NETWORK DESIGN REPORT

Module CCNA COHORT 9

Lecturer In Charge – ENG.Esraa-Hasan

BY – Farah Mohammad

Table of Contents

Network design scenario

• A new infrastructure consists of Head Quarter (HQ) and three branches (Amman, Istanbul, and Beirut) with different requirements.

• The Head Quarter (HQ) must have a server to support NTP and Syslog to save traps and messages in the company.

• HQ will have vlan5 include a WLC with one LAP for wireless clients

• The HQ will have to provide wired communication for 21 machines as a basic workplace

• The Multilayer Switch will be situated In the heart of the Head Quarters, One will be active and the other standby. Therefore, both are connected by EtherChannel (3 fast Ethernet ports) its type is a trunk.

• The Multilayer Switches will be connected with the router by "Router on a stick" and configuring HSRP.

• The three branches (Amman, Istanbul, and Beirut) will be similar , Each branch will have to provide wired communication for10 machines as a basic workplace consists of 2 switches and 2 routers as HSRP , the switches are connected by EtherChannel (3 fast Ethernet ports)its type is a trunk.

• The HQ area 0: will be connected with ISP (ZAIN & ORANGE)

• The AMMAN branch area 1, the Beirut branch area 2, and the Istanbul branch area 3: will be connected with ISP (ZAIN & ORANGE).

Head Quarter network design diagram

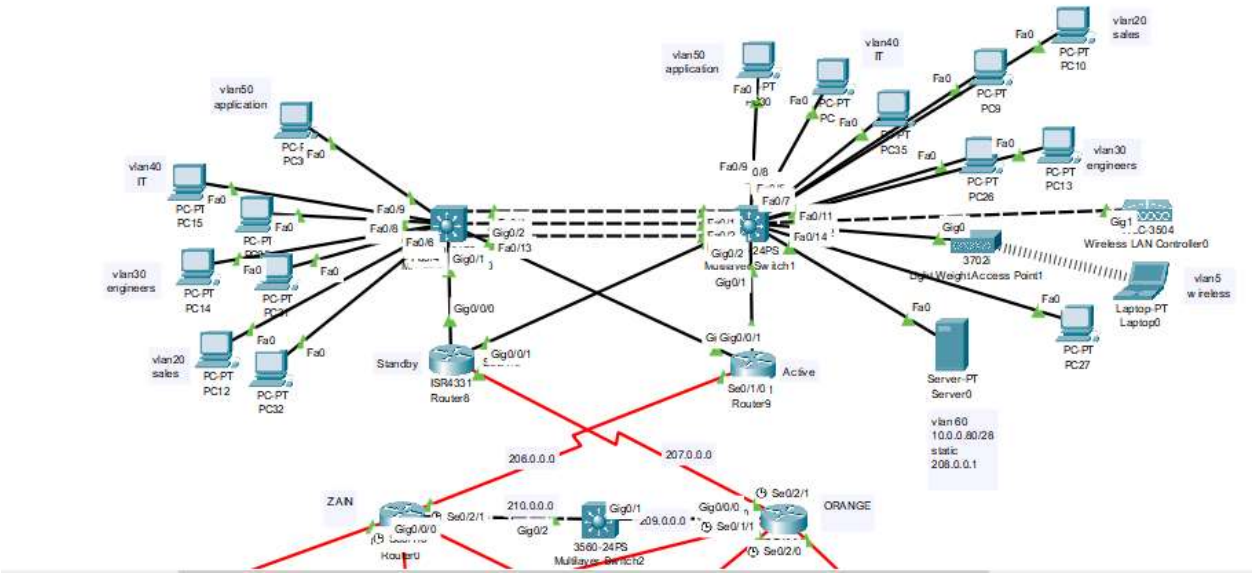

Fig 1-HQ topology.

Branches interconnected design diagram

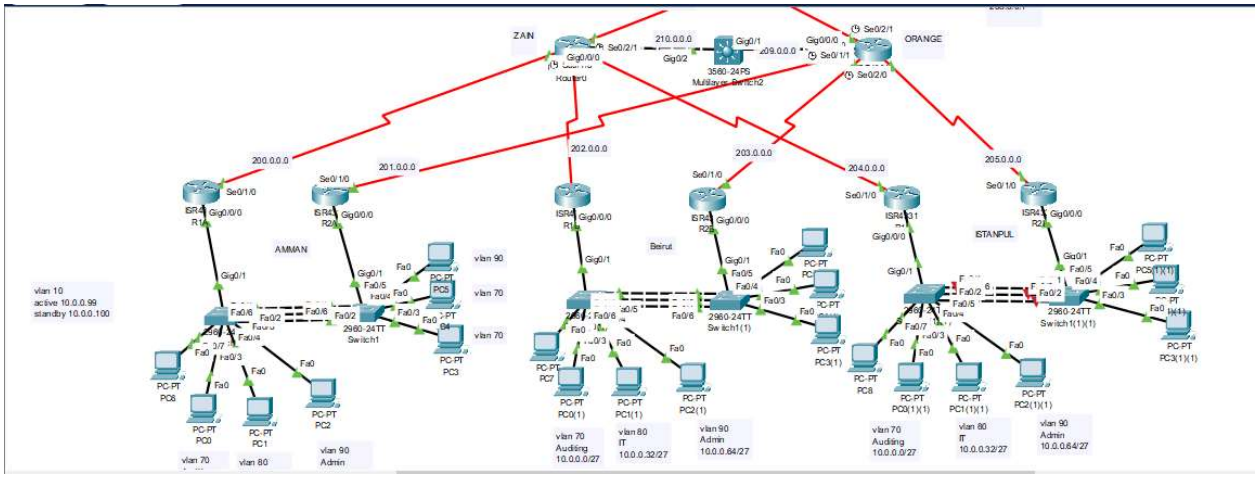

Fig 2-Three branches (Amman, Istanbul, and Beirut) topology.

✓ In HQ the PC full connections with each other by VLANs.

✓ All devices have an IPv4,IPv6 add from DHCP.

✓ In each branch the PC full a Connection to each other by VLANs.

✓ All required types of security have been activated on routers and switches.[user name: FARAH, password :shqair]

✓ Redundancy for all network.

✓ Apply OSPF on routers.

Assumptions made on the connection between branches and HQ

1. Take the time clock for all sites from the server located in the HQ, as it stores traps and messages on it.

2. HQ to Branch (Amman, Istanbul, and Beirut) Connection made of serial (secure, dedicated connection required)by NAT "PAT".

3. Branch AMMAN can reach the HQ network using VPN over the Internet.

Configurations Considerations of this network and Assumptions made

***Branch Configurations:**

-DHCPv4&6: Dynamic Host Considerations Protocol.

Tack the Ip add from router and use statfull for virgin 6.

```
!
ip dhcp excluded-address 10.0.0.1 10.0.0.10
ip dhcp excluded-address 10.0.0.33 10.0.0.43
ip dhcp excluded-address 10.0.0.65 10.0.0.75
!
ip dhcp pool vlan70
 network 10.0.0.0 255.255.255.224
 default-router 10.0.0.2
ip dhcp pool vlan80
 network 10.0.0.32 255.255.255.224
 default-router 10.0.0.34
ip dhcp pool vlan90
 network 10.0.0.64 255.255.255.224
 default-router 10.0.0.66
```

Fig 3-DHCPv6 for VLANs

```
ip cef
no ipv6 cef
!
ipv6 dhcp pool VLAN80
 address prefix 2001:db8:10:10::/64 lifetime 172800 86400
!
ipv6 dhcp pool VLAN90
 address prefix 2001:db8:10:11::/64 lifetime 172800 86400
!
ipv6 dhcp pool VLAN70
 address prefix 2001:db8:1::/64 lifetime 172800 86400
!
!
```

Fig 4-DHCPv4 for VLANs

-Switchport mode Access & Trunk:

Switchport mode Access :between switch &PC.

Switchport mode Trunk :between switch& switch in chaneel1.

Switchport mode Trunk :between switch &router.

```
!
interface Port-channel1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/3
 switchport access vlan 70
 switchport mode access
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
interface FastEthernet0/4
 switchport access vlan 80
 switchport mode access
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
interface FastEthernet0/5
 switchport access vlan 90
 switchport mode access
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 --More--
```

Fig 5-switch port mode

-Security in switch, router for port and device:

User name: FARAH , Password: shqair for remote access.

using enable password, SSH in router and switch ,crypto key (RSA 2048), port security ,

max mac=4 by sticky, violation restrict.

```
banner motd ^C Authorized A Access Only!^C
!
!
!
line con 0
 password 7 0832445F081017
 login
!
line vty 0 4
 password 7 0832445F081017
 login local
 transport input ssh
line vty 5 15
 password 7 0832445F081017
 login local
 transport input ssh
!
```

Fig 6- Security in switch, router

```
switchport port-security maximum 4
switchport port-security mac-address sticky
switchport port-security violation restrict
shutdown
```

Fig 7- Security in port

-Ethercannel between switches DTP[PAG-P]:

Use 3 fast Ethernet[1,2,6] they were encapsulated in chaneel1 and activate the negotiation in just one switch, and assign mode trunk.

```
interface Port-channel1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
 channel-group 1 mode desirable
!
```

```
interface FastEthernet0/6
 switchport trunk native vlan 99
 switchport mode trunk
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 channel-group 1 mode desirable
```

Fig 8- Ethercannel.

-Router on a stick ,Redundancy HSRP ,Sub interface

```
interface GigabitEthernet0/0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/0.10
 encapsulation dot1Q 10
 ip address 10.0.0.97 255.255.255.224
 standby 10 ip 10.0.0.98
 standby 10 priority 150
 standby 10 preempt
!
interface GigabitEthernet0/0/0.70
 encapsulation dot1Q 70
 ip address 10.0.0.1 255.255.255.224
 ip nat inside
 ipv6 address 2001:DB8:1::1/64
 ipv6 nd managed-config-flag
 ipv6 dhcp server VLAN70
 standby 1 ip 10.0.0.2
 standby 1 priority 101
 standby 1 preempt
!
interface GigabitEthernet0/0/0.80
 encapsulation dot1Q 80
 ip address 10.0.0.33 255.255.255.224
 ip nat inside
 ipv6 address 2001:DB8:10:10::1/64
 ipv6 nd managed-config-flag
 ipv6 dhcp server VLAN80
 standby 2 ip 10.0.0.34
 standby 2 priority 101
 standby 2 preempt
!
interface GigabitEthernet0/0/0.90
 encapsulation dot1Q 90
 ip address 10.0.0.65 255.255.255.224
 ip nat inside
```

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Gig	10	150	P	Active	local	unknown	10.0.0.98
Gig	1	101	P	Active	local	10.0.0.1	10.0.0.2
Gig	2	101	P	Active	local	10.0.0.33	10.0.0.34
Gig	3	101	P	Active	local	10.0.0.65	10.0.0.66

Fig 9- HSRP ,Sub interface.

-Routing protocol :OSPF 10

Branch AMMAN area 1

Branch BEIRUT area 2

Branch ISTANPUL area 3

```
router ospf 10
 log-adjacency-changes
 passive-interface GigabitEthernet0/0/0
 passive-interface GigabitEthernet0/0/0.70
 passive-interface GigabitEthernet0/0/0.80
 passive-interface GigabitEthernet0/0/0.90
 network 200.0.0.0 0.0.0.255 area 1
!
```

```
router ospf 10
 log-adjacency-changes
 passive-interface GigabitEthernet0/0/0.70
 passive-interface GigabitEthernet0/0/0.80
 passive-interface GigabitEthernet0/0/0.90
 network 201.0.0.0 0.0.0.255 area 1
!
```

```
router ospf 10
 log-adjacency-changes
 passive-interface GigabitEthernet0/0/0.70
 passive-interface GigabitEthernet0/0/0.80
 passive-interface GigabitEthernet0/0/0.90
 network 202.0.0.0 0.0.0.255 area 2
!
```

```
router ospf 10
 log-adjacency-changes
 passive-interface GigabitEthernet0/0/0.70
 passive-interface GigabitEthernet0/0/0.80
 passive-interface GigabitEthernet0/0/0.90
 network 203.0.0.0 0.0.0.255 area 2
!
```

```
router ospf 10
 log-adjacency-changes
 passive-interface GigabitEthernet0/0/0.70
 passive-interface GigabitEthernet0/0/0.80
 passive-interface GigabitEthernet0/0/0.90
 network 204.0.0.0 0.0.0.255 area 3
!
```

```
router ospf 10
 log-adjacency-changes
 passive-interface GigabitEthernet0/0/0.70
 passive-interface GigabitEthernet0/0/0.80
 passive-interface GigabitEthernet0/0/0.90
 network 205.0.0.0 0.0.0.255 area 3
!
```

Fig 9-OSPF in Branches.

-NAT(PAT).

Translation the privet IP to public IP

```
R1A#Show ip nat t
R1A#Show ip nat s
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/1/0
Inside Interfaces: GigabitEthernet0/0/0.70 , GigabitEthernet0/0/0.80 ,
GigabitEthernet0/0/0.90
Hits: 0  Misses: 92
Expired translations: 4
Dynamic mappings:
-- Inside Source
access-list 70 pool zain refCount 0
 pool zain: netmask 255.255.255.0
       start 200.0.0.1 end 200.0.0.1
       type generic, total addresses 1 , allocated 0 (0%), misses 0
-- Inside Source
access-list 80 pool zain refCount 0
 pool zain: netmask 255.255.255.0
       start 200.0.0.1 end 200.0.0.1
       type generic, total addresses 1 , allocated 0 (0%), misses 0
-- Inside Source
access-list 90 pool zain refCount 0
 pool zain: netmask 255.255.255.0
       start 200.0.0.1 end 200.0.0.1
       type generic, total addresses 1 , allocated 0 (0%), misses 0
```

Fig 10-NAT in AMMAN.

-ACL (only IT vlan can SSH in the network device in ISTANBUL branch)

```
ip access-list standard ssh2
 permit 10.0.0.32 0.0.0.31
 deny any
!
banner motd ^CAuthorized a access only!^C
!
!
!
!
logging 208.0.0.1
line con 0
 password shqair
 login
!
line aux 0
!
line vty 0 4
 access-class ssh2 in
 password shqair
 login local
```

Fig 11-ACL in ISTANBUL.

**** All requirements are met on the Branches****

*** HQ And SPI Configurations:**

-Router CONFIG..[OSPF, NTP, NAT, VPN]

```
router ospf 10
 log-adjacency-changes
 passive-interface GigabitEthernet0/0/0
 network 206.0.0.0 0.0.0.255 area 0
!
ip nat pool zain 206.0.0.1 206.0.0.1 netmask 255.255.255.0
ip nat inside source list 1 pool zain overload
ip nat inside source list 2 pool zain overload
ip nat inside source list 20 pool zain overload
ip nat inside source list 30 pool zain overload
ip nat inside source list 40 pool zain overload
ip nat inside source list 5 pool zain overload
ip nat inside source list 50 pool zain overload
ip nat inside source static 10.0.0.81 208.0.0.1
ip classless
ip route 10.0.0.0 255.255.255.240 GigabitEthernet0/0/0
ip route 10.0.0.16 255.255.255.240 GigabitEthernet0/0/0
ip route 10.0.0.32 255.255.255.240 GigabitEthernet0/0/0
ip route 10.0.0.64 255.255.255.240 GigabitEthernet0/0/0
ip route 10.0.0.48 255.255.255.240 GigabitEthernet0/0/0
ip route 10.0.0.80 255.255.255.240 GigabitEthernet0/0/0
!
```

```
interface Tunnel0
 ip address 10.20.0.1 255.255.255.252
 mtu 1476
 tunnel source Serial0/1/0
 tunnel destination 200.0.0.1
!
interface GigabitEthernet0/0/0
 ip address 10.10.0.2 255.255.255.240
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/1
 ip address 10.10.20.2 255.255.255.240
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/1/0
 ip address 206.0.0.1 255.255.255.0
 ip nat outside
!
interface Serial0/1/1
 no ip address
 clock rate 2000000
 shutdown
```

```
!
access-list 20 permit 10.0.0.0 0.0.0.15
access-list 30 permit 10.0.0.16 0.0.0.15
access-list 40 permit 10.0.0.32 0.0.0.15
access-list 50 permit 10.0.0.48 0.0.0.15
access-list 5 permit 10.0.0.64 0.0.0.15
access-list 1 permit 10.10.0.0 0.0.0.15
access-list 2 permit 10.10.20.0 0.0.0.15
!
no cdp run
!
banner motd ^CAuthorized a access only!^C
!
!
!
!
logging 208.0.0.1
logging 10.0.0.81
```

Fig 12-config in QH router Active.

```
router ospf 10
 log-adjacency-changes
 network 200.0.0.0 0.0.0.255 area 1
 network 202.0.0.0 0.0.0.255 area 2
 network 204.0.0.0 0.0.0.255 area 3
 network 206.0.0.0 0.0.0.255 area 0
 network 210.0.0.0 0.0.0.3 area 0
!
ip classless
ip route 208.0.0.0 255.255.255.0 Serial0/2/1
!
ip flow-export version 9
!
!
!
banner motd ^CAuthorized a access only!^C
!
!
!
!
logging 208.0.0.1
line con 0
 password shqair
 login
!
line aux 0
!
line vty 0 4
 password shqair
 login
!
!
ntp server 208.0.0.1
```

Fig 13- config in ISP router Active.

- Multilayer Switch CONFIG..[DHCPv4,6, ETHERCANNEL (fast Ethernet 1,2,13), ACL in vlan50, HSRP, NTP& Syslog server, Violation Restrict , port security ,max mac 4 by sticky]

```
!
interface Port-channel1
 switchport trunk native vlan 99
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode desirable
!
```

```
swl#show standby b
                    P indicates configured to preempt.
                    |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
V15         5    150   Active   local           10.0.0.67       10.0.0.66
V120        1    101 P Active   local           10.0.0.3        10.0.0.2
V130        2    101 P Active   local           10.0.0.19       10.0.0.18
V140        3    101 P Active   local           10.0.0.35       10.0.0.34
V150        4    101 P Active   local           10.0.0.51       10.0.0.50
V160        60   150 P Active   local           10.0.0.84       10.0.0.83
swl#
```

```
!
interface FastEthernet0/13
 switchport trunk native vlan 99
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode desirable
!
```

Fig 13- SWL3 Config

Wireless access is ensured for VLAN 5 IN HQ

The Wells Infrastructure topology was built of the ESS type using three Fast Ethernet cables with a range of 10-12

Create a private urine for vlan5 via DHCP 10.0.0.64 255.255.255.240 on the multiswitch.

Fast Ethernet 10: is connected to the PC responsible for the configuration of the controller with Ip add 192.168.1.10 255.255.255.0 and access to the controller is done through the username ADMIN and the password Admin123 through the https protocol.

Fast Ethernet 12 :connected with the controller gave an Ip add of 192.168.1.2 255.255.255.0 on Port Gig 0 and then it was changed to Ip add 192.168.1.20 255.255.255.0 and an SSD was made: HQ-wireless with PSK security and at the same time it was given to the AP Range DHCP 192.168.1.10 - 192.186.1.19 and activate WLAN as

B id = 1 ccna9 After that, connect the AP to electricity, and activate the DHCP on it

Fast Ethernet 11: is connected to the AP

Name-vlan: wirless

ID-vlan:10.0.0.64 0.0.0.15

Active interface IP :10.0.0.65

Standby interface IP:10.0.0.67

Virtual interface IP:10.0.0.66

VLAN description and IP Address scheme used in this network design

HQ VLANS

NAME	ID	IP-Active	IP-Standby	IP-Virtual	Devices-nu	interface
Native 99	99				-	Fa0/13, Fa0/1, Fa0/2
Management 10	10				-	-
Sales 20	10.0.0.0/28	10.0.0. 1	10.0.0.3	10.0.0.2	3	Fa0/3, Fa0/4, Fa0/5
Eng 30	10.0.0.16/28	10.0.0.17	10.0.0.19	10.0.0.18	2	Fa0/6, Fa0/7
IT 40	10.0.0.32/28	10.0.0.33	10.0.0.35	10.0.0.34	1	Fa0/8
App 50	10.0.0.48/28	10.0.0.49	10.0.0.51	10.0.0.50	1	Fa0/9
VLAN0060	10.0.0.80/28	10.0.0.82	10.0.0.83	10.0.0.84	1(server)	Fa0/14

Tab 1-vlan in multilayer switch (HQ).

*Network between Active multilayer switch and active Router: 10.10.0.0/28

*Network between Active multilayer switch and Standby Router: 10.10.10.0/28

*Network between Standby multilayer switch and Active Router: 10.10.20.0/28

*Network between Standby multilayer switch and Standby Router: 10.10.0.0/28

BRANCHS VLANS

NAME	ID	IP-Active	IP-Standby	IP-Virtual	Devices-nu	interface
managment 10	10.0.0.96	10.0.0.99	10.0.0.100	10.0.0.98	-	
Auditing 70	10.0.0.32/27	10.0.0.33	10.0.0.33	10.0.0.34	2	Fa0/3, Fa0/7
IT 90	10.0.0.0/27	10.0.0.1	10.0.0.1	10.0.0.2	1	Fa0/4
Admin 80	10.0.0.64/27	10.0.0.65	10.0.0.65	10.0.0.66	2	Fa0/5
native 99	-	-	-	-	-	Fa0/1-2, Fa0/6

*IP default for Active and Standby switch :10.0.0.98

Network Protocols used in this Network Design

***Routing**

1. Static Routing – Static routes are configured on gateway/core routers of each branches and in main site, to route the traffic from inside network to another branch network. As the next hop (IP of each branch network) is known this can be used. Since this is a small network using static routes are simple and easy. It's secure because no any routing advertisements are exchanged between neighbors and computing resources are conserved because no routing algorithm or update mechanisms required.

2. Default routing – This is configured on core routers to route the traffic from inside network to ISP router for unknown traffic (towards internet)

3. Inter VLAN routing – Core routers are configured to route the traffic between different

VLAN in the network. The traffic will reach the core routers from core switch which are connected by trunk link. All VLAN networks will be shown as directly connected routes in routing table (sub interfaces are used).

***DHCP (Dynamic Host Configuration Protocol)**

DHCP service is installed in the DHCP server which resides in server room. IP address pool for different VLAN will be created in DHCP server. So DHCP server dynamically assign the IP address to the hosts in the network. Static IP address that will be used with in the VLAN can be removed from the IP address pool (excluded address) in DHCP server. Main advantage of using this protocol is reliable IP address configuration to hosts (reduce configuration errors caused by manual IP assignment), and reduced network administration (centralized management)

***NAT (Network Address Translation)**

Class B private range IP address is used with in inside this network. But the hosts cannot communicate with this private IP address over Internet because private IP address are not routable in Internet. Therefore, they must be converted to public IP address for the communication over Internet. So, NAT becomes an essential part of this network design. PAT (Port Address Translation) is used in the core router to map one/two public IP address provided by ISP to map the private IP address used inside the network. By using PAT, we can save the number of public IP address used for the translation. Static NAT will be used for communication of web server over the Internet. Because the web server should be visible and accessible from the Internet. By using NAT, public IPv4 address can be saved and internal IP plan of this network can be hidden from the outside world.

***HSRP (Rapid Standby Router Protocol)**

HSRP is configured by combining all two primary routers in this network. Therefore, the two primary routers will act as one virtual router for the internal hosts. Primary router 1 will take over as the active router while the other will take over as the backup router. If the active router fails, the standby router takes over the role of the active router. Since the new forwarding router uses the same MAC and IP addresses, the hosts can connect without any interruption until one primary router fails.

***VLAN (Virtual Local Area Network)**

There are different VLANs created across this network. Each VLAN for different floor and separate VLAN for network in each branch. VLAN also provides a layer of network security and cost reduction option by logically separating hosts which is connected to the same switch (no need for additional switches). Here each VLAN is assigned with different IP address subnet.