# HCIP-IENP Lab Manual

**Developed By: Waleed Adlan**

# MPLS VPN Module

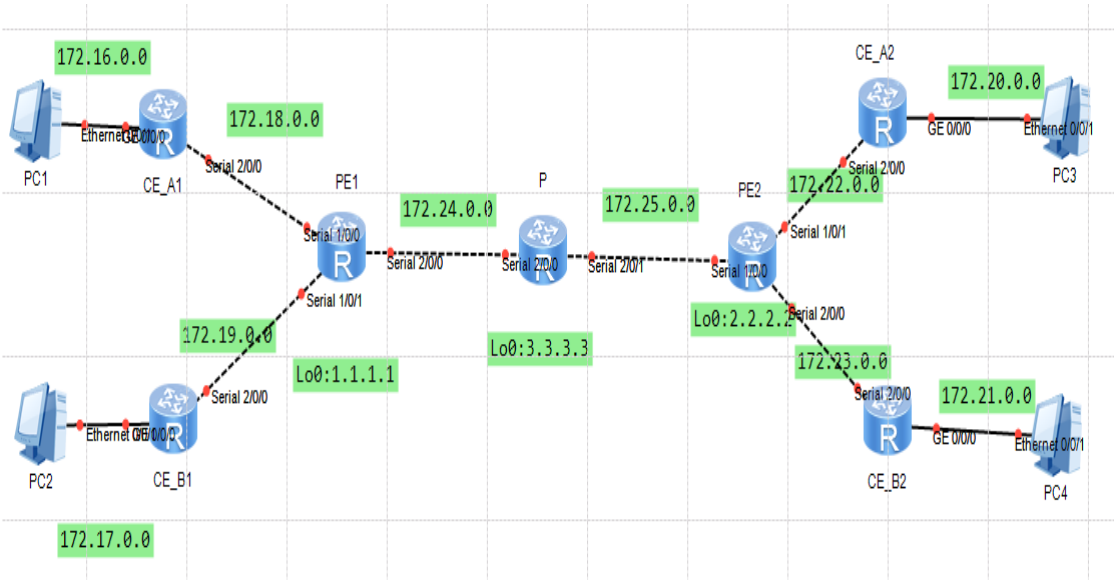
# Lab 1

## MPLS VPN Configuration

**Task 1:**

Connect the below network and assign IP addresses to all interfaces as depicted in the diagram

**Diagram:**




**Task 2:**

Configure Customer routers in BGP, by Putting CE-A1, CE-A2, CE-B1 & CE-B2 in AS 100,200,300,400 respectively. Then in another task put the core into AS 500.

**!CE-A1**

bgp 100

peer 172.18.0.2 as-number 500

ipv4-family unicast

network 172.16.0.0 255.255.0.0

peer 172.18.0.2 enable

**!CE-B1**

bgp 200

peer 172.19.0.2 as-number 500

ipv4-family unicast

network 172.17.0.0 255.255.0.0

peer 172.19.0.2 enable

**!CE-A2**

bgp 300

peer 172.22.0.1 as-number 500

ipv4-family unicast

network 172.20.0.0 255.255.0.0

peer 172.22.0.1 enable

**!CE-B2**

bgp 400

peer 172.23.0.1 as-number 500

ipv4-family unicast

network 172.21.0.0 255.255.0.0

peer 172.23.0.1 enable

**Task 3:**

Configure OSPF on the backbone network, and don't forget to configure the loopback interfaces as their router-id

!PE1

Router id 1.1.1.1

Ospf 1

Area 0

Network 1.1.1.1 0.0.0.0

Network 172.24.0.0 0.0.255.255

!PE2

Router id 2.2.2.2

Ospf 1

Area 0

Network 2.2.2.2 0.0.0.0

Network 172.25.0.0 0.0.255.255

!P

Router id 3.3.3.3

Ospf 1

Area 0

Network 3.3.3.3 0.0.0.0

Network 172.25.0.0 0.0.255.255

Network 172.24.0.0 0.0.255.255

**!Verification:**

**!P**

Display ospf peer brief

```
OSPF Process 1 with Router ID 3.3.3.3
             Peer Statistic Information
 ----------------------------------------------------------------
---------------
 Area Id          Interface                       Neighbor id
State
 0.0.0.0          Serial2/0/0                     1.1.1.1
Full
 0.0.0.0          Serial2/0/1                     2.2.2.2
Full
 ----------------------------------------------------------------
--------------
```

**Task 5:**

Configure two VPN instances in each one of the PEs, and assign the relevant interfaces to the equivalent VPN instance, and also don't forget to configure the RD and route-target.

!PE1

Ip vpn-instance vpn1

Ipv4-family

Route-distinguisher 1:1

Vpn-target 1:1 export-extcommunity

Vpn-target 1:1 import-extcommunity

#

Ip vpn-instance vpn2

Ipv4-family

```
Route-distinguisher 2:2
Vpn-target 2:2 export-extcommunity
Vpn-target 2:2 import-extcommunity
#
Interface serial 1/0/0
Ip binding vpn-instance vpn1
Ip address 172.18.0.2 16
#
Interface serial 1/0/1
Ip binding vpn-instance vpn2
Ip address 172.19.0.2 16
#


!PE2
Ip vpn-instance vpn1
Ipv4-family
Route-distinguisher 1:1
Vpn-target 1:1 export-extcommunity
Vpn-target 1:1 import-extcommunity
#
Ip vpn-instance vpn2
Ipv4-family
Route-distinguisher 2:2
```

Vpn-target 2:2 export-extcommunity

Vpn-target 2:2 import-extcommunity

#

Interface serial 1/0/1

Ip binding vpn-instance vpn1

Ip address 172.22.0.1 16

#

Interface serial 2/0/0

Ip binding vpn-instance vpn2

Ip address 172.23.0.1 16

#

**Task 6:**

Configure MP-BGP between PE1 & PE2, and configure BGP peer between PE and equivalent CE.

!PE1

Bgp 500

Peer 2.2.2.2 as-number 500

Peer 2.2.2.2 connect-interface lo0

Ipv4-family vpnv4

Peer 2.2.2.2 enable

#

Ipv4-family vpn-instance vpn1

Peer 172.18.0.1 as-number 100

#

Ipv4-family vpn-instance vpn2

Peer 172.19.0.1 as-number 200

#

!PE2

Bgp 500

Peer 1.1.1.1 as-number 500

Peer 1.1.1.1 connect-interface lo0

Ipv4-family vpnv4

Peer 1.1.1.1 enable

#

Ipv4-family vpn-instance vpn1

Peer 172.22.0.2 as-number 300

#

Ipv4-family vpn-instance vpn2

Peer 172.23.0.2 as-number 400

#

**Task 7:**

Enable MPLS in the backbone routers (PE1/PE2/P)

!PE1

Mpls lsr-id 1.1.1.1

Mpls

Mpls ldp

Interface s2/0/0

Mpls

Mpls ldp

!PE2

Mpls lsr-id 2.2.2.2

Mpls

Mpls ldp

Interface s1/0/0

Mpls

Mpls ldp

!P

Mpls lsr-id 3.3.3.3

Mpls

Mpls ldp

Interface s2/0/0

Mpls

Mpls ldp

Interface s2/0/1

Mpls

Mpls ldp

# QOS Module

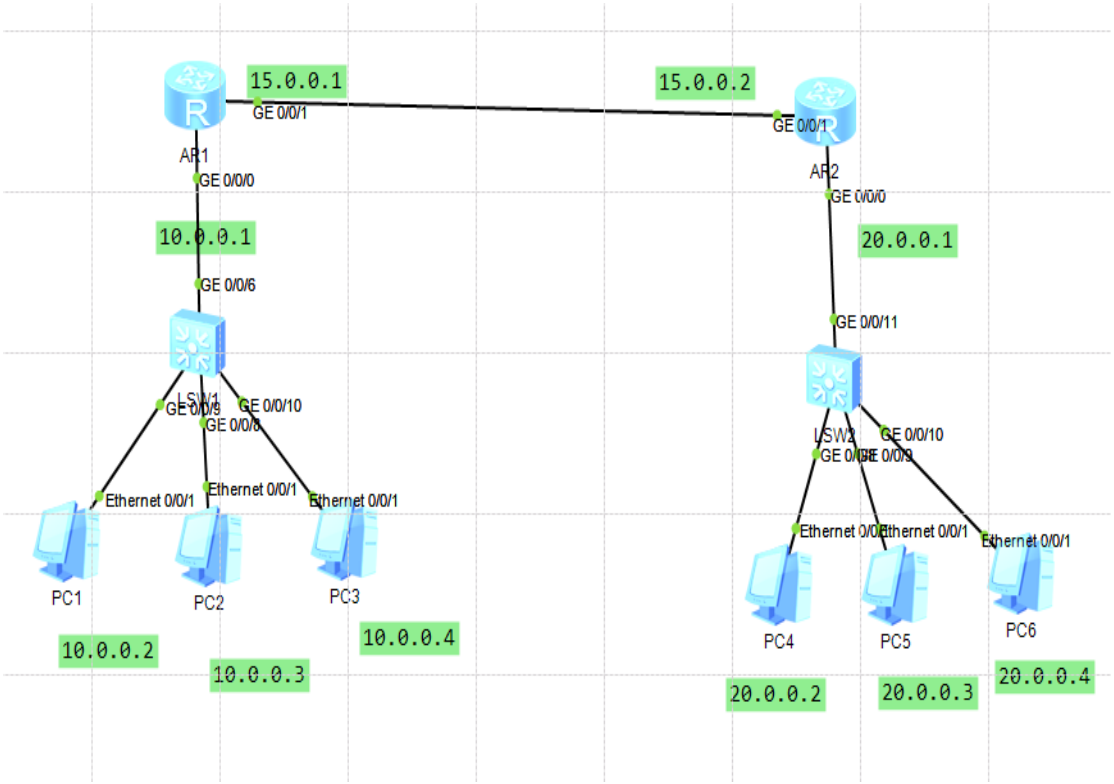
# Lab 3

## Quality of Service Configuration

**Task 1:**

Connect the below network and assign IP addresses to all interfaces as depicted in the diagram, and configure rip to ensure connectivity between PCs

**Diagram:**




**Task 2:**

Configure a traffic policy in AR1 that have three classes:

Class 1 any http traffic sourced from 10.0.0.0 network

Class 2 any ftp traffic sourced from 10.0.0.0 network

Class 3 any voice traffic sourced from 10.0.0.0 network

The policy that applied to interface g0/0/0 inbound, should have the following rules:

Class 1 → Should be assigned 10000 mbps

Class 2 → Should be assigned 5000 mbps

Class 3 → Should be assigned 70000 mbps

**!AR1**

```
acl number 3000
 rule 5 permit tcp source 10.0.0.0 0.255.255.255
destination-port eq www
 rule 10 deny ip
#
acl number 3001
 rule 5 permit tcp source 10.0.0.0 0.255.255.255
destination-port eq ftp
 rule 10 deny ip
#
acl number 3002
 rule 5 permit ip source 10.0.0.0 0.255.255.255
 rule 10 deny ip
#
traffic classifier http operator or
 if-match acl 3000
traffic classifier ftp operator or
 if-match acl 3001
traffic classifier voice operator and
 if-match acl 3002
 if-match dscp ef
#
traffic behavior http
 car cir 10000
traffic behavior ftp
 car cir 5000
traffic behavior voice
 car cir 70000
#
traffic policy policy
 classifier http behavior http
 classifier ftp behavior ftp
 classifier voice behavior voice
#
Interface g0/0/0
Traffic-policy policy inbound
```

```
! Verification:
display traffic-policy applied-record policy
-----------------------------------------------
  Policy Name:   policy
  Policy Index:  0
     Classifier:http     Behavior:http
     Classifier:ftp     Behavior:ftp
     Classifier:voice     Behavior:voice
-----------------------------------------------
 *interface GigabitEthernet0/0/0
    traffic-policy policy inbound
      slot 0    :  success
   Classifier: http
    Operator: OR
    Rule(s) :
     if-match acl 3000
     Behavior: http
      Committed Access Rate:
        CIR 10000 (Kbps), PIR 0 (Kbps), CBS 1880000
(byte), PBS 3130000 (byte)
        Color Mode: color Blind
        Conform Action: pass
        Yellow  Action: pass
        Exceed  Action: discard
   Classifier: ftp
    Operator: OR
    Rule(s) :
     if-match acl 3001
     Behavior: ftp
      Committed Access Rate:
        CIR 5000 (Kbps), PIR 0 (Kbps), CBS 940000 (byte),
PBS 1565000 (byte)
        Color Mode: color Blind
        Conform Action: pass
        Yellow  Action: pass
        Exceed  Action: discard
   Classifier: voice
    Operator: AND
    Rule(s) :
     if-match acl 3002
     if-match dscp ef
     Behavior: voice
      Committed Access Rate:
        CIR 70000 (Kbps), PIR 0 (Kbps), CBS 13160000
(byte), PBS 21910000 (byte)
        Color Mode: color Blind
        Conform Action: pass
        Yellow  Action: pass
        Exceed  Action: discard
-----------------------------------------------
  Policy total applied times: 1.
```

# Firewall Module

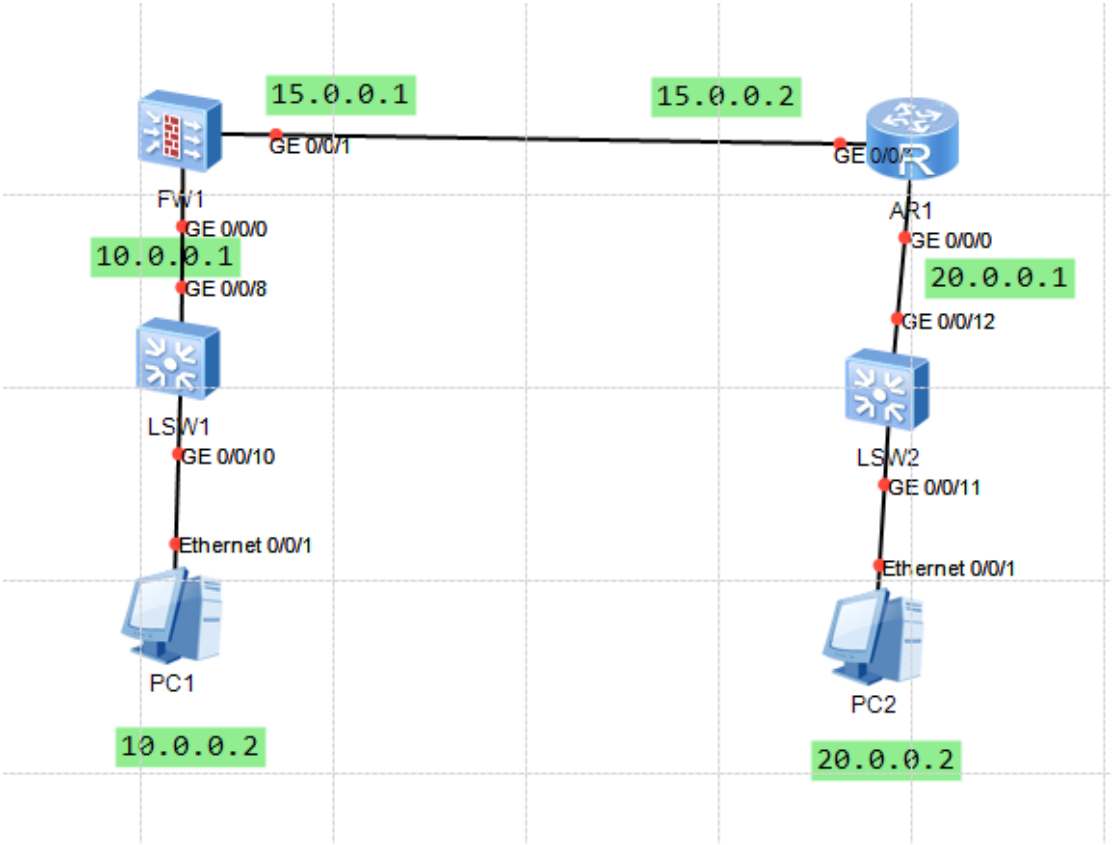
# Lab 4

## Basic Firewall Configuration

**Task 1:**

Connect the below network and assign IP addresses to all interfaces as depicted in the diagram, and configure rip, and make sure the ping is not working, because the firewall default behavior is deny.

**Diagram:**




**Task 2:**

Configure a security policy in the FW1 to allow traffic from network 10.0.0.0 to go through

**!FW**

```
Firewall zone trust
Add interface g0/0/0

Firewall zone untrust
Add interface g0/0/1
#
Security-policy
Rule name policy
Source-zone trust
Destination-zone untrust
Source-address 10.0.0.0 8
Action permit
```

**!Verification:**

The ping should be working between PC and the 20.0.0.0 network.

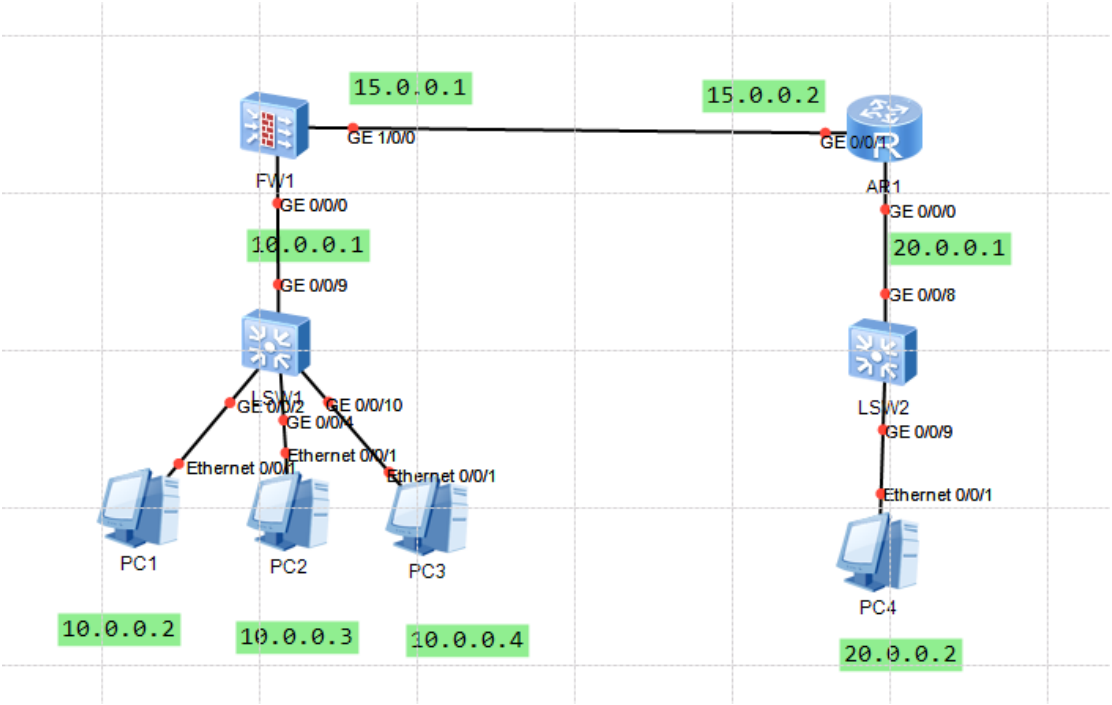
# Lab 5

## NAT Configuration

**Task 1:**

Connect the below network and assign IP addresses to all interfaces as depicted in the diagram, and a default-route in the firewall, and make sure the ping is not working, because the firewall default behavior is deny. Then Configure NAPT to allow all 10.0.0.0 network to be PATed through 15.0.0.3 and 15.0.0.4 public IP addresses.

**Diagram:**




```
!FW
Ip route-static 0.0.0.0 0.0.0.0 g0/0/1
#
Firewall zone trust
Add interface g0/0/0

Firewall zone untrust
Add interface g0/0/1
#
Security-policy
Rule name policy
Source-zone trust
Destination-zone untrust
```

```
Source-address 10.0.0.0 8
Action permit
#
Nat address-group group1 15.0.0.3 15.0.0.4
#
Nat-policy
Rule name policy-nat1
Source-zone trust
Destination-zone untrust
Source-address 10.1.1.0 24
Action nat address-group group1
#
Ip route-static 15.0.0.3 255.255.255.255 null0
Ip route-static 15.0.0.4 255.255.255.255 null0
```

**!Verification:**

Ping should be working from the private network to 20.0.0.2

# VRRP Module

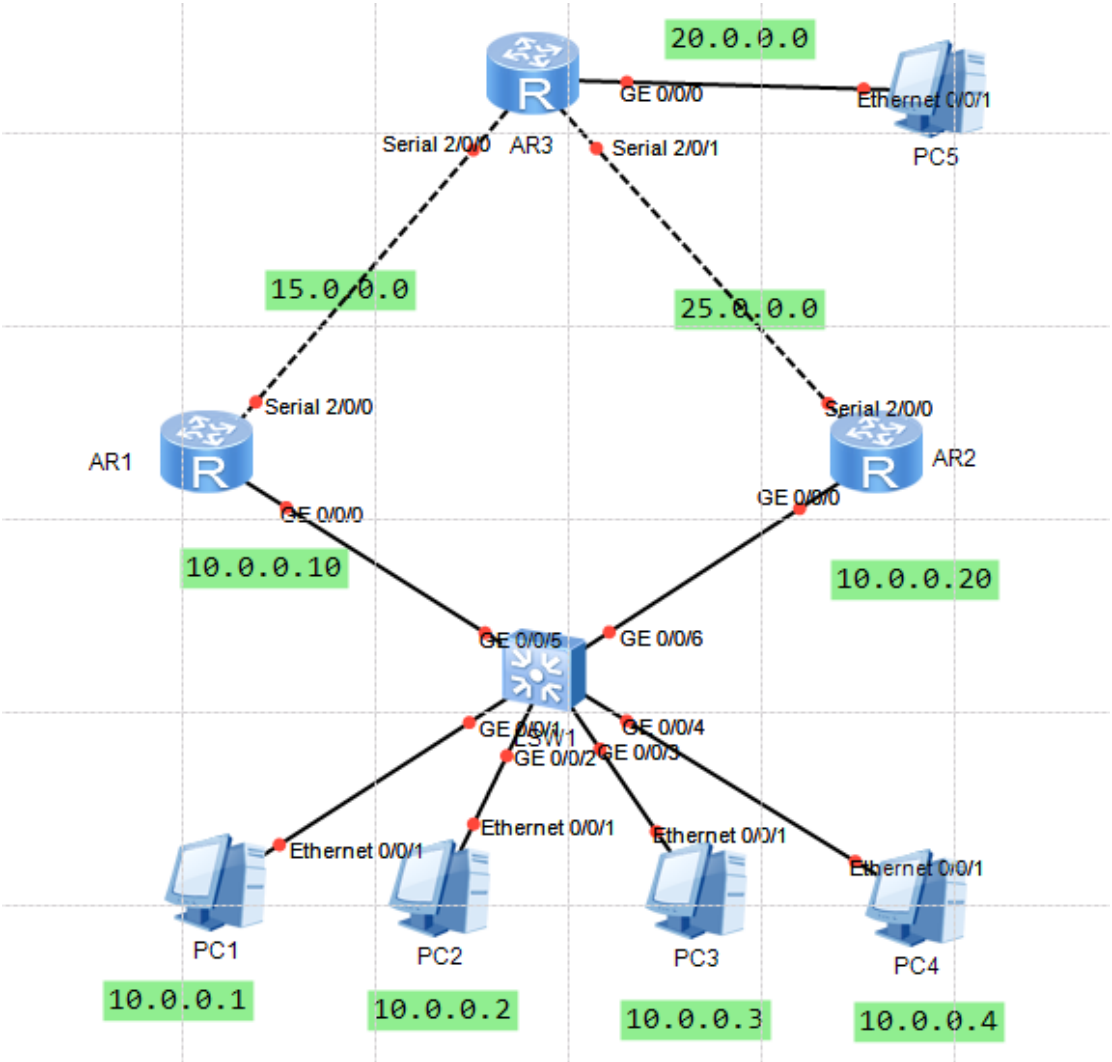
# Lab 6

## VRRP Configuration

**Task 1:**

Connect the below network and assign IP addresses to all interfaces as depicted in the diagram, and configure rip between the three routers.

**Diagram:**



**Task 2:**

Configure VRRP in AR1 & AR2 and make 10.0.0.100 as the virtual ip address, and the default gateway for the PCs. Make AR1 as the master router by putting it a higher priority 200. If you did a trace route from the PCs, the will be leaving the LAN through AR1 (Because it is the master). The ping should be working.

!AR1

Int g0/0/0

Vrrp vrid 1 virtual-ip 10.0.0.100

Vrrp vrid 1 priority 200

!AR2

Int g0/0/0

Vrrp vrid 1 virtual-ip 10.0.0.100

## !Verification:

```
[Huawei]display vrrp brief
Total:1     Master:1     Backup:0     Non-active:0
VRID  State        Interface                Type     Virtual IP
------------------------------------------------------------------
1     Master       GE0/0/0                  Normal   10.0.0.100
[Huawei]
```

**It is showing that AR1 is the Master Router**

**Task 3:**

Configure AR1 to track the interface s2/0/0, if it goes down then decrement the priority of AR1 by 110, So to allow AR2 to be the Master router.

!AR1

Int g0/0/0

Vrrp vrid 1 track interface s2/0/0 reduced 110

**!Verification:**

Shutdown interface s2/0/0 in AR1, and check AR2 it will be the master router.

!AR1

Int s2/0/0

Shutdown

Quit

!

!AR2

Display vrrp brief

```
Total:1     Master:1     Backup:0     Non-active:0
VRID  State        Interface                Type     Virtual IP
------------------------------------------------------------------
1     Master       GE0/0/0                  Normal   10.0.0.100
```

## Task 4:

Configure AR1 & AR2 to form a new virtual router 10.0.0.200. AR1 should be the master router for 10.0.0.100 and backup router for 10.0.0.200, and AR2 is the master for 10.0.0.200 and the backup for 10.0.0.100. The goal behind this step is to allow load balancing by making the gateway of the half of the PCs to be 10.0.0.100, and the other half to be 10.0.0.200.

!AR1

Int g0/0/0

Vrrp vrid 2 virtual-ip 10.0.0.200

!AR2

Int g0/0/0

Vrrp vrid 2 virtual-ip 10.0.0.200

Vrrp vrid 2 priority 200

**!Verification**

!AR1

Display vrrp brief

```
Total:2     Master:1     Backup:1     Non-active:0
VRID  State        Interface                Type     Virtual IP
------------------------------------------------------------------
1     Master       GE0/0/0                  Normal   10.0.0.100
2     Backup       GE0/0/0                  Normal   10.0.0.200
```

PCs 1 & 2 tracert should go through AR1 while PCs 3&4 should go through AR2

# BFD Module

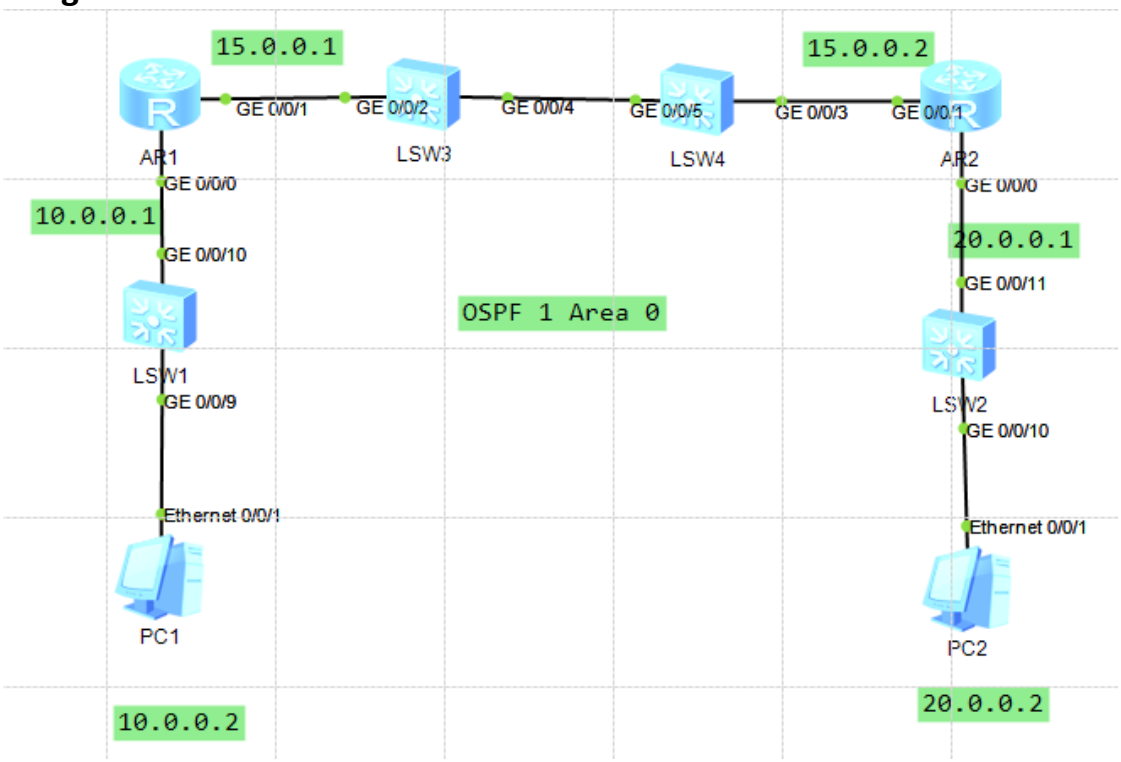
# Lab 7

## BFD Configuration

**Task 1:**

Connect the below network, and configure OSPF area 0 between the two routers and enable BFD tracking between OSPF

**Diagram:**




!AR1

Bfd

#

Ospf 1

Area 0

Network 10.0.0.0 0.255.255.255

Network 15.0.0.0 0.255.255.255

Bfd all-interface enable

!AR2

Bfd

#

Ospf 1

Area 0

Network 20.0.0.0 0.255.255.255

Network 15.0.0.0 0.255.255.255

Bfd all-interface enable

**!Verification:**

!AR1

Display Ospf peer brief

```
<Huawei>display ospf peer brief

        OSPF Process 1 with Router ID 10.0.0.1
                Peer Statistic Information
 ----------------------------------------------------------------------------
-
 Area Id          Interface                       Neighbor id      State
 0.0.0.0          GigabitEthernet0/0/1            20.0.0.1         Full
 ----------------------------------------------------------------------------
-
```

Display BFD session all

```
<Huawei>display bfd session all
--------------------------------------------------------------------------------
----
Local Remote     PeerIpAddr      State     Type        InterfaceName
--------------------------------------------------------------------------------
----

8192  8192       15.0.0.2        Up        D_IP_IF     GigabitEthernet0/0/1
--------------------------------------------------------------------------------
----
     Total UP/DOWN Session Number : 1/0
```

**Task 2:**

Shutdown the link between the two switches, and check the BFD convergence.

**!Verification:**

!AR1

```
<Huawei>display bfd session all
<Huawei>
```

!AR2

```
Display ospf peer brief
```

```
<Huawei>display ospf peer brief

        OSPF Process 1 with Router ID 10.0.0.1
                Peer Statistic Information
 ----------------------------------------------------------------------------
-
 Area Id          Interface                       Neighbor id      State
 -------------
```