.255 area 0


! R2
router ospf 1
network 15.0.0.0 0.255.255.255 area 0
 network 25.0.0.0 0.255.255.255 area 1
redistribute eigrp 1 subnets
!
router eigrp 1
 network 20.0.0.0
 no auto-summary


!R3
router ospf 1
network 25.0.0.0 0.255.255.255 area 1
 network 30.0.0.0 0.255.255.255 area 1
!
```

Verification:

```
R1#sh ip route
O E2 20.0.0.0/8 [110/20] via 15.0.0.2, 00:02:09, Serial1/0
O IA 25.0.0.0/8 [110/128] via 15.0.0.2, 00:08:48, Serial1/0
C    10.0.0.0/8 is directly connected, FastEthernet0/0
O IA 30.0.0.0/8 [110/129] via 15.0.0.2, 00:08:22, Serial1/0
C    15.0.0.0/8 is directly connected, Serial1/0
```

Note: If we want the redistributed link to show up as OE1, we can do the following configuration

!R2

router ospf 1

redistribute eigrp 1 metric-type 1 subnets

R1#sh ip route

O E1 20.0.0.0/8 [110/84] via 15.0.0.2, 00:01:38, Serial1/0

O IA 25.0.0.0/8 [110/128] via 15.0.0.2, 00:14:05, Serial1/0

C 10.0.0.0/8 is directly connected, FastEthernet0/0

O IA 30.0.0.0/8 [110/129] via 15.0.0.2, 00:13:39, Serial1/0

C 15.0.0.0/8 is directly connected, Serial1/0

R1#sh ip ospf border-routers

i 25.0.0.2 [64] via 15.0.0.2, Serial1/0, ABR/ASBR, Area 0, SPF 5

R1#

Ping should be successful between all PCs...

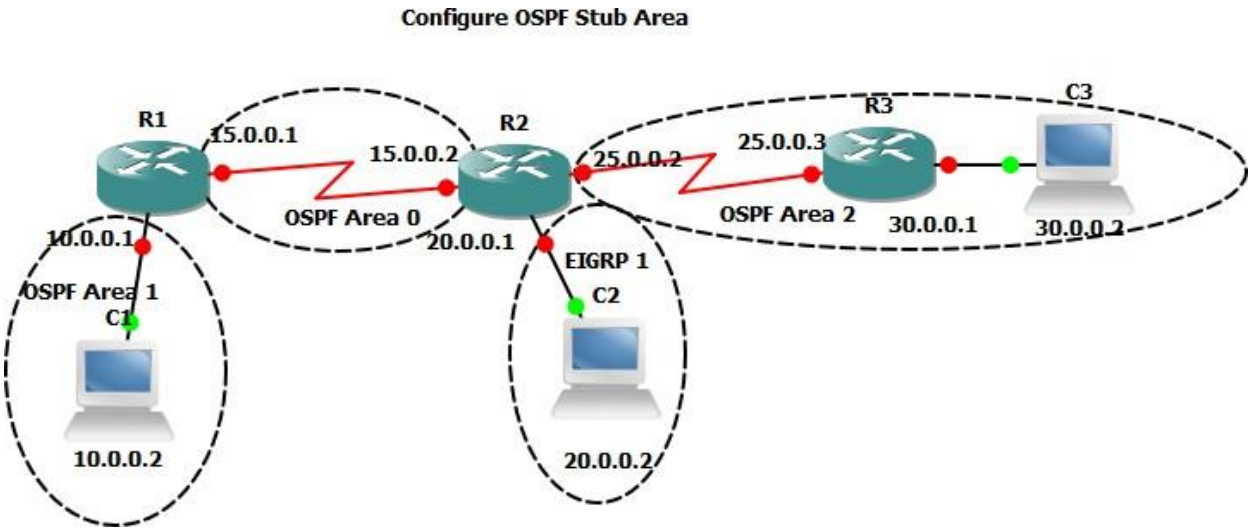
Lab 13

Configuring OSPF Stub Area

Objective:

The main purpose of this Lab, is configure ospf stub area, and check the routing table accordingly to see the default route advertised in the Stub area.

Diagram:



Preliminary Tasks:

Connect the network as shown in the diagram, and configure IP addresses as described above.

Task 1:

Configure OSPF & EIGRP as shown in the diagram, and redistribute eigrp into ospf

!R1

router ospf 1

network 10.0.0.0 0.255.255.255 area 1

```
 network 15.0.0.0 0.255.255.255 area 0


!R2
router eigrp 1
 network 20.0.0.0
 no auto-summary
!
router ospf 1
redistribute eigrp 1 subnets
 network 15.0.0.0 0.255.255.255 area 0
 network 25.0.0.0 0.255.255.255 area 2


!R3
router ospf 1
 log-adjacency-changes
 network 25.0.0.0 0.255.255.255 area 2
 network 30.0.0.0 0.255.255.255 area 2
!
```

Verification

R3#sh ip route

O E2 20.0.0.0/8 [110/20] via 25.0.0.2, 00:03:37, Serial1/0

C 25.0.0.0/8 is directly connected, Serial1/0

O IA 10.0.0.0/8 [110/129] via 25.0.0.2, 00:03:37, Serial1/0

C 30.0.0.0/8 is directly connected, FastEthernet0/0

O IA 15.0.0.0/8 [110/128] via 25.0.0.2, 00:03:37, Serial1/0

R3#

R3#sh ip ospf database

OSPF Router with ID (30.0.0.1) (Process ID 1)

Router Link States (Area 2)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
25.0.0.2	25.0.0.2	304	0x80000004	0x00EA2A	2
30.0.0.1	30.0.0.1	293	0x80000002	0x00A63F	3

Summary Net Link States (Area 2)

Link ID	ADV Router	Age	Seq#	Checksum
10.0.0.0	25.0.0.2	329	0x80000001	0x00A531
15.0.0.0	25.0.0.2	329	0x80000001	0x005A78

Type-5 AS External Link States

Link ID	ADV Router	Age	Seq#	Checksum Tag
20.0.0.0	25.0.0.2	361	0x80000001	0x00F47C 0

Task 3:

Configure OSPF area 2 as STUB

!R2/R3

router ospf 1

area 2 stub

Verification

R3#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
25.0.0.2	0	FULL/ -	00:00:32	25.0.0.2	Serial1/0

R3#sh ip route

C   25.0.0.0/8 is directly connected, Serial1/0

O IA 10.0.0.0/8 [110/129] via 25.0.0.2, 00:01:44, Serial1/0

C   30.0.0.0/8 is directly connected, FastEthernet0/0

O IA 15.0.0.0/8 [110/128] via 25.0.0.2, 00:01:44, Serial1/0

O*IA 0.0.0.0/0 [110/65] via 25.0.0.2, 00:01:44, Serial1/0

R3#

R3#sh ip ospf database

OSPF Router with ID (30.0.0.1) (Process ID 1)

Router Link States (Area 2)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
25.0.0.2	25.0.0.2	173	0x80000006	0x00FE18	2
30.0.0.1	30.0.0.1	170	0x80000004	0x00C025	3

Summary Net Link States (Area 2)

Link ID	ADV Router	Age	Seq#	Checksum

0.0.0.0 25.0.0.2 191 0x80000001 0x00C35F

10.0.0.0 25.0.0.2 191 0x80000002 0x00C116

15.0.0.0 25.0.0.2 191 0x80000002 0x00765D

R3#

Note: Stub configuration should be done on both routers.

Ping should be working between all devices.....

Lab 14

Configuring Totally Stub Area

Objective:

The purpose of this lab, is to configure Totally Stub Area in OSPF, and checking the changes on the OSPF database accordingly.

Diagram:

Based on the same network on Lab 11

Task 1:

Continue on Lab 11, disable the area stub configuration on Both R2 & R3.

!R2

router ospf 1

no area 2 stub

!R3

router ospf 1

no area 2 stub

Verification

R3#sh ip ospf database

OSPF Router with ID (30.0.0.1) (Process ID 1)

Router Link States (Area 2)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
25.0.0.2	25.0.0.2	43	0x80000002	0x00EE28	2
30.0.0.1	30.0.0.1	35	0x80000002	0x00A63F	3

Summary Net Link States (Area 2)

Link ID	ADV Router	Age	Seq#	Checksum
10.0.0.0	25.0.0.2	150	0x80000001	0x00A531
15.0.0.0	25.0.0.2	150	0x80000001	0x005A78

Type-5 AS External Link States

Link ID	ADV Router	Age	Seq#	Checksum	Tag
20.0.0.0	25.0.0.2	149	0x80000001	0x00F47C	0

R3#sh ip route

O E2 20.0.0.0/8 [110/20] via 25.0.0.2, 00:02:08, Serial1/0

C 25.0.0.0/8 is directly connected, Serial1/0

O IA 10.0.0.0/8 [110/129] via 25.0.0.2, 00:02:08, Serial1/0

C 30.0.0.0/8 is directly connected, FastEthernet0/0

O IA 15.0.0.0/8 [110/128] via 25.0.0.2, 00:02:08, Serial1/0

Task 2:

Configure Area 2 as Totally Stubby area as follows:

!R2

router ospf 1

area 2 stub no-summary

!R3

router ospf 1

area 2 stub no-summary

Verification

R3#sh ip ospf database

OSPF Router with ID (30.0.0.1) (Process ID 1)

Router Link States (Area 2)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
25.0.0.2	25.0.0.2	8	0x80000004	0x000316	2
30.0.0.1	30.0.0.1	7	0x80000004	0x00C025	3

Summary Net Link States (Area 2)

Link ID	ADV Router	Age	Seq#	Checksum
0.0.0.0	25.0.0.2	30	0x80000001	0x00C35F

R3#

R3#sh ip route

Gateway of last resort is 25.0.0.2 to network 0.0.0.0

C 25.0.0.0/8 is directly connected, Serial1/0

C 30.0.0.0/8 is directly connected, FastEthernet0/0

O*IA 0.0.0.0/0 [110/65] via 25.0.0.2, 00:01:35, Serial1/0

Lab 15

Configuring NSSA

Objective:

The main goal of this lab is to configure NSSA area, and checking the ospf database accordingly.

Diagram:

Based on Lab 11.

Task 1:

(Following Lab 12), Disable total sub area configuration on area 2

!R2/R3

router ospf 1

no area 2 stub

Verification:

R3#sh ip ospf database

OSPF Router with ID (30.0.0.1) (Process ID 1)

Router Link States (Area 2)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
25.0.0.1	25.0.0.1	20	0x80000004	0x00FA1C	2
30.0.0.1	30.0.0.1	7	0x80000002	0x009056	3

Summary Net Link States (Area 2)

Link ID	ADV Router	Age	Seq#	Checksum
10.0.0.0	25.0.0.1	115	0x80000001	0x00AB2C
15.0.0.0	25.0.0.1	115	0x80000001	0x006073

Type-5 AS External Link States

Link ID	ADV Router	Age	Seq#	Checksum	Tag
20.0.0.0	25.0.0.1	341	0x80000001	0x00FA77	0

R3# show ip route

O E2 20.0.0.0/8 [110/20] via 25.0.0.2, 00:03:09, Serial1/0

C 25.0.0.0/8 is directly connected, Serial1/0

O IA 10.0.0.0/8 [110/129] via 25.0.0.2, 00:03:09, Serial1/0

C 30.0.0.0/8 is directly connected, FastEthernet0/0

O IA 15.0.0.0/8 [110/128] via 25.0.0.2, 00:03:09, Serial1/0

R3#

Task 2:

Configure Area 2 as NSSA area

!R2/R3

router ospf 1

area 2 nssa

Verification:

R3#sh ip ospf database

OSPF Router with ID (30.0.0.1) (Process ID 1)

Router Link States (Area 2)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
25.0.0.1	25.0.0.1	82	0x80000006	0x009C72	2
30.0.0.1	30.0.0.1	83	0x80000004	0x0032AC	3

Summary Net Link States (Area 2)

Link ID	ADV Router	Age	Seq#	Checksum
10.0.0.0	25.0.0.1	87	0x80000002	0x004F81

15.0.0.0 25.0.0.1 87 0x80000002 0x0004C8

Type-7 AS External Link States (Area 2)

Link ID ADV Router Age Seq# Checksum Tag

20.0.0.0 25.0.0.1 86 0x80000001 0x00DE91 0

R3#

R3#sh ip route

O N2 20.0.0.0/8 [110/20] via 25.0.0.2, 00:02:12, Serial1/0

C 25.0.0.0/8 is directly connected, Serial1/0

O IA 10.0.0.0/8 [110/129] via 25.0.0.2, 00:02:12, Serial1/0

C 30.0.0.0/8 is directly connected, FastEthernet0/0

O IA 15.0.0.0/8 [110/128] via 25.0.0.2, 00:02:12, Serial1/0

R3#

Ping should successful between devices....

Lab 16

Configuring NSSA Total Sub

Objective:

The main goal of this lab is to configure NSSA total stub and check the ospf database accordingly.

Diagram:

Follow the diagram On Lab 11.

Task 1:

Disable the area NSSA configuration on R2 & R3

!R2/R3

router ospf 1

no area 2 nssa

Verification:

R3#show ip ospf database

OSPF Router with ID (30.0.0.1) (Process ID 1)

Router Link States (Area 2)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
25.0.0.1	25.0.0.1	54	0x80000008	0x00F220	2

30.0.0.1 30.0.0.1 53 0x80000006 0x00885A 3

Summary Net Link States (Area 2)

Link ID ADV Router Age Seq# Checksum

10.0.0.0 25.0.0.1 63 0x80000003 0x00A72E

15.0.0.0 25.0.0.1 63 0x80000003 0x005C75

Type-5 AS External Link States

Link ID ADV Router Age Seq# Checksum Tag

20.0.0.0 25.0.0.1 1758 0x80000001 0x00FA77 0

R3#

R3#sh ip route

O E2 20.0.0.0/8 [110/20] via 25.0.0.2, 00:01:41, Serial1/0

C 25.0.0.0/8 is directly connected, Serial1/0

O IA 10.0.0.0/8 [110/129] via 25.0.0.2, 00:01:41, Serial1/0

C 30.0.0.0/8 is directly connected, FastEthernet0/0

O IA 15.0.0.0/8 [110/128] via 25.0.0.2, 00:01:41, Serial1/0

R3#

Task 2:

Configure Area 2 as NSSA total stub network

!R2/R3

router ospf 1

area 2 nssa no-summary

Verification:

R3#sh ip ospf database

OSPF Router with ID (30.0.0.1) (Process ID 1)

Router Link States (Area 2)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
25.0.0.1	25.0.0.1	28	0x8000000A	0x009476	2
30.0.0.1	30.0.0.1	26	0x80000008	0x002AB0	3

Summary Net Link States (Area 2)

Link ID	ADV Router	Age	Seq#	Checksum
0.0.0.0	25.0.0.1	44	0x80000001	0x0051CA

Type-7 AS External Link States (Area 2)

Link ID	ADV Router	Age	Seq#	Checksum	Tag
20.0.0.0	25.0.0.1	43	0x80000001	0x00DE91	0

R3#

R3#sh ip route

O N2 20.0.0.0/8 [110/20] via 25.0.0.2, 00:01:06, Serial1/0

C 25.0.0.0/8 is directly connected, Serial1/0

C 30.0.0.0/8 is directly connected, FastEthernet0/0

O*IA 0.0.0.0/0 [110/65] via 25.0.0.2, 00:01:06, Serial1/0

R3#

Ping between PCs should be working fine....

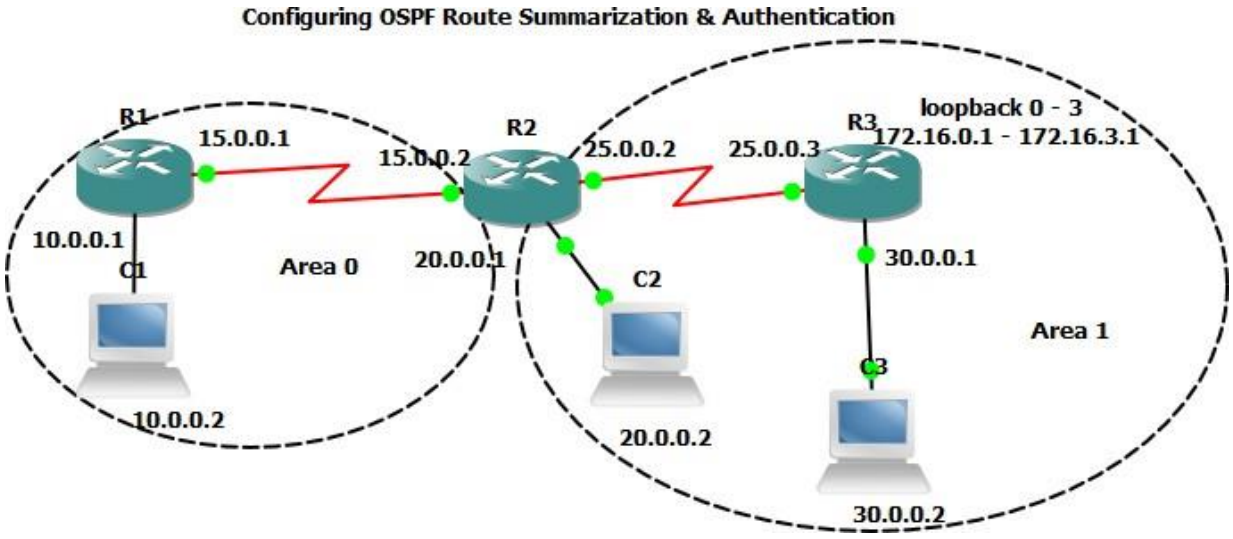
Lab 17

Configure OSPF Route Summarization & OSPF Authentication

Objective:

The target of this lab is to enable students deal with OSPF route summarization, and also learn how to configure ospf authentication.

Diagram:



Preliminary Task:

Connect the network as shown in the diagram, and configure IP address for all the physical interfaces as described above.

Task1:

Configure the loopback interfaces on R3 from Loopback 0 to Loopback 3 as described above, and change their network type to pint-to-point to allow these networks later to be advertised in OSPF as /24 networks

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

```
!R3
interface Loopback0
 ip address 172.16.0.1 255.255.255.0
ip ospf network point-to-point
!
interface Loopback1
 ip address 172.16.1.1 255.255.255.0
ip ospf network point-to-point
!
interface Loopback2
 ip address 172.16.2.1 255.255.255.0
ip ospf network point-to-point
!
interface Loopback3
 ip address 172.16.3.1 255.255.255.0
ip ospf network point-to-point
!
```

Task 2:

Configure OSPF areas as shown in the diagram

```
!R1
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
```

```
 network 15.0.0.0 0.255.255.255 area 0
!
!R2
router ospf 1
 network 15.0.0.0 0.255.255.255 area 0
 network 20.0.0.0 0.255.255.255 area 1
 network 25.0.0.0 0.255.255.255 area 1
!
!R3
router ospf 1
 log-adjacency-changes
 network 25.0.0.0 0.255.255.255 area 1
 network 30.0.0.0 0.255.255.255 area 1
 network 172.16.0.0 0.0.0.255 area 1
 network 172.16.1.0 0.0.0.255 area 1
 network 172.16.2.0 0.0.0.255 area 1
 network 172.16.3.0 0.0.0.255 area 1
!
```

Verification:

```
R1#sh ip route


O IA 20.0.0.0/8 [110/65] via 15.0.0.2, 00:11:05, Serial1/0
```

172.16.0.0/24 is subnetted, 4 subnets

O IA 172.16.0.0 [110/129] via 15.0.0.2, 00:00:03, Serial1/0

O IA 172.16.1.0 [110/129] via 15.0.0.2, 00:00:03, Serial1/0

O IA 172.16.2.0 [110/129] via 15.0.0.2, 00:00:03, Serial1/0

O IA 172.16.3.0 [110/129] via 15.0.0.2, 00:00:03, Serial1/0

O IA 25.0.0.0/8 [110/128] via 15.0.0.2, 00:10:55, Serial1/0

C 10.0.0.0/8 is directly connected, FastEthernet0/0

O IA 30.0.0.0/8 [110/129] via 15.0.0.2, 00:08:56, Serial1/0

C 15.0.0.0/8 is directly connected, Serial1/0

R1#

Task 3:

Configure R2 to summarize loopback networks towards R1

!R2

router ospf 1

area 1 range 172.16.0.0 255.255.252.0

Verification:

R1#sh ip route

O IA 20.0.0.0/8 [110/65] via 15.0.0.2, 00:15:08, Serial1/0

172.16.0.0/22 is subnetted, 1 subnets

O IA 172.16.0.0 [110/129] via 15.0.0.2, 00:00:18, Serial1/0

O IA 25.0.0.0/8 [110/128] via 15.0.0.2, 00:14:58, Serial1/0

C 10.0.0.0/8 is directly connected, FastEthernet0/0

O IA 30.0.0.0/8 [110/129] via 15.0.0.2, 00:12:59, Serial1/0

C 15.0.0.0/8 is directly connected, Serial1/0

R1#

Task 4:

Configure Simple password ospf authentication between R1 & R2 using key-string **cisco123**

!R1/R2

interface s1/0

ip ospf authentication-key cisco123

ip ospf authentication

Verification:

R2#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
15.0.0.1	0	FULL/ -	00:00:33	15.0.0.1	Serial1/0
172.16.3.1	0	FULL/ -	00:00:31	25.0.0.3	Serial1/1

R2#

Task 5:

Configure the most secure ospf authentication between R2 & R3, using md5 authentication, key 1 & key-string cisco123

!R2

interface s1/1

ip ospf message-digest-key 1 md5 cisco123

ip ospf authentication message-digest

!R3

interface s1/0

ip ospf message-digest-key 1 md5 cisco123

ip ospf authentication message-digest

Verification:

R3#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
25.0.0.2	0	FULL/ -	00:00:32	25.0.0.2	Serial1/0

R3#

Ping should be working fine between PCs....

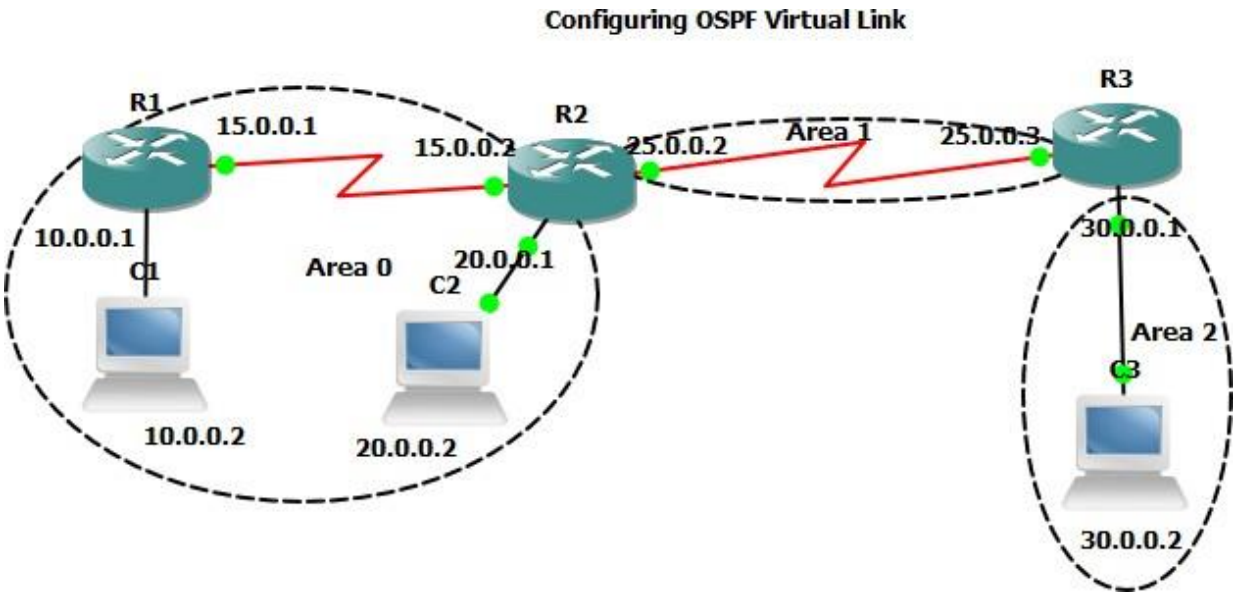
Lab 18

Configuring OSPF Virtual Links

Objective:

The main target of this lab is configure virtual link which enables remote areas to be connected to area 0 through virtual connection.

Diagram:



Preliminary Task:

Connect the network as shown in diagram above, assign all the ip addresses as described.

Task 1:

Configure OSPF areas as shown in the diagram

!R1

router ospf 1

log-adjacency-changes

network 10.0.0.0 0.255.255.255 area 0

network 15.0.0.0 0.255.255.255 area 0

!

!R2

router ospf 1

network 15.0.0.0 0.255.255.255 area 0

network 20.0.0.0 0.255.255.255 area 0

network 25.0.0.0 0.255.255.255 area 1

!

!R3

router ospf 1

network 25.0.0.0 0.255.255.255 area 1

network 30.0.0.0 0.255.255.255 area 2

!

!Verification

R1#sh ip route

O 20.0.0.0/8 [110/65] via 15.0.0.2, 00:03:29, Serial1/0

O IA 25.0.0.0/8 [110/128] via 15.0.0.2, 00:03:19, Serial1/0

C 10.0.0.0/8 is directly connected, FastEthernet0/0

C 15.0.0.0/8 is directly connected, Serial1/0

You can notice that network 30.0.0.0/8 is not shown in R1's routing table, because it is in an area that is not directly connected to area 0.

Task 2:

Configure a virtual link between R2 & R3 to enable R3 to have a direct virtual link to area 0

!R2

router ospf 1

area 1 virtual-link 30.0.0.1

!

R3

router ospf 1

area 1 virtual-link 25.0.0.2

!Verification:

R3#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
25.0.0.2	0	FULL/ -	-	25.0.0.2	OSPF_VL0
25.0.0.2	0	FULL/ -	00:00:34	25.0.0.2	Serial1/0

R3#

R3#

O 20.0.0.0/8 [110/65] via 15.0.0.2, 00:18:24, Serial1/0

O IA 25.0.0.0/8 [110/128] via 15.0.0.2, 00:18:14, Serial1/0

C 10.0.0.0/8 is directly connected, FastEthernet0/0

O IA 30.0.0.0/8 [110/129] via 15.0.0.2, 00:00:21, Serial1/0

C 15.0.0.0/8 is directly connected, Serial1/0

R1#

Ping between all devices should be working...

Redistribution, Route Filtering and Manipulation Module

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

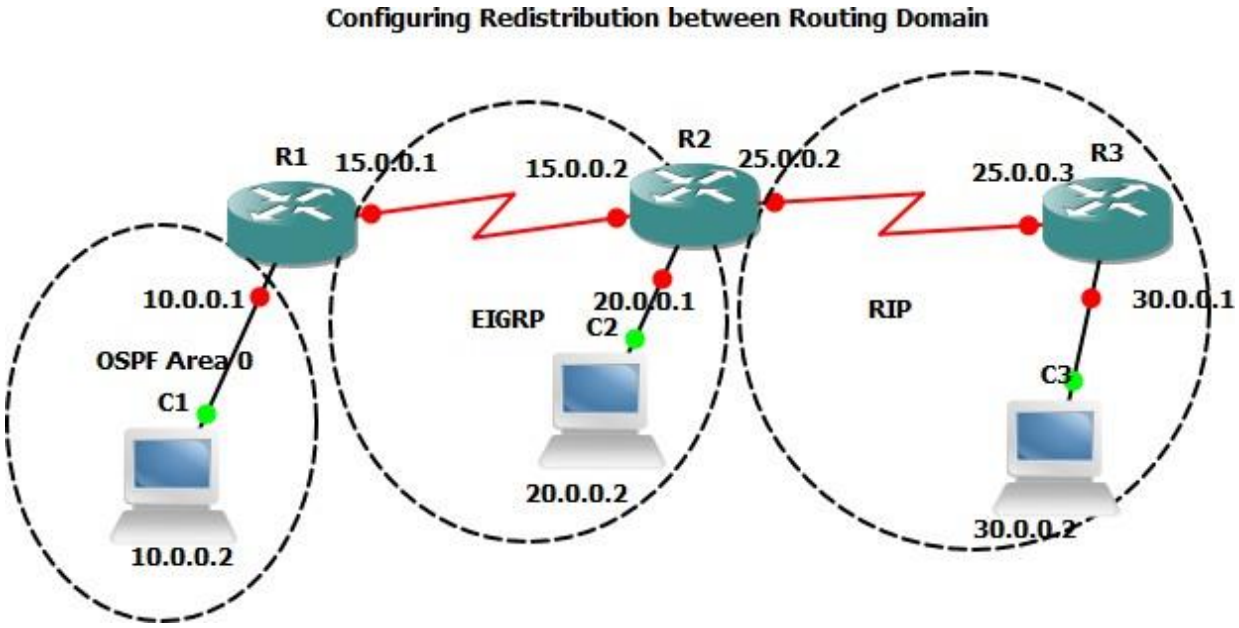
Lab 19

Redistribution Between Routing Protocols & Passive-Interface On RIP

Objective:

The main purpose of this lab is enable students to configure mutual redistribution between RIP, EIGRP & OSPF.

Diagram:



Preliminary Task:

Connect the network as shown in the above diagram, configure the ip addresses as described.

Task 1:

Configure RIP version 2, EIGRP & OSPF as shown in the figure.

!R1

router ospf 1

```
network 10.0.0.0 0.255.255.255 area 0
!
router eigrp 1
network 15.0.0.0
no auto-summary

!R2
router eigrp 1
network 15.0.0.0
network 20.0.0.0
no auto-summary
!
router rip
version 2
network 25.0.0.0
no auto-summary
!R3
router rip
version 2
network 25.0.0.0
network 30.0.0.0
no auto-summary
```

Task 2:

Redistribute from OSPF into EIGRP at R1, then mutual redistribute between EIGRP & RIP setting the routes metric injected into RIP to be 2.

!R1

router eigrp 1

redistribute ospf 1 metric 10000 100 1 255 1500

!R2

router eigrp 1

redistribute rip metric 10000 100 1 255 1500

!

router rip

redistribute eigrp 1 metric 2

Verification:

R1#sh ip route

D 20.0.0.0/8 [90/2172416] via 15.0.0.2, 00:03:24, Serial1/0

D EX 25.0.0.0/8 [170/2195456] via 15.0.0.2, 00:00:28, Serial1/0

C 10.0.0.0/8 is directly connected, FastEthernet0/0

D EX 30.0.0.0/8 [170/2195456] via 15.0.0.2, 00:00:28, Serial1/0

C 15.0.0.0/8 is directly connected, Serial1/0

R3#sh ip route

R 20.0.0.0/8 [120/2] via 25.0.0.2, 00:00:04, Serial1/0

C 25.0.0.0/8 is directly connected, Serial1/0

R 10.0.0.0/8 [120/2] via 25.0.0.2, 00:00:04, Serial1/0

C 30.0.0.0/8 is directly connected, FastEthernet0/0

R 15.0.0.0/8 [120/2] via 25.0.0.2, 00:00:04, Serial1/0

R3#

Ping should be successful between all devices....

Task 3:

Configure passive interface S1/0 on R3, and check the routing table on R3 & R2, after clearing the routing table.

!R3

router rip

passive-interface s1/0

Verification:

R3#clear ip route *

R2# clear ip route *

R3#sh ip route

R 20.0.0.0/8 [120/2] via 25.0.0.2, 00:00:11, Serial1/0

C 25.0.0.0/8 is directly connected, Serial1/0

R 10.0.0.0/8 [120/2] via 25.0.0.2, 00:00:11, Serial1/0

C 30.0.0.0/8 is directly connected, FastEthernet0/0

R 15.0.0.0/8 [120/2] via 25.0.0.2, 00:00:11, Serial1/0

R3#

R2#sh ip route

C 20.0.0.0/8 is directly connected, FastEthernet0/0

C 25.0.0.0/8 is directly connected, Serial1/1

D EX 10.0.0.0/8 [170/2195456] via 15.0.0.1, 00:01:21, Serial1/0

C 15.0.0.0/8 is directly connected, Serial1/0

R2#

Note: R2 is receiving any routes from R3, because its serial is configured passive-interface.

Lab 20

Route Filtering Using Distribute-List & Route-map

Objective:

The target of this lab is to do some route manipulation using Distribute-list and Route-map.

Diagram:

Based on the Diagram in Lab 17

Task 1:

Continue on Lab 17, disable the passive-interface configuration on R3

```
!R3
router rip
no passive-interface s1/0
!
```

Task 2:

Configure on R3 loopback interfaces ranging from Loopback 0 to loopback 7 which should be having addresses from 192.168.0.1 to 192.168.7.1, and then advertise them into RIP.

```
!R3
interface Loopback0
 ip address 192.168.0.1 255.255.255.0
!
interface Loopback1
 ip address 192.168.1.1 255.255.255.0
```

```
!
interface Loopback2
 ip address 192.168.2.1 255.255.255.0
!
interface Loopback3
 ip address 192.168.3.1 255.255.255.0
!
interface Loopback4
 ip address 192.168.4.1 255.255.255.0
!
interface Loopback5
 ip address 192.168.5.1 255.255.255.0
!
interface Loopback6
 ip address 192.168.6.1 255.255.255.0
!
interface Loopback7
 ip address 192.168.7.1 255.255.255.0
!
router rip
 network 192.168.0.0
 network 192.168.1.0
```

network 192.168.2.0

network 192.168.3.0

network 192.168.4.0

network 192.168.5.0

network 192.168.6.0

network 192.168.7.0

Verification:

R2#sh ip route

C 20.0.0.0/8 is directly connected, FastEthernet0/0

C 25.0.0.0/8 is directly connected, Serial1/1

R 192.168.4.0/24 [120/1] via 25.0.0.3, 00:00:05, Serial1/1

R 192.168.5.0/24 [120/1] via 25.0.0.3, 00:00:05, Serial1/1

D EX 10.0.0.0/8 [170/2195456] via 15.0.0.1, 00:28:32, Serial1/0

R 192.168.6.0/24 [120/1] via 25.0.0.3, 00:00:05, Serial1/1

R 192.168.7.0/24 [120/1] via 25.0.0.3, 00:00:05, Serial1/1

R 192.168.0.0/24 [120/1] via 25.0.0.3, 00:00:05, Serial1/1

R 192.168.1.0/24 [120/1] via 25.0.0.3, 00:00:05, Serial1/1

R 192.168.2.0/24 [120/1] via 25.0.0.3, 00:00:05, Serial1/1

R 192.168.3.0/24 [120/1] via 25.0.0.3, 00:00:05, Serial1/1

R 30.0.0.0/8 [120/1] via 25.0.0.3, 00:00:05, Serial1/1

C 15.0.0.0/8 is directly connected, Serial1/0

R2#

Task 3:

Configure distribute-list on R2 to accept only networks from 192.168.4.0 to 192.168.7.0

!R2

access-list 18 deny 192.168.0.0 0.0.3.255

access-list 18 permit any

!

router rip

distribute-list 18 in s1/1

Verification:

R2#clear ip route *

R2#sh ip route

C 20.0.0.0/8 is directly connected, FastEthernet0/0

C 25.0.0.0/8 is directly connected, Serial1/1

R 192.168.4.0/24 [120/1] via 25.0.0.3, 00:00:00, Serial1/1

R 192.168.5.0/24 [120/1] via 25.0.0.3, 00:00:00, Serial1/1

D EX 10.0.0.0/8 [170/2195456] via 15.0.0.1, 00:00:08, Serial1/0

R 192.168.6.0/24 [120/1] via 25.0.0.3, 00:00:00, Serial1/1

R 192.168.7.0/24 [120/1] via 25.0.0.3, 00:00:00, Serial1/1

R 30.0.0.0/8 [120/1] via 25.0.0.3, 00:00:00, Serial1/1

C 15.0.0.0/8 is directly connected, Serial1/0

R1#sh ip route

D   20.0.0.0/8 [90/2172416] via 15.0.0.2, 00:59:13, Serial1/0

D EX 25.0.0.0/8 [170/2195456] via 15.0.0.2, 00:56:17, Serial1/0

D EX 192.168.4.0/24 [170/2195456] via 15.0.0.2, 00:02:58, Serial1/0

D EX 192.168.5.0/24 [170/2195456] via 15.0.0.2, 00:02:58, Serial1/0

C   10.0.0.0/8 is directly connected, FastEthernet0/0

D EX 192.168.6.0/24 [170/2195456] via 15.0.0.2, 00:02:58, Serial1/0

D EX 192.168.7.0/24 [170/2195456] via 15.0.0.2, 00:02:58, Serial1/0

D EX 30.0.0.0/8 [170/2195456] via 15.0.0.2, 00:02:58, Serial1/0

C   15.0.0.0/8 is directly connected, Serial1/0

R1#

Task 4:

Configure R2 to modify redistribution from RIP to EIGRP to deny networks 192.168.4.0 & 192.168.5.0 from being redistributed.

!R2

access-list 19 permit 192.168.4.0 0.0.1.255

route-map rip-to-eigrp deny 10

match ip address 19

route-map rip-to-eigrp permit 100

!

router eigrp 1

redistribute rip metric 1000 100 1 255 1500 route-map rip-to-eigrp

Verification:

R1#sh ip route

D 20.0.0.0/8 [90/2172416] via 15.0.0.2, 01:15:13, Serial1/0

D EX 25.0.0.0/8 [170/3097600] via 15.0.0.2, 00:00:17, Serial1/0

C 10.0.0.0/8 is directly connected, FastEthernet0/0

D EX 192.168.6.0/24 [170/3097600] via 15.0.0.2, 00:00:17, Serial1/0

D EX 192.168.7.0/24 [170/3097600] via 15.0.0.2, 00:00:17, Serial1/0

D EX 30.0.0.0/8 [170/3097600] via 15.0.0.2, 00:00:17, Serial1/0

C 15.0.0.0/8 is directly connected, Serial1/0

R1#

BGP Module

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

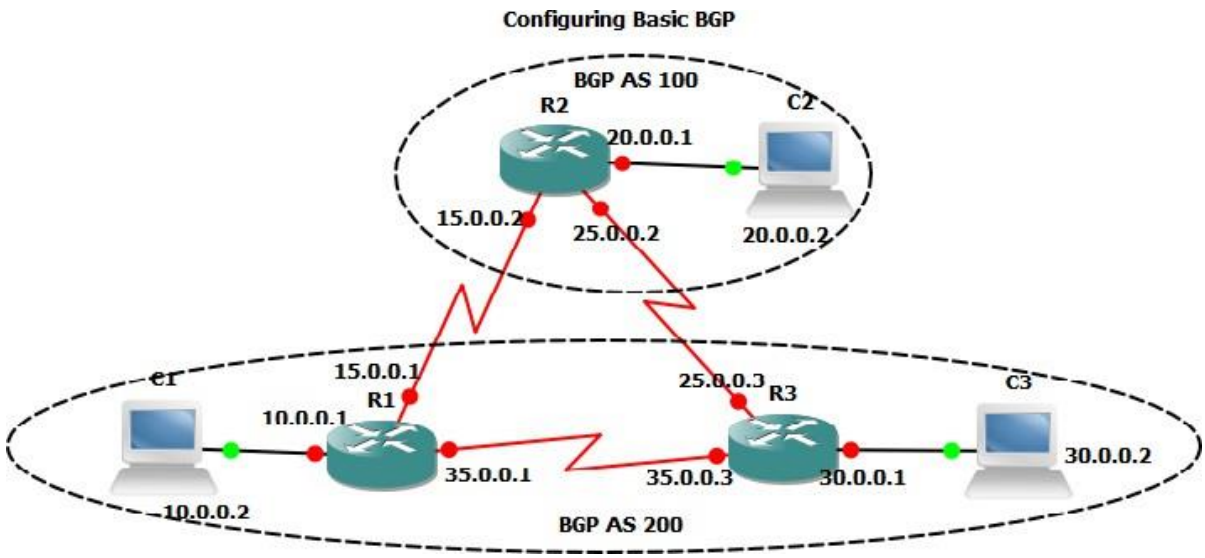
Lab 21

Basic BGP Configuration

Objective:

The main target of this lab is configure basic BGP configuration, and to check the BGP & routing table.

Diagram:



Preliminary Tasks:

Connect the network as shown in the diagram, and assign the described IP addresses.

Task 1:

Configure BGP neighbor relationship between R1, R2 & R3. R1 & R3 should be in AS 200, R1 should be in AS 100. Then advertise all the connected network into BGP.

```
!R1
router bgp 200
network 10.0.0.0
 network 15.0.0.0
 network 35.0.0.0
 neighbor 15.0.0.2 remote-as 100
 neighbor 35.0.0.3 remote-as 200

!R2
router bgp 100
network 15.0.0.0
 network 20.0.0.0
 network 25.0.0.0
 neighbor 15.0.0.1 remote-as 200
 neighbor 25.0.0.3 remote-as 200

!R3
router bgp 200
 network 25.0.0.0
 network 30.0.0.0
 network 35.0.0.0
 neighbor 25.0.0.2 remote-as 100
```

neighbor 35.0.0.1 remote-as 200

!

Verification

R1#sh ip bgp summary

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
15.0.0.2	4	100	14	15	8	0	0	00:10:38	3
35.0.0.3	4	200	15	14	8	0	0	00:08:26	4

R1#

R1#sh ip route

C 35.0.0.0/8 is directly connected, Serial1/1

B 20.0.0.0/8 [20/0] via 15.0.0.2, 00:11:22

B 25.0.0.0/8 [200/0] via 35.0.0.3, 00:09:51

C 10.0.0.0/8 is directly connected, FastEthernet0/0

B 30.0.0.0/8 [200/0] via 35.0.0.3, 00:09:57

C 15.0.0.0/8 is directly connected, Serial1/0

R1#

R1#sh ip bgp

```
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.0.0.0         0.0.0.0                  0         32768 i
*  15.0.0.0         15.0.0.2                 0             0 100 i
*>                  0.0.0.0                  0         32768 i
* i20.0.0.0         25.0.0.2                 0    100      0 100 i
*>                  15.0.0.2                 0             0 100 i
*>i25.0.0.0         35.0.0.3                 0    100      0 i
*                   15.0.0.2                 0             0 100 i
*>i30.0.0.0         35.0.0.3                 0    100      0 i
* i35.0.0.0         35.0.0.3                 0    100      0 i
*>                  0.0.0.0                  0         32768 i
R1#
```

Ping Should be successful between All PCs.....

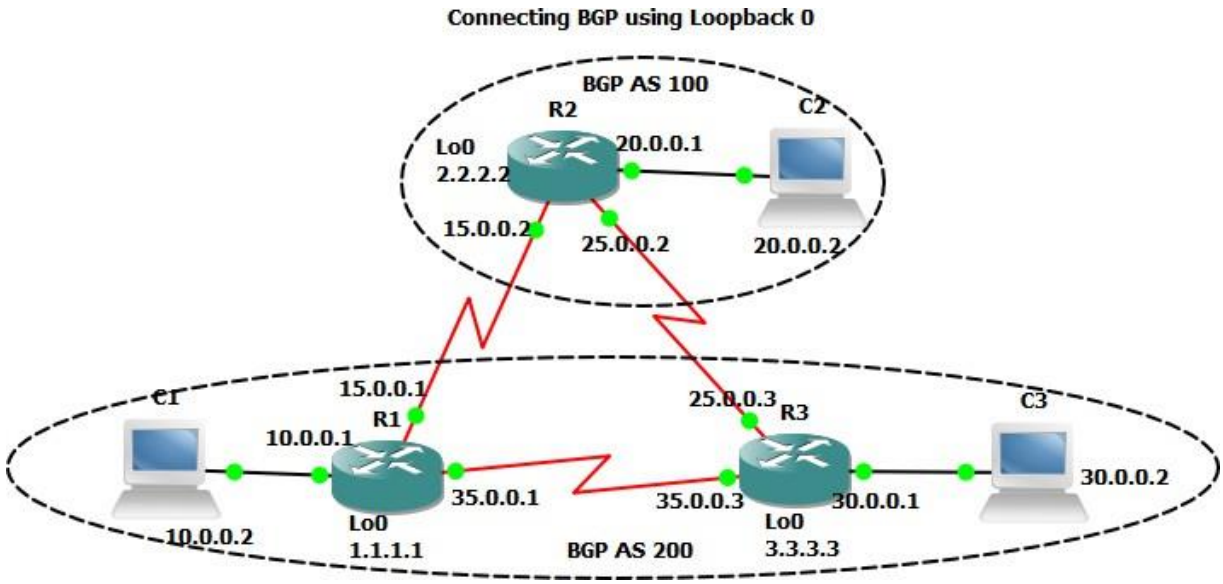
Lab 22

Connecting BGP Using Loopback 0

Objective:

The main target of this lab is to configure BGP using loopback addresses, and to configure ebgp-multihop on the ebgp neighbor relation.

Diagram:



Task 1:

Following Lab 19, remove the bgp configuration on all routers. Then configure loopback interfaces on all routers as shown in the diagram.

!R1/R3

no router bgp 200

!R2

no router bgp 100

!

!R1

int lo0

ip add 1.1.1.1 255.255.255.255

!R2

int lo0

ip add 2.2.2.2 255.255.255.255

!

!R3

int lo0

ip add 3.3.3.3 255.255.255.255

Task 2:

Configure static routes on all routers to point to the neighbor router's loopback addresses, as the BGP won't establish peering with addresses that can't reach in IGP.

!R1

ip route 2.2.2.2 255.255.255.255 15.0.0.2

ip route 3.3.3.3 255.255.255.255 35.0.0.3

!R2

ip route 1.1.1.1 255.255.255.255 15.0.0.1

ip route 3.3.3.3 255.255.255.255 25.0.0.3

!R3

ip route 2.2.2.2 255.255.255.255 25.0.0.2

ip route 1.1.1.1 255.255.255.255 35.0.0.2

Task 3:

Configure BGP as shown in the diagram, and use loopback 0 for peering instead of the physical interfaces. However, don't forget the ebgp-multihop command when you do ebgp peering, as the ebgp peering is expected to peer up by default with the physical interface, and to have the ebgp neighbor directly connected. So, we configure the command ebgp multi-hop to allow multiple hops between ebgp neighbors.

!R1

router bgp 200

neighbor 2.2.2.2 remote-as 100

neighbor 2.2.2.2 update-source lo0

neighbor 2.2.2.2 ebgp-multihop 2

neighbor 3.3.3.3 remote-as 200

neighbor 3.3.3.3 update-source lo0

network 10.0.0.0

network 15.0.0.0

network 35.0.0.0

!R2

```
router bgp 100
neighbor 1.1.1.1 remote-as 200
neighbor 1.1.1.1 update-source lo0
neighbor 1.1.1.1 ebgp-multihop 2
neighbor 3.3.3.3 remote-as 200
neighbor 3.3.3.3 update-source lo0
neighbor 3.3.3.3 ebgp-multihop 2
network 20.0.0.0
network 25.0.0.0
network 15.0.0.0

!R3
router bgp 200
neighbor 2.2.2.2 remote-as 100
neighbor 2.2.2.2 update-source lo0
neighbor 2.2.2.2 ebgp-multihop 2
neighbor 1.1.1.1 remote-as 200
neighbor 1.1.1.1 update-source lo0
network 30.0.0.0
network 25.0.0.0
network 35.0.0.0
```

Verification:

R1#sh ip bgp summary

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2.2.2.2         4   100       6       6        8    0    0 00:02:27        3
3.3.3.3         4   200       6       7        8    0    0 00:01:58        4
```

R1#sh ip bgp

```
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.0.0.0         0.0.0.0                  0         32768 i
*  15.0.0.0         2.2.2.2                  0             0 100 i
*>                  0.0.0.0                  0         32768 i
* i20.0.0.0         2.2.2.2                  0    100      0 100 i
*>                  2.2.2.2                  0             0 100 i
*>i25.0.0.0         3.3.3.3                  0    100      0 i
*                   2.2.2.2                  0             0 100 i
*>i30.0.0.0         3.3.3.3                  0    100      0 i
* i35.0.0.0         3.3.3.3                  0    100      0 i
*>                  0.0.0.0                  0         32768 i
```

Ping should still be working between devices....

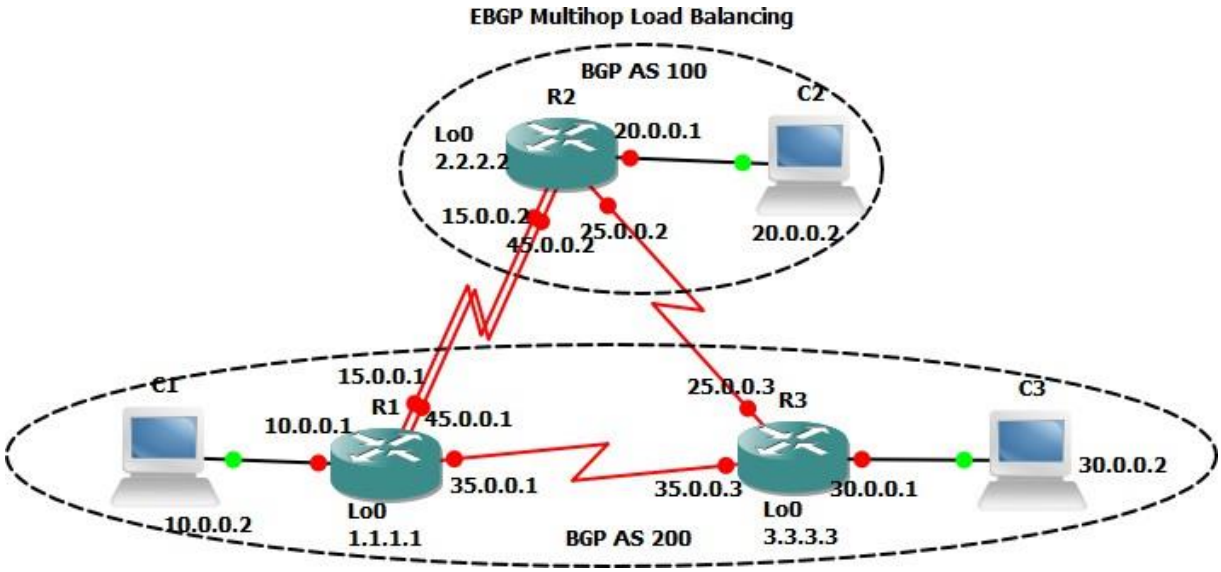
Lab 23

EBGP Multihop Load Balancing

Objective:

The main target of this lab is to configure load balancing design between two ebgp neighbors.

Diagram:



Preliminary Task:

Based on Lab 20, Connect additional serial cable between R1 & R2, configure the new IP addresses for the two serial ports.

Task 1:

Configure static route on R1 & R2 to point out to the loopback interfaces of R2/R1 through the new serial connection.

!R1

ip route 2.2.2.2 255.255.255.255 45.0.0.2

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

!R2

ip route 1.1.1.1 255.255.255.255 45.0.0.1

Verification:

R1#sh ip bgp summary

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
2.2.2.2	4	100	15	14	7	0	0	00:10:53	3
3.3.3.3	4	200	14	14	7	0	0	00:10:56	4

R1#

R1#show ip route

```
    1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback0
C    35.0.0.0/8 is directly connected, Serial1/1
    2.0.0.0/32 is subnetted, 1 subnets
S       2.2.2.2 [1/0] via 45.0.0.2
                [1/0] via 15.0.0.2
    3.0.0.0/32 is subnetted, 1 subnets
S       3.3.3.3 [1/0] via 35.0.0.3
B    20.0.0.0/8 [20/0] via 2.2.2.2, 00:11:13
B    25.0.0.0/8 [200/0] via 3.3.3.3, 00:11:14
C    10.0.0.0/8 is directly connected, FastEthernet0/0
```

C 45.0.0.0/8 is directly connected, Serial1/2

B 30.0.0.0/8 [200/0] via 3.3.3.3, 00:11:14

C 15.0.0.0/8 is directly connected, Serial1/0

R1#traceroute 2.2.2.2

1 45.0.0.2 72 msec

15.0.0.2 20 msec

45.0.0.2 44 msec

R1#

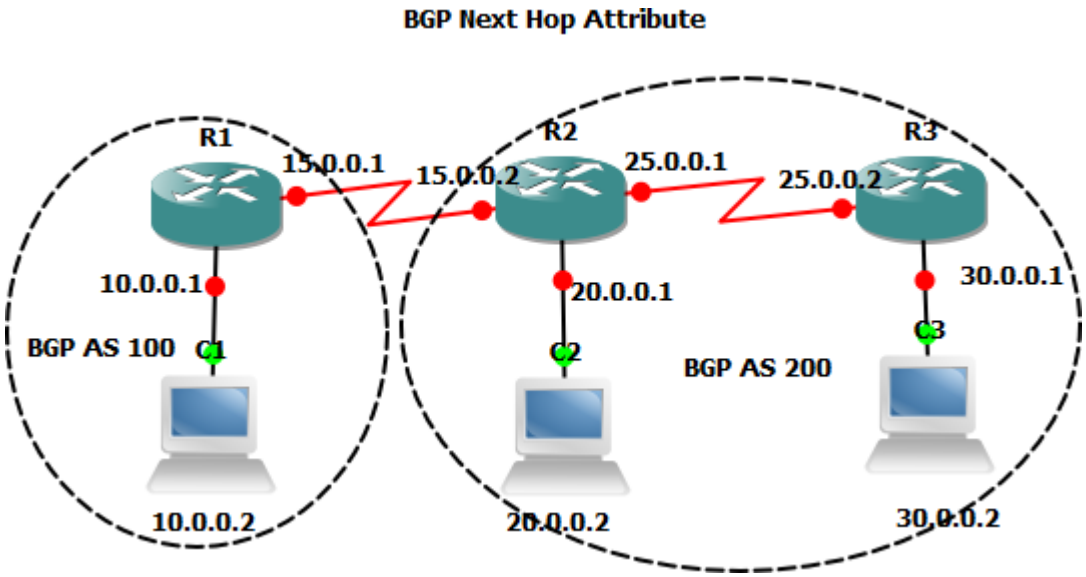
Lab 24

BGP Next Hop Attribute

Objective:

The target of this lab is to configure Next Hop Self command, to resolve the problems that could arise from advertising an ebgp route to an ibgp neighbor using default bgp configuration.

Diagram:



Preliminary Task:

Connect the network as shown in the diagram, and assign the ip addresses as explained in the above figure.

Task 1:

Configure BGP neighbor relation between R1 & R2, R2 & R3 relation according to AS numbers explained in the figure. Then advertise all the Ethernet networks into BGP.

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

!R1

router bgp 100

neighbor 15.0.0.2 remote-as 200

network 10.0.0.0

!R2

router bgp 200

neighbor 15.0.0.1 remote-as 100

neighbor 25.0.0.3 remote-as 200

network 20.0.0.0

!R3

router bgp 200

neighbor 25.0.0.2 remote-as 200

network 30.0.0.0

Verification:

R3#sh ip route

B 20.0.0.0/8 [200/0] via 25.0.0.2, 00:06:14

C 25.0.0.0/8 is directly connected, Serial1/0

C 30.0.0.0/8 is directly connected, FastEthernet0/0

Note: Network 10.0.0.0 is not in R3's routing table

R3#sh ip bgp

BGP table version is 9, local router ID is 30.0.0.1

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

r RIB-failure, S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
* i10.0.0.0	15.0.0.1	0	100	0	100 i
*>i20.0.0.0	25.0.0.2	0	100	0	i
*> 30.0.0.0	0.0.0.0	0		32768	i

Network 10.0.0.0 is in the BGP table, but it hasn't been indicated as a best route, because the next hop (15.0.0.1) is not known in R3's routing table.

Task 2:

Configure R2 to advertise BGP routes to R1 & R3 with a next hop set to be R2's physical interface.

!R2

router bgp 200

neighbor 15.0.0.1 next-hop-self

neighbor 25.0.0.3 next-hop-self

Verification:

R3#sh ip bgp

Network	Next Hop	Metric	LocPrf	Weight	Path
*>i10.0.0.0	25.0.0.2	0	100	0	100 i
*>i20.0.0.0	25.0.0.2	0	100	0	i
*> 30.0.0.0	0.0.0.0	0		32768	i

R3#

R3#sh ip route

B 20.0.0.0/8 [200/0] via 25.0.0.2, 00:17:53

C 25.0.0.0/8 is directly connected, Serial1/0

B 10.0.0.0/8 [200/0] via 25.0.0.2, 00:01:10

C 30.0.0.0/8 is directly connected, FastEthernet0/0

R3#

Note: Network 10.0.0.0 has shown up in R3's routing table after changing the next hop.

Ping between all devices should be working fine.....

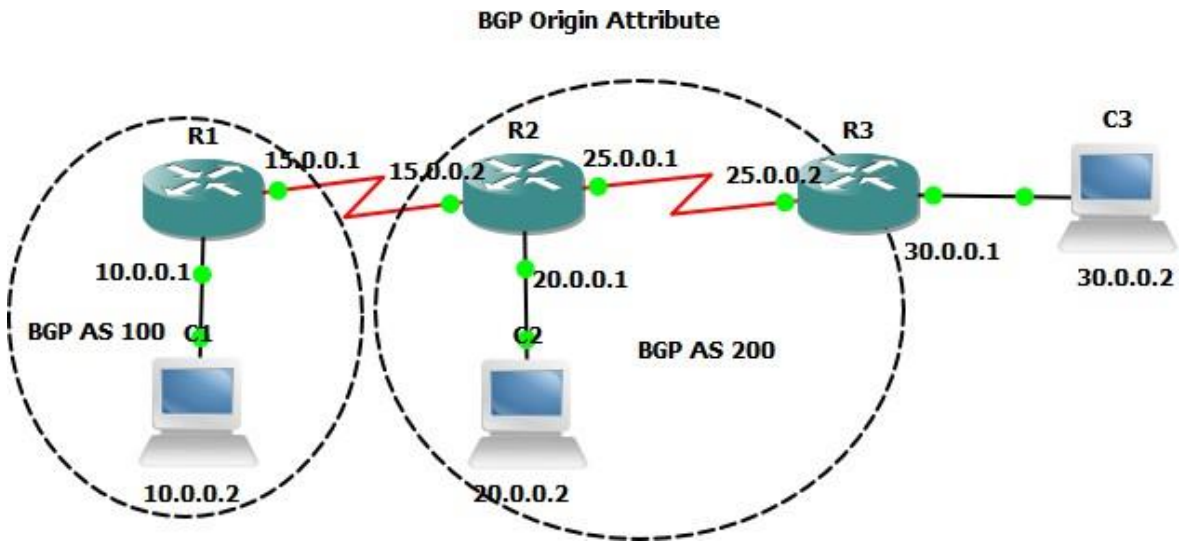
Lab 25

BGP Origin Attribute

Objective:

The main target of this lab is to configure BGP network that shows the different types of Origin Attribute, and its influence in BGP selection criteria.

Diagram:



Task 1:

Continuing on Lab 22, disable BGP configuration on all routers, and then configure BGP as shown in the diagram, and advertise all the connected networks that fall within the BGP domain (Don't Advertise network 30.0.0.0 into the BGP).

!R1

no router BGP 100

!R2/R3

no router BGP 200

!R1

router bgp 100

neighbor 15.0.0.2 remote-as 200

network 10.0.0.0

network 15.0.0.0

!R2

router bgp 200

neighbor 15.0.0.1 remote-as 100

neighbor 25.0.0.3 remote-as 200

network 15.0.0.0

network 25.0.0.0

network 20.0.0.0

!R3

router bgp 200

neighbor 25.0.0.2 remote-as 200

network 25.0.0.0

!Verification:

R2#sh ip bgp summary

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
15.0.0.1	4	100	6	7	8	0	0	00:02:53	2
25.0.0.3	4	200	6	9	8	0	0	00:02:55	2

Task 2:

Configure a Static Route on R2 to point out to network 30.0.0.0, then redistribute this route into BGP.

!R2

ip route 30.0.0.0 255.0.0.0 25.0.0.3

router bgp 200

redistribute static

!Verification:

R1#sh ip bgp

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 10.0.0.0	0.0.0.0	0		32768	i
* 15.0.0.0	15.0.0.2	0		0	200 i
*>	0.0.0.0	0		32768	i
*> 20.0.0.0	15.0.0.2	0		0	200 i
*> 25.0.0.0	15.0.0.2	0		0	200 i
*> 30.0.0.0	15.0.0.2	0		0	200 ?

Note: On R1 BGP table, the 200? explains that the network has been learned through redistribution.

Ping should be working fine between all devices....

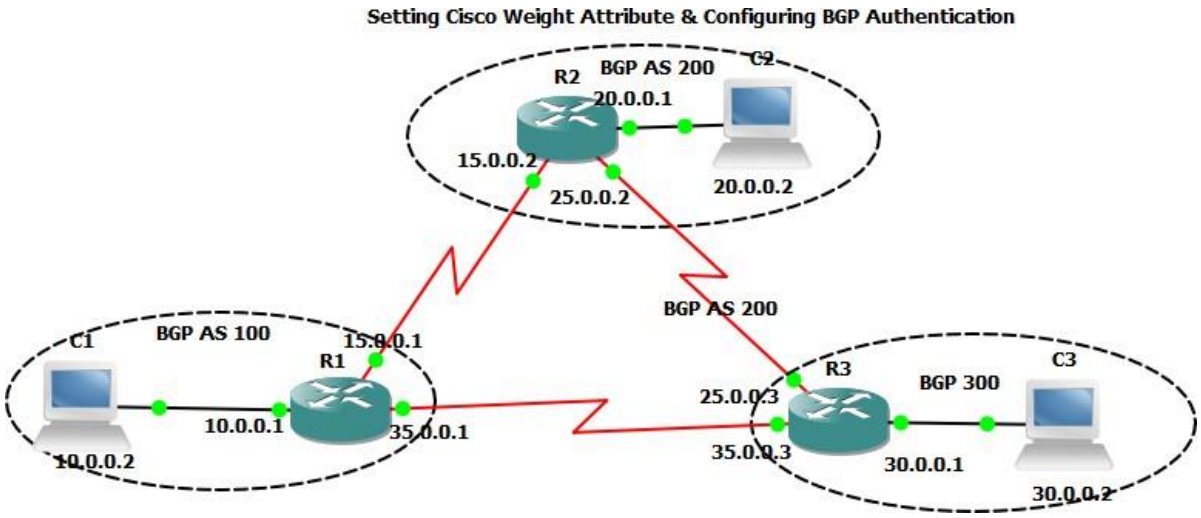
Lab 26

Setting Cisco Weight Attribute & Configuring BGP Authentication

Objective:

The main target of this lab is to set the Cisco Weight attribute as a selection criteria, and establish a secure BGP neighbor relationship.

Diagram:



Preliminary Task :

Connect the network as shown in the diagram, and assign the ip addresses as described in the figure above.

Task 1:

Configure BGP on all routers as shown in the figure using secure neighbor relationship, then advertise all the connected network in BGP.

!R1

router bgp 100

neighbor 15.0.0.2 remote-as 200

neighbor 15.0.0.2 password 123

neighbor 35.0.0.3 remote-as 300

neighbor 35.0.0.3 password 123

network 10.0.0.0

network 15.0.0.0

network 35.0.0.0

!R2

router bgp 200

neighbor 15.0.0.1 remote-as 100

neighbor 15.0.0.1 password 123

neighbor 25.0.0.3 remote-as 300

neighbor 25.0.0.3 password 123

network 20.0.0.0

network 25.0.0.0

network 15.0.0.0

!R3

router bgp 300

neighbor 25.0.0.2 remote-as 200

neighbor 25.0.0.2 password 123

neighbor 35.0.0.1 remote-as 100

neighbor 35.0.0.1 password 123

network 30.0.0.0

network 25.0.0.0

network 35.0.0.0

!Verification:

R2#sh ip bgp summary

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
15.0.0.1	4	100	6	6	7	0	0	00:02:53	3
25.0.0.3	4	300	6	6	7	0	0	00:01:33	4

R2#

R1#sh ip bgp

	Network	Next Hop	Metric	LocPrf	Weight	Path
*>	10.0.0.0	0.0.0.0	0		32768	i
*	15.0.0.0	35.0.0.3			0	300 200 i
*		15.0.0.2	0		0	200 i
*>		0.0.0.0	0		32768	i
*	20.0.0.0	35.0.0.3			0	300 200 i
*>		15.0.0.2	0		0	200 i
*	25.0.0.0	35.0.0.3	0		0	300 i
*>		15.0.0.2	0		0	200 i

*> 30.0.0.0 35.0.0.3 0 0 300 i

* 15.0.0.2 0 200 300 i

* 35.0.0.0 35.0.0.3 0 0 300 i

*> 0.0.0.0 0 32768 i

R1#

Task 2:

As highlighted in the previous BGP table of R1, network 20.0.0.0 has been preferred through R2, because of the shorter AS-path Attribute. Change the weight parameter on R1 to prefer network through R3.

!R1

router bgp 100

neighbor 35.0.0.3 weight 1000

R1#clear ip bgp 35.0.0.3 soft in

R1#sh ip bgp

Network Next Hop Metric LocPrf Weight Path

*> 10.0.0.0 0.0.0.0 0 32768 i

* 15.0.0.0 35.0.0.3 1000 300 200 i

* 15.0.0.2 0 0 200 i

*> 0.0.0.0 0 32768 i

```
*> 20.0.0.0         35.0.0.3                 1000 300 200 i
*                   15.0.0.2                 0          0 200 i
*> 25.0.0.0         35.0.0.3                 0          1000 300 i
*                   15.0.0.2                 0          0 200 i
*> 30.0.0.0         35.0.0.3                 0          1000 300 i
*                   15.0.0.2                            0 200 300 i
*  35.0.0.0         35.0.0.3                 0          1000 300 i
*>                  0.0.0.0                  0          32768 i
R1#
```

Note: After changing the weight Parameter on R1, the router prefers the network 20.0.0.0 through R3 instead.

Ping should be working fine between PCs....

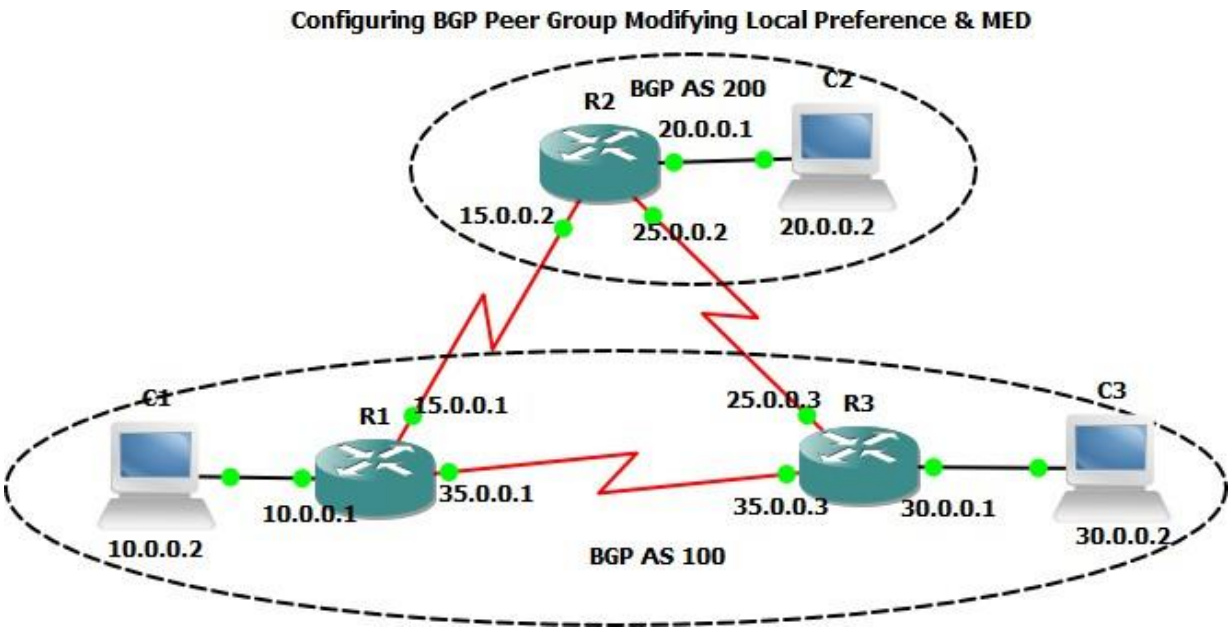
Lab 27

Configuring BGP using Peer Group, Modifying Local Preference & MED

Objective:

The main goal of this lab is configure BGP using Peer Group Feature, and to do modification on Local Preference & MED to change the route for certain networks.

Diagram:



Task 1:

Continuing on Lab 24, disable BGP configuration on all routers, then reconfigure BGP as shown in the figure. However, Use BGP peer group command when configuring R2. Then advertise all connected networks into BGP.

!R1

no router bgp 100

!R2

no router bgp 200

!R3

no router bgp 300

!R1

router bgp 100

neighbor 15.0.0.2 remote-as 200

neighbor 35.0.0.3 remote-as 100

network 10.0.0.0

network 15.0.0.0

network 35.0.0.0

!R2

router bgp 200

neighbor EBGP_Peers peer-group

neighbor EBGP_Peers remote-as 100

neighbor 15.0.0.1 peer-group EBGP_Peers

neighbor 25.0.0.3 peer-group EBGP_Peers

network 20.0.0.0

network 15.0.0.0

network 25.0.0.0

!R3

router bgp 100

neighbor 35.0.0.1 remote-as 100

neighbor 25.0.0.2 remote-as 200

network 30.0.0.0

network 25.0.0.0

network 15.0.0.0

!Verification:

R1#sh ip bgp summary

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
15.0.0.2	4	200	2	3	0	0	0	00:00:57	0
35.0.0.3	4	100	2	2	0	0	0	00:00:44	0

R1#

R1#sh ip bgp

	Network	Next Hop	Metric	LocPrf	Weight	Path
*>	10.0.0.0	0.0.0.0	0		32768	i
*	15.0.0.0	15.0.0.2	0		0	200 i
*>		0.0.0.0	0		32768	i
* i	20.0.0.0	25.0.0.2	0	100	0	200 i
*>		15.0.0.2	0		0	200 i

*>i25.0.0.0 35.0.0.3 0 100 0 i

* 15.0.0.2 0 0 200 i

*>i30.0.0.0 35.0.0.3 0 100 0 i

*> 35.0.0.0 0.0.0.0 0 32768 i

R1#

Task 2:

Modify BGP configuration using local preference attribute in AS 100, so network 20.0.0.0 is to be preferred through R3 for all customers in AS 100.

!R3

access-list 1 permit 20.0.0.0 0.255.255.255

!

route-map local permit 10

match ip address 1

set local-preference 200

route-map local permit 100

!

router bgp 100

neighbor 25.0.0.2 route-map local in

!Verification:

R3#clear ip bgp 25.0.0.2 soft in

R3#sh ip bgp

```
   Network          Next Hop            Metric LocPrf Weight Path
*>i10.0.0.0         35.0.0.1                 0    100      0 i
*>i15.0.0.0         35.0.0.1                 0    100      0 i
*                   25.0.0.2                 0             0 200 i
*> 20.0.0.0         25.0.0.2                 0    200      0 200 i
*  25.0.0.0         25.0.0.2                 0             0 200 i
*>                  0.0.0.0                  0         32768 i
*> 30.0.0.0         0.0.0.0                  0         32768 i
r>i35.0.0.0         35.0.0.1                 0    100      0 i
R3#


R1#sh ip bgp
BGP table version is 8, local router ID is 35.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.0.0.0         0.0.0.0                  0         32768 i
*  15.0.0.0         15.0.0.2                 0             0 200 i
*>                  0.0.0.0                  0         32768 i
*>i20.0.0.0         25.0.0.2                 0    200      0 200 i
```

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

```
*                15.0.0.2              0          0 200 i
*>i25.0.0.0      35.0.0.3              0    100   0 i
*                15.0.0.2              0          0 200 i
*>i30.0.0.0      35.0.0.3              0    100   0 i
*> 35.0.0.0      0.0.0.0               0        32768 i
R1#
```

Note: R1 preferred network 20.0.0.0 through R3, because its having a higher Local Preference Value.

Task 3:

Modify the BGP configuration on AS 100 so all incoming traffic from AS 200 for network 10.0.0.0 & 30.0.0.0 is to come through R1.

```
!R1
access-list 11 permit 10.0.0.0 0.255.255.255
access-list 11 permit 30.0.0.0 0.255.255.255
route-map med permit 10
match ip add 11
set metric 50
route-map med permit 100
!
router bgp 100
neighbor 15.0.0.2 route-map med out
```

!R3

access-list 33 permit 10.0.0.0 0.255.255.255

access-list 33 permit 30.0.0.0 0.255.255.255

route-map med permit 10

match ip address 33

set metric 100

route-map med permit 100

!

router bgp 100

neighbor 25.0.0.2 route-map med out

!Verification:

R1#clear ip bgp 15.0.0.2 soft out

R3#clear ip bgp 25.0.0.2 soft out

R2#sh ip bgp

Network	Next Hop	Metric	LocPrf	Weight	Path
* 10.0.0.0	25.0.0.3	100		0	100 i
*>	15.0.0.1	50		0	100 i
* 15.0.0.0	25.0.0.3			0	100 i
*	15.0.0.1	0		0	100 i
*>	0.0.0.0	0		32768	i
*> 20.0.0.0	0.0.0.0	0		32768	i

```
*  25.0.0.0        15.0.0.1                    0 100 i
*                25.0.0.3              0          0 100 i
*>               0.0.0.0               0       32768 i
*> 30.0.0.0       15.0.0.1              50         0 100 i
*                25.0.0.3              100        0 100 i
*> 35.0.0.0       25.0.0.3                    0 100 i
*                15.0.0.1              0          0 100 i
R2#
```

Note: All the networks o R2 as shown, has been preferred to go through R1, after we changed the MED attribute (Lowest MED is preferred).

Ping between all devices should work fine.....

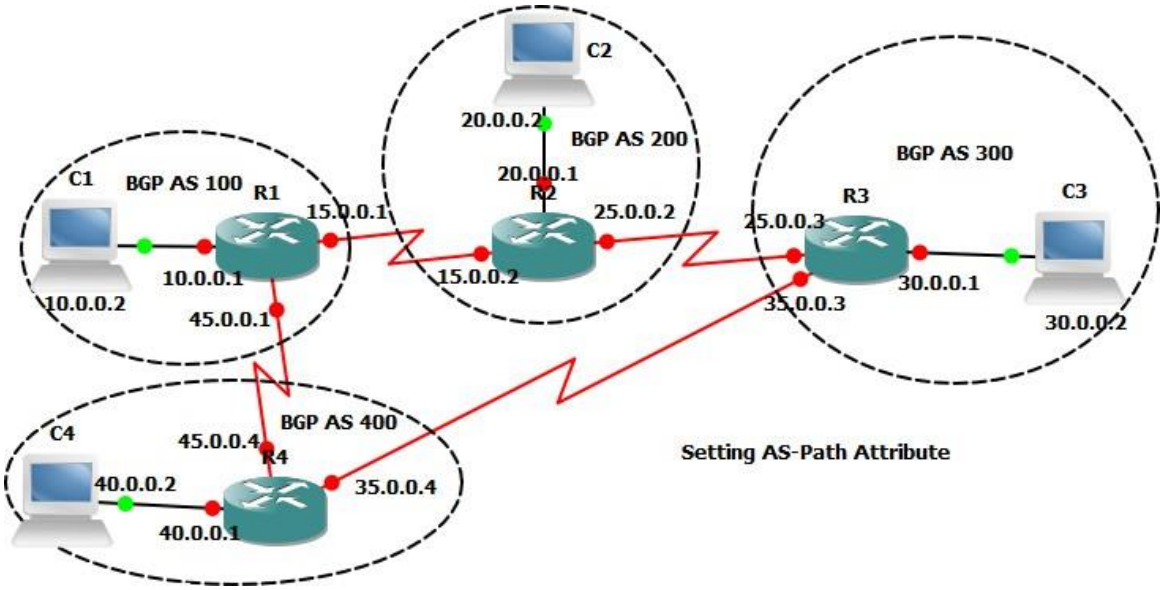
Lab 28

AS Path Attribute

Objective:

The main goal of this lab is to modify the AS path Attribute to Influence the outbound traffic for a certain BGP AS.

Diagram:



Preliminary Task:

Connect the network as shown in the diagram, and assign IP addresses ad described in the above figure.

Task 1:

Configure BGP on all routers as explained in the diagram, and advertise all the connected network into BGP.

!R1

router bgp 100

neighbor 15.0.0.2 remote-as 200

neighbor 45.0.0.4 remote-as 400

network 10.0.0.0

network 15.0.0.0

network 45.0.0.0

!R2

router bgp 200

neighbor 15.0.0.1 remote-as 100

neighbor 25.0.0.3 remote-as 300

network 20.0.0.0

network 15.0.0.0

network 25.0.0.0

!R3

router bgp 300

neighbor 25.0.0.2 remote-as 200

neighbor 35.0.0.4 remote-as 400

network 30.0.0.0

network 25.0.0.0

network 35.0.0.0

!R4

router bgp 400

neighbor 45.0.0.1 remote-as 100

neighbor 35.0.0.3 remote-as 300

network 40.0.0.0

network 35.0.0.0

network 45.0.0.0

!Verification:

R4#sh ip bgp summary

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
35.0.0.3	4	300	2	2	0	0	0	00:00:21	0
45.0.0.1	4	100	5	2	0	0	0	00:00:21	5

R4#sh ip bgp

	Network	Next Hop	Metric	LocPrf	Weight	Path
*	10.0.0.0	35.0.0.3			0	300 200 100 i
*>		45.0.0.1	0		0	100 i
*	15.0.0.0	35.0.0.3			0	300 200 i
*>		45.0.0.1	0		0	100 i
*>	20.0.0.0	35.0.0.3			0	300 200 i
*		45.0.0.1			0	100 200 i

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

*> 25.0.0.0 35.0.0.3 0 0 300 i

* 45.0.0.1 0 100 200 i

* 30.0.0.0 45.0.0.1 0 100 200 300 i

*> 35.0.0.3 0 0 300 i

* 35.0.0.0 35.0.0.3 0 0 300 i

*> 0.0.0.0 0 32768 i

*> 40.0.0.0 0.0.0.0 0 32768 i

* 45.0.0.0 45.0.0.1 0 0 100 i

*> 0.0.0.0 0 32768 i

R4#

Note: We can see that most of EBGP routes have been selected based on the shorter AS-Path.

Task 2:

Configure R4 to select all EBGP routes through R1 based on the AS-Path Attribute.

!R4

route-map aspath permit 10

set as-path-prepend 400 400 400

router bgp 400

neighbor 35.0.0.3 route-map aspath in

!

!Verification:

```
 R4#clear ip bgp 35.0.0.3 soft in
R4#sh ip bgp
BGP table version is 12, local router ID is 45.0.0.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
* 10.0.0.0         35.0.0.3                               0 400 400 400 300 200 100 i
*>                 45.0.0.1                 0             0 100 i
* 15.0.0.0         35.0.0.3                               0 400 400 400 300 200 i
*>                 45.0.0.1                 0             0 100 i
* 20.0.0.0         35.0.0.3                               0 400 400 400 300 200 i
*>                 45.0.0.1                               0 100 200 i
* 25.0.0.0         35.0.0.3                 0             0 400 400 400 300 i
*>                 45.0.0.1                               0 100 200 i
*> 30.0.0.0        45.0.0.1                               0 100 200 300 i
*                  35.0.0.3                 0             0 400 400 400 300 i
* 35.0.0.0         35.0.0.3                 0             0 400 400 400 300 i
*>                 0.0.0.0                  0         32768 i
*> 40.0.0.0        0.0.0.0                  0         32768 i
```

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

```
*  45.0.0.0        45.0.0.1               0           0 100 i
   Network          Next Hop            Metric LocPrf Weight Path
*>                  0.0.0.0                  0         32768 i
```

```
R4#sh ip route
C    35.0.0.0/8 is directly connected, Serial1/0
B    20.0.0.0/8 [20/0] via 45.0.0.1, 00:03:11
B    25.0.0.0/8 [20/0] via 45.0.0.1, 00:03:11
C    40.0.0.0/8 is directly connected, FastEthernet0/0
B    10.0.0.0/8 [20/0] via 45.0.0.1, 00:18:17
C    45.0.0.0/8 is directly connected, Serial1/1
B   30.0.0.0/8 [20/0] via 45.0.0.1, 00:03:11
B   15.0.0.0/8 [20/0] via 45.0.0.1, 00:18:17
R4#
```

Ping between all device should be working.....

Lab29

BGP Route Reflector

Topology:

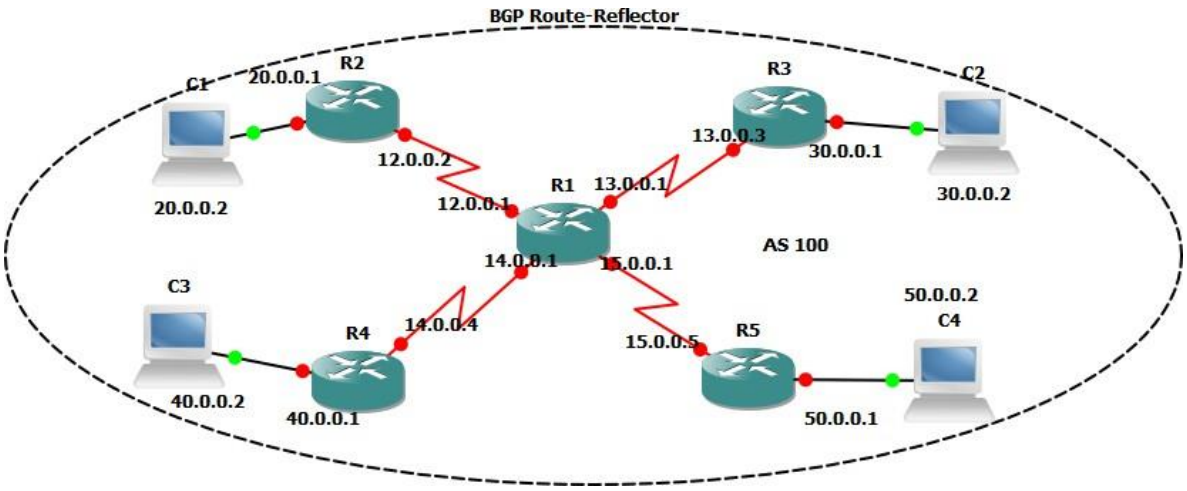


Figure 1.1

Task 1: Preliminary Configuration

- Connect the topology as shown in the figure
- Configure the IP addresses as shown in the figure

Task 2:

Configure all routers to run BGP AS 100, and to configure BGP neighbor relationship between every router and R1 (The proposed Route Reflector)

!R2

router bgp 100

no synchronization

bgp log-neighbor-changes

```
 neighbor 12.0.0.1 remote-as 100
 no auto-summary
!R3
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 13.0.0.1 remote-as 100
 no auto-summary
!R4
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 14.0.0.1 remote-as 100
 no auto-summary
!R5
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 15.0.0.1 remote-as 100
 no auto-summary
```

!R1

```
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 12.0.0.2 remote-as 100
neighbor 13.0.0.3 remote-as 100
neighbor 14.0.0.4 remote-as 100
neighbor 15.0.0.5 remote-as 100
no auto-summary
```

! **verification commands**

R1#show ip bgp summary

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
12.0.0.2	4	100	3	2	0	0	0	00:00:14	0
13.0.0.3	4	100	2	2	0	0	0	00:00:12	0
14.0.0.4	4	100	2	2	0	0	0	00:00:14	0
15.0.0.5	4	100	2	2	0	0	0	00:00:12	0

Task 3:

Configure R1 as a Route Reflector and advertise the LAN network in BGP for Routers

R2/R3/R4/R5

!R1

router bgp 100

neighbor 12.0.0.2 route-reflector-client

neighbor 13.0.0.3 route-reflector-client

neighbor 14.0.0.4 route-reflector-client

neighbor 15.0.0.5 route-reflector-client

!R2

router bgp 100

network 20.0.0.0

!R3

router bgp 100

network 30.0.0.0

!R4

router bgp 100

network 40.0.0.0

!R5

router bgp 100

network 50.0.0.0

!Verification:

R1#show ip bgp summary

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
12.0.0.2	4	100	13	13	5	0	0	00:03:38	1
13.0.0.3	4	100	12	14	5	0	0	00:02:53	1
14.0.0.4	4	100	12	14	5	0	0	00:02:39	1
15.0.0.5	4	100	12	14	5	0	0	00:02:47	1

R1#

R3#show ip bgp

BGP table version is 2, local router ID is 30.0.0.1

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

r RIB-failure, S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
* i20.0.0.0	12.0.0.2	0	100	0	i
*> 30.0.0.0	0.0.0.0	0		32768	i
* i40.0.0.0	14.0.0.4	0	100	0	i
* i50.0.0.0	15.0.0.5	0	100	0	i

Note: We can notice the other routers LAN networks is not considered valid in the bgp table, because the next hop is not reachable.

Task 4:

Configure R1 to advertise all its connected network in BGP

!R1

router bgp 100

network 12.0.0.0

network 13.0.0.0

network 14.0.0.0

network 15.0.0.0

!Verification commands:

R3#show ip bgp

Network	Next Hop	Metric	LocPrf	Weight	Path
*>i12.0.0.0	13.0.0.1	0	100	0	i
r>i13.0.0.0	13.0.0.1	0	100	0	i
*>i14.0.0.0	13.0.0.1	0	100	0	i
*>i15.0.0.0	13.0.0.1	0	100	0	i
*>i20.0.0.0	12.0.0.2	0	100	0	i
*> 30.0.0.0	0.0.0.0	0		32768	i
*>i40.0.0.0	14.0.0.4	0	100	0	i
*>i50.0.0.0	15.0.0.5	0	100	0	i

R3#show ip route

B 50.0.0.0/8 [200/0] via 15.0.0.5, 00:01:31

B 20.0.0.0/8 [200/0] via 12.0.0.2, 00:01:31

B 40.0.0.0/8 [200/0] via 14.0.0.4, 00:01:31

B 12.0.0.0/8 [200/0] via 13.0.0.1, 00:01:36

C 13.0.0.0/8 is directly connected, Serial1/0

B 14.0.0.0/8 [200/0] via 13.0.0.1, 00:01:35

C 30.0.0.0/8 is directly connected, FastEthernet0/0

B 15.0.0.0/8 [200/0] via 13.0.0.1, 00:01:35

R3#

Now the ping between the devices should be working, after the bgp next hop behavior has been resolved.

IPv6 Module

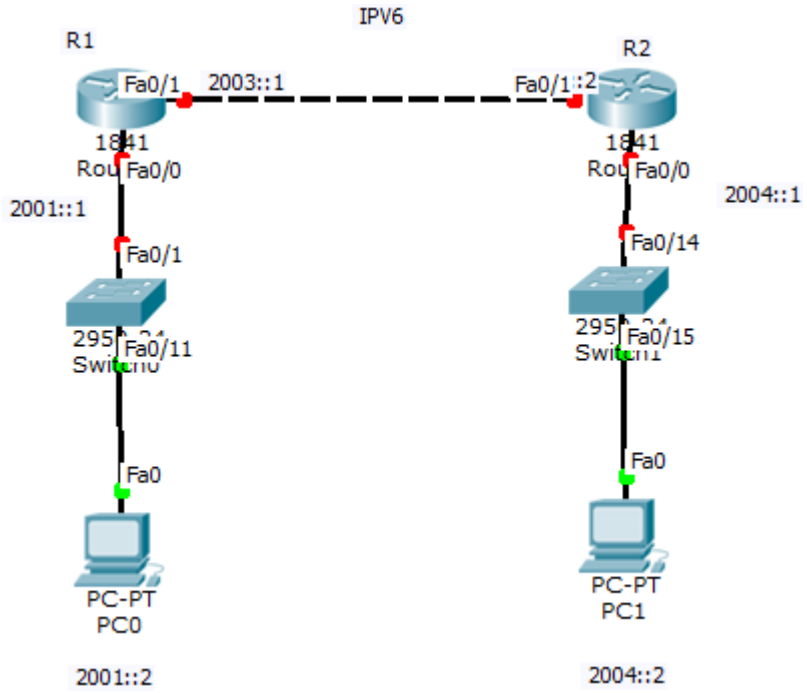
Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

Lab 30
Configuring RIPng for IPV6

Objective:

The main goal of this lab is to configure the basic ipv6 addresses, and to apply RIPng as a routing protocol.

Diagram:



Preliminary Task:

Connect the network as shown in the diagram above.

Task 1:

Configure IPV6 addresses for all physical interfaces, and configure all interfaces to be participating in RIPng.

!R1

ipv6 unicast-routing

```
!
interface fa0/0
no shutdown
ipv6 address 2001::1/64
ipv6 rip 1 enable
!
interface fa0/1
no shutdown
ipv6 address 2003::1/64
ipv6 rip 1 enable
!

!R2
ipv6 unicast-routing
!
interface fa0/0
no shutdown
ipv6 address 2004::1/64
ipv6 rip 1 enable
!
interface fa0/1
no shutdown
ipv6 address 2003::2/64
```

ipv6 rip 1 enable

!Verification

```
R2#show ipv6 route
R 2001::/64 [120/2]
via FE80::200:CFF:FE03:E102, FastEthernet0/1
C 2003::/64 [0/0]
via ::, FastEthernet0/1
L 2003::2/128 [0/0]
via ::, FastEthernet0/1
C 2004::/64 [0/0]
via ::, FastEthernet0/0
L 2004::1/128 [0/0]
via ::, FastEthernet0/0
L FF00::/8 [0/0]
via ::, Null0

R2#
```

Ping between PCs should be working fine.....

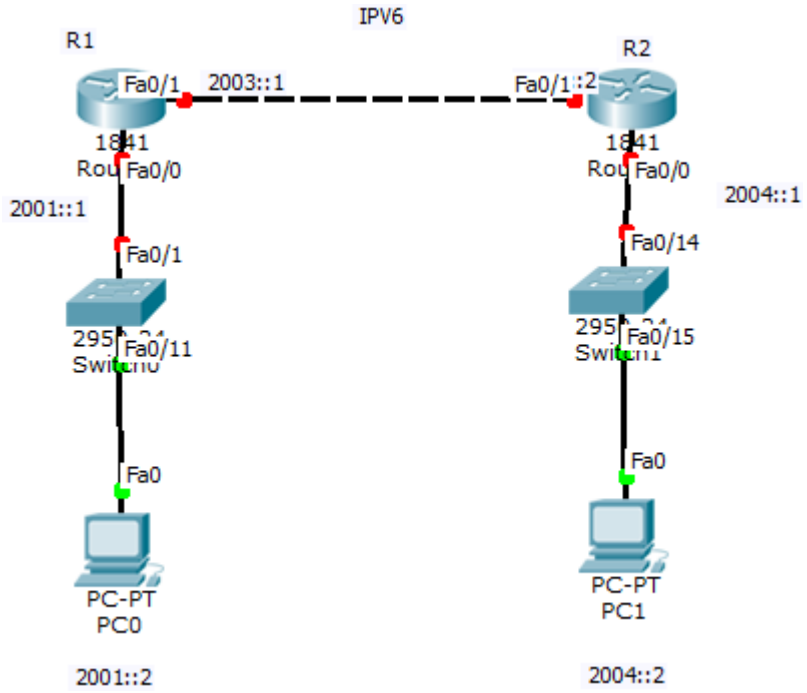
Lab 31

Configuring EIGRP for IPV6

Objective:

The main goal of this lab is to configure the basic ipv6 addresses, and to apply EIGRPv6 as a routing protocol.

Diagram:



Preliminary Task:

Connect the network as shown in the diagram above.

Task 1:

Configure IPV6 addresses for all physical interfaces, and configure all interfaces to be participating in EIGRPv6.

!R1

ipv6 unicast-routing

```
!
interface fa0/0
no shutdown
ipv6 address 2001::1/64
ipv6 eigrp 1
!
interface fa0/1
no shutdown
ipv6 address 2003::1/64
ipv6 eigrp 1
!
Ipv6 router eigrp 1
Eigrp router-id 1.1.1.1
No shutdown
!


!R2
ipv6 unicast-routing
!
interface fa0/0
no shutdown
ipv6 address 2004::1/64
ipv6 eigrp 1
!
interface fa0/1
```

no shutdown

ipv6 address 2003::2/64

ipv6 eigrp 1

!
Ipv6 router eigrp 1
Eigrp router-id 2.2.2.2
No shutdown
!

!Verification

R2#show ipv6 route
D 2001::/64 [90/30720]
via FE80::200:CFF:FE03:E102, FastEthernet0/1
C 2003::/64 [0/0]
via ::, FastEthernet0/1
L 2003::2/128 [0/0]
via ::, FastEthernet0/1
C 2004::/64 [0/0]
via ::, FastEthernet0/0
L 2004::1/128 [0/0]
via ::, FastEthernet0/0
L FF00::/8 [0/0]
via ::, Null0

R2#
Ping between PCs should be working fine.....

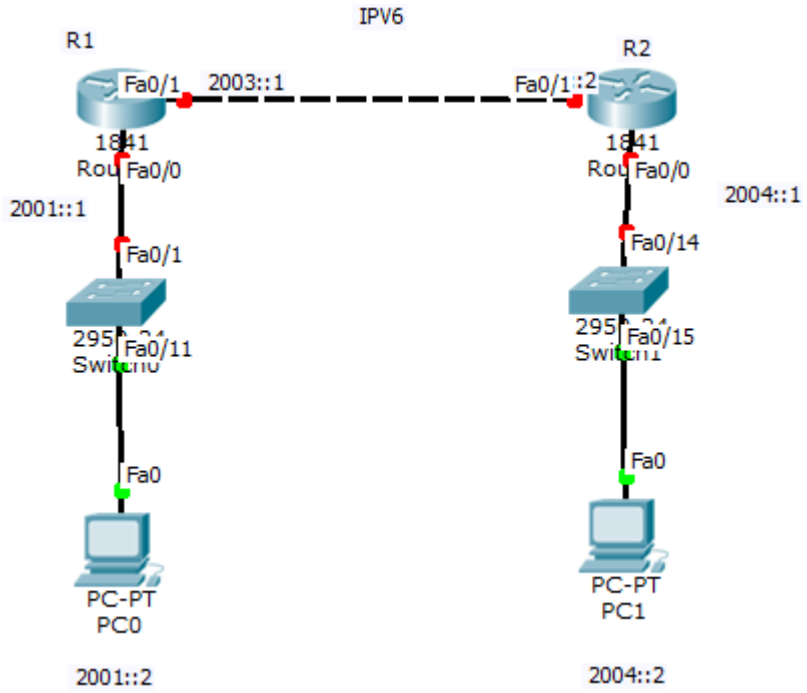
Lab 32

Configuring OSPF for IPV6

Objective:

The main goal of this lab is to configure the basic ipv6 addresses, and to apply OSPFv3 as a routing protocol.

Diagram:



Preliminary Task:

Connect the network as shown in the diagram above.

Task 1:

Configure IPV6 addresses for all physical interfaces, and configure all interfaces to be participating in OSPFv3.

!R1

ipv6 unicast-routing

```
!
interface fa0/0
no shutdown
ipv6 address 2001::1/64
ipv6 ospf 1 area 0
!
interface fa0/1
no shutdown
ipv6 address 2003::1/64
ipv6 ospf 1 area 0
!
Ipv6 router ospf 1
router-id 1.1.1.1
!


!R2
ipv6 unicast-routing
!
interface fa0/0
no shutdown
ipv6 address 2004::1/64
ipv6 ospf 1 area 0
!
interface fa0/1
```

no shutdown

ipv6 address 2003::2/64

ipv6 ospf 1 area 0

!
Ipv6 router ospf 1
router-id 2.2.2.2
No shutdown
!

!Verification

```
R2#show ipv6 route
O 2001::/64 [110/2]
via FE80::200:CFF:FE03:E102, FastEthernet0/1
C 2003::/64 [0/0]
via ::, FastEthernet0/1
L 2003::2/128 [0/0]
via ::, FastEthernet0/1
C 2004::/64 [0/0]
via ::, FastEthernet0/0
L 2004::1/128 [0/0]
via ::, FastEthernet0/0
L FF00::/8 [0/0]
  via ::, Null0
R2#
```

Ping between PCs should be working fine.....

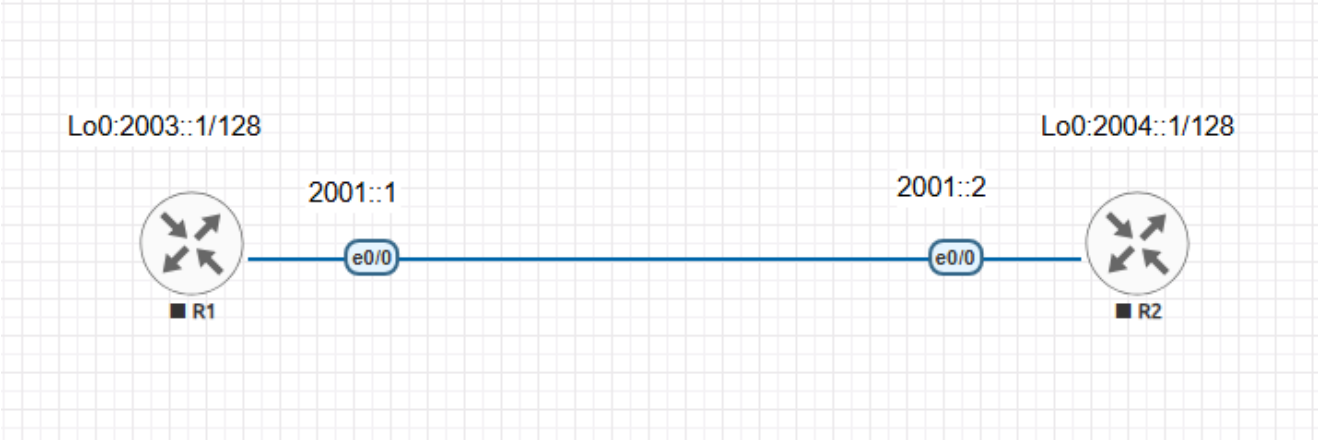
Lab 33

Configuring EIGRP Named Mode

Objective:

The main goal of this lab is to configure the basic ipv6 addresses, and to apply EIGRP Named Mode for IPv6 as a routing protocol.

Diagram:



Preliminary Task:

Connect the network as shown in the diagram above.

Task 1:

Configure IPV6 addresses for all interfaces, and configure all interfaces to be participating in EIGRP Named Mode.

!R1

ipv6 unicast-routing

!

interface fa0/0
no shutdown

ipv6 address 2001::1/64

```
!
Interface Lo0

Ipv6 address 2003::1/128

!
Router eigrp CCNP
Address-family ipv6 unicast autonomous-system 1
Eigrp router-id 1.1.1.1
!
Af-interface lo0
No shutdown
!
Af-interface e0/0
No shutdown



!R2

ipv6 unicast-routing

!

interface fa0/0
no shutdown

ipv6 address 2001::2/64

!
Interface Lo0

Ipv6 address 2004::1/128

!
Router eigrp CCNP
Address-family ipv6 unicast autonomous-system 1
Eigrp router-id 2.2.2.2
!
Af-interface lo0
No shutdown
```

!
Af-interface e0/0
No shutdown

!Verification
Ping between PCs should be working fine.....

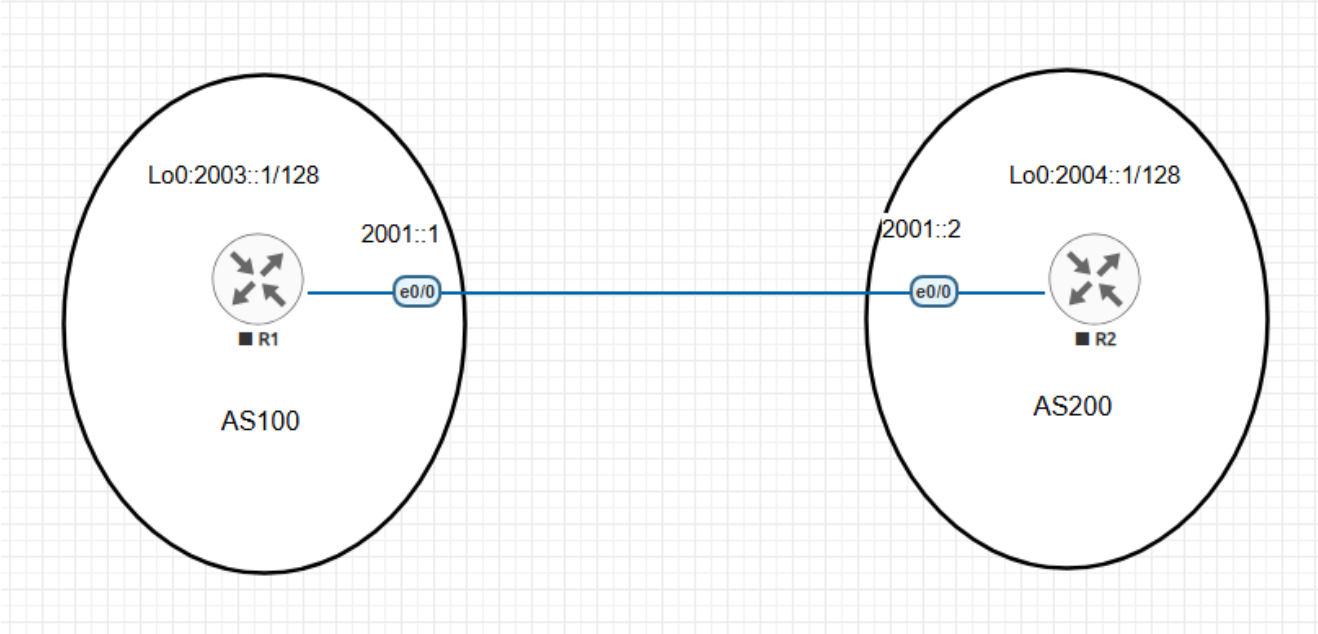
Lab 34

Configuring BGP for IPv6

Objective:

The main goal of this lab is to configure the basic ipv6 addresses, and to apply BGP for IPv6 as a routing protocol.

Diagram:



Preliminary Task:

Connect the network as shown in the diagram above.

Task 1:

Configure IPV6 addresses for all interfaces, and configure BGP as depicted in the diagram.

!R1

ipv6 unicast-routing

!

```
interface fa0/0
no shutdown

ipv6 address 2001::1/64

!
Interface Lo0

Ipv6 address 2003::1/128

!
Router bgp 100
Bgp router-id 1.1.1.1
No bgp default ipv4-unicast
Neighbor 2001::2 remote-as 200
!
Address-family ipv6
Neighbor 2001::2 activate
Network 2003::1/128
```

```
!R2

ipv6 unicast-routing

!

interface fa0/0
no shutdown

ipv6 address 2001::2/64

!
Interface Lo0

Ipv6 address 2004::1/128

!
```

```
Router bgp 200
Bgp router-id 2.2.2.2
No bgp default ipv4-unicast
Neighbor 2001::1 remote-as 100
!
Address-family ipv6
Neighbor 2001::1 activate
Network 2004::1/128
```

!Verification

```
!R2
show bgp ipv6 unicast summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State
/PfxRcd
2001::1         4          100       8       8        3    0    0 00:03:45
1

Show ipv6 route

  C   2001::/64 [0/0]
       via Ethernet0/0, directly connected
  L   2001::2/128 [0/0]
       via Ethernet0/0, receive
  B   2003::1/128 [20/0]
       via FE80::A8BB:CCFF:FE00:1000, Ethernet0/0
  LC  2004::1/128 [0/0]
       via Loopback0, receive
  L   FF00::/8 [0/0]
     via Null0, receive
```

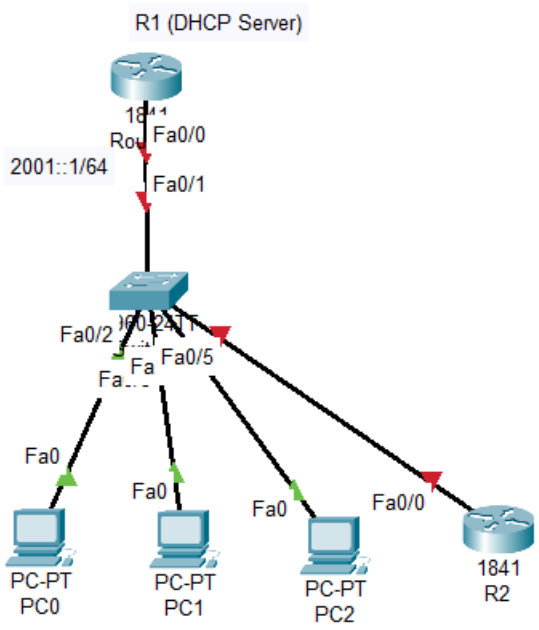
Lab 35

DHCP for IPv6

Objective:

The main goal of this lab is to configure DHCPv6 Server and Client

Diagram:



Preliminary Task:

Connect the network as shown in the diagram above.

Task 1:

Configure IPv6 address for R1, and configure it as DHCP Server, and Configure R2 as DHCP Client.

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

```
!R1
Ipv6 unicast-routing
!
Ipv6 dhcp pool cisco
Address prefix 2001::/64
Exit
!
Interface fa0/0
No shutdown
Ipv6 address 2001::1/64
Ipv6 dhcp server cisco
!


!R2
Interface fa0/0
No shutdown
Ipv6 enable
Ipv6 address dhcp
!
```

!Verification

Make sure all PCs and R2 are getting ipv6 address from 2001::/64

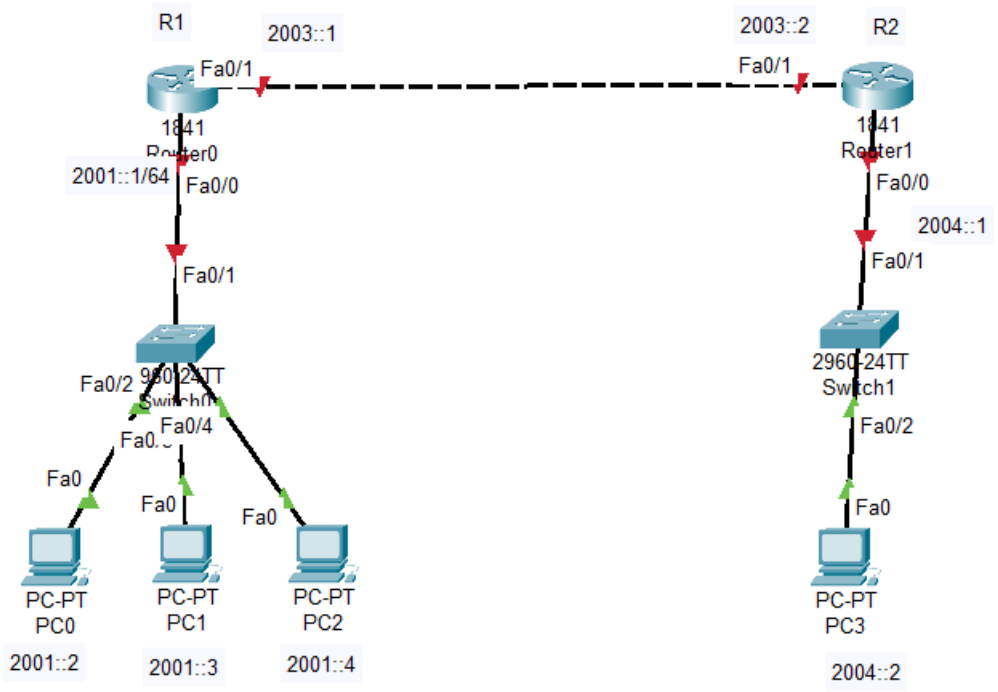
Lab 36

IPv6 Access List

Objective:

The main goal of this lab is to configure IPv6 access-list

Diagram:



Preliminary Task:

Connect the network as shown in the diagram above.

Task 1:

Configure IPv6 address as depicted in the figure and enable ripng as routing protocol, and make sure PCs can ping each other.

!R1

Ipv6 unicast-routing

!

```
Interface fa0/0
No shutdown
Ipv6 address 2001::1/64
Ipv6 rip 1 enable
!
Interface fa0/1
No shutdown
Ipv6 address 2003::1/64
Ipv6 rip 1 enable
!

!R2
Ipv6 unicast-routing
!
Interface fa0/0
No shutdown
Ipv6 address 2004::1/64
Ipv6 rip 1 enable
!
Interface fa0/1
No shutdown
Ipv6 address 2003::2/64
Ipv6 rip 1 enable
!
```

Task 2:

Configure access list on R1 so that the ping from 2001::2 to 2004::2 is denied while all other traffic is permitted to the rest of the network

!R1

Ipv6 access-list list1

Deny ipv6 host 2001::2 host 2004::2

Permit ipv6 any any

!

Interface fa0/0

Ipv6 traffic-filter list1 in

!Verification

Verify that the ping is behaving as requested in the task

VPN and VRF Lite Module

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

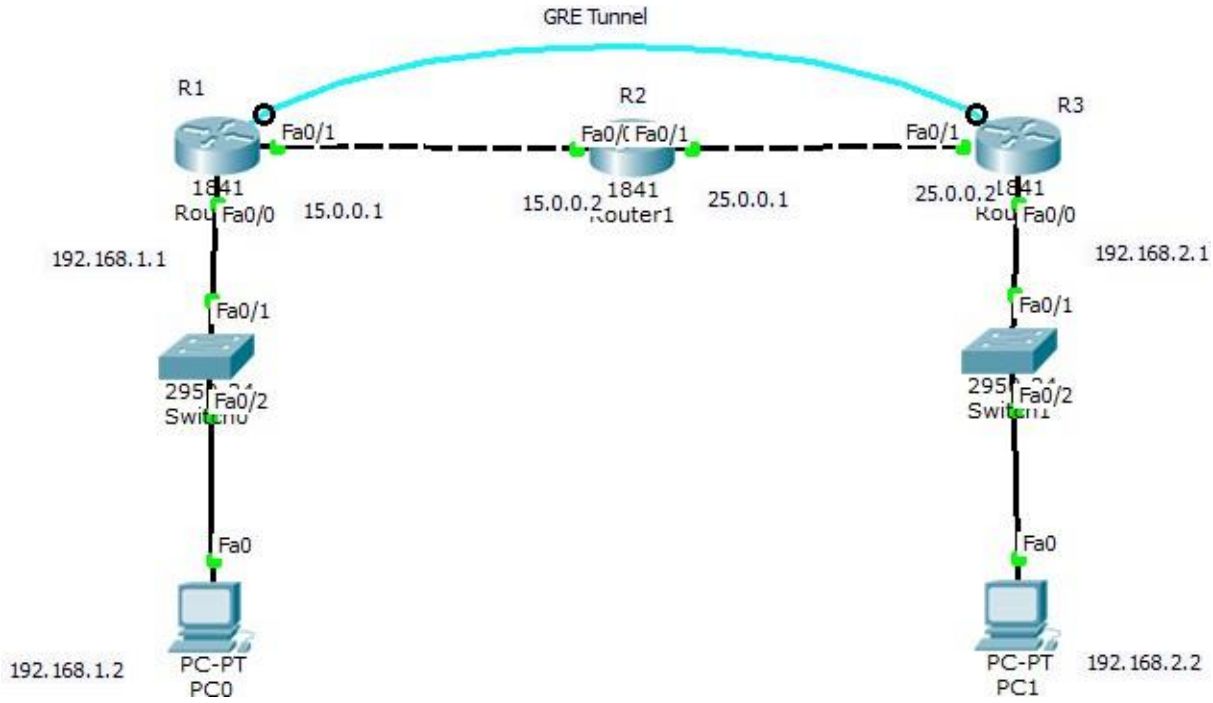
Lab 37

Point-to-Point GRE Tunnels Configuration

Objective:

The main goal of this lab is to configure GRE tunnel between two distant sites, and to allow traffic to pass over it normally

Diagram:



Task 1:

Connect the above diagram, and configure the IP addresses as explained in the figure, and configure a default route on R1 pointed to R2, and in R3 pointed to R2.

!R1

ip route 0.0.0.0 0.0.0.0 fa0/1
!R3

ip route 0.0.0.0 0.0.0.0 fa0/1

Veritifcation:

!R1

show ip route

C 15.0.0.0/8 is directly connected, FastEthernet0/1

C 192.168.1.0/24 is directly connected, FastEthernet0/0

S* 0.0.0.0/0 is directly connected, FastEthernet0/1

Task 2:

Configure R1 & R3 with GRE Tunnel having Interface IP address of 30.0.0.1 and 30.0.0.2.

!R1

interface Tunnel0
ip address 30.0.0.1 255.0.0.0
tunnel source FastEthernet0/1
tunnel destination 25.0.0.2
tunnel mode gre ip
!

!R3

interface Tunnel0
ip address 30.0.0.2 255.0.0.0
tunnel source FastEthernet0/1
tunnel destination 15.0.0.1
tunnel mode gre ip

Verification:

!R1

show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.1.1	YES	manual	up	up
FastEthernet0/1	15.0.0.1	YES	manual	up	up
Tunnel0	30.0.0.1	YES	manual	up	up

Task 3:
enable RIP on R1 & R3, and advertise only the LAN networks for every router, and the GRE tunnel network, and ensure the PCs can ping each other normally.
!R1
router rip
version 2
network 192.168.1.0
network 30.0.0.0

!R3
router rip
version 2
network 192.168.2.0
network 30.0.0.0

Verification:
!R1
show ip route
C 15.0.0.0/8 is directly connected, FastEthernet0/1
C 30.0.0.0/8 is directly connected, Tunnel0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
R 192.168.2.0/24 [120/1] via 30.0.0.2, 00:00:03, Tunnel0
S* 0.0.0.0/0 is directly connected, FastEthernet0/1

Ping Between the PCs should be working normally....

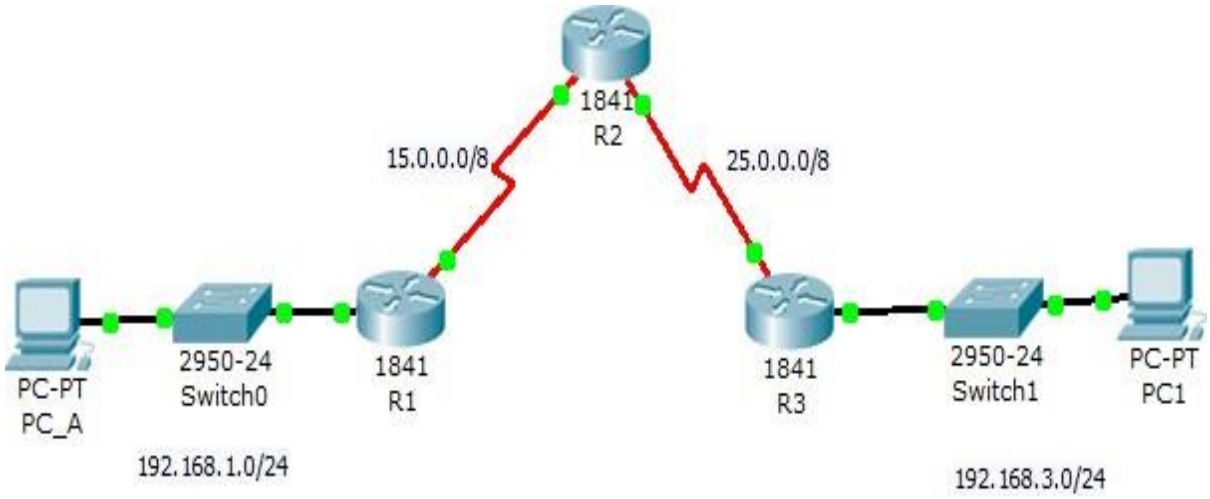
Lab 38

IPSEC SITE-to-SITE VPN Configuration

Objective:

The main goal of this lab is to configure IPSEC tunnel between two distant sites, and to allow traffic to pass over it normally

Diagram:



Task 1:

Connect the network as shown in the above diagram, configure the IP addresses for all routers, and configure a default route on R1 pointed to R2, and in R3 pointed to R2.

!R1

ip route 0.0.0.0 0.0.0.0 S0/1/0

!R3

ip route 0.0.0.0 0.0.0.0 s0/1/0

Task 2

Configure Interesting VPN traffic on R1 & R3, and Then Configure the ISAKMP Parameters and IPSEC Tunnels

!R1

access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

crypto isakmp policy 2

hash md5

authentication pre-share

group 2

life 600

encryption aes 128

exit

crypto isakmp key cisco123 address 25.0.0.3

crypto ipsec transform-set MY-SET esp-aes 256 esp-sha-hmac

crypto map MY-MAP 1 ipsec-isakmp

match address 100

set transform-set MY-SET

set peer 25.0.0.3

int s0/1/0

crypto map MY-MAP

!R3

access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

crypto isakmp policy 2

hash md5

authentication pre-share

group 2

life 600

encryption aes 128

exit

crypto isakmp key cisco123 address 15.0.0.1

crypto ipsec transform-set MY-SET esp-aes 256 esp-sha-hmac

crypto map MY-MAP 1 ipsec-isakmp

match address 100

set transform-set MY-SET

set peer 15.0.0.1

int s0/1/0

crypto map MY-MAP

Verification:

sh crypto ipsec sa

interface: Serial0/1/0

Crypto map tag: MY-MAP, local addr 15.0.0.1

protected vrf: (none)

local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)

current_peer 25.0.0.3 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.: 15.0.0.1, remote crypto endpt.:25.0.0.3

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0

current outbound spi: 0x0(0)

inbound esp sas:

--More—

Ping between PCs should be working normally.....

Verify the IPSEC tunnel

R1#sh crypto ipsec sa

interface: Serial0/1/0

Crypto map tag: MY-MAP, local addr 15.0.0.1

protected vrf: (none)

local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)

current_peer 25.0.0.3 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0

#pkts decaps: 6, #pkts decrypt: 6, #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 1, #recv errors 0

local crypto endpt.: 15.0.0.1, remote crypto endpt.:25.0.0.3

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0

current outbound spi: 0x14E32B46(350432070)

inbound esp sas:

spi: 0x5FED374C(1609381708)

--More—

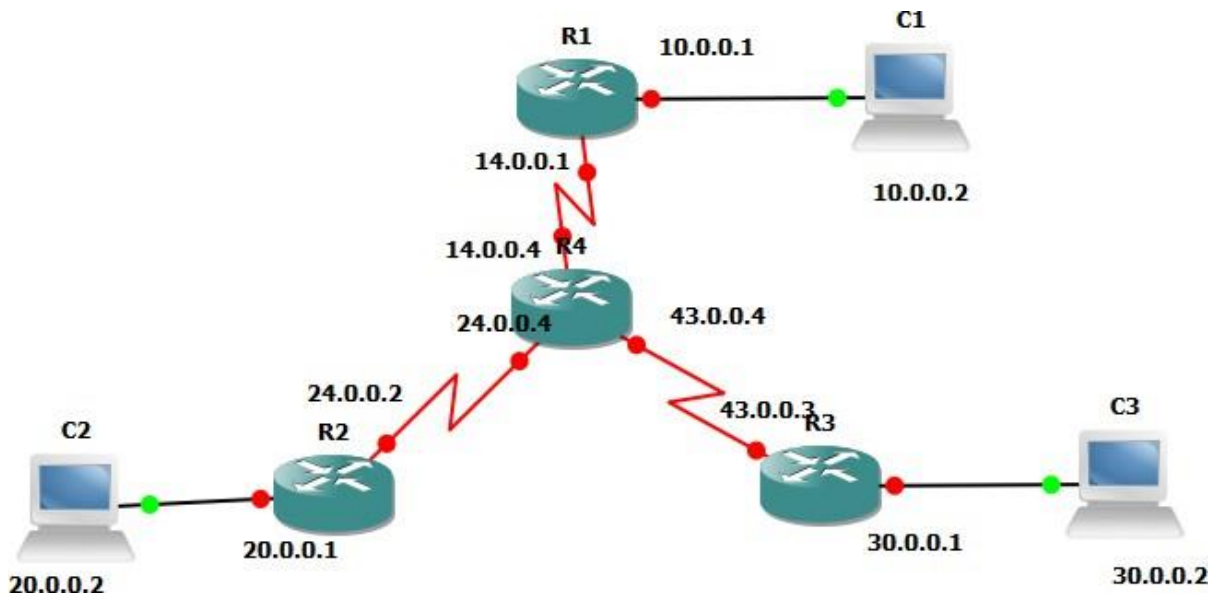
Lab 39

Dynamic Multipoint VPN Configuration

Objective:

The main goal of this lab is to configure DMVPN tunnel between Three distant sites in a HUB and SPOKE topology, and to allow traffic to pass over it normally

Diagram:



Task 1:

Connect the network as shown in the diagram, assign IP addresses as depicted in the figure and configure a default route on R1 (HUB), R2 & R3 (Spokes) pointed to R4 (DMVPN Cloud).

Verification:

Ensure the ping is working normally between the routers....

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

Task 2

Configure an MGRE Tunnel on every router, setting up R1 as the HUB of the MGRE Tunnel, and NHRP Server (NHS) for the Spokes. Configure the NHRP network id to be 99,NHRP authentication key should be cisco123 and the GRE tunnel key to be 123. Don't Forget to allow multicast traffic to be passed throughout the GRE Tunnel. Tunnel interface IP addresses for R1, R2 & R3 should 123.0.0.1, 123.0.0.2 & 123.0.0.3 respectively.

```
!R1 (HUB)
interface Tunnel0
 ip address 123.0.0.1 255.0.0.0
ip mtu 1412
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 99
 tunnel source Serial1/0
 tunnel mode gre multipoint
 tunnel key 123
!


!R2 (SPOKE)
interface Tunnel0
 ip address 123.0.0.2 255.0.0.0
ip mtu 1412
```

```
 ip nhrp authentication cisco123
ip nhrp map 123.0.0.1 14.0.0.1
ip nhrp map multicast 14.0.0.1
ip nhrp network-id 99
ip nhrp nhs 123.0.0.1
 tunnel source Serial1/0
 tunnel mode gre multipoint
 tunnel key 123
!


!R3 (SPOKE)
interface Tunnel0
 ip address 123.0.0.3 255.0.0.0
ip mtu 1412
 ip nhrp authentication cisco123
ip nhrp map 123.0.0.1 14.0.0.1
ip nhrp map multicast 14.0.0.1
ip nhrp network-id 99
ip nhrp nhs 123.0.0.1
 tunnel source Serial1/0
 tunnel mode gre multipoint
 tunnel key 123
```

Verification:

!R1

show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	10.0.0.1	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down
Serial1/0	14.0.0.1	YES	manual	up	up
Serial1/1	unassigned	YES	unset	administratively down	down
Serial1/2	unassigned	YES	unset	administratively down	down
Serial1/3	unassigned	YES	unset	administratively down	down
SSLVPN-VIF0	unassigned	NO	unset	up	up
Tunnel0	123.0.0.1	YES	manual	up	up

Ping between the tunnel interfaces should be working normally.....

Task 3:

Enable Eigrp 100 on the three routers R1, R2 & R3 and only advertise the Tunnel network and the LAN network for every router. Don't forget to disable the split horizon on the eigrp in tunnel interface.

!R1

router eigrp 100

network 123.0.0.0

```
network 10.0.0.0
!
interface tunnel 0
no ip split-horizon eigrp 100

!R2
router eigrp 100
network 123.0.0.0
network 20.0.0.0
!
interface tunnel 0
no ip split-horizon

!R3
router eigrp 100
network 123.0.0.0
network 30.0.0.0
!
interface tunnel 0
no ip split-horizon
```

Verification:

!R1

show ip route

D 20.0.0.0/8 [90/26882560] via 123.0.0.2, 00:00:40, Tunnel0

C 10.0.0.0/8 is directly connected, FastEthernet0/0

C 123.0.0.0/8 is directly connected, Tunnel0

C 14.0.0.0/8 is directly connected, Serial1/0

D 30.0.0.0/8 [90/26882560] via 123.0.0.3, 00:00:22, Tunnel0

S* 0.0.0.0/0 is directly connected, Serial1/0

ping between the PCs should be working normally.....

Task 4:

Now It is time to protect the tunnel by applying IPSEC on it. Use the suitable hashing, encryption algorithms for both ISAKMP and IPSEC tunnels. Then apply the new profile on the tunnel interface.

!R1/R2/R3

crypto isakmp policy 20

encryption des

hash md5

authentication pre-share

group 2

exit

!

crypto isakmp key hello address 0.0.0.0 0.0.0.0

!

crypto ipsec transform-set MY-SET esp-aes 256 esp-sha-hmac

exit

!

crypto ipsec profile DMVPN

set transform-set MY-SET

!

interface tunnel 0

tunnel protection ipsec profile DMVPN

Verification:

The ping should still be working fine between the PCs.....

However, the tunnel should be protected.

!R1

R1#show crypto ipsec sa

interface: Tunnel0

Crypto map tag: Tunnel0-head-0, local addr 14.0.0.1

protected vrf: (none)

local ident (addr/mask/prot/port): (14.0.0.1/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (24.0.0.2/255.255.255.255/47/0)

current_peer 24.0.0.2 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 38, #pkts encrypt: 38, #pkts digest: 38

#pkts decaps: 38, #pkts decrypt: 38, #pkts verify: 38

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 6, #recv errors 0

local crypto endpt.: 14.0.0.1, remote crypto endpt.: 24.0.0.2

path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0

current outbound spi: 0xF7137341(4145247041)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x4971E78C(1232201612)

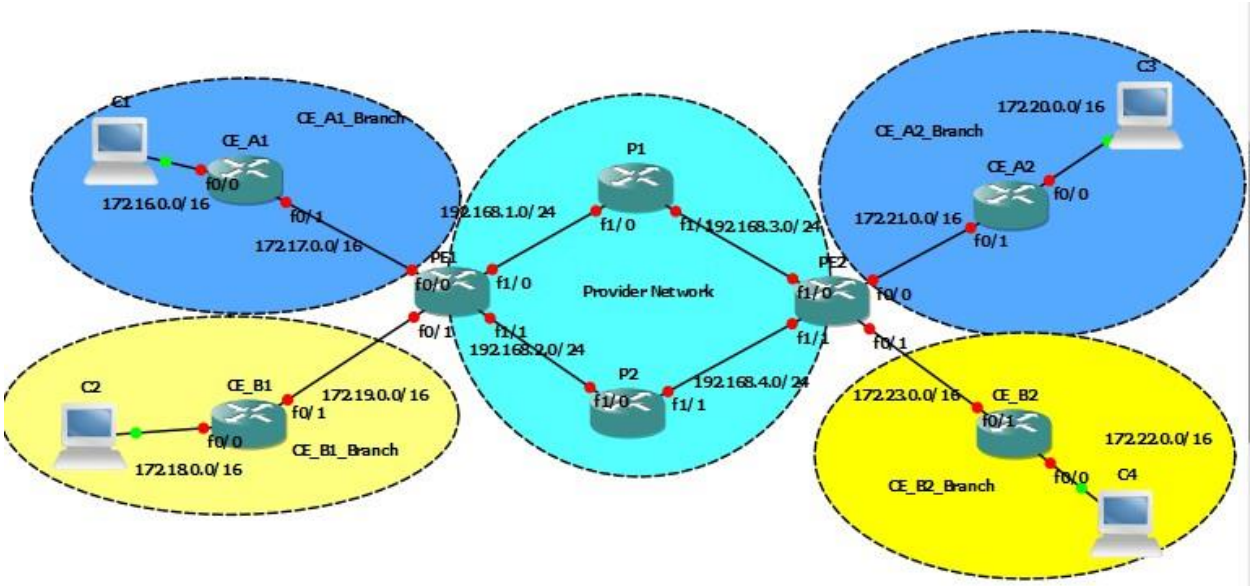
Lab 40

Layer 3 MPLS VPN

Objective:

The target of this lab is to configure MPLS VPN in service provider network, and to check the connectivity between the customer networks

Diagram:



Preliminary Task:

Connect the network as shown in the diagram, and assign the ip addresses as explained in the above figure.

Configure Loopback addresses for PE & P routers as follows:

PE1: 1.1.1.1/32, PE2: 2.2.2.2/32, P1: 3.3.3.3/32 , P2:4.4.4.4/32

Task 1:

Configure two VRFs (CE_A & CE_B) on each of the PE routers, and put the PE-CE interfaces into the equivalent interfaces:

```
!PE1
ip vrf CE_A
rd 1:1
route-target both 1:1
!
ip vrf CE_B
rd 2:2
route-target both 2:2
!
int fa0/0
ip vrf forwarding CE_A
ip address 172.17.0.1 255.255.0.0
!
int fa0/1
 ip vrf forwarding CE_B
ip address 172.19.0.1 255.255.0.0


!PE2
ip vrf CE_A
rd 1:1
route-target both 1:1
!
```

```
ip vrf CE_B
rd 2:2
route-target both 2:2
!
int fa0/0
ip vrf forwarding CE_A
ip address 172.21.0.1 255.255.0.0
!
int fa0/1
 ip vrf forwarding CE_B
ip address 172.23.0.1 255.255.0.0
```

Task 2:

Configure OSPF 10 between the PE & CE routers and ensure the OSPF adjacencies have been established.

```
!CE_A1
router ospf 10
network 172.16.0.0 0.0.255.255 area 0
network 172.17.0.0 0.0.255.255 area 0
```

```
!CE_B1
router ospf 11
network 172.18.0.0 0.0.255.255 area 0
network 172.19.0.0 0.0.255.255 area 0


!PE1
router ospf 10 vrf CE_A
 log-adjacency-changes
 network 172.17.0.0 0.0.255.255 area 0
!
router ospf 11 vrf CE_B
 log-adjacency-changes
 network 172.19.0.0 0.0.255.255 area 0

!CE_A2
router ospf 10
network 172.20.0.0 0.0.255.255 area 0
network 172.21.0.0 0.0.255.255 area 0
!CE_B2
router ospf 11
network 172.22.0.0 0.0.255.255 area 0
```

```
network 172.23.0.0 0.0.255.255 area 0



!PE2
router ospf 10 vrf CE_A
 log-adjacency-changes
 network 172.21.0.0 0.0.255.255 area 0
!
router ospf 11 vrf CE_B
 log-adjacency-changes
 network 172.23.0.0 0.0.255.255 area 0
```

Verification:

```
PE1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.19.0.2        1   FULL/BDR        00:00:34    172.19.0.2      FastEthernet0/1
172.17.0.2        1   FULL/BDR        00:00:32    172.17.0.2      FastEthernet0/0

PE2#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.23.0.2	1	FULL/DR	00:00:35	172.23.0.2	FastEthernet0/1
172.21.0.2	1	FULL/DR	00:00:34	172.21.0.2	FastEthernet0/0

Task 3:

Configure OSPF process 1 between all the routers in the provider network and don't forget to include loopback interfaces advertisement.

!PE1

router ospf 1

network 1.1.1.1 0.0.0.0 area 0

network 192.168.1.0 0.0.0.255 area 0

network 192.168.2.0 0.0.0.255 area 0

!PE2

router ospf 1

network 2.2.2.2 0.0.0.0 area 0

network 192.168.3.0 0.0.0.255 area 0

network 192.168.4.0 0.0.0.255 area 0

!P1

router ospf 1

network 3.3.3.3 0.0.0.0 area 0

network 192.168.3.0 0.0.0.255 area 0

network 192.168.1.0 0.0.0.255 area 0

!P2

router ospf 1

network 4.4.4.4 0.0.0.0 area 0

network 192.168.2.0 0.0.0.255 area 0

network 192.168.4.0 0.0.0.255 area 0

Verification:

P1#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.1.1	1	FULL/DR	00:00:34	192.168.1.2	FastEthernet1/0
2.2.2.2	1	FULL/BDR	00:00:34	192.168.3.1	FastEthernet1/1

P2#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	1	FULL/DR	00:00:31	192.168.4.1	FastEthernet1/1
1.1.1.1	1	FULL/BDR	00:00:38	192.168.2.2	FastEthernet1/0

Task 4:

Configure BGP AS 100 between the PE routers, and use loopback interface as the update source.

```
!PE1
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback0


!PE2
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback0
```

Verification:

```
PE1#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 1, main routing table version 1
```

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd

2.2.2.2 4 100 2 2 0 0 0 00:00:29 0

Task 5:

Activate MP-BGP neighborhood between the PE routers, in order to advertise the VRF customer routes later with their route distinguisher.

```
!PE1
router bgp 100
address-family vpnv4
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 send-community extended
 !
!PE2
router bgp 100
address-family vpnv4
 neighbor 1.1.1.1 activate
 neighbor 1.1.1.1 send-community extended
```

Verification:

PE1#show ip bgp vpnv4 all summary

BGP router identifier 1.1.1.1, local AS number 100

BGP table version is 1, main routing table version 1

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd

2.2.2.2 4 100 9 9 1 0 0 00:00:25 0

Task 6:

Redistribute Mutually between the OSPF and the BGP VPNv4 on PE1 & PE2:

!PE1/PE2

router bgp 100

address-family ipv4 vrf CE_A

redistribute ospf 10 vrf CE_A match internal external 1 external 2

address-family ipv4 vrf CE_B

redistribute ospf 11 vrf CE_B match internal external 1 external 2

!

router ospf 10 vrf CE_A

redistribute bgp 100 subnets

!

router ospf 11 vrf CE_B

redistribute bgp 100 subnets

Verification:

!CE_A1#show ip route

C 172.17.0.0/16 is directly connected, FastEthernet0/1

C 172.16.0.0/16 is directly connected, FastEthernet0/0

O IA 172.21.0.0/16 [110/2] via 172.17.0.1, 00:03:28, FastEthernet0/1

O IA 172.20.0.0/16 [110/3] via 172.17.0.1, 00:03:28, FastEthernet0/1

!CE_B1#show ip route

Gateway of last resort is not set

C 172.19.0.0/16 is directly connected, FastEthernet0/1

C 172.18.0.0/16 is directly connected, FastEthernet0/0

O IA 172.23.0.0/16 [110/2] via 172.19.0.1, 00:03:57, FastEthernet0/1

O IA 172.22.0.0/16 [110/3] via 172.19.0.1, 00:03:57, FastEthernet0/1

Task7:

Enable MPLS on all interfaces within the provider network

```
!PE1/PE2/P1/P2
int fa1/0
mpls ip
!
int fa1/1
mpls ip
```

Verification:

```
PE2#sh mpls ldp neighbor
   Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 2.2.2.2:0
       TCP connection: 3.3.3.3.39927 - 2.2.2.2.646
       State: Oper; Msgs sent/rcvd: 11/11; Downstream
       Up time: 00:00:45
       LDP discovery sources:
         FastEthernet1/0, Src IP addr: 192.168.3.2
       Addresses bound to peer LDP Ident:
       192.168.1.1     192.168.3.2     3.3.3.3
   Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 2.2.2.2:0
       TCP connection: 4.4.4.4.20674 - 2.2.2.2.646
       State: Oper; Msgs sent/rcvd: 11/11; Downstream
       Up time: 00:00:24
       LDP discovery sources:
```

FastEthernet1/1, Src IP addr: 192.168.4.2

Addresses bound to peer LDP Ident:

192.168.2.1 192.168.4.2 4.4.4.4

PE1#show mpls ldp neighbor

Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 1.1.1.1:0

TCP connection: 3.3.3.3.41239 - 1.1.1.1.646

State: Oper; Msgs sent/rcvd: 12/13; Downstream

Up time: 00:01:40

LDP discovery sources:

FastEthernet1/0, Src IP addr: 192.168.1.1

Addresses bound to peer LDP Ident:

192.168.1.1 192.168.3.2 3.3.3.3

Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 1.1.1.1:0

TCP connection: 4.4.4.4.60863 - 1.1.1.1.646

State: Oper; Msgs sent/rcvd: 12/12; Downstream

Up time: 00:01:14

LDP discovery sources:

FastEthernet1/1, Src IP addr: 192.168.2.1

Addresses bound to peer LDP Ident:

192.168.2.1 192.168.4.2 4.4.4.4

PE1#show mpls forwarding-table

Local Label	Outgoing Label or VC	Prefix or Tunnel Id	Bytes Label Switched	Outgoing interface	Next Hop
16	17	2.2.2.2/32	0	Fa1/0	192.168.1.1
	17	2.2.2.2/32	0	Fa1/1	192.168.2.1
17	Pop Label	3.3.3.3/32	0	Fa1/0	192.168.1.1
18	Pop Label	4.4.4.4/32	0	Fa1/1	192.168.2.1
19	Pop Label	192.168.3.0/24	0	Fa1/0	192.168.1.1
20	Pop Label	192.168.4.0/24	0	Fa1/1	192.168.2.1
21	No Label	172.16.0.0/16[V]	0	Fa0/0	172.17.0.2
22	No Label	172.17.0.0/16[V]	0	aggregate/CE_A	
23	No Label	172.18.0.0/16[V]	0	Fa0/1	172.19.0.2
24	No Label	172.19.0.0/16[V]	0	aggregate/CE_B	

Ping Between PCs on CE_A should be working & on CE_B should be working as well.

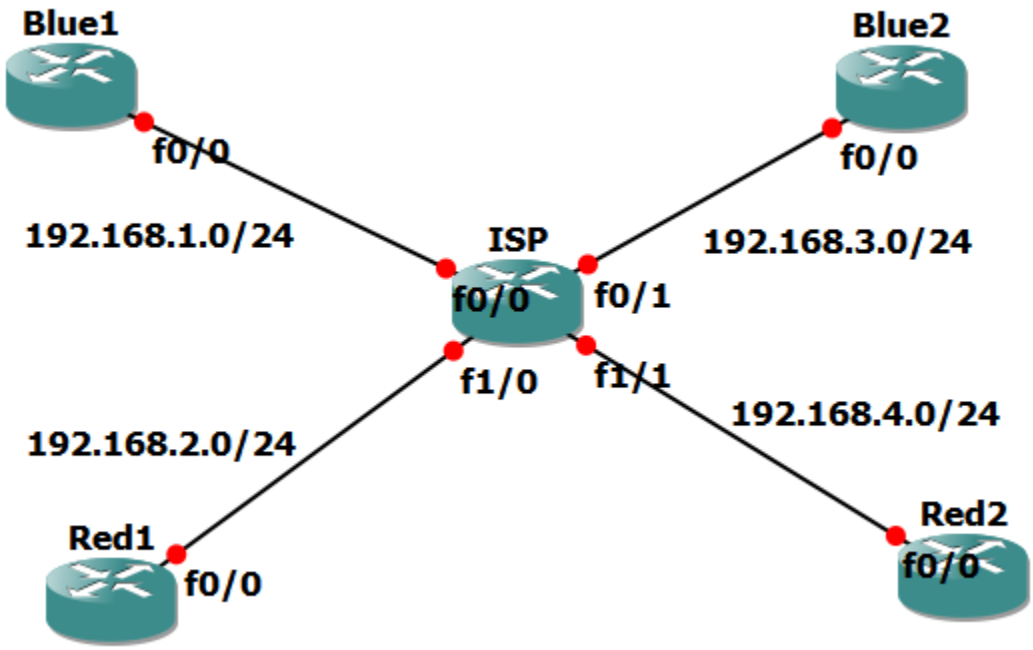
Lab 41

VRF

Objective:

The main goal of this lab is to configure and verify VRF configuration on Cisco Routers

Diagram:



Preliminary Tasks:

- Connect the network as shown in the diagram
- Assign IP addresses as depicted in the figure

- Configure Default routes in all four routers toward the ISP

Task 1:

- Configure the ISP with VRFs Red and Blue and assign ISP interfaces to the relevant VRF

```
!ISP
IP vrf Red
exit
!
IP vrf Blue
Exit
!
Interface fa0/0
Ip vrf forwarding Blue
Ip address 192.168.1.1 255.255.255.0
!
Interface fa0/1
Ip vrf forwarding Blue
Ip address 192.168.3.1 255.255.255.0
!
Interface fa1/0
```

Ip vrf forwarding Red

Ip address 192.168.2.1 255.255.255.0

!

Interface fa1/1

Ip vrf forwarding Red

Ip address 192.168.4.1 255.255.255.0

Exit

!

!Verification

!ISP

Show ip vrf

Name	Default RD	Interfaces
Blue	<not set>	Fa0/1
		Fa0/0
Red	<not set>	Fa1/0
		Fa1/1

!Ensure Ping is only working between the Routers belonging to the same VRF

Security, Services and Device Management Module

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

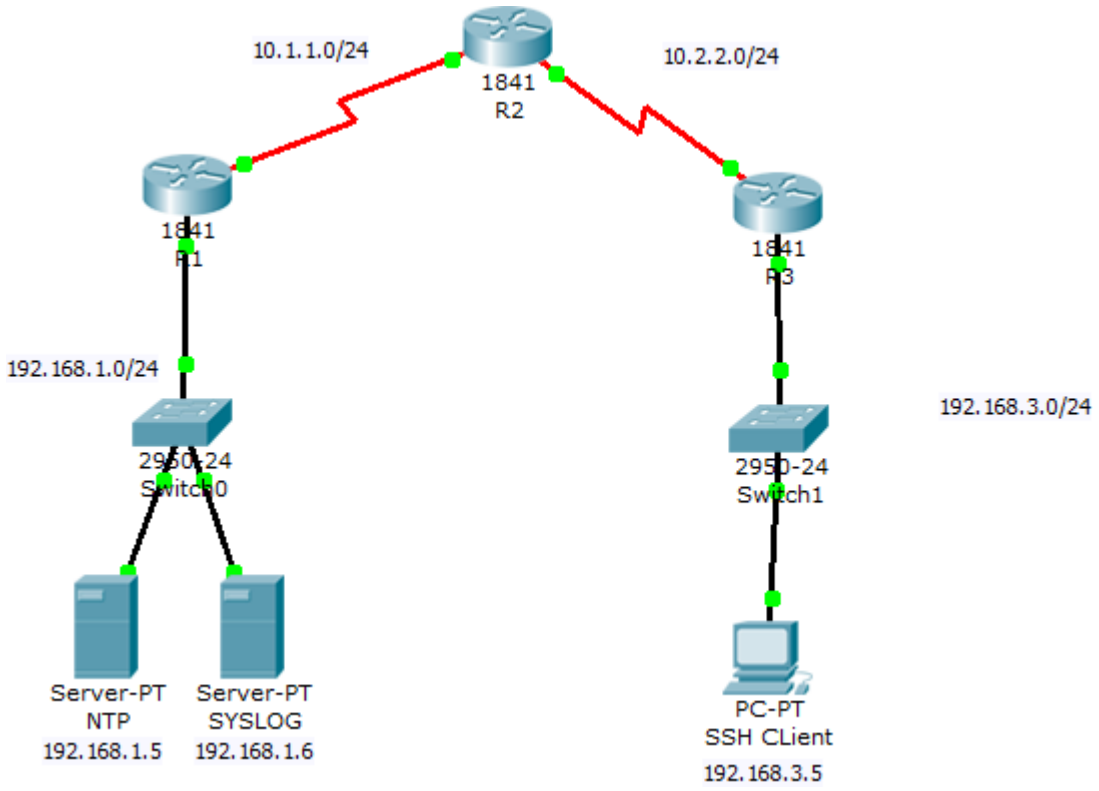
Lab42

Configure Cisco Routers for SSH, NTP and SYSLOG Operations

Objective:

The goal of this lab is to enable cisco routers to be managed by SSH, NTP and SYSLOG.

Diagram:



Task 1: Preliminary Configuration

- Connect the topology as shown in the figure
- Configure the IP addresses as shown in the figure
- Configure router rip version 2 in all routers.
- Ensure full connectivity between all hosts.

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

Task 2: Configure R1, R2, R3 as ntp authenticating clients:

!R1/R2/R3

ntp authentication-key 1 md5 cisco123

ntp authenticate

ntp trusted-key 1

ntp server 192.168.1.5 key 1

! **verification commands**

!R1

sh ntp status

Clock is synchronized, stratum 2, reference is 192.168.1.5

nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**19

reference time is D50AE633.0000001F (18:21:39.031 UTC Sat May 4 2013)

clock offset is 0.00 msec, root delay is 0.00 msec

root dispersion is 0.02 msec, peer dispersion is 0.02 msec.

R1#

Task 3: Configure routers to log messages to the Syslog Server, with time and date shown in the logged message

!R1/R2/R3

logging 192.168.1.6

service timestamps debug datetime msec

!Verification:

R1

sh logging

Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,

0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 11 messages logged, xml disabled,

filtering disabled

Monitor logging: level debugging, 0 messages logged, xml disabled,

filtering disabled

Buffer logging: disabled, xml disabled,

filtering disabled

Logging Exception size (4096 bytes)

Count and timestamp logging messages: disabled

Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped

Trap logging: level informational, 11 message lines logged

Logging to 192.168.1.6 (udp port 514, audit disabled,

authentication disabled, encryption disabled, link up),

2 message lines logged,

0 message lines rate-limited,

0 message lines dropped-by-MD,

xml disabled, sequence number disabled

filtering disabled

Note: You should also check the logging messages in the logging server.

Task 4: Enable SSH on Router2

- Configure Hostname other than the default name

  !R2

  hostname CCNP

- Configure Domain Name
  !R2
  ip domain-name cisco.com

- Generate RSA keys
  !R2
  crypto key generate rsa
  The name for the keys will be: CCNP.cisco.com
  Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

  How many bits in the modulus [512]: 1024
  % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

- Configure Username and Password on the router locally
  !R2
  username ccna privilege 15 password cisco

- Apply local authentication on the Line VTY
  !R2
  line vty 0 4
  login local

!Verification commands:

From one of the PC's try to ssh to the router using the following command

Ssh –l ccna 10.1.1.2

Password:

You can also issue show ssh to check the ssh connections

CCNP#show ssh

Connection Version Mode Encryption Hmac State Username

67	1.99	IN	aes128-cbc	hmac-sha1	Session Started	ccna
67	1.99	OUT	aes128-cbc	hmac-sha1	Session Started	ccna

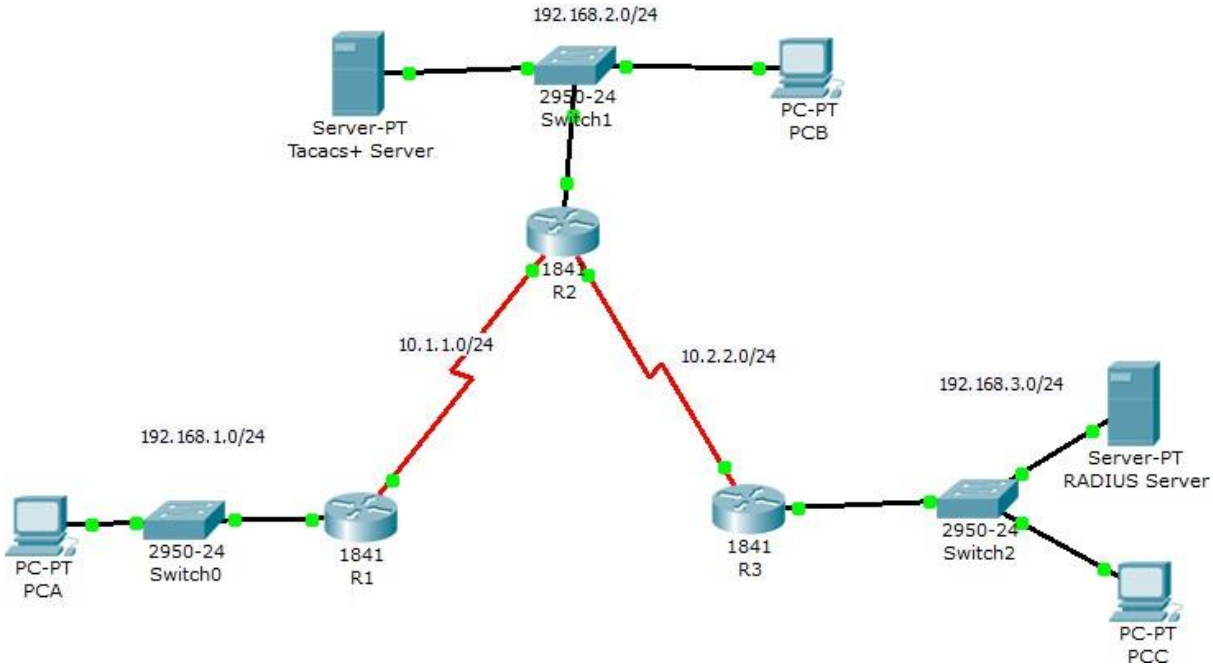
Lab43

Configure AAA authentication On Cisco Routers

Objective:

The goal of this lab is control access to cisco routers through radius Servers and Tacacs servers.

Diagram:



Task 1: Preliminary Configuration

- Connect the topology as shown in the Figure
- Do the relevant configuration to allow ping between all devices.

Task 2: Configure Local AAA authentication using named Method list for console Access on R1:

- Configure Username/Password on R1 local database
  !R1
  username CCNP password cisco
- Configure named AAA authentication method list for console access on R1
  !R1
  aaa new-model
  aaa authentication login task1 local
  line con 0
  login authentication task1

! Verification:

Do the verification for the previous task by logging out and try to relogin to the console mode.

User Access Verification

Username: CCNP

Password:

R1>

Task 3: Configure Local AAA authentication using default method list for VTY lines:

- Configure a default aaa authentication method for vty
  !R1
  aaa authentication login default local
- Enable default authentication method under line vty
  !R1
  line vty 0 15
  login authentication default

!verification:

Try to telnet to R1 from PCA to R1

PC>telnet 192.168.1.1

Trying 192.168.1.1 ...Open

User Access Verification

Username: CCNP

Password:

R1>

Task 4: Configure Server-Based AAA authentication using tacacs+ on R2:

- Configure a Backup username/password on R2's Local database
  !R2
  username admin password adminpass
- Configure the tacacs server
  The configuration depends on the tool that you use to represent a tacacs server.
- Configure the tacacs+ server specifics on R2
  !R2
  tacacs-server host 192.168.2.3 key cisco
- Configure AAA login authentication for console access on R2
  !R2
  aaa authentication login R2 group tacacs local
- Configure the line console to use the defined console authentication method
  !R2
  line con 0
  login authentication R2

!Verification:

Verify by logging out and try to access the router using the tacacs credentials

User Access Verification

Username: sudan

Password:

R2>

Task 5: Configure Server-Based AAA authentication using radius on R3:

- Configure a Backup username/password on R3's Local database
  !R3
  username admin password adminpass
- Configure the radius server
  The configuration depends on the tool that you use to represent a radius server.
- Configure the radius server specifics on R3
  !R3
  radius-server host 192.168.2.3 key cisco
- Configure AAA login authentication for console access on R3
  !R3
  aaa authentication login R3 group radius local
- Configure the line console to use the defined console authentication method
  !R3
  line con 0
  login authentication R3

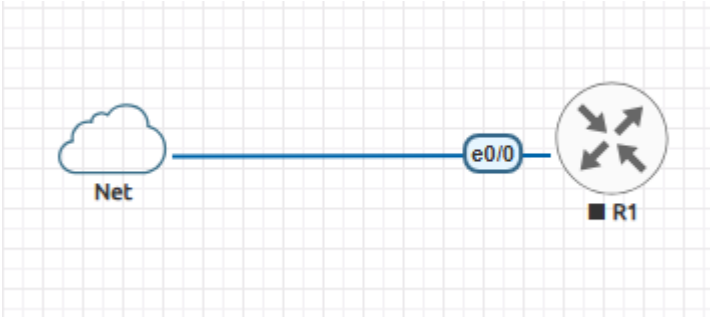
Lab44

Configure HTTP & HTTPS on Cisco Router

Objective:

The goal of this lab is HTTP management on Cisco router.

Diagram:



Task 1: Preliminary Configuration

- Connect the topology as shown in the Figure using eve-ng
- Configure e0/0 to be getting ip address through DHCP.

Task 2: Enable HTTP & HTTPS on R1, and configure local authentication

!R1

Ip http server

Ip http secure-server

Ip http authentication local

Username ccnp privilege 15 password cisco

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

! Verification:

Use the browser to check the http login to the router by doing the following:

http://router-ip-address

Username: ccnp

Password:

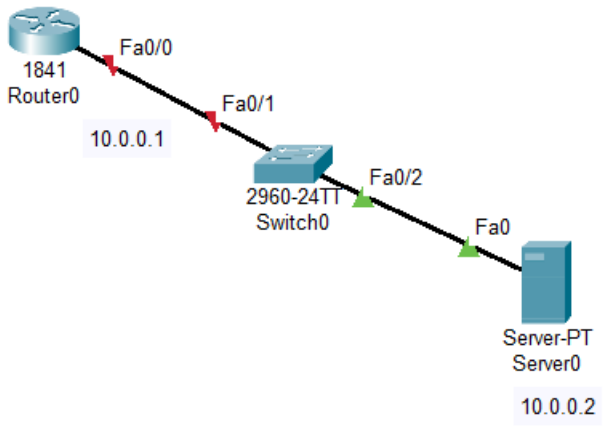
Lab 45

Configure TFTP & FTP on Cisco Router

Objective:

The goal of this lab is to configure FTP & TFTP on Cisco router.

Diagram:



Task 1: Preliminary Configuration

- Connect the topology as shown in the Figure
- Assign IP addresses as depicted in the figure.

Task 2: Enable TFTP on the router and verify by copying the ios of the router to the server

!R1

Show flash:

!Copy the name of the ios

Copy flash tftp

!Then you will be asked first for the name of the file, you can paste the name of the

!IOS

!Then you will be asked the ip address of the TFTP server, you can type 10.0.0.2

!Then you will be asked for the file name in the destination, you can press enter to !keep the same name

!Then it will start copying from the router to the TFTP server

Task 3: Enable FTP on the router and verify by copying the ios of the router to the server

!R1
Ip ftp username cisco
Ip ftp password cisco

!Setup the ftp server with the same username and password

!R1
Copy flash ftp

!Then follow the same steps that you have done for the tftp server, but the difference is that the connection is authenticated

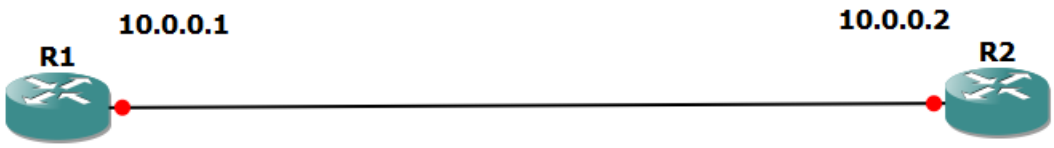
Lab 46

Configure SCP on Cisco Router

Objective:

The goal of this lab is to configure SCP on Cisco router.

Diagram:



Task 1: Preliminary Configuration

- Connect the topology as shown in the Figure
- Assign IP addresses as depicted in the figure.

Task 2: Enable SCP on R1

!R1

Hostname R1

Ip domain-name cisco.com

Crypto key generate rsa modulus 1024

Username CCNP privilege 15 password cisco

Ip scp server enable

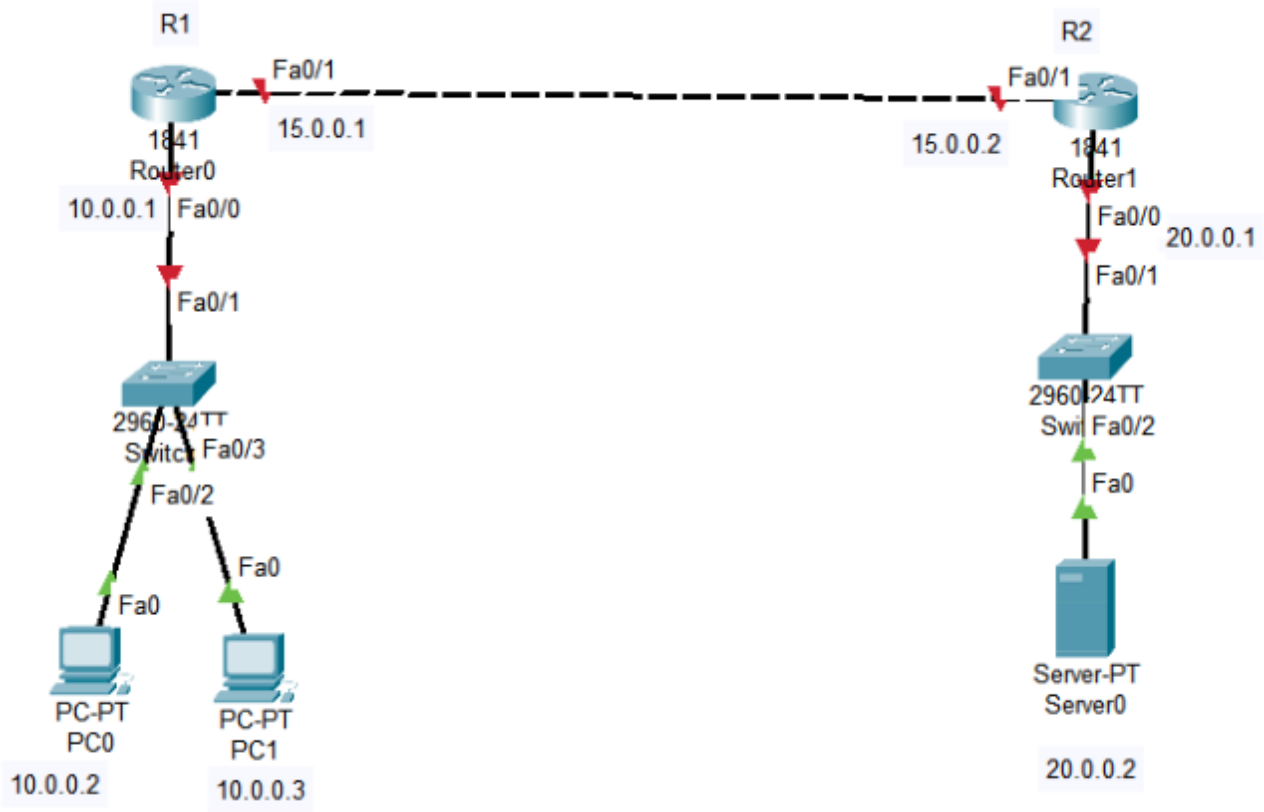
Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

Lab 47
Access List

Objective:

The goal of this lab is to configure and verify standard, extended and time-based ACL.

Diagram 1:



Preliminary Tasks:

- Connect the network as shown in the figure
- Assign IP addresses as depicted in the figure
- Configure routing protocol and verify the connectivity between the PCs

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

Task 1:

- Configure Standard ACL on R1 that blocks 10.0.0.2 and permits all other traffic
- Verify ACL functionality by trying to ping from 10.0.0.2

!R1

Access-list 1 deny 10.0.0.2 0.0.0.0

Access-list 1 permit any

Interface fa0/0

Ip access-group 1 in

Task 2:

- Remove the access list
- Configure extended access list on R1 that blocks icmp and permits http traffic from 10.0.0.0 to host 20.0.0.2

!R1

No access-list 1

!

Interface fa0/0

No ip access-group 1 in

!

Access-list 100 deny icmp 10.0.0.0 0.255.255.255 host 20.0.0.2

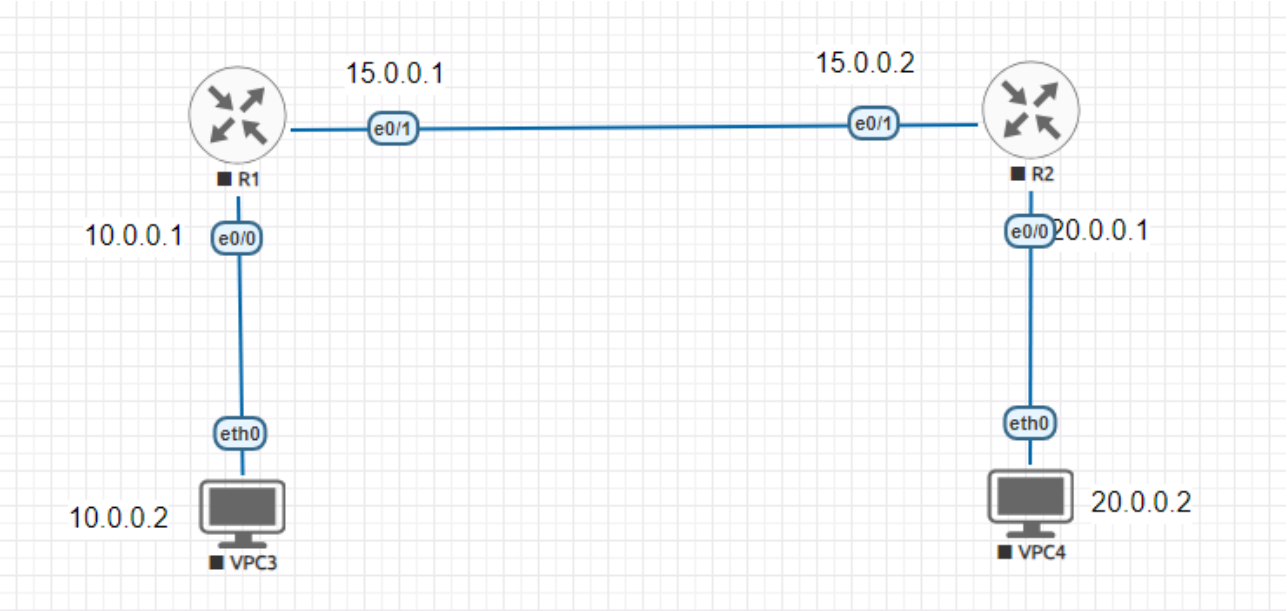
Access-list 100 permit tcp 10.0.0.0 0.255.255.255 host 20.0.0.2 eq 80

!

Interface fa0/0

Ip access-group 100 in

Diagram 2:



Preliminary Tasks:

- Connect the above network and assign IP addresses as depicted
- Configure Routing Protocol and verify connectivity

Task 3:

- Configure on R1 with time based acl that denies icmp traffic from 00:00 to 06:00 and allow rest of traffic
- The icmp is also allowed outside this time range

!R1

Time-range icmp-deny

Periodic daily 00:00 to 06:00

Exit

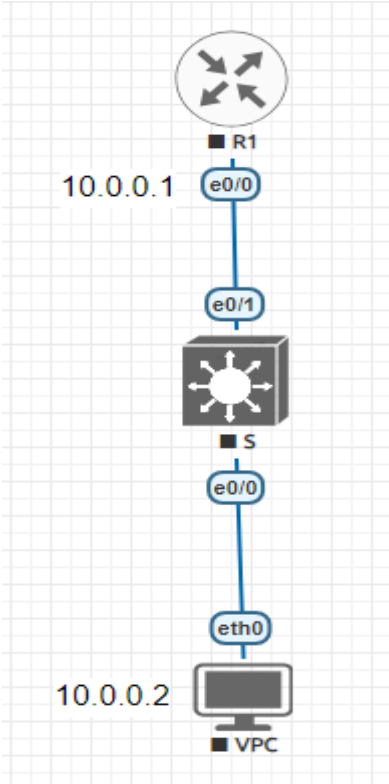
```
Ip access-list ext block_icmp
Deny icmp any any time-range icmp-deny
Permit ip any any
Interface e0/0
Ip access-group block_icmp in
```

Lab 48
Control Plane Policing

Objective:

The goal of this lab is to configure and verify control plane policing on Cisco Routers

Diagram:



Preliminary Tasks:

- Connect the network as shown in figure
- Assign IP addresses as depicted in the diagram

Task 1:

- Configure Control Plane Policing, so that ping is limited to 8000 bps on R1

!R1

Ip access-list extended icmp

Permit icmp any any

Class-map ping

Match access-group name icmp

Exit

!

Policy-map ping-policy

Class ping

Police 8000 conform-action transmit exceed-action drop

Exit

Control-plane

Service-policy input ping-policy

!Verification

From the VPCS, adjust the ping parameters so that you can reach the threshold in order to see the dropped packets example below

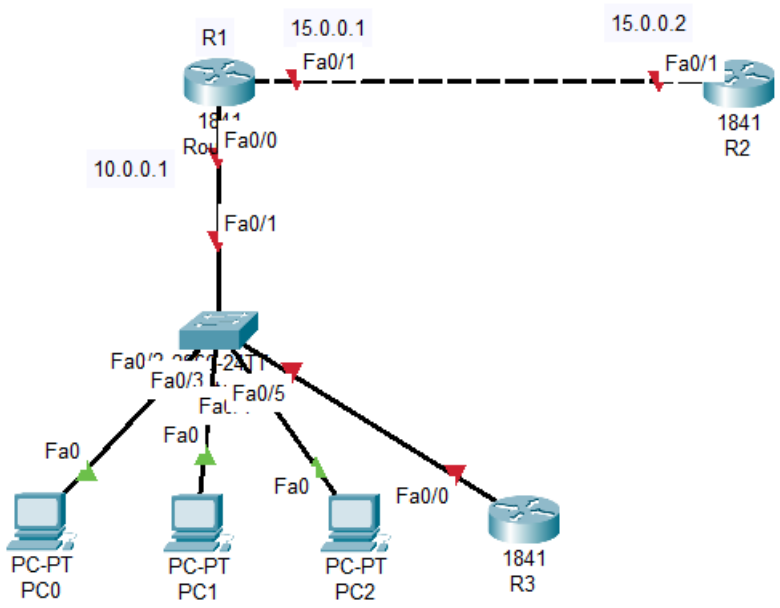
VPCS> ping 10.0.0.1 –t –l 1200

Lab 49
DHCP

Objective:

The goal of this lab is to configure and verify DHCP Client, Server and Relay on Cisco Routers

Diagram:



Preliminary Tasks:

- Connect the network as shown in figure
- Assign IP addresses as depicted in the diagram

Task 1:

- Configure R1 as DHCP Server to advertise IP addresses in the range of 10.0.0.0 network excluding IP addresses from 10.0.0.1 10.0.0.100, make 10.0.0.1 to be acting as Default Gateway and DNS server

!R1

Ip dhcp excluded-address 10.0.0.1 10.0.0.100

Ip dhcp pool Cisco

Network 10.0.0.0 255.0.0.0

Default-gateway 10.0.0.1

Dns-sever 10.0.0.1

Task 2:

- Configure R3 to get Its IP address through dhcp

!R3

Interface fa0/0

No shutdown

Ip address dhcp

Task 3:

- Remove the DHCP Configuration from R1
- Make R2 as the DHCP Server for 10.0.0.0 network with 10.0.0.1 as gateway and DNS, and 10.0.0.1 to 10.0.0.100 are excluded
- Configure R1 as DHCP Relay to forward all dhcp requests to R2
- Don’t forget to make network 10.0.0.0 reachable for R2

!R1

No ip dhcp excluded-address 10.0.0.1 10.0.0.100

No ip dhcp pool cisco

Interface fa0/0

Ip helper-address 15.0.0.2

!R2

Ip route 10.0.0.0 255.0.0.0 15.0.0.1

Ip dhcp excluded-address 10.0.0.1 10.0.0.100

Ip dhcp pool cisco

Network 10.0.0.0 255.0.0.0

Default-router 10.0.0.1

Dns-server 10.0.0.1

!Verification

Make sure PCs and R3 are getting ip address dynamically from R2 (DHCP Server)

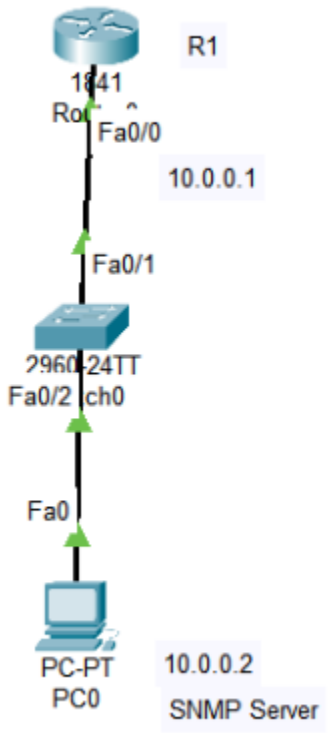
Lab 50

SNMP

Objective:

The main goal of this lab is to configure and verify SNMP on Cisco Router

Diagram:



Preliminary Tasks:

- Connect the network as shown in the depicted figure.
- Assign IP addresses as depicted in the diagram

Task 1:

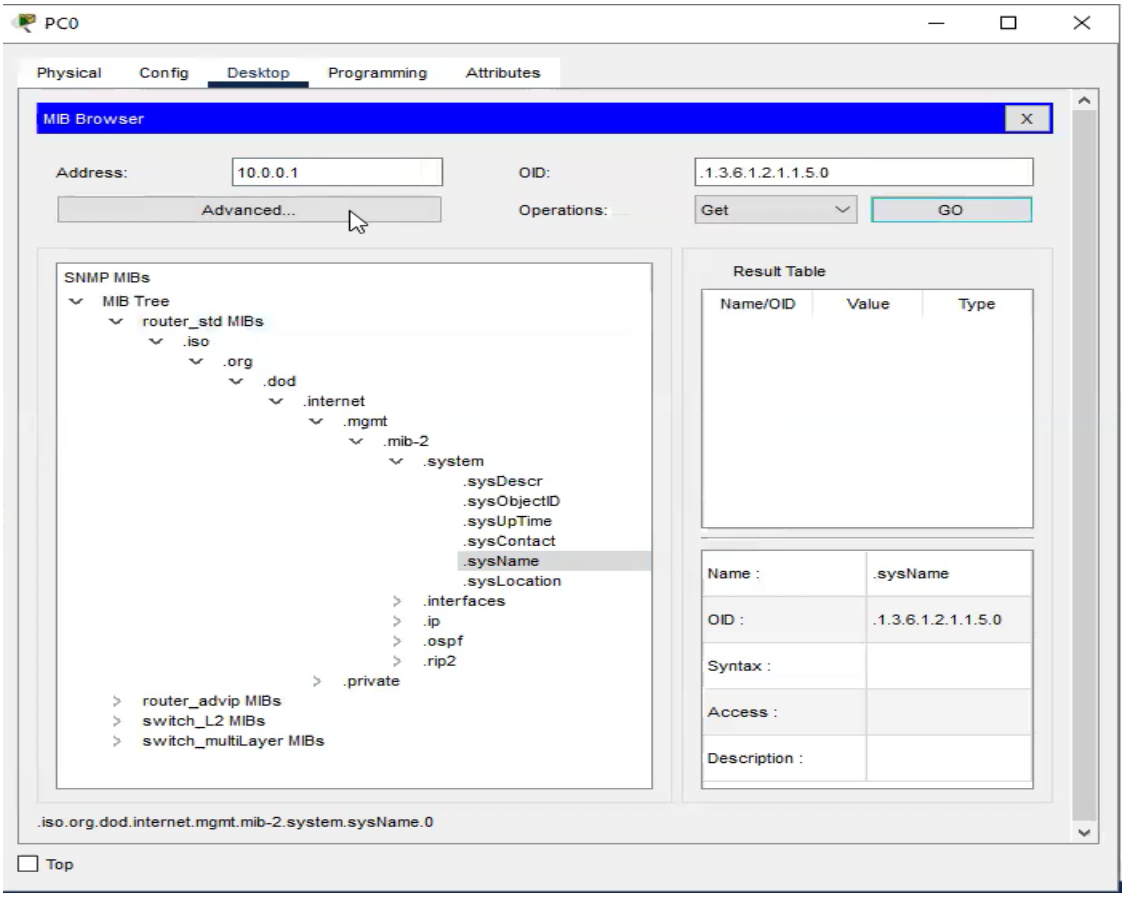
- Configure The router with SNMP and read/write community of cisco
- Set the NMS to get the system name of the Router, and uptime
- Don’t forget to set the managed ip and community in the NMS

!R1

Snmp-server community cisco rw

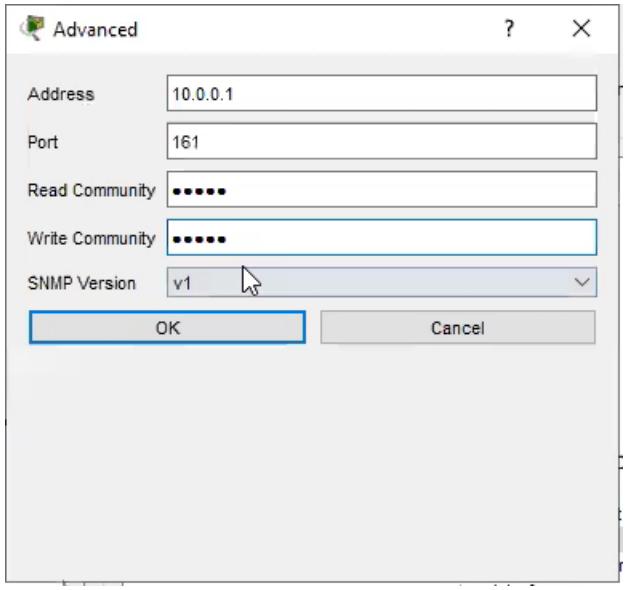
!NMS

Navigate to Sysname and sysuptime



!Don’t Forget to configure the Router IP address in MIB NMS

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

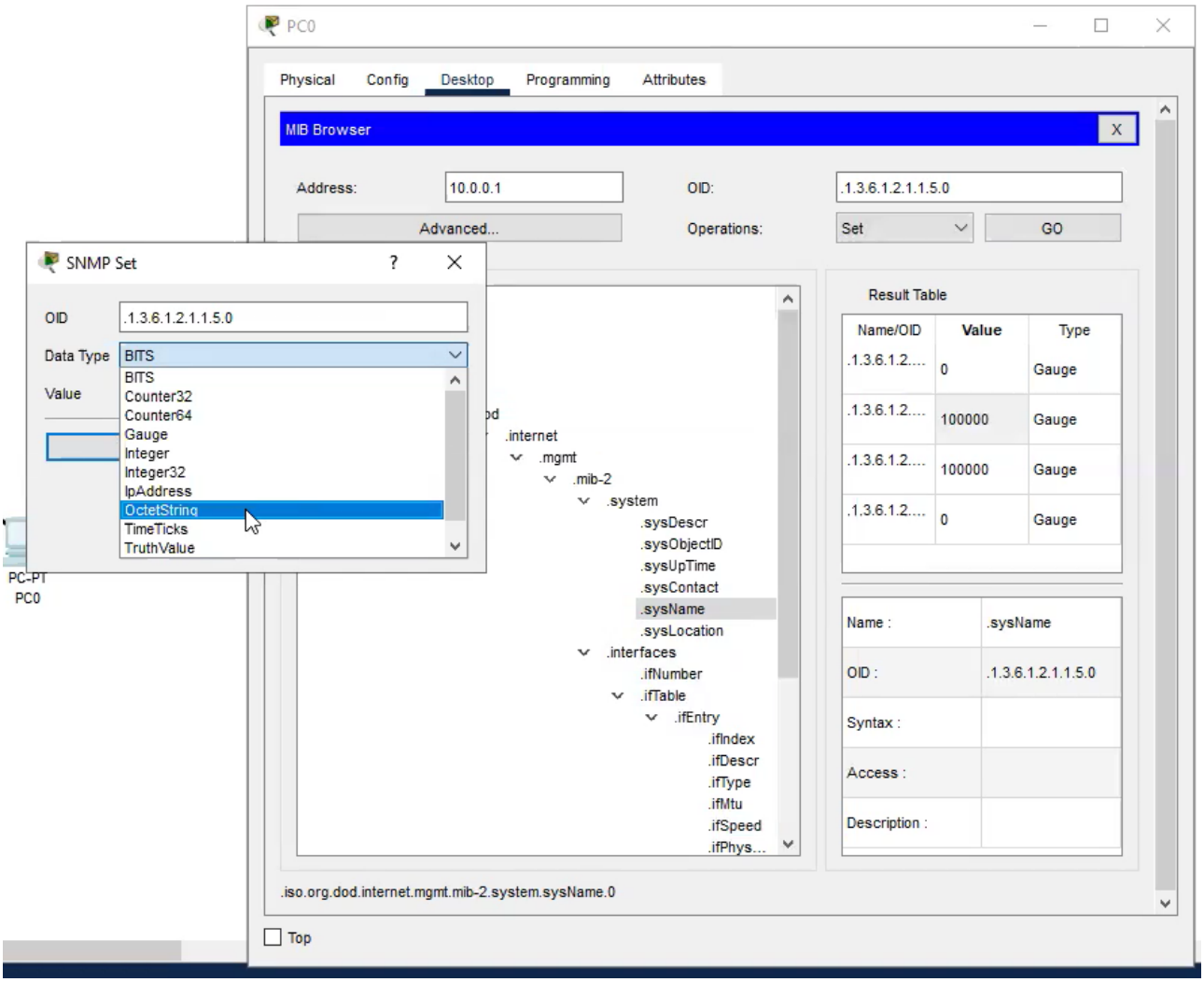


Task 2:

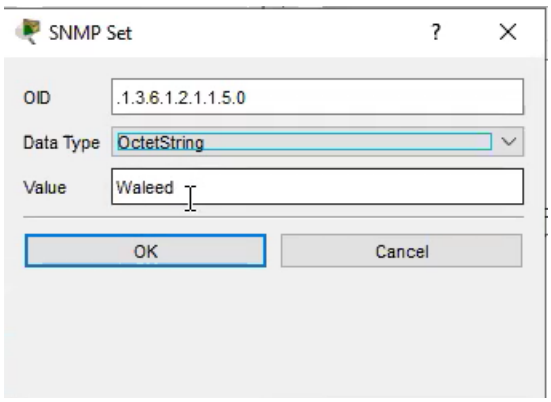
- Configure the MIB Browser to set the Router Name by using the Set parameter

!NMS

In the MIB Browser:



Then



Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

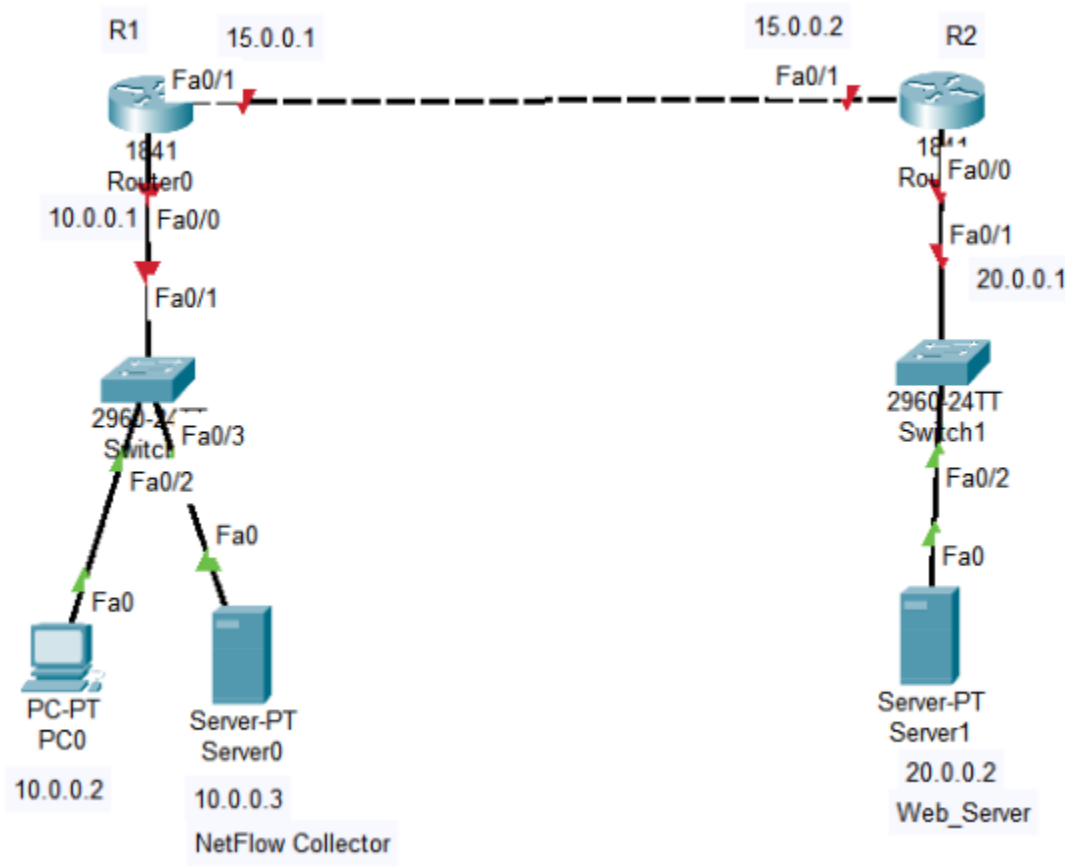
Lab 51

NETFLOW

Objective:

The main goal of this lab is to configure and verify NETFLOW on Cisco Router

Diagram:



Preliminary Tasks:

- Connect the network as shown in the figure and assign IP addresses as shown in the diagram
- Enable Routing Protocol between the two routers

Task 1:

- Configure R1 to monitor the traffic entering interface fa0/0 using Netflow

- Configure 10.0.0.3 as Netflow collector.

!R1
Interface fa0/0
Ip flow ingress
Exit
Ip flow-export version 9
Ip flow-export destination 10.0.0.3 9996
Ip flow-export source fa0/0

!Verification
Make ping and http traffic from 10.0.0.2 to the 20.0.0.0 network and then issue the show commands and check the netflow collector data

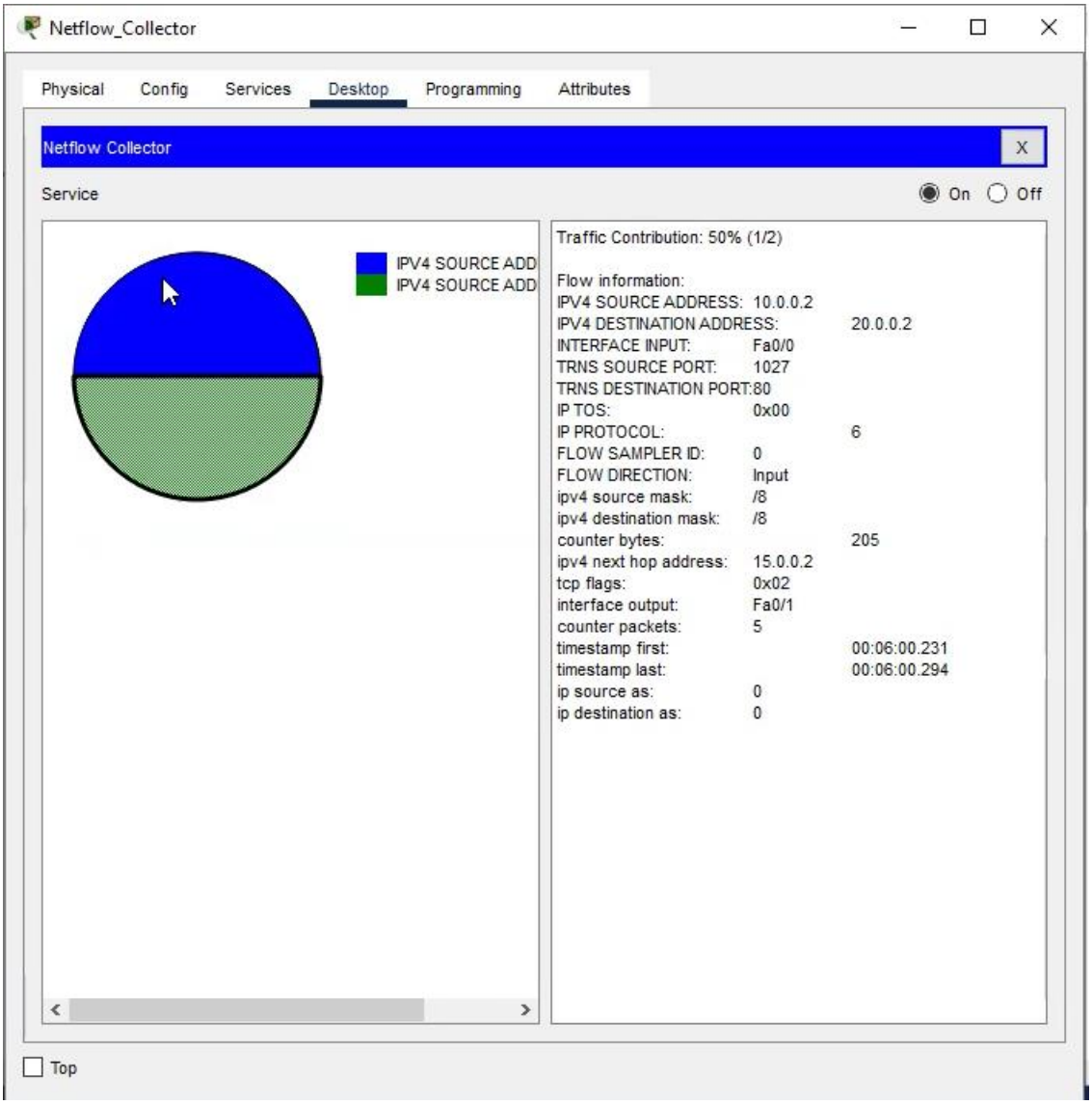
Show ip cache flow

```
IP packet size distribution (170 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .088 .000 .912 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  1 active, 4095 inactive, 4 added
  0 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-HTTP             3      0.0         5    41      0.0       0.0    3397.0
Total:               3      0.0         5    41      0.0       0.0    3397.0

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0         10.0.0.2        Fa0/1         20.0.0.2        01 0000 0000   155
```


Netflow_Collector
Physical
Config
Services
Desktop
Programming
Attributes
Netflow Collector
X
Service
On
Off
IPV4 SOURCE ADD
IPV4 SOURCE ADD
Traffic Contribution: 50% (1/2)
Flow information:
IPV4 SOURCE ADDRESS: 10.0.0.2
IPV4 DESTINATION ADDRESS: 20.0.0.2
INTERFACE INPUT: Fa0/0
TRNS SOURCE PORT: 1027
TRNS DESTINATION PORT:80
IP TOS: 0x00
IP PROTOCOL: 6
FLOW SAMPLER ID: 0
FLOW DIRECTION: Input
ipv4 source mask: /8
ipv4 destination mask: /8
counter bytes: 205
ipv4 next hop address: 15.0.0.2
tcp flags: 0x02
interface output: Fa0/1
counter packets: 5
timestamp first: 00:06:00.231
timestamp last: 00:06:00.294
ip source as: 0
ip destination as: 0
Top

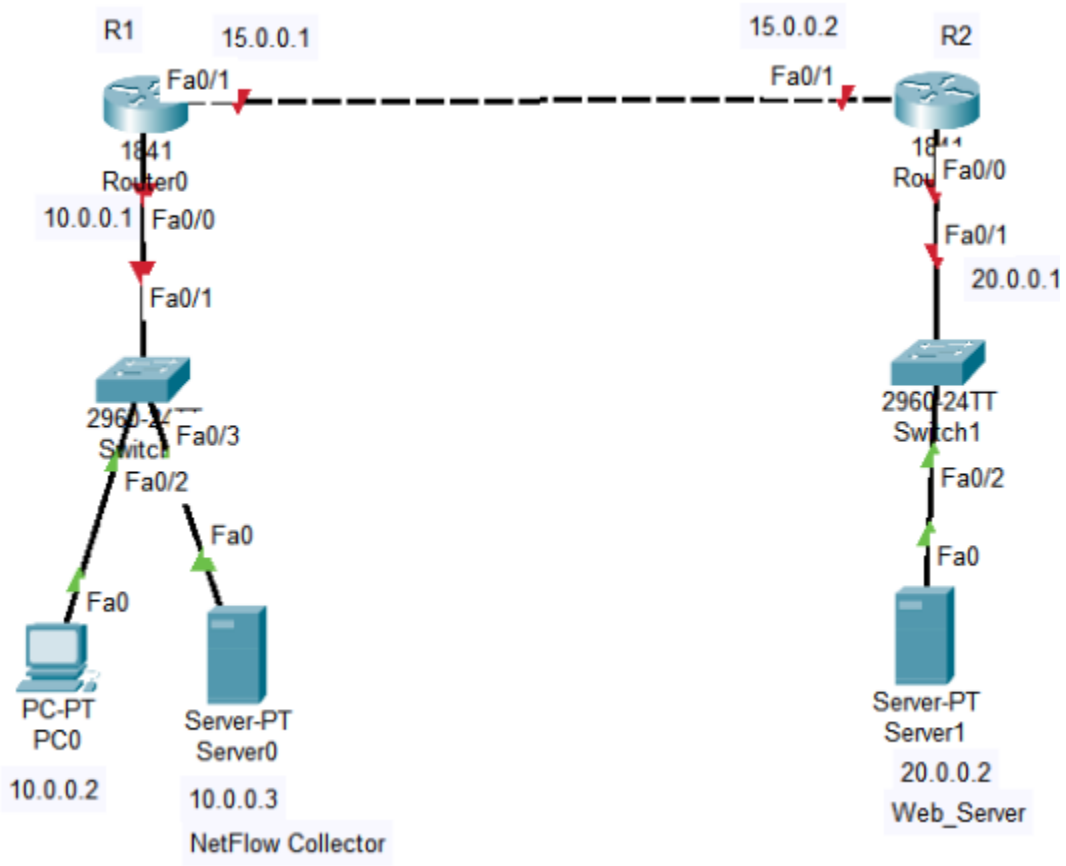
Lab 52

Flexible NETFLOW

Objective:

The main goal of this lab is to configure and verify Flexible NETFLOW on Cisco Router

Diagram:



Preliminary Tasks:

- Connect the network as shown in the figure and assign IP addresses as shown in the diagram
- Enable Routing Protocol between the two routers

Task 1:

- Configure R1 to monitor the traffic using flexible netflow collector

- Make a flow record to match the destination address
- Make the flow record to collect counter Bytes
- Make a flow exporter with a destination of 10.0.0.3 and version 9

```
!R1
Flow record custom
Match ipv4 destination address
Collect counter bytes
!
Flow exporter custom
Destination 10.0.0.3
Export-protocol netflow-v9
Transport udp 9996
!
Flow monitor custom
Record custom
Exporter custom
!
Interface fa0/0
Ip flow monitor custom input
```

!Verification

Make ping and http traffic from 10.0.0.0 to 20.0.0.0 network and check the following

!R1

Show flow monitor custom cache

```
Cache type:                               Normal
Cache size:                                 4096
Current entries:                               1
High Watermark:                                1

Flows added:                                   1
Flows aged:                                    0
  - Active timeout    (  1800 secs)            0
  - Inactive timeout (    15 secs)            0
  - Event aged                                 0
  - Watermark aged                             1
  - Emergency aged                             0

IPV4 DST ADDR      counter bytes
=============      =============
20.0.0.2           31898
Router#
```

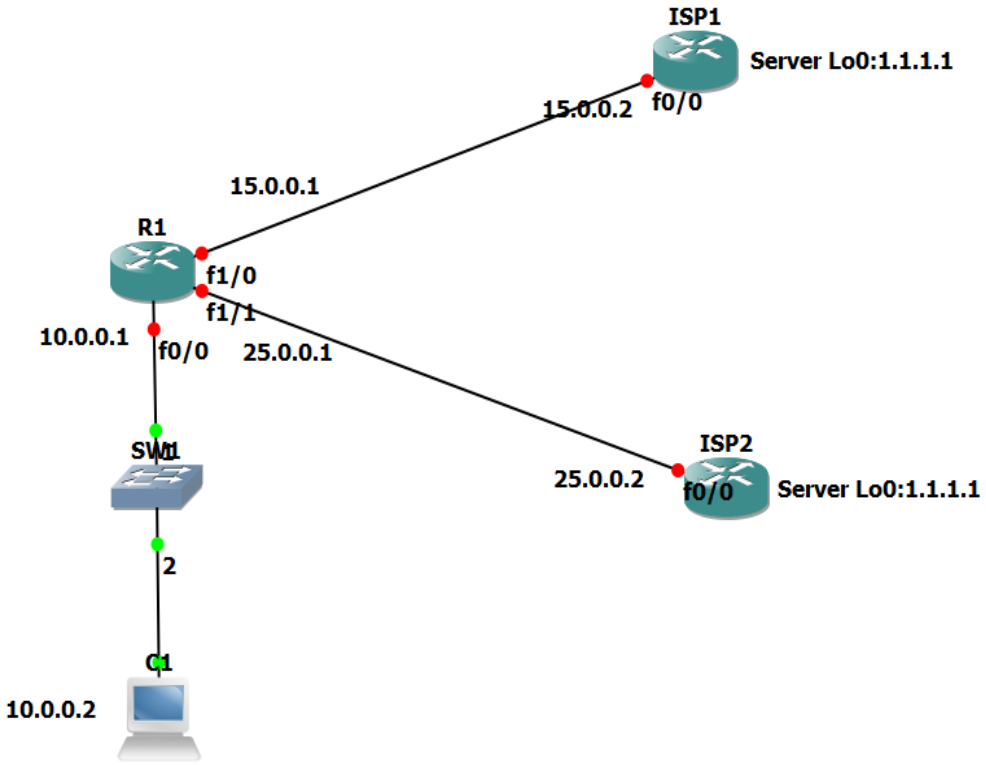
Lab 53

IP SLA

Objective:

The main goal of this lab is to configure and verify IP SLA Configuration on Cisco Router

Diagram:



Preliminary Tasks:

- Connect the network as shown in the figure and assign IP addresses as shown in the diagram
- Configure Static route on ISP1 & ISP2 toward 10.0.0.0 network

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

Task 1:

- Configure Static route on R1 for 1.1.1.1 network toward ISP1
- Configure IP SLA on R1 to ping 1.1.1.1 using Fa1/0 interface with 1000 ms as timeout and 1 s as frequency
- Track ip sla reachability state
-

!R1
Ip route 1.1.1.1 255.255.255.255 15.0.0.2
!
Ip sla 1
Icmp-echo 1.1.1.1 source-interface fa1/0
Timeout 1000
Frequency 1
Exit
!
Ip sla schedule 1 start-time now life forever
!
Track 1 ip sla 1 reachability
!

Task 2:

- Configure primary conditional default route on R1 toward ISP1, and the condition is based on the track status
- Configure a secondary default route on R1 toward ISP2

!R1
Ip route 0.0.0.0 0.0.0.0 15.0.0.2 5 track 1
Ip route 0.0.0.0 0.0.0.0 25.0.0.2 10

!Verification:
Show the ip route status on R1, and the track 1 and SLA1

!R1
Show ip route

Gateway of last resort is 15.0.0.2 to network 0.0.0.0

    1.0.0.0/32 is subnetted, 1 subnets
S   1.1.1.1 [1/0] via 15.0.0.2
C   25.0.0.0/8 is directly connected, FastEthernet1/1
C   10.0.0.0/8 is directly connected, FastEthernet0/0
C   15.0.0.0/8 is directly connected, FastEthernet1/0
S*   0.0.0.0/0 [5/0] via 15.0.0.2

Show ip sla statistics

IPSLAs Latest Operation Statistics

IPSLA operation id: 1
Type of operation: icmp-echo
       Latest RTT: 39 milliseconds
Latest operation start time: *18:28:13.319 UTC Tue Jul 15 2025
Latest operation return code: OK
Number of successes: 143
Number of failures: 57
Operation time to live: Forever

Show track 1
Track 1
  IP SLA 1 reachability
  Reachability is Up
    2 changes, last change 00:03:14
  Latest operation return code: OK
  Latest RTT (millisecs) 64
  Tracked by:
    STATIC-IP-ROUTING 0

Task 3

Create another loopback on both ISP1 & ISP2 30.0.0.1, and make a continuous ping from the PC 10.0.0.2 toward 30.0.0.1, and disconnect or shutdown the 1.1.1.1 interface or the 15.0.0.0 interest to test the failover of the default route to the secondary path

!ISP1&ISP2
Int lo1
Ip add 30.0.0.1 255.255.255.255
!

!Verification

You will notice the fast failover to the second link seamlessly

DNA Center Module

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

Lab 54

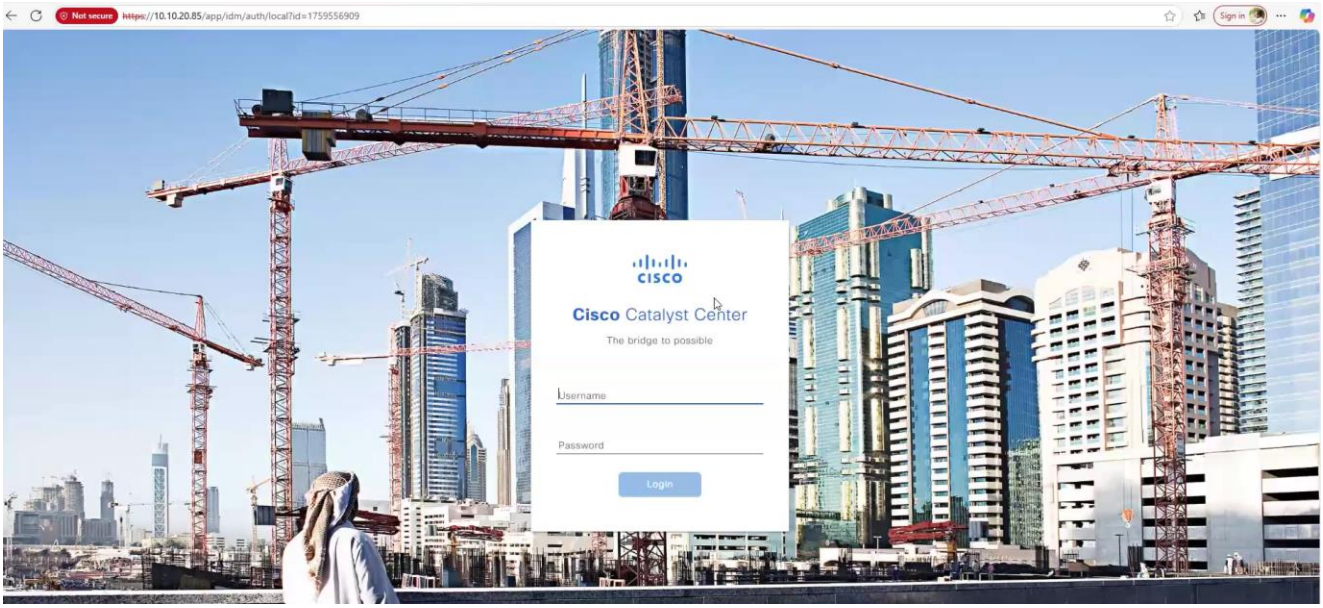
DNA Center

Objective:

The main goal of this lab is to explore DNA Center GUI Management Platform

Task 1:

Login to the DNA Center GUI using IP address and Credentials Provided. If you don't have a DNA Center, I recommend you to use DNA Center in one of the Cisco Sandboxes

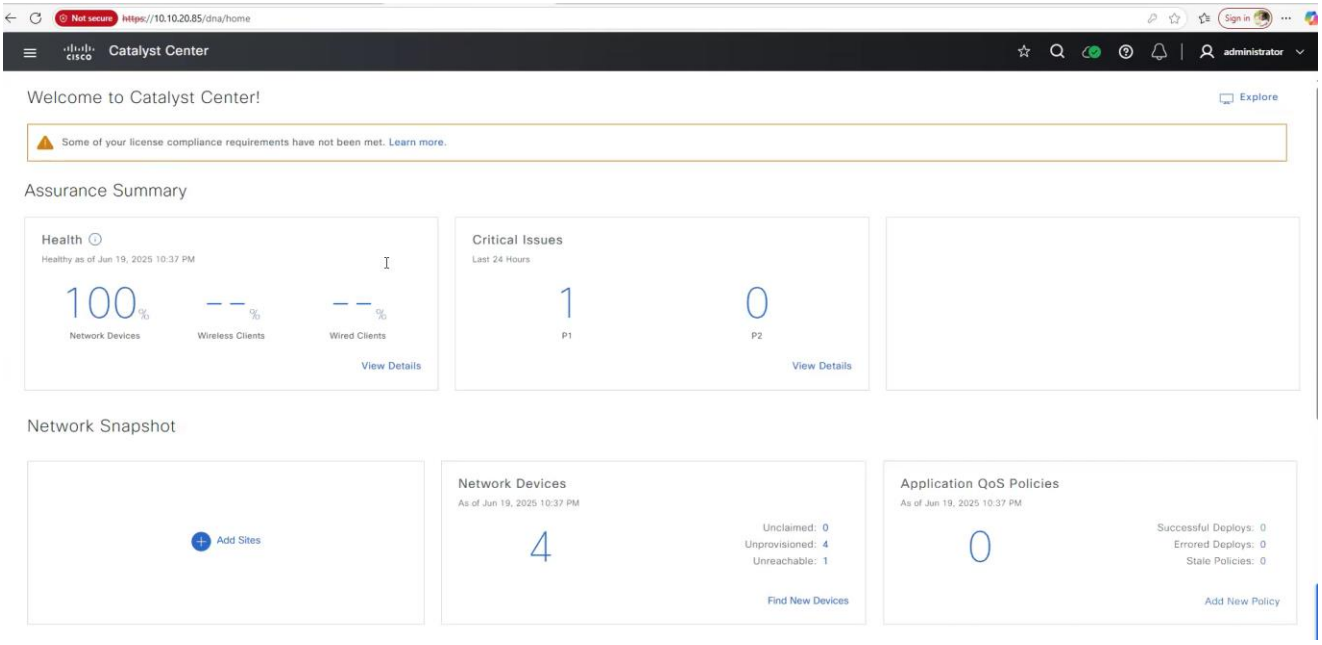


Task 2:

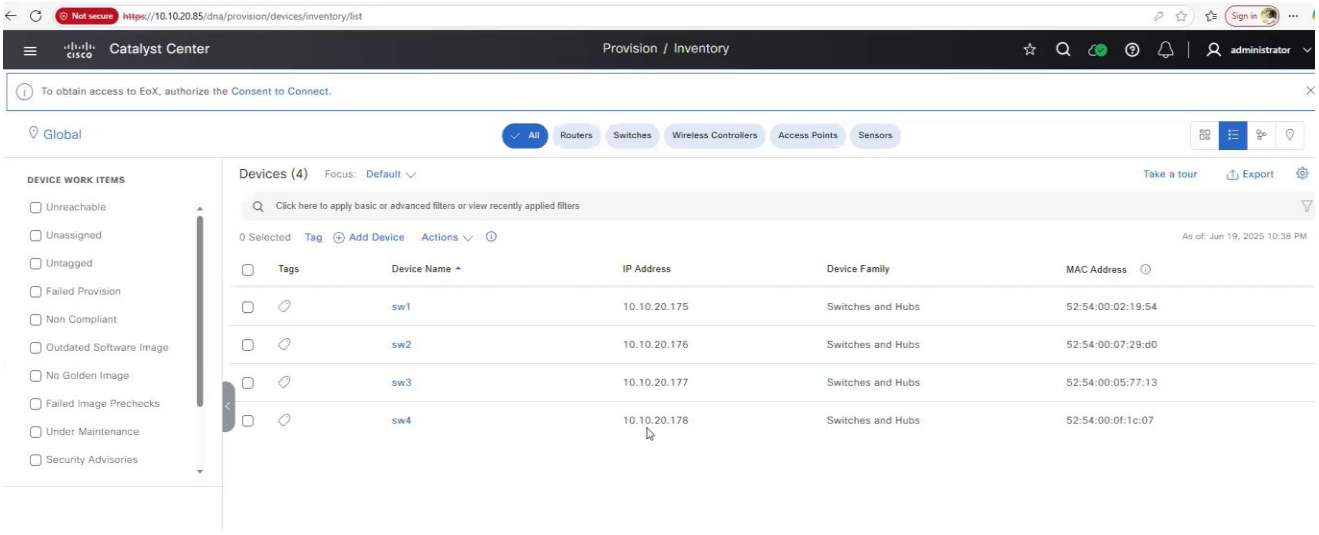
Start Exploring and checking the different features of the DNA Center

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

Main Page of the DNA Center (Catalyst Center)

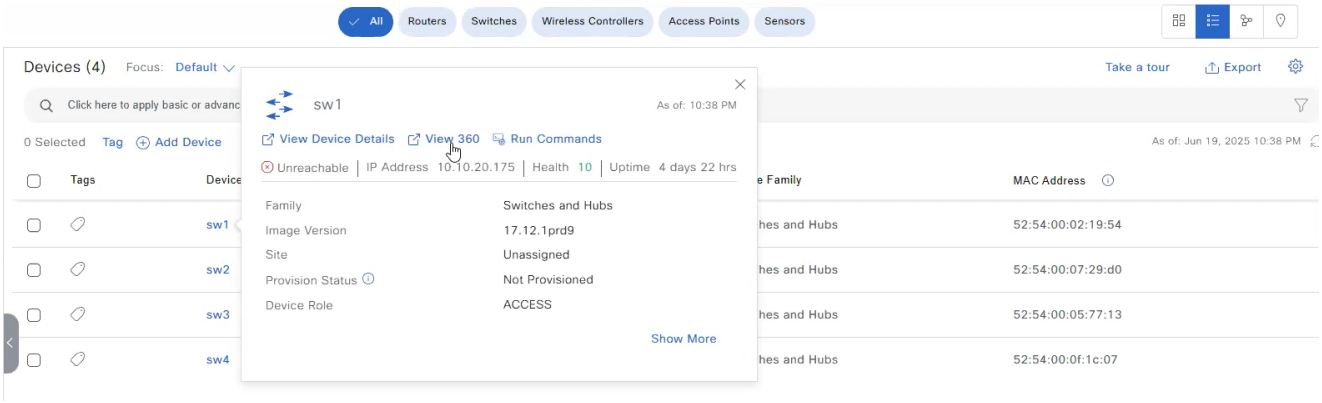


If you clicked in the (4) Shown in the network devices in the main page, It will display the network devices

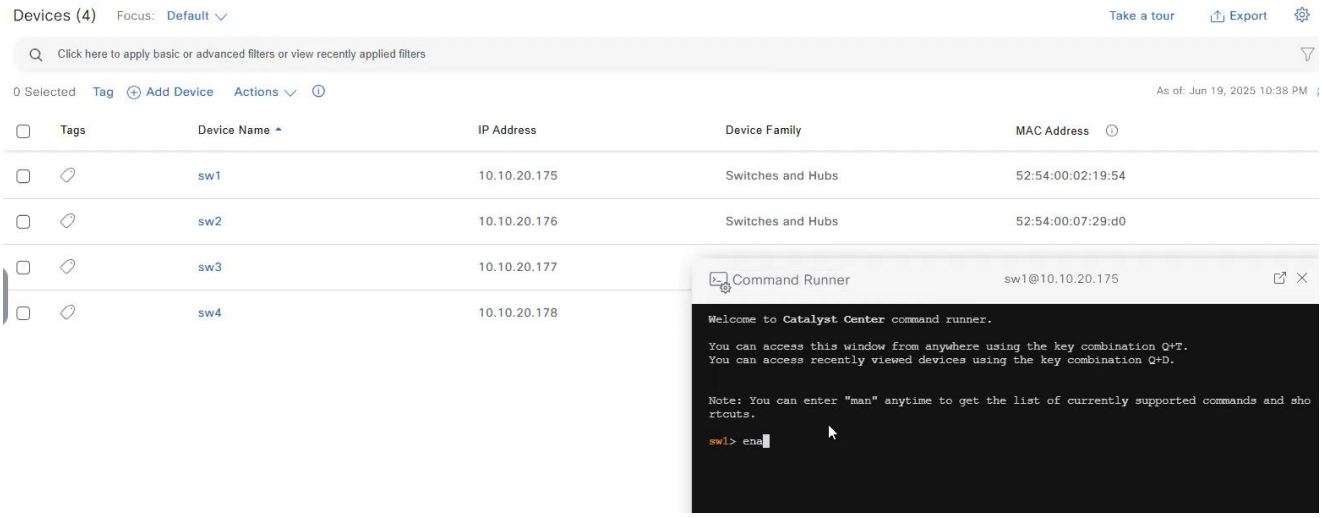


Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

You can point to SW1, and choose to see the 360 status

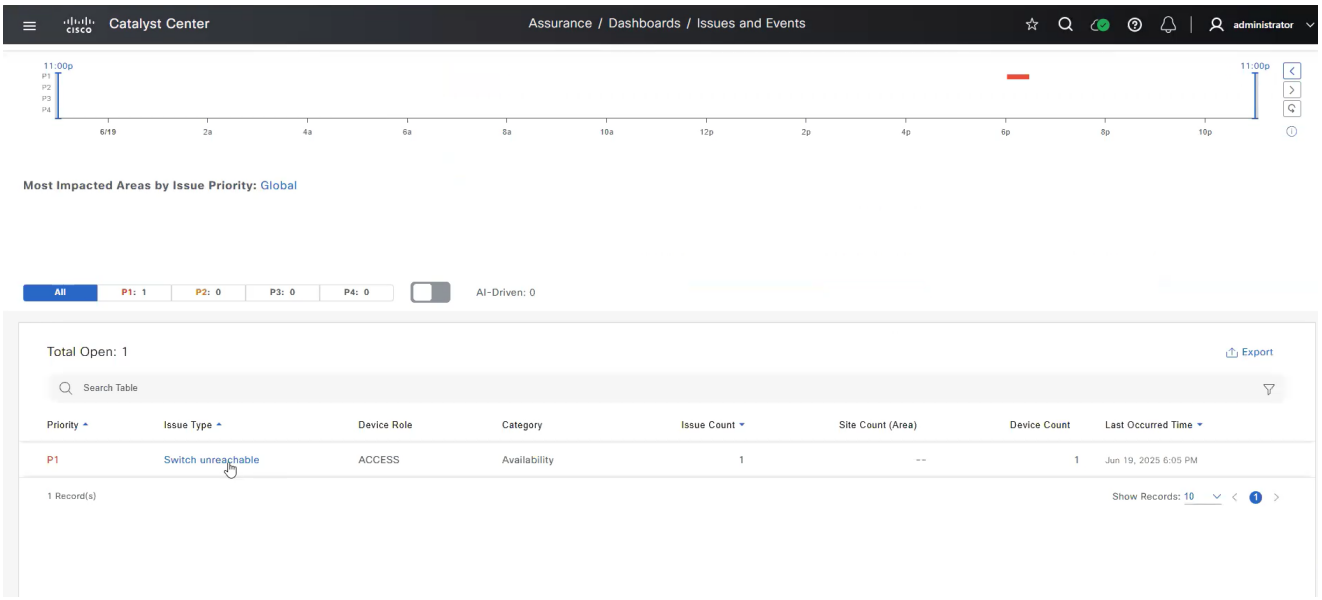


You can alternatively choose to select run commands to run commands

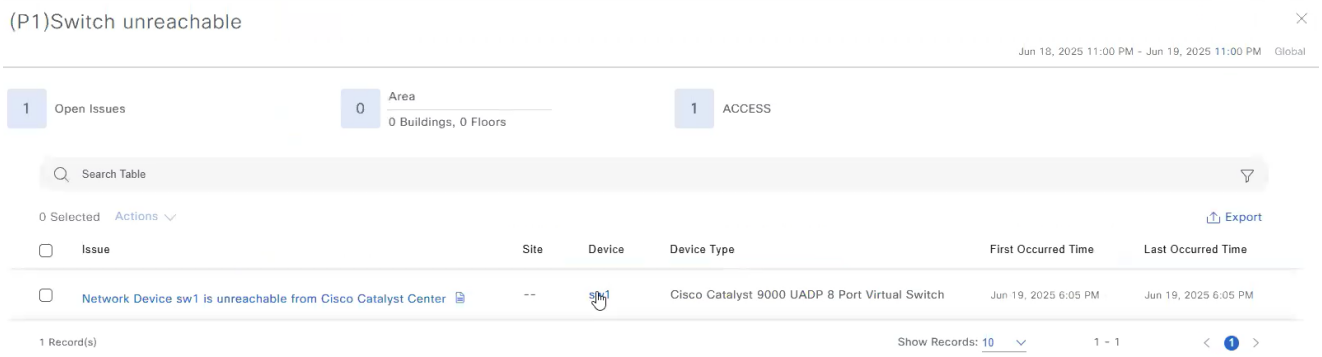


Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

You can go to the main menu and then go to Assurance>Issues and Events

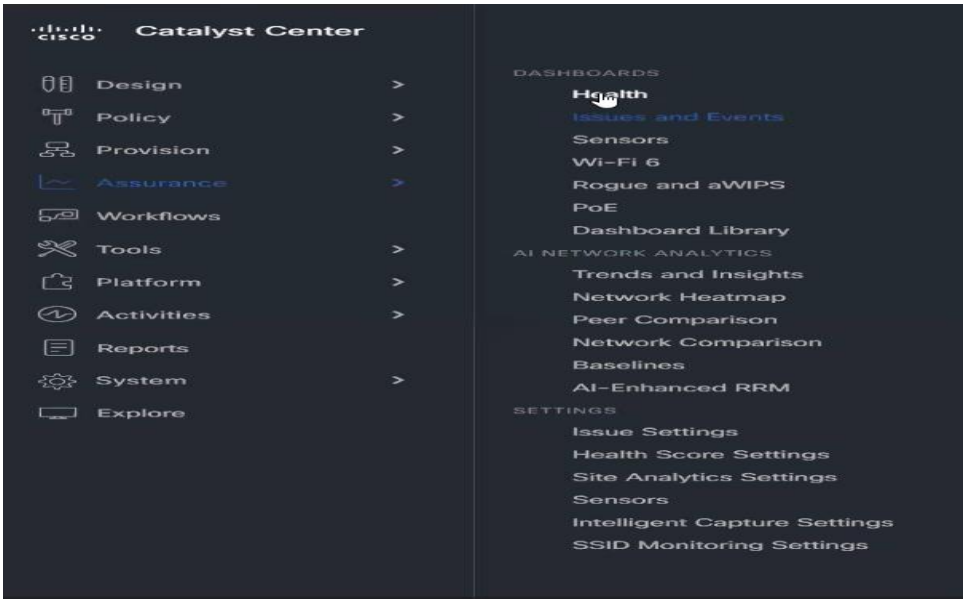


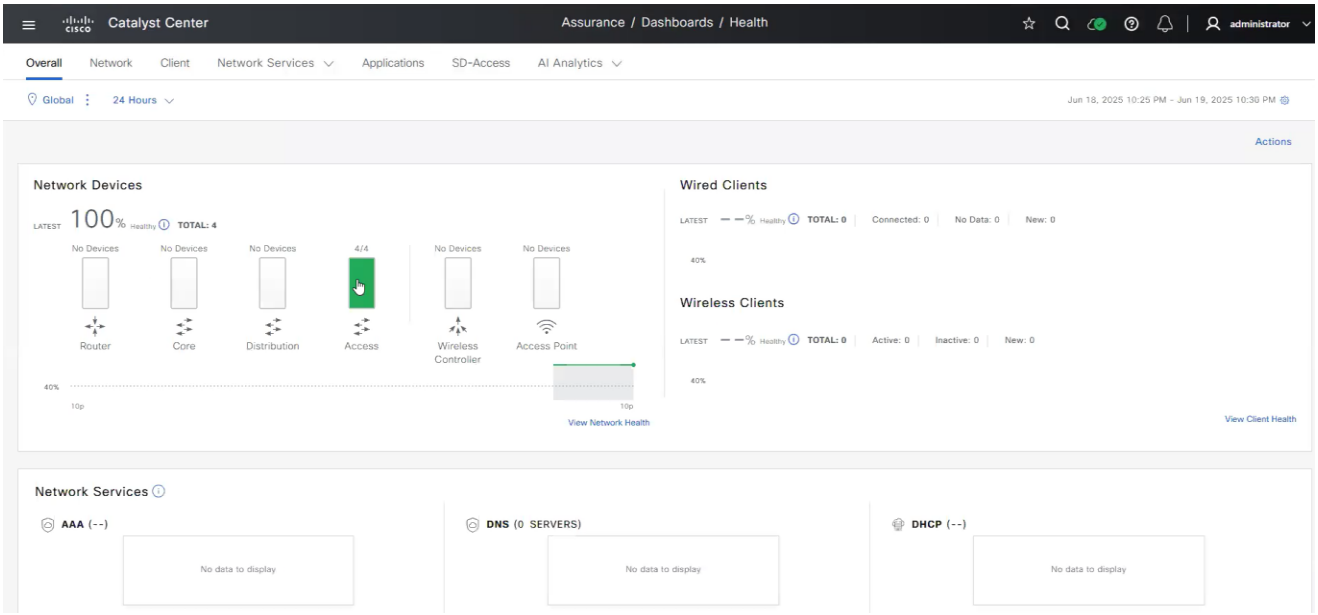
You can select that switch



You can go to
Main Menu>Assurance>Health

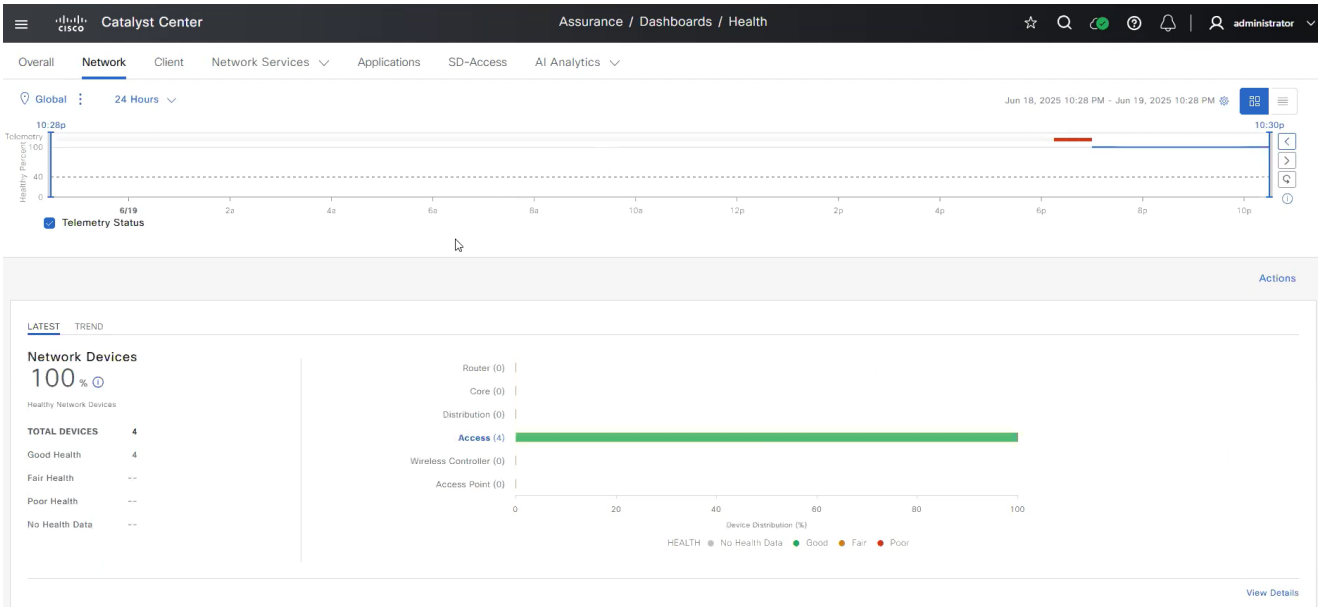
Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com



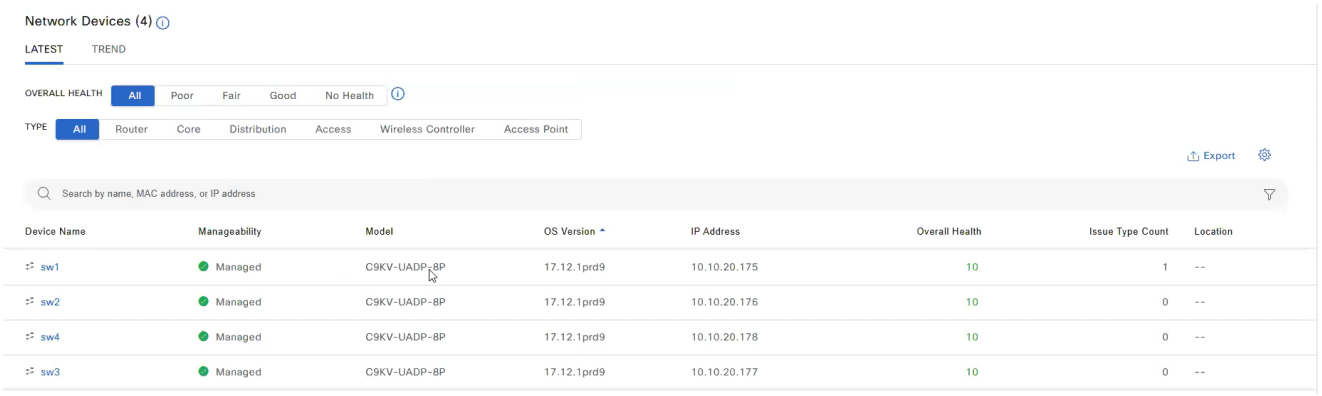


We can go to the Network Tab in the same page

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

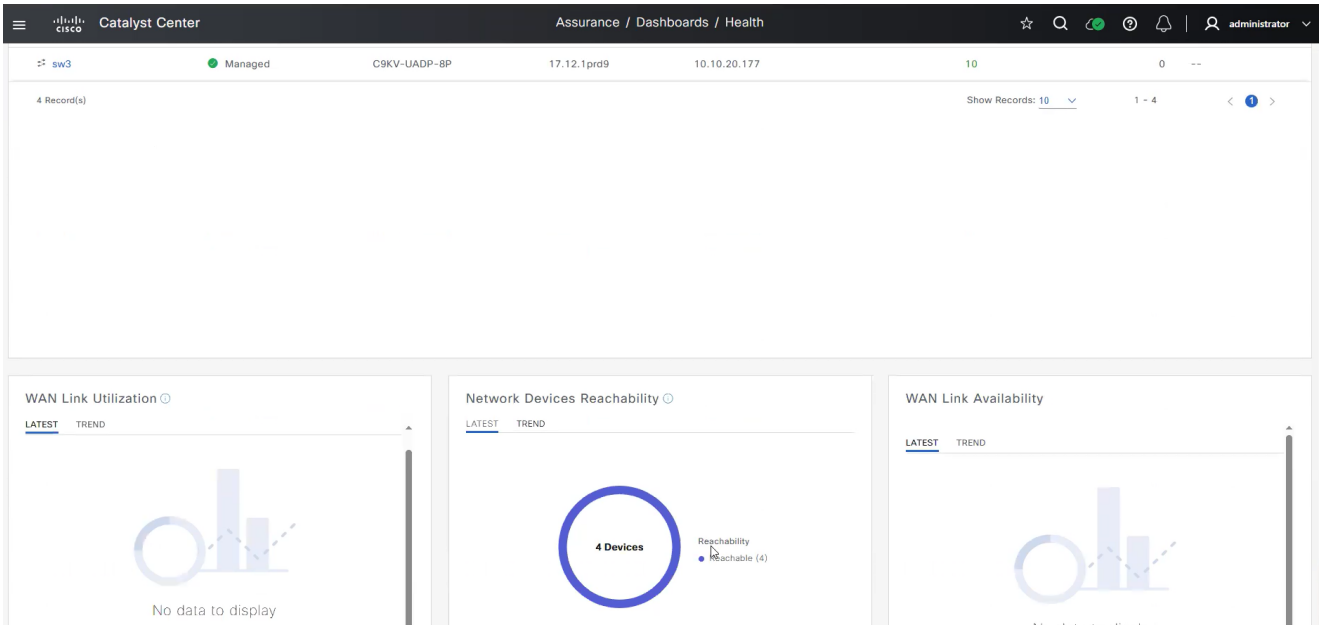


If we scroll down, we can see the details of the network devices

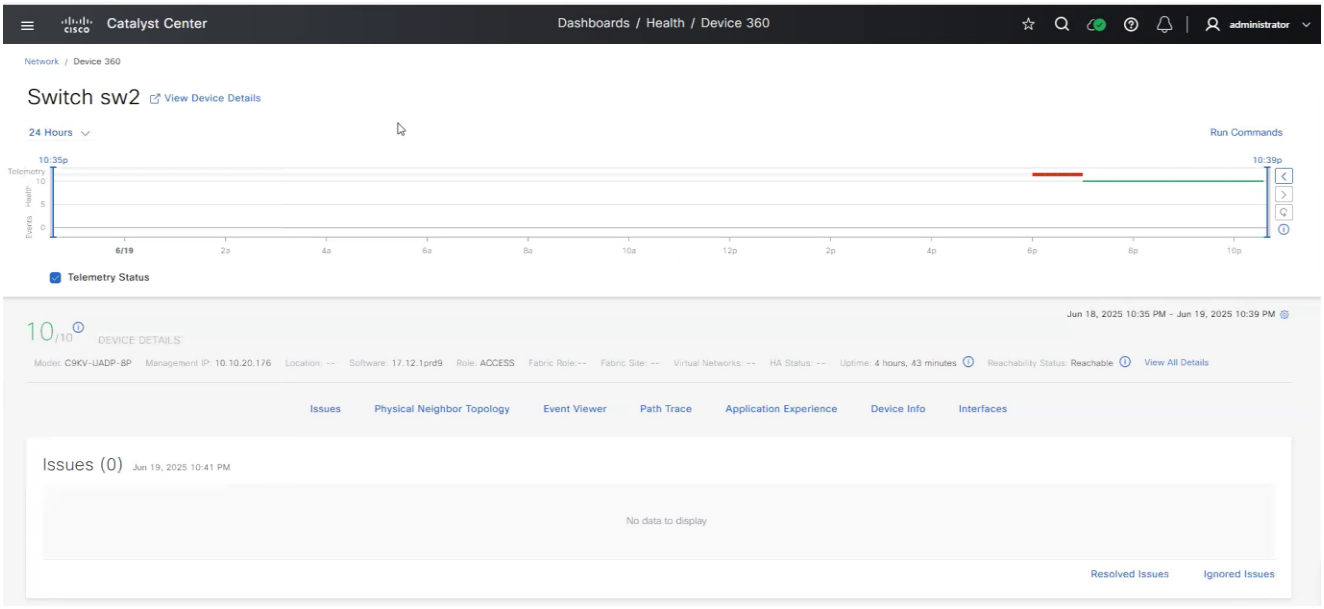


If we scroll down further

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

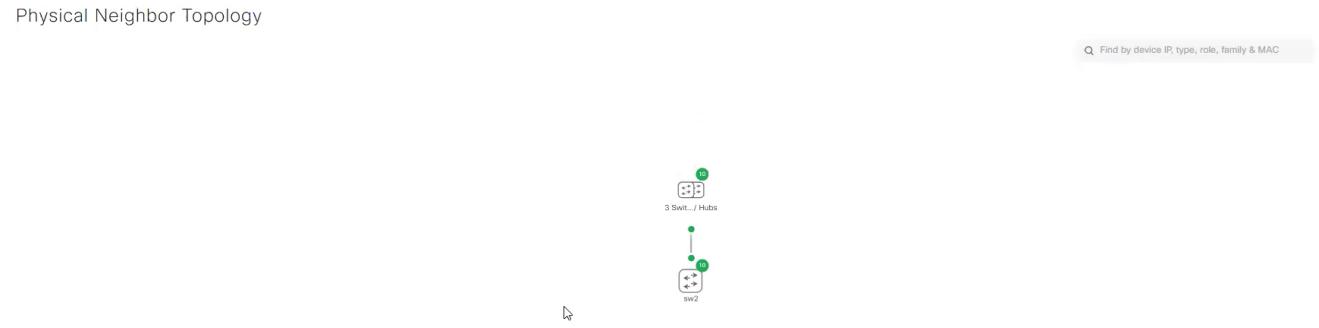


In the same page you can go to SW2 for example under Network Devices

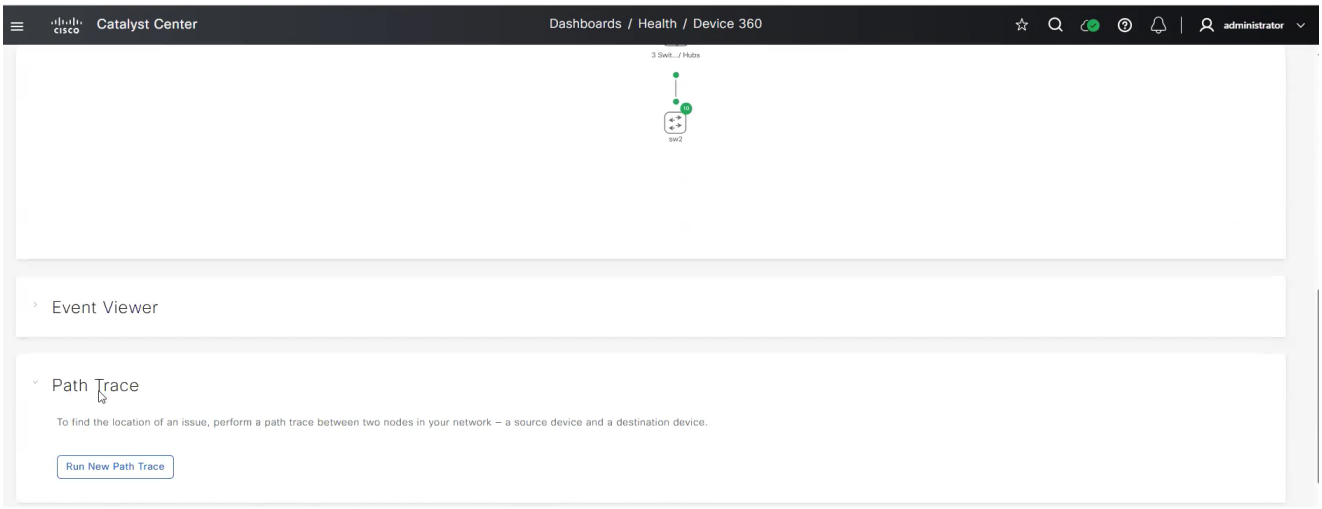


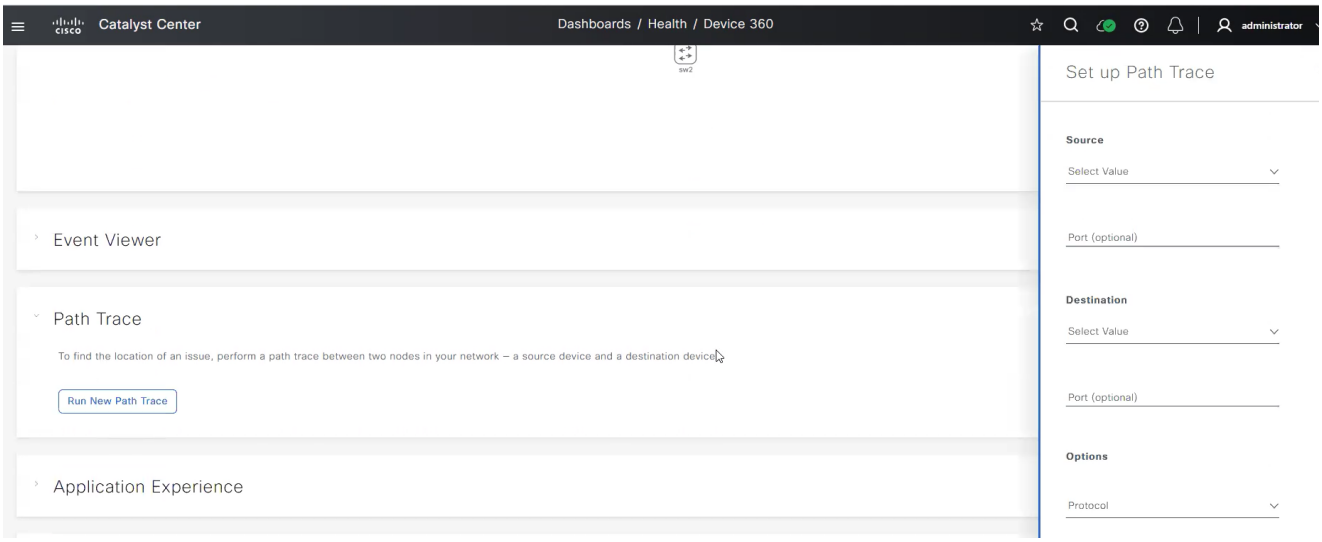
You can scroll down to check the physical topology

Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com



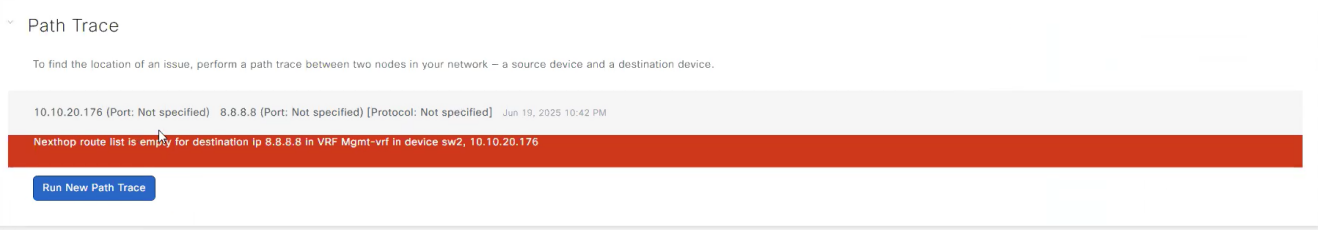
You can Scroll down to check a very powerful feature called path trace, that enables engineers to make test of a certain traffic if it will pass through the network or not





Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

If I tried to make a test of ping between SW2 (10.10.20.176) and 8.8.8.8 the path trace result will be:



Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com