Project 3

Difeng Li

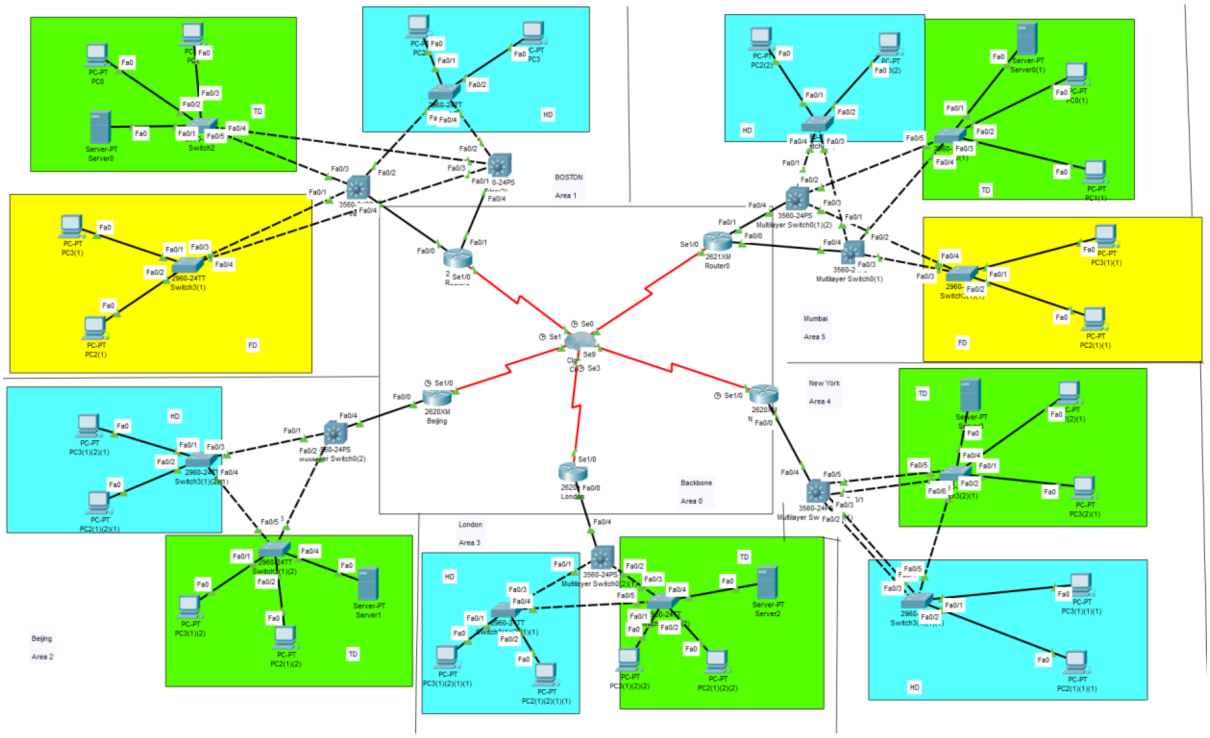
NUID: 001050353

Northeastern University

TABLE OF CONTENTS

Project Design:

Topological graph:



Green Area ----- Technical Department

Yellow Area ---- Finance Department

Blue Area ----- HR Department

Cost:

Model	Price / $	Quantity
Cisco 2620XM Router	100	3
Cisco 2621XM Router	150	2
Cisco 3560-24PS Switch	250	7
Cisco 2960-24TT Switch	250	12

Total cost: $5350

Assignment of IP address

In order to meet the requirement that each office has 50 IP addresses, the IP address I provided is 192.168.0.0/24 to meet this requirement. Therefore, the subnet available for each office contains 256-2 = 254 IP addresses to meet the redundancy requirements. So, the IP address of the whole network is shown in the figure below. (FD = Finance Department; HD = HR

Department; TD = Technical Department).

BostonFD	BostonTD	BostonHD	MumbaiFD	MumbaiHD	MumbaiTD
192.168.2.0	192.168.0.0	192.168.1.0	192.168.5.0	192.168.4.0	192.168.3.0
BeijingHD	BeijingTD	NewYorkHD	NewYorkTD	LondonHD	LondonTD
192.168.11.0	192.168.10.0	192.168.9.0	192.168.8.0	192.168.7.0	192.168.6.0

Detailed Network Architecture:

OSPF:

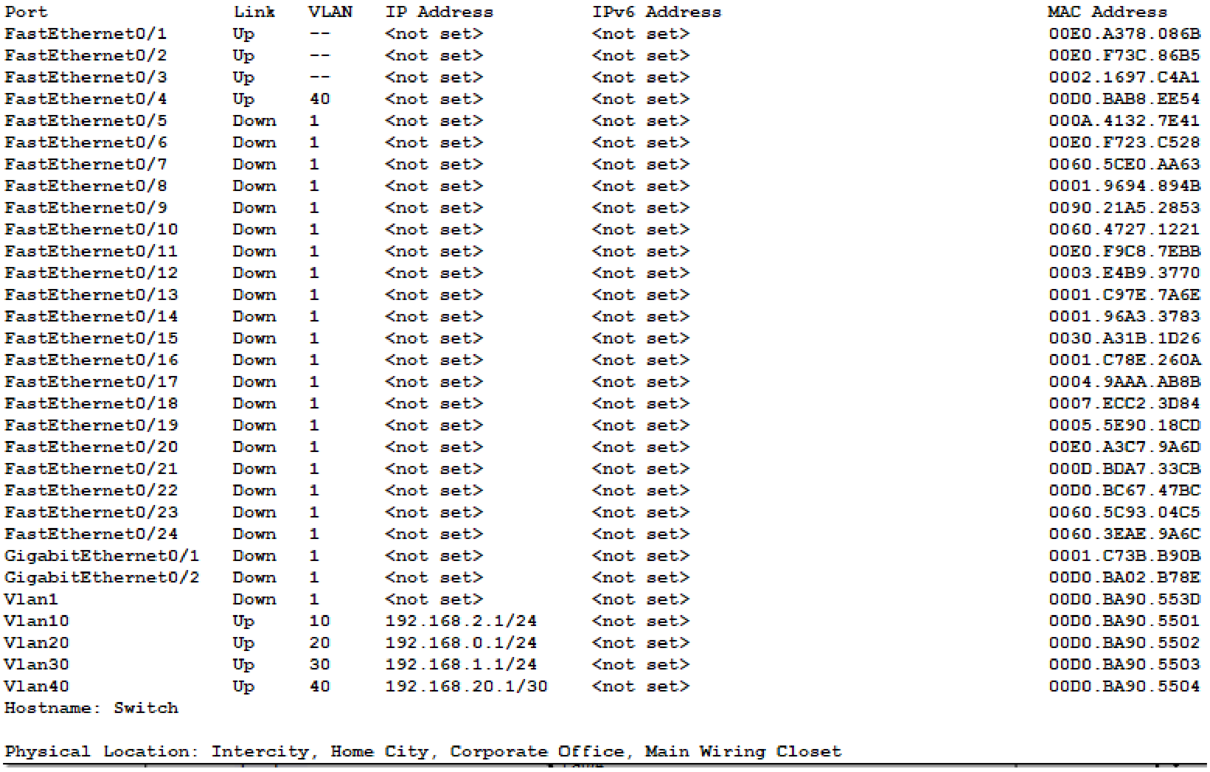
The OSPF routing protocols are set in the routers and the Multilayer switches. The subnets that are connected directly to the devices are added to the OSPF list in it, and the network can broadcast the OSPF lists so that the packages can find their ways to the destination. The subnets that are used in 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, and at the same time, it would not waste any IP. While setting the OSPF protocol, the offices are configured in separate areas: Boston-Area 1, Mumbai- Area5, Beijing- Area2, London-Area 3 and New York- Area4 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)

Boston2R	Boston1R	Mumbai2R	Mumbai1R	BeijingR	LondonR	NewYorkR
192.168.20.1	192.168.21.1	192.168.60.1	192.168.61.1	192.168.30.1	192.168.40.1	192.168.50.1
Boston2S	Boston1S	Mumbai2R	Mumbai1R	BeijingS	LondonS	NewYorkS
192.168.20.2	192.168.21.2	192.168.60.2	192.168.61.2	192.168.30.2	192.168.40.2	192.168.50.2

VLAN:

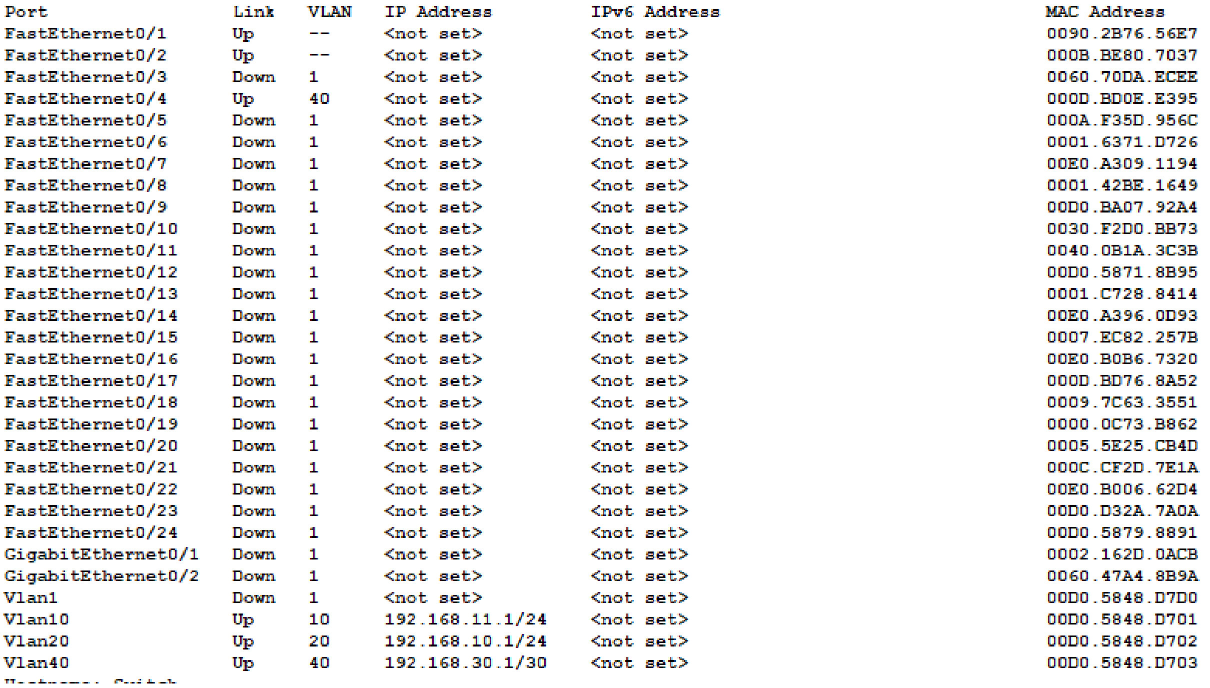
Each department in each office is provided a different VLAN related to its own subnet that is provided to them. In Boston office, the finance department is provided the VLAN number 10, the technical department is provided the VLAN number 20, HR department is provided the VLAN number 30. In other offices, In Mumbai office, the finance department is provided the VLAN number 10, the technical department is provided the VLAN number 20, HR department is provided the VLAN number 30. In other offices, HR departments are provided VLAN number 10 and technical departments are provided VLAN number 20. The VLANs are allowed on the trunk. At the same time, vlan40 is provided as the link between layer 3 switch and router in local offices. As shown in the figure below.

BOS Multilayer Switch:



```
Port                   Link   VLAN   IP Address          IPv6 Address                               MAC Address
FastEthernet0/1        Up     --     <not set>           <not set>                                  00E0.A378.086B
FastEthernet0/2        Up     --     <not set>           <not set>                                  00E0.F73C.86B5
FastEthernet0/3        Up     --     <not set>           <not set>                                  0002.1697.C4A1
FastEthernet0/4        Up     40     <not set>           <not set>                                  00D0.BAB8.EE54
FastEthernet0/5        Down   1      <not set>           <not set>                                  000A.4132.7E41
FastEthernet0/6        Down   1      <not set>           <not set>                                  00E0.F723.C528
FastEthernet0/7        Down   1      <not set>           <not set>                                  0060.5CE0.AA63
FastEthernet0/8        Down   1      <not set>           <not set>                                  0001.9694.894B
FastEthernet0/9        Down   1      <not set>           <not set>                                  0090.21A5.2853
FastEthernet0/10       Down   1      <not set>           <not set>                                  0060.4727.1221
FastEthernet0/11       Down   1      <not set>           <not set>                                  00E0.F9C8.7EBB
FastEthernet0/12       Down   1      <not set>           <not set>                                  0003.E4B9.3770
FastEthernet0/13       Down   1      <not set>           <not set>                                  0001.C97E.7A6E
FastEthernet0/14       Down   1      <not set>           <not set>                                  0001.96A3.3783
FastEthernet0/15       Down   1      <not set>           <not set>                                  0030.A31B.1D26
FastEthernet0/16       Down   1      <not set>           <not set>                                  0001.C78E.260A
FastEthernet0/17       Down   1      <not set>           <not set>                                  0004.9AAA.AB8B
FastEthernet0/18       Down   1      <not set>           <not set>                                  0007.ECC2.3D84
FastEthernet0/19       Down   1      <not set>           <not set>                                  0005.5E90.18CD
FastEthernet0/20       Down   1      <not set>           <not set>                                  00E0.A3C7.9A6D
FastEthernet0/21       Down   1      <not set>           <not set>                                  000D.BDA7.33CB
FastEthernet0/22       Down   1      <not set>           <not set>                                  00D0.BC67.47BC
FastEthernet0/23       Down   1      <not set>           <not set>                                  0060.5C93.04C5
FastEthernet0/24       Down   1      <not set>           <not set>                                  0060.3EAE.9A6C
GigabitEthernet0/1     Down   1      <not set>           <not set>                                  0001.C73B.B90B
GigabitEthernet0/2     Down   1      <not set>           <not set>                                  00D0.BA02.B78E
Vlan1                  Down   1      <not set>           <not set>                                  00D0.BA90.553D
Vlan10                 Up     10     192.168.2.1/24      <not set>                                  00D0.BA90.5501
Vlan20                 Up     20     192.168.0.1/24      <not set>                                  00D0.BA90.5502
Vlan30                 Up     30     192.168.1.1/24      <not set>                                  00D0.BA90.5503
Vlan40                 Up     40     192.168.20.1/30     <not set>                                  00D0.BA90.5504
Hostname: Switch

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

Beijing Multilayer Switch:

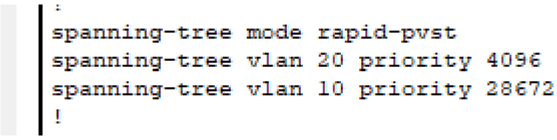


```
Port                   Link   VLAN   IP Address          IPv6 Address                               MAC Address
FastEthernet0/1        Up     --     <not set>           <not set>                                  0090.2B76.56E7
FastEthernet0/2        Up     --     <not set>           <not set>                                  000B.BE80.7037
FastEthernet0/3        Down   1      <not set>           <not set>                                  0060.70DA.ECEE
FastEthernet0/4        Up     40     <not set>           <not set>                                  000D.BD0E.E395
FastEthernet0/5        Down   1      <not set>           <not set>                                  000A.F35D.956C
FastEthernet0/6        Down   1      <not set>           <not set>                                  0001.6371.D726
FastEthernet0/7        Down   1      <not set>           <not set>                                  00E0.A309.1194
FastEthernet0/8        Down   1      <not set>           <not set>                                  0001.42BE.1649
FastEthernet0/9        Down   1      <not set>           <not set>                                  00D0.BA07.92A4
FastEthernet0/10       Down   1      <not set>           <not set>                                  0030.F2D0.BB73
FastEthernet0/11       Down   1      <not set>           <not set>                                  0040.0B1A.3C3B
FastEthernet0/12       Down   1      <not set>           <not set>                                  00D0.5871.8B95
FastEthernet0/13       Down   1      <not set>           <not set>                                  0001.C728.8414
FastEthernet0/14       Down   1      <not set>           <not set>                                  00E0.A396.0D93
FastEthernet0/15       Down   1      <not set>           <not set>                                  0007.EC82.257B
FastEthernet0/16       Down   1      <not set>           <not set>                                  00E0.B0B6.7320
FastEthernet0/17       Down   1      <not set>           <not set>                                  000D.BD76.8A52
FastEthernet0/18       Down   1      <not set>           <not set>                                  0009.7C63.3551
FastEthernet0/19       Down   1      <not set>           <not set>                                  0000.0C73.B862
FastEthernet0/20       Down   1      <not set>           <not set>                                  0005.5E25.CB4D
FastEthernet0/21       Down   1      <not set>           <not set>                                  000C.CF2D.7E1A
FastEthernet0/22       Down   1      <not set>           <not set>                                  00E0.B006.62D4
FastEthernet0/23       Down   1      <not set>           <not set>                                  00D0.D32A.7A0A
FastEthernet0/24       Down   1      <not set>           <not set>                                  00D0.5879.8891
GigabitEthernet0/1     Down   1      <not set>           <not set>                                  0002.162D.0ACB
GigabitEthernet0/2     Down   1      <not set>           <not set>                                  0060.47A4.8B9A
Vlan1                  Down   1      <not set>           <not set>                                  00D0.5848.D7D0
Vlan10                 Up     10     192.168.11.1/24     <not set>                                  00D0.5848.D701
Vlan20                 Up     20     192.168.10.1/24     <not set>                                  00D0.5848.D702
Vlan40                 Up     40     192.168.30.1/30     <not set>                                  00D0.5848.D703
Hostname: Switch
```

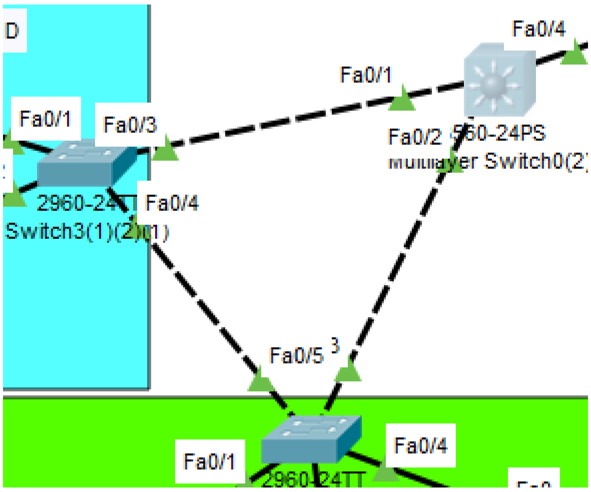
Rapid STP, switch redundancy, Port fast and BPDU guard:

The Rapid STP and switch redundancy is set in New York, Beijing and London offices. The setting is shown as the following picture in which the native VLAN, VLAN number 20, is set to a higher priority.

Beijing Multilayer Switch:

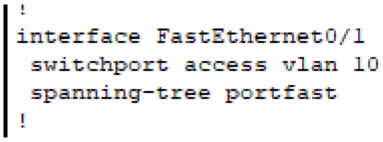


```
!
spanning-tree mode rapid-pvst
spanning-tree vlan 20 priority 4096
spanning-tree vlan 10 priority 28672
!
```



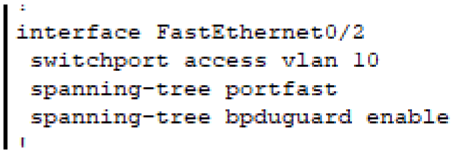
Connect the switch of HR department in Beijing with that of TD department.

The setting of port fast is shown as the following picture:



```
!
interface FastEthernet0/1
 switchport access vlan 10
 spanning-tree portfast
!
```

The setting of BPDU guard is also shown in the previous picture



```
!
interface FastEthernet0/2
 switchport access vlan 10
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

Frame Relay:

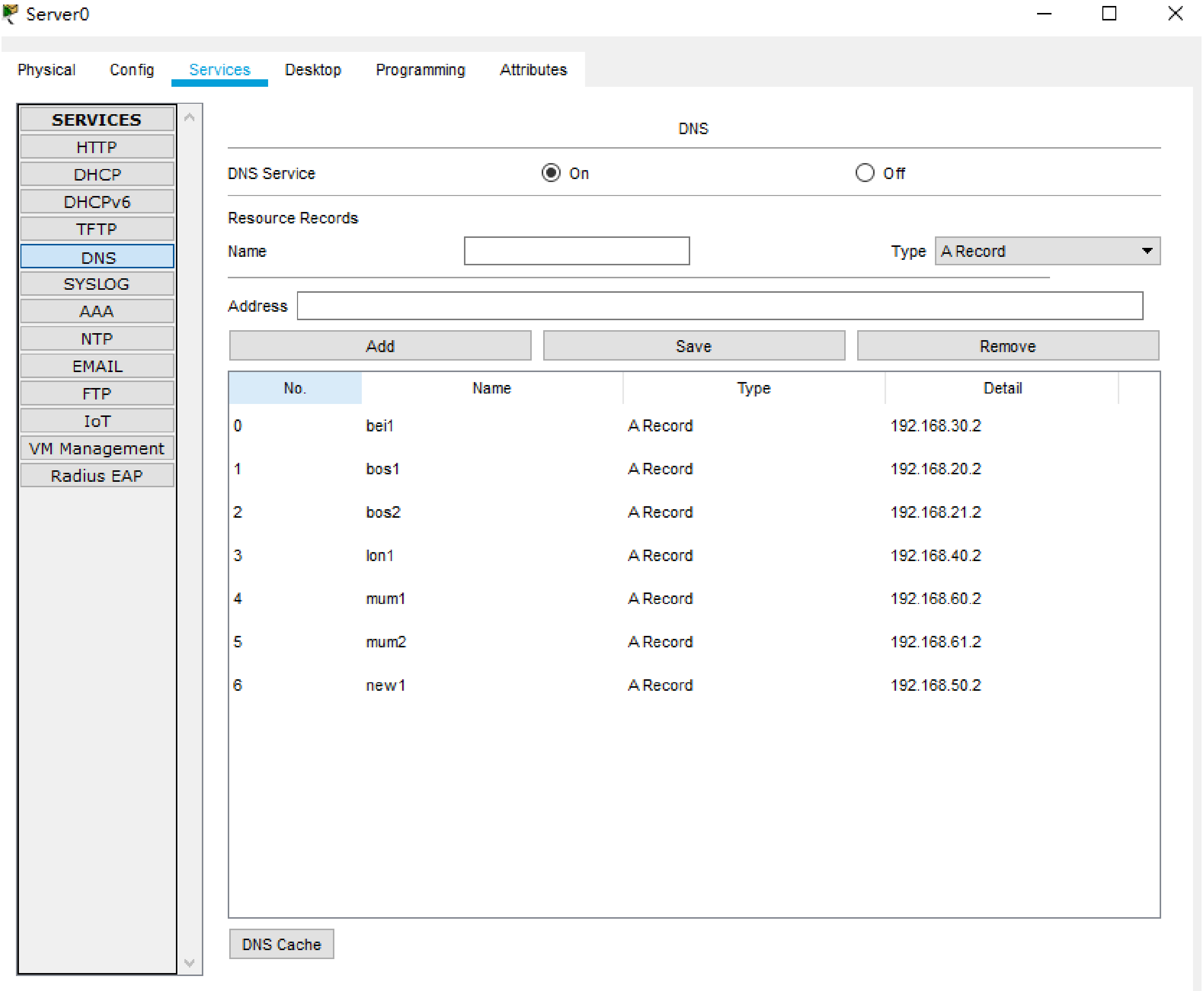
Frame Relay is a way of connecting between LANs or WANs to reach a cost-efficient data transmission.

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 are 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 to 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. In this way, the OSPF routing list can be broadcast through the network.

The setting of DLCI in this project is simple which only has 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 needs to go through the PT-Cloud one more time which may spend more time. If all four destinations are set to the Frame Relay system, the phenomenon could be solved.

DNS Configuration

Configure a DNS server in Boston Office. This server should be able to resolve the domain names of all the routers. As shown in the figure below.



DNS

DNS Service ● On ○ Off

Resource Records

Name

Type A Record

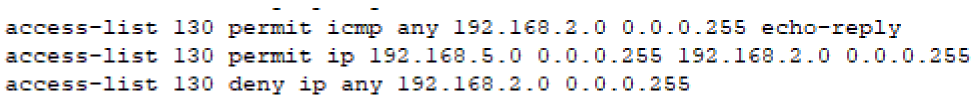
Address

No.	Name	Type	Detail
0	bei1	A Record	192.168.30.2
1	bos1	A Record	192.168.20.2
2	bos2	A Record	192.168.21.2
3	lon1	A Record	192.168.40.2
4	mum1	A Record	192.168.60.2
5	mum2	A Record	192.168.61.2
6	new1	A Record	192.168.50.2

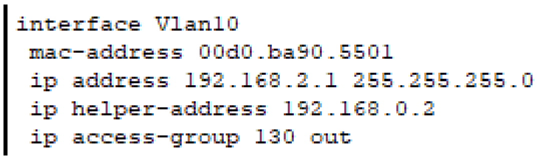
Access-List:

The access-list is a list that can determine which packages could pass the port.
In the project 3, three requirements should use the ACL to access.
The first one is the requirement that • Finance shouldn’t be accessed by any other departments, but Finance can access all other departments. (This filtering should be applied to all packets not just ICMP echo request/ ICMP reply). The second one is that the two finance departments can reach each other. This final requirement is all other departments should be able to access each other within the same department.

The settings of the ACLs are listed as the following pictures:
BOS:

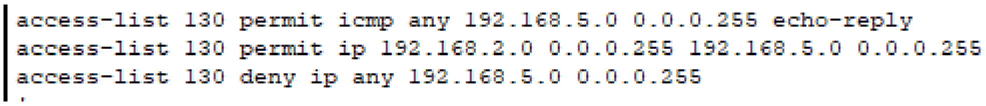


```
 access-list 130 permit icmp any 192.168.2.0 0.0.0.255 echo-reply
 access-list 130 permit ip 192.168.5.0 0.0.0.255 192.168.2.0 0.0.0.255
 access-list 130 deny ip any 192.168.2.0 0.0.0.255
```

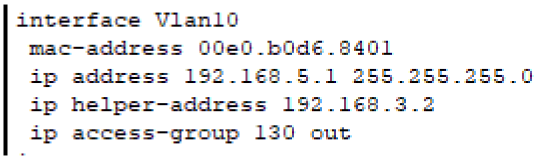


```
interface Vlan10
 mac-address 00d0.ba90.5501
 ip address 192.168.2.1 255.255.255.0
 ip helper-address 192.168.0.2
 ip access-group 130 out
```

Mum:



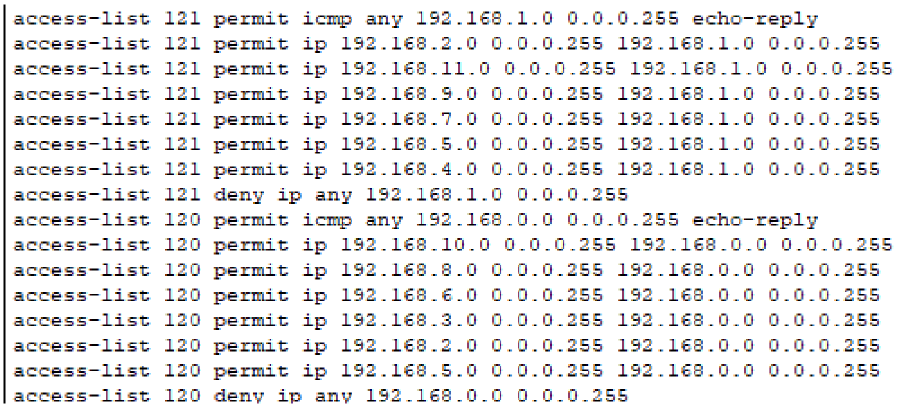
```
access-list 130 permit icmp any 192.168.5.0 0.0.0.255 echo-reply
access-list 130 permit ip 192.168.2.0 0.0.0.255 192.168.5.0 0.0.0.255
access-list 130 deny ip any 192.168.5.0 0.0.0.255
```



```
interface Vlan10
 mac-address 00e0.b0d6.8401
 ip address 192.168.5.1 255.255.255.0
 ip helper-address 192.168.3.2
 ip access-group 130 out
```

In this case, Boston's financial sector only allows access to Bombay's financial sector, and no other sector can access Boston's financial sector. The next request is all other departments should be able to access each other within the same department, and the financial sector can access any sector.

Take Boston as an example:
BOS:



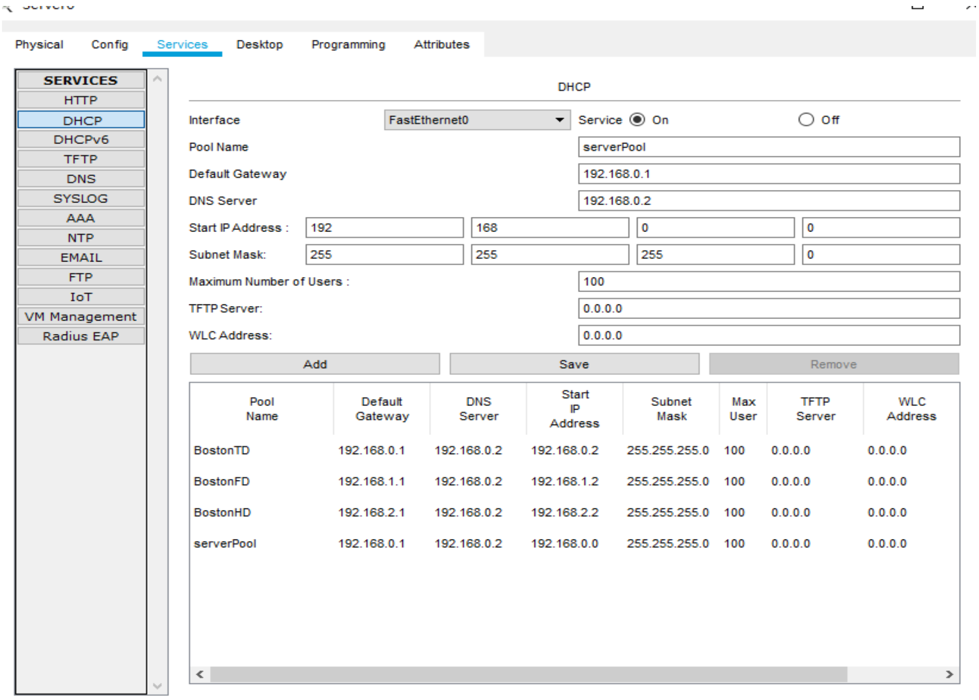
```
access-list 121 permit icmp any 192.168.1.0 0.0.0.255 echo-reply
access-list 121 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 121 permit ip 192.168.11.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 121 permit ip 192.168.9.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 121 permit ip 192.168.7.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 121 permit ip 192.168.5.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 121 permit ip 192.168.4.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 121 deny ip any 192.168.1.0 0.0.0.255
access-list 120 permit icmp any 192.168.0.0 0.0.0.255 echo-reply
access-list 120 permit ip 192.168.10.0 0.0.0.255 192.168.0.0 0.0.0.255
access-list 120 permit ip 192.168.8.0 0.0.0.255 192.168.0.0 0.0.0.255
access-list 120 permit ip 192.168.6.0 0.0.0.255 192.168.0.0 0.0.0.255
access-list 120 permit ip 192.168.3.0 0.0.0.255 192.168.0.0 0.0.0.255
access-list 120 permit ip 192.168.2.0 0.0.0.255 192.168.0.0 0.0.0.255
access-list 120 permit ip 192.168.5.0 0.0.0.255 192.168.0.0 0.0.0.255
access-list 120 deny ip any 192.168.0.0 0.0.0.255
```

This means that Boston's HR department can access other HR departments, but the technical department can't. The technical department can access the HR department, but the HR department cannot access the technical department. The financial sector has access to both sectors. permit icmp any 192.168.64.0 0.0.1.255 echo-reply permits Boston HR Department to reach other departments, otherwise, the reply of the message sent out from the Boston HR Department will be rejected. Same as the Technical department.

DHCP server:

The DHCP servers are in the technical departments. The DHCP servers are set as the following pictures:

Boston DHCP server:



DHCP

Interface: FastEthernet0 Service ● On ○ Off

Pool Name: serverPool

Default Gateway: 192.168.0.1

DNS Server: 192.168.0.2

Start IP Address : 192 168 0 0

Subnet Mask: 255 255 255 0

Maximum Number of Users : 100

TFTP Server: 0.0.0.0

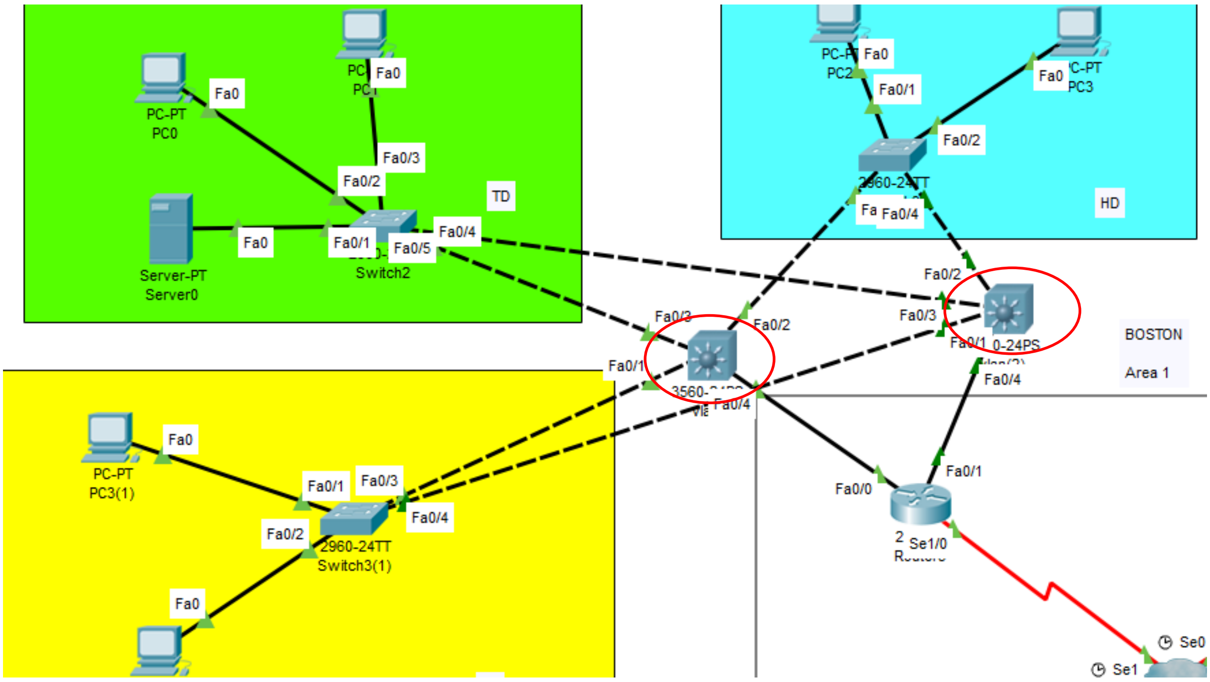
WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
BostonTD	192.168.0.1	192.168.0.2	192.168.0.2	255.255.255.0	100	0.0.0.0	0.0.0.0
BostonFD	192.168.1.1	192.168.0.2	192.168.1.2	255.255.255.0	100	0.0.0.0	0.0.0.0
BostonHD	192.168.2.1	192.168.0.2	192.168.2.2	255.255.255.0	100	0.0.0.0	0.0.0.0
serverPool	192.168.0.1	192.168.0.2	192.168.0.0	255.255.255.0	100	0.0.0.0	0.0.0.0

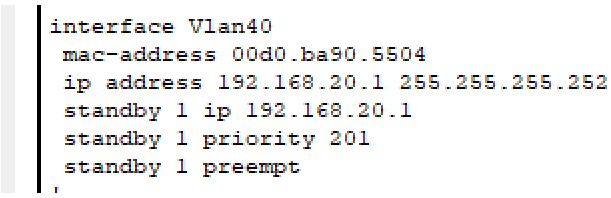
HSRP:

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 an 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:

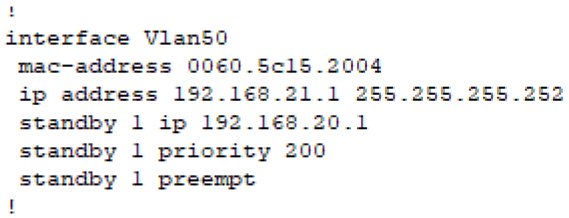


In Boston, a multi-layer switch is designed as a backup switch.
The settings of active multilayer switches are as follows:



```
interface Vlan40
 mac-address 00d0.ba90.5504
 ip address 192.168.20.1 255.255.255.252
 standby 1 ip 192.168.20.1
 standby 1 priority 201
 standby 1 preempt
!
```

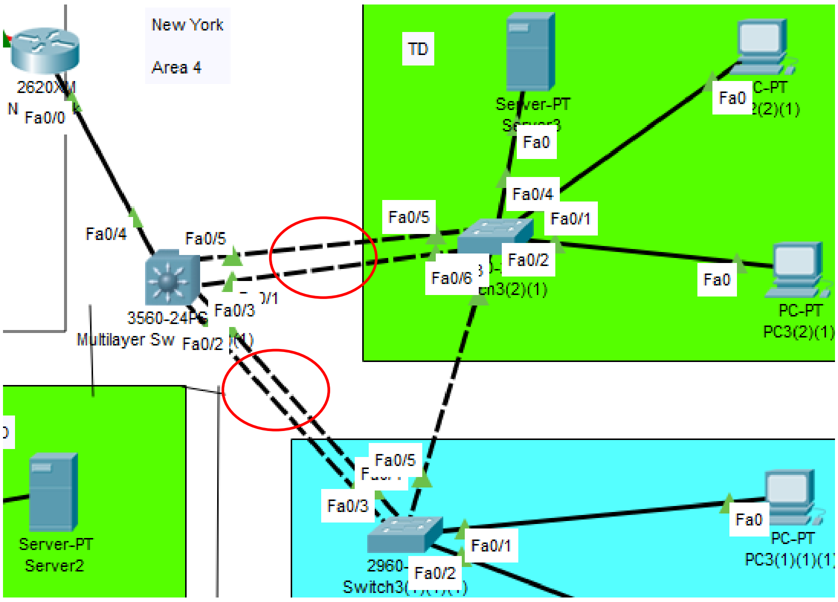
The settings of backup multilayer switch are as follows:



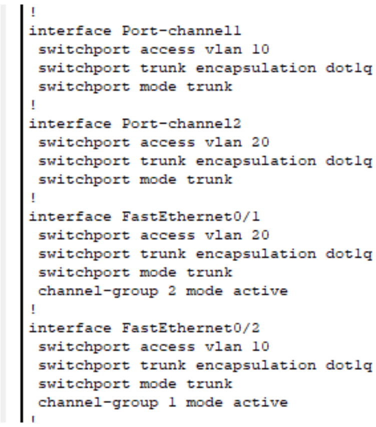
```
!
interface Vlan50
 mac-address 0060.5c15.2004
 ip address 192.168.21.1 255.255.255.252
 standby 1 ip 192.168.20.1
 standby 1 priority 200
 standby 1 preempt
!
```

LACP:

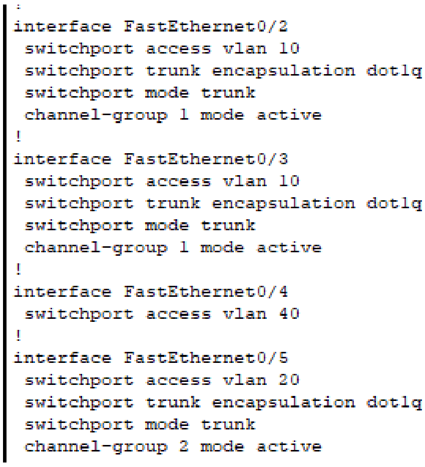
Link Aggregation Control Protocol (LACP) allows multiple physical connections between devices in network, especially between switches so that it can reduce the cost of breakdowns. In this project, LACP is used between the Multilayer switches and the other switches in New York office. The physical connection is shown as the following picture:



The settings are listed as the following pictures:

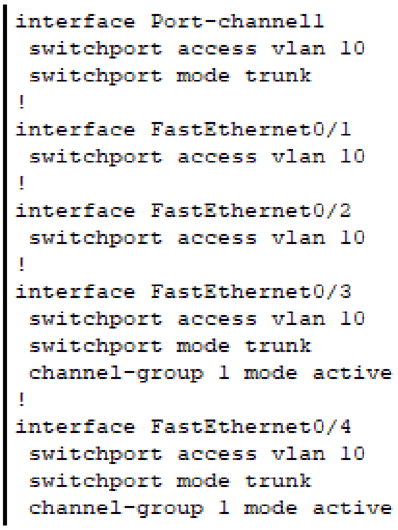


```
!
interface Port-channel1
 switchport access vlan 10
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel2
 switchport access vlan 20
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/1
 switchport access vlan 20
 switchport trunk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



```
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/4
 switchport access vlan 40
!
interface FastEthernet0/5
 switchport access vlan 20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode active
```

Port 2 and 3 are grouped together while ports 1 and 5 are grouped together. So, the ports on 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 in the following picture:



```
interface Port-channel1
 switchport access vlan 10
 switchport mode trunk
!
interface FastEthernet0/1
 switchport access vlan 10
!
interface FastEthernet0/2
 switchport access vlan 10
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/4
 switchport access vlan 10
 switchport mode trunk
 channel-group 1 mode active
```

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, 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 like PVSTP but it works with RSTP instead of STP. It is defined in 802.1s standard.

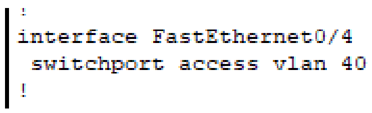
Test Plan for the Network:

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, and whether the VLANs allowed on trunk consist only of the VLANs used in the networks.

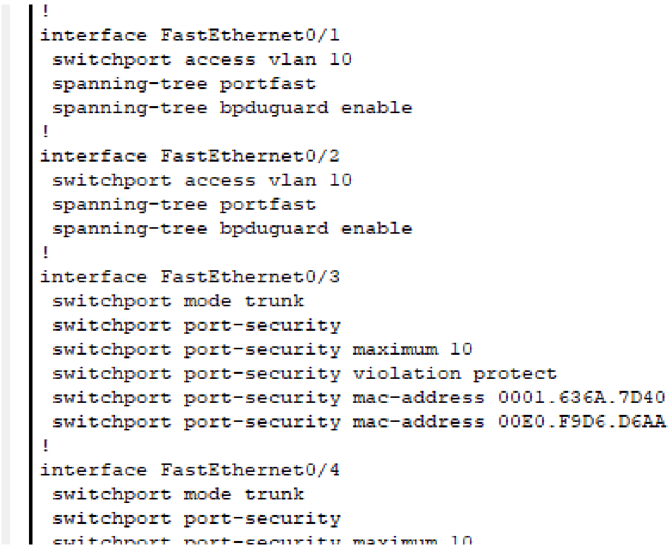
Take Boston as an example, the result is shown as the following pictures:

Multilayer switch:



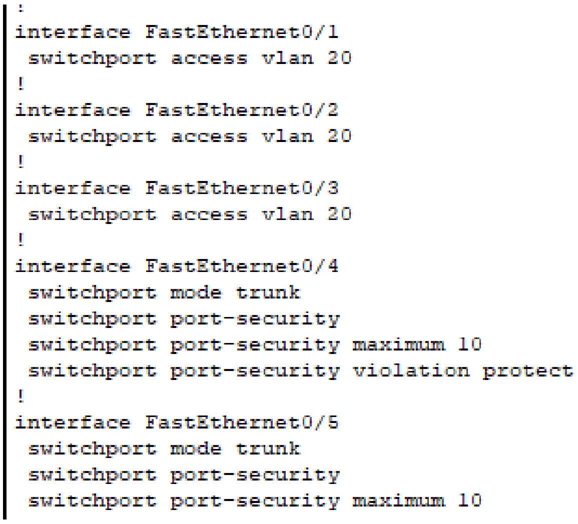
```
!
interface FastEthernet0/4
 switchport access vlan 40
!
```

Finance department switch:



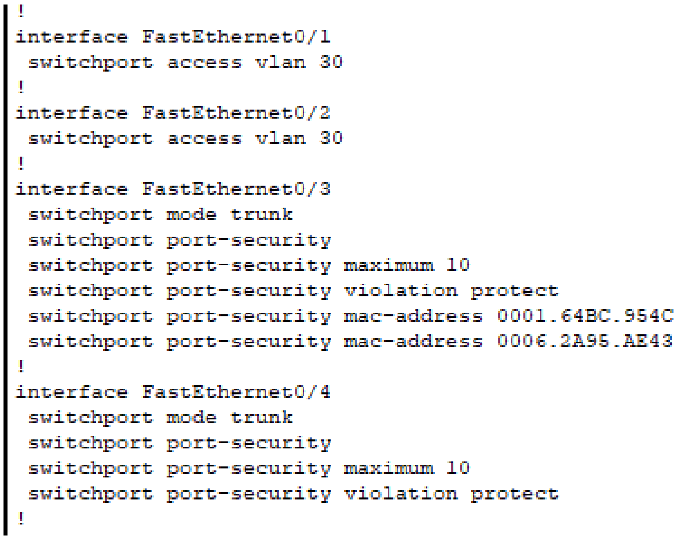
```
!
interface FastEthernet0/1
 switchport access vlan 10
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/2
 switchport access vlan 10
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/3
 switchport mode trunk
 switchport port-security
 switchport port-security maximum 10
 switchport port-security violation protect
 switchport port-security mac-address 0001.636A.7D40
 switchport port-security mac-address 00E0.F9D6.D6AA
!
interface FastEthernet0/4
 switchport mode trunk
 switchport port-security
 switchport port-security maximum 10
```

Technical department switch:



```
!
interface FastEthernet0/1
 switchport access vlan 20
!
interface FastEthernet0/2
 switchport access vlan 20
!
interface FastEthernet0/3
 switchport access vlan 20
!
interface FastEthernet0/4
 switchport mode trunk
 switchport port-security
 switchport port-security maximum 10
 switchport port-security violation protect
!
interface FastEthernet0/5
 switchport mode trunk
 switchport port-security
 switchport port-security maximum 10
```

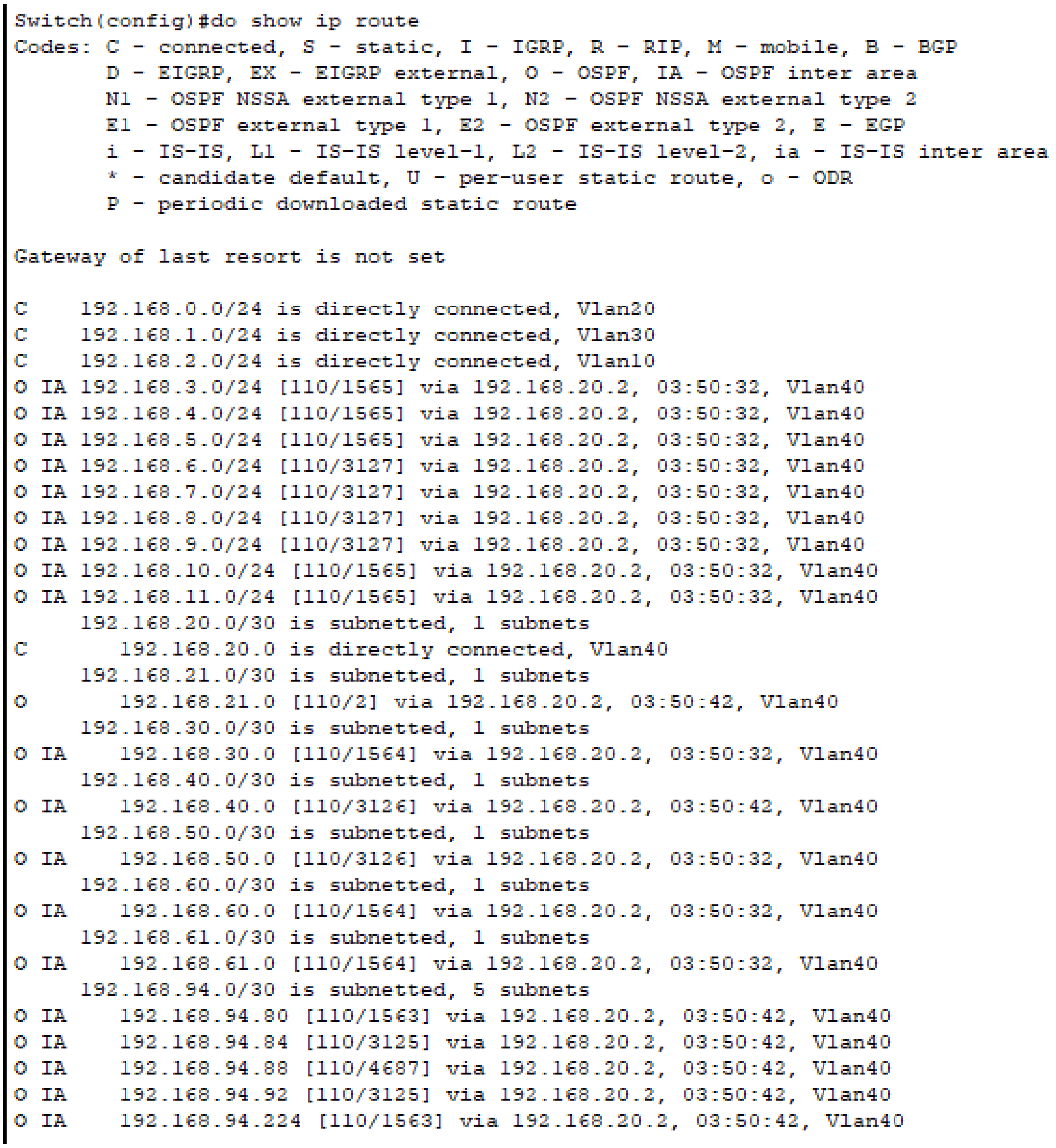
HR department switch:



```
!
interface FastEthernet0/1
 switchport access vlan 30
!
interface FastEthernet0/2
 switchport access vlan 30
!
interface FastEthernet0/3
 switchport mode trunk
 switchport port-security
 switchport port-security maximum 10
 switchport port-security violation protect
 switchport port-security mac-address 0001.64BC.954C
 switchport port-security mac-address 0006.2A95.AE43
!
interface FastEthernet0/4
 switchport mode trunk
 switchport port-security
 switchport port-security maximum 10
 switchport port-security violation protect
!
```

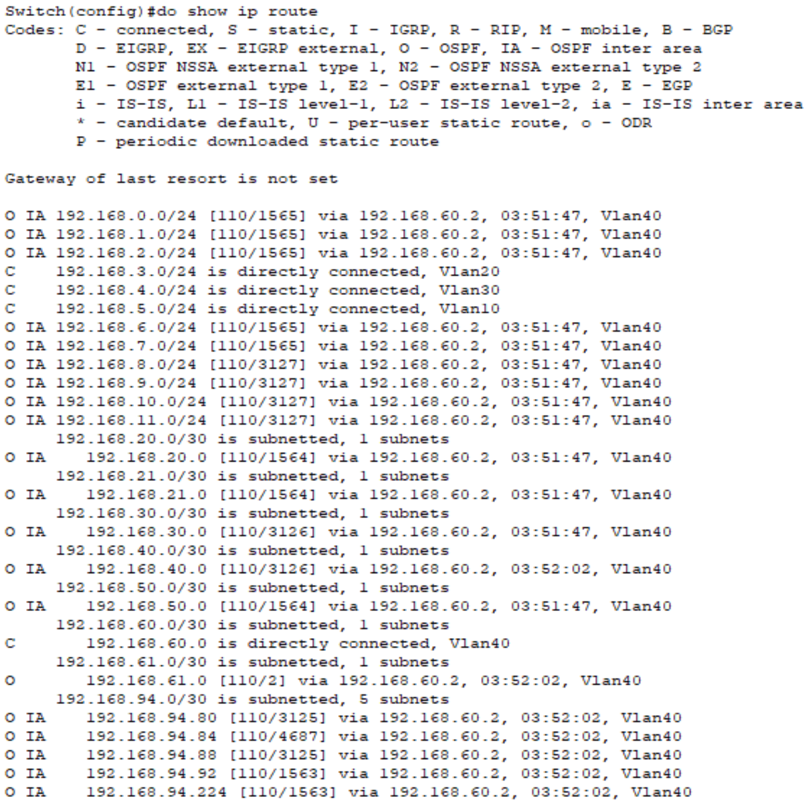
Routing protocol:

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:



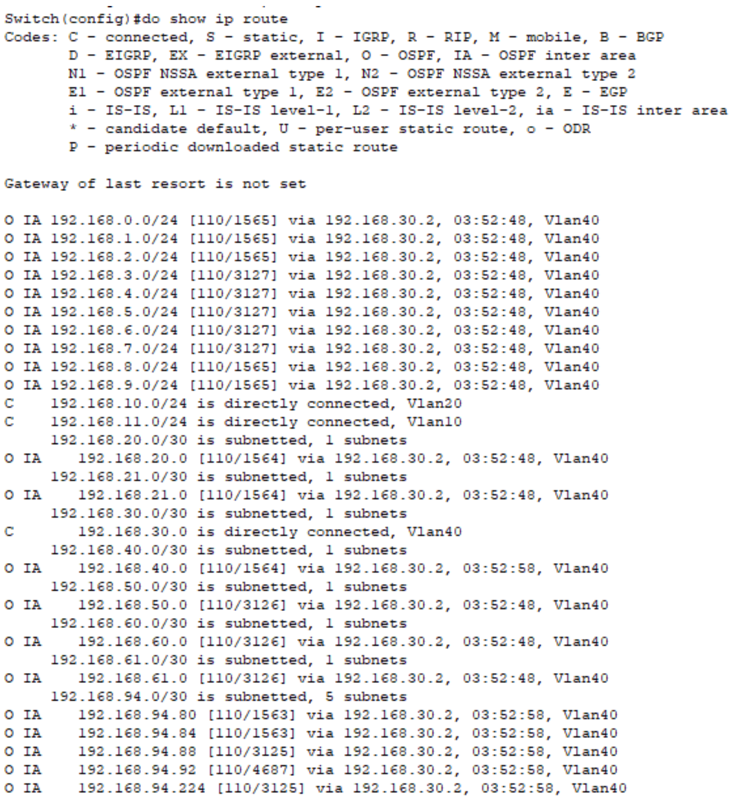
```
Switch(config)#do show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external 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

C    192.168.0.0/24 is directly connected, Vlan20
C    192.168.1.0/24 is directly connected, Vlan30
C    192.168.2.0/24 is directly connected, Vlan10
O IA 192.168.3.0/24 [110/1565] via 192.168.20.2, 03:50:32, Vlan40
O IA 192.168.4.0/24 [110/1565] via 192.168.20.2, 03:50:32, Vlan40
O IA 192.168.5.0/24 [110/1565] via 192.168.20.2, 03:50:32, Vlan40
O IA 192.168.6.0/24 [110/3127] via 192.168.20.2, 03:50:32, Vlan40
O IA 192.168.7.0/24 [110/3127] via 192.168.20.2, 03:50:32, Vlan40
O IA 192.168.8.0/24 [110/3127] via 192.168.20.2, 03:50:32, Vlan40
O IA 192.168.9.0/24 [110/3127] via 192.168.20.2, 03:50:32, Vlan40
O IA 192.168.10.0/24 [110/1565] via 192.168.20.2, 03:50:32, Vlan40
O IA 192.168.11.0/24 [110/1565] via 192.168.20.2, 03:50:32, Vlan40
     192.168.20.0/30 is subnetted, 1 subnets
C       192.168.20.0 is directly connected, Vlan40
     192.168.21.0/30 is subnetted, 1 subnets
O       192.168.21.0 [110/2] via 192.168.20.2, 03:50:42, Vlan40
     192.168.30.0/30 is subnetted, 1 subnets
O IA    192.168.30.0 [110/1564] via 192.168.20.2, 03:50:32, Vlan40
     192.168.40.0/30 is subnetted, 1 subnets
O IA    192.168.40.0 [110/3126] via 192.168.20.2, 03:50:42, Vlan40
     192.168.50.0/30 is subnetted, 1 subnets
O IA    192.168.50.0 [110/3126] via 192.168.20.2, 03:50:32, Vlan40
     192.168.60.0/30 is subnetted, 1 subnets
O IA    192.168.60.0 [110/1564] via 192.168.20.2, 03:50:32, Vlan40
     192.168.61.0/30 is subnetted, 1 subnets
O IA    192.168.61.0 [110/1564] via 192.168.20.2, 03:50:32, Vlan40
     192.168.94.0/30 is subnetted, 5 subnets
O IA    192.168.94.80 [110/1563] via 192.168.20.2, 03:50:42, Vlan40
O IA    192.168.94.84 [110/3125] via 192.168.20.2, 03:50:42, Vlan40
O IA    192.168.94.88 [110/4687] via 192.168.20.2, 03:50:42, Vlan40
O IA    192.168.94.92 [110/3125] via 192.168.20.2, 03:50:42, Vlan40
O IA    192.168.94.224 [110/1563] via 192.168.20.2, 03:50:42, Vlan40
```

Mumbai:



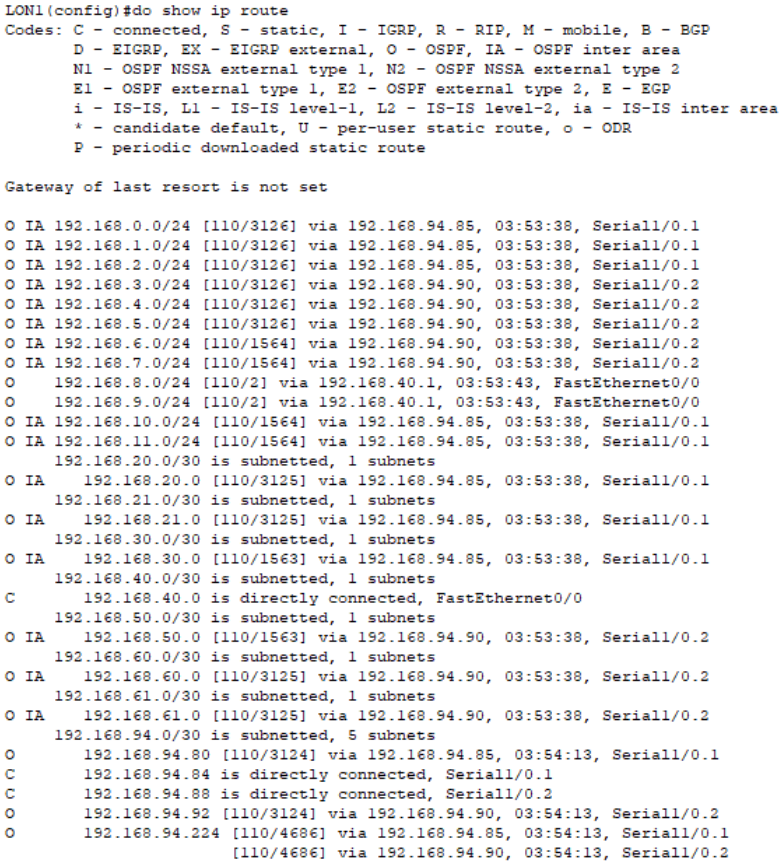
```
Switch(config)#do show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external 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 192.168.0.0/24 [110/1565] via 192.168.60.2, 03:51:47, Vlan40
O IA 192.168.1.0/24 [110/1565] via 192.168.60.2, 03:51:47, Vlan40
O IA 192.168.2.0/24 [110/1565] via 192.168.60.2, 03:51:47, Vlan40
C    192.168.3.0/24 is directly connected, Vlan20
C    192.168.4.0/24 is directly connected, Vlan30
C    192.168.5.0/24 is directly connected, Vlan10
O IA 192.168.6.0/24 [110/1565] via 192.168.60.2, 03:51:47, Vlan40
O IA 192.168.7.0/24 [110/1565] via 192.168.60.2, 03:51:47, Vlan40
O IA 192.168.8.0/24 [110/3127] via 192.168.60.2, 03:51:47, Vlan40
O IA 192.168.9.0/24 [110/3127] via 192.168.60.2, 03:51:47, Vlan40
O IA 192.168.10.0/24 [110/3127] via 192.168.60.2, 03:51:47, Vlan40
O IA 192.168.11.0/24 [110/3127] via 192.168.60.2, 03:51:47, Vlan40
     192.168.20.0/30 is subnetted, 1 subnets
O IA    192.168.20.0 [110/1564] via 192.168.60.2, 03:51:47, Vlan40
     192.168.21.0/30 is subnetted, 1 subnets
O IA    192.168.21.0 [110/1564] via 192.168.60.2, 03:51:47, Vlan40
     192.168.30.0/30 is subnetted, 1 subnets
O IA    192.168.30.0 [110/3126] via 192.168.60.2, 03:51:47, Vlan40
     192.168.40.0/30 is subnetted, 1 subnets
O IA    192.168.40.0 [110/3126] via 192.168.60.2, 03:52:02, Vlan40
     192.168.50.0/30 is subnetted, 1 subnets
O IA    192.168.50.0 [110/1564] via 192.168.60.2, 03:51:47, Vlan40
     192.168.60.0/30 is subnetted, 1 subnets
C       192.168.60.0 is directly connected, Vlan40
     192.168.61.0/30 is subnetted, 1 subnets
O       192.168.61.0 [110/2] via 192.168.60.2, 03:52:02, Vlan40
     192.168.94.0/30 is subnetted, 5 subnets
O IA    192.168.94.80 [110/3125] via 192.168.60.2, 03:52:02, Vlan40
O IA    192.168.94.84 [110/4687] via 192.168.60.2, 03:52:02, Vlan40
O IA    192.168.94.88 [110/3125] via 192.168.60.2, 03:52:02, Vlan40
O IA    192.168.94.92 [110/1563] via 192.168.60.2, 03:52:02, Vlan40
O IA    192.168.94.224 [110/1563] via 192.168.60.2, 03:52:02, Vlan40
```

Beijing:



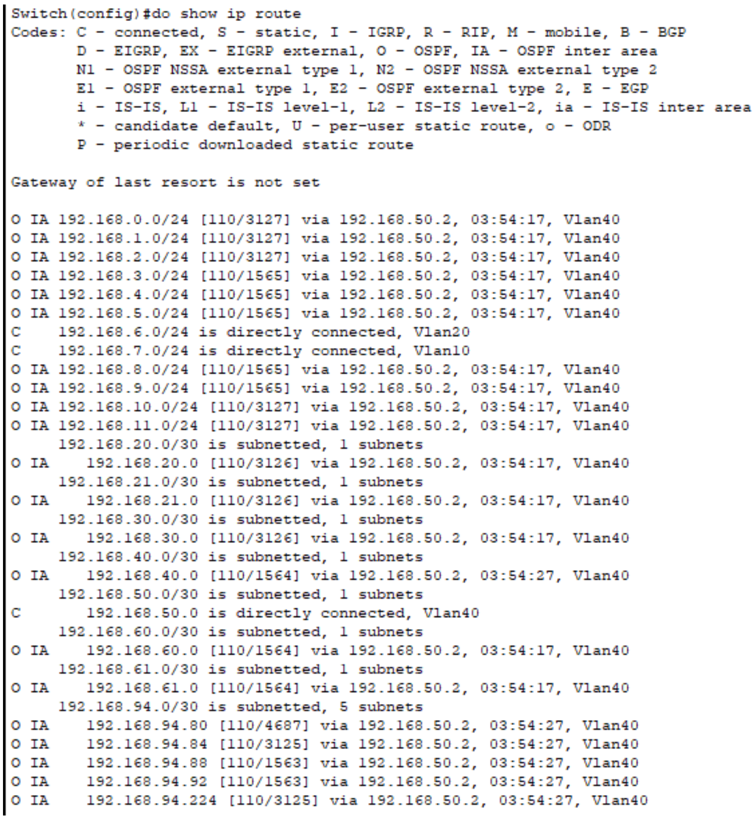
```
Switch(config)#do show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external 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 192.168.0.0/24 [110/1565] via 192.168.30.2, 03:52:48, Vlan40
O IA 192.168.1.0/24 [110/1565] via 192.168.30.2, 03:52:48, Vlan40
O IA 192.168.2.0/24 [110/1565] via 192.168.30.2, 03:52:48, Vlan40
O IA 192.168.3.0/24 [110/3127] via 192.168.30.2, 03:52:48, Vlan40
O IA 192.168.4.0/24 [110/3127] via 192.168.30.2, 03:52:48, Vlan40
O IA 192.168.5.0/24 [110/3127] via 192.168.30.2, 03:52:48, Vlan40
O IA 192.168.6.0/24 [110/3127] via 192.168.30.2, 03:52:48, Vlan40
O IA 192.168.7.0/24 [110/3127] via 192.168.30.2, 03:52:48, Vlan40
O IA 192.168.8.0/24 [110/1565] via 192.168.30.2, 03:52:48, Vlan40
O IA 192.168.9.0/24 [110/1565] via 192.168.30.2, 03:52:48, Vlan40
C    192.168.10.0/24 is directly connected, Vlan20
C    192.168.11.0/24 is directly connected, Vlan10
     192.168.20.0/30 is subnetted, 1 subnets
O IA    192.168.20.0 [110/1564] via 192.168.30.2, 03:52:48, Vlan40
     192.168.21.0/30 is subnetted, 1 subnets
O IA    192.168.21.0 [110/1564] via 192.168.30.2, 03:52:48, Vlan40
     192.168.30.0/30 is subnetted, 1 subnets
C       192.168.30.0 is directly connected, Vlan40
     192.168.40.0/30 is subnetted, 1 subnets
O IA    192.168.40.0 [110/1564] via 192.168.30.2, 03:52:58, Vlan40
     192.168.50.0/30 is subnetted, 1 subnets
O IA    192.168.50.0 [110/3126] via 192.168.30.2, 03:52:48, Vlan40
     192.168.60.0/30 is subnetted, 1 subnets
O IA    192.168.60.0 [110/3126] via 192.168.30.2, 03:52:48, Vlan40
     192.168.61.0/30 is subnetted, 1 subnets
O IA    192.168.61.0 [110/3126] via 192.168.30.2, 03:52:48, Vlan40
     192.168.94.0/30 is subnetted, 5 subnets
O IA    192.168.94.80 [110/1563] via 192.168.30.2, 03:52:58, Vlan40
O IA    192.168.94.84 [110/1563] via 192.168.30.2, 03:52:58, Vlan40
O IA    192.168.94.88 [110/3125] via 192.168.30.2, 03:52:58, Vlan40
O IA    192.168.94.92 [110/4687] via 192.168.30.2, 03:52:58, Vlan40
O IA    192.168.94.224 [110/3125] via 192.168.30.2, 03:52:58, Vlan40
```

London:



```
LON1(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 192.168.0.0/24 [110/3126] via 192.168.94.85, 03:53:38, Serial1/0.1
O IA 192.168.1.0/24 [110/3126] via 192.168.94.85, 03:53:38, Serial1/0.1
O IA 192.168.2.0/24 [110/3126] via 192.168.94.85, 03:53:38, Serial1/0.1
O IA 192.168.3.0/24 [110/3126] via 192.168.94.90, 03:53:38, Serial1/0.2
O IA 192.168.4.0/24 [110/3126] via 192.168.94.90, 03:53:38, Serial1/0.2
O IA 192.168.5.0/24 [110/3126] via 192.168.94.90, 03:53:38, Serial1/0.2
O IA 192.168.6.0/24 [110/1564] via 192.168.94.90, 03:53:38, Serial1/0.2
O IA 192.168.7.0/24 [110/1564] via 192.168.94.90, 03:53:38, Serial1/0.2
O    192.168.8.0/24 [110/2] via 192.168.40.1, 03:53:43, FastEthernet0/0
O    192.168.9.0/24 [110/2] via 192.168.40.1, 03:53:43, FastEthernet0/0
O IA 192.168.10.0/24 [110/1564] via 192.168.94.85, 03:53:38, Serial1/0.1
O IA 192.168.11.0/24 [110/1564] via 192.168.94.85, 03:53:38, Serial1/0.1
     192.168.20.0/30 is subnetted, 1 subnets
O IA    192.168.20.0 [110/3125] via 192.168.94.85, 03:53:38, Serial1/0.1
     192.168.21.0/30 is subnetted, 1 subnets
O IA    192.168.21.0 [110/3125] via 192.168.94.85, 03:53:38, Serial1/0.1
     192.168.30.0/30 is subnetted, 1 subnets
O IA    192.168.30.0 [110/1563] via 192.168.94.85, 03:53:38, Serial1/0.1
     192.168.40.0/30 is subnetted, 1 subnets
C       192.168.40.0 is directly connected, FastEthernet0/0
     192.168.50.0/30 is subnetted, 1 subnets
O IA    192.168.50.0 [110/1563] via 192.168.94.90, 03:53:38, Serial1/0.2
     192.168.60.0/30 is subnetted, 1 subnets
O IA    192.168.60.0 [110/3125] via 192.168.94.90, 03:53:38, Serial1/0.2
     192.168.61.0/30 is subnetted, 1 subnets
O IA    192.168.61.0 [110/3125] via 192.168.94.90, 03:53:38, Serial1/0.2
     192.168.94.0/30 is subnetted, 5 subnets
O       192.168.94.80 [110/3124] via 192.168.94.85, 03:54:13, Serial1/0.1
C       192.168.94.84 is directly connected, Serial1/0.1
C       192.168.94.88 is directly connected, Serial1/0.2
O       192.168.94.92 [110/3124] via 192.168.94.90, 03:54:13, Serial1/0.2
O       192.168.94.224 [110/4686] via 192.168.94.85, 03:54:13, Serial1/0.1
                       [110/4686] via 192.168.94.90, 03:54:13, Serial1/0.2
```

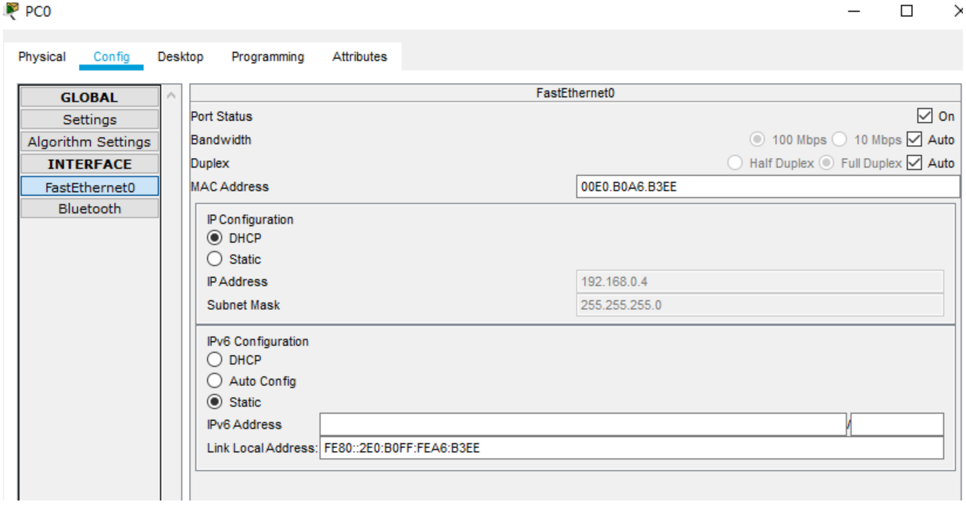
New York:



```
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 192.168.0.0/24 [110/3127] via 192.168.50.2, 03:54:17, Vlan40
O IA 192.168.1.0/24 [110/3127] via 192.168.50.2, 03:54:17, Vlan40
O IA 192.168.2.0/24 [110/3127] via 192.168.50.2, 03:54:17, Vlan40
O IA 192.168.3.0/24 [110/1565] via 192.168.50.2, 03:54:17, Vlan40
O IA 192.168.4.0/24 [110/1565] via 192.168.50.2, 03:54:17, Vlan40
O IA 192.168.5.0/24 [110/1565] via 192.168.50.2, 03:54:17, Vlan40
C    192.168.6.0/24 is directly connected, Vlan20
C    192.168.7.0/24 is directly connected, Vlan10
O IA 192.168.8.0/24 [110/1565] via 192.168.50.2, 03:54:17, Vlan40
O IA 192.168.9.0/24 [110/1565] via 192.168.50.2, 03:54:17, Vlan40
O IA 192.168.10.0/24 [110/3127] via 192.168.50.2, 03:54:17, Vlan40
O IA 192.168.11.0/24 [110/3127] via 192.168.50.2, 03:54:17, Vlan40
     192.168.20.0/30 is subnetted, 1 subnets
O IA    192.168.20.0 [110/3126] via 192.168.50.2, 03:54:17, Vlan40
     192.168.21.0/30 is subnetted, 1 subnets
O IA    192.168.21.0 [110/3126] via 192.168.50.2, 03:54:17, Vlan40
     192.168.30.0/30 is subnetted, 1 subnets
O IA    192.168.30.0 [110/3126] via 192.168.50.2, 03:54:17, Vlan40
     192.168.40.0/30 is subnetted, 1 subnets
O IA    192.168.40.0 [110/1564] via 192.168.50.2, 03:54:27, Vlan40
     192.168.50.0/30 is subnetted, 1 subnets
C       192.168.50.0 is directly connected, Vlan40
     192.168.60.0/30 is subnetted, 1 subnets
O IA    192.168.60.0 [110/1564] via 192.168.50.2, 03:54:17, Vlan40
     192.168.61.0/30 is subnetted, 1 subnets
O IA    192.168.61.0 [110/1564] via 192.168.50.2, 03:54:17, Vlan40
     192.168.94.0/30 is subnetted, 5 subnets
O IA    192.168.94.80 [110/4687] via 192.168.50.2, 03:54:27, Vlan40
O IA    192.168.94.84 [110/3125] via 192.168.50.2, 03:54:27, Vlan40
O IA    192.168.94.88 [110/1563] via 192.168.50.2, 03:54:27, Vlan40
O IA    192.168.94.92 [110/1563] via 192.168.50.2, 03:54:27, Vlan40
O IA    192.168.94.224 [110/3125] via 192.168.50.2, 03:54:27, Vlan40
```

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:



FastEthernet0

Port Status ☑ On

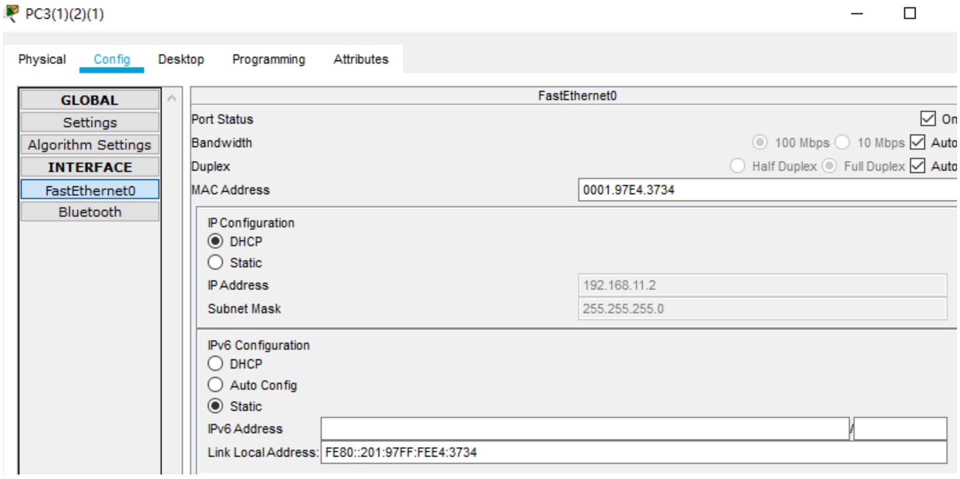
Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 00E0.B0A6.B3EE

IP Configuration
● DHCP
○ Static
IP Address 192.168.0.4
Subnet Mask 255.255.255.0

IPv6 Configuration
○ DHCP
○ Auto Config
● Static
IPv6 Address
Link Local Address: FE80::2E0:B0FF:FEA6:B3EE



FastEthernet0

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

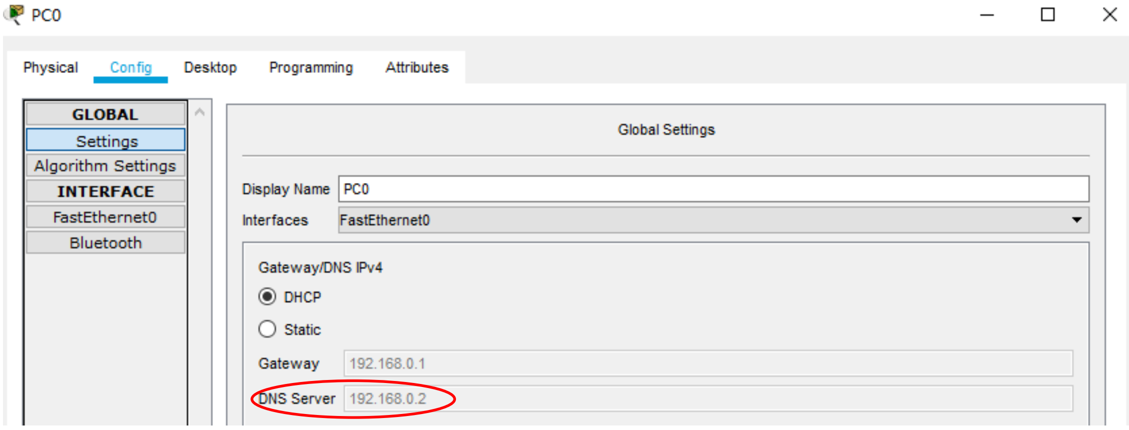
MAC Address 0001.97E4.3734

IP Configuration
● DHCP
○ Static
IP Address 192.168.11.2
Subnet Mask 255.255.255.0

IPv6 Configuration
○ DHCP
○ Auto Config
● Static
IPv6 Address
Link Local Address: FE80::201:97FF:FEE4:3734

DNS Configuration:

A DNS server was set up in the Boston office. The IP address of the server is 192.168.0.2.



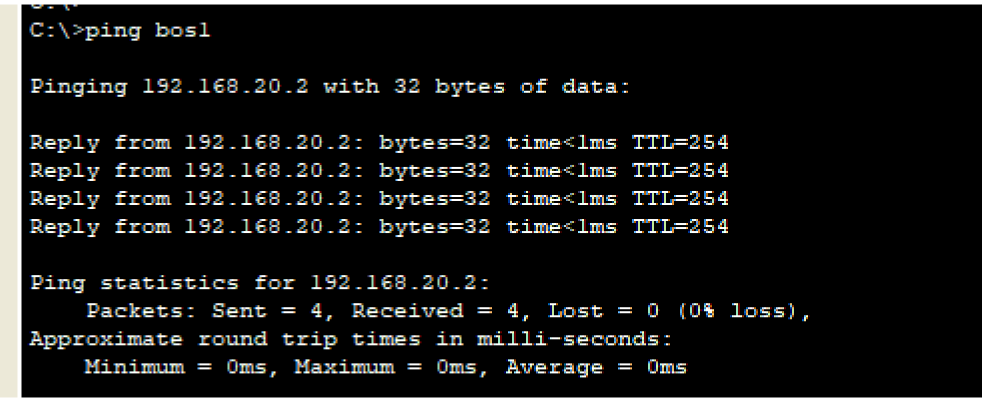
Global Settings

Display Name PC0

Interfaces FastEthernet0

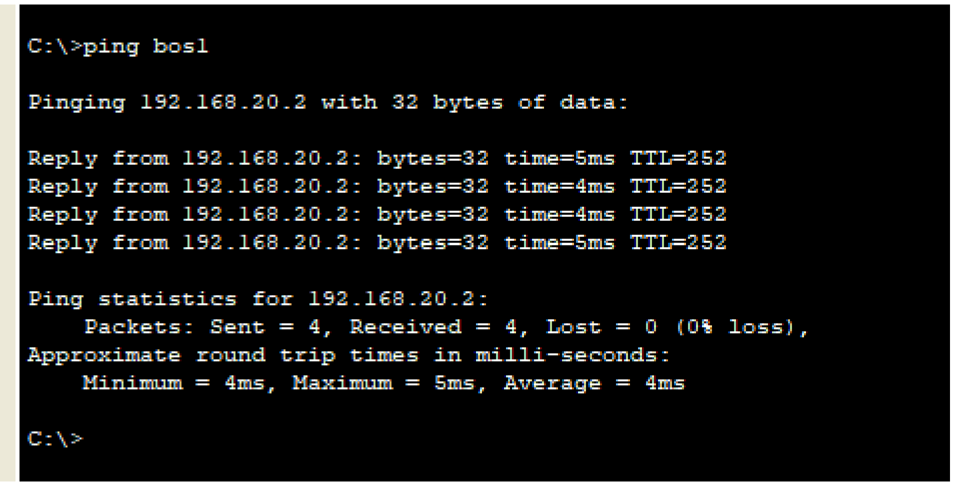
Gateway/DNS IPv4
● DHCP
○ Static
Gateway 192.168.0.1
DNS Server 192.168.0.2

Use this PC to Ping bos1.



```
C:\>
C:\>ping bos1

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time<1ms TTL=254
Reply from 192.168.20.2: bytes=32 time<1ms TTL=254
Reply from 192.168.20.2: bytes=32 time<1ms TTL=254
Reply from 192.168.20.2: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Use PC of Technical Department London to Ping bos1.



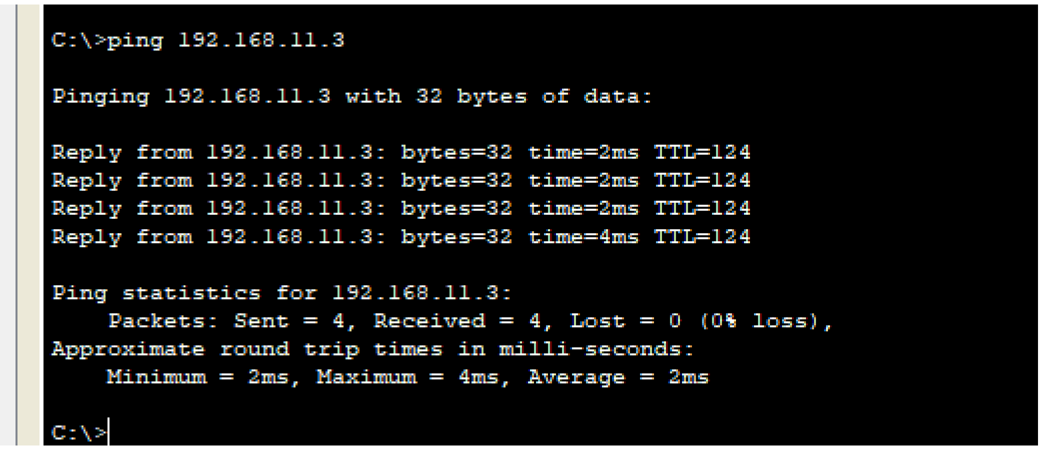
```
C:\>ping bos1

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time=5ms TTL=252
Reply from 192.168.20.2: bytes=32 time=4ms TTL=252
Reply from 192.168.20.2: bytes=32 time=4ms TTL=252
Reply from 192.168.20.2: bytes=32 time=5ms TTL=252

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5ms, Average = 4ms

C:\>
```

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

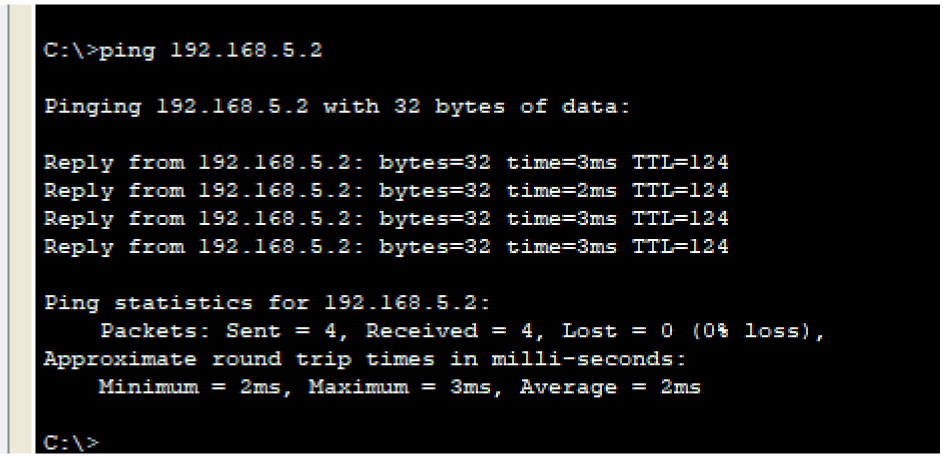
To test this, click on ✉ button, click on the computer you want to start the ping and then the other one you want to receive it. It's an easy way to test but hard to get screenshots. Use the run Command Prompt can also test this one. The results are shown as the following pictures:

Boston finance department ping Beijing HR department:



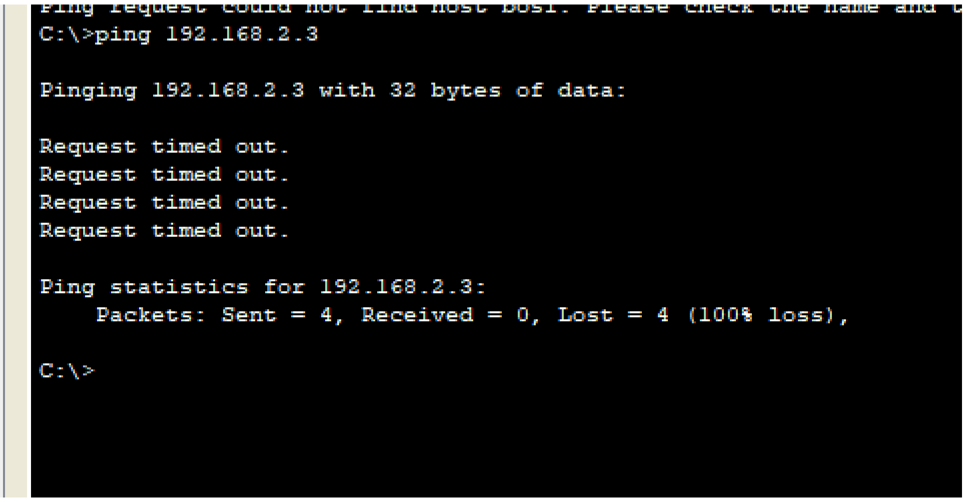
```
C:\>ping 192.168.11.3

Pinging 192.168.11.3 with 32 bytes of data:

Reply from 192.168.11.3: bytes=32 time=2ms TTL=124
Reply from 192.168.11.3: bytes=32 time=2ms TTL=124
Reply from 192.168.11.3: bytes=32 time=2ms TTL=124
Reply from 192.168.11.3: bytes=32 time=4ms TTL=124

Ping statistics for 192.168.11.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 2ms

C:\>
```

Boston finance department ping Mumbai finance department:



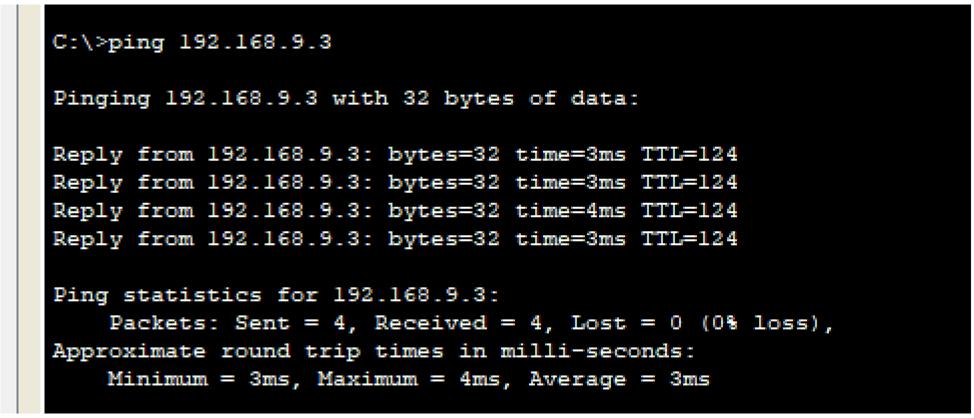
```
C:\>ping 192.168.5.2

Pinging 192.168.5.2 with 32 bytes of data:

Reply from 192.168.5.2: bytes=32 time=3ms TTL=124
Reply from 192.168.5.2: bytes=32 time=2ms TTL=124
Reply from 192.168.5.2: bytes=32 time=3ms TTL=124
Reply from 192.168.5.2: bytes=32 time=3ms TTL=124

Ping statistics for 192.168.5.2:
    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:



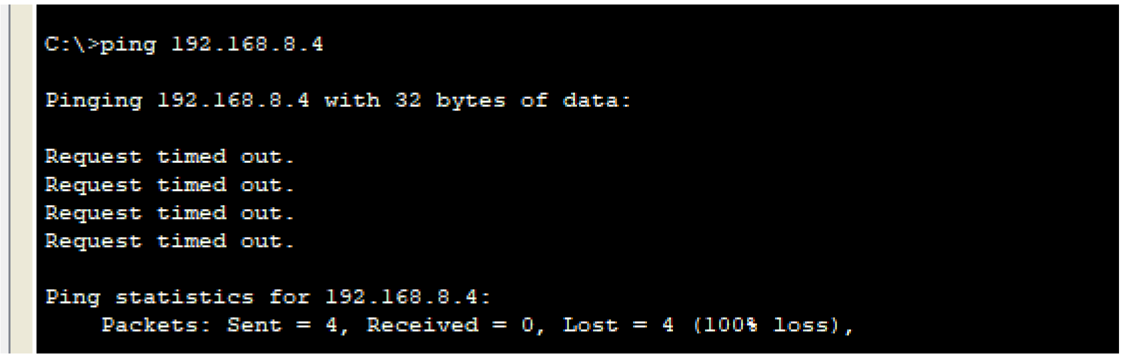
```
Ping request could not find host bost. Please check the name and t
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Beijing HR department ping London HR department:



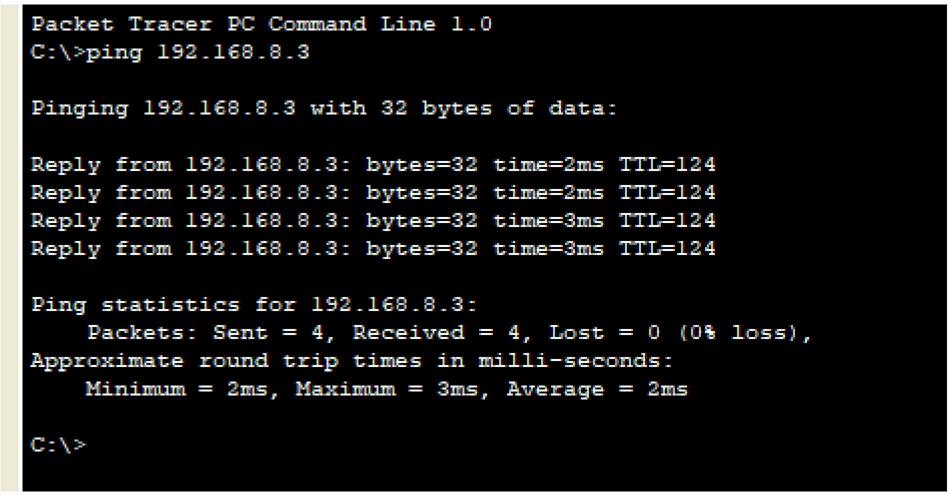
```
C:\>ping 192.168.9.3

Pinging 192.168.9.3 with 32 bytes of data:

Reply from 192.168.9.3: bytes=32 time=3ms TTL=124
Reply from 192.168.9.3: bytes=32 time=3ms TTL=124
Reply from 192.168.9.3: bytes=32 time=4ms TTL=124
Reply from 192.168.9.3: bytes=32 time=3ms TTL=124

Ping statistics for 192.168.9.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

Beijing HR department ping London Technical department:



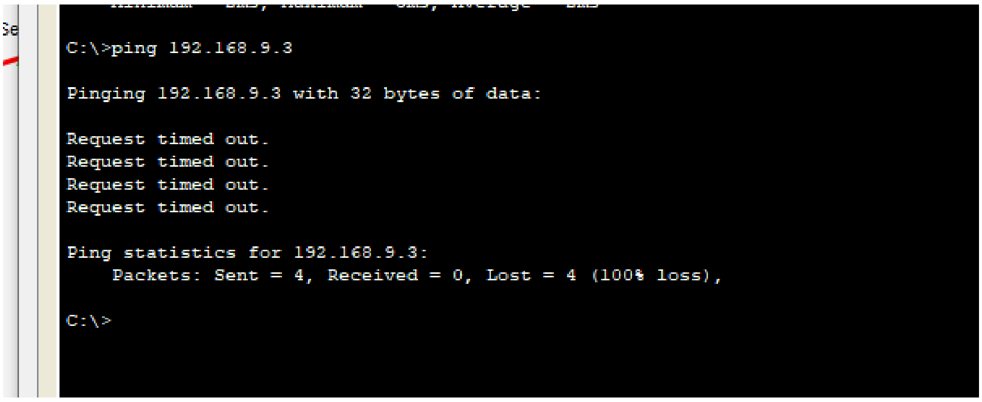
```
C:\>ping 192.168.8.4

Pinging 192.168.8.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.8.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

New York Technical department ping London Technical department:



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.8.3

Pinging 192.168.8.3 with 32 bytes of data:

Reply from 192.168.8.3: bytes=32 time=2ms TTL=124
Reply from 192.168.8.3: bytes=32 time=2ms TTL=124
Reply from 192.168.8.3: bytes=32 time=3ms TTL=124
Reply from 192.168.8.3: bytes=32 time=3ms TTL=124

Ping statistics for 192.168.8.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>
```

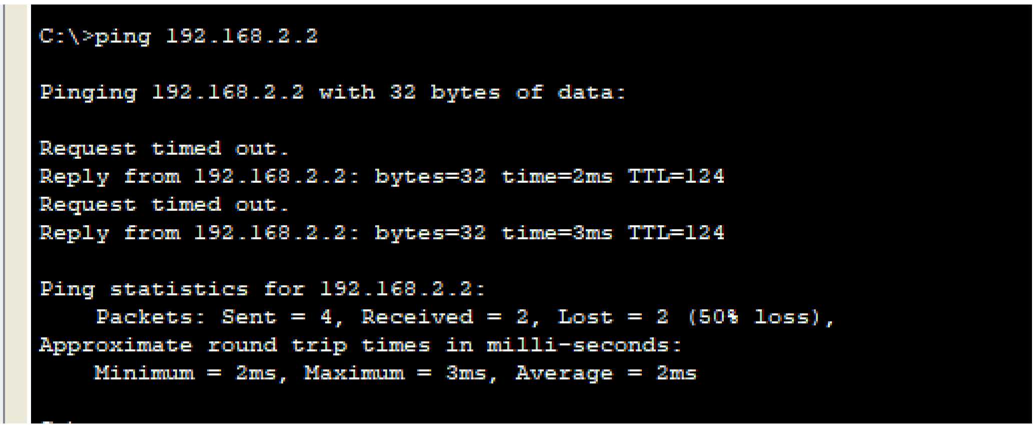
New York Technical department ping London HR department:



```
C:\>ping 192.168.9.3

Pinging 192.168.9.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.9.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

HSRP

Use Mumbai's financial sector to Ping Boston's financial sector. Time out is performed in between.



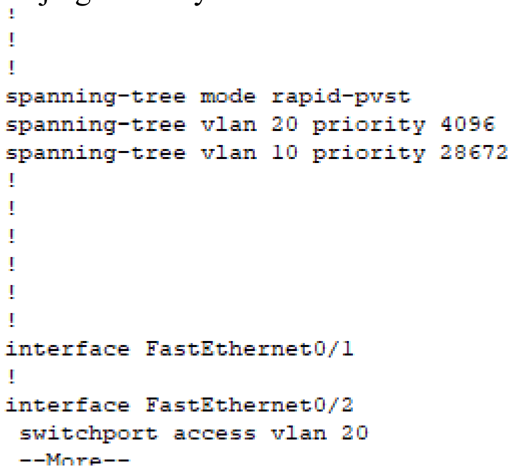
```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.2: bytes=32 time=2ms TTL=124
Request timed out.
Reply from 192.168.2.2: bytes=32 time=3ms TTL=124

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

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:

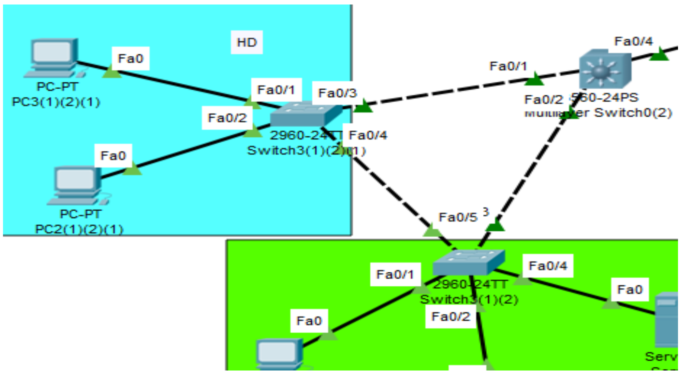
Port-security:

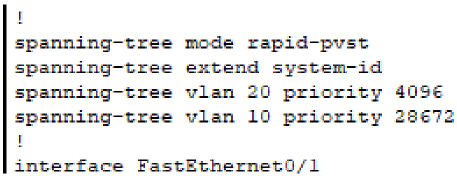
Beijing Multilayer switch:



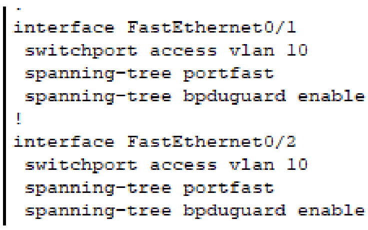
```
!
!
!
spanning-tree mode rapid-pvst
spanning-tree vlan 20 priority 4096
spanning-tree vlan 10 priority 28672
!
!
!
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
 switchport access vlan 20
 --More--
```

Beijing HR department switch:



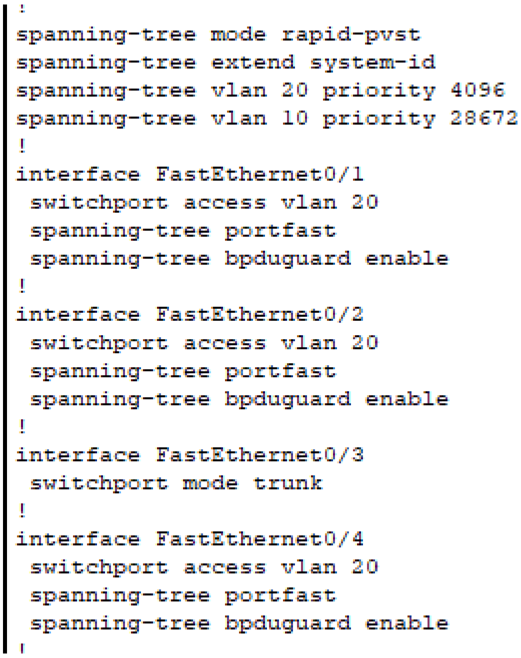


```
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 20 priority 4096
spanning-tree vlan 10 priority 28672
!
interface FastEthernet0/1
```



```
!
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
```

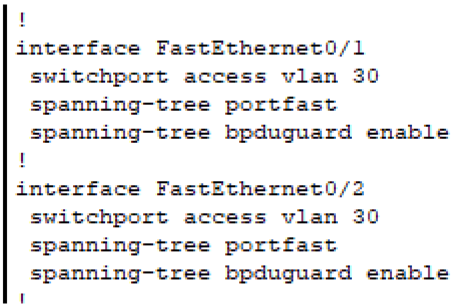
Beijing Technical department switch:



```
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 20 priority 4096
spanning-tree vlan 10 priority 28672
!
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 mode trunk
!
interface FastEthernet0/4
 switchport access vlan 20
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

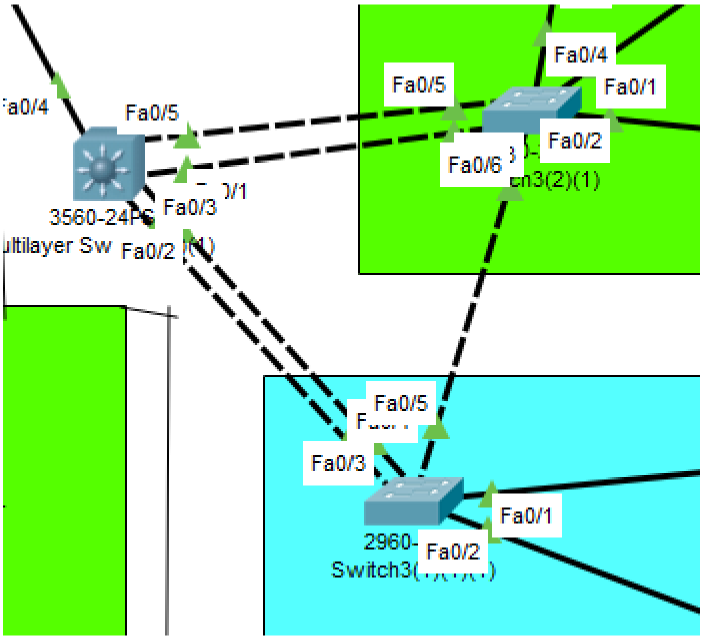
Redundancy plan:

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

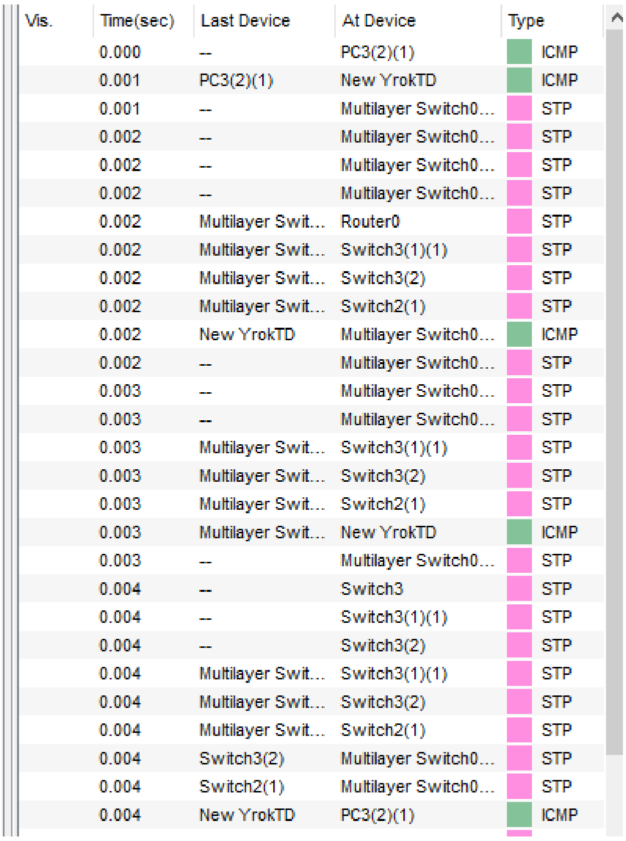


```
!
interface FastEthernet0/1
 switchport access vlan 30
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/2
 switchport access vlan 30
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

LACP:



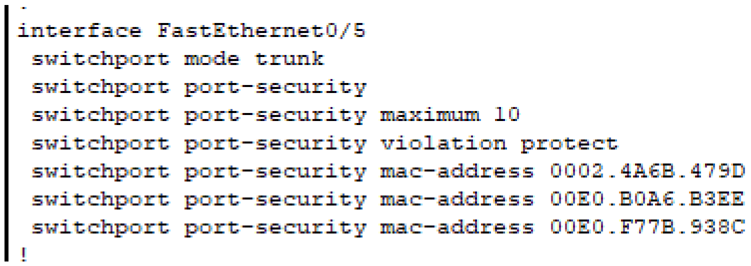
As shown in the picture is the LACP I used in New York office. To test this protocol, checking on the path of the package that New York technical department pings the multilayer switch is an efficient way:



Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC3(2)(1)	ICMP
	0.001	PC3(2)(1)	New YrokTD	ICMP
	0.001	--	Multilayer Switch0...	STP
	0.002	--	Multilayer Switch0...	STP
	0.002	--	Multilayer Switch0...	STP
	0.002	--	Multilayer Switch0...	STP
	0.002	Multilayer Swit...	Router0	STP
	0.002	Multilayer Swit...	Switch3(1)(1)	STP
	0.002	Multilayer Swit...	Switch3(2)	STP
	0.002	Multilayer Swit...	Switch2(1)	STP
	0.002	New YrokTD	Multilayer Switch0...	ICMP
	0.002	--	Multilayer Switch0...	STP
	0.003	--	Multilayer Switch0...	STP
	0.003	--	Multilayer Switch0...	STP
	0.003	Multilayer Swit...	Switch3(1)(1)	STP
	0.003	Multilayer Swit...	Switch3(2)	STP
	0.003	Multilayer Swit...	Switch2(1)	STP
	0.003	Multilayer Swit...	New YrokTD	ICMP
	0.003	--	Multilayer Switch0...	STP
	0.004	--	Switch3	STP
	0.004	--	Switch3(1)(1)	STP
	0.004	--	Switch3(2)	STP
	0.004	Multilayer Swit...	Switch3(1)(1)	STP
	0.004	Multilayer Swit...	Switch3(2)	STP
	0.004	Multilayer Swit...	Switch2(1)	STP
	0.004	Switch3(2)	Multilayer Switch0...	STP
	0.004	Switch2(1)	Multilayer Switch0...	STP
	0.004	New YrokTD	PC3(2)(1)	ICMP

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:
Considering Boston as the head office, we set up MAC in Boston. As shown in the figure below, the switch of Boston Technology Department is shown.



```
interface FastEthernet0/5
 switchport mode trunk
 switchport port-security
 switchport port-security maximum 10
 switchport port-security violation protect
 switchport port-security mac-address 0002.4A6B.479D
 switchport port-security mac-address 00E0.B0A6.B3EE
 switchport port-security mac-address 00E0.F77B.938C
!
```

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 LP address controlled by the server. When the client logs in to the server, it can automatically obtain the LP 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, 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.

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).

DNS: As a distributed database mapping domain name and IP address, it can make people access the Internet more conveniently.

Conclusion:

Through the study of this project, I have a deeper understanding of computer and data network knowledge, and this project helps me to be familiar with various operations. By completing this project, I transformed my theoretical knowledge into practical knowledge. As a network engineer, I clearly understand that the configuration of the network is a very important link. It can make computers and computers communicate with each other, thus constituting our network events. By understanding the DHCP configuration, I understand the computer's IP address assignment. Through DNS, I understand the resolution of domain name. In the light of some Internet failures, we solve them in various ways, which deepens our impression. Because of the time, there are a lot of work that I still haven't finished, and I still need to solve these problems.