

# Project 2

Yuchen Zhao

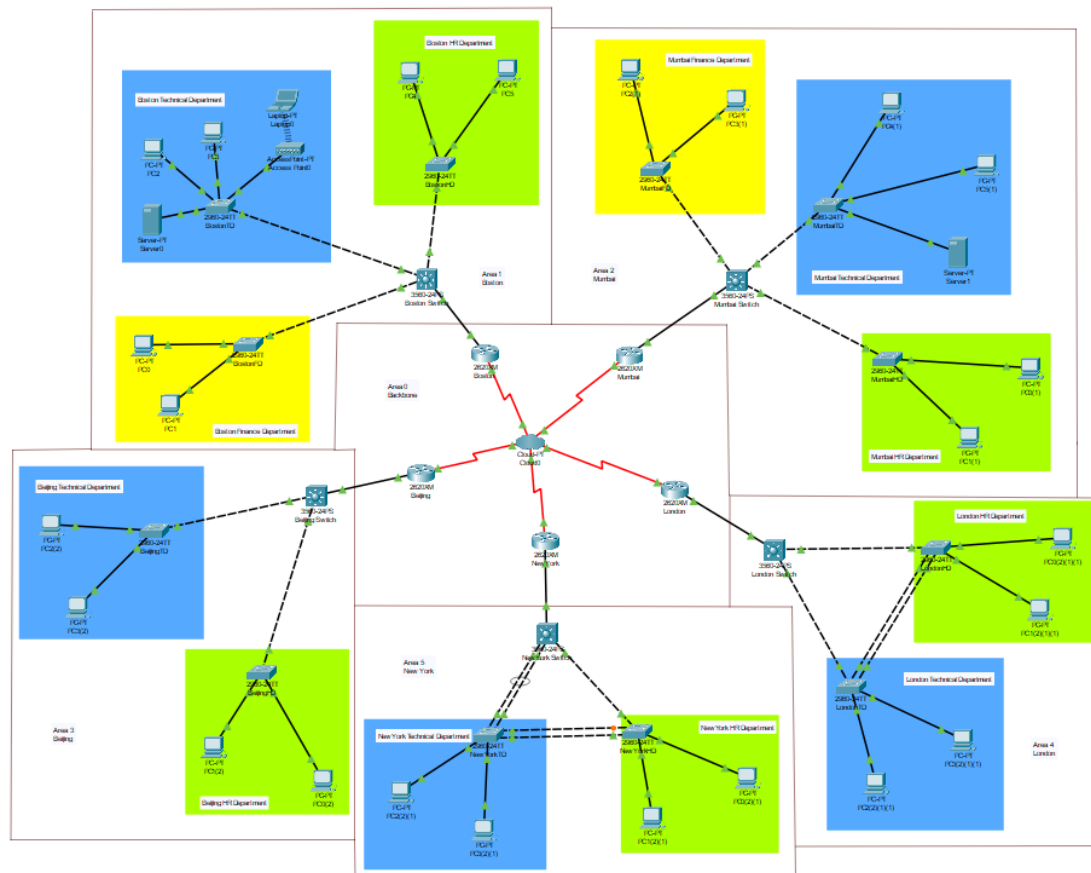
NUID: 001089667

Northeastern University

# TABLE OF CONTENTS

<b>Project 2 .....</b>	<b>0</b>
<i>Project Design:</i> .....	2
Cost: .....	2
Assignment of IP address .....	2
<i>Detailed Network Architecture:</i> .....	3
Physical structure: .....	3
OSPF: .....	3
HSRP: .....	4
VLAN: .....	4
Rapid STP, switch redundancy, Port fast and BPDU guard: .....	5
Frame Relay: .....	5
MAC flooding attack: .....	5
Access-List: .....	6
DHCP server: .....	8
LACP: .....	9
<i>Take Away Questions:</i> .....	11
<i>Test Plan for the Network:</i> .....	12
VLAN: .....	12
Routing protocol: .....	14
Security plan: .....	23
Redundancy plan: .....	24
Add-ons: .....	25
<i>Concepts learned during the project:</i> .....	30
<i>Conclusion:</i> .....	31

## Project Design:



## Cost:

Model	Price / \$	Quantity
Cisco 2620XM Router	1,640	5
Cisco 3560-24PS Switch	2,167	5
Cisco 2960-24TT Switch	1,403	12

Total cost:  $1640 * 5 + 2167 * 5 + 1403 * 12 = 35,871$

The total cost of the network is \$35,871.

## Assignment of IP address

The IP that I am provided is 192.168.67.0/19 (NUIID: 001089667), which is actually 192.168.64.0/19. To meet the requirement of the redundancy of 85%, each office should be offered more than  $250 / 85\% = 295$  IP addresses. So I offer each office a /23 subnet which holds  $256 * 2 - 2 = 510$  IP addresses that can meet the requirement of the

redundancy. So the IP addresses of the whole network is listed as the following diagram.  
(FD = Finance Department; HD = HR Department; TD = Technical Department)

BostonFD	BostonTD	BostonHD	MumbaiFD	MumbaiHD	MumbaiTD
192.168.64.0	192.168.66.0	192.168.68.0	192.168.70.0	192.168.72.0	192.168.74.0
BeijingHD	BeijingTD	NewYorkHD	NewYorkTD	LondonHD	LondonTD
192.168.76.0	192.168.78.0	192.168.80.0	192.168.82.0	192.168.84.0	192.168.86.0

The backbone network is provided IP subnet 192.168.95.0/23.

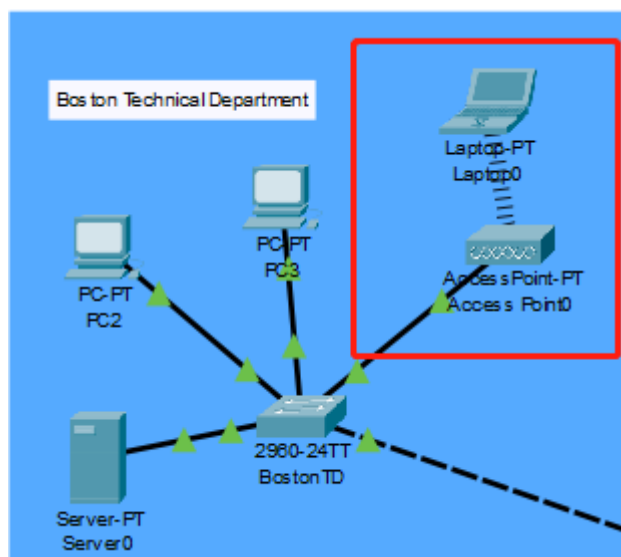
## Detailed Network Architecture:

### Physical structure:

In each city, a three-layer switch is used to separate the three or two departments. The IP routing function in the switches are turned on to separate the VLANs. In each city, each department is provided a different VLAN which belongs to a particular /23 subnet as is listed in the previous section.

The Multilayer switches are connected to the five backbone routers directly, and the five backbone routers are connected to each other through the PT-cloud to implement the Frame Relay to improve the data rate.

An access-point is added in the technical department of Boston office and a laptop is connected to it through wireless connection. It is shown as the following picture:



### OSPF:

The OSPF routing protocols are set in the routers and the Multilayer switches. The subnets that are connected directly to the devices are added to the OSPF list in it, and

the network can broadcast the OSPF lists so that the packages can find their ways to the destination. The subnets that are used in the backbone area are the five /30 subnets of the /23 subnet 192.168.95.0/23 which contains only two hosts to avoid the overlap and can also save more IP addresses. While setting the OSPF protocol, the offices are configured in separate areas: Boston-Area 1, Mumbai- Area2, Beijing- Area3, London-Area 4 and New York- Area5 and Backbone network as area 0.

The router-id of the OSPF routers are also set related to their areas. The setting is are listed as the following diagram: (S = Multilayer Switch, R = Router)

BostonR	MumbaiR	BeijingR	LondonR	NewYorkR
1.1.1.1	2.2.2.2	3.3.3.3	4.4.4.4	5.5.5.5
BostonS	MumbaiS	BeijingS	LondonS	NewYorkS
6.6.6.6	7.7.7.7	8.8.8.8	9.9.9.9	10.10.10.10

## HSRP:

The Hot Standby Router Protocol is a protocol that belongs to cisco which is used to build a fault-tolerant default gateway. The router that has the highest priority in the network will require the ARP and ND requests. When the primary router fails, the router that has the secondary priority will take over the duty to respond the request.

The HSRP is implemented by the Multilayer switch in Boston and Mumbai office and the Hello timer is changed to 2s, the hold timer is changed to 6s. The settings are showed as the following picture:

```
standby 1 ip 192.168.95.253
standby 1 priority 120
standby 1 preempt
standby 1 timers 2 6
```

## VLAN:

Each department in each office are provided a different VLAN related to their own subnet that is provided to them. In Boston office, finance department is provided the VLAN number 4, technical department is provided the VLAN number 3, HR department is provided the VLAN number 2. In other offices, In Mumbai office, finance department is provided the VLAN number 10, technical department is provided the VLAN number 30, HR department is provided the VLAN number 20. In other offices, HR departments are provided VLAN number 10 and technical departments are provided VLAN number 20. The VLANs are allowed on trunk and the native VLAN of Boston is set to VLAN number 2, Mumbai is set to VLAN number 20 and the other offices are set to VLAN number 10 which are the VLAN number of the HR department of theirs.

### **Rapid STP, switch redundancy, Port fast and BPDU guard:**

The Rapid STP and switch redundancy are set in New York and London offices. The setting is shown as the following picture in which the native VLAN, VLAN number 10, is set to a higher priority.

```
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 20 priority 4096
spanning-tree vlan 10 priority 28672
```

The setting of BPDU guard is also shown in the previous picture, and the setting of port fast is shown as the following picture:

```
interface FastEthernet0/2
 switchport access vlan 20
 spanning-tree portfast
```

### **Frame Relay:**

Frame Relay is a way of connection between LANs or WANs to reach a cost-efficient data transmission.

In this project, a PT-Cloud is used to establish the Frame Relay network. To make sure the routing list is broadcast through the Frame Relay network, two logical interfaces are built in each interface of the routers that is connected to the PT-Cloud. As an example, The Serial 1/0 interface of the Boston Router is divided into two point-to-point interfaces which are Serial 1/0.1 and Serial 1/0.2. These two interfaces are forced to point different routers. In this case, Serial 1/0.1 points to Serial 1/0.2 of Mumbai Router and Serial 1/0.2 points to Serial 1/0.1 of Beijing Router. Through this way, the OSPF routing list can be broadcast through the network.

The setting of DLCI in this project is simple which only have two DLCIs in each router pointing to their two neighbors. Through this way, it's easier to set but the package that has the destination which isn't adjacent to it need to go through the PT-Cloud one more time which may spend more time. If the all four destinations are set to the Frame Relay system, the phenomenon could be solved.

### **MAC flooding attack:**

MAC flooding attack is the case that the attacker sends a huge number of Ethernet Frames to fill the MAC address table of the switch. The switch will then broadcast the packages in the network which means the attacker can get the package too.

There are several ways to defend the MAC flooding attack. The way that is used in the project is the port-security. The setting of one of the switches is shown as the following picture:

```

interface FastEthernet0/1
 switchport trunk native vlan 2
 switchport mode trunk
 switchport port-security
 switchport port-security maximum 10
 switchport port-security violation protect
 switchport port-security mac-address 0123.ABCD.0001
 switchport port-security mac-address 0123.ABCD.0002

```

The HQ location is considered as Boston office. So the three switches in the three departments in Boston office are set to port-security mode.

## Access-List:

The access-list is a list that can determine which packages could pass the port.

In project 2, two requirements should use the ACL to access.

The first one is the requirement that finance departments can reach other departments but not reverse and two finance departments can reach each other. This requirement is met through the setting of the ACL in the Multilayer switch in Boston and Mumbai. The settings of the ACLs are listed as the following pictures:

Boston:

```

access-list 1 deny any
ip access-list extended out
 permit icmp any 192.168.64.0 0.0.1.255 echo-reply
 permit icmp 192.168.70.0 0.0.1.255 192.168.64.0 0.0.1.255

interface Vlan4
 mac-address 00d0.d3b5.9503
 ip address 192.168.64.1 255.255.254.0
 ip helper-address 192.168.66.4
 ip access-group out out

```

Mumbai:

```

ip access-list extended out
 permit icmp any 192.168.70.0 0.0.1.255 echo-reply
 permit icmp 192.168.64.0 0.0.1.255 192.168.70.0 0.0.1.255

interface Vlan10
 mac-address 00d0.582c.c901
 ip address 192.168.70.1 255.255.254.0
 ip helper-address 192.168.66.4
 ip access-group out out

```

In this case, permit icmp any 192.168.64.0 0.0.1.255 echo-reply permits Boston Financial Department to reach other departments, otherwise, the reply of the message sent out from the Boston Financial Department will be rejected. Permit icmp 192.168.70.0 0.0.1.255 192.168.64.0 0.0.1.255 permits Mumbai Financial Department to reach Boston Financial Department. The similar setting is set in the Mumbai switch. The second requirement is that ABR in Boston can reach other ABRs but not reverse and the technical department in Boston alone has an access to ABR in Boston. The settings are listed as the following pictures:

```

ip access-list extended in
  permit icmp 192.168.66.0 0.0.1.255 192.168.95.252 0.0.0.3
  permit icmp 192.168.66.0 0.0.1.255 192.168.95.248 0.0.0.3
  permit icmp 192.168.66.0 0.0.1.255 192.168.95.240 0.0.0.3
  permit icmp any 192.168.95.252 0.0.0.3 echo-reply
  permit icmp any 192.168.95.248 0.0.0.3 echo-reply
  permit icmp any 192.168.95.240 0.0.0.3 echo-reply
ip access-list extended in1
  permit udp any any
  permit ospf any any
  permit tcp any any
  permit icmp any any echo-reply
  deny icmp 192.168.64.0 0.0.1.255 host 192.168.95.254
  deny icmp 192.168.68.0 0.0.1.255 host 192.168.95.254
  permit icmp any any
  permit ip any any
ip access-list extended in2
  permit udp any any
  permit ospf any any
  permit tcp any any
  permit icmp any any echo-reply
  deny icmp any host 192.168.95.249
  permit icmp any any
  permit ip any any
ip access-list extended in3
  permit udp any any
  permit ospf any any
  permit tcp any any
  permit icmp any any echo-reply
  deny icmp any host 192.168.95.241
  permit icmp any any
  permit ip any any

interface FastEthernet0/0
  ip address 192.168.95.254 255.255.255.252
  ip access-group in1 in
  duplex auto
  speed auto

interface Serial1/0.1 point-to-point
  bandwidth 64
  ip address 192.168.95.249 255.255.255.252
  frame-relay interface-dlci 102
  ip access-group in2 in
!
interface Serial1/0.2 point-to-point
  bandwidth 64
  ip address 192.168.95.241 255.255.255.252
  frame-relay interface-dlci 105
  ip access-group in3 in

```

First, let's discuss the access-list that is used in the fa0/0 port which is the access list in. The first three sentences in the list in ensure that the technical department in Boston can reach the Boston ABR. In fact, the first sentence alone is enough for the requirement, the other two are used to make sure it works. The following three sentences ensures that the Boston ABR can reach other devices. The rest access from those are not listed are denied through the default "deny any any" sentence in the end of the list.

When it comes to the second and the third access-list which are actually similar to each other, the first three sentences are written to make sure that UDP, OSPF and TCP connections won't be influenced. The fourth sentence is written to make sure that the replies won't be rejected. The following sentence is written to deny the icmp packages



from the other devices which means they can no longer access Boston ABR. As the access-list works in order and stops when the requirements are fulfilled, the next sentence which is permit icmp any any is written to ensure the other icmp packages won't be rejected and the last sentence is written to ensure the other internet protocols can work as usual.

## DHCP server:

The DHCP servers are located in the technical departments of Boston and Mumbai. The DHCP server in Boston is in charge of the IP addressing of Boston office and Mumbai office. The DHCP server in Mumbai is in charge of the IP addressing of the rest three offices. The DHCP servers are set as the following pictures:

Boston DHCP server:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.66.1	0.0.0.0	192.168.66.0	255.255.255.0	255	0.0.0.0	0.0.0.0
BostonTD	192.168.66.1	0.0.0.0	192.168.66.2	255.255.254.0	510	0.0.0.0	0.0.0.0
BostonHD	192.168.66.1	0.0.0.0	192.168.66.2	255.255.254.0	510	0.0.0.0	0.0.0.0
MumbaiTD	192.168.74.1	0.0.0.0	192.168.74.2	255.255.254.0	510	0.0.0.0	0.0.0.0
MumbaiHD	192.168.72.1	0.0.0.0	192.168.72.2	255.255.254.0	510	0.0.0.0	0.0.0.0
MumbaiFD	192.168.70.1	0.0.0.0	192.168.70.2	255.255.254.0	510	0.0.0.0	0.0.0.0
BostonFD	192.168.64.1	0.0.0.0	192.168.64.2	255.255.254.0	510	0.0.0.0	0.0.0.0

Mumbai DHCP server:

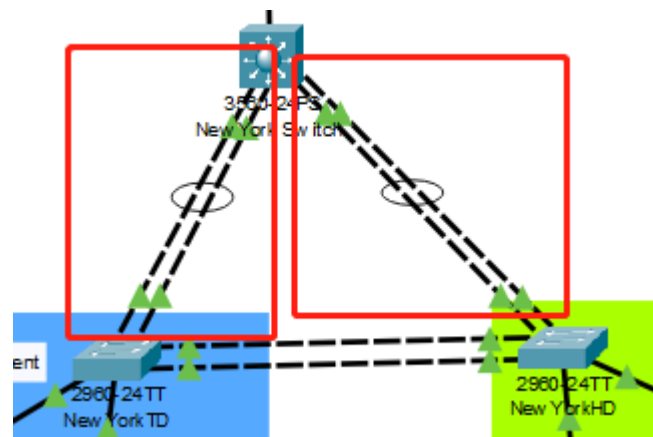
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	0.0.0.0	0.0.0.0	192.168.88.0	255.255.255.0	255	0.0.0.0	0.0.0.0
LondonTD	192.168.86.1	0.0.0.0	192.168.86.2	255.255.254.0	510	0.0.0.0	0.0.0.0
LondonHD	192.168.84.1	0.0.0.0	192.168.84.2	255.255.254.0	510	0.0.0.0	0.0.0.0
NewYorkTD	192.168.82.1	0.0.0.0	192.168.82.2	255.255.254.0	510	0.0.0.0	0.0.0.0
NewYorkHD	192.168.80.1	0.0.0.0	192.168.80.2	255.255.254.0	510	0.0.0.0	0.0.0.0
BeijingTD	192.168.78.1	0.0.0.0	192.168.78.2	255.255.254.0	510	0.0.0.0	0.0.0.0
BeijingHD	192.168.76.1	0.0.0.0	192.168.76.2	255.255.254.0	510	0.0.0.0	0.0.0.0

The IP address of the DHCP server in Boston is 192.168.66.4 which means the ip-helper address in the VLAN interfaces of the Multilayer switches in both Boston and Mumbai should be 192.168.66.4. Those of Beijing, New York and London are 192.168.74.4 which is the IP address of the DHCP server in Mumbai.

## LACP:

Link Aggregation Control Protocol (LACP) allows multiple physical connections between devices in network, especially between switches so that it can reduce the cost of breakdowns.

In this project, LACP is used between the Multilayer switches and the other switches in New York office. The physical connection is shown as the following picture:



The two connections in the red rectangles are the connections that have implements LACP. The settings are listed as following pictures:

```
interface Port-channel1
  switchport access vlan 20
  switchport trunk native vlan 10
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Port-channel2
  switchport access vlan 10
  switchport trunk native vlan 10
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface FastEthernet0/1
  switchport access vlan 10
  switchport trunk native vlan 10
  switchport trunk encapsulation dot1q
  switchport mode trunk
  channel-group 2 mode active
  spanning-tree portfast
!
interface FastEthernet0/2
  switchport access vlan 20
  switchport trunk native vlan 10
  switchport trunk encapsulation dot1q
  switchport mode trunk
  channel-group 1 mode active
  shutdown
```

```

interface FastEthernet0/3
  no switchport
  ip address 192.168.95.222 255.255.255.252
  duplex auto
  speed auto
!
interface FastEthernet0/4
  switchport access vlan 20
  switchport trunk native vlan 10
  switchport trunk encapsulation dot1q
  switchport mode trunk
  channel-group 1 mode active
!
interface FastEthernet0/5
  switchport access vlan 10
  switchport trunk native vlan 10
  switchport trunk encapsulation dot1q
  switchport mode trunk
  channel-group 2 mode active
  shutdown

```

Port 4 and 2 are grouped together while port 1 and 5 are grouped together. One of the connections should be shut down in each group. So port fa0/2 and fa0/5 are shut down. All of the ports in the Multilayer switch side are set to active. So the ports in the other side could be any state. They are set to passive in this project. The setting of one of the other switches is shown as the following picture:

```

interface Port-channel1
  switchport access vlan 20
  switchport trunk native vlan 10
  switchport mode trunk
!
interface FastEthernet0/1
  switchport access vlan 20
  switchport trunk native vlan 10
  switchport mode trunk
  channel-group 1 mode passive
!
interface FastEthernet0/2
  switchport access vlan 20
  spanning-tree portfast
!
interface FastEthernet0/3
  switchport access vlan 20
  spanning-tree portfast
!
interface FastEthernet0/4
  switchport access vlan 20
  switchport mode trunk
  channel-group 1 mode passive
!

```

## Take Away Questions:

### 1. Routing Protocol OSPF: Explain the following

- **Which one is better Routing protocol RIPv2 or OSPF? Why? Explain why do we use the area concept in OSPF?**

It depends on the scale of the network. When it's small, RIPv2 is better because OSPF is more complicated and it needs intense memory and CPU. When it's large, OSPF is better because RIPv2 need to send the RIP list to every router in the network but OSPF don't. We use the area concept in OSPF because it can segment the network topology into pieces which can help manage the network.

- **Why do we configure backbone network as area 0?**

We consider the backbone network as a whole area to avoid routing loop. Otherwise, there will be much more redundant paths.

- **List and explain the different types of LSA in OSPF**

1. Router LSA: routers within an area will flood Router LSA, and send packets to each other that contains its neighbors and its own information.

2. Network LSA: generated by the Designated Router and created for multi-access network.

3. Summary LSA: generated by ABR, and flooded to multiple areas.

4. Summary ASBR LSA: generated by the ABR to advertise the presence and router ID of an ASBR to other areas.

5. ASBR External LSA: generated by the ASBR to pass the information of external routers.

6. Multicast OSPF LSA: support multicast routing, it is not support and widely used.

7. Not-so-stubby area LSA: generated by ASBR to mask the Type 5 packets for passing through the areas that blocks the external routers.

8. External attribute LSA for BGP: used to work with Border Gateway Protocol.

9. a link-local "opaque" LSA (defined by RFC2370) in OSPFv2 and the Intra-Area-Prefix LSA in OSPFv3. It is the OSPFv3 LSA that contains prefixes for stub and transit networks in the link-state ID. It is also used for IETF NSF (Non-Stop Forwarding).

10. an area-local "opaque" LSA as defined by RFC2370. Opaque LSAs contain information which should be flooded by other routers even if the router is not able to understand the extended information itself. Typically type 10 LSAs are used for traffic engineering (MPLS-TE) extensions to OSPF for creating the Traffic Engineering Database (TED), by flooding extra information about links beyond just their metric, such as link bandwidth and color.

11. an AS "opaque" LSA defined by RFC 5250, which is flooded everywhere except stub areas. This is the opaque equivalent of the type 5 external LSA.

### 2. Security and Redundancy plan

Security plan: Network security plan is a plan to protect the hardware, software and data in the network system from damage, change and leakage due to accidental or

malicious reasons.

Redundancy plan: Redundancy plan is a guarantee strategy of industrial network. It helps reduce the risk of unexpected interruption and ensure the continuity of production through immediate response, so as to reduce the impact of any point of failure on the critical data flow.

### 3. How does STP avoid looping? Explain its working in detail

First, a root bridge is chosen. The other bridges will then decide which is the shortest way to the root bridge and block the other paths. So the looping could be avoided.

### 4. Difference between STP, PVSTP and MSTP.

STP is used to avoid looping, broadcast storms. PVSTP is used for the switches containing different VLANs and it is defined in 802.1d standard. In this case, VLAN need to set an example of STP with the goal that we can change the parameters for each VLAN. MSTP is similar to PVSTP but it works with RSTP instead of STP. It is defined in 802.1s standard.

## Test Plan for the Network:

### VLAN:

Use the instruction “do show r” in the privilege mode of the switches to check whether the interfaces are set to the right state: trunk or access, the setting of the VLANs, whether the native VLAN on the trunk is set to the VLAN of the HR department also requires consideration, and whether the VLANs allowed on trunk consist only of the VLANs used in the networks.

Take Boston as an example, the result is shown as the following pictures:

Multilayer switch:

```
interface FastEthernet0/1
switchport access vlan 4
switchport trunk native vlan 2
switchport trunk allowed vlan 2-4
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/2
switchport access vlan 3
switchport trunk native vlan 2
switchport trunk allowed vlan 2-4
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 2
switchport trunk native vlan 2
switchport trunk allowed vlan 2-4
switchport trunk encapsulation dot1q
switchport mode trunk
```

HR department switch:

```
interface FastEthernet0/1
  switchport trunk native vlan 2
  switchport trunk allowed vlan 2
  switchport mode trunk
  switchport port-security
  switchport port-security maximum 10
  switchport port-security violation protect
  switchport port-security mac-address 0123.ABCD.0001
  switchport port-security mac-address 0123.ABCD.0002
!
interface FastEthernet0/2
  switchport access vlan 2
  spanning-tree portfast
!
interface FastEthernet0/3
  switchport access vlan 2
  spanning-tree portfast
!
```

Technical department switch:

```
interface FastEthernet0/1
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3
  switchport mode trunk
  switchport port-security
  switchport port-security maximum 10
  switchport port-security violation protect
!
interface FastEthernet0/2
  switchport access vlan 3
  spanning-tree portfast
!
interface FastEthernet0/3
  switchport access vlan 3
  spanning-tree portfast
!
interface FastEthernet0/4
  switchport access vlan 3
  spanning-tree portfast
!
```

Finance department switch:

```
interface FastEthernet0/1
  switchport access vlan 4
  spanning-tree portfast
!
interface FastEthernet0/2
  switchport access vlan 4
  spanning-tree portfast
!
interface FastEthernet0/3
  switchport trunk native vlan 2
  switchport trunk allowed vlan 4
  switchport mode trunk
  switchport port-security
  switchport port-security maximum 10
  switchport port-security violation protect
!
```

## Routing protocol:

### OSPF:

Click on the Multilayer switches, execute “do show ip route” to see whether all the subnets of the whole network are in the list.

### Boston:

```
Switch0(config)#do show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.64.0/23 is directly connected, Vlan4
C    192.168.66.0/23 is directly connected, Vlan3
C    192.168.68.0/23 is directly connected, Vlan2
O IA 192.168.70.0/23 [110/1565] via 192.168.95.254, 00:09:14, FastEthernet0/4
O IA 192.168.72.0/23 [110/1565] via 192.168.95.254, 00:09:14, FastEthernet0/4
O IA 192.168.74.0/23 [110/1565] via 192.168.95.254, 00:09:14, FastEthernet0/4
O IA 192.168.76.0/23 [110/1565] via 192.168.95.254, 00:09:14, FastEthernet0/4
O IA 192.168.78.0/23 [110/1565] via 192.168.95.254, 00:09:14, FastEthernet0/4
O IA 192.168.80.0/23 [110/3127] via 192.168.95.254, 00:09:14, FastEthernet0/4
O IA 192.168.82.0/23 [110/3127] via 192.168.95.254, 00:09:14, FastEthernet0/4
O IA 192.168.84.0/23 [110/3127] via 192.168.95.254, 00:09:14, FastEthernet0/4
O IA 192.168.86.0/23 [110/3127] via 192.168.95.254, 00:09:14, FastEthernet0/4
    192.168.95.0/30 is subnetted, 10 subnets
O IA    192.168.95.216 [110/3126] via 192.168.95.254, 00:09:14, FastEthernet0/4
O IA    192.168.95.220 [110/3126] via 192.168.95.254, 00:09:14, FastEthernet0/4
O IA    192.168.95.224 [110/1564] via 192.168.95.254, 00:09:14, FastEthernet0/4
O IA    192.168.95.228 [110/3125] via 192.168.95.254, 00:09:24, FastEthernet0/4
O IA    192.168.95.232 [110/4687] via 192.168.95.254, 00:09:24, FastEthernet0/4
O IA    192.168.95.236 [110/3125] via 192.168.95.254, 00:09:24, FastEthernet0/4
O IA    192.168.95.240 [110/1563] via 192.168.95.254, 00:09:24, FastEthernet0/4
O IA    192.168.95.244 [110/1564] via 192.168.95.254, 00:09:14, FastEthernet0/4
O IA    192.168.95.248 [110/1563] via 192.168.95.254, 00:09:24, FastEthernet0/4
C    192.168.95.252 is directly connected, FastEthernet0/4
```

## Mumbai:

```
Switch(config)#do show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O IA 192.168.64.0/23 [110/1565] via 192.168.95.245, 00:11:23, FastEthernet0/4
O IA 192.168.66.0/23 [110/1565] via 192.168.95.245, 00:11:23, FastEthernet0/4
O IA 192.168.68.0/23 [110/1565] via 192.168.95.245, 00:11:23, FastEthernet0/4
C    192.168.70.0/23 is directly connected, Vlan10
C    192.168.72.0/23 is directly connected, Vlan20
C    192.168.74.0/23 is directly connected, Vlan30
O IA 192.168.76.0/23 [110/3127] via 192.168.95.245, 00:11:23, FastEthernet0/4
O IA 192.168.78.0/23 [110/3127] via 192.168.95.245, 00:11:23, FastEthernet0/4
O IA 192.168.80.0/23 [110/3127] via 192.168.95.245, 00:11:23, FastEthernet0/4
O IA 192.168.82.0/23 [110/3127] via 192.168.95.245, 00:11:23, FastEthernet0/4
O IA 192.168.84.0/23 [110/1565] via 192.168.95.245, 00:11:23, FastEthernet0/4
O IA 192.168.86.0/23 [110/1565] via 192.168.95.245, 00:11:23, FastEthernet0/4
    192.168.95.0/30 is subnetted, 10 subnets
O IA    192.168.95.216 [110/1564] via 192.168.95.245, 00:11:23, FastEthernet0/4
O IA    192.168.95.220 [110/3126] via 192.168.95.245, 00:11:23, FastEthernet0/4
O IA    192.168.95.224 [110/3126] via 192.168.95.245, 00:11:23, FastEthernet0/4
O IA    192.168.95.228 [110/1563] via 192.168.95.245, 00:11:33, FastEthernet0/4
O IA    192.168.95.232 [110/3125] via 192.168.95.245, 00:11:33, FastEthernet0/4
O IA    192.168.95.236 [110/4687] via 192.168.95.245, 00:11:33, FastEthernet0/4
O IA    192.168.95.240 [110/3125] via 192.168.95.245, 00:11:33, FastEthernet0/4
C    192.168.95.244 is directly connected, FastEthernet0/4
O IA    192.168.95.248 [110/1563] via 192.168.95.245, 00:11:33, FastEthernet0/4
O IA    192.168.95.252 [110/1564] via 192.168.95.245, 00:11:23, FastEthernet0/4
```

## Beijing:



```

interface FastEthernet0/1
  switchport access vlan 10
  switchport trunk native vlan 10

Switch(config)#do show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O IA 192.168.64.0/23 [110/1565] via 192.168.95.225, 00:12:04, FastEthernet0/3
O IA 192.168.66.0/23 [110/1565] via 192.168.95.225, 00:12:04, FastEthernet0/3
O IA 192.168.68.0/23 [110/1565] via 192.168.95.225, 00:12:04, FastEthernet0/3
O IA 192.168.70.0/23 [110/3127] via 192.168.95.225, 00:12:04, FastEthernet0/3
O IA 192.168.72.0/23 [110/3127] via 192.168.95.225, 00:12:04, FastEthernet0/3
O IA 192.168.74.0/23 [110/3127] via 192.168.95.225, 00:12:04, FastEthernet0/3
C    192.168.76.0/23 is directly connected, Vlan10
C    192.168.78.0/23 is directly connected, Vlan20
O IA 192.168.80.0/23 [110/1565] via 192.168.95.225, 00:12:04, FastEthernet0/3
O IA 192.168.82.0/23 [110/1565] via 192.168.95.225, 00:12:04, FastEthernet0/3
O IA 192.168.84.0/23 [110/3127] via 192.168.95.225, 00:12:04, FastEthernet0/3
O IA 192.168.86.0/23 [110/3127] via 192.168.95.225, 00:12:04, FastEthernet0/3
    192.168.95.0/30 is subnetted, 10 subnets
O IA    192.168.95.216 [110/3126] via 192.168.95.225, 00:12:04, FastEthernet0/3
O IA    192.168.95.220 [110/1564] via 192.168.95.225, 00:12:04, FastEthernet0/3
C    192.168.95.224 is directly connected, FastEthernet0/3
O IA    192.168.95.228 [110/4687] via 192.168.95.225, 00:12:14, FastEthernet0/3
O IA    192.168.95.232 [110/3125] via 192.168.95.225, 00:12:14, FastEthernet0/3
O IA    192.168.95.236 [110/1563] via 192.168.95.225, 00:12:14, FastEthernet0/3
O IA    192.168.95.240 [110/1563] via 192.168.95.225, 00:12:14, FastEthernet0/3
O IA    192.168.95.244 [110/3126] via 192.168.95.225, 00:12:04, FastEthernet0/3
O IA    192.168.95.248 [110/3125] via 192.168.95.225, 00:12:14, FastEthernet0/3
O IA    192.168.95.252 [110/1564] via 192.168.95.225, 00:12:04, FastEthernet0/3

```

## New York:

```

Switch(config)#do show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O IA 192.168.64.0/23 [110/3127] via 192.168.95.221, 00:12:52, FastEthernet0/3
O IA 192.168.66.0/23 [110/3127] via 192.168.95.221, 00:12:52, FastEthernet0/3
O IA 192.168.68.0/23 [110/3127] via 192.168.95.221, 00:12:52, FastEthernet0/3
O IA 192.168.70.0/23 [110/3127] via 192.168.95.221, 00:12:52, FastEthernet0/3
O IA 192.168.72.0/23 [110/3127] via 192.168.95.221, 00:12:52, FastEthernet0/3
O IA 192.168.74.0/23 [110/3127] via 192.168.95.221, 00:12:52, FastEthernet0/3
O IA 192.168.76.0/23 [110/1565] via 192.168.95.221, 00:12:52, FastEthernet0/3
O IA 192.168.78.0/23 [110/1565] via 192.168.95.221, 00:12:52, FastEthernet0/3
C    192.168.80.0/23 is directly connected, Vlan10
C    192.168.82.0/23 is directly connected, Vlan20
O IA 192.168.84.0/23 [110/1565] via 192.168.95.221, 00:12:52, FastEthernet0/3
O IA 192.168.86.0/23 [110/1565] via 192.168.95.221, 00:12:52, FastEthernet0/3
    192.168.95.0/30 is subnetted, 10 subnets
O IA    192.168.95.216 [110/1564] via 192.168.95.221, 00:12:52, FastEthernet0/3
C    192.168.95.220 is directly connected, FastEthernet0/3
O IA    192.168.95.224 [110/1564] via 192.168.95.221, 00:12:52, FastEthernet0/3
O IA    192.168.95.228 [110/3125] via 192.168.95.221, 00:13:02, FastEthernet0/3
O IA    192.168.95.232 [110/1563] via 192.168.95.221, 00:13:02, FastEthernet0/3
O IA    192.168.95.236 [110/1563] via 192.168.95.221, 00:13:02, FastEthernet0/3
O IA    192.168.95.240 [110/3125] via 192.168.95.221, 00:13:02, FastEthernet0/3
O IA    192.168.95.244 [110/3126] via 192.168.95.221, 00:12:52, FastEthernet0/3
O IA    192.168.95.248 [110/4687] via 192.168.95.221, 00:13:02, FastEthernet0/3
O IA    192.168.95.252 [110/3126] via 192.168.95.221, 00:12:52, FastEthernet0/3

```

London:

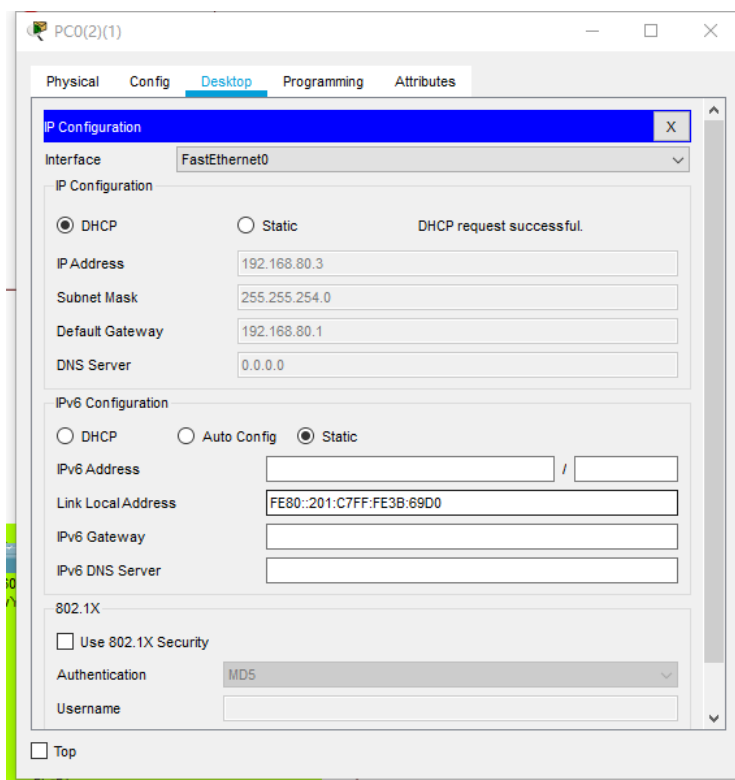
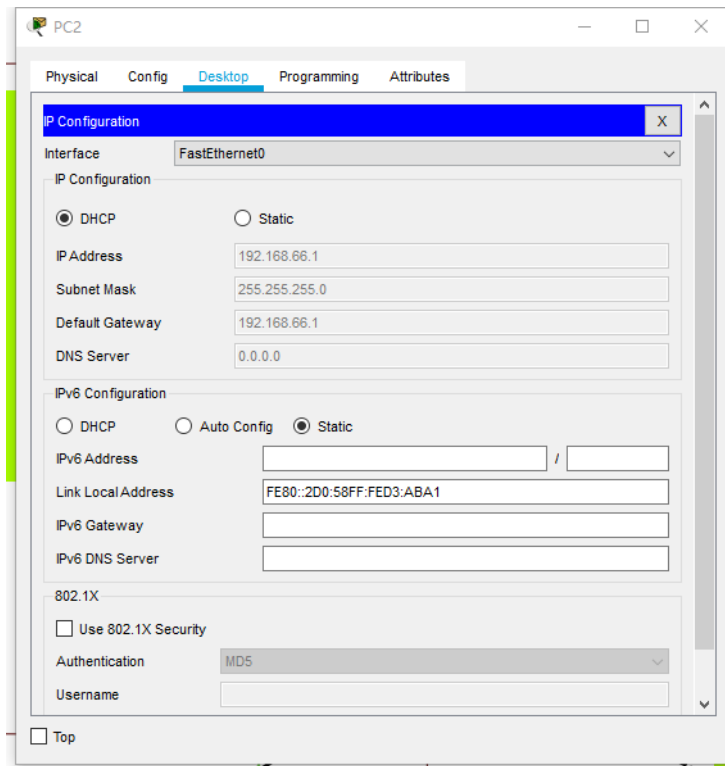
```
Switch(config)#do show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

O IA 192.168.64.0/23 [110/3127] via 192.168.95.217, 00:13:24, FastEthernet0/3
O IA 192.168.66.0/23 [110/3127] via 192.168.95.217, 00:13:24, FastEthernet0/3
O IA 192.168.68.0/23 [110/3127] via 192.168.95.217, 00:13:24, FastEthernet0/3
O IA 192.168.70.0/23 [110/1565] via 192.168.95.217, 00:13:24, FastEthernet0/3
O IA 192.168.72.0/23 [110/1565] via 192.168.95.217, 00:13:24, FastEthernet0/3
O IA 192.168.74.0/23 [110/1565] via 192.168.95.217, 00:13:24, FastEthernet0/3
O IA 192.168.76.0/23 [110/3127] via 192.168.95.217, 00:13:24, FastEthernet0/3
O IA 192.168.78.0/23 [110/3127] via 192.168.95.217, 00:13:24, FastEthernet0/3
O IA 192.168.80.0/23 [110/1565] via 192.168.95.217, 00:13:24, FastEthernet0/3
O IA 192.168.82.0/23 [110/1565] via 192.168.95.217, 00:13:24, FastEthernet0/3
C    192.168.84.0/23 is directly connected, Vlan10
C    192.168.86.0/23 is directly connected, Vlan20
    192.168.95.0/30 is subnetted, 10 subnets
C      192.168.95.216 is directly connected, FastEthernet0/3
O IA   192.168.95.220 [110/1564] via 192.168.95.217, 00:13:24, FastEthernet0/3
O IA   192.168.95.224 [110/3126] via 192.168.95.217, 00:13:24, FastEthernet0/3
O IA   192.168.95.228 [110/1563] via 192.168.95.217, 00:13:34, FastEthernet0/3
O IA   192.168.95.232 [110/1563] via 192.168.95.217, 00:13:34, FastEthernet0/3
O IA   192.168.95.236 [110/3125] via 192.168.95.217, 00:13:34, FastEthernet0/3
O IA   192.168.95.240 [110/4687] via 192.168.95.217, 00:13:34, FastEthernet0/3
O IA   192.168.95.244 [110/1564] via 192.168.95.217, 00:13:24, FastEthernet0/3
O IA   192.168.95.248 [110/3125] via 192.168.95.217, 00:13:34, FastEthernet0/3
O IA   192.168.95.252 [110/3126] via 192.168.95.217, 00:13:24, FastEthernet0/3
```


DHCP:

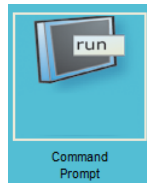
Click on any one of the computers in the network. In the “ip configuration” section, click on DHCP to gain IP address. This may fail at the first time. If it fails, click on “Static” and then click on “DHCP” again to refresh several times. The result is show as the follow pictures:




## ACL:

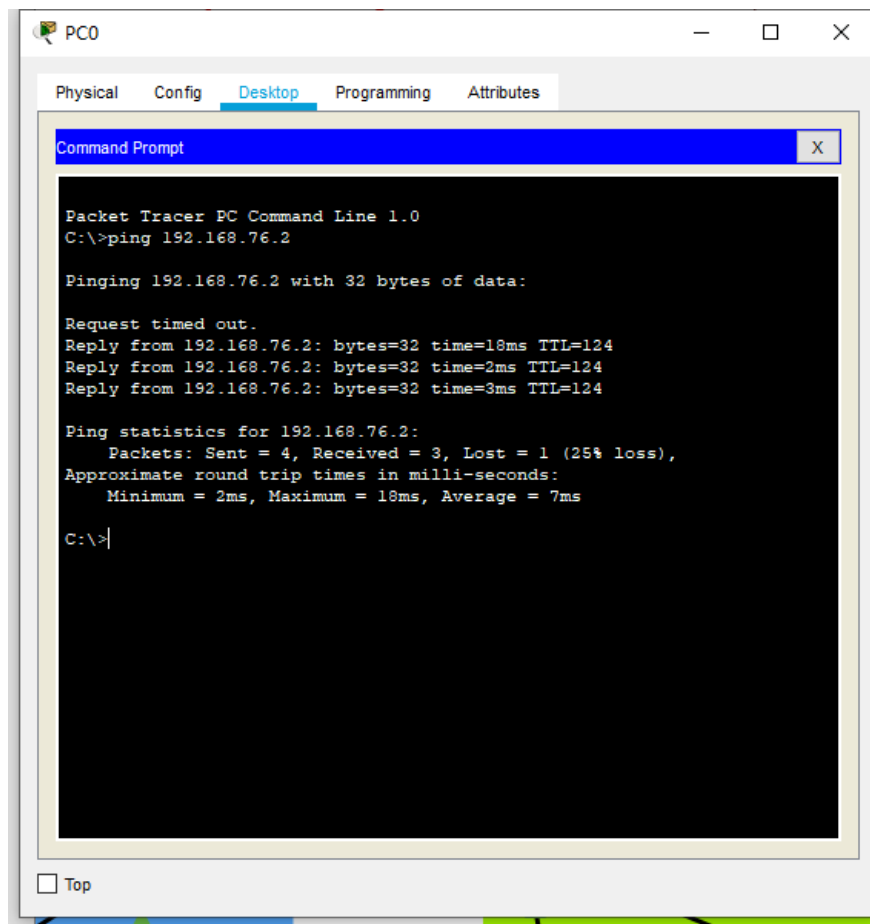
There are two parts while testing ACL. First one is that Finance departments shouldn't be accessed by any other departments, but Finance can access any other department, two Finance departments can access each other, and all other departments should be able to access each other

To test this, click on  button, click on the computer you want to start the ping and then the other one you want to receive it. It's an easy way to test but hard to get



screenshots. Use the  can also test this one. The results are shown as the following pictures:

Boston finance department ping Beijing HR department:



The first one always gets timed out.

Boston finance department ping Mumbai finance department:

The screenshot shows a Packet Tracer PC window for PC0. The 'Desktop' tab is active, displaying a Command Prompt window. The Command Prompt shows the execution of two ping commands. The first command is 'ping 192.168.76.2', which results in a 'Request timed out.' followed by three successful replies from 192.168.76.2 with times of 18ms, 2ms, and 3ms. The second command is 'ping 192.168.70.2', which results in four successful replies from 192.168.70.2 with times of 2ms, 2ms, 2ms, and 3ms. The ping statistics for 192.168.70.2 are highlighted with a red box, showing 4 packets sent, 4 received, and 0% loss.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.76.2

Pinging 192.168.76.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.76.2: bytes=32 time=18ms TTL=124
Reply from 192.168.76.2: bytes=32 time=2ms TTL=124
Reply from 192.168.76.2: bytes=32 time=3ms TTL=124

Ping statistics for 192.168.76.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 18ms, Average = 7ms

C:\>ping 192.168.70.2

Pinging 192.168.70.2 with 32 bytes of data:

Reply from 192.168.70.2: bytes=32 time=2ms TTL=124
Reply from 192.168.70.2: bytes=32 time=2ms TTL=124
Reply from 192.168.70.2: bytes=32 time=2ms TTL=124
Reply from 192.168.70.2: bytes=32 time=3ms TTL=124

Ping statistics for 192.168.70.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>
```

Beijing HR department ping Boston finance department:

The screenshot shows a Packet Tracer PC window for PC1(2). The 'Desktop' tab is active, displaying a Command Prompt window. The Command Prompt shows the execution of a ping command 'ping 192.168.64.2'. The result shows four 'Destination host unreachable' messages from 192.168.95.253. The ping statistics for 192.168.64.2 show 4 packets sent, 0 received, and 100% loss.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.64.2

Pinging 192.168.64.2 with 32 bytes of data:

Reply from 192.168.95.253: Destination host unreachable.
Reply from 192.168.95.253: Destination host unreachable.
Reply from 192.168.95.253: Destination host unreachable.
Reply from 192.168.95.253: Destination host unreachable.

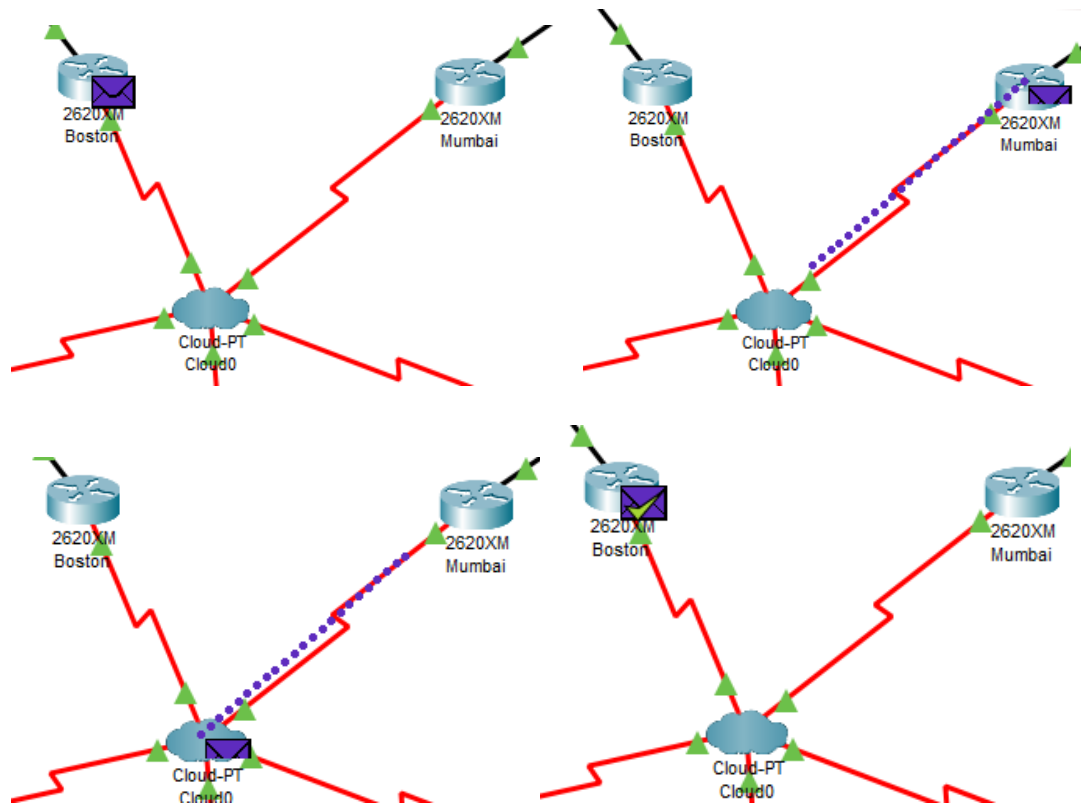
Ping statistics for 192.168.64.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

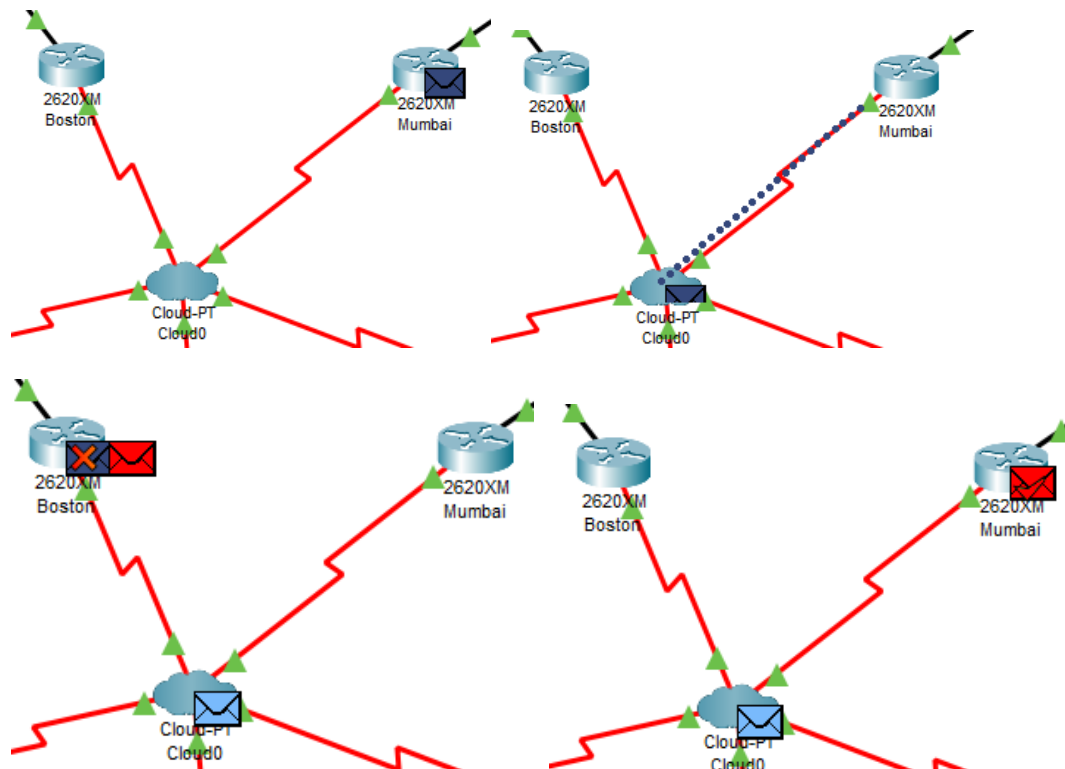
The second part is to test Area Border Router (ABR) in Boston can access all other

locations ABR but not reverse. A technical department from Boston alone has an access to ABR of Boston.

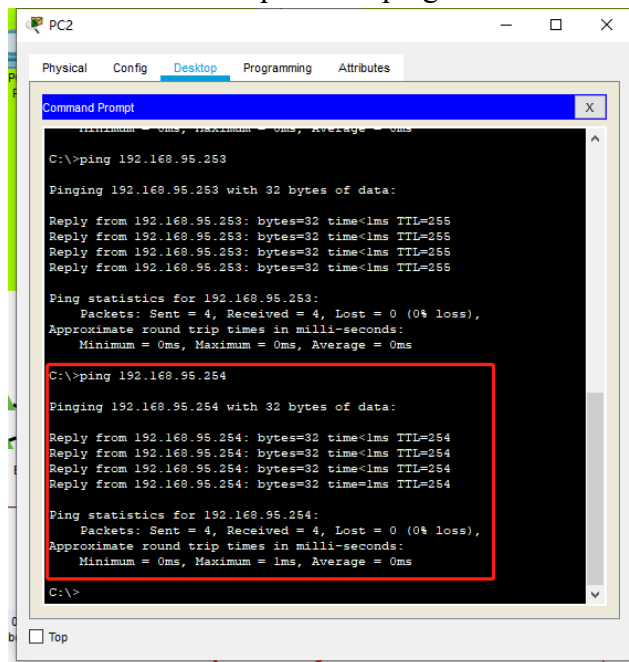
Boston ABR ping Mumbai ABR:



Mumbai ABR ping Boston ABR:



Boston technical department ping Boston ABR:



The screenshot shows a Windows Command Prompt window titled 'PC2'. The window has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes', with 'Desktop' selected. The command prompt shows the following output:

```
C:\>ping 192.168.95.253

Pinging 192.168.95.253 with 32 bytes of data:

Reply from 192.168.95.253: bytes=32 time<1ms TTL=255
Reply from 192.168.95.253: bytes=32 time<1ms TTL=255
Reply from 192.168.95.253: bytes=32 time<1ms TTL=255
Reply from 192.168.95.253: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.95.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.95.254

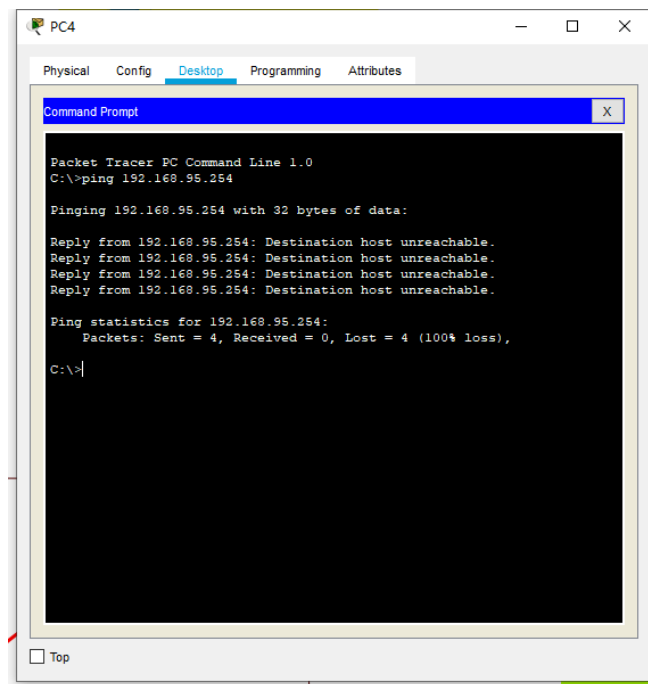
Pinging 192.168.95.254 with 32 bytes of data:

Reply from 192.168.95.254: bytes=32 time<1ms TTL=254
Reply from 192.168.95.254: bytes=32 time<1ms TTL=254
Reply from 192.168.95.254: bytes=32 time<1ms TTL=254
Reply from 192.168.95.254: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.95.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Boston HR department ping Boston ABR:



The screenshot shows a Packet Tracer PC Command Line window titled 'PC4'. The window has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes', with 'Desktop' selected. The command prompt shows the following output:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.95.254

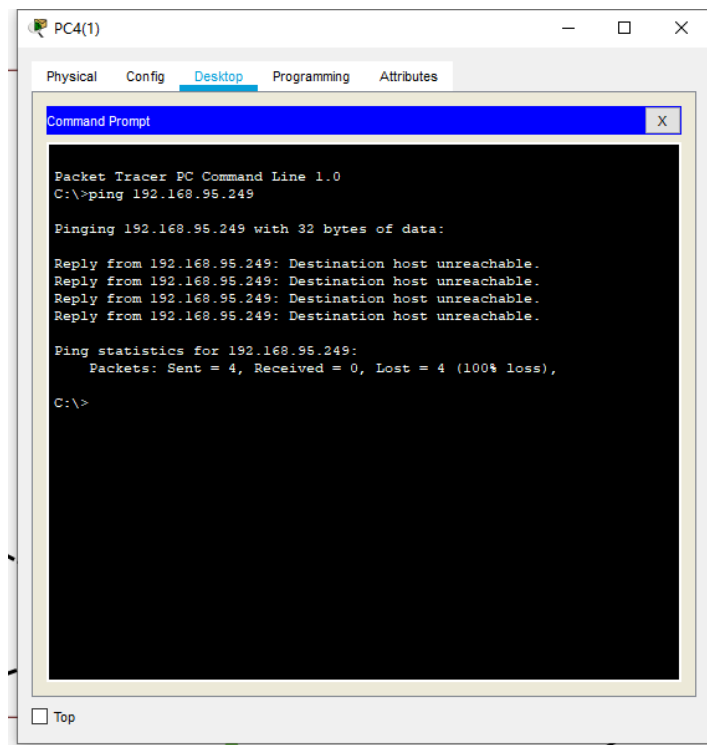
Pinging 192.168.95.254 with 32 bytes of data:

Reply from 192.168.95.254: Destination host unreachable.
Reply from 192.168.95.254: Destination host unreachable.
Reply from 192.168.95.254: Destination host unreachable.
Reply from 192.168.95.254: Destination host unreachable.

Ping statistics for 192.168.95.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Mumbai technical department ping Boston ABR:



HSRP:

Use “do show r” to check the configuration:

```

interface FastEthernet0/4
  no switchport
  ip address 192.168.95.253 255.255.255.252
  duplex auto
  speed auto
  standby 1 ip 192.168.95.253
  standby 1 priority 120
  standby 1 preempt
  standby 1 timers 2 6

```

## Security plan:

To test security plan, an efficient way is to check the configuration in the HQ location. HQ location is considered as the three departments in Boston. So the three switches are set in the security mode. The results are shown as the following pictures:

Port-security:

Boston HR department switch:

```

interface FastEthernet0/1
  switchport trunk native vlan 2
  switchport trunk allowed vlan 2
  switchport mode trunk
  switchport port-security
  switchport port-security maximum 10
  switchport port-security violation protect
  switchport port-security mac-address 0123.ABCD.0001
  switchport port-security mac-address 0123.ABCD.0002

```



## Redundancy plan:

STP:

Check whether the ports are set to STP portfast mode using “do show r”:

Boston HR department:

```
interface FastEthernet0/1
  switchport trunk native vlan 2
  switchport trunk allowed vlan 2
  switchport mode trunk
  switchport port-security
  switchport port-security maximum 10
  switchport port-security violation protect
  switchport port-security mac-address 0123.ABCD.0001
  switchport port-security mac-address 0123.ABCD.0002
!
interface FastEthernet0/2
  switchport access vlan 2
  spanning-tree portfast
!
interface FastEthernet0/3
  switchport access vlan 2
  spanning-tree portfast
!
```

Check whether the switches are set to PVST mode and whether the bpduguard is set using “do show r”:

Boston HR department:

```
spanning-tree mode pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
```

In London and New York offices, check whether priorities are set correctly using “do show r”:

London Multilayer switch:

```
spanning-tree mode pvst
spanning-tree vlan 20 priority 0
spanning-tree vlan 10 priority 20480
spanning-tree vlan 1-9,11-19,21-4094 priority 24576
.
```

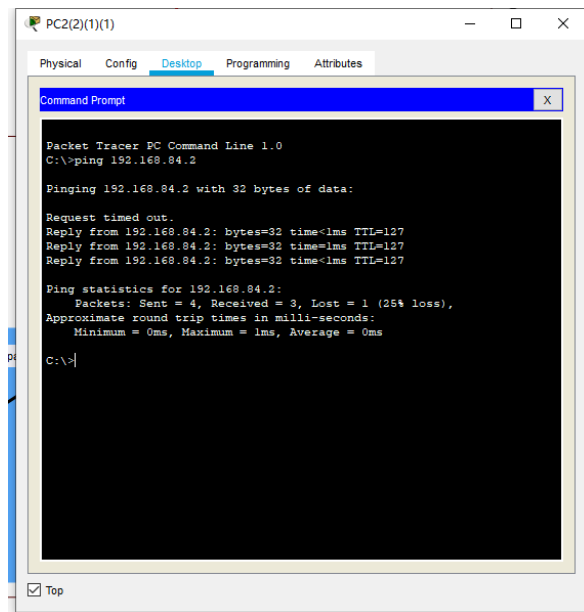
London other switches:

```
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 20 priority 4096
spanning-tree vlan 10 priority 24576
!
```

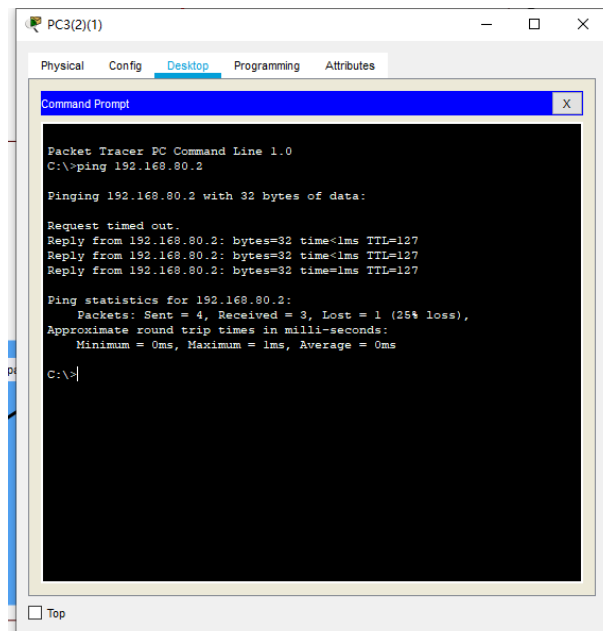
Vlan 20 is set as the root bridge.

Then, check whether the terminals can access each other in the offices:

London:



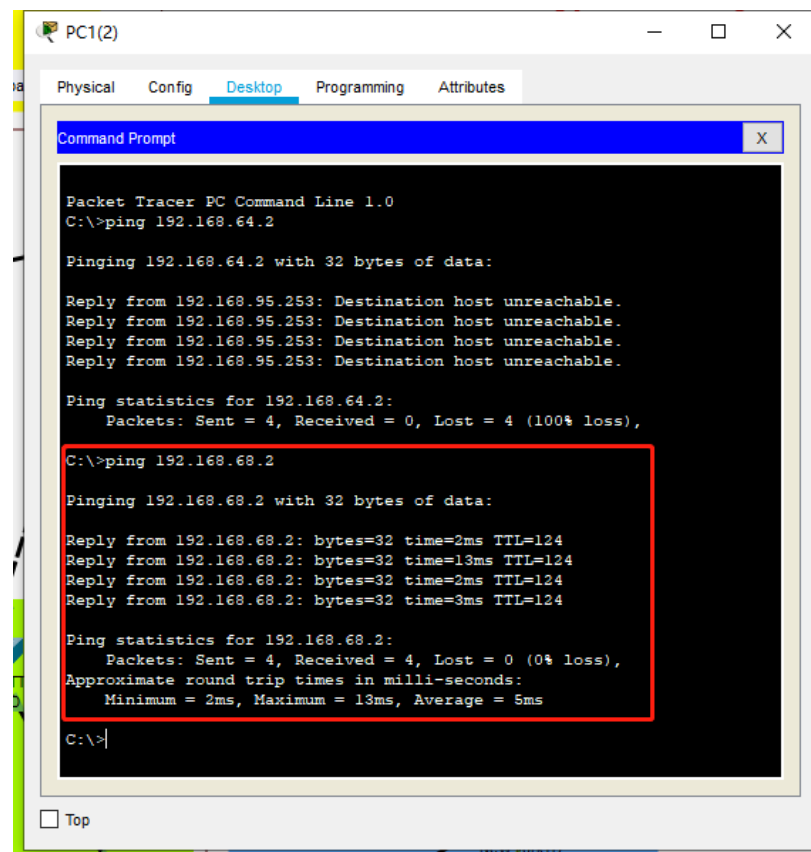
New York:



## Add-ons:

Multi-layer is actually used in every office in this project. I determined the structure of using the multi-layer switches before I saw the add-ons. The discussions are mostly covered in the previous discussions. To test more, we can check whether the terminals in Beijing office can reach terminals in other offices and see the configuration of the multilayer switch in Beijing office:

Beijing HR department ping Boston HR department:



### Configuration of Beijing multilayer switch:

```
ip routing
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
|
!
!
!
!
!
interface FastEthernet0/1
    switchport access vlan 10
    switchport trunk native vlan 10
    switchport trunk allowed vlan 10,20
    switchport trunk encapsulation dot1q
    switchport mode trunk
    switchport nonegotiate
```

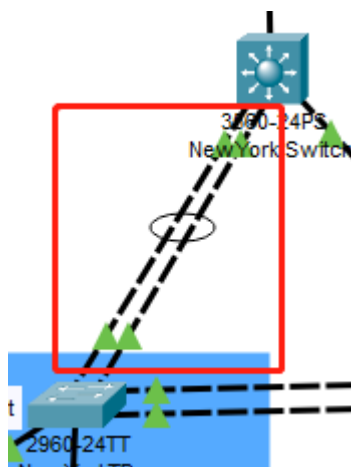
```

interface FastEthernet0/2
  switchport access vlan 20
  switchport trunk native vlan 10
  switchport trunk allowed vlan 10,20
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport nonegotiate
!
interface FastEthernet0/3
  no switchport
  ip address 192.168.95.226 255.255.255.252
  duplex auto
  speed auto
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan10
  mac-address 0005.5eea.a301
  ip address 192.168.76.1 255.255.254.0
  ip helper-address 192.168.74.4
!
interface Vlan20
  mac-address 0005.5eea.a302
  ip address 192.168.78.1 255.255.254.0
  ip helper-address 192.168.74.4
!
router ospf 1
  router-id 8.8.8.8
  log-adjacency-changes
  network 192.168.95.224 0.0.0.3 area 3
  network 192.168.76.0 0.0.1.255 area 3
  network 192.168.78.0 0.0.1.255 area 3
!
router rip
  network 192.168.76.0
  network 192.168.78.0
!

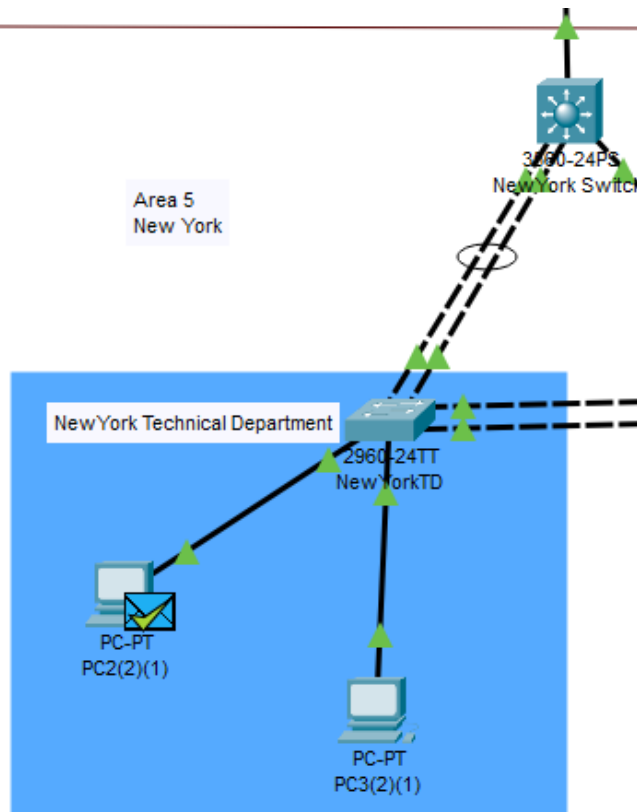
```

RIP is actually not necessary in this project, the settings of RIP in the project can all be ignored.

LACP:



As shown in the picture is the LACP I used in New York office. To test this protocol, checking on the path of the package that New York technical department pings the multilayer switch is an efficient way:



0.000	--	PC2	ICMP
0.000	--	PC2(2)(1)	ICMP
0.000	--	PC2(2)(1)	ARP
0.001	PC2	BostonTD	ICMP
0.001	PC2(2)(1)	NewYorkTD	ARP
0.002	BostonTD	Boston Switch	ICMP
0.002	NewYorkTD	PC3(2)(1)	ARP
0.002	NewYorkTD	NewYorkHD	ARP
0.002	NewYorkTD	NewYorkHD	ARP
0.002	NewYorkTD	NewYork S...	ARP
0.003	Boston Switch	Boston	ICMP
0.003	NewYork Switch	NewYorkTD	ARP
0.004	Boston	Boston Switch	ICMP
0.004	NewYorkTD	PC2(2)(1)	ARP
0.004	--	PC2(2)(1)	ICMP
0.005	Boston Switch	BostonTD	ICMP
0.005	PC2(2)(1)	NewYorkTD	ICMP
0.006	BostonTD	PC2	ICMP
0.006	NewYorkTD	NewYork S...	ICMP
0.007	NewYork Switch	NewYorkTD	ICMP
0.008	NewYorkTD	PC2(2)(1)	ICMP

As is shown in the pictures, the package actually goes through the EtherChannel which means it is working correctly.

The setting of the EtherChannel is shown as the following pictures:

Multilayer switch:

```
interface Port-channel1
switchport access vlan 20
switchport trunk native vlan 10
switchport trunk allowed vlan 20
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/1
switchport access vlan 10
switchport trunk native vlan 10
switchport trunk allowed vlan 2-1001
switchport trunk encapsulation dot1q
switchport mode trunk
spanning-tree portfast
!
interface FastEthernet0/2
switchport access vlan 20
switchport trunk native vlan 10
switchport trunk allowed vlan 20
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode passive
!
interface FastEthernet0/3
no switchport
ip address 192.168.95.222 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/4
switchport access vlan 20
switchport trunk native vlan 10
switchport trunk allowed vlan 20
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode passive
!
```

Normal switch:

```
interface Port-channel1
switchport access vlan 20
switchport trunk native vlan 10
switchport trunk allowed vlan 20
switchport mode trunk
!
interface FastEthernet0/1
switchport access vlan 20
switchport trunk native vlan 10
switchport trunk allowed vlan 20
switchport mode trunk
channel-group 1 mode active
!
interface FastEthernet0/2
switchport access vlan 20
spanning-tree portfast
!
interface FastEthernet0/3
switchport access vlan 20
spanning-tree portfast
!
interface FastEthernet0/4
switchport access vlan 20
switchport trunk native vlan 10
switchport trunk allowed vlan 20
switchport mode trunk
channel-group 1 mode active
!
```

## Concepts learned during the project:

**VLAN:** Virtual local area network (VLAN), is a LAN based switching technology (Switch) network management technology, through which the network management personnel can effectively dispatch the messages in and out of the LAN to the correct access port through the control switch, so as to achieve the logical grouping management of the devices in the different entity LAN, and reduce the blocking problem caused by too many useless messages when a large number of data flows in the LAN, and improve the information of the LAN Security.

**DHCP:** Dynamic Host Configuration Protocol (DHCP) is a LAN network protocol. It refers to the range of IP address controlled by the server. When the client logs in to the server, it can automatically obtain the IP address and subnet mask assigned by the server.

**OSPF:** Open shortest path first (OSPF) is a routing protocol based on IP protocol. It is a widely used IGP protocol on large and medium-sized networks. OSPF is an implementation of link state routing protocol, which operates in the autonomous system.

**HSRP:** The design goal of the Hot Backup Router Protocol (HSRP) is to support the IP traffic failover without confusion under specific circumstances, to allow the host to use a single router, and to maintain the connectivity between routers even if the actual first hop router fails to use. The condition to implement HSRP is that there are multiple routers in the system, which form a "hot backup group", which forms a virtual router. In other words, when the source host cannot dynamically know the IP address of the first hop router, the HSRP protocol can protect the first hop router from failure.

**STP:** Spanning tree protocol (STP) is a second layer (data link layer) communication protocol working in OSI network model. Its basic application is to prevent the loops generated by redundant links of switches. It is used to ensure the logical topology without loops in Ethernet, so as to avoid broadcast storm and occupy a lot of switch resources

**Frame relay:** Frame relay is a new public data network communication protocol, which emerged in 1992. It began to develop rapidly in 1994. Frame relay is an effective data transmission technology, which can transmit digital information quickly and cheaply in one-to-one or one to many applications. It can be used in voice and data communication, as well as LAN and WAN communication. Each frame relay user will get a dedicated line to the frame relay node. For end users, frame relay network processes data transmission with other users through a channel that is often changed and invisible to users.

**MAC flooding attack:** MAC flooding attack is the case that the attacker sends a huge

number of Ethernet Frames to fill the MAC address table of the switch. The switch will then broadcast the packages in the network which means the attacker can get the package too.

**ABR:** ABR is a router that connects one or more OSPF areas to the backbone.

**Multilayer switch:** Multilayer switch is a kind of switch which combines two-layer switch and three-layer routing function.

**EtherChannel:** EtherChannel combines more than two physical interfaces into one logical interface for use. There are three setting methods: Static (on mode), PAgP (Port Aggregation Protocol) and LACP (Link Aggregation Control Protocol).

## **Conclusion:**

This project is a complete one that includes many of the knowledge we learnt about the network this semester. The project helps me review the knowledge and even have a deeper learning of them.

This project also helps me get familiar with the configuration of the network which I have never touched upon. The configuration of the network should be very important in my future work as a network engineer. It's even very useful in my daily life since we are always facing problems of setting Wi-Fi or LANs in our home. It also helps us solve internet fails as well.

In fact, it's really a hard time working on the project because the mostly used way for me to gain related knowledge is the internet where some of the knowledge is not that comprehensive which confuses me a lot sometimes. There are also some remaining problems I have not yet figured out since the time is limited, and I will keep on working on these problems even if the due date is passed because they really helps me a lot.