CCNP LAB GUIDE

ENCOR

Version 1.1

Developed By: Waleed Adlan

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

EIGRP

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

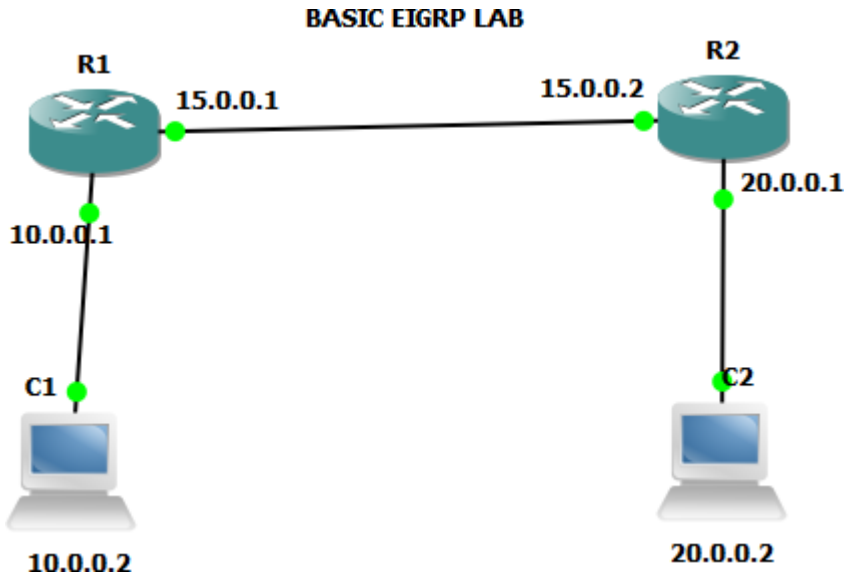
LAB 1

Basic EIGRP Configuration

Objective:

The lab main goal is to configure eigrp between two routers as shown in the below diagarm, and ensure basic connectivity between the distant 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
```

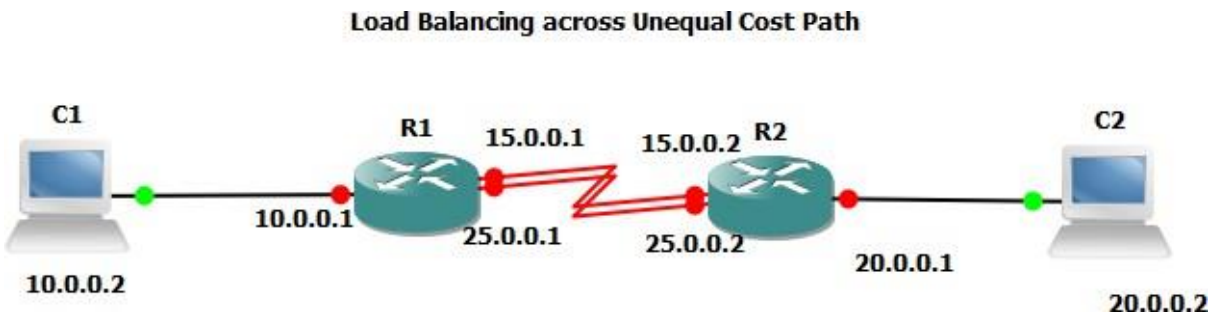
Lab 2

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.

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

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

OSPF

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

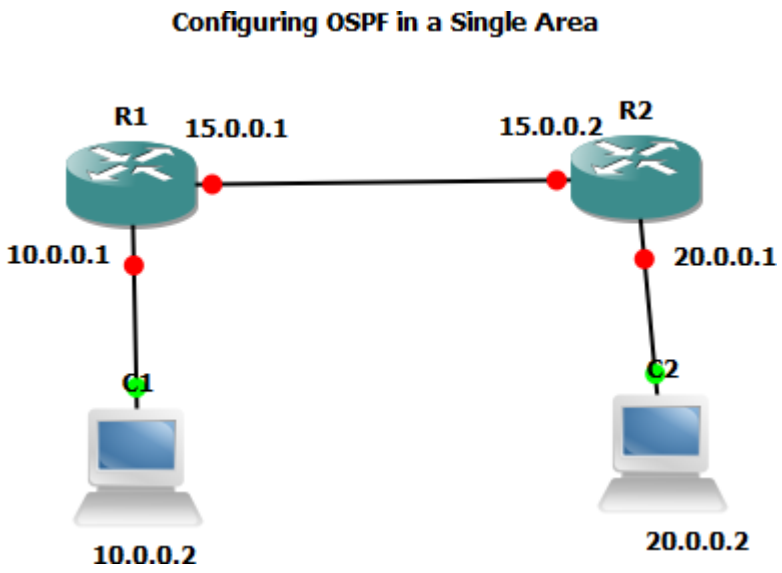
Lab 3

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

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

!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....

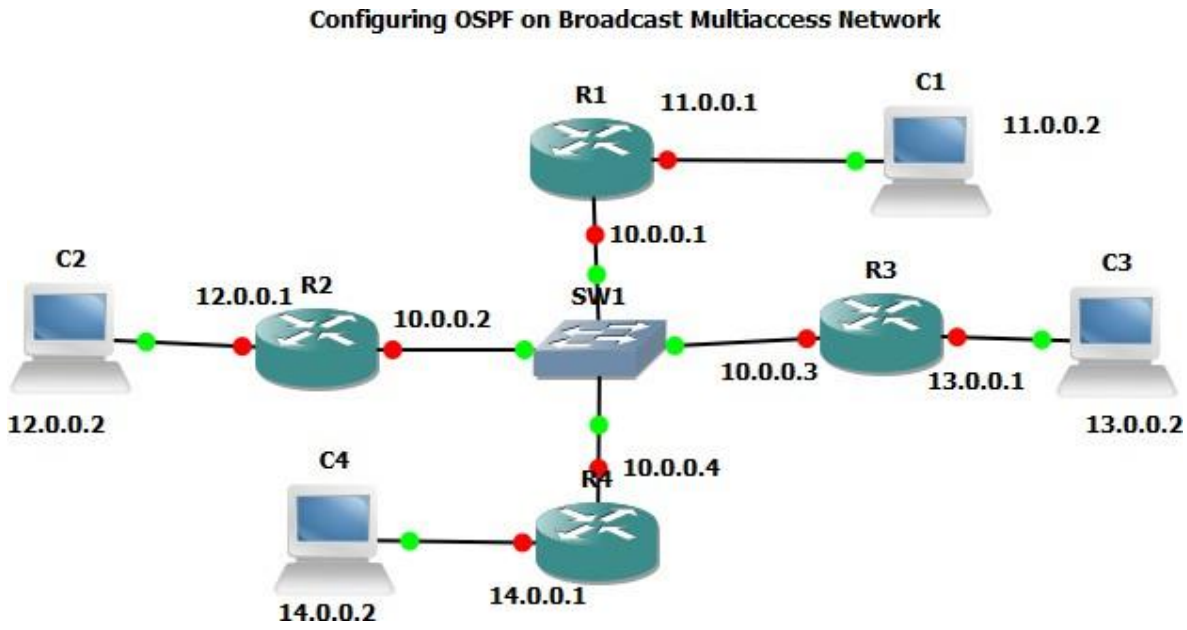
Lab 4

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...

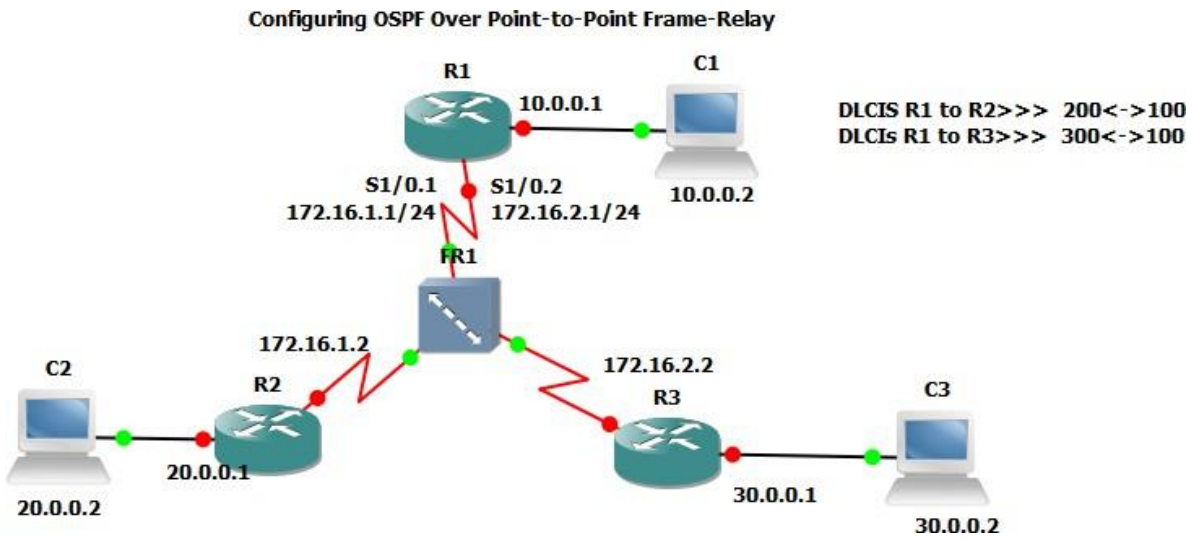
Lab 5

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....

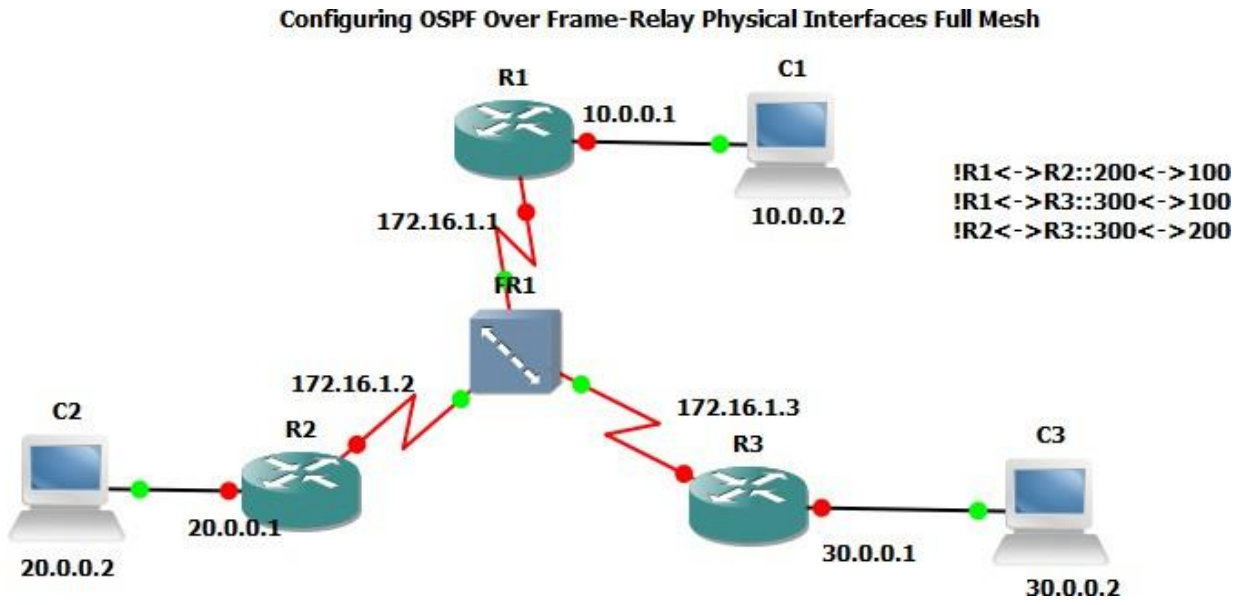
Lab 6

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……

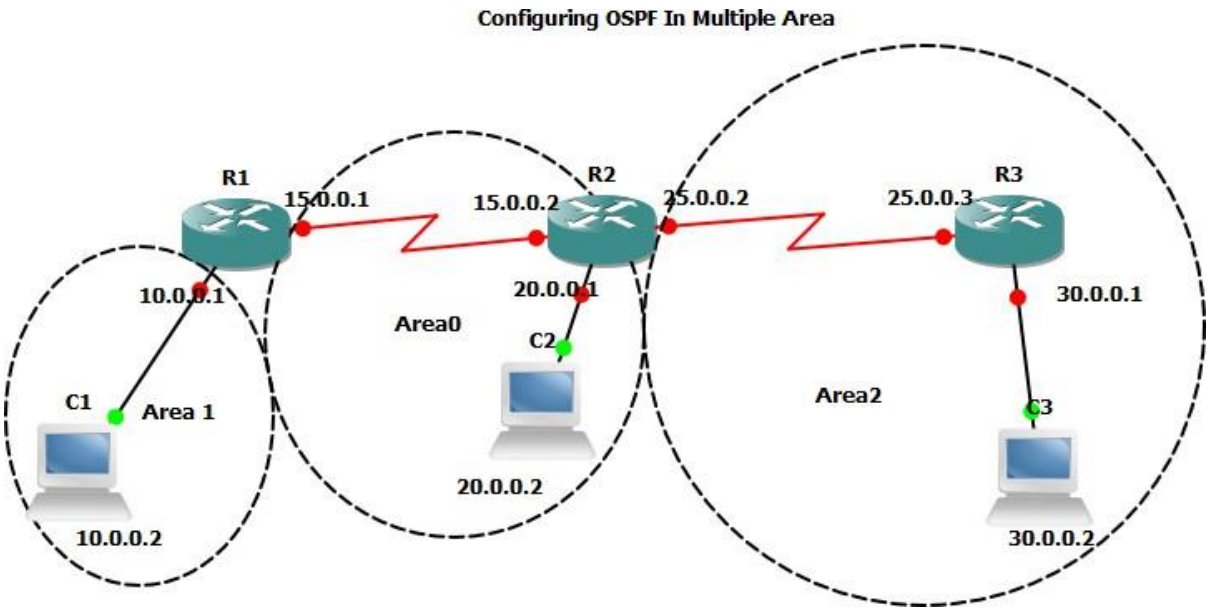
Lab 7

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 5

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#

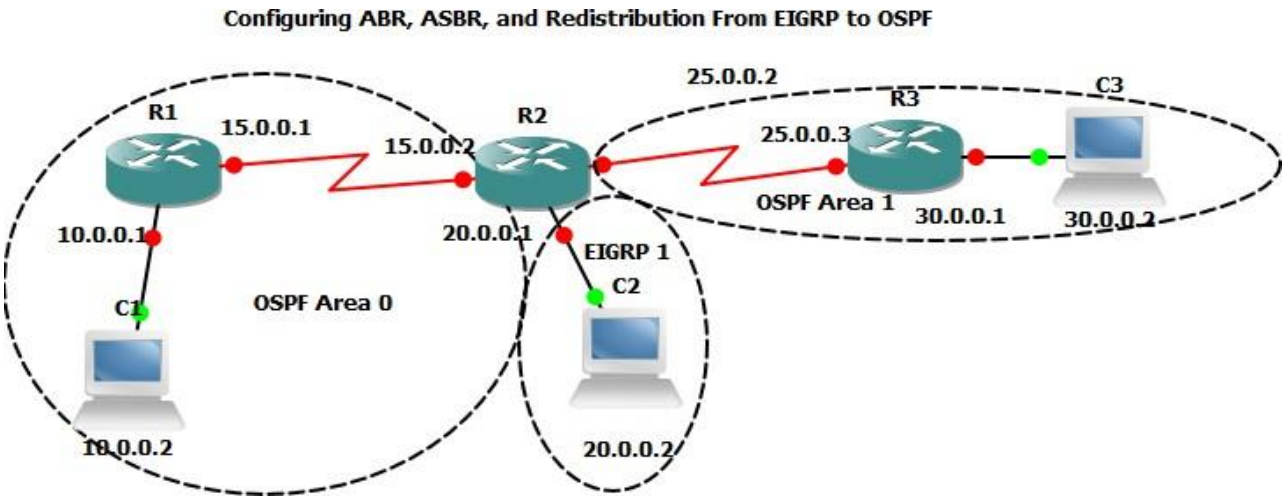
Lab 8

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...

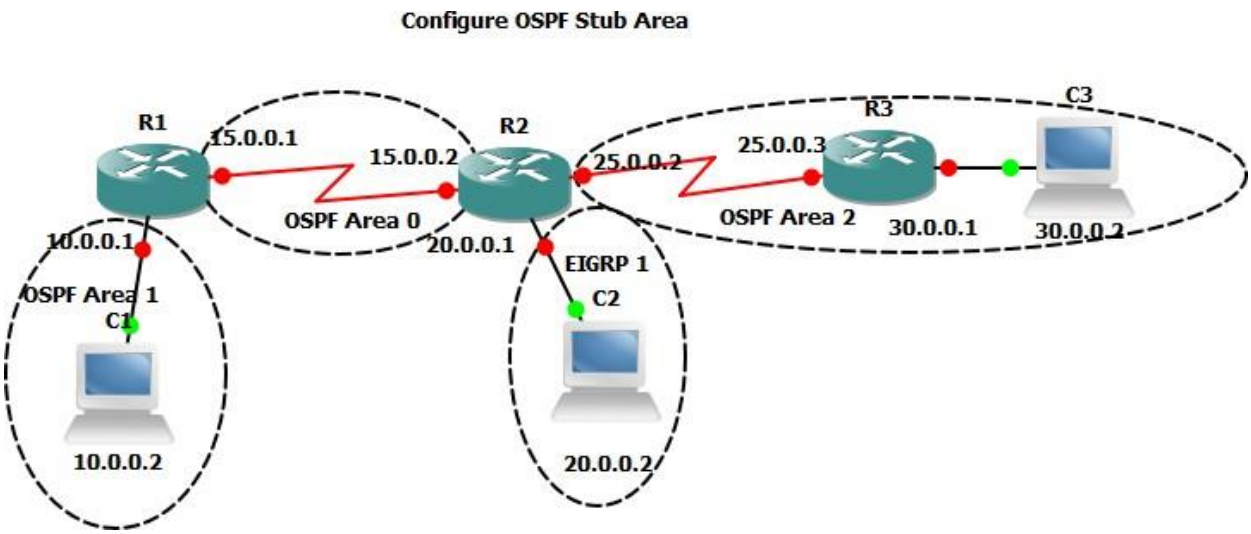
Lab 9

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 10

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 11

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 12

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.

BGP

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

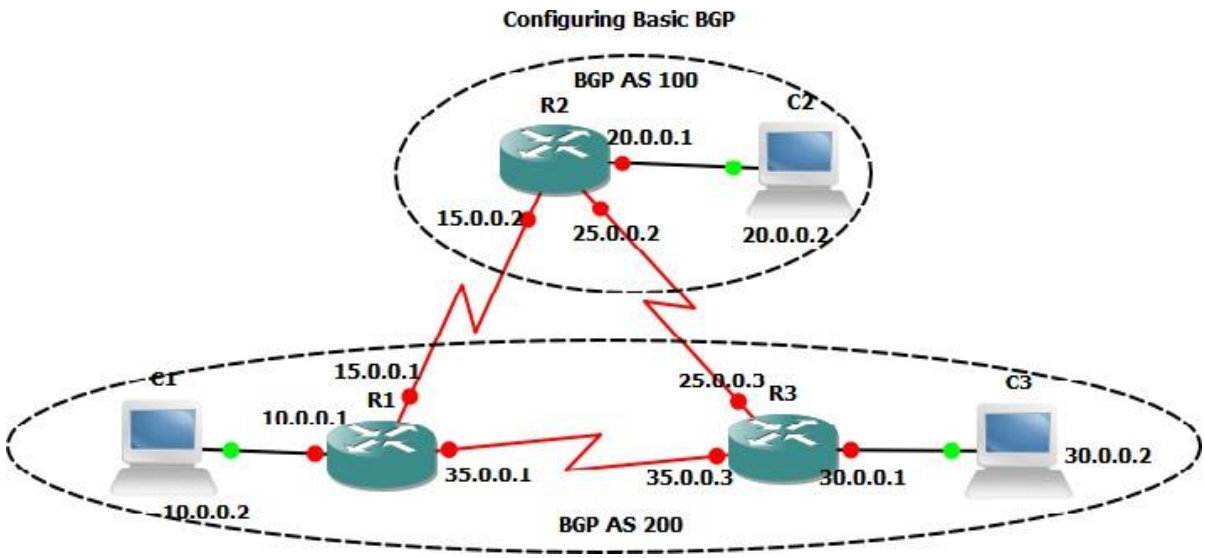
Lab 13

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.

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

```
!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.....

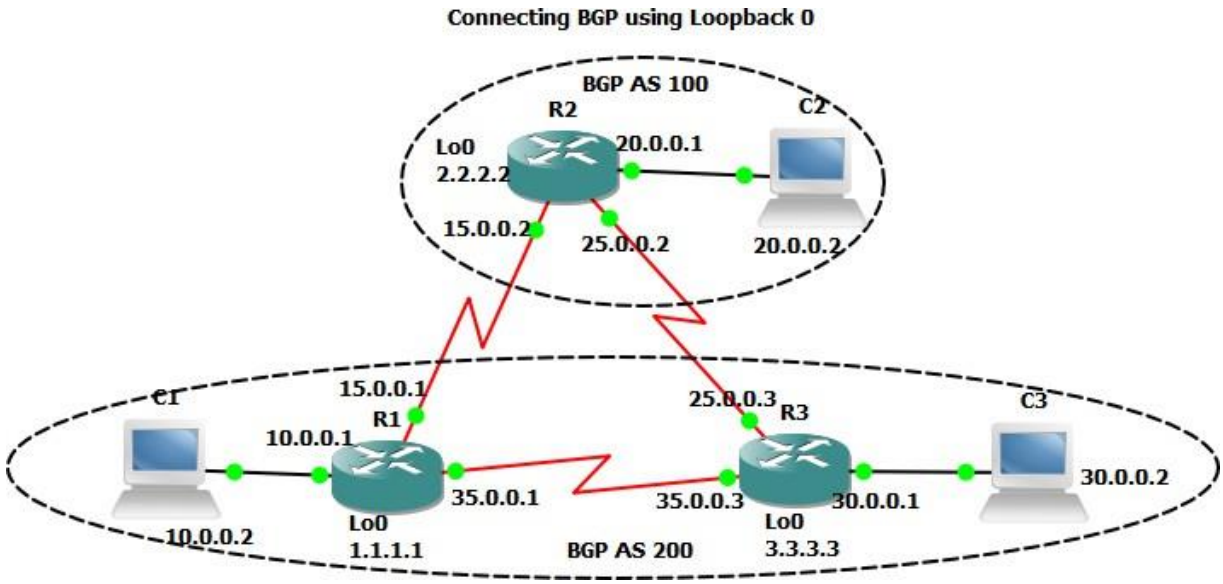
Lab 14

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....

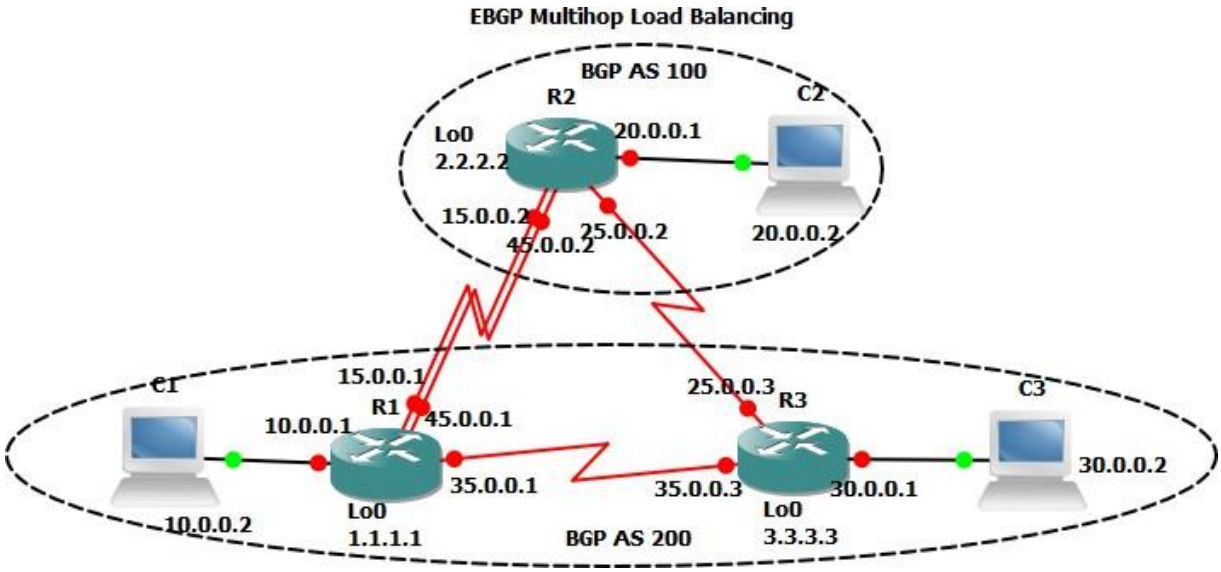
Lab 15

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#

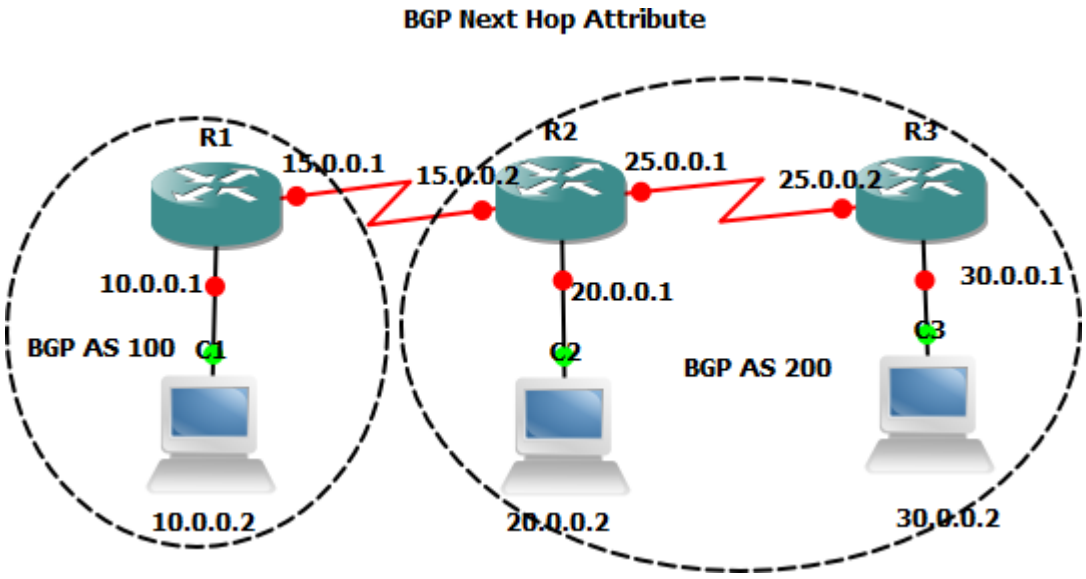
Lab 16

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.....

Switching

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

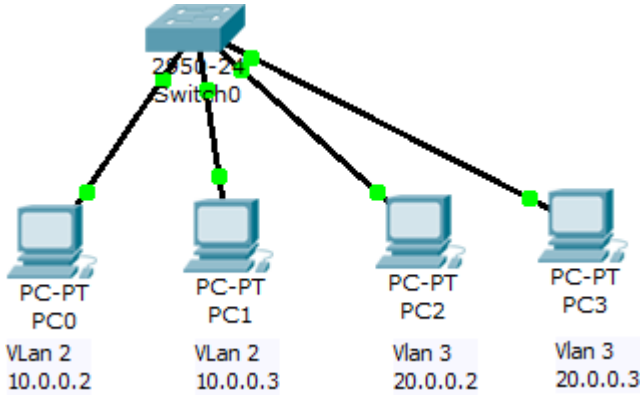
Lab 17

Basic Vlan Configuration

Objective:

The main goal of this lab is to allow customers to configure vlan on the switches, and to verify that communication can be achieved only between devices on the same vlan.

Diagram:



Preliminary Task:

Configure the network as shown in the figure, and assign ip addresses for PCs as described.

Task 1:

Configure vlan 2, and name it Red, then create vlan 3 and name it Blue. Configure interfaces fa0/1 & fa0/2 as mode access, and put them into vlan 2. Then configure fa0/3 & fa0/4 as mode access and put them into vlan 3.

!SW1

vlan 2

name red

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

vlan 3

name blue

exit

interface fa0/1

switchport mode access

interface fa0/2

switchport mode access

switchport access vlan 2

interface range fa0/3 - 4

switchport mode access

switchport access vlan 3

!Verification:

Switch#show vlan

VLAN Name Status Ports

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

1 default active Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/11, Fa0/12

Fa0/13, Fa0/14, Fa0/15, Fa0/16

Fa0/17, Fa0/18, Fa0/19, Fa0/20

Fa0/21, Fa0/22, Fa0/23, Fa0/24

2 red active Fa0/1, Fa0/2

3 blue active Fa0/3, Fa0/4

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

Ping should only work between devices belonging to the same Vlan...

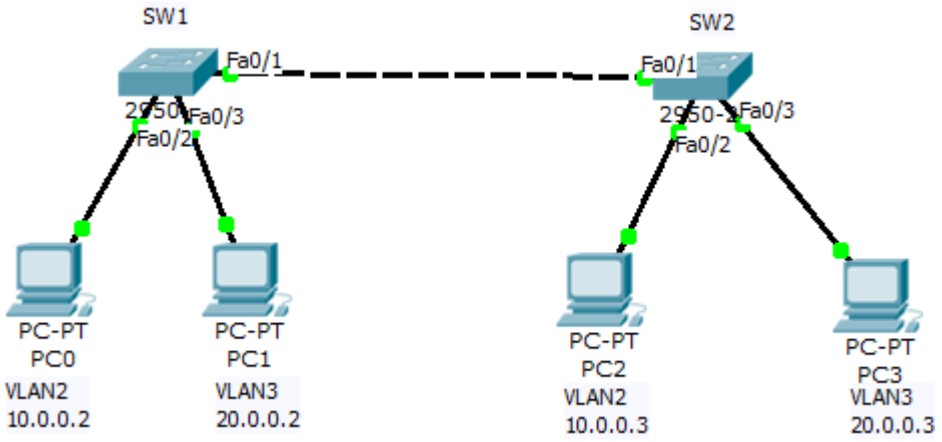
Lab 18

Trunking Between Two Switches

Objective:

The main goal of this lab is to configure a trunk link between two switches, and check the connectivity through the switches.

Diagram:



Preliminary Tasks:

Connect the network as show in the diagram, and assign the ip addresses to the computers as explained.

Task 1:

Configure vlan 2 & vlan 3 on both switches, and assign port fa0/2 to vlan 2 and port fa0/3 to vlan 3. Then check the connectivity between the PCs belonging to the same vlan.

!SW1/SW2

vlan 2

name red

exit

vlan 3

name blue

exit

interface fa0/2

switchport mode access

switchport access vlan 2

interface fa0/3

switchport mode access

switchport access vlan 3

Verification:

You can notice that the ping between PCs belonging to the same vlan is not working, and this is because, we are trying to ping between two PCs in Vlan 2 or 3, and the port between the two switches belong to vlan 1 (not trunk)

!SW1

SW1#show vlan

VLAN Name Status Ports

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

1 default active Fa0/1, Fa0/4, Fa0/5, Fa0/6

Fa0/7, Fa0/8, Fa0/9, Fa0/10

Fa0/11, Fa0/12, Fa0/13, Fa0/14

Fa0/15, Fa0/16, Fa0/17, Fa0/18

Fa0/19, Fa0/20, Fa0/21, Fa0/22

Fa0/23, Fa0/24

2 Red active Fa0/2

3 Blue active Fa0/3

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

Task 2:

Configure the link between switches to be trunk.

Use either one of the following commands

!SW1

interface fa0/1

switchport mode dynamic desirable

OR

interface fa0/1

switchport mode trunk

!Verification:

The ping between the two computers should be working fine, as the link between the two switches is configured as a trunk.

!SW1

SW1#show interface trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	auto	n-802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/1	1-1005

Port	Vlans allowed and active in management domain
Fa0/1	1,2,3

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1,2,3

Task 3:

Modify the trunk configuration to allow only vlan 3 on the link, and then check the connectivity between 10.0.0.2 & 10.0.0.3.

interface fa0/1

switchport trunk allowed vlan 3

!Verification:

We can notice the ping between 10.0.0.2 & 10.0.0.3 is not working and between 20.0.0.2 20.0.0.3 is working, because the only allowed vlan is vlan 3.

SW1#show interface trunk

Port Mode Encapsulation Status Native vlan

Fa0/1 auto n-802.1q trunking 1

Port Vlans allowed on trunk

Fa0/1 3

Port Vlans allowed and active in management domain

Fa0/1 3

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 3

SW1#

!Note: remove this command before moving to the next command

interface fa0/1

no switchport trunk allowed vlan 3

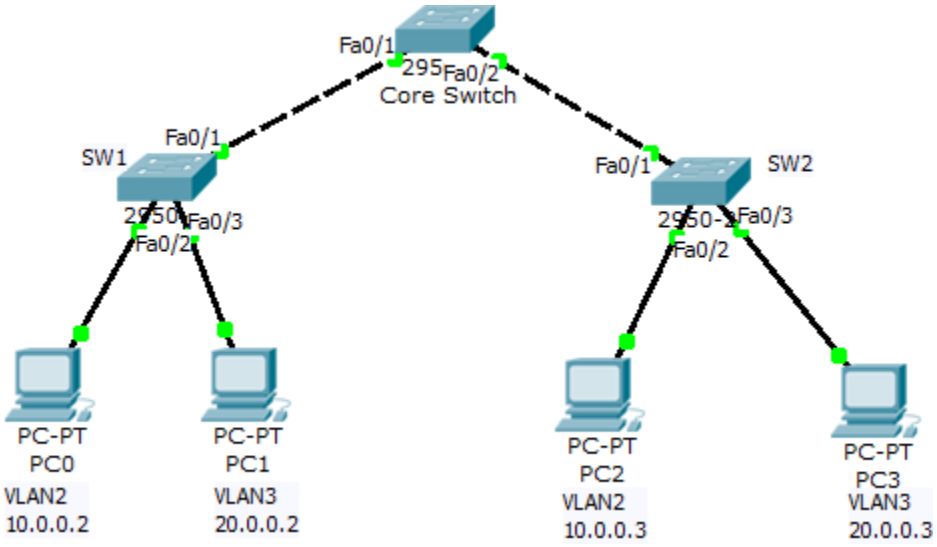
Lab 19

VLAN Trunking Case Study

Objective:

One of the most common mistakes in core switch real life configuration, we are going to explain how the issue could arise, and how we can resolve it.

Diagram:



Preliminary Task:

Based on lab 2, Connect SW1 to a core switch, then connect to SW2 as shown in the above figure.

Task 1:

Make sure the link between switches is trunk, and check the connectivity between 10.0.0.2 and 10.0.0.3

!SW1/SW2

interface fa0/1

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

switchport mode trunk

!Verification:

SW1#show interface trunk

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 1

Port Vlans allowed on trunk

Fa0/1 1-1005

Port Vlans allowed and active in management domain

Fa0/1 1,2,3

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 1,2,3

SW1#

SW2#show interface trunk

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 1

Port Vlans allowed on trunk

Fa0/1 1-1005

Port Vlans allowed and active in management domain

Fa0/1 1,2,3

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 1,2,3

SW2#

Although the trunk is up, and it is allowing the vlan 2 & 3, the ping between 10.0.0.2 & 10.0.0.3 won't work because the core switch is not configured with the vlans 2 and 3. So the core switch will not pass any traffic towards those two vlans, as they are not existing on the trunk link to SW1/SW2.

CORE-SWITCH#show interface trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	auto	n-802.1q	trunking	1
Fa0/2	auto	n-802.1q	trunking	1

Port Vlans allowed on trunk

Fa0/1 1-1005

Fa0/2 1-1005

Port Vlans allowed and active in management domain

Fa0/1 1

Fa0/2 1

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 1

Fa0/2 1

CORE-SWITCH#

Task 3:

Confiugre Vlan 2 & 3 on the core switch to allow the traffic on the trunk link of the core switch.

!CORE-SWITCH

vlan 2

exit

vlan 3

exit

!

!Verification:

The ping should be working fine between 10.0.0.2 & 10.0.0.3.....

CORE-SWITCH#show interface trunk

Port Mode Encapsulation Status Native vlan

Fa0/1	auto	n-802.1q	trunking	1
Fa0/2	auto	n-802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/1	1-1005
Fa0/2	1-1005

Port	Vlans allowed and active in management domain
Fa0/1	1,2,3
Fa0/2	1,2,3

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1,2,3
Fa0/2	1,2,3

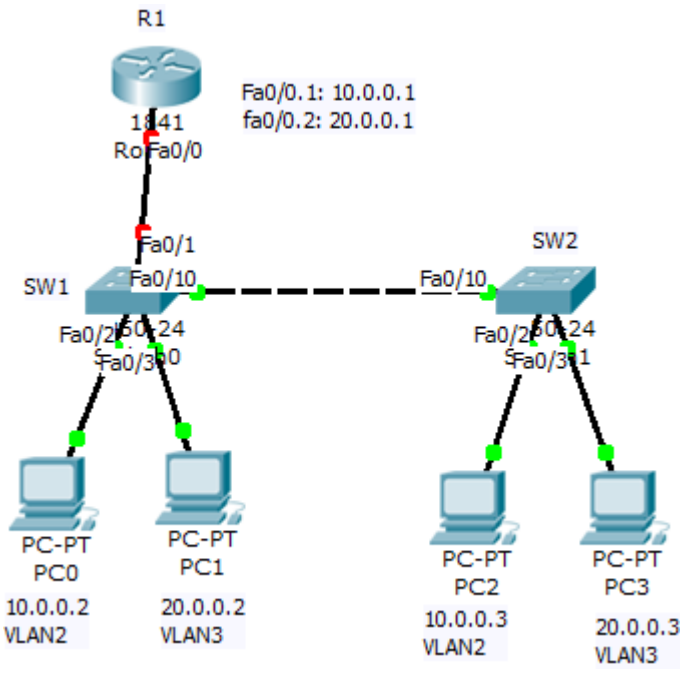
Lab 20

Router Configuration for Intervlan Routing

Objective:

The main target of this lab is to configure router to allow communication between different vlans.

Diagram:



Preliminary Task:

Connect the network as shown in the diagram, and assign ip addresses and default gateway for PCs as described in the figure.

Task 1:

- Configure vlan 2 & 3 in both switches
- Assign Ports Fa0/2 into vlan 2 & Fa0/3 into vlan 3 in both switches
- Configure port fa0/10 as a tunk

!SW1/SW2

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

vlan 2

exit

vlan 3

exit

interface fa0/2

switchport access vlan 2

interface fa0/3

switchport access vlan 3

interface fa0/10

switchport mode trunk

!Verification:

SW1#show vlan

VLAN Name Status Ports

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

1 default active Fa0/1, Fa0/4, Fa0/5, Fa0/6

Fa0/7, Fa0/8, Fa0/9, Fa0/11

Fa0/12, Fa0/13, Fa0/14, Fa0/15

Fa0/16, Fa0/17, Fa0/18, Fa0/19

Fa0/20, Fa0/21, Fa0/22, Fa0/23

Fa0/24

2 VLAN0002 active Fa0/2

3 VLAN0003 active Fa0/3

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

SW1#show interface trunk

Port Mode Encapsulation Status Native vlan

Fa0/10 on 802.1q trunking 1

Port Vlans allowed on trunk

Fa0/10 1-1005

Port Vlans allowed and active in management domain

Fa0/10 1,2,3

Port Vlans in spanning tree forwarding state and not pruned

Fa0/10 1,2,3

SW1#

At this stage, ping is working only between PCs belonging to the same vlan.

Task 2:

- Divide R1's Fa0/0 interface into two sub-interfaces to allow routing between different vlan, and assign them the ip addresses shown in the diagram.
- configure port fa0/1 in SW1 as a trunk.

!R1

interface fa0/0

no shutdown

interface fa0/0.1

encapsulation dot1q 2

ip address 10.0.0.1 255.0.0.0

interface fa0/0.2

encapsulation dot1q 3

ip address 20.0.0.1 255.0.0.0

!SW1

interface fa0/1

switchport mode trunk

!Verification:

R1#show ip interface brief

Interface IP-Address OK? Method Status Protocol

FastEthernet0/0 unassigned YES unset up up

FastEthernet0/0.1 10.0.0.1 YES manual up up

FastEthernet0/0.2 20.0.0.1 YES manual up up

FastEthernet0/1 unassigned YES unset administratively down down

Vlan1 unassigned YES unset administratively down down

R1#

SW1#show interface trunk

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 1

Fa0/10 on 802.1q trunking 1

Port Vlans allowed on trunk

Fa0/1 1-1005

Fa0/10 1-1005

Port Vlans allowed and active in management domain

Fa0/1 1,2,3

Fa0/10 1,2,3

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 1,2,3

Fa0/10 1,2,3

SW1#

Ping Between ALL PCs should be working fine....

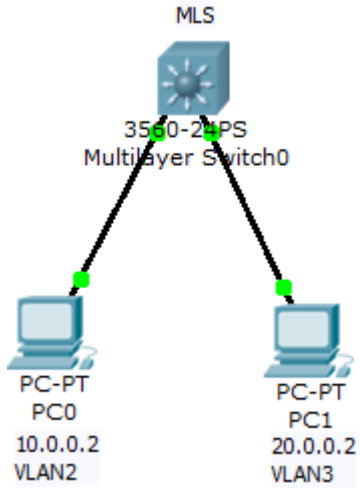
Lab 21

Multilayer Switch SVI Configuration for Intervlan Routing

Objective:

The main goal of this lab is to configure intervlan routing in Layer 3 switch through SVI configuration.

Diagram:



Preliminary Task:

Connect the network as shown in the diagram (PC0 connected to port Fa0/1 & PC1 connected to port Fa0/2). Then assign ip addresses to the computers as described above.

Task 1:

Configure Vlan 2 & Vlan 3 in the switch, and assign port fa0/1 to Vlan 2, then assign port fa0/2 to Vlan 3.

!MLS

vlan 2

exit

vlan 3

exit

interface fa0/1

switchport access vlan 2

interface fa0/2

switchport access vlan 3

!Verification:

MLS#show vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6
			Fa0/7, Fa0/8, Fa0/9, Fa0/10
			Fa0/11, Fa0/12, Fa0/13, Fa0/14
			Fa0/15, Fa0/16, Fa0/17, Fa0/18
			Fa0/19, Fa0/20, Fa0/21, Fa0/22
			Fa0/23, Fa0/24, Gig0/1, Gig0/2
2	VLAN0002	active	Fa0/1
3	VLAN0003	active	Fa0/2

Task 2:

Configure Vlan 2 SVI to have the ip address 10.0.0.1 & Vlan 3 to have 20.0.0.1 and enable IP routing on the MLS.

!MLS

interface vlan 2

no shut

ip address 10.0.0.1 255.0.0.0

interface vlan 3

no shut

ip address 20.0.0.1 255.0.0.0

exit

ip routing

!Verification:

MLS#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	up	up
FastEthernet0/3	unassigned	YES	unset	down	down

FastEthernet0/4	unassigned	YES unset	down	down
FastEthernet0/5	unassigned	YES unset	down	down
FastEthernet0/6	unassigned	YES unset	down	down
FastEthernet0/7	unassigned	YES unset	down	down
FastEthernet0/8	unassigned	YES unset	down	down
FastEthernet0/9	unassigned	YES unset	down	down
FastEthernet0/10	unassigned	YES unset	down	down
FastEthernet0/11	unassigned	YES unset	down	down
FastEthernet0/12	unassigned	YES unset	down	down
FastEthernet0/13	unassigned	YES unset	down	down
FastEthernet0/14	unassigned	YES unset	down	down

FastEthernet0/15 unassigned YES unset down down

FastEthernet0/16 unassigned YES unset down down

FastEthernet0/17 unassigned YES unset down down

FastEthernet0/18 unassigned YES unset down down

FastEthernet0/19 unassigned YES unset down down

FastEthernet0/20 unassigned YES unset down down

FastEthernet0/21 unassigned YES unset down down

FastEthernet0/22 unassigned YES unset down down

FastEthernet0/23 unassigned YES unset down down

FastEthernet0/24 unassigned YES unset down down

GigabitEthernet0/1 unassigned YES unset down down

GigabitEthernet0/2 unassigned YES unset down down

Vlan1 unassigned YES unset administratively down down

Vlan2 10.0.0.1 YES manual up up

Vlan3 20.0.0.1 YES manual up up

MLS#show ip route

C 10.0.0.0/8 is directly connected, Vlan2

C 20.0.0.0/8 is directly connected, Vlan3

MLS#

Ping Should be working between PCs....

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

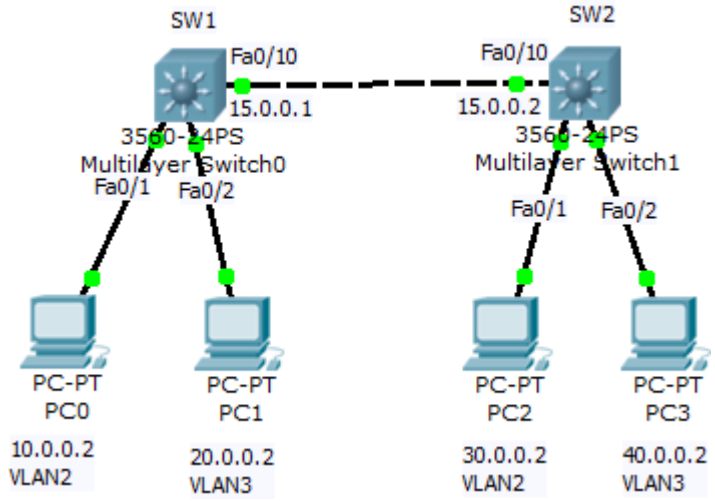
Lab 22

Routed Port Configuration on MLS & Routing between two MLSs

Objective:

The main goal of this lab is to configure a routed port on MLS to allow layer 3 communication between two MLS and their connected PCs.

Diagram:



Preliminary Task:

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

Task 1:

- Configure vlan 2 & vlan 3 on both switches.
- Assign Port fa0/1 to vlan 2 and port fa0/2 to vlan 3 on both switches.
- Assign ip addresses to vlan interfaces on both switches (vlan 2,SW1 -> 10.0.0.1, vlan 3,SW1-> 20.0.0.1, vlan 2,SW2->30.0.0.1, vlan 3,sw2->40.0.0.1), then enable IP routing.

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

```
!SW1/SW2
vlan 2
exit
vlan 3
exit
interface fa0/1
switchport access vlan 2
interface fa0/2
switchport access vlan 3
exit
ip routing

!SW1
interface vlan 2
no shutdown
ip address 10.0.0.1 255.0.0.0
interface vlan 3
no shutdown
ip address 20.0.0.1 255.0.0.0

!SW2
interface vlan 2
```

no shutdown

ip address 30.0.0.1 255.0.0.0

interface vlan 3

no shutdown

ip address 40.0.0.1 255.0.0.0

!Verification:

SW1#show vlan

VLAN Name Status Ports

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

1 default active Fa0/3, Fa0/4, Fa0/5, Fa0/6

Fa0/7, Fa0/8, Fa0/9, Fa0/10

Fa0/11, Fa0/12, Fa0/13, Fa0/14

Fa0/15, Fa0/16, Fa0/17, Fa0/18

Fa0/19, Fa0/20, Fa0/21, Fa0/22

Fa0/23, Fa0/24, Gig0/1, Gig0/2

2 VLAN0002 active Fa0/1

3 VLAN0003 active Fa0/2

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

SW1#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	up	up
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	down	down
FastEthernet0/6	unassigned	YES	unset	down	down
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down

FastEthernet0/10	unassigned	YES unset	up	up
FastEthernet0/11	unassigned	YES unset	down	down
FastEthernet0/12	unassigned	YES unset	down	down
FastEthernet0/13	unassigned	YES unset	down	down
FastEthernet0/14	unassigned	YES unset	down	down
FastEthernet0/15	unassigned	YES unset	down	down
FastEthernet0/16	unassigned	YES unset	down	down
FastEthernet0/17	unassigned	YES unset	down	down
FastEthernet0/18	unassigned	YES unset	down	down
FastEthernet0/19	unassigned	YES unset	down	down
FastEthernet0/20	unassigned	YES unset	down	down

FastEthernet0/21 unassigned YES unset down down

FastEthernet0/22 unassigned YES unset down down

FastEthernet0/23 unassigned YES unset down down

FastEthernet0/24 unassigned YES unset down down

GigabitEthernet0/1 unassigned YES unset down down

GigabitEthernet0/2 unassigned YES unset down down

Vlan1 unassigned YES unset administratively down down

Vlan2 10.0.0.1 YES manual up up

Vlan3 20.0.0.1 YES manual up up

Task 2:

Configure the port connecting the switches as a routed port and assign it the ip address shown in the diagram, then configure a routing protocol to allow network advertisements between the MLSs.

!SW1

interface fa0/10

no switchport

ip address 15.0.0.1 255.0.0.0

router rip

version 2

network 10.0.0.0

network 20.0.0.0

network 15.0.0.0

!SW2

interface fa0/10

no switchport

ip address 15.0.0.2 255.0.0.0

router rip

version 2

network 30.0.0.0

network 40.0.0.0

network 15.0.0.0

!Verification:

SW2#show ip route

R 10.0.0.0/8 [120/1] via 15.0.0.1, 00:00:24, FastEthernet0/10

C 15.0.0.0/8 is directly connected, FastEthernet0/10

R 20.0.0.0/8 [120/1] via 15.0.0.1, 00:00:24, FastEthernet0/10

C 30.0.0.0/8 is directly connected, Vlan2

C 40.0.0.0/8 is directly connected, Vlan3

SW2#

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

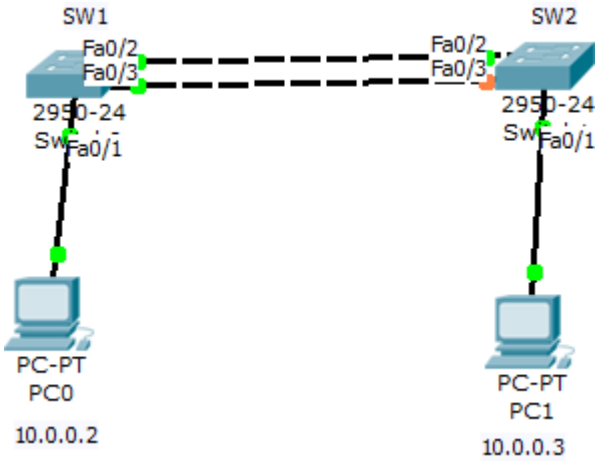
Lab 23

Layer 2 Ether-channel Configuration (PAGP)

Objective:

The main target of this lab is to bundle two 100 Mbps links to one layer-2 200 Mbps connection through ether-channel configuration using PAGP protocol.

Diagram:



Preliminary Tasks:

Connect the network as shown in the diagram, and configure the PCs with the described IP addresses. The PCs should be belonging to the default vlan.

Task 1:

Configure ether-channel on SW1 & SW2 using cisco bundling protocol (PAGP), and make sure that SW1 is the one that starts the negotiation.

!SW1

interface range fa0/2 - 3

channel-group 1 mode desirable

!SW2

interface range fa0/2 - 3

channel-group 1 mode auto

!Verification

SW1#show etherchannel summary

Flags: D - down P - in port-channel

I - stand-alone s - suspended

H - Hot-standby (LACP only)

R - Layer3 S - Layer2

U - in use f - failed to allocate aggregator

u - unsuitable for bundling

w - waiting to be aggregated

d - default port

Number of channel-groups in use: 1

Number of aggregators: 1

Group Port-channel Protocol Ports

----+---------+-------------+-------------------------------

1 Po1(SU) PAgP Fa0/2(P) Fa0/3(P)

SW1#show vlan

VLAN Name Status Ports

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

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/11, Fa0/12

Fa0/13, Fa0/14, Fa0/15, Fa0/16

Fa0/17, Fa0/18, Fa0/19, Fa0/20

Fa0/21, Fa0/22, Fa0/23, Fa0/24

Po1

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

Task 2:

As we can notice that the etherchannel got established, but the port-channel is automatically assigned to vlan 1. So configure the port-channel to be trunk.

!SW1

interface po1

switchport mode trunk

!Verification:

SW1#show interface trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/2	on	802.1q	trunking	1
Fa0/3	on	802.1q	trunking	1
Po1	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/2	1-1005
Fa0/3	1-1005
Po1	1-1005

Port	Vlans allowed and active in management domain
Fa0/2	1
Fa0/3	1
Po1	1

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/2	1
Fa0/3	1
Po1	1

SW1#

Ping should be working between PCs....

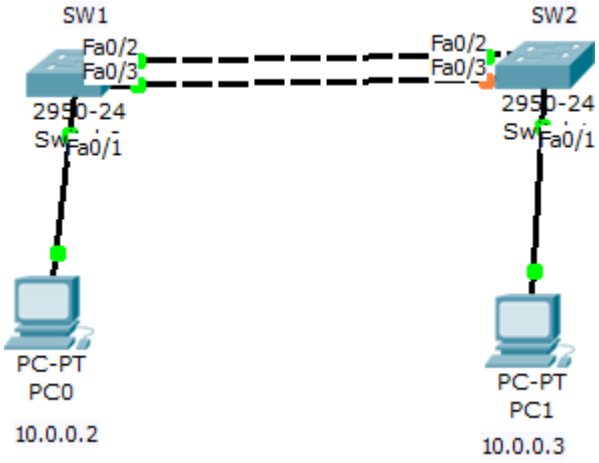
Lab 24

Layer 2 Ether-channel Configuration (LACP)

Objective:

The main target of this lab is to bundle two 100 Mbps links to one layer-2 200 Mbps connection through ether-channel configuration using standard LACP protocol.

Diagram:



Preliminary Tasks:

Connect the network as shown in the diagram, and configure the PCs with the described IP addresses. The PCs should be belonging to the default vlan.

Task 1:

Configure ether-channel on SW1 & SW2 using standard bundling protocol (LACP), and make sure that SW1 is the one that starts the negotiation.

!SW1

interface range fa0/2 - 3

channel-group 1 mode active

!SW2

interface range fa0/2 - 3

channel-group 1 mode passive

!Verification:

sw1#show etherchannel summary

Flags: D - down P - in port-channel

I - stand-alone s - suspended

H - Hot-standby (LACP only)

R - Layer3 S - Layer2

U - in use f - failed to allocate aggregator

u - unsuitable for bundling

w - waiting to be aggregated

d - default port

Number of channel-groups in use: 1

Number of aggregators: 1

Group Port-channel Protocol Ports

----+---------+-----------+----------

```
1      Po1(SU)          LACP   Fa0/2(P) Fa0/3(P)

sw1#

sw1#show vlan


VLAN Name                              Status    Ports

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

1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2, Po1
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Task 2:

As we can notice that the etherchannel got established, but the port-channel is automatically assigned to vlan 1. So configure the port-channel to be trunk.

!SW1

interface po1

switchport mode trunk

!Verification:

SW1#show interface trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/2	on	802.1q	trunking	1
Fa0/3	on	802.1q	trunking	1
Po1	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/2	1-1005
Fa0/3	1-1005
Po1	1-1005

Port	Vlans allowed and active in management domain
Fa0/2	1
Fa0/3	1
Po1	1

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/2	1
Fa0/3	1
Po1	1

Ping should be working between PCs....

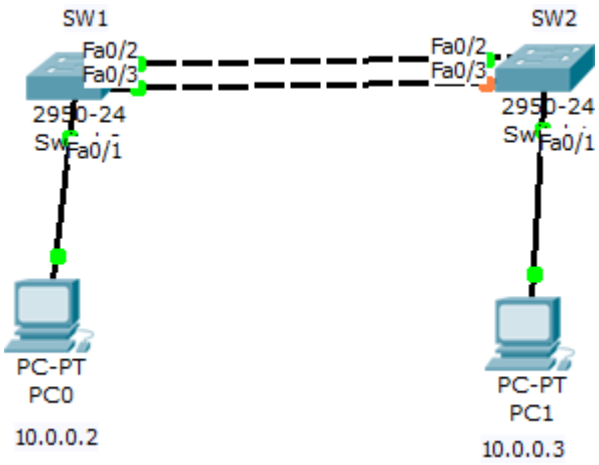
Lab 25

Manual Layer 2 Ether-channel Configuration

Objective:

The main target of this lab is to manual bundle two 100 Mbps links to one layer-2 200 Mbps connection through ether-channel manual configuration.

Diagram:



Preliminary Tasks:

Connect the network as shown in the diagram, and configure the PCs with the described IP addresses. The PCs should be belonging to the default vlan.

Task 1:

Manual configure ether-channel on SW1 & SW2.

!SW1

interface range fa0/2 - 3

channel-group 1 mode on

!SW2

interface range fa0/2 - 3

channel-group 1 mode on

!Verification:

SW1#show etherchannel summary

Number of channel-groups in use: 1

Number of aggregators: 1

Group Port-channel Protocol Ports

----+---------+-----------+-------------------------------

1 Po1(SU) - Fa0/2(P) Fa0/3(P)

sw1#

SW1#show vlan

VLAN Name Status Ports

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

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/11, Fa0/12

Fa0/13, Fa0/14, Fa0/15, Fa0/16

Fa0/17, Fa0/18, Fa0/19, Fa0/20

Fa0/21, Fa0/22, Fa0/23, Fa0/24

Gig0/1, Gig0/2, Po1

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

Task 2:

As we can notice that the etherchannel got established, but the port-channel is automatically assigned to vlan 1. So configure the port-channel to be trunk.

!SW1

interface po1

switchport mode trunk

!Verification:

SW1#show interface trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/2	on	802.1q	trunking	1
Fa0/3	on	802.1q	trunking	1
Po1	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/2	1-1005
Fa0/3	1-1005

Po1 1-1005

Port Vlans allowed and active in management domain

Fa0/2 1

Fa0/3 1

Po1 1

Port Vlans in spanning tree forwarding state and not pruned

Fa0/2 1

Fa0/3 1

Po1 1

SW1#

Ping should be working between PCs....

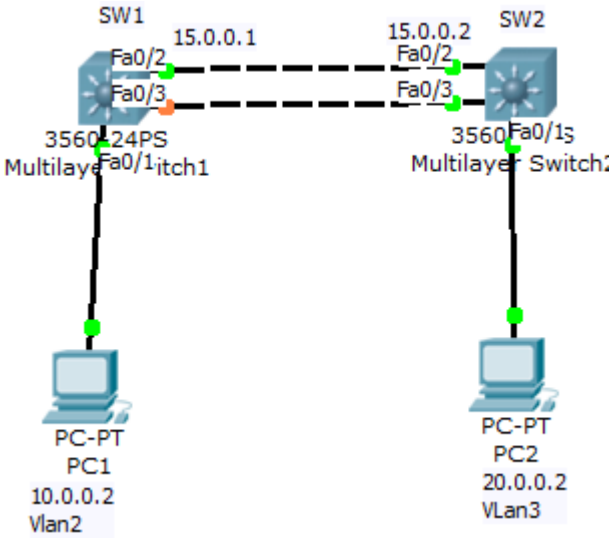
Lab 26

Layer 3 Ether-Channel Configuration

Objective:

The main goal of this lab is to configure a Layer 3 ether-channel between two layer 3 switches, and to verify the connectivity over the two switches.

Diagram:



Preliminary Task:

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

Task 1:

- On Both Switches, configure vlan 2 & vlan 3, and assign interface fa0/1 to vlan 2 on SW1, and interface fa0/1 to vlan 3 on SW2
- configure ip address vlan 2 SVI to be 10.0.0.1 on SW1 & vlan 3 SVI to be 20.0.0.1

!SW1/SW2

vlan 2

exit

vlan 3

!SW1

interface fa0/1

switchport access vlan 2

!

interface vlan 2

no shutdown

ip address 10.0.0.1 255.0.0.0

!

!SW2

interface fa0/1

switchport access vlan 3

!

interface vlan 3

no shutdown

ip address 20.0.0.1 255.0.0.0

!Verification:

SW1#show vlan

```
VLAN Name                      Status    Ports
---- -------------------------- ------ -------------------------------
1    default                   active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                         Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                         Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                         Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                         Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                         Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                         Gig0/2
2    VLAN0002                  active    Fa0/1
3    VLAN0003                  active
1002 fddi-default              act/unsup
1003 token-ring-default        act/unsup
1004 fddinet-default           act/unsup
1005 trnet-default             act/unsup


 SW1#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/1        unassigned      YES unset  up                    up

FastEthernet0/2        unassigned      YES unset  up                    up
```

FastEthernet0/3 unassigned YES unset up up

FastEthernet0/4 unassigned YES unset down down

FastEthernet0/5 unassigned YES unset down down

FastEthernet0/6 unassigned YES unset down down

FastEthernet0/7 unassigned YES unset down down

FastEthernet0/8 unassigned YES unset down down

FastEthernet0/9 unassigned YES unset down down

FastEthernet0/10 unassigned YES unset down down

FastEthernet0/11 unassigned YES unset down down

FastEthernet0/12 unassigned YES unset down down

FastEthernet0/13 unassigned YES unset down down

FastEthernet0/14	unassigned	YES unset	down	down
FastEthernet0/15	unassigned	YES unset	down	down
FastEthernet0/16	unassigned	YES unset	down	down
FastEthernet0/17	unassigned	YES unset	down	down
FastEthernet0/18	unassigned	YES unset	down	down
FastEthernet0/19	unassigned	YES unset	down	down
FastEthernet0/20	unassigned	YES unset	down	down
FastEthernet0/21	unassigned	YES unset	down	down
FastEthernet0/22	unassigned	YES unset	down	down
FastEthernet0/23	unassigned	YES unset	down	down
FastEthernet0/24	unassigned	YES unset	down	down

GigabitEthernet0/1 unassigned YES unset down down

GigabitEthernet0/2 unassigned YES unset down down

Vlan1 unassigned YES unset administratively down down

Vlan2 10.0.0.1 YES manual up up

Task 2:

- Manual configure ether-channel on ports fa0/2 & fa0/3 on Both Switches
- convert the port-channel port into a routed port
- Assign ip address 15.0.0.1/2 for the port-channel interfaces.

!SW1

interface fa0/2 - 3

channel-group 1 mode on

exit

interface po1

no switchport

ip address 15.0.0.1 255.0.0.0

!SW2

interface fa0/2 - 3

channel-group 1 mode on

exit

interface po1

no switchport

ip address 15.0.0.2 255.0.0.0

!Verification:

SW1#show etherchannel summary

Flags: D - down P - in port-channel

I - stand-alone s - suspended

H - Hot-standby (LACP only)

R - Layer3 S - Layer2

U - in use f - failed to allocate aggregator

u - unsuitable for bundling

w - waiting to be aggregated

d - default port

Number of channel-groups in use: 1

Number of aggregators: 1

Group Port-channel Protocol Ports

----+---------+-------------+------------------------------

1 Po1(RU) - Fa0/2(P) Fa0/3(P)

SW1#

SW1#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	up	up
FastEthernet0/3	unassigned	YES	unset	up	up
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	down	down
FastEthernet0/6	unassigned	YES	unset	down	down
FastEthernet0/7	unassigned	YES	unset	down	down

FastEthernet0/8	unassigned	YES unset	down	down
FastEthernet0/9	unassigned	YES unset	down	down
FastEthernet0/10	unassigned	YES unset	down	down
FastEthernet0/11	unassigned	YES unset	down	down
FastEthernet0/12	unassigned	YES unset	down	down
FastEthernet0/13	unassigned	YES unset	down	down
FastEthernet0/14	unassigned	YES unset	down	down
FastEthernet0/15	unassigned	YES unset	down	down
FastEthernet0/16	unassigned	YES unset	down	down
FastEthernet0/17	unassigned	YES unset	down	down
FastEthernet0/18	unassigned	YES unset	down	down

FastEthernet0/19 unassigned YES unset down down

FastEthernet0/20 unassigned YES unset down down

FastEthernet0/21 unassigned YES unset down down

FastEthernet0/22 unassigned YES unset down down

FastEthernet0/23 unassigned YES unset down down

FastEthernet0/24 unassigned YES unset down down

GigabitEthernet0/1 unassigned YES unset down down

GigabitEthernet0/2 unassigned YES unset down down

Vlan1 unassigned YES unset administratively down down

Vlan2 10.0.0.1 YES manual up up

Port-channel 1 15.0.0.1 YES manual up up

Task 3:

Enable IP routing on both switches, and advertise all connected networks through RIP version 2

!SW1

ip routing

router rip

version 2

network 10.0.0.0

network 15.0.0.0

!SW2

ip routing

router rip

version 2

network 20.0.0.0

network 15.0.0.0

!Verification:

SW1#show ip route

Gateway of last resort is not set

C 10.0.0.0/8 is directly connected, Vlan2

C 15.0.0.0/8 is directly connected, Port-channel 1

R 20.0.0.0/8 [120/1] via 15.0.0.2, 00:00:09, Port-channel 1

SW1#

Ping should be working fine between PCs....

Lab 27

Basic Spanning-tree Configuration and Customization

Objective:

The main objective of this goal is to practice the basic modification commands of the spanning-tree, and to check its effect on the topology of the spanning-tree.

Diagram:

Preliminary Task:

Connect the network as shown in the diagram, and configure the link as Tunk

!SW1/SW2

interface range fa1/0 - 1

switchport mode trunk

Task 1:

Verify the spanning-tree status, and identify the root switch, root port, and the designated ports for vlan 1.

SW1#show spanning-tree vlan 1 brief

VLAN1

Spanning tree enabled protocol ieee

Root ID Priority 32768

Address c403.0778.0000

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768

Address c403.0778.0000

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface Name	Port ID	Prio	Cost	Sts	Cost	Designated Bridge ID	Port ID
FastEthernet1/0	128.41	128	19	FWD	0	32768 c403.0778.0000	128.41
FastEthernet1/1	128.42	128	19	FWD	0	32768 c403.0778.0000	128.42

So SW1 is the root Bridge, and all its ports are designated ports.

SW2#show spanning-tree vlan 1 brief

VLAN1

Spanning tree enabled protocol ieee

Root ID Priority 32768

Address c403.0778.0000

Cost 19

Port 41 (FastEthernet1/0)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768

Address c404.0778.0000

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface Name	Port ID	Prio	Cost	Sts	Cost	Designated Bridge ID	Port ID
FastEthernet1/0	128.41	128	19	FWD	0	32768 c403.0778.0000	128.41
FastEthernet1/1	128.42	128	19	BLK	0	32768 c403.0778.0000	128.42

And SW2's port Fa1/0 is the root port.

Task 2:

Modify the spanning-tree topology so that SW2 is to be the root switch.

!SW2

spanning-tree vlan 1 priority 0

OR

spanning-tree vlan 1 root primary

!Verification

SW2#show spanning-tree vlan 1 brief

VLAN1

Spanning tree enabled protocol ieee

Root ID Priority 0

Address c404.0778.0000

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 0

Address c404.0778.0000

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface	Designated				
Name	Port ID Prio Cost	Sts Cost	Bridge ID	Port ID	
----------	----------	---	----------	----------	

FastEthernet1/0 128.41 128 19 FWD 0 0 c404.0778.0000 128.41

FastEthernet1/1 128.42 128 19 FWD 0 0 c404.0778.0000 128.42

SW1#show spanning-tree vlan 1 brief

VLAN1

Spanning tree enabled protocol ieee

Root ID Priority 0

Address c404.0778.0000

Cost 19

Port 41 (FastEthernet1/0)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768

Address c403.0778.0000

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface Designated

Name Port ID Prio Cost Sts Cost Bridge ID Port ID

FastEthernet1/0 128.41 128 19 FWD 0 0 c404.0778.0000 128.41

FastEthernet1/1 128.42 128 19 BLK 0 0 c404.0778.0000 128.42

Task 3:

Make SW1's Fa1/1 is the root port by only modifying SW2 configuration.

!SW2

interface fa1/1

spanning-tree vlan 1 port-priority 0

!Verification:

SW1#show spanning-tree vlan 1 brief

VLAN1

Spanning tree enabled protocol ieee

Root ID Priority 0

Address c404.0778.0000

Cost 19

Port 42 (FastEthernet1/1)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768

Address c403.0778.0000

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface Name	Port ID	Prio	Cost	Sts	Cost	Bridge ID	Port ID
FastEthernet1/0	128.41	128	19	BLK	0	0 c404.0778.0000	128.41
FastEthernet1/1	128.42	128	19	FWD	0	0 c404.0778.0000	0.42

Task 4:

Return Root Port Status back to SW1's Fa1/0 port by doing modification only in SW1

!SW1

interface fa1/0

spanning-tree vlan 1 cost 1

!Verification:

SW1#show spanning-tree vlan 1 brief

VLAN1

Spanning tree enabled protocol ieee

Root ID Priority 0

Address c404.0778.0000

Cost 1

Port 41 (FastEthernet1/0)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768

Address c403.0778.0000

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface Name	Port ID	Prio	Cost	Sts	Cost	Designated Bridge ID	Port ID
FastEthernet1/0	128.41	128	1	FWD	0	0 c404.0778.0000	128.41
FastEthernet1/1	128.42	128	19	BLK	0	0 c404.0778.0000	0.42

Task 5:

Configure Vlan 2 on Both Switches, and make sure that SW1 is the root switch for vlan 2 & SW2 is the root switch for vlan 1.

!SW1/SW2

vlan 2

exit

!SW1

spanning-tree vlan 2 priority 0

!SW2

spanning-tree vlan 1 priority 0

!Verification:

SW1#show spanning-tree vlan 2 brief

VLAN2

Spanning tree enabled protocol ieee

Root ID Priority 0

Address c403.0778.0001

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 0

Address c403.0778.0001

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface Name	Port ID	Prio	Cost	Sts	Cost	Designated Bridge ID	Port ID
FastEthernet1/0	128.41	128	19	FWD	0	0 c403.0778.0001	128.41

FastEthernet1/1 128.42 128 19 FWD 0 0 c403.0778.0001 128.42

SW2#show spanning-tree vlan 1 brief

VLAN1

Spanning tree enabled protocol ieee

Root ID Priority 0

Address c404.0778.0000

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 0

Address c404.0778.0000

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface					Designated	
Name	Port ID	Prio	Cost	Sts	Cost	Bridge ID	Port ID
FastEthernet1/0	128.41	128	19	FWD	0	0 c404.0778.0000	128.41
FastEthernet1/1	0.42	0	19	FWD	0	0 c404.0778.0000	0.42

Note: By using PVST, All ports are forwarding but for certain Vlans

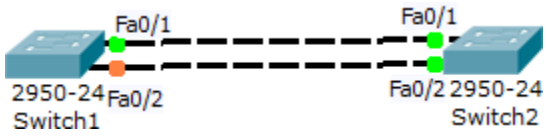
Lab 28

Rapid Spanning-tree Protocol

Objective:

The main goal of this lab, is to compare the transition states between traditional STP and the rapid STP.

Diagram:



Preliminary Task:

Connect the network as shown in the diagram, and configure port Fa0/1 & Fa0/2 as trunk links on Both Switches.

!SW1/SW2

interface range fa0/1 - 2

switchport mode trunk

Task 1:

Verify the spanning tree topology and then shutdown the root port in the non root switch to see the convergence in the traditional STP.

SW1#show spanning-tree vlan 1

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 0090.2BB0.16C7

Cost 19

Port 1(FastEthernet0/1)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 00D0.BC25.8BE7

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

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

Fa0/2 Altn BLK 19 128.2 P2p

Fa0/1 Root FWD 19 128.1 P2p

SW1#

Then:

!SW1

interface fa0/1

shutdown

!Verification:

SW1#show spanning-tree vlan 1

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 0090.2BB0.16C7

Cost 19

Port 2(FastEthernet0/2)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 00D0.BC25.8BE7

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

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

Fa0/2 Root LSN 19 128.2 P2p

SW1#show spanning-tree vlan 1

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 0090.2BB0.16C7

```
        Cost      19
        Port      2(FastEthernet0/2)
        Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
        Address     00D0.BC25.8BE7
        Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
        Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Root LRN 19        128.2    P2p

SW1#show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
        Address     0090.2BB0.16C7
        Cost      19
        Port      2(FastEthernet0/2)
        Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

Bridge ID Priority   32769 (priority 32768 sys-id-ext 1)

Address   00D0.BC25.8BE7

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/2	Root	FWD	19	128.2	P2p

!We can notice that in traditional spanning-tree, we went through Listening, Learning & Forwarding.

Task 2:

Configure !SW1 & SW2 to use rapid STP, and to no shutdown the interface on Fa0/2, and check the convergence on RSTP.

!SW1/SW2

spanning-tree mode rapid-pvst

!SW1

interface fa0/1

no shutdown

!Verification:

SW1#show spanning-tree vlan 1

VLAN0001

Spanning tree enabled protocol rstp

Root ID Priority 32769

Address 0090.2BB0.16C7

Cost 19

Port 1(FastEthernet0/1)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 00D0.BC25.8BE7

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/2	Altn	BLK	19	128.2	P2p
Fa0/1	Root	FWD	19	128.1	P2p

!We can notice that the convergence went immediately, because port Fa0/1 was the alternative port of the root port in the RSTP topology.

Task 3:

Configure port fa0/3 as mode access, and configure portfast default on SW1, then connect PC0 to port fa0/3, and check the transition to forwarding on port fa0/3.

!SW1

spanning-tree portfast default

interface fa0/3

switchport mode access

!Verification:

SW1#sh spanning-tree vlan 1

VLAN0001

Spanning tree enabled protocol rstp

Root ID Priority 32769

Address 0090.2BB0.16C7

Cost 19

Port 1(FastEthernet0/1)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 00D0.BC25.8BE7

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/2	Altn	BLK	19	128.2	P2p
Fa0/3	Desg	FWD	19	128.3	P2p
Fa0/1	Root	FWD	19	128.1	P2p

!We can notice that port fa0/3 has gone immediately to the forwarding state, after configuring portfast default.

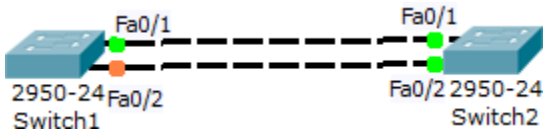
Lab 29

MST

Objective:

The main goal of this lab is configure MST on SW1 & SW2, and to set multiple vlans for one stp instance.

Diagram:



Preliminary Task:

Connect the network as shown in the diagram, and configure vlan 2 - 10 on both switches, and also configure port fa0/1 & fa0/2 as trunks.

!SW1/SW2

vlan 2 - 10

exit

interface range fa0/1 - 2

switchport mode trunk

Task 1:

- Configure spanning tree mode mst for both switches.
- Instance 1 should include the odd vlans
- Instance 2 should include the even vlans
- SW1 should be the root switch for instance 1
- SW2 should be the root switch for instance 2

- mst name should be cisco
- mst revision should be 1

!SW1

spanning-tree mode mst

spanning-tree mst configuration

name cisco

revision 1

instance 1 vlan 1,3,5,7,9

instance 2 vlan 2,4,6,8,10

exit

spanning-tree mst 1 root primary

spanning-tree mst 2 root secondary

!SW2

spanning-tree mode mst

spanning-tree mst configuration

name cisco

revision 1

instance 1 vlan 1,3,5,7,9

instance 2 vlan 2,4,6,8,10

exit

spanning-tree mst 2 root primary

spanning-tree mst 1 root secondary

!Verification:

SW1#show spanning-tree mst 1

MST1 vlans mapped: 1,3,5,7,9

Bridge address 08cc.68ab.6780 priority 24577 (24576 sysid 1)

Root this switch for MST1

Interface Role Sts Cost Prio.Nbr Type

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

Fa0/1 Desg FWD 200000 128.1 P2p

Fa0/2 Desg FWD 200000 128.2 P2p

SW1#show spanning-tree mst configuration

Name [cisco]

Revision 1 Instances configured 3

Instance Vlans mapped

-------- ---

0 11-4094

1 1,3,5,7,9

2 2,4,6,8,10

- -

SW1#

SW1#show spanning-tree mst 2

MST2 vlans mapped: 2,4,6,8,10

Bridge address 08cc.68ab.6780 priority 28674 (28672 sysid 2)

Root address 08cc.68dd.0800 priority 24578 (24576 sysid 2)

port Fa0/1 cost 200000 rem hops 19

Interface Role Sts Cost Prio.Nbr Type

- -

Fa0/1 Root FWD 200000 128.1 P2p

Fa0/2 Altn BLK 200000 128.2 P2p

SW1#

First Hop Redundancy Protocols

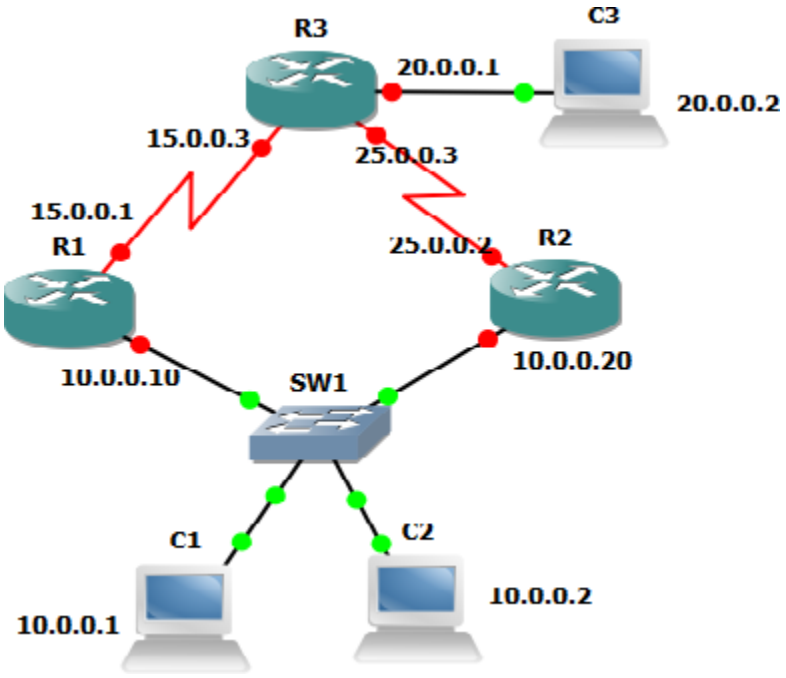
Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

Lab 30
FHRP (HSRP and VRRP)

Objective:

The main goal of this lab is to configure a layer 3 redundant topology using HSRP and VRRP protocol, and to show the convergence when the active router goes down.

Diagram:



Preliminary Task:

- Connect the network as show in the diagram.
- Assign the IP addresses for computers and interfaces as explained.
- Enable RIP version 2 on all routers, and advertise the connected networks.
- The default gateway for computers should be the virtual ip address 10.0.0.100

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

!R1

router rip

version 2

network 10.0.0.0

network 15.0.0.0

!R2

router rip

version 2

network 25.0.0.0

network 10.0.0.0

!R3

router rip

version 2

network 20.0.0.0

network 15.0.0.0

network 25.0.0.0

Task 1:

Configure HSRP on R1 & R2 for the Ethernet segment as follows:

- R1 to be the active Router with a priority 110

- The virtual ip address should be 10.0.0.100
- Both routers should enable preempt feature.
- Both routers should track their interface s1/0, and to decrement their priority by 15 in case of losing the serial interface (S1/0).

!R1/R2

interface fa0/0

standby 1 ip 10.0.0.100

standby 1 preempt

standby 1 track s1/0 15

!R1

interface fa0/0

standby 1 priority 110

!Verification:

R1#show standby brief

P indicates configured to preempt.

|

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Fa0/0	1	110	P	Active	local	10.0.0.20	10.0.0.100

R1#

Ping should be working between all PCs....

VPCS[1]> trace 20.0.0.2

trace to 20.0.0.2, 8 hops max, press Ctrl+C to stop

1 10.0.0.10 62.400 ms 46.800 ms 31.200 ms

2 15.0.0.3 109.200 ms 62.400 ms 62.400 ms

3 *20.0.0.2 109.200 ms (ICMP type:3, code:3, Destination port unreachable)

Task 2:

Shutdown the interface S1/0 on R1, and check the HSRP status

!R1

interface s1/0

shutdown

!Verification:

R1#show standby brief

P indicates configured to preempt.

|

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Fa0/0	1	95	P	Standby	10.0.0.20	local	10.0.0.100

Task 3:

- No shutdown the interface S1/0
- remove the HSRP configuration from both routers
- Configure two HSRP groups, R1 to be the active router for group 1, and R2 for group 2 to allow load balancing between the two routers.

- The default gateway for PC1 should be 10.0.0.100, and for PC2 10.0.0.200
- Both routers should enable preempt feature
- Both routers should track their S1/0 interface, and decrement priority by 15 in case of failure.
- The virtual ip address for group 1 should be 10.0.0.100, and for group 2 10.0.0.200

```
!R1/R2
interface fa0/0
no standby 1
!R1
interface fa0/0
standby 1 ip 10.0.0.100
standby 1 preempt
standby 1 track s1/0 15
standby 1 priority 110
standby 2 ip 10.0.0.200
standby 2 preempt
standby 2 track s1/0 15
interface s1/0
no shutdown

!R2
interface fa0/0
```

standby 1 ip 10.0.0.100

standby 1 preempt

standby 1 track s1/0 15

standby 2 ip 10.0.0.200

standby 2 preempt

standby 2 track s1/0 15

standby 2 priority 110

!Verification:

R1#show standby brief

P indicates configured to preempt.

|

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Fa0/0	1	110	P	Active	local	10.0.0.20	10.0.0.100
Fa0/0	2	100	P	Standby	10.0.0.20	local	10.0.0.200

R1#

R2#show standby brief

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Fa0/0	1	100	P	Standby	10.0.0.10	local	10.0.0.100
Fa0/0	2	110	P	Active	local	10.0.0.10	10.0.0.200

R2#

VPCS[1]> trace 20.0.0.2

trace to 20.0.0.2, 8 hops max, press Ctrl+C to stop

1 10.0.0.10 78.001 ms 31.200 ms 31.200 ms

2 15.0.0.3 93.600 ms 62.400 ms 78.000 ms

3 *20.0.0.2 93.600 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS[2]> trace 20.0.0.2

trace to 20.0.0.2, 8 hops max, press Ctrl+C to stop

1 10.0.0.20 62.400 ms 46.800 ms 46.800 ms

2 25.0.0.3 93.600 ms 78.000 ms 46.800 ms

3 *20.0.0.2 93.600 ms (ICMP type:3, code:3, Destination port unreachable)

!We can notice that traffic from PC1 has gone through R1, and traffic from PC2 has gone through R2. So, the load balancing has been achieved by configuring two HSRP groups, and pointing each PC to a certain virtual IP address.

Task 4:

- Remove HSRP from both routers R1 & R2
- Configure VRRP on both routers
- R1 to be the master Router with a priority 110

- The virtual ip address should be 10.0.0.100

!R1/R2

interface fa0/0

no standby 1

vrrp 1 ip 10.0.0.100

!R1

interface fa0/0

vrrp 1 priority 110

!Verification

!R1

Show vrrp brief

Interface	Grp	Pri	Time	Own	Pre	State	Master addr	Group addr
Fa0/0	1	110	3570	Y		Master	10.0.0.10	10.0.0.100

!R2

Show vrrp brief

Interface	Grp	Pri	Time	Own	Pre	State	Master addr	Group addr
Fa0/0	1	100	3609	Y		Backup	10.0.0.10	10.0.0.100

Task 5:

- Remove the VRRP configuration from both routers
- Configure two VRRP groups, R1 to be the master router for group 1, and R2 is the master for group 2 to allow load balancing between the two routers.
- The default gateway for PC1 should be 10.0.0.100, and for PC2 10.0.0.200
- The virtual ip address for group 1 should be 10.0.0.100, and for group 2 10.0.0.200

```
!R1/R2

interface fa0/0

no vrrp 1

!R1

interface fa0/0

vrrp 1 ip 10.0.0.100

vrrp 1 priority 110

vrrp 2 ip 10.0.0.200



!R2

interface fa0/0

vrrp 1 ip 10.0.0.100

vrrp 2 ip 10.0.0.200

vrrp 2 priority 110
```

!Verification:

!R1

Show vrrp brief

Interface	Grp	Pri	Time	Own	Pre	State	Master addr	Group addr
Fa0/0	1	110	3570	Y		Master	10.0.0.10	10.0.0.100
Fa0/0	2	100	3609	Y		Backup	10.0.0.20	10.0.0.200

!R2

Show vrrp brief

Fa0/0	1	100	3609	Y		Backup	10.0.0.10	10.0.0.100
Fa0/0	2	110	3570	Y		Master	10.0.0.20	10.0.0.200

IP Services

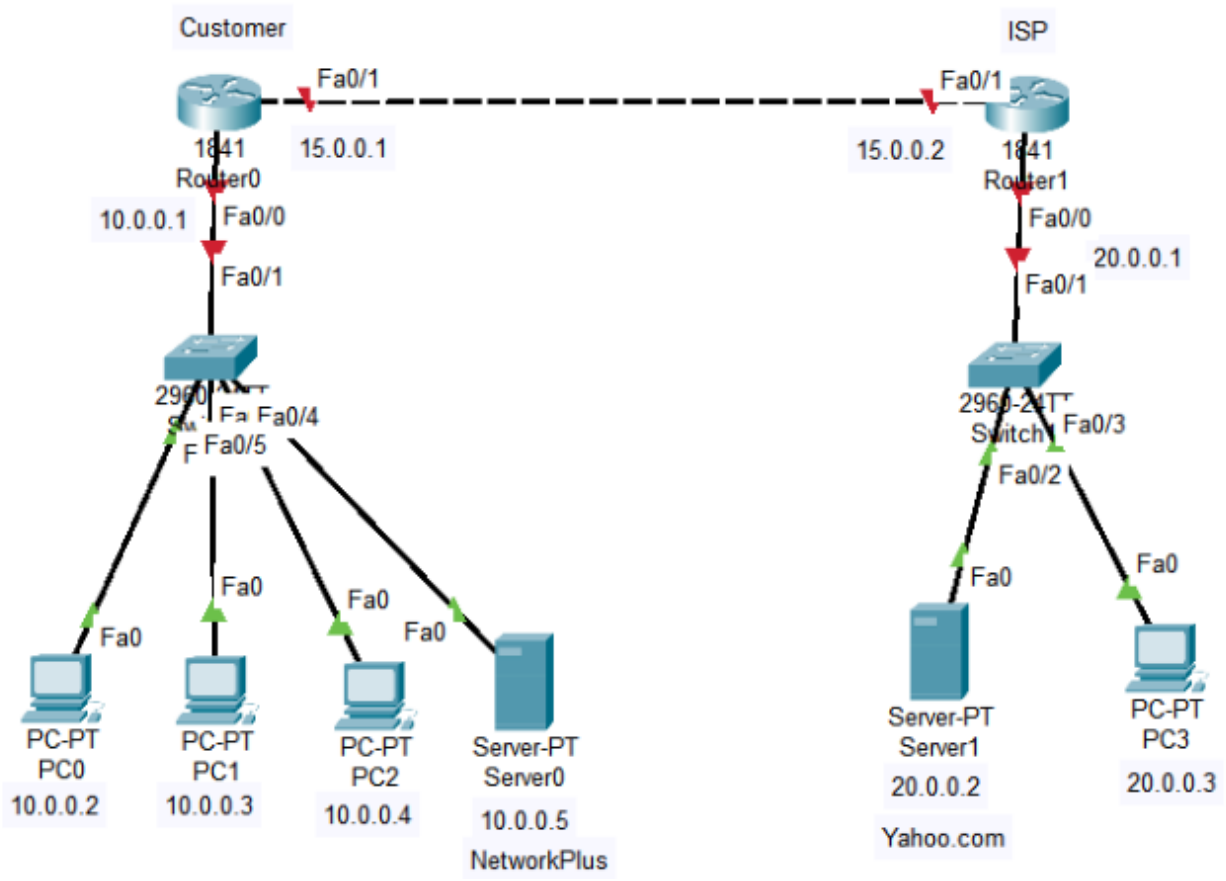
Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

Lab 31

NAT

Objective:
The main goal of this lab is to configure a Network Address Translation (PAT) on Customer Router that is connected to the ISP, while configuring static NAT on the same router for internal web server

Diagram:



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

Preliminary Task:

- Connect the above network
- Assign IP addresses as shown in the diagram
- Configure a default route on the customer router towards the ISP router

Task 1:

- Configure PAT on Customer Router so that all 10.0.0.2,10.0.0.3 and 10.0.0.4 ip addresses are leaving to the internet by getting translated into one public ip address (15.0.0.1)
- Configure static nat on the customer router so that networkplus server is accessible from the internet through 15.0.0.3

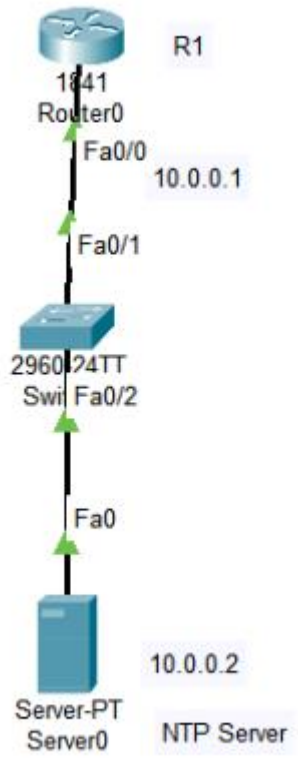
```
!Customer
Interface fa0/0
Ip nat inside
!
Interface fa0/1
Ip nat outside
!
Ip nat inside source static 10.0.0.5 15.0.0.3
!
Access-list 1 permit host 10.0.0.2
Access-list 1 permit host 10.0.0.3
Access-list 1 permit host 10.0.0.4
!
Ip nat inside source list 1 interface fa0/1 overload
```

Lab 32

NTP

Objective:
The main goal of this lab is to configure and verify NTP Configuration.

Diagram:



Preliminary Tasks:

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

Task 1: Configure the Router as NTP client and the server as NTP Server and verify the configuration

!Router
Ntp server 10.0.0.2

!Server
Services>NTP>Enable

!Verification
!Router
Show ntp status

Clock is synchronized, stratum 16, reference is 10.0.0.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is 27764901.000002C1 (0:57:37.705 UTC Fri Mar 9 2057)
clock offset is 1.00 msec, root delay is 3.00 msec
root dispersion is 20.58 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system poll interval is 4, last update was 10 sec ago.

Show clock

0:37:31.216 UTC Wed Mar 5 2025

Virtualization

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

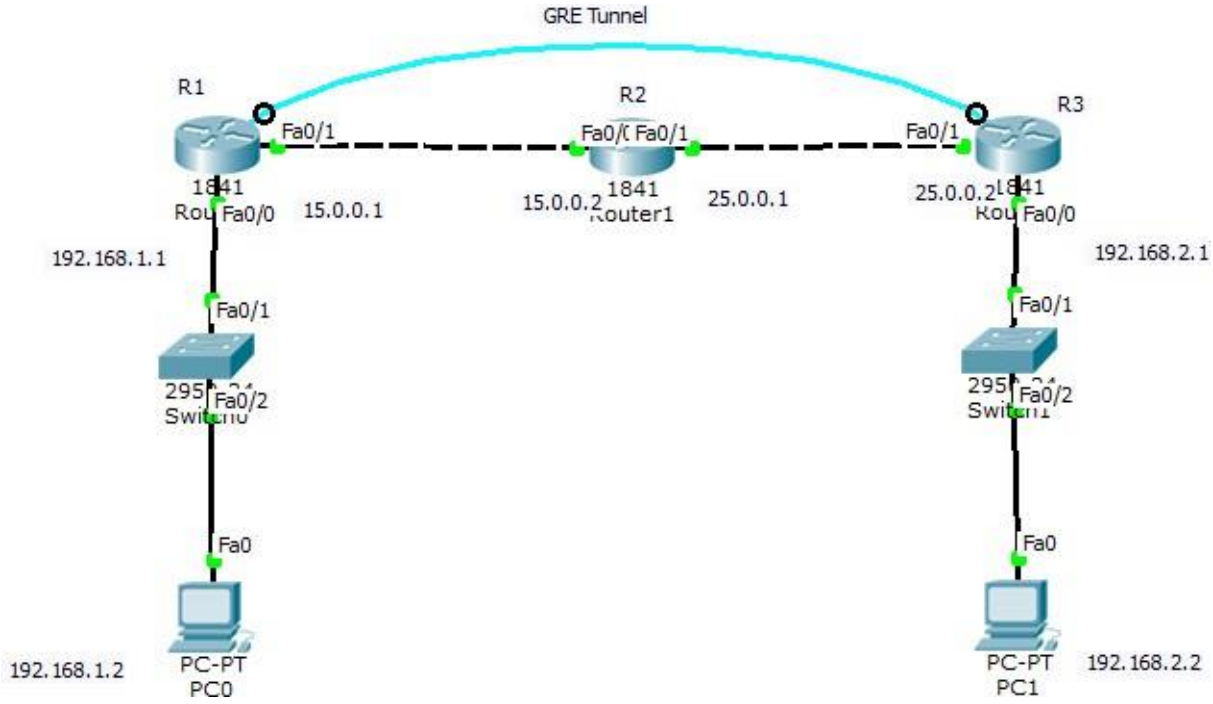
Lab 33

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....

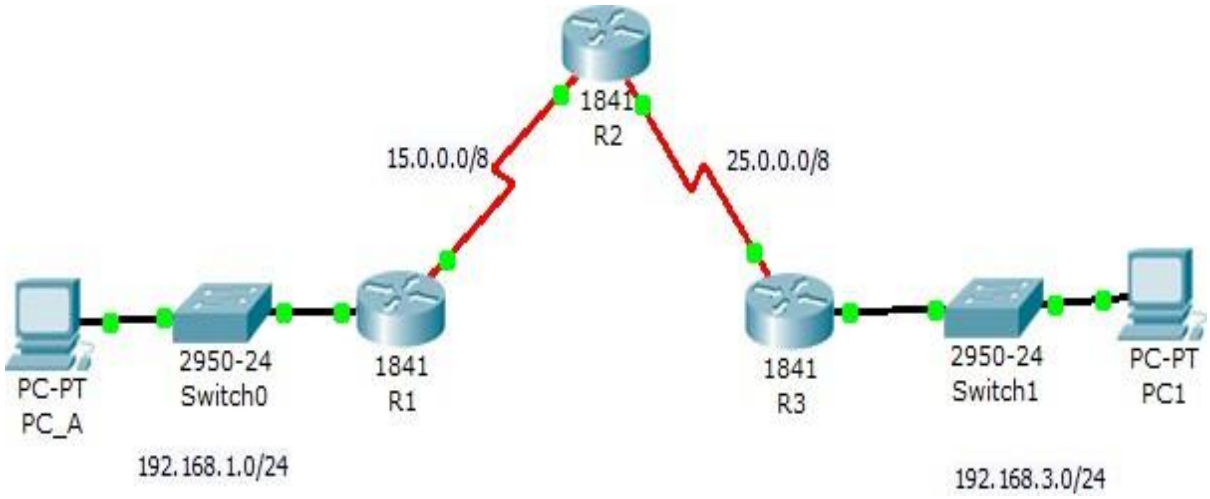
Lab 34

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—

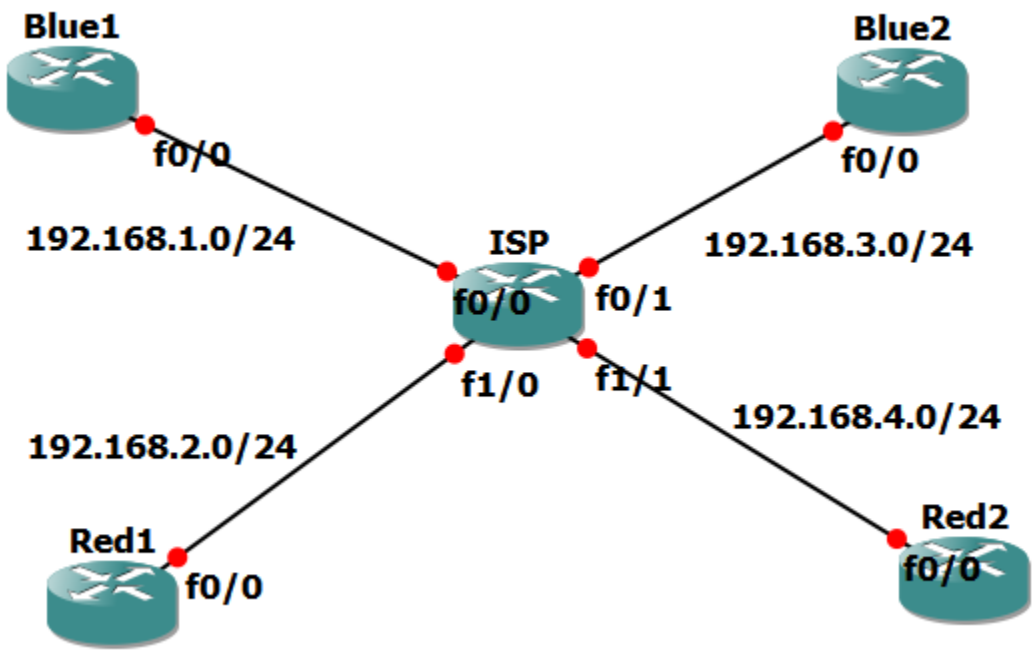
Lab 35

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

Task 1:

- Configure the ISP to enable VRF Leakage so that different VRF can communicate with each other

!ISP

Ip route vrf Blue 192.168.2.2 255.255.255.255 192.168.2.2 global

Ip route 192.168.2.2 255.255.255.255 fa1/0

Ip route vrf Blue 192.168.4.2 255.255.255.255 192.168.4.2 global

Ip route 192.168.4.2 255.255.255.255 fa1/1

Ip route vrf Red 192.168.1.2 255.255.255.255 192.168.1.2 global

Ip route 192.168.1.2 255.255.255.255 fa0/0

Ip route vrf Red 192.168.3.2 255.255.255.255 192.168.3.2 global

Ip route 192.168.3.2 255.255.255.255 fa0/1

Network Assurance

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

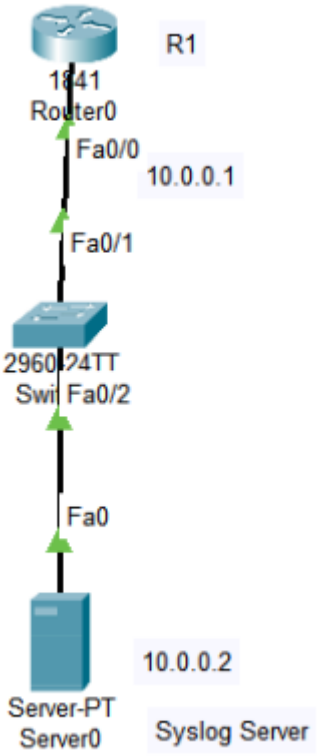
Lab 36

SYSLOG

Objective:

The main goal of this lab is to configure and verify SYSLOG configuration

Diagram:



Preliminary Tasks:

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

Task 1:

- Configure the Server as Syslog and ntp Server
- Configure the router to send its logging messages to the syslog server
- Configure the router to send its logging messages stamped with time

!R1
Ntp server 10.0.0.2
Logging 10.0.0.2
Logging on
Service timestamps debug datetime msec
!

!Server
Services>NTP>Enable
Services>Syslog>Enable

Task 2:

- Shutdown and no shutdown the loopback interface to see the logging messages in the syslog server

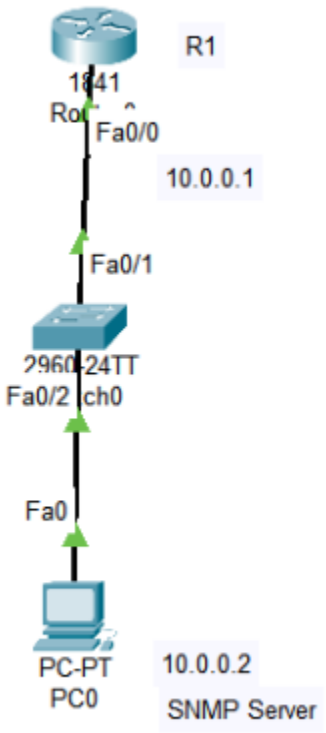
Lab 37

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:

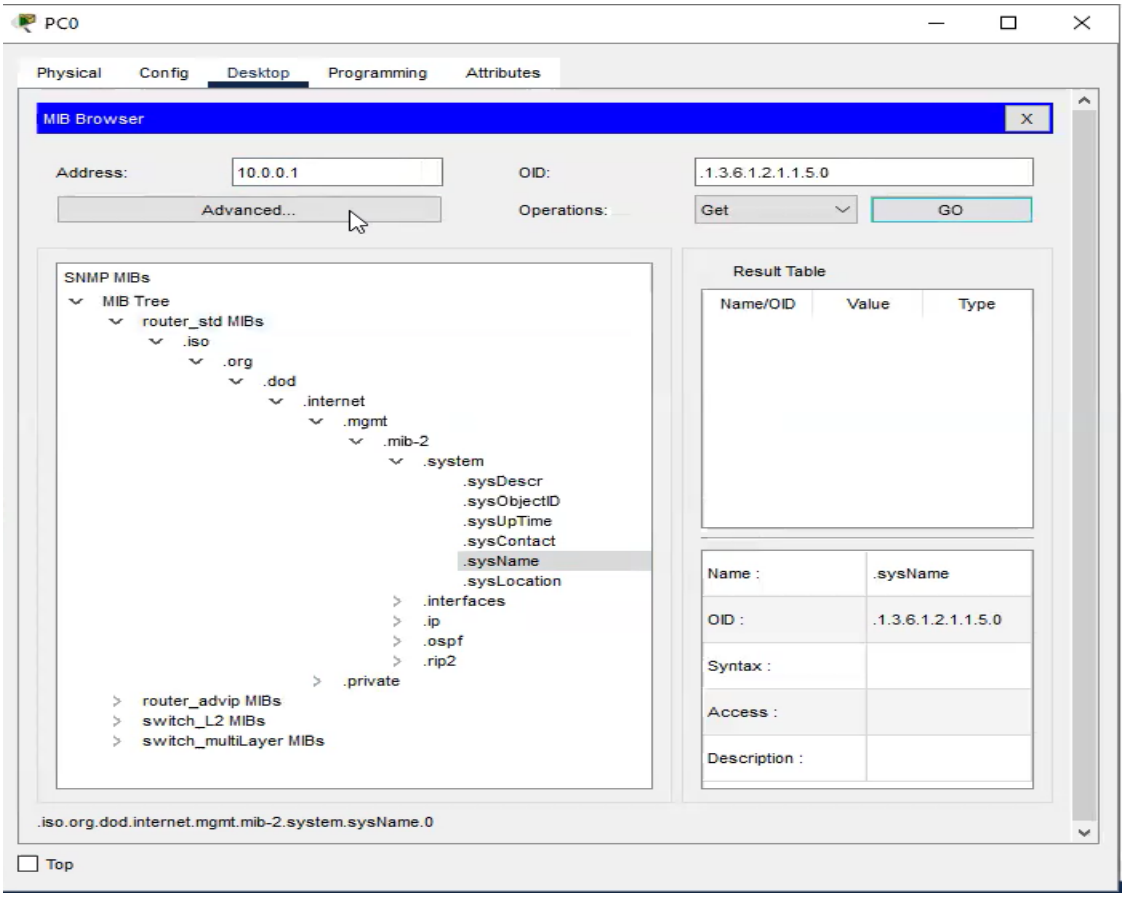
- Configure The router with SNMP and read/write community of cisco
- Set the NMS to get the system name of the Router, and uptime
- Don’t forget to set the managed ip and community in the NMS

!R1

Snmp-server community cisco rw

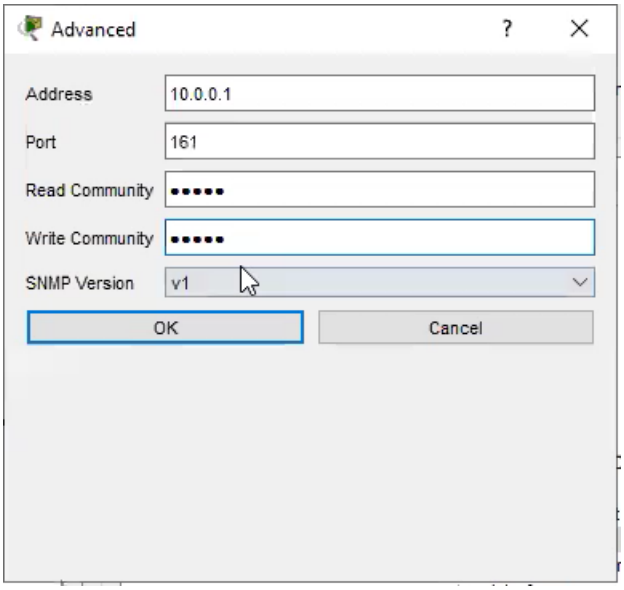
!NMS

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

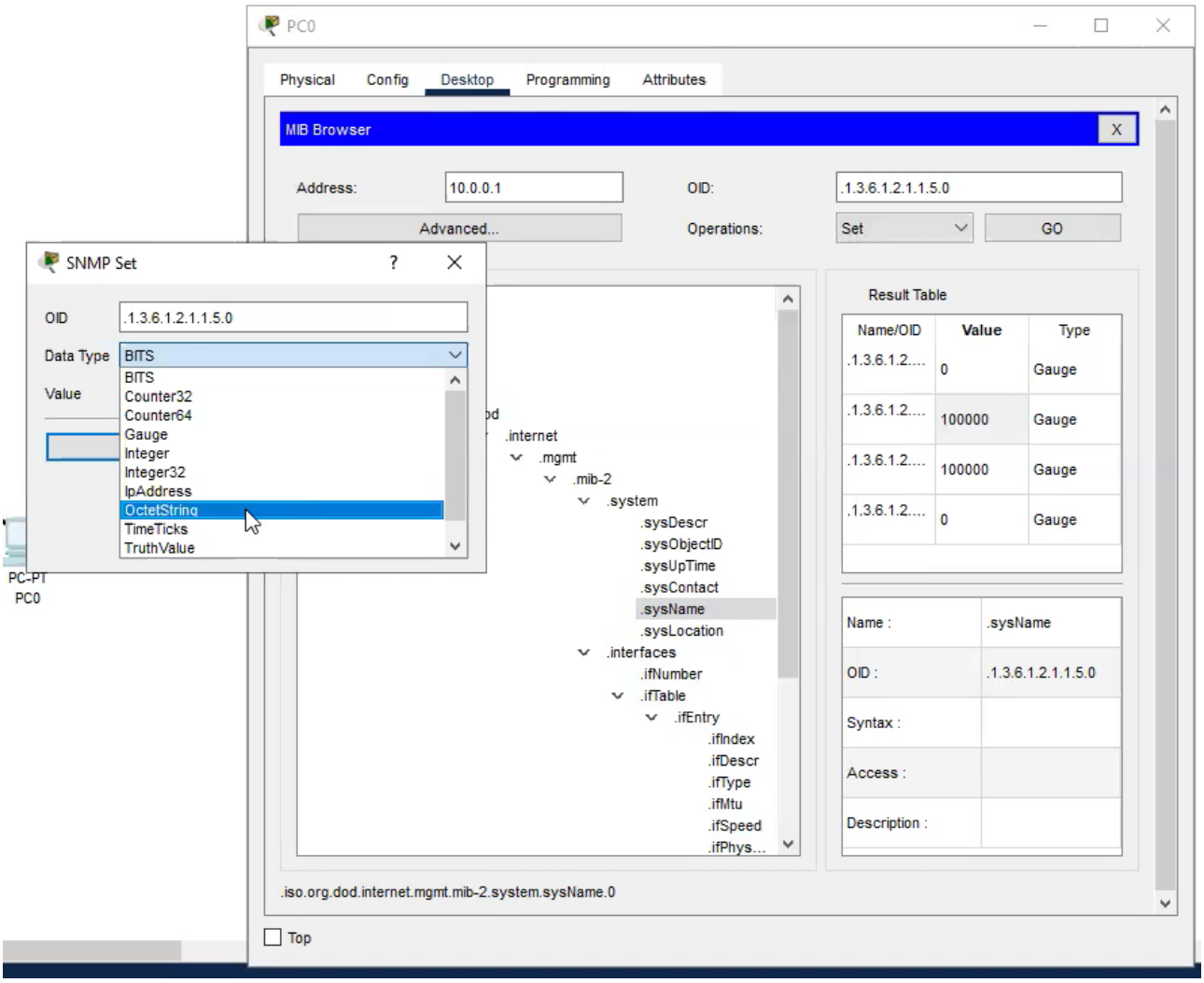


Task 2:

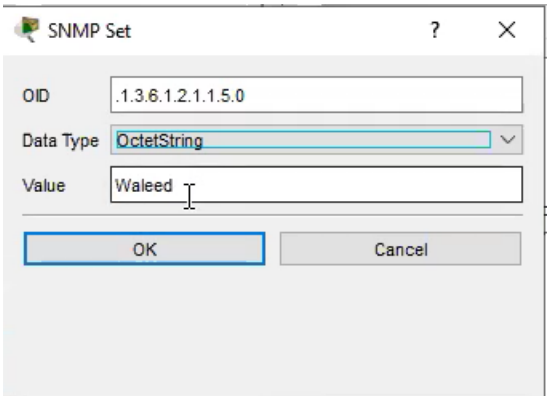
- Configure the MIB Browser to set the Router Name by using the Set parameter

!NMS

In the MIB Browser:



Then



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

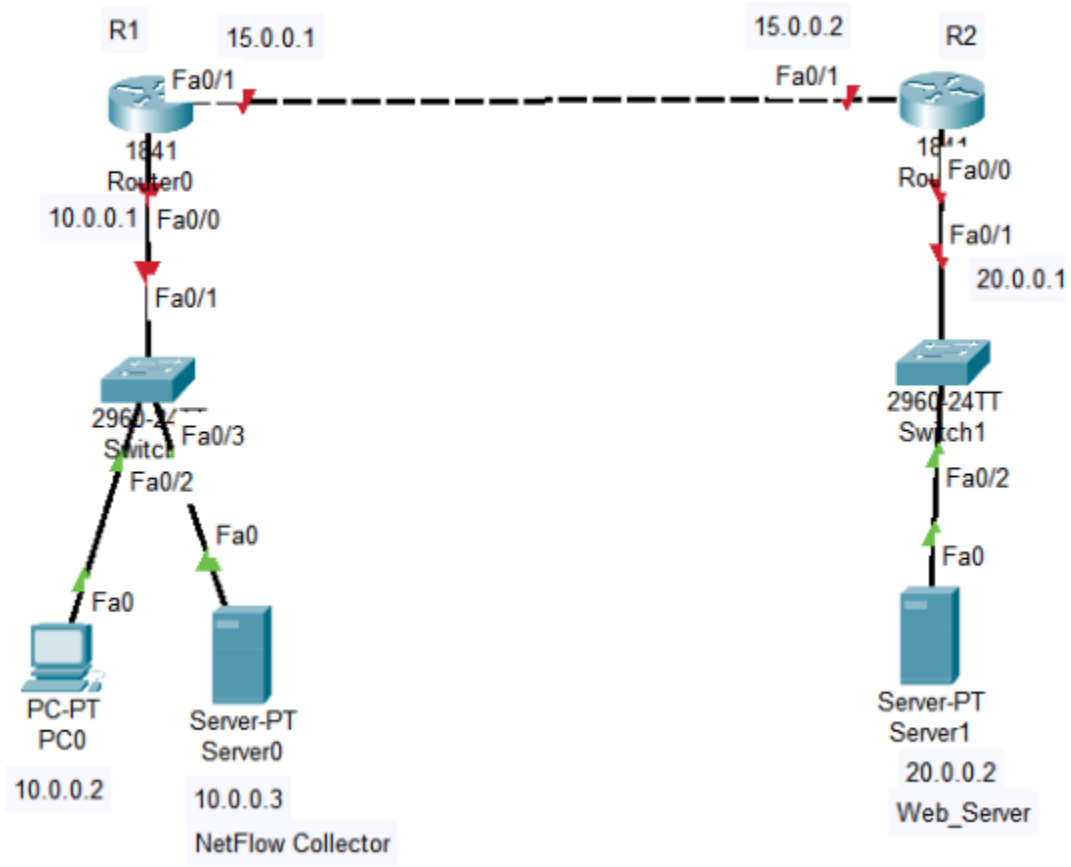
Lab 38

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

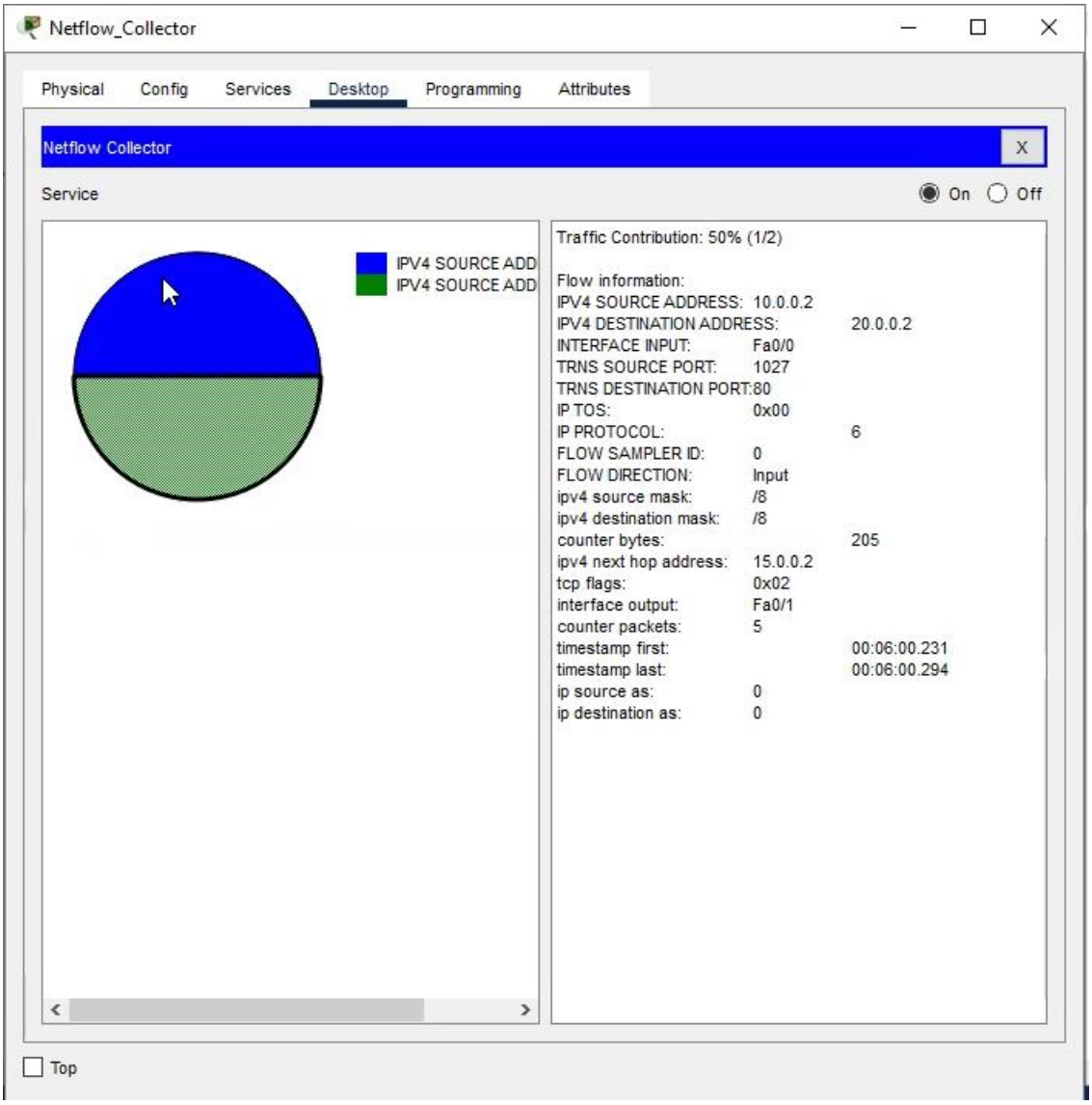
Show ip cache flow

```
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

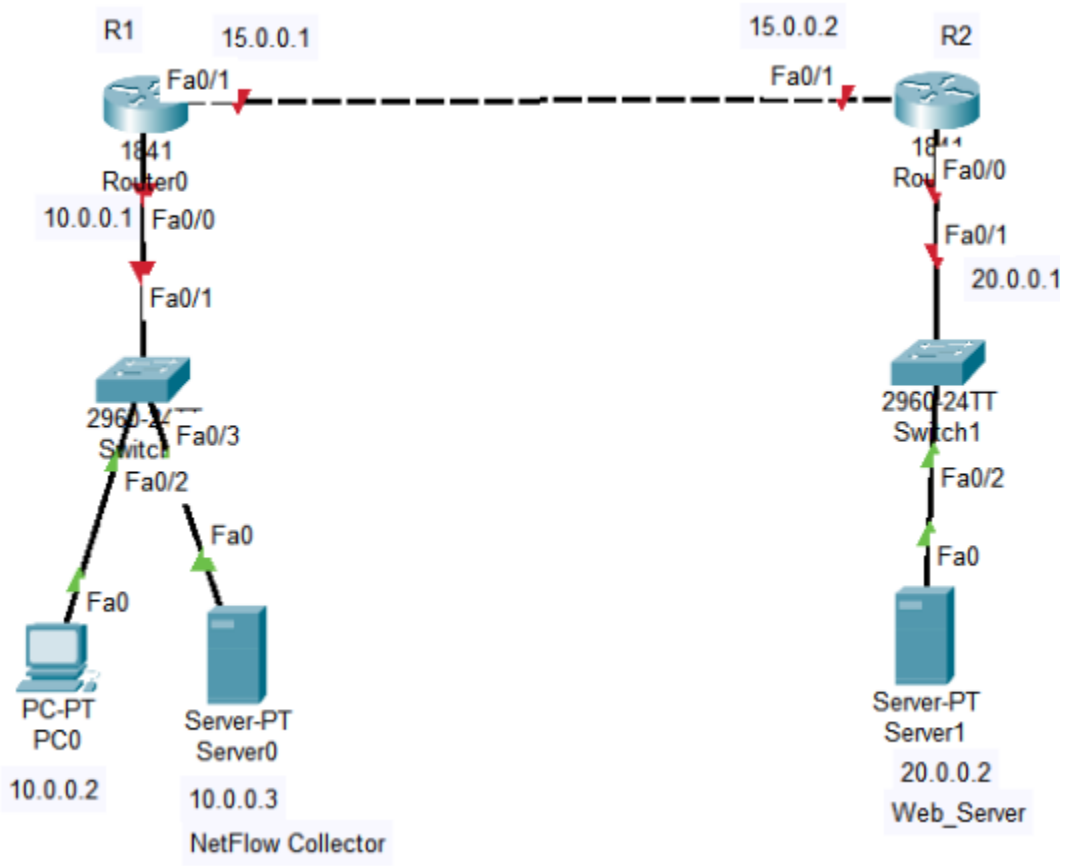
Lab 39

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#
```

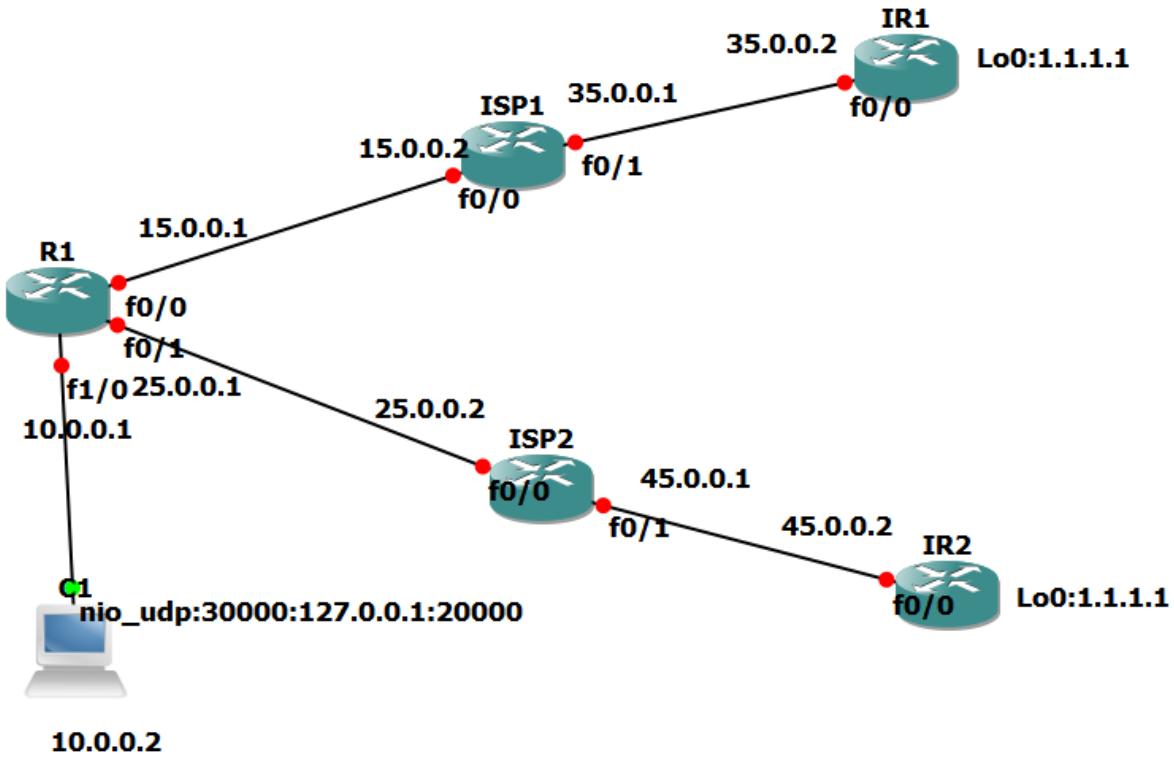
Lab 40

IP SLA

Objective:

The main goal of this lab is to configure and verify IP SLA Setup On Cisco Routers

Diagram:



Preliminary Tasks:

- Connect the network as shown in the depicted diagram
- Assign IP addresses as shown in the figure
- Configure Static Routes on the ISP Routers (ISP1&ISP2) towards 1.1.1.1
- Configure Static routes on ISP Routers for 10.0.0.0 towards R1
- Configure default routes on IR1 & IR2 towards ISP1 & ISP2

Task 1:

- Configure default route on R1 pointed to 15.0.0.2 with AD 10 and secondary default route pointed to 25.0.0.2 with AD 20.

- Verify the failover when the primary link fails
- Verify the failover when the indirect failure happens

!R1
Ip route 0.0.0.0 0.0.0.0 15.0.0.2 10
Ip route 0.0.0.0 0.0.0.0 25.0.0.2 20

!**Verification**
You can notice when the primary link direct failure occurs, the failover is successfully triggered to the backup link. However, when Indirect primary link failure occurs, no failover is triggered which leads us to the importance of using IP SLA

Task 2:

- Configure SLA to monitor icmp echo to 35.0.0.2 with timeout and threshold of 1000 and frequency 1
- Link the SLA with trackable object which then linked to the primary default route on R1

!R1
Ip sla 1
Icmp-echo 1.1.1.1
Timeout 1000
Threshold 1000
Frequency 1
Exit
Ip sla schedule 1 life forever start-time now
Track 1 ip sla 1 reachability
Ip route 0.0.0.0 0.0.0.0 15.0.0.2 track 1

!Verification
We can notice in this scenario failover is successfully achieved for both direct and indirect failure.

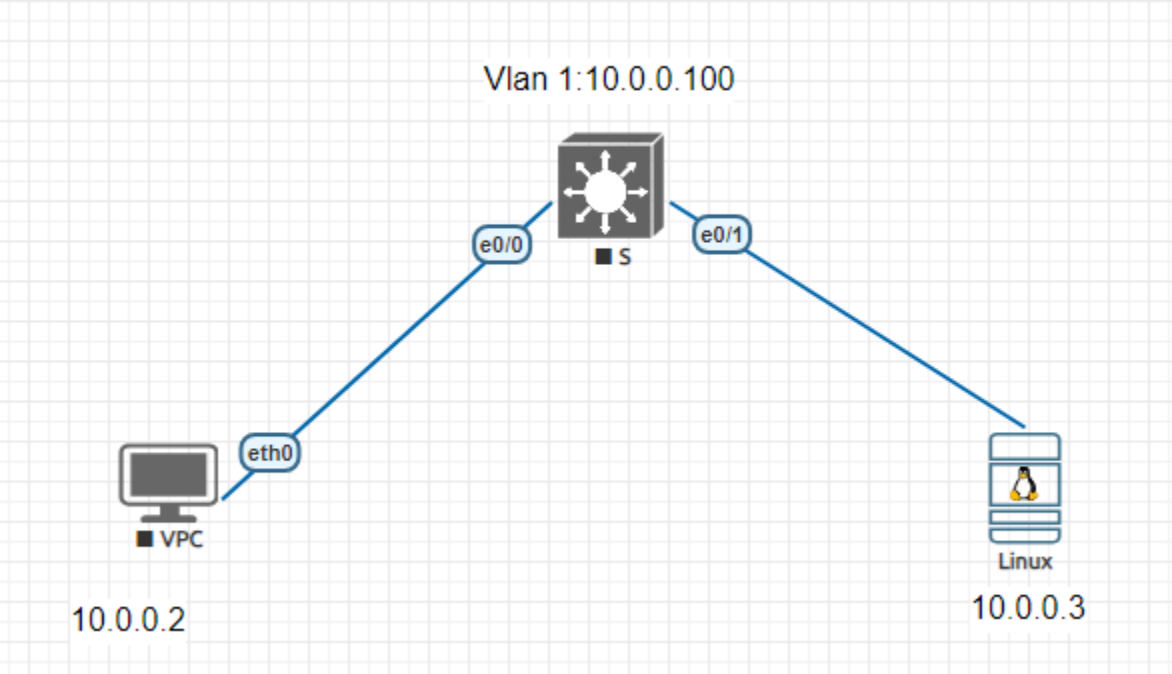
Lab 41

Local SPAN

Objective:

The main goal of this lab is to configure and verify Local SPAN on Cisco Devices

Diagram:



Preliminary Tasks:

- Connect the network as shown in the above network
- Assign IP addresses as depicted in the diagram
- Run wireshark on the linux server on Eve-ng

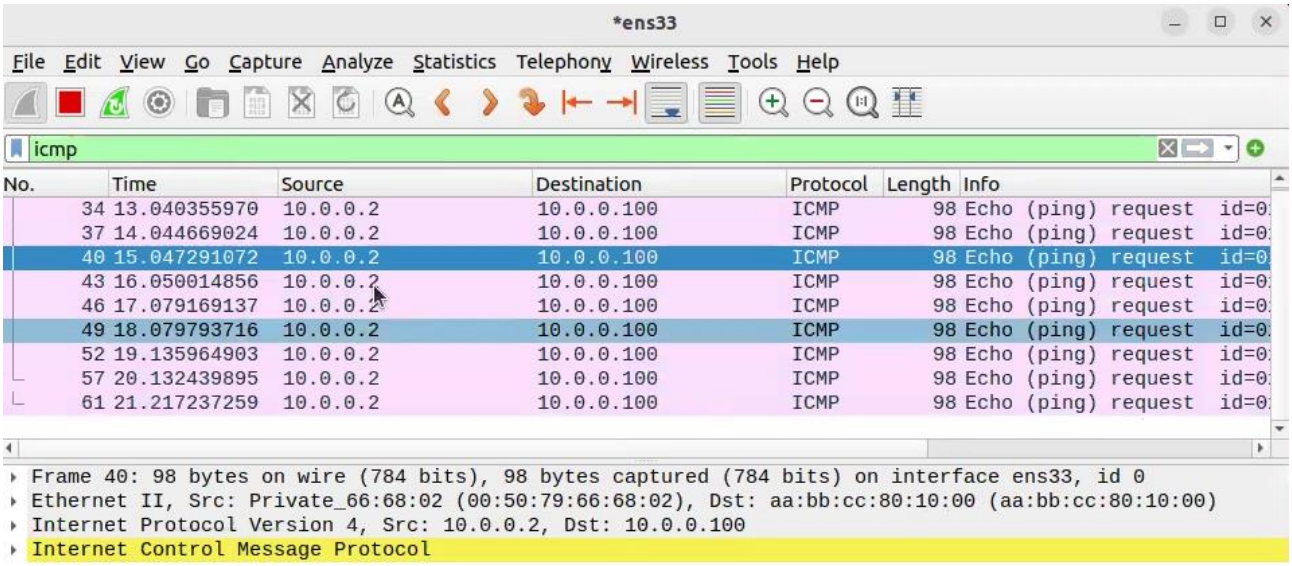
Task 1:

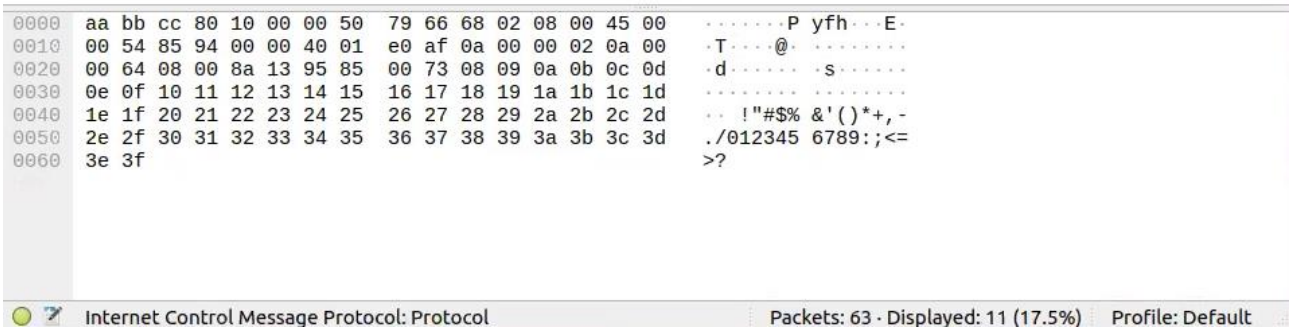
- Configure Local SPAN on the switch
- Make a ping between 10.0.0.2 and Vlan 1 ip address

- Verify the capture of the ping in the server wireshark

!SW
Monitor session 1 source interface e0/0 rx
Monitor session 1 destination interface e0/1
!

!Verification on the Linux Server





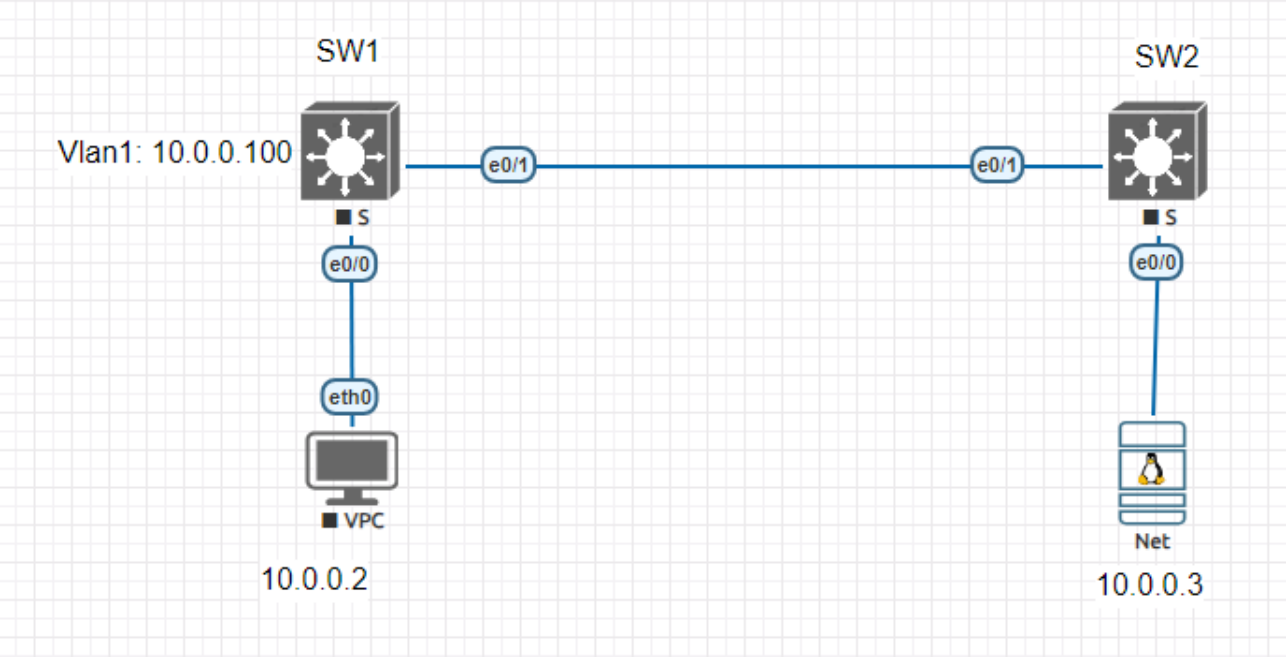
Lab 42

Remote SPAN

Objective:

The main goal of this lab is to configure and verify Remote SPAN on Cisco Devices

Diagram:



Preliminary Tasks:

- Connect the network as shown in the figure
- Assign IP addresses as depicted in the diagram
- Configure the link as trunk between the two switches

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

Task 1:

- Configure Vlan 100 as remote span on both switches
- Configure SW1 to mirror traffic from port e0/0 (rx) to vlan 100
- Configure SW2 to mirror traffic from vlan 100 to port e0/0
- Issue ping from 10.0.0.2 to 10.0.0.100
- Finally Verify the mirrored traffic on the linux Server

!SW1/SW2

Vlan 100

Remote-span

!

!SW1

Monitor session 1 source interface e0/0 rx

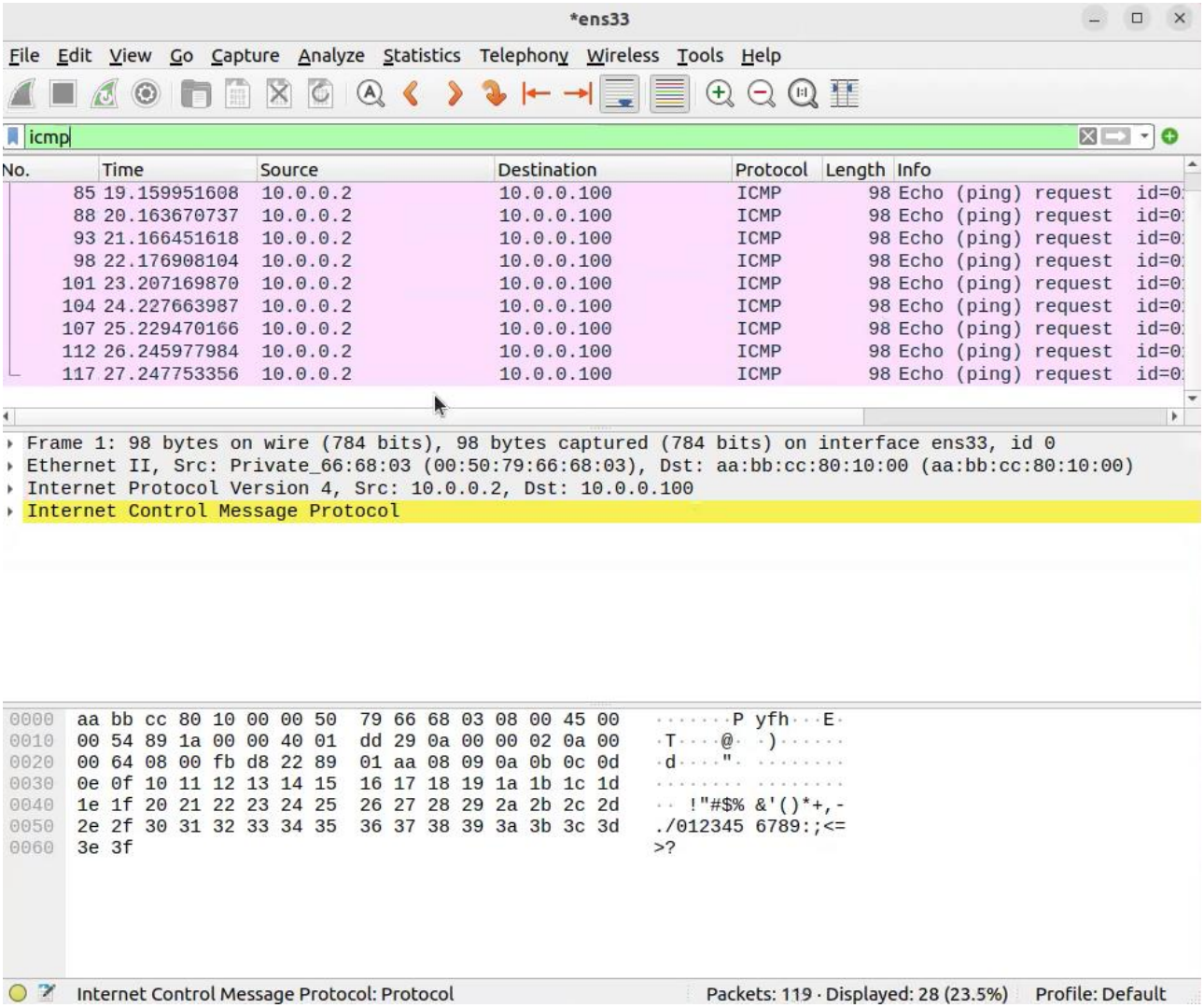
Monitor session 1 destination remote vlan 100

!SW2

Monitor session 1 source remote vlan 100

Monitor session 1 destination interface e0/0

! Verification



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

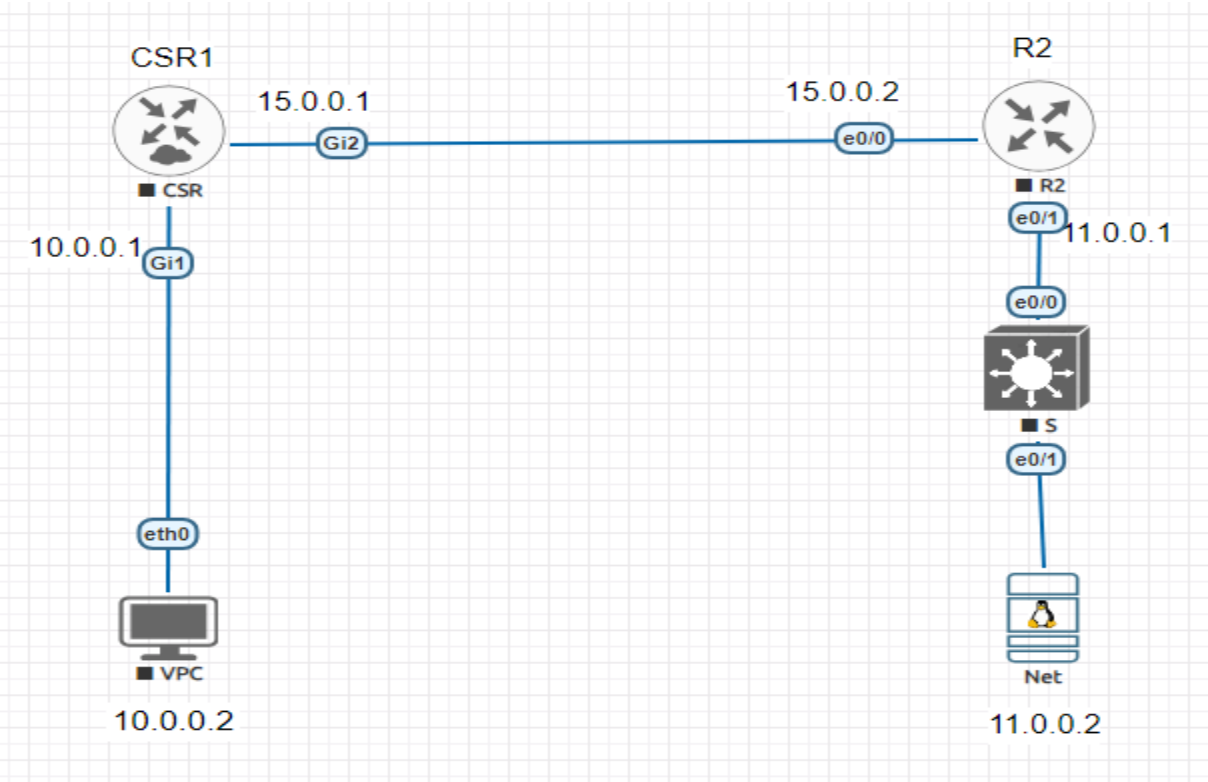
Lab 43

ERSPAN

Objective:

The main goal of this lab is to configure and verify ERSPAN on Cisco CSR Devices

Diagram:



Preliminary Tasks:

- Connect the network as shown in the figure
- Assign IP addresses as depicted in the diagram
- Ensure the connectivity between PC and Server

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

Task 1:

- Configure CSR1 to mirror traffic the server
- Issue a ping from 10.0.0.2 to 10.0.0.1
- Use wireshark on the server to verify the mirrored traffic

!CSR1

Monitor session 1 type erspan-source

Source interface g1 rx

No shutdown

Destination

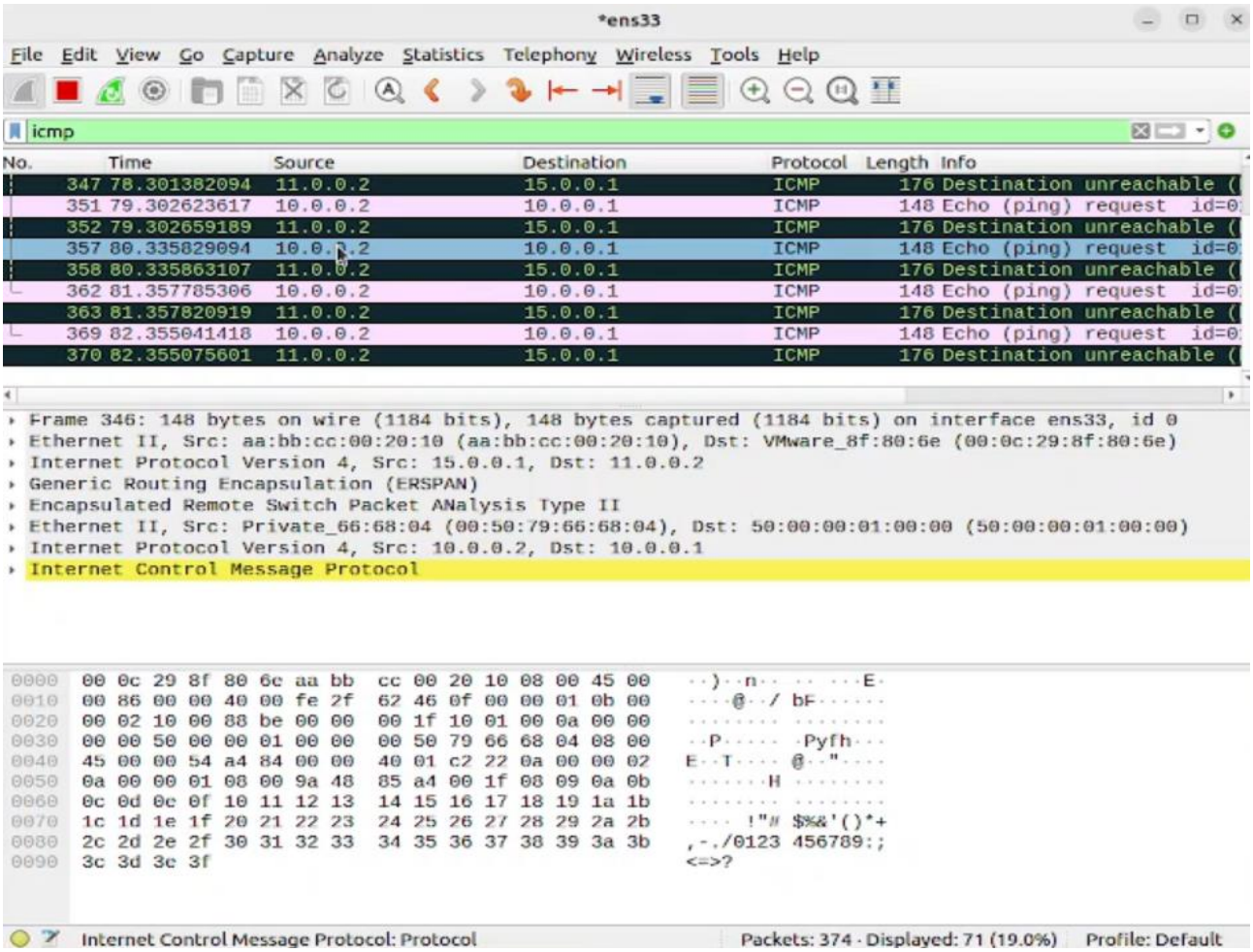
Erspan-id 10

Ip address 11.0.0.2

Origin ip address 15.0.0.1

!Verification

Use Wireshark on the server to verify the mirroring process



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

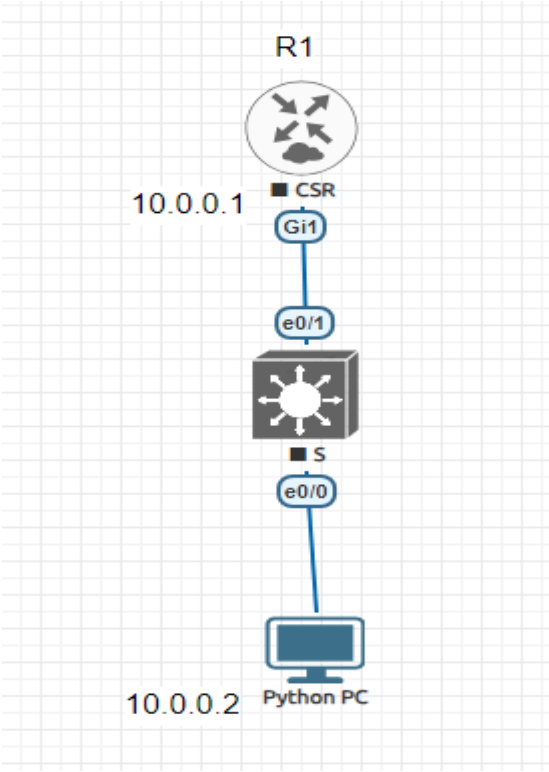
Lab 44

NETCONF

Objective:

The main goal of this lab is to configure and verify NETCONF on Cisco CSR Router, and verify the configuration by retrieving the running configuration using python code.

Diagram:



Preliminary Tasks:

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

Task 1:

- Enable SSH on R1
- Enable NETConf on R1

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

```
!R1
Hostname R1
Ip domain-name cisco.com
Crypto key generate rsa modulus 1024
Username admin privilege 15 password cisco
Line vty 0 4
Login local
Transport input ssh
Exit
Netconf-yang
```

!Verification

Verify the configuration by using the following python script

```
!Python_PC
from ncclient import manager

with manager.connect(host="10.0.0.1", port=830, username="admin",
password="cisco", hostkey_verify=False) as m:
   config = m.get_config(source="running").data_xml
   print(config)
```

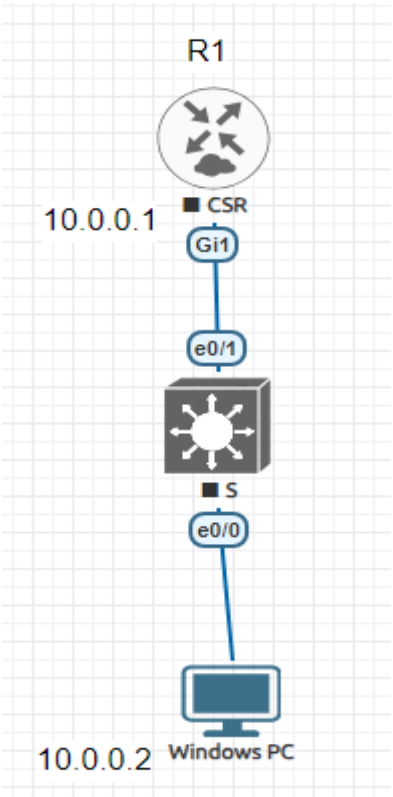
Lab 45

RESTCONF

Objective:

The main goal of this lab is to configure and verify RESTCONF on Cisco CSR Router, and verify the configuration by retrieving interfaces status using web browser and curl command.

Diagram:



Preliminary Tasks:

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

Task 1:

- Enable HTTP and HTTPs Authentication
- Configure HTTP Authentication using Local Database
- Enable Restconf

!R1

Ip http server

Ip http secure-server

Ip http authentication local

Username admin privilege 15 password cisco

Restconf

!Verification:

Use Web browser to get interface status from the router

https://10.0.0.1/restconf/data/ietf-interfaces:interfaces

or use Curl

curl -u admin:cisco -k -X GET "https://192.168.25.141/restconf/data/Cisco-IOS-XE-native:native/interface" -H "Accept: application/yang-data+json"

Security

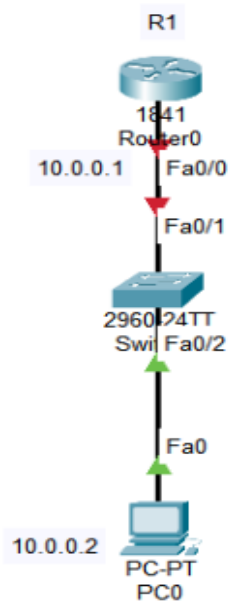
Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

Lab 46
Line and Local User Authentication

Objective:

The goal of this lab is to configure and verify line and local user authentication for telnet and console access

Diagram:



Preliminary Tasks:

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

Task 1:

- Configure the router with telnet using password authentication
- Verify Telnet

!R1
Line con 0
Password cisco
Login
!
Line vty 0 4
Password cisco
Login

!Verification
Verify the configuration of telnet and console

Task 2:

- Modify the configuration by making telnet authentication using local authentication

!R1
Username user1 password cisco
Line vty 0 4
No password
Login local
!

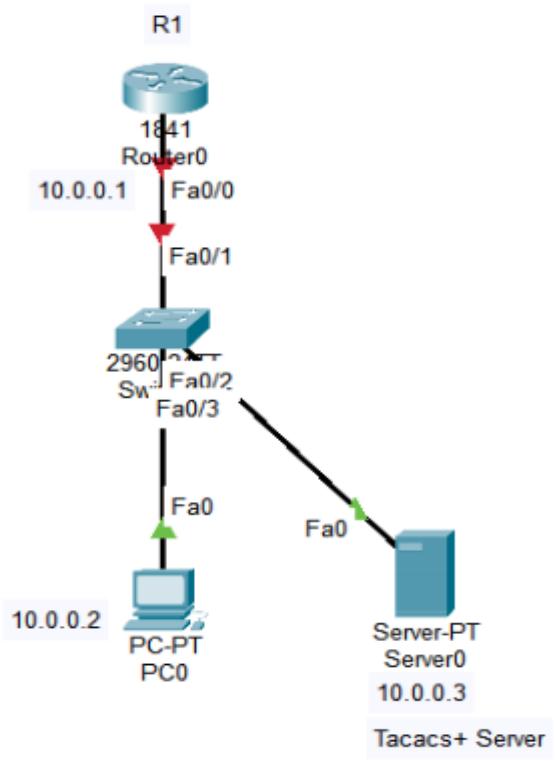
!Verification
Verify telnet configuration by telnet from PC to the router.

Lab 47
Authentication and Authorization Using AAA

Objective:

The goal of this lab is to configure and verify AAA Authentication and Authorization

Diagram:



Preliminary Tasks:

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

Task 1:

- Configure R1 to enable telnet using AAA authentication
- Configure 10.0.0.3 to act as Tacacs+ Server

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

- Verify Telnet Authentication

!R1

Aaa new-model

Aaa authentication login default group tacacs

Tacacs-server host 10.0.0.3 key cisco

Line vty 0 4

Login authentication default

!Server

Services>aaa>Enable

Client Name:Router

Client IP:10.0.0.1

Secret: cisco

ServerType:Tacacs

Username: user1

Password: cisco

Task 2:

- Configure R1 to use local database for authorization
- Use the same credentials in the local database with privilege level 15

!R1

Username user1 privilege 15 password cisco

Aaa authorization exec default local

Line vty 0 4

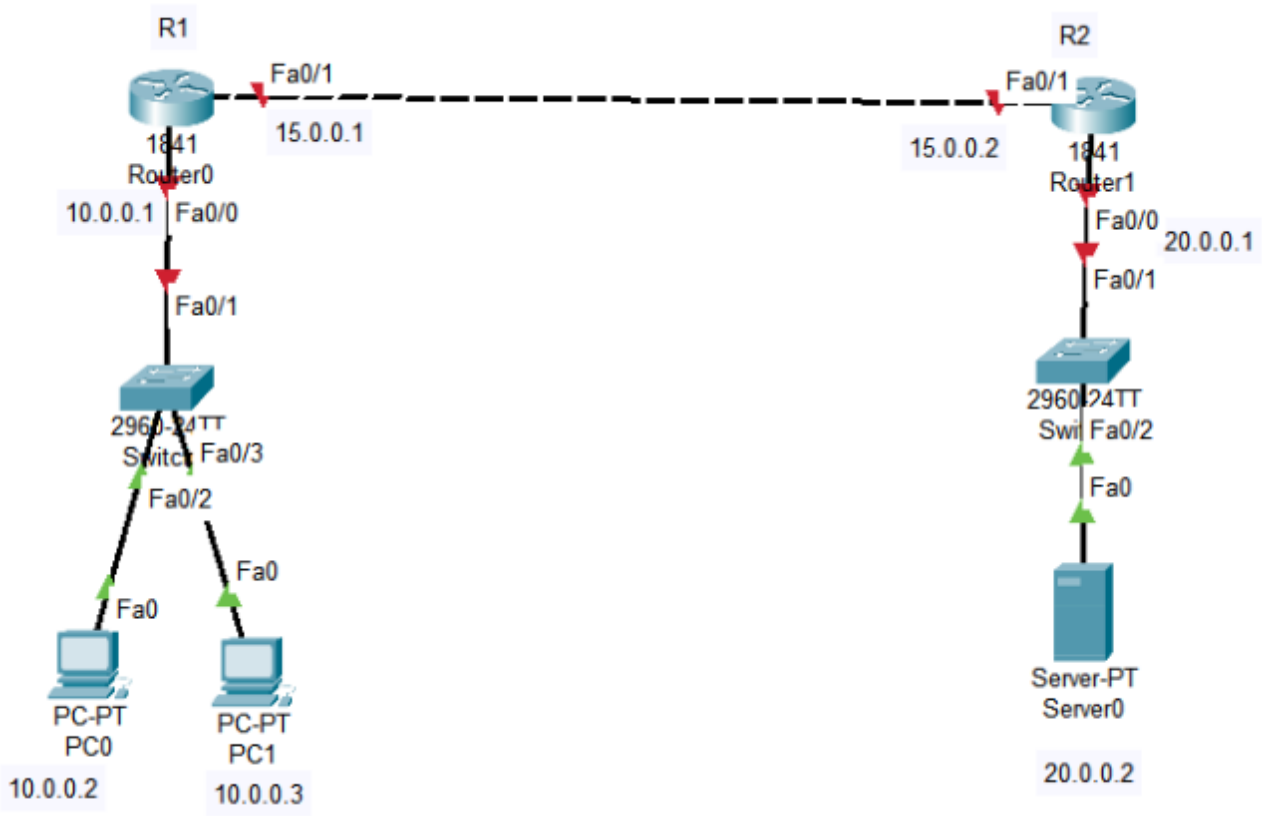
Aaa authorization exec default

Lab 48
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

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

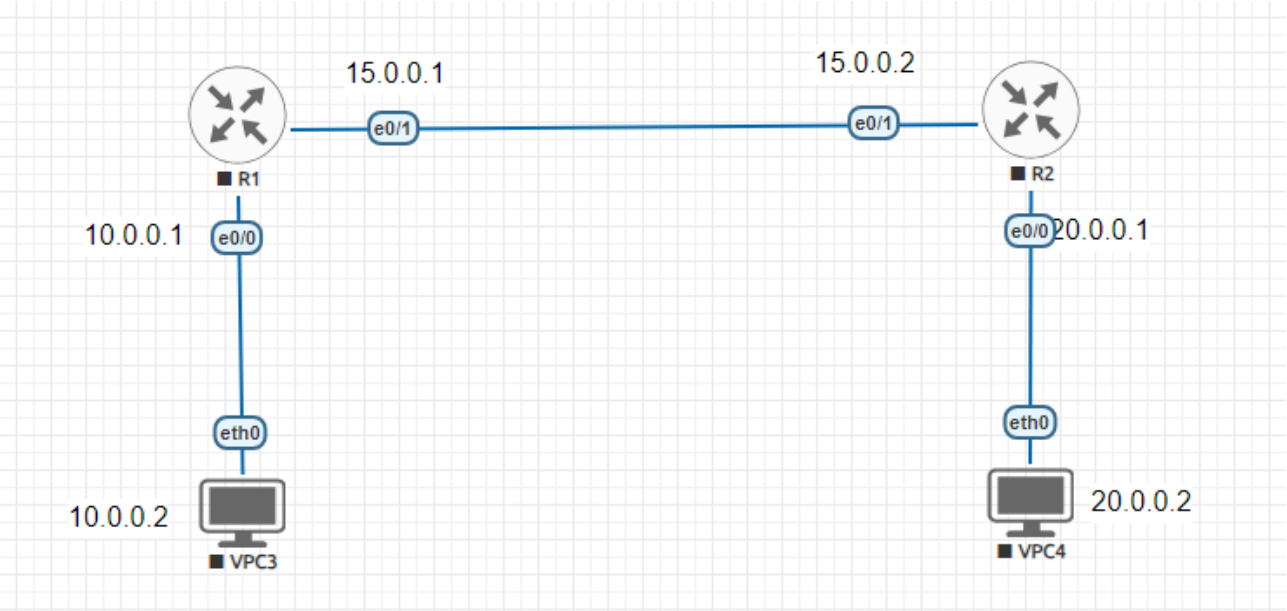
Access-list 100 permit tcp 10.0.0.0 0.255.255.255 host 20.0.0.2 eq 80

!

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

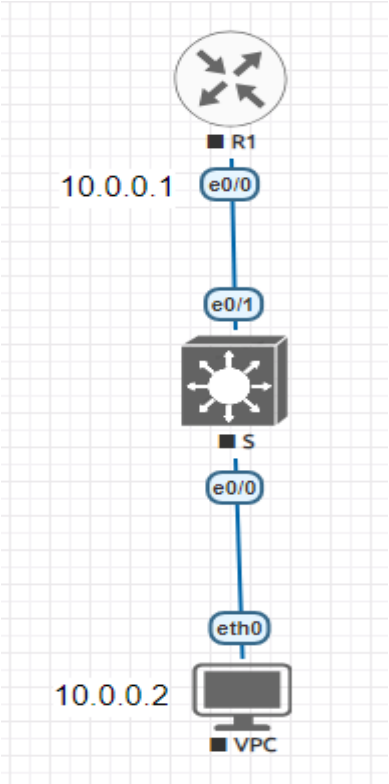
Ip access-group block_icmp in

Lab 49
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

Wireless Networks

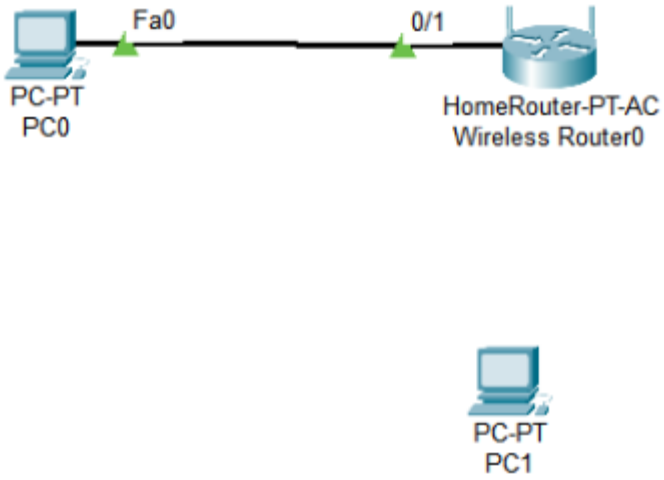
Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

Lab 50
Autonomous Access Point Configuration

Objective:

The goal of this lab is to configure WiFi using Autonomous Access point and enable PSK authentication

Diagram:



Preliminary Tasks:

- Connect the network as shown in the diagram
- Let PC0 to get ip address dynamically from the Wireless router

Task 1:

- Make PC0 manage the wireless router by http to 192.168.0.1
- Use admin/admin as credentials
- Configure the SSID to NetworkPlus and Password to cisco123456
- Verify by making sure that PC1 is getting WiFi connectivity

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

!PC0

http://192.168.0.1

Username:admin

Password:admin

!PC0 (From GUI)

Wireless>Basic Wireless Settings>SSID: NetworkPlus

Then > Save

Wireless>Wireless Security

Security Mode> WPA2 Personal

Passphrase> cisco123456

Then Save Settings

!Verification

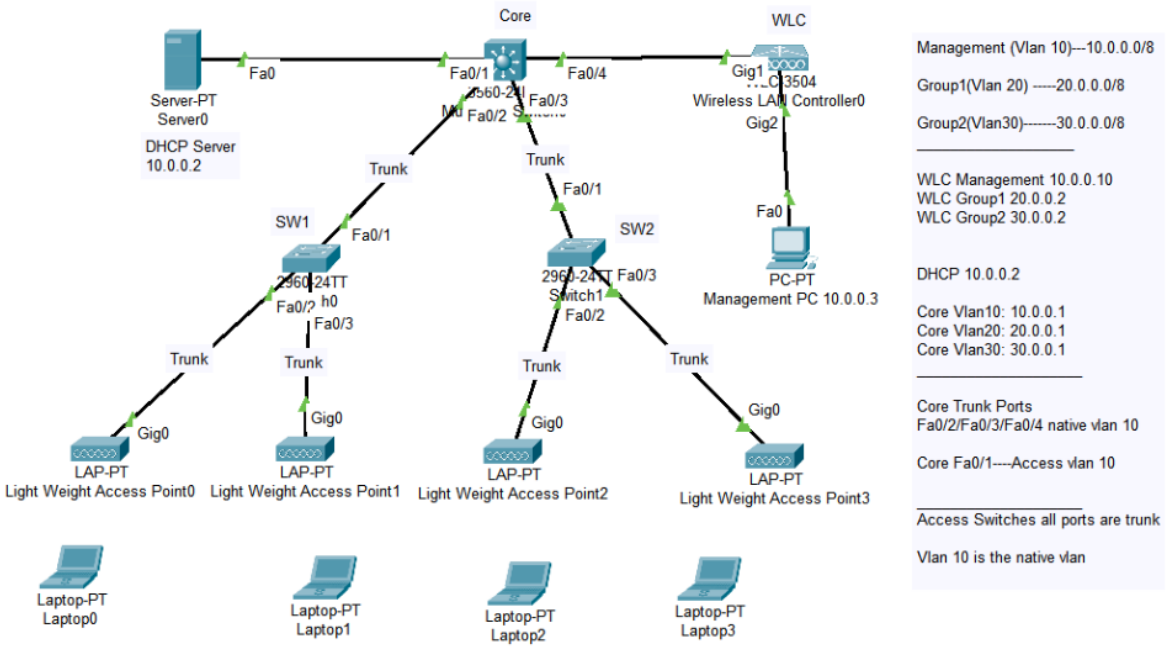
Verify that PC1 is connected to the SSID>NetworkPlus with the above password cisco123456

Lab 51
Wireless Controller Configuration

Objective:

The goal of this lab is to configure Cisco WLC with lightweight Access Point, and using VLANs

Diagram:



Preliminary Tasks:

- Connect the network as shown in the diagram

Task 1:

- Initialize the WLC, by firstly change the management IP to 10.0.0.10
- Login to the WLC from the Management PC using http to set the initial configuration

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

!WLC

WLC>Config>Management>IP Configuration

IPv4 Address: 10.0.0.10

Subnet Mask: 255.0.0.0

!WLC GUI

Use the management pc to login to the 10.0.0.10 of the WLC

Username: admin

Password: Cisco@123

System Name: WLC

Management IP address: 10.0.0.10

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

Employee Network:

Network Name: group1

Passphrase: Cisco@123

Task 2:

- Configure the WLC with a second WLAN named group2
- Use WPA2 Personal Authentication as well

!WLC

Login to the WLC using https://10.0.0.10

Username: admin

Password: Cisco@123

!In WLC GUI:

WLAN>Create New

Profile Name: group2

SSID: group2

!Then Apply

General>Status>Enabled

Security>Layer2 Security>WPA+WPA2

Security>WPA+WPA2 Policy>Enabled

Security>Authentication Key Management>PSK>Enabled

Security>Authentication Key Management>PSK>PSK Format>Cisco@123

!Then Apply

Task 3:

- Configure the core switch with vlan 10,20,30
- Create the SVIs for the Vlans
- Configure the ports as trunk as depicted in the figure with vlan 10 as native vlan
- Configure the port that is connected to the DHCP Server as access in vlan 10

!Core-SW

Vlan 10

```
Name mgmt.
!
Vlan 20
Name group1
!
Vlan 30
Name group2
!
Interface vlan 10
No shutdown
Ip address 10.0.0.1 255.0.0.0
!
Interface vlan 20
No shutdown
Ip address 20.0.0.1 255.0.0.0
!
Interface vlan 30
No shutdown
Ip address 30.0.0.1 255.0.0.0
Exit
!
Interface range fa0/2-4
Switchport trunk encaps dot1q
Switchport mode trunk
```

Switchport trunk native vlan 10

!

Interface fa0/1

Switchport mode access

Switchport access vlan 10

Task 4:

- Create SW1 & SW2 with vlans 10,20,30.
- Configure Fa0/1,Fa0/2 & Fa0/3 as trunk with vlan 10 as native vlan

!SW1/SW2

Vlan 10

Name mgmt

Exit

Vlan 20

Name group1

Exit

Vlan 30

Name group2

Exit

Interface range fa0/1-3

Switchport mode trunk

Switchport trunk native vlan 10

Task 5:

- Configure the DHCP server with three pools 10.0.0.0/8,20.0.0.0/8,30.0.0.0/8
- Configure the Gateway for each pool to be the core switch 10.0.0.1/20.0.0.1 and 30.0.0.1
- Configure the IP of the WLC to be 10.0.0.10 in the DHCP Pool

!DHCP Server

Services>DHCP>On

Create the Pools as follows:

Pool Name:Management

Default Gateway: 10.0.0.1

Stating IP Address: 10.0.0.100

Subnet Mask: 255.0.0.0

Maximum Number of Users: 50

WLC IP Address: 10.0.0.10

Pool Name:group1

Default Gateway: 20.0.0.1

Stating IP Address: 20.0.0.100

Subnet Mask: 255.0.0.0

Maximum Number of Users: 50

Pool Name:group2

Default Gateway: 30.0.0.1

Stating IP Address: 30.0.0.100

Subnet Mask: 255.0.0.0

Maximum Number of Users: 50

Task 6:

- Configure the WLC with two interface ip addresses for group1 and group2 to have ip address 20.0.0.2 and 30.0.0.2 respectively
- Configure WLAN group1 to use the interface of group1 in the WLC which is 20.0.0.2
- Configure WLAN group2 to use the interface of group2 in the WLC which is 30.0.0.2
- Enable Flexconnect for WLAN1 and WLAN2

!WLC
Controller> Interfaces> New
Interface Name: vlan20
VLAN ID: 20

!Then Apply
Physical Information>Port Number> 1
Interface Address>IP Address> 20.0.0.2
Interface Address>Netmask> 255.0.0.0
Interface Address>Gateway> 20.0.0.1

DHCP Information>Primary DHCP Server> 10.0.0.2

!Then Apply

Controller> Interfaces> New
Interface Name: vlan30
VLAN ID: 30

!Then Apply
Physical Information>Port Number> 1
Interface Address>IP Address> 30.0.0.2
Interface Address>Netmask> 255.0.0.0
Interface Address>Gateway> 30.0.0.1

DHCP Information>Primary DHCP Server> 10.0.0.2

!Then Apply

WLANS> WLAN ID 1> Interface > Vlan 20
WLANS> WLAN ID 1> Advanced> Flexconnect>Flexcconnect local switching>Enabled
WLANS> WLAN ID 1> Advanced> Flexconnect>Flexcconnect localAuth>Enabled

WLANS> WLAN ID 2> Interface > Vlan 30
WLANS> WLAN ID 2> Advanced> Flexconnect>Flexcconnect local switching>Enabled
WLANS> WLAN ID 2> Advanced> Flexconnect>Flexcconnect localAuth>Enabled

Task 7:

- Configure the IP Helper-address under vlan 20 and Vlan 30 in the core switch, pointing to the dhcp server ip address 10.0.0.2

!Core-SW

Interface vlan 20

Ip helper-address 10.0.0.2

!

Interface vlan 30

Ip helper-address 10.0.0.2

!Verification

Verify the configuration by going to one of the clients

PC Wireless>Connect>group1(or group2)>Password>Cisco@123

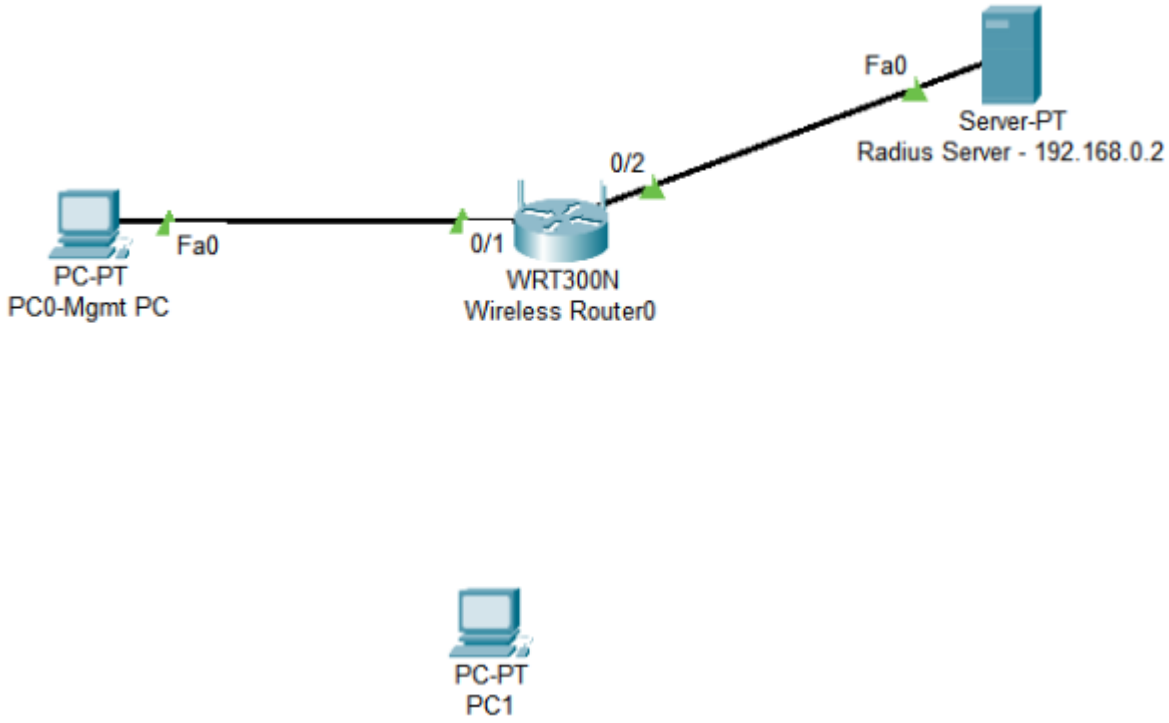
Verify that you are getting IP address from the right dhcp pool

Lab 52
Autonomous Access Point Configuration Using 802.1x

Objective:

The goal of this lab is to configure Cisco Autonomous Access Point using 802.1x authentication.

Diagram:



Preliminary Tasks:

- Connect the diagram as show in the figure
- Let the management PC get ip address from DHCP
- Assign IP Address 192.168.0.2 to the Radius Server

Task 1:

- Enable Radius Server on the server
- Configure the Network Configuration on the Radius Server
- Configure Username and Password on the Radius Server

- Configure the SSID on the Autonomous Access Point
- Configure the Wireless Security to be WPA2 Enterprise
- Specify the IP address of the Radius Server on the Wireless router with the shared secret

!Radius Server
Services>AAA>Service>On
Services>AAA>Network Configuration
Client Name: Wireless Router
Client IP: 192.168.0.1
Secret: cisco
Services>AAA>User Setup
Username: user1
Password: cisco

!Wireless Router
Wireless>Basic Wireless Settings>Network Name (SSID)> NetworkPlus
Wireless>Wireless Security>
Security Mode>WPA2 Enterprise
Radius Server: 192.168.0.2
Shared Secret: cisco

!Verification:
Check the wireless association from the PC Wireless

!PC1
PC Wireless> Profiles>New
Profile Name: NetworkPlus
Select NetworkPlus>Advanced Setup
Wireless Network Name>NetworkPlus>Next
DHCP>Next

Security>WPA2 Enterprise>Next
Login Name: user1
Password: cisco
Next>Save

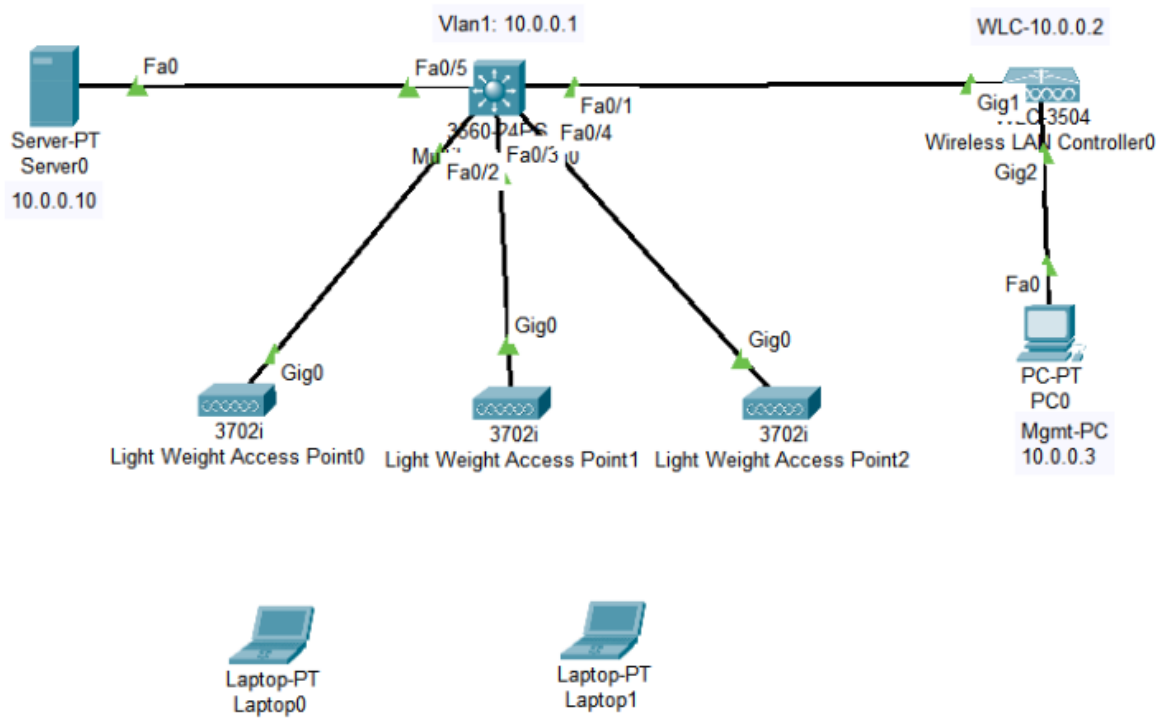
Then Connect the NetworkPlus on the Profile tab

Lab 53
WLC Configuration Using 802.1x

Objective:

The goal of this lab is to configure Cisco WLC using 802.1x authentication.

Diagram:



Preliminary Tasks:

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

Task 1:

- Initialize the WLC by setting the username as admin and password is Cisco@123

- Configure the WLC System name, Management IP address Settings
- Configure the WLC WLAN settings by specifying the SSID and WPA2 Enterprise for Security
- Specify the IP address of the Radius Server and the shared password

!WLC
Username: admin
Password: Cisco@123
System Name: WLC
Management IP address: 10.0.0.2
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.1
Network Name: group1
Security: WPA2 Enterprise
Authentication Server IP Address: 10.0.0.10
Shared Secret: cisco

!Then Save and Aplly

Task 2:

- Configure the Core Switch as DHCP Server in 10.0.0.0/8 network
- Exclude IP addresses from 10.0.0.1 to 10.0.0.100
- Advertise 10.0.0.2 as WLC controller

!Core
Ip dhcp excluded-address 10.0.0.1 10.0.0.100
Ip dhcp pool wireless
Network 10.0.0.0 255.0.0.0
Default-router 10.0.0.1
Option 43 ip 10.0.0.2

Task 3:

- Enable the AAA Service on the Server
- Complete AAA network configuration on the server side
- Complete the user Setup on the server

!Server
Services>AAA>Service>On
Services>AAA>Service>Radius Port>1812
Services>AAA>Network Configuration
Client Name: WLC
Client IP: 10.0.0.2
Secret: cisco
Services>AAA>User Setup
Username: user1
Password: cisco

Task 4:

- Complete the WLC Configuration by enabling the Flexconnect mode (This is because of some limitations on the Packet Tracer)

!WLC
WLANS>WLAN ID 1> Advanced> Flexconnect Local Switching> Enabled
WLANS>WLAN ID 1> Advanced> Flexconnect Local Auth> Enabled

!Verification:

Verify the setup by making sure that Laptops and Wireless clients can get connected using wireless profile creation with the same dot1x parameters and then connect to the WiFI Network.

Quality of Service

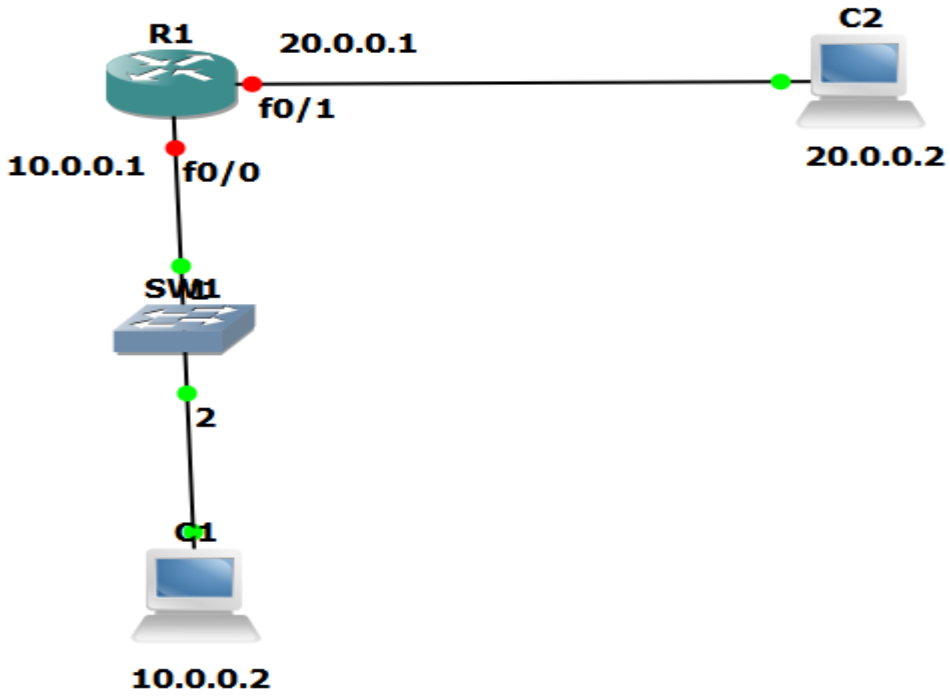
Prepared By:Waleed Adlan-CCIE 41999-waleed_hashim@hotmail.com

Lab 54
Quality of Service

Objective:

The goal of this lab is to configure Quality of Service on Cisco router using MQC (Modular QoS CLI)

Diagram:



Preliminisary Tasks:

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

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

Task 1:

- Configure R1 with policy that limits bandwidth of emails to 512 kbps, and enable random detection based on DSCP
- Put the voice in the priority class with bandwidth of 256 bps
- Scavanger traffic like bittorrent should be policed to 128000 bps
- Rest of traffic should be fair-queued
- The Service Policy should be applied output to the interface of Fastethernet 0/1

```
!R1
Class-map match-any email
Match protocol pop3
Match protocol imap
Match protocol exchange
Match protocol smtp
!
Class-map voice
Match protocol rtp audio
!
Class-map SCAVENGER
Match protocol bittorrent
!
Policy-map network_qos
Class email
Bandwidth 512
Random-detect dscp-based
!
Class voice
Priority 256
!
Class SCAVENGER
Police 128000
Exit
```

!
Class class-default
Fair-queue
!
Interface fa0/0
Service-policy output network_qos

!Verification
!R1
Show policy-map interface fa0/1 output