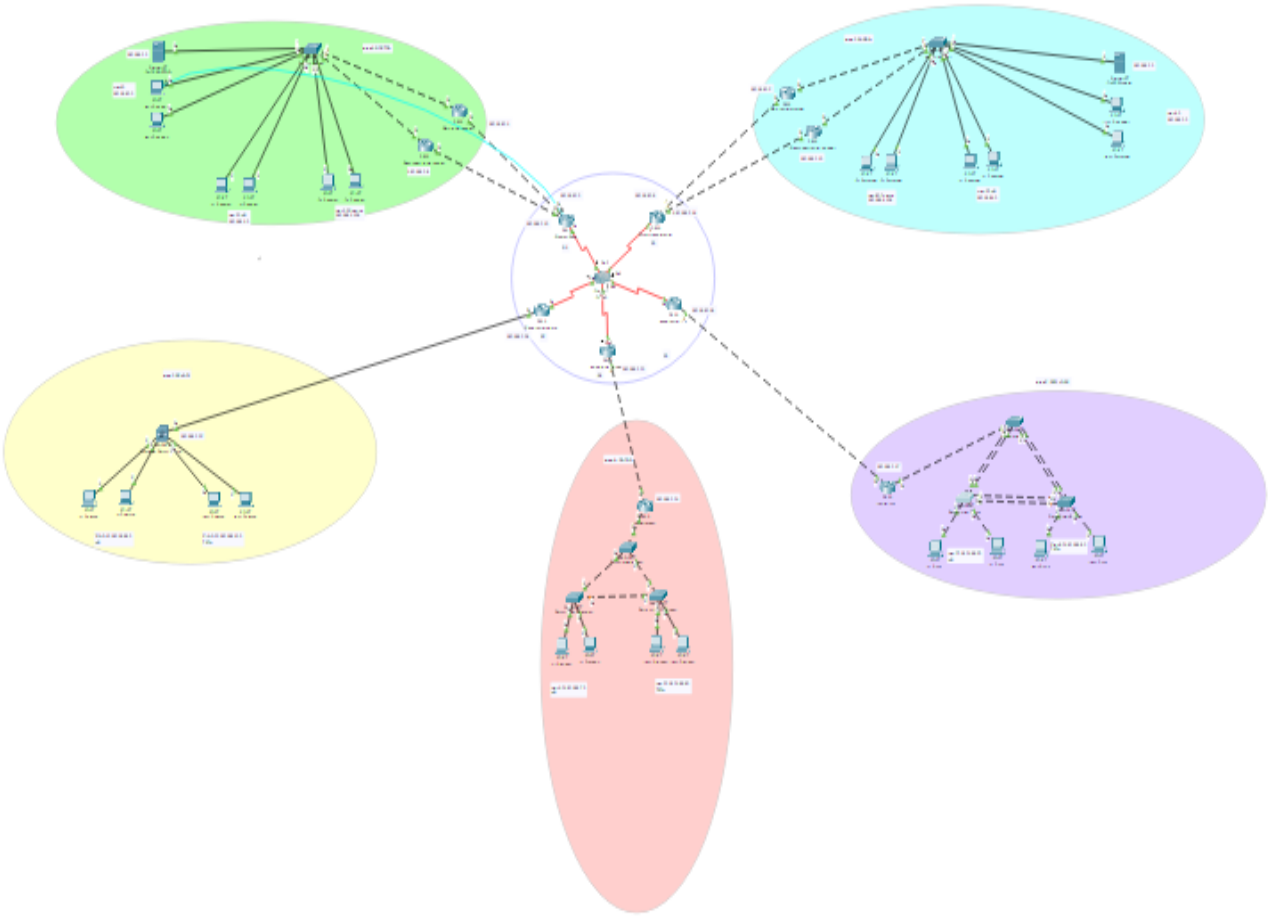
PROJECT 2 – REPORT

1. PROJECT DESIGN

HIGH LEVEL DIAGRAM:



Design:

The corporate organization has geographically separated five offices. Each office communicates with each other using frame relay. Each of them is considered to be an area to implement OSPF to route the packets using the shortest path. The area specification is:

Area 1: Boston, Area 2: Mumbai, Area 3: Beijing, Area 4: London, Area 5: New York.

VLAN is used to separate departments within each location. This helps to subdivide a physical network into individual broadcast domains. Each VLAN has PCs in a unique subnet. A router is needed to route the packets from and to the specific VLAN.

The DHCP server in Boston assigns IP addresses for Boston and Mumbai. The DHCP server of Mumbai assigns IP addresses for Beijing, London and New York. All locations have Technical and HR departments. Boston and Mumbai have additional Finance departments.

COST OF EQUIPMENTS:

#Routers – 12

Total cost of routers: 500*12= $6000

#Switches – 8

Total cost of switches: 300*8=$2400

#DHCP Servers – 2

Total cost of DHCP servers: 150*2 =$300

Cost of Multi-Layer Switch: $500

Cost of copper straight-through cable per feet: $1.6

Cost of copper cross-over cable per feet: $2.4

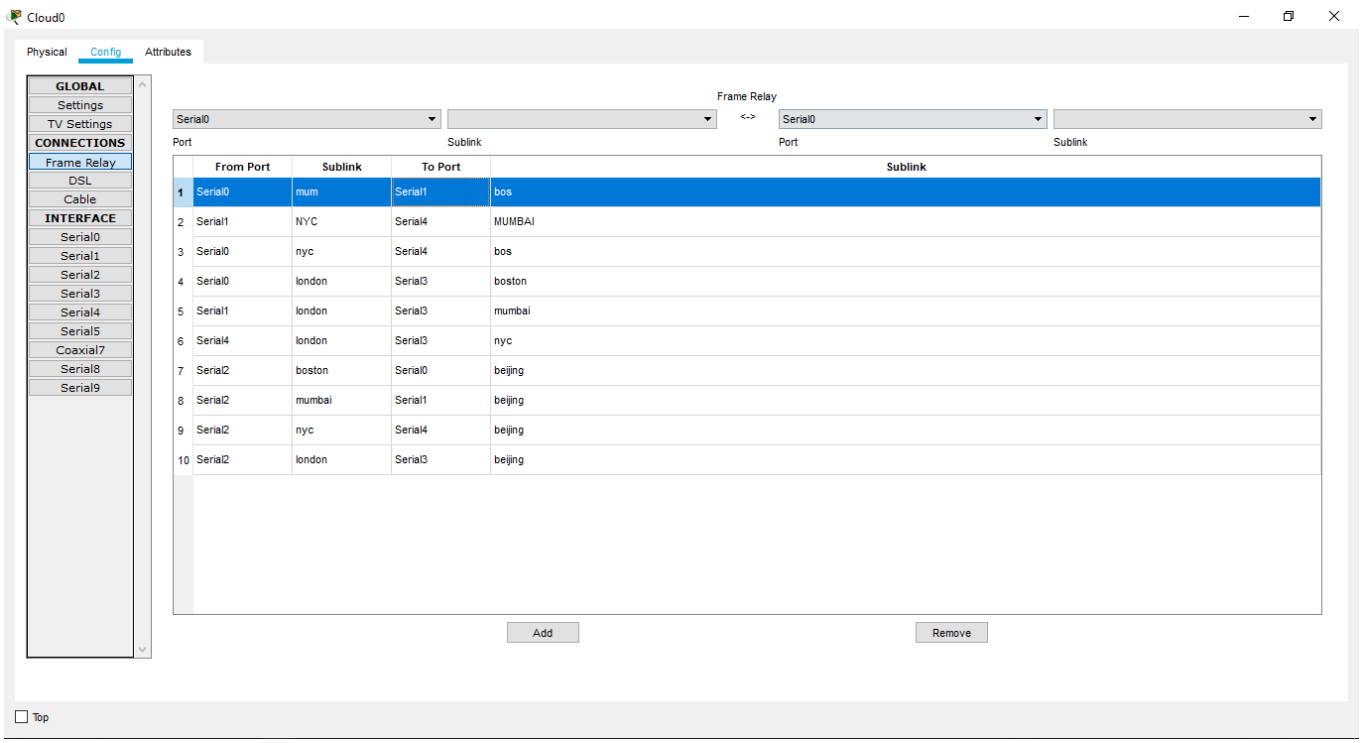
2. NETWORK OPTIMIZATION

COST OPTIMIZATION OF NETWORK:

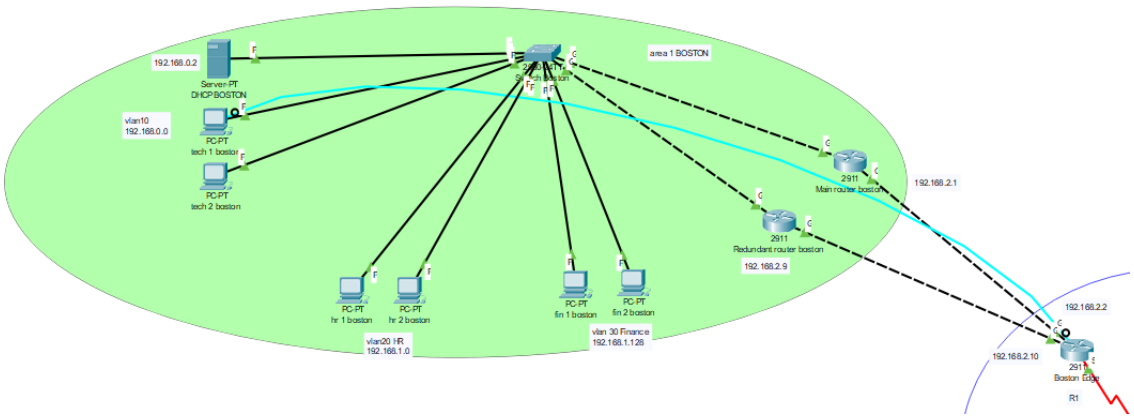
To optimize cost of the network some factors had been taken into consideration. Only 2 DHCP servers are used for all 5 cities. VLANS are used to minimize the number of switches required. Only one switch is used for multiple departments. By following these optimizations, the total cost of the network is reduced.

DETAILED NETWORK ARCHITECTURE:

Frame relay is implemented in the backbone [area 0] and its configuration is as follows:



Boston:

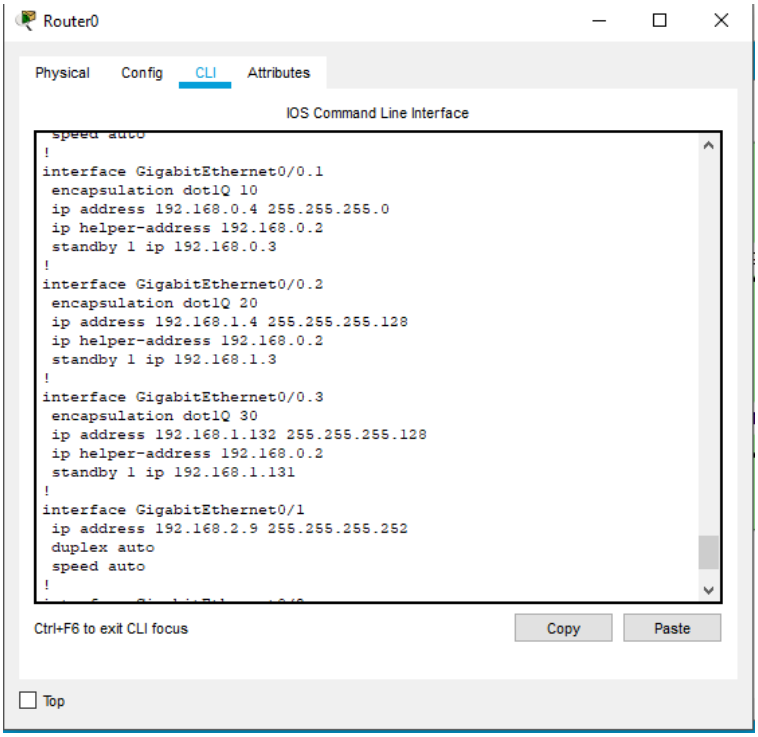


Configuration of main router:

```
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.1
 encapsulation dot1Q 10
 ip address 192.168.0.3 255.255.255.0
 ip helper-address 192.168.0.2
 ip access-group 100 in
 standby 1 ip 192.168.0.3
 standby 1 priority 105
 standby 1 preempt
 standby 1 timers 2 6
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 20 native
 ip address 192.168.1.1 255.255.255.128
 ip helper-address 192.168.0.2
 ip access-group 100 in
 standby 1 ip 192.168.1.3
 standby 1 priority 105
 standby 1 preempt
 standby 1 timers 2 6
!
interface GigabitEthernet0/0.3
 encapsulation dot1Q 30
 ip address 192.168.1.129 255.255.255.128
 ip helper-address 192.168.0.2
 ip access-group 100 in
 standby 1 ip 192.168.1.131
 standby 1 priority 105
 standby 1 preempt
 standby 1 timers 2 6
!
interface GigabitEthernet0/1
 ip address 192.168.2.1 255.255.255.252
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 192.168.0.0 0.0.0.255 area 1
 network 192.168.1.0 0.0.0.127 area 1
 network 192.168.1.128 0.0.0.127 area 1
 network 192.168.2.0 0.0.0.3 area 0
!
```

```
ip classless
!
ip flow-export version 9
!
!
access-list 100 permit ip host 192.168.0.2 any
access-list 100 permit icmp any 192.168.1.128 0.0.0.127 echo-reply
access-list 100 permit icmp any 192.168.4.128 0.0.0.127 echo-reply
access-list 100 deny ip 192.168.0.0 0.0.0.255 192.168.1.128 0.0.0.127
access-list 100 deny ip 192.168.0.0 0.0.0.255 192.168.4.128 0.0.0.127
access-list 100 deny ip 192.168.1.0 0.0.0.127 192.168.4.128 0.0.0.127
access-list 100 deny ip 192.168.1.0 0.0.0.127 192.168.1.128 0.0.0.127
access-list 100 permit ip any any
!
```

The redundant router has the following configuration:

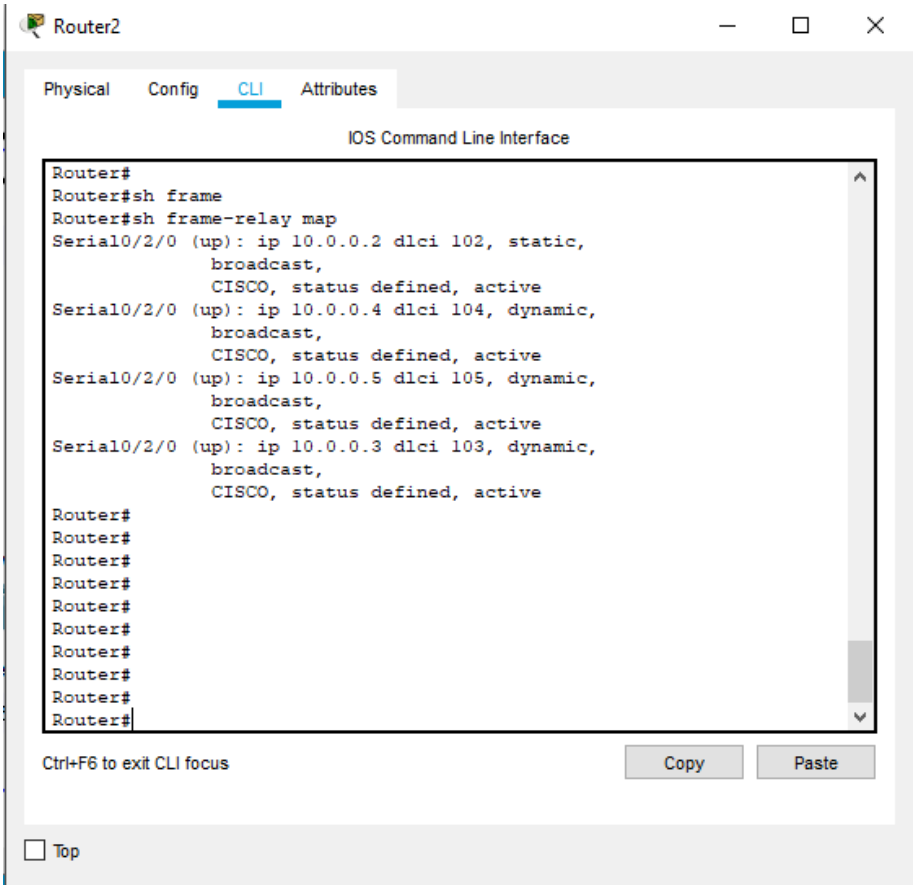


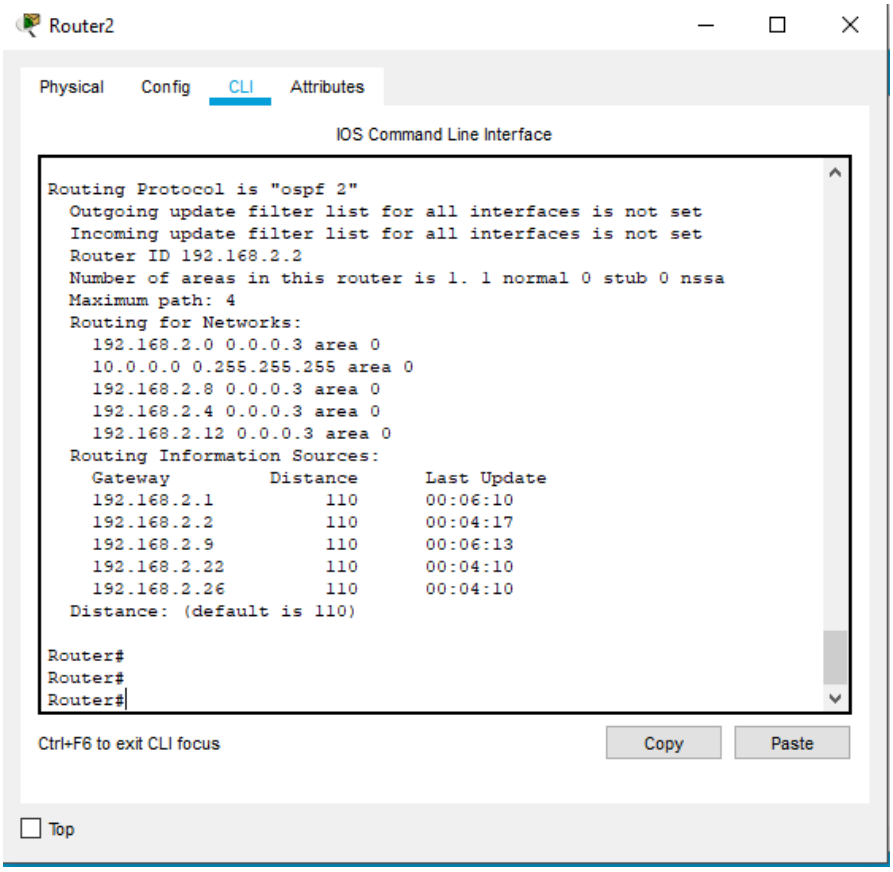
Configuration of Switch:

```
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0001.9617.4995
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0060.3EDB.EB94
 spanning-tree portfast
```

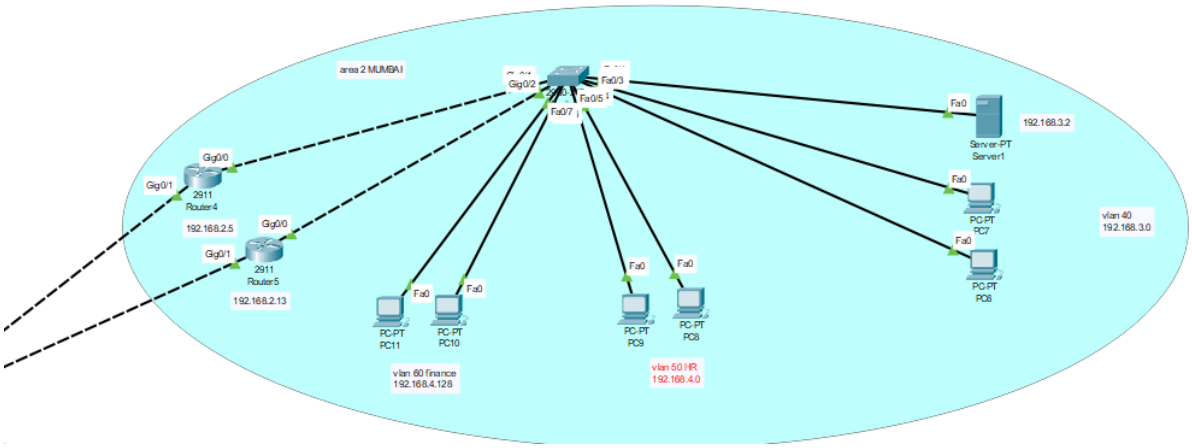
```
 spanning-tree bpduguard enable
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 000C.8592.7E71
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/4
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 00D0.FFAE.B3D4
 switchport port-security mac-address sticky 00E0.A322.99CC
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/5
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0006.2A76.A317
 switchport port-security mac-address sticky 0090.210D.8707
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/6
 switchport access vlan 30
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 00D0.BC26.7ECA
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/7
 switchport access vlan 30
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 000A.F398.426A
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/1
 switchport trunk native vlan 20
 switchport trunk allowed vlan 1-1001
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk native vlan 20
 switchport trunk allowed vlan 1-1001
 switchport mode trunk
!
```

The edge router has the following configuration:





Mumbai

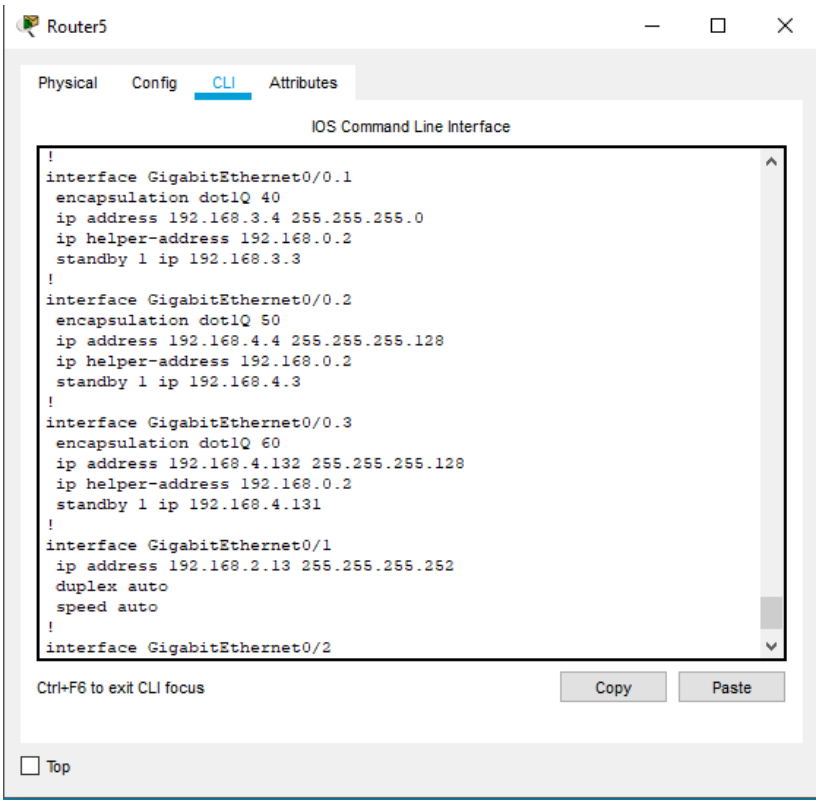


Configuration of main router:

```
spanning-tree mode pvst
!
interface GigabitEthernet0/0.1
 encapsulation dot1Q 40
 ip address 192.168.3.1 255.255.255.0
 ip helper-address 192.168.0.2
 ip access-group 100 in
 standby 1 ip 192.168.3.3
 standby 1 priority 105
 standby 1 preempt
 standby 1 timers 2 6
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 50 native
 ip address 192.168.4.1 255.255.255.128
 ip helper-address 192.168.0.2
 ip access-group 100 in
 standby 1 ip 192.168.4.3
 standby 1 priority 105
 standby 1 preempt
 standby 1 timers 2 6
!
interface GigabitEthernet0/0.3
 encapsulation dot1Q 60
 ip address 192.168.4.129 255.255.255.128
 ip helper-address 192.168.0.2
 ip access-group 100 in
 standby 1 ip 192.168.4.131
 standby 1 priority 105
 standby 1 preempt
 standby 1 timers 2 6
!
interface GigabitEthernet0/1
 ip address 192.168.2.5 255.255.255.252
 duplex auto
 speed auto
!
router ospf 4
 router-id 192.168.2.5
 log-adjacency-changes
 network 192.168.3.0 0.0.0.255 area 2
 network 192.168.4.0 0.0.0.127 area 2
```

```
 network 192.168.4.128 0.0.0.127 area 2
 network 192.168.2.4 0.0.0.3 area 0
!
ip classless
!
ip flow-export version 9
!
access-list 100 permit ip host 192.168.3.2 any
access-list 100 permit icmp any 192.168.4.128 0.0.0.127 echo-reply
access-list 100 permit icmp any 192.168.1.128 0.0.0.127 echo-reply
access-list 100 deny ip 192.168.3.0 0.0.0.255 192.168.4.128 0.0.0.127
access-list 100 deny ip 192.168.3.0 0.0.0.255 192.168.1.128 0.0.0.127
access-list 100 deny ip 192.168.4.0 0.0.0.127 192.168.1.128 0.0.0.127
access-list 100 deny ip 192.168.4.0 0.0.0.127 192.168.4.128 0.0.0.127
access-list 100 permit ip any any
!
```

The redundant router has the following configuration:



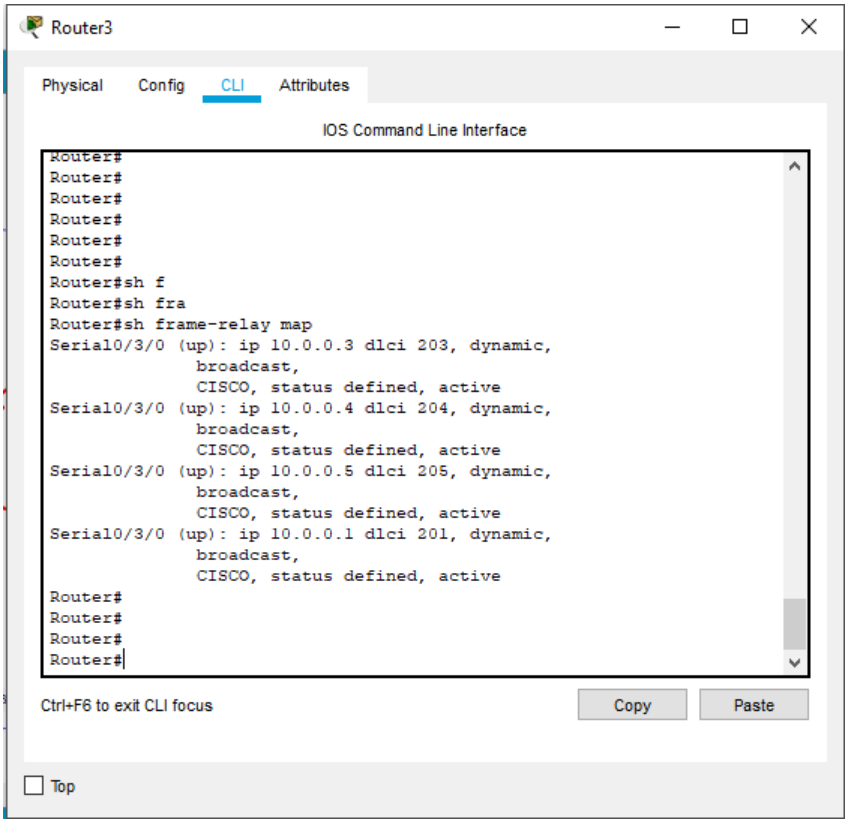
Configuration of Switch:

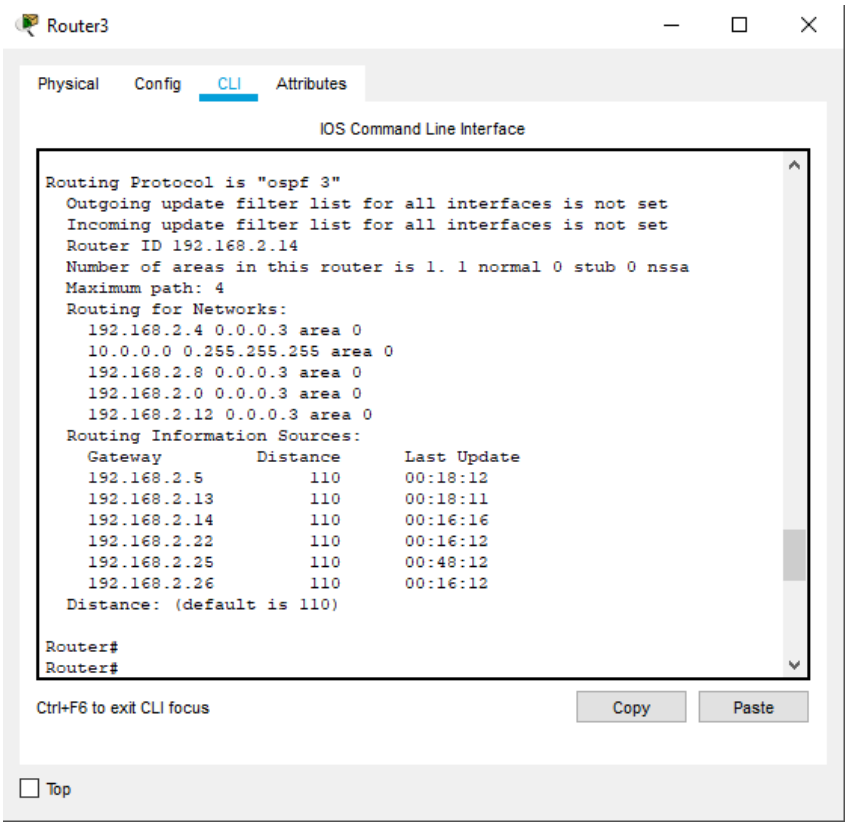
```
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 40
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0001.C94C.C291
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/2
 switchport access vlan 40
 switchport mode access
```

```
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0060.5C70.EB78
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/3
 switchport access vlan 40
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 00E0.A3D1.4AE2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/4
 switchport access vlan 50
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0060.3E0A.42E9
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/5
 switchport access vlan 50
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0060.2F70.72DC
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/6
 switchport access vlan 60
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0005.5E59.87B2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/7
 switchport access vlan 60
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 00D0.9792.BEC1
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/1
 switchport trunk native vlan 50
 switchport trunk allowed vlan 1-1001
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk native vlan 50
```

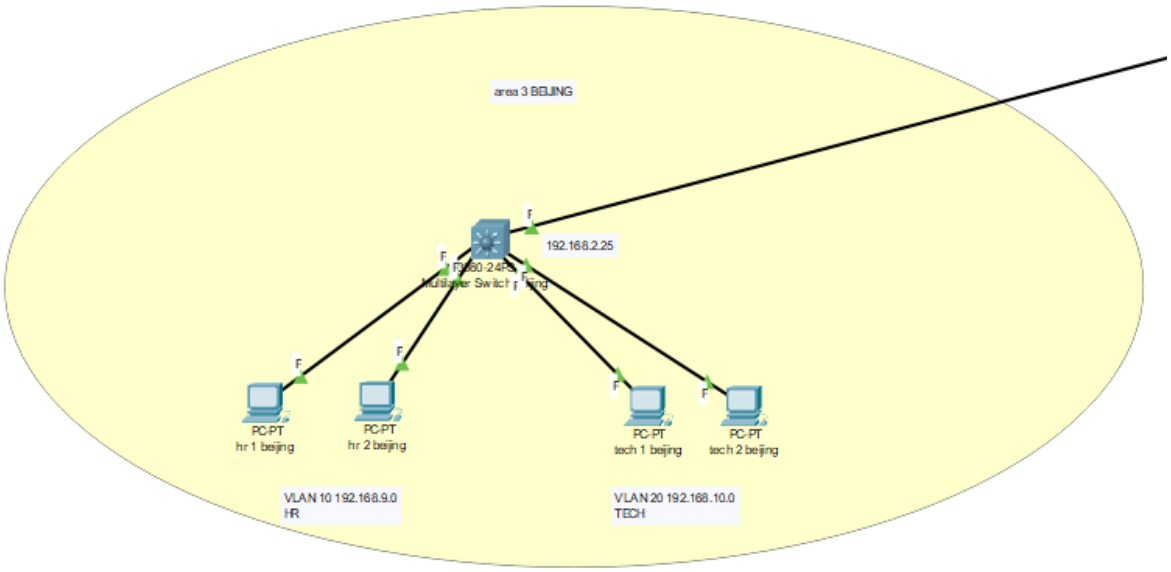
switchport trunk allowed vlan 1-1001
switchport mode trunk
!

The edge router has the following configuration:





Beijing

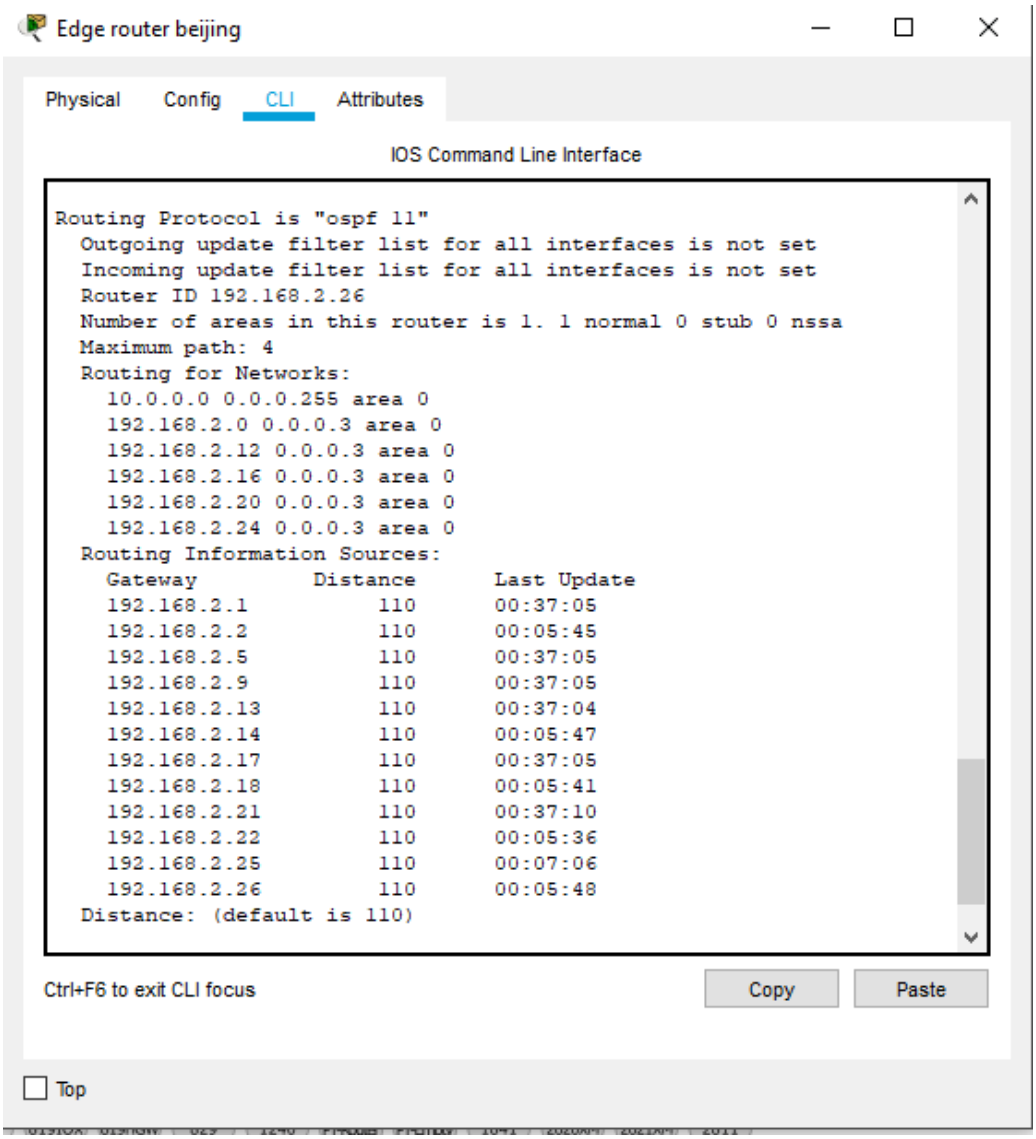


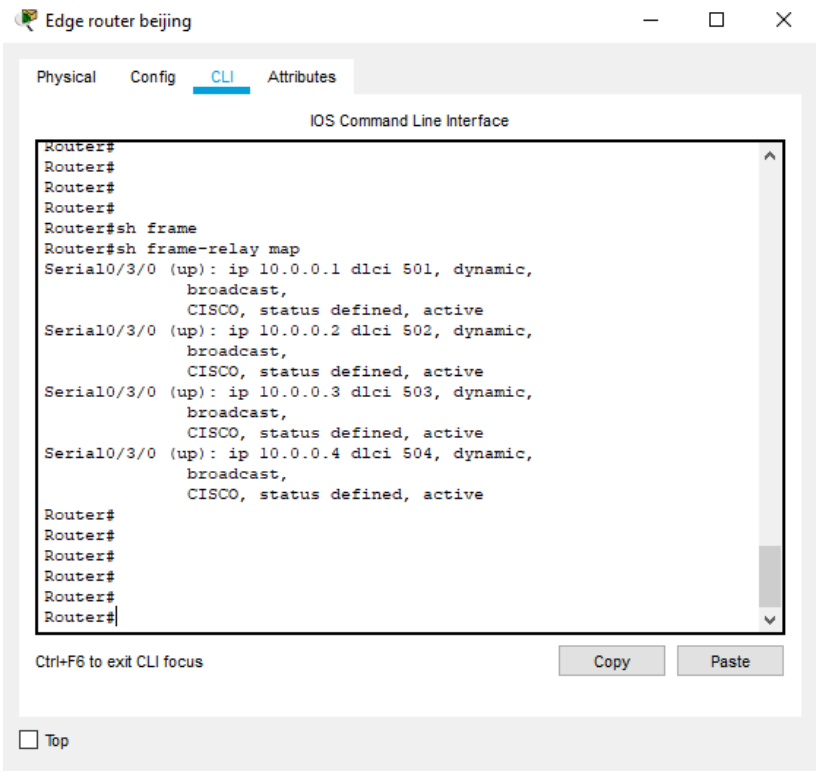
Configuration of multi-layer switch:

```
interface FastEthernet0/1
 switchport access vlan 10
!
interface FastEthernet0/2
 switchport access vlan 10
!
interface FastEthernet0/3
 switchport access vlan 20
!
interface FastEthernet0/4
 switchport access vlan 20
!
interface FastEthernet0/5
 no switchport
 ip address 192.168.2.25 255.255.255.252
 duplex auto
 speed auto
!
interface Vlan10
 mac-address 000a.4126.ea01
 ip address 192.168.9.1 255.255.255.0
 ip helper-address 192.168.3.2
 ip access-group 100 in
!
interface Vlan20
 mac-address 000a.4126.ea02
 ip address 192.168.10.1 255.255.255.0
 ip helper-address 192.168.3.2
 ip access-group 100 in
!
router ospf 12
 router-id 192.168.2.25
 log-adjacency-changes
 network 192.168.9.0 0.0.0.255 area 3
 network 192.168.10.0 0.0.0.255 area 3
 network 192.168.2.24 0.0.0.3 area 0
!
ip classless
```

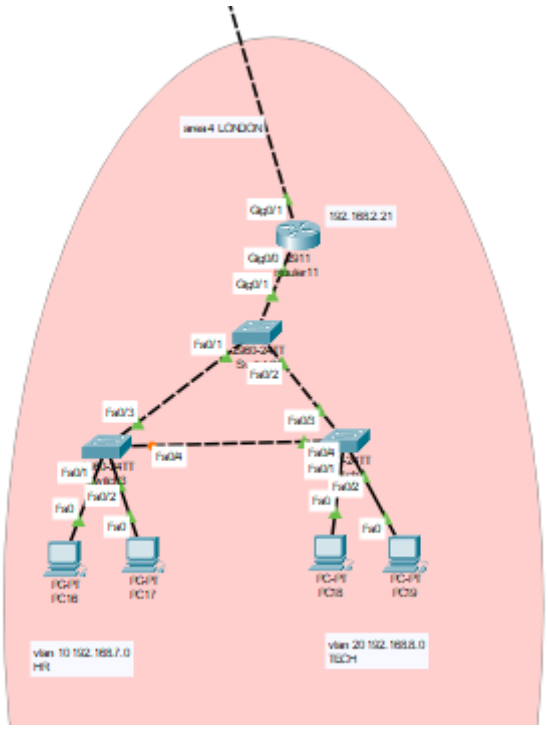
```
!
ip flow-export version 9
!
!
access-list 100 permit icmp any 192.168.1.128 0.0.0.127 echo-reply
access-list 100 permit icmp any 192.168.4.128 0.0.0.127 echo-reply
access-list 100 deny ip 192.168.9.0 0.0.0.255 192.168.4.128 0.0.0.127
access-list 100 deny ip 192.168.9.0 0.0.0.255 192.168.1.128 0.0.0.127
access-list 100 deny ip 192.168.10.0 0.0.0.255 192.168.1.128 0.0.0.127
access-list 100 deny ip 192.168.10.0 0.0.0.255 192.168.4.128 0.0.0.127
access-list 100 permit ip any any
!
```

The edge router has the following configuration:





London



Configuration of router:

!
interface GigabitEthernet0/0.1
encapsulation dot1Q 10 native
ip address 192.168.7.1 255.255.255.0

```
 ip helper-address 192.168.3.2
 ip access-group 100 in
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 20
 ip address 192.168.8.1 255.255.255.0
 ip helper-address 192.168.3.2
 ip access-group 100 in
!
interface GigabitEthernet0/1
 ip address 192.168.2.21 255.255.255.252
 duplex auto
 speed auto
!
router ospf 9
 router-id 192.168.2.21
 log-adjacency-changes
 network 192.168.7.0 0.0.0.255 area 4
 network 192.168.8.0 0.0.0.255 area 4
 network 192.168.2.20 0.0.0.3 area 0
!
ip classless
!
ip flow-export version 9
!
access-list 100 permit icmp any 192.168.4.128 0.0.0.127 echo-reply
access-list 100 permit icmp any 192.168.1.128 0.0.0.127 echo-reply
access-list 100 deny ip 192.168.7.0 0.0.0.255 192.168.4.128 0.0.0.127
access-list 100 deny ip 192.168.7.0 0.0.0.255 192.168.1.128 0.0.0.127
access-list 100 deny ip 192.168.8.0 0.0.0.255 192.168.1.128 0.0.0.127
access-list 100 deny ip 192.168.8.0 0.0.0.255 192.168.4.128 0.0.0.127
access-list 100 permit ip any any
!
```

Configuration of Switches:

1.

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 10
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/2
 switchport access vlan 10
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/3
 switchport trunk native vlan 10
 switchport trunk allowed vlan 1-1001
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 10
 switchport trunk allowed vlan 1-1001
 switchport mode trunk
!
```

2.

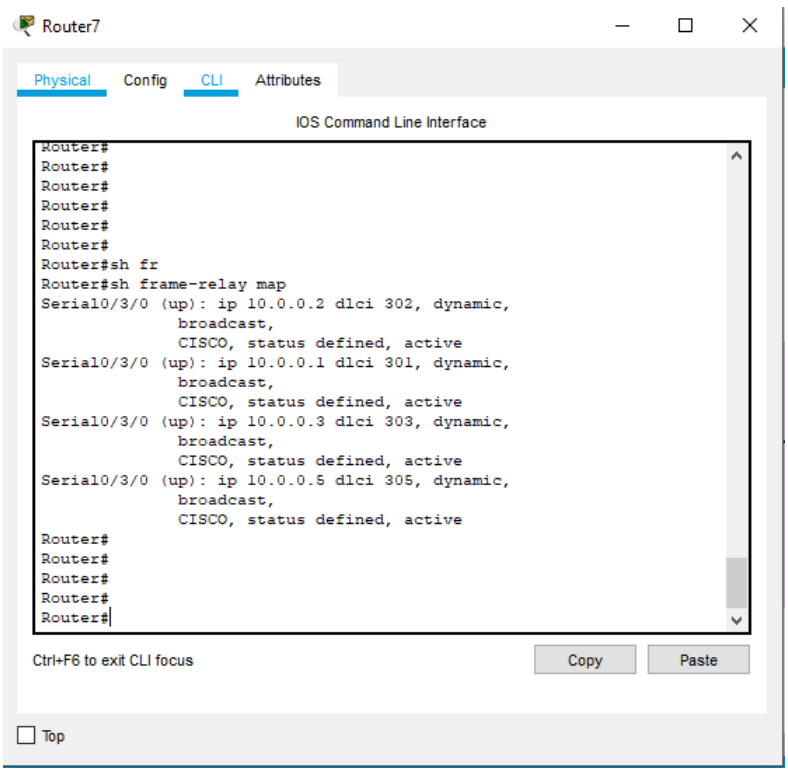
```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 20
 spanning-tree portfast
```

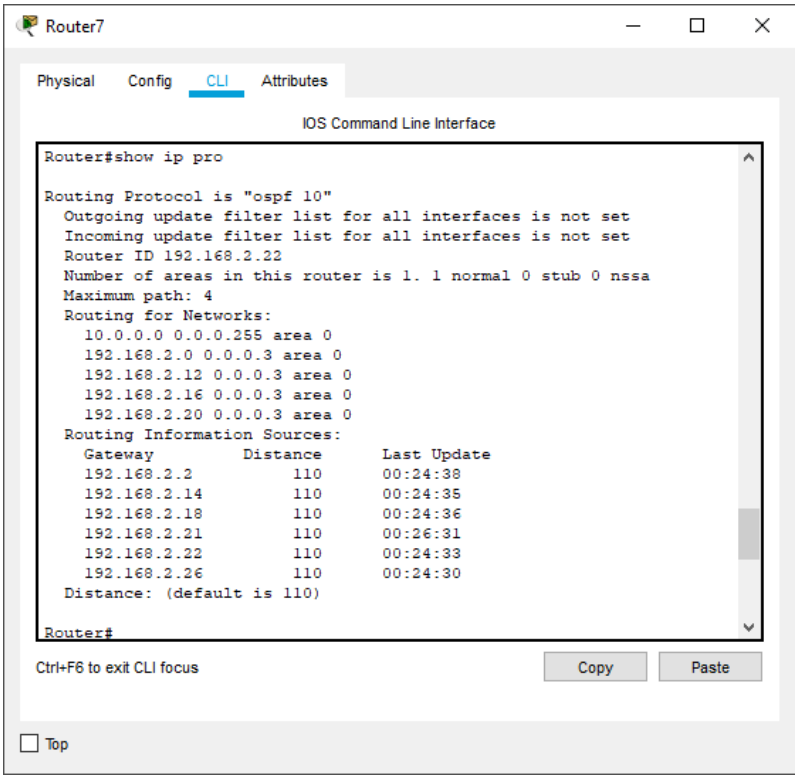
spanning-tree bpduguard enable
!
interface FastEthernet0/2
switchport access vlan 20
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/3
switchport trunk native vlan 10
switchport trunk allowed vlan 1-1001
switchport mode trunk
!
interface FastEthernet0/4
switchport trunk native vlan 10
switchport trunk allowed vlan 1-1001
switchport mode trunk
!

3.

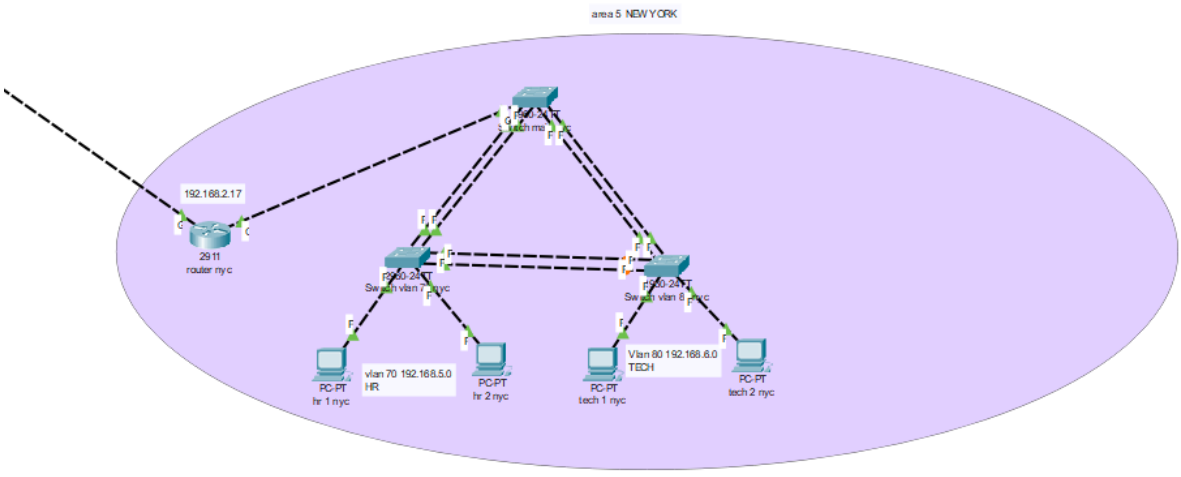
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport trunk native vlan 10
switchport trunk allowed vlan 1-1001
switchport mode trunk
!
interface FastEthernet0/2
switchport trunk native vlan 10
switchport trunk allowed vlan 1-1001
switchport mode trunk
!
interface FastEthernet0/3
switchport mode trunk
!
interface GigabitEthernet0/1
switchport trunk native vlan 10
switchport mode trunk
!

The edge router has the following configuration:





NEW YORK



The switches have the following configuration:

1.

spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Port-channel1
switchport trunk native vlan 70
switchport trunk allowed vlan 70,80
switchport mode trunk
!
interface Port-channel2
switchport trunk native vlan 70
switchport trunk allowed vlan 70,80
switchport mode trunk
!

```
interface FastEthernet0/1
 switchport access vlan 70
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/2
 switchport access vlan 70
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/3
 switchport trunk native vlan 70
 switchport trunk allowed vlan 70,80
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/4
 switchport trunk native vlan 70
 switchport trunk allowed vlan 70,80
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/5
 switchport trunk native vlan 70
 switchport trunk allowed vlan 70,80
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/6
 switchport trunk native vlan 70
 switchport trunk allowed vlan 70,80
 switchport mode trunk
 channel-group 2 mode active
!
```

2.

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Port-channel1
 switchport trunk native vlan 70
 switchport trunk allowed vlan 70,80
 switchport mode trunk
!
interface Port-channel5
 switchport trunk native vlan 70
 switchport trunk allowed vlan 70,80
 switchport mode trunk
!
interface FastEthernet0/1
 switchport access vlan 80
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/2
 switchport access vlan 80
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/3
 switchport trunk native vlan 70
 switchport trunk allowed vlan 70,80
 switchport mode trunk
 channel-group 1 mode active
!
```

```
interface FastEthernet0/4
 switchport trunk native vlan 70
 switchport trunk allowed vlan 70,80
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/10
 switchport trunk native vlan 70
 switchport trunk allowed vlan 70,80
 switchport mode trunk
 channel-group 5 mode active
!
interface FastEthernet0/11
 switchport trunk native vlan 70
 switchport trunk allowed vlan 70,80
 switchport mode trunk
 channel-group 5 mode active
!
```

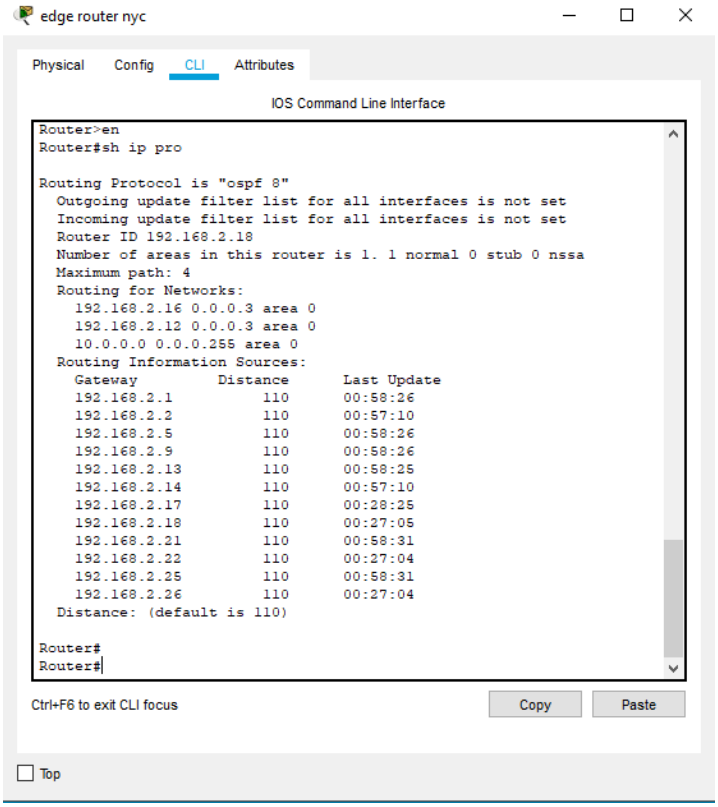
3.

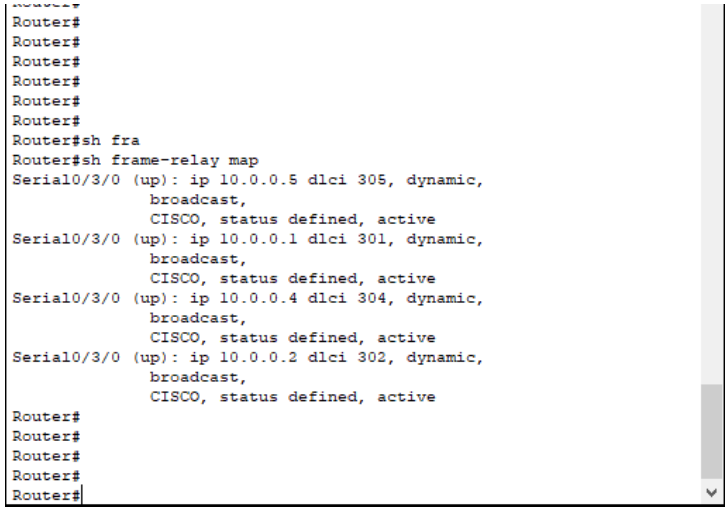
```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Port-channel2
 switchport trunk native vlan 70
 switchport trunk allowed vlan 70,80
 switchport mode trunk
!
interface Port-channel5
 switchport trunk native vlan 70
 switchport trunk allowed vlan 70,80
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 70
 switchport trunk allowed vlan 70,80
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/6
 switchport trunk native vlan 70
 switchport trunk allowed vlan 70,80
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/10
 switchport trunk native vlan 70
 switchport trunk allowed vlan 70,80
 switchport mode trunk
 channel-group 5 mode active
!
interface FastEthernet0/11
 switchport trunk native vlan 70
 switchport trunk allowed vlan 70,80
 switchport mode trunk
 channel-group 5 mode active
!
interface GigabitEthernet0/1
 switchport trunk native vlan 70
 switchport trunk allowed vlan 1-1001
 switchport mode trunk
!
```

The router has the following configuration:

```
interface GigabitEthernet0/0.1
 encapsulation dot1Q 70 native
 ip address 192.168.5.1 255.255.255.0
 ip helper-address 192.168.3.2
 ip access-group 100 in
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 80
 ip address 192.168.6.1 255.255.255.0
 ip helper-address 192.168.3.2
 ip access-group 100 in
!
interface GigabitEthernet0/1
 ip address 192.168.2.17 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/3/0
 bandwidth 64
 no ip address
 encapsulation frame-relay
 clock rate 2000000
!
interface Serial0/3/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 7
 router-id 192.168.2.17
 log-adjacency-changes
 network 192.168.5.0 0.0.0.255 area 5
 network 192.168.6.0 0.0.0.255 area 5
 network 192.168.2.16 0.0.0.3 area 0
!
ip classless
!
ip flow-export version 9
!
!
access-list 100 permit icmp any 192.168.4.128 0.0.0.127 echo-reply
access-list 100 permit icmp any 192.168.1.128 0.0.0.127 echo-reply
access-list 100 deny ip 192.168.5.0 0.0.0.255 192.168.1.128 0.0.0.127
access-list 100 deny ip 192.168.6.0 0.0.0.255 192.168.1.128 0.0.0.127
access-list 100 deny ip 192.168.6.0 0.0.0.255 192.168.4.128 0.0.0.127
access-list 100 deny ip 192.168.5.0 0.0.0.255 192.168.4.128 0.0.0.127
access-list 100 permit ip any any
!
```

The configuration of the edge router is as follows:





INDIVIDUAL OFFICE NETWORK:

VLAN 10 is considered to be the Technical department. VLAN 20 as HR and 30 as Finance in Boston.

Boston's Technical department has IP address range from 192.168.0.5 to 192.168.0.254

Boston's HR department has IP address range from 192.168.1.5 to 192.168.1.126

Boston's Technical department has IP address range from 192.168.1.133 to 192.168.1.254

Mumbai's Technical department has IP address range from 192.168.3.5 to 192.168.3.254

Mumbai's HR department has IP address range from 192.168.4.5 to 192.168.4.126

Mumbai's Finance department has IP address range from 192.168.4.133 to 192.168.4.254

Finance department can access all other departments but not vice versa.

ABR at Boston can access all other locations ABR but not vice versa. The tech department from Boston alone has access to the ABR of Boston.

HSRP is implemented and the given hello and wait timers are set.

Switchport port security is used in the switch as a defensive mechanism for MAC flooding attacks.

ASSIGNMENT OF IP ADDRESSES:

Each office has 250 employees and 85% redundancy of IP addresses for them. So, each office should have 463 IP addresses.

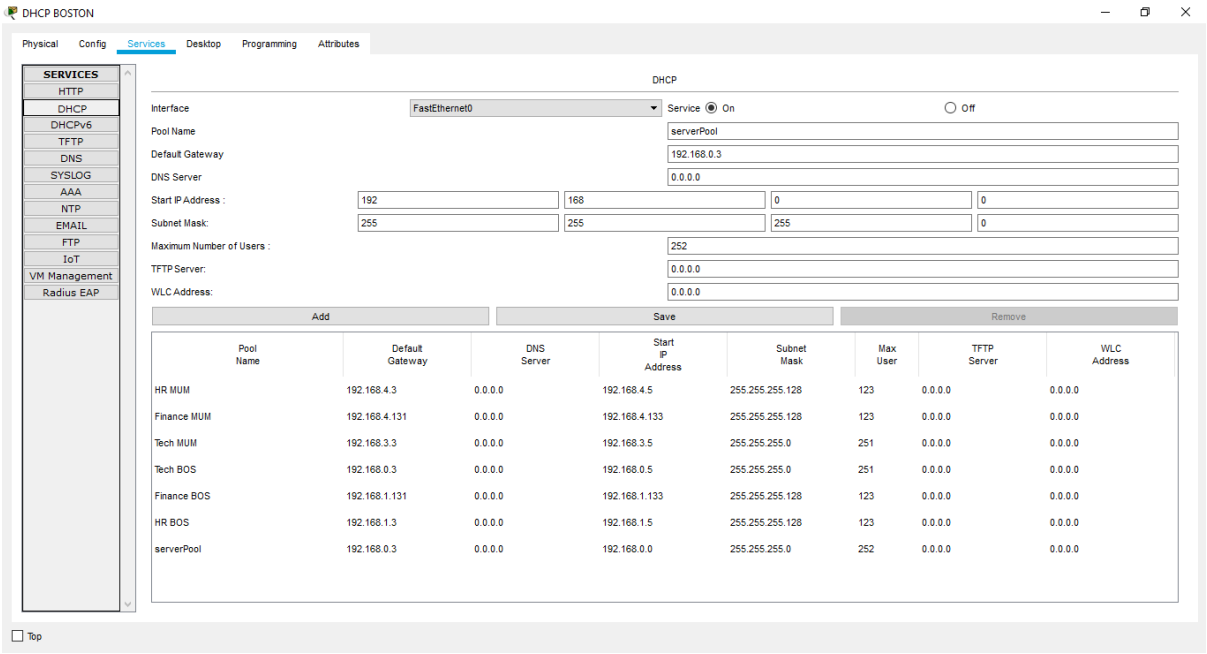
In HQ locations, Tech department has 251 host IP addresses, HR department and Finance department has 123 host IP addresses for each.

So, Technical dept uses the subnet /24, the other 2 uses the subnet /25

In other locations, Tech department and HR department has 254 host IP addresses for each.

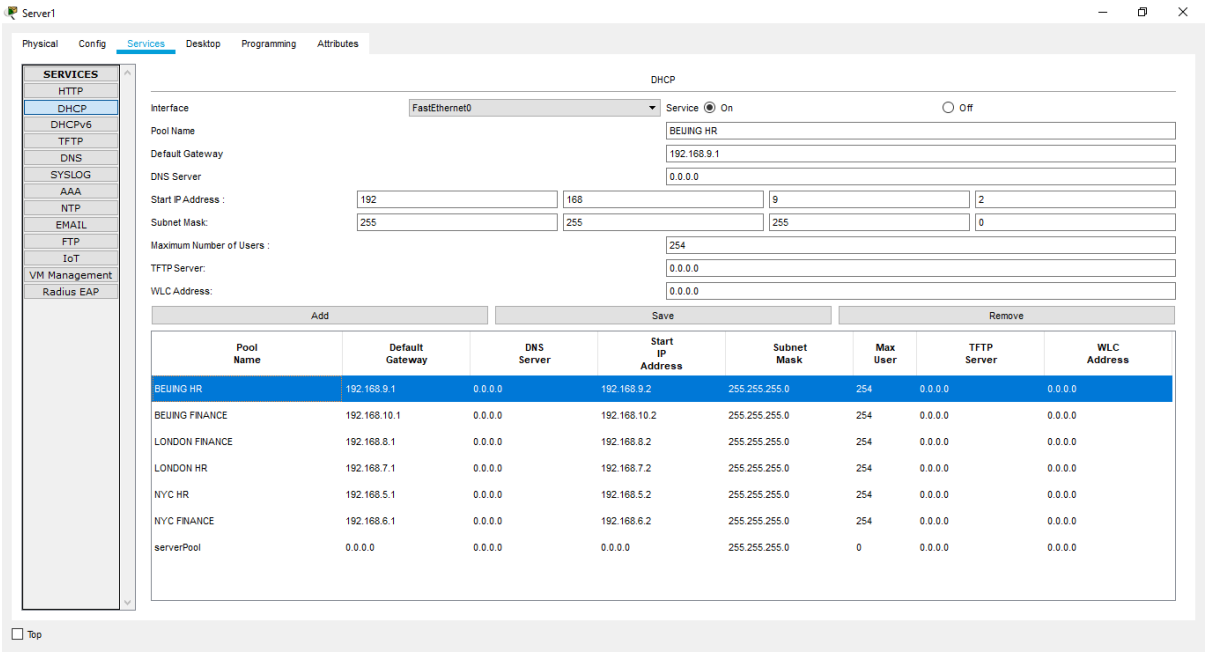
So, all the departments use the subnet /24.

The DHCP pool of Boston's server is as follows:



The IP address of the DHCP server at Boston is 192.168.0.2

The DHCP pool of Mumbai's server is as follows:



Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
BEIJING HR	192.168.9.1	0.0.0.0	192.168.9.2	255.255.255.0	254	0.0.0.0	0.0.0.0
BEIJING FINANCE	192.168.10.1	0.0.0.0	192.168.10.2	255.255.255.0	254	0.0.0.0	0.0.0.0
LONDON FINANCE	192.168.8.1	0.0.0.0	192.168.8.2	255.255.255.0	254	0.0.0.0	0.0.0.0
LONDON HR	192.168.7.1	0.0.0.0	192.168.7.2	255.255.255.0	254	0.0.0.0	0.0.0.0
NYC HR	192.168.5.1	0.0.0.0	192.168.5.2	255.255.255.0	254	0.0.0.0	0.0.0.0
NYC FINANCE	192.168.6.1	0.0.0.0	192.168.6.2	255.255.255.0	254	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	0.0.0.0	255.255.255.0	0	0.0.0.0	0.0.0.0

The IP address of the DHCP server at Mumbai is 192.168.3.2

The area border routers are assigned an IP address in the range 192.168.2.0/30.

192.168.x.1 is used as the default gateway for the primary router.

192.168.x.3 is used as the virtual default gateway for standby in HSRP.

192.168.x.4 is used as the default gateway for the redundant router.

3. TAKEAWAY QUESTIONS

1. a. OSPF is better for complex networks as it calculates the shortest path with minimum traffic. RIP on the other hand decides the best path only based on the hop count. Moreover, OSPF provides authentication by default. So, provides more security to the network. RIP can be used for small networks.

b. The area concept in OSPF allows us to have a greater level of control of our network my helping us to segment our network topology in high scalable networks. An OSPF network is subdivided into areas of collection of logical network entities allowing it to have the same identification. A router in each area maintains the topological database for its area and it doesn't need to have the detailed topology of the routers outside its area. This helps to reduce the size of the database in the routers.

c. In OSPF there must be a backbone area and all other areas must have a connection to the backbone. Since OSPF uses distance-vector approach, it uses this strict area hierarchy that avoids the counting to infinity problem. This also helps to eliminate the routing loops which in turn reduces network traffic.

d.

1: ROUTER LSA – It is generated by each router for its area
2: NETWORK LSA – Generated by designated router.
3: SUMMARY LSA – Generated by ABR and broadcast to other areas.

4: SUMMARY ASBR LSA - To find the location of Autonomous System Boundary Router, ABR will generate an ASBR with the router-id.
5: AUTONOMOUS SYSTEM EXTERNAL LSA – Generated by ASBR
6: MULTICAST LSA – Not used
7: NOT SO STUBBY AREA LSA – This is generated where the area doesn't allow external LSA.

2. Redundancy plan:

If the main router in the HQ location fails, the HSRP protocol kicks in the redundant router and the network works normally just like it would work with the main router.

If a link in a switch fails, the passive link which stayed dormant before gets activated and the network works as required.

Security plan:

The finance departments in the HQ locations should not be accessed by other departments but finance department can access other departments. This is implemented using access-lists in the router.

MAC flooding attack is prevented in the HQ locations by implementing port security on the switches. The maximum number of MAC address per port is defined as 2. So, if a 3rd different PC(with a different MAC address) tries to connect, it will be discarded.

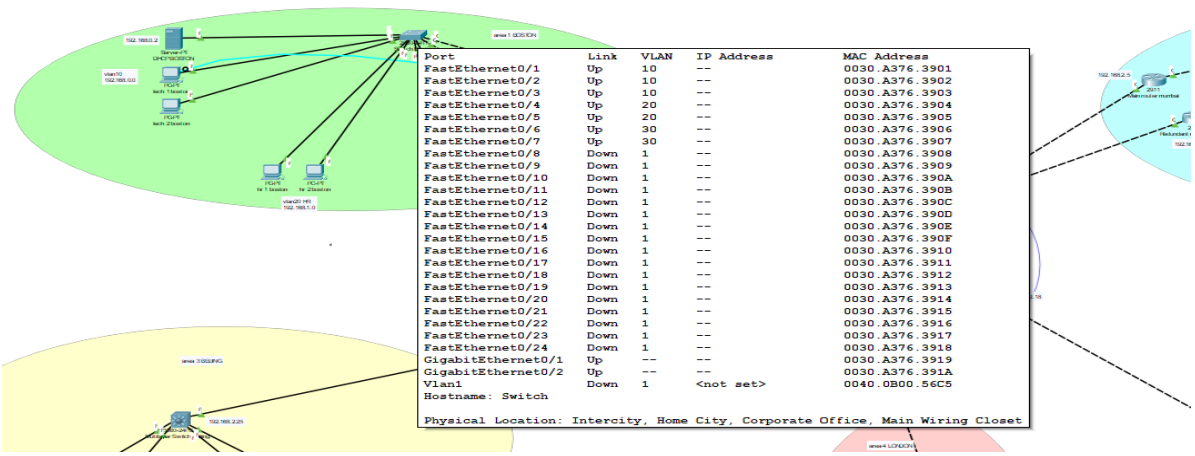
3. If STP is not implemented and the switches are connected in a loop, all the switches will duplicate the first broadcast packet as there's nothing to prevent a loop. STP prevents this by blocking one or more links. If one link is down, that link will fail to the previous blocked link. The link that is chosen to go down is entirely dependant on the topology that the spanning tree can see.

4. STP is the old standard that supports only a single instance. PVSTP is a cisco proprietary standard and runs a STP instance per VLAN and offers enhancements that are not found in the standard protocols. MSTP is a standard which supports fast convergence and supports multiple instances.

4. TEST PLAN FOR THE NETWORK

VLAN:

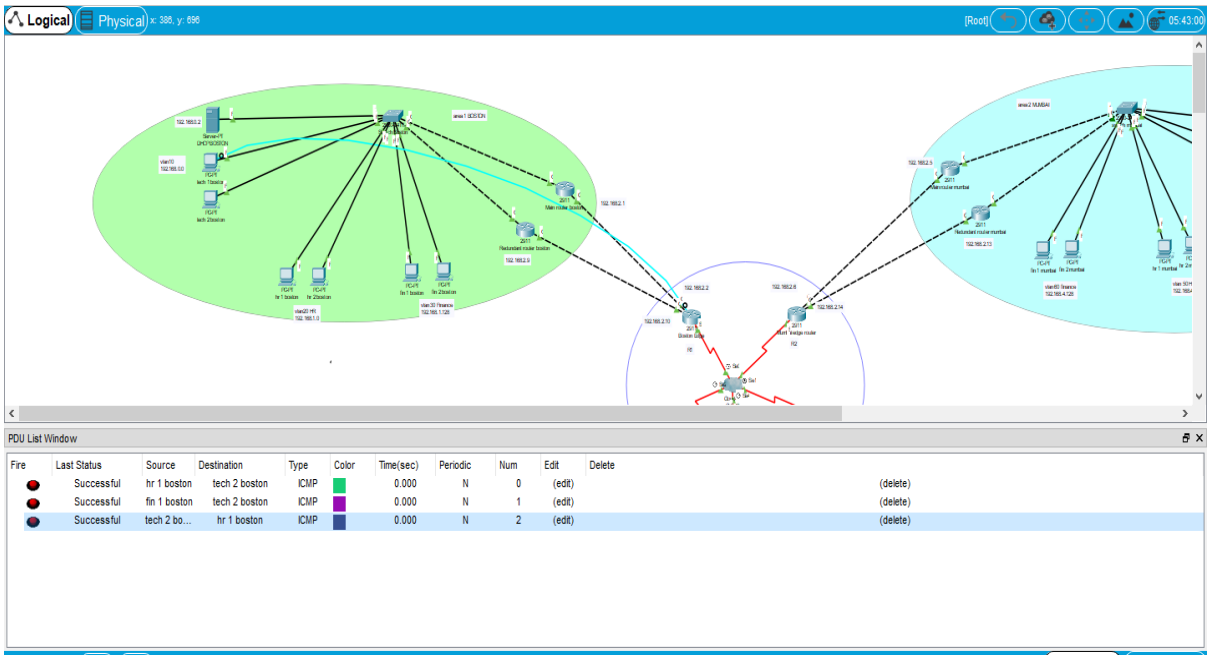
Each department is assigned a separate VLAN in the same switch. The routing of data packets to the corresponding VLAN is done by the router. In order to test the VLAN and the routing, the PC from different VLANs can be pinged. If the ping is successful, the VLAN works. The command "show run" displays the running config of the switch where the VLAN information will also be displayed.



Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	10	--	0030.A376.3901
FastEthernet0/2	Up	10	--	0030.A376.3902
FastEthernet0/3	Up	10	--	0030.A376.3903
FastEthernet0/4	Up	20	--	0030.A376.3904
FastEthernet0/5	Up	20	--	0030.A376.3905
FastEthernet0/6	Up	30	--	0030.A376.3906
FastEthernet0/7	Up	30	--	0030.A376.3907
FastEthernet0/8	Down	1	--	0030.A376.3908
FastEthernet0/9	Down	1	--	0030.A376.3909
FastEthernet0/10	Down	1	--	0030.A376.390A
FastEthernet0/11	Down	1	--	0030.A376.390B
FastEthernet0/12	Down	1	--	0030.A376.390C
FastEthernet0/13	Down	1	--	0030.A376.390D
FastEthernet0/14	Down	1	--	0030.A376.390E
FastEthernet0/15	Down	1	--	0030.A376.390F
FastEthernet0/16	Down	1	--	0030.A376.3910
FastEthernet0/17	Down	1	--	0030.A376.3911
FastEthernet0/18	Down	1	--	0030.A376.3912
FastEthernet0/19	Down	1	--	0030.A376.3913
FastEthernet0/20	Down	1	--	0030.A376.3914
FastEthernet0/21	Down	1	--	0030.A376.3915
FastEthernet0/22	Down	1	--	0030.A376.3916
FastEthernet0/23	Down	1	--	0030.A376.3917
FastEthernet0/24	Down	1	--	0030.A376.3918
GigabitEthernet0/1	Up	--	--	0030.A376.3919
GigabitEthernet0/2	Up	--	--	0030.A376.391A
Vlan1	Down	1	<not set>	0040.0B00.56C5

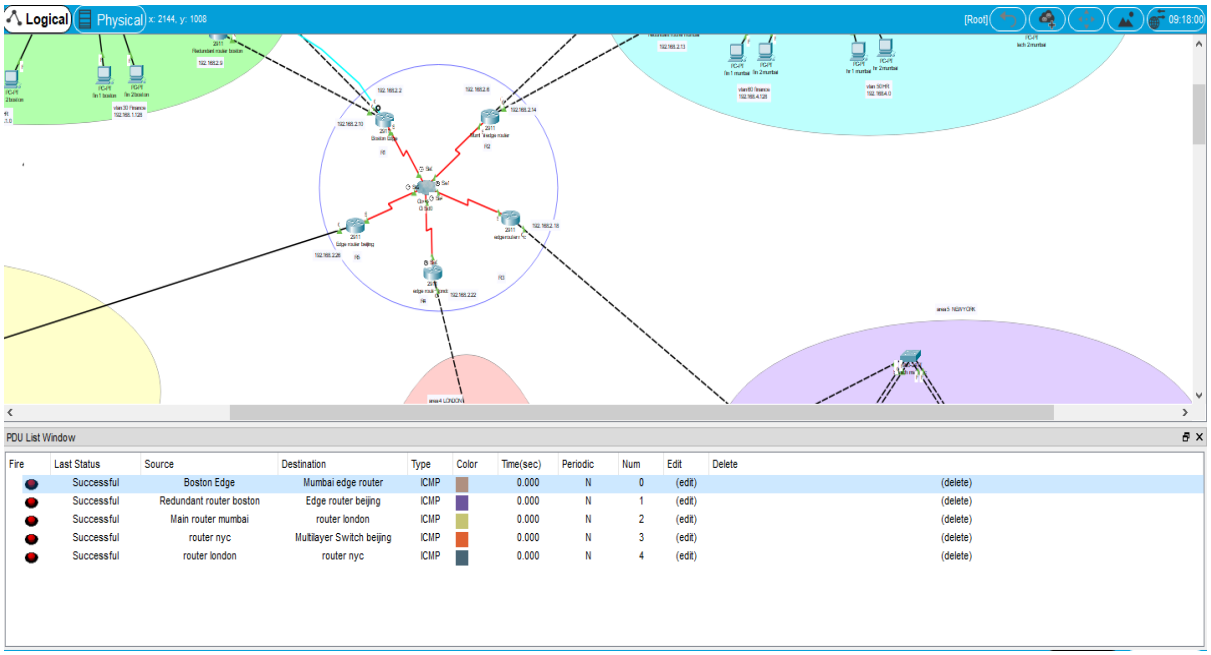
Hostname: Switch

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet



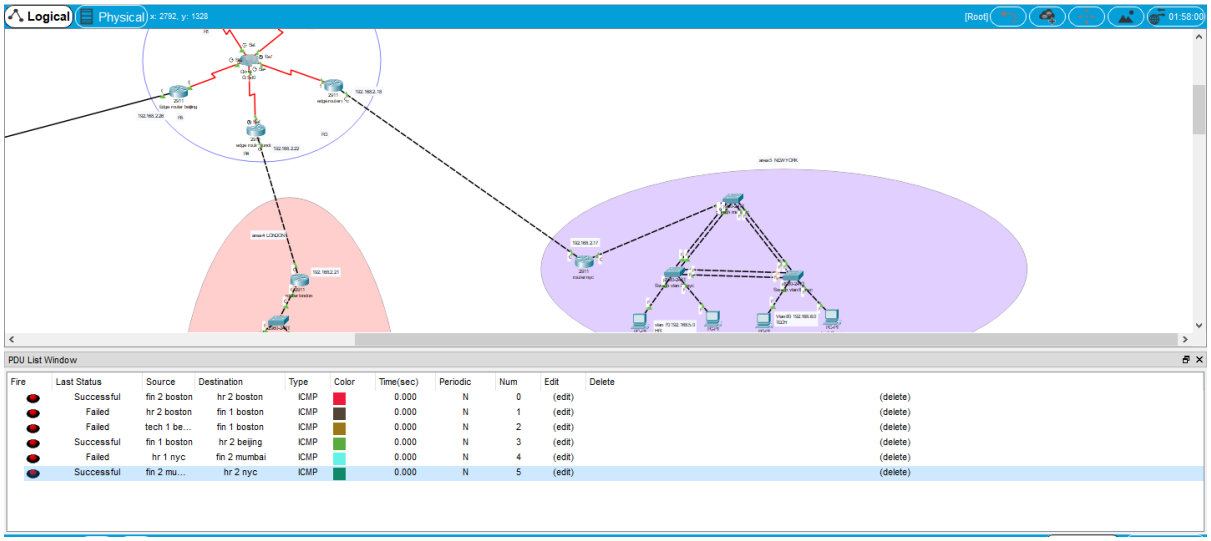
ROUTING PROTOCOL:

The routing protocol used in this project is OSPF. The command "show ip protocols" displays the OSPF configuration of the router. In order to test the routing protocol, a packet can be sent from and to all the edge routers. If all the packets are delivered successfully, the routing protocols is properly working.



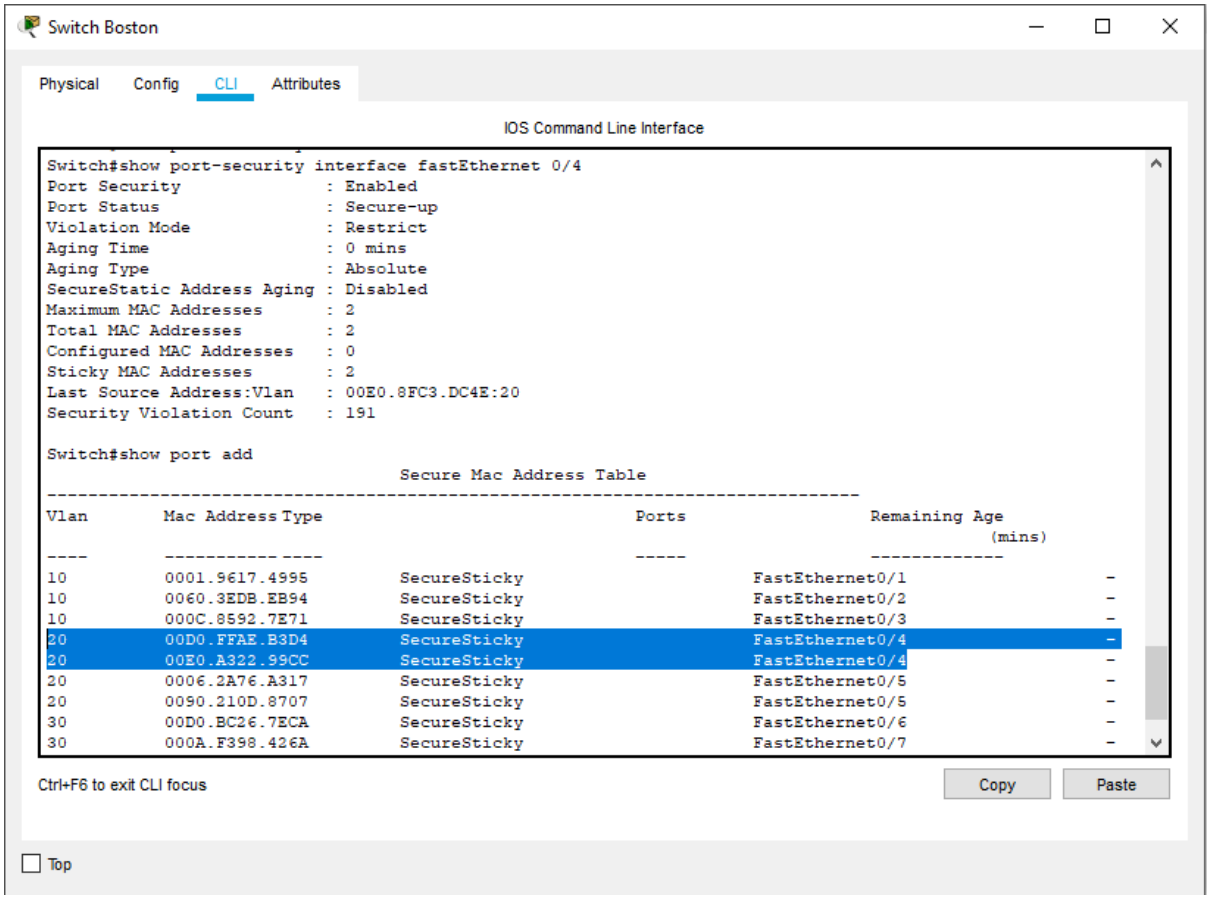
SECURITY PLAN:

The finance department of HQ locations should not be accessed by other departments, but finance department should be able to access all other departments. To make this happen access-lists were implemented in the router. To test this, a ping from any other department should be sent to the finance department. That ping should fail. But, if the finance department pings any other department, the ping should be successful. The same should be tried from all cities.



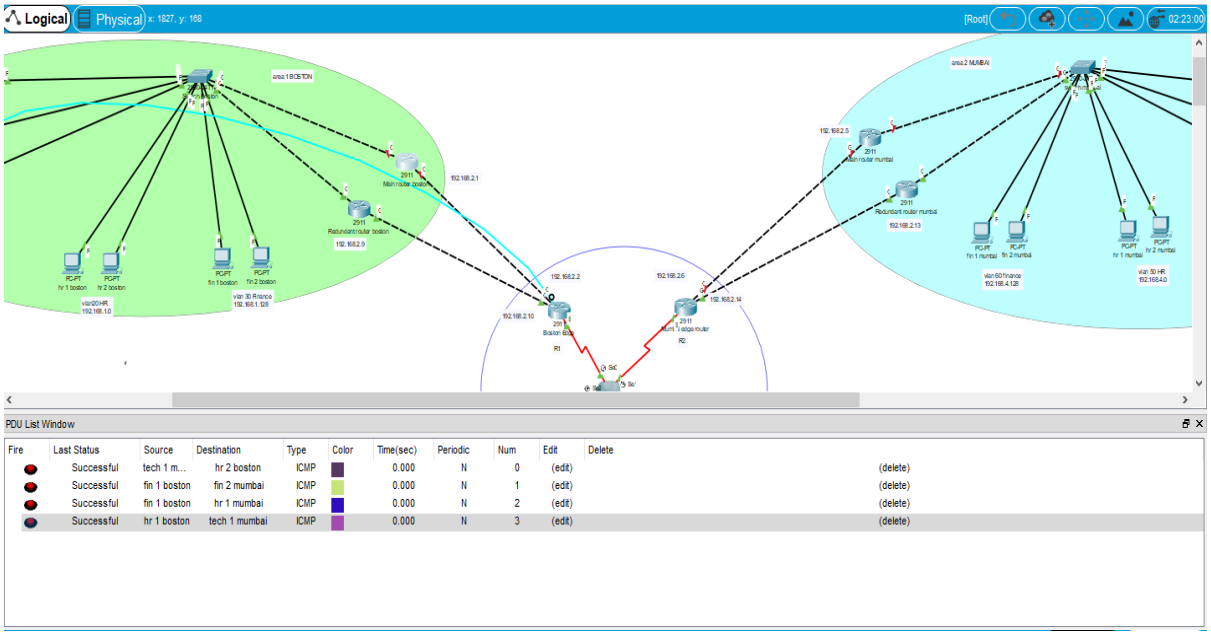
Prevention of MAC flooding attacks:

The switches in the headquarters are implemented with port security for up to 2 devices. So, 2 different PCs can be able to ping from the same port. Both the MAC addresses will be stuck to the MAC table of the switch for the specific port. If a 3rd PC connects and pings, the connection will be refused. The packet will not go through. This can be checked on all the ports where end devices are connected.



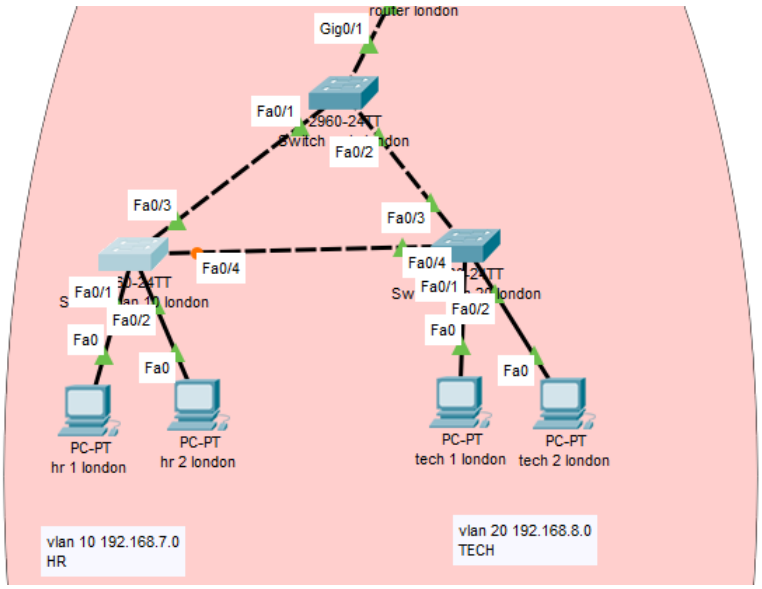
REDUNDANCY PLAN:

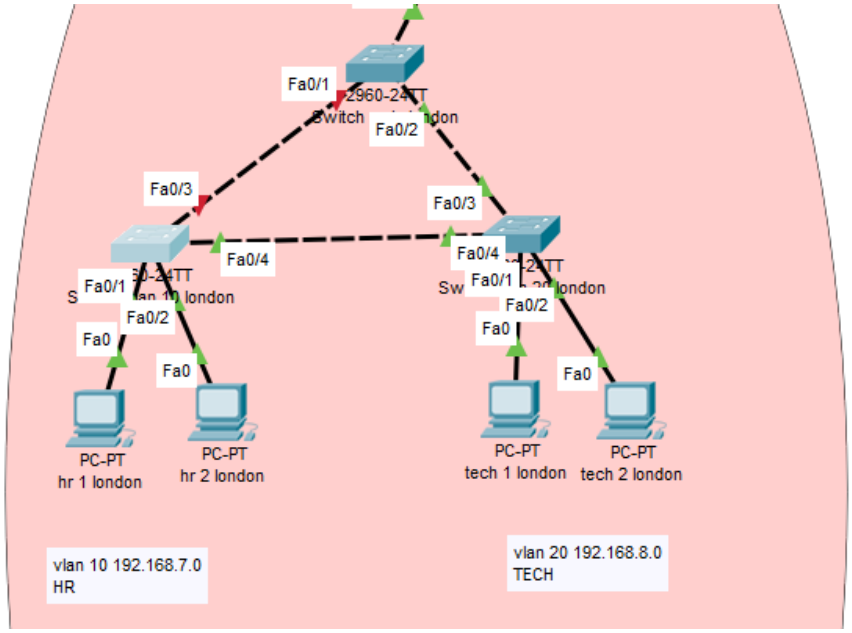
If the main router fails in any of the HQ location, the redundant router should work using HSRP. To test this, the main router can be turned off for one location and a packet can be sent from one city to another. The same steps can be performed by switching off the router of the other location and testing. If this is successful, the redundancy plan works.



Switch Redundancy:

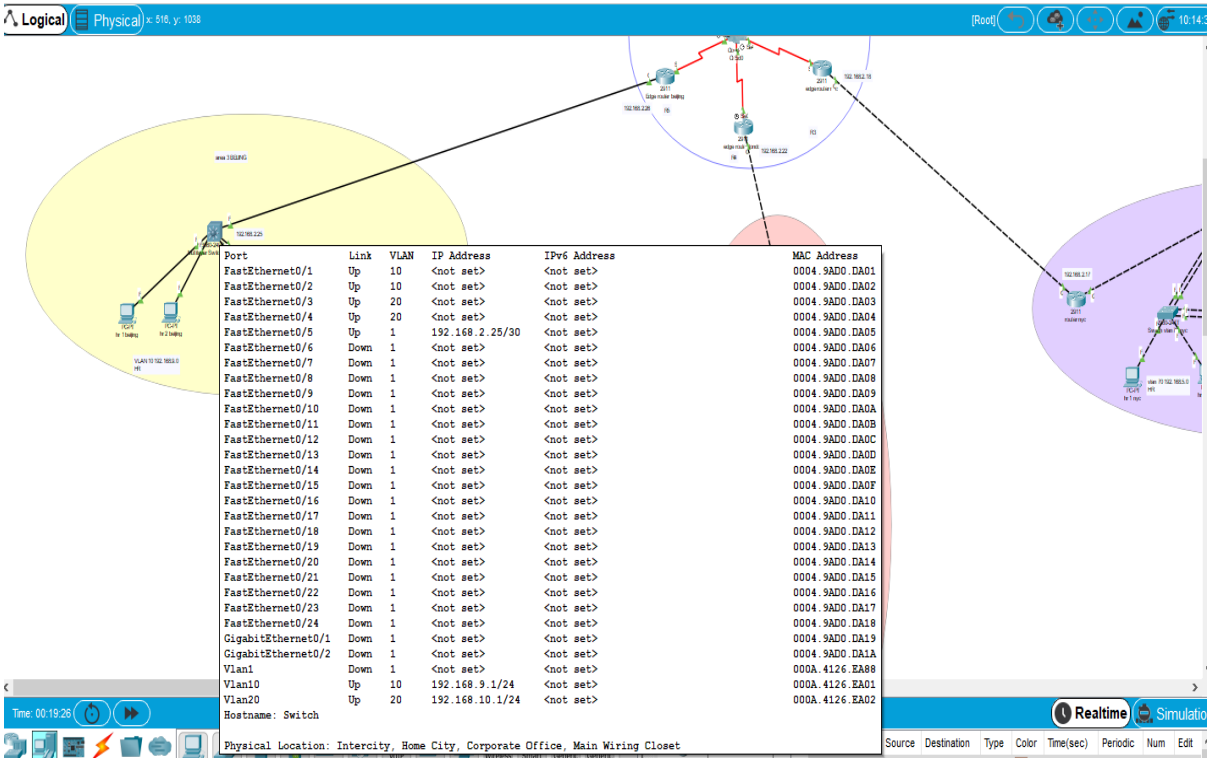
When switch redundancy is implemented, a link is in standby. If any of the other link fails, this link will turn on and start working. To test this any of the link can be turned off and check if the network is working.

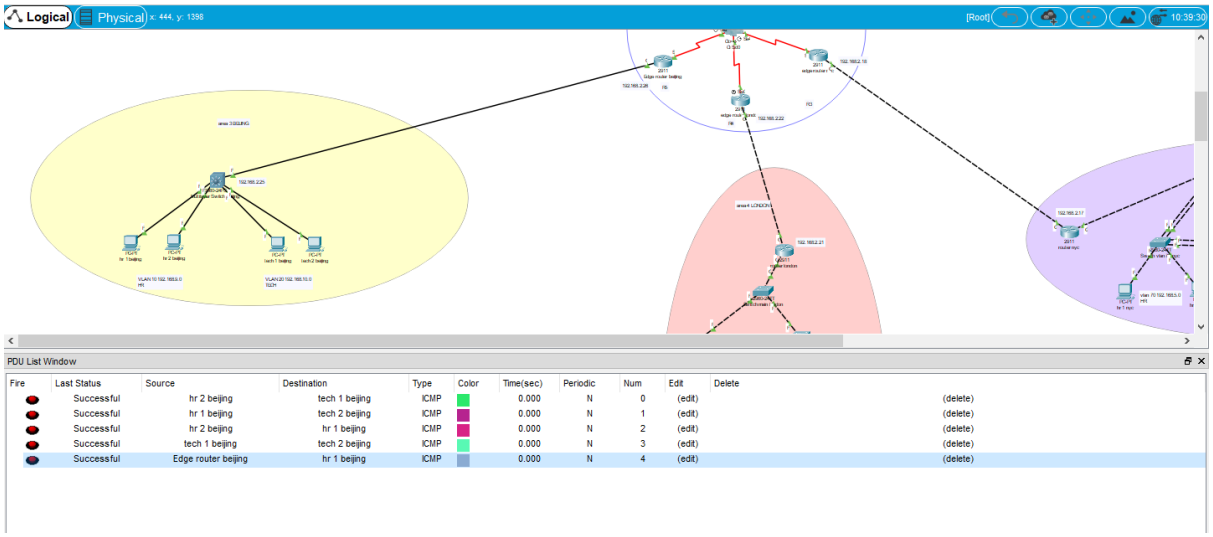




ADD-ONS:

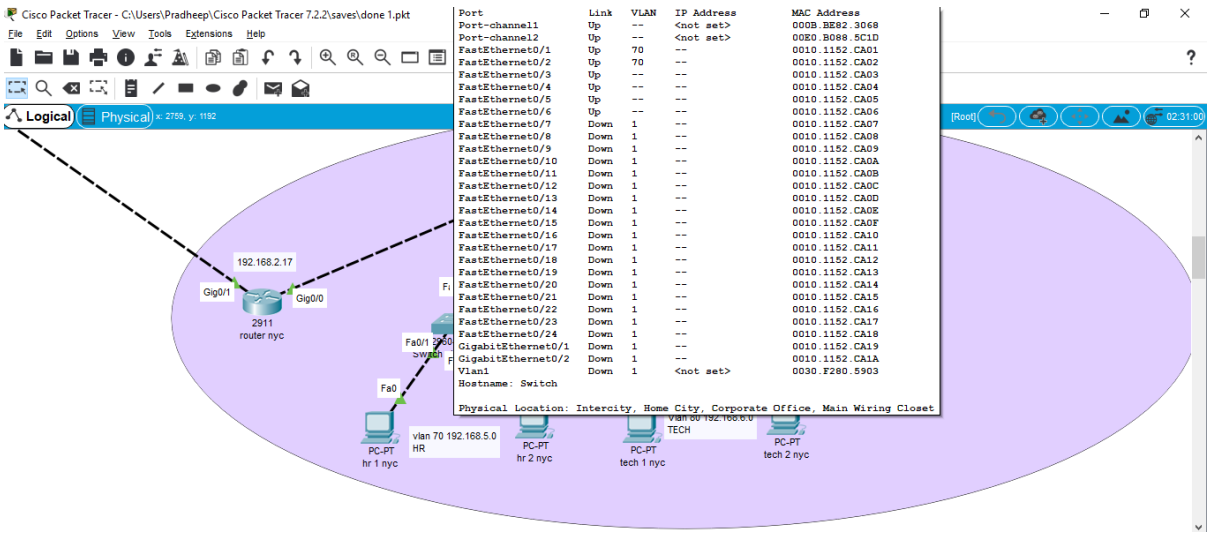
A multilayer switch is used in Beijing. This switch will perform the inter-VLAN routing. This can be tested by sending a packet from a pc in one VLAN to the other. A successful ping shows that the inter-VLAN routing works.





Ether channel LACP:

When LACP is implemented, the bandwidth gets increased. This can be tested in the same way as switch redundancy is tested. If a link fails, the passive link gets activated and the network works as usual.



5. CONCEPTS LEARNT DURING THE PROJECT

Concepts and protocols such as HSRP, OSPF, RSTP, LACP have been exposed to and thoroughly understood practically by working on this project. This project also helped understand subnetting and the internetworking concepts such as VLAN, frame-relay and routing better. Finally, this project has taught a cyber defensive point of view approach while implementing a security plan for the entire network.

6. CONCLUSION

A multi-location, inter-networking strategy for a small and stable organization was designed and implemented with the given network constraints on Cisco Packet Tracer.