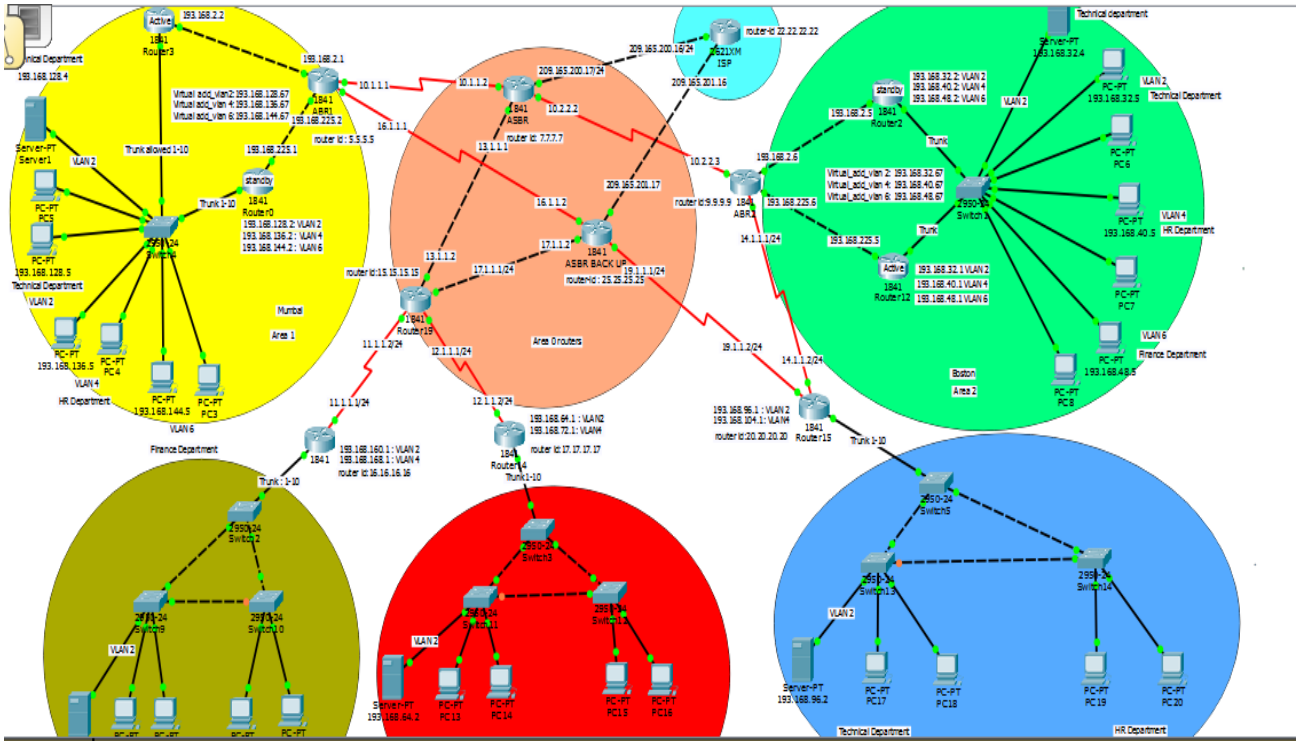
Data Networking
CPT Project

1. PROJECT DESIGN

Proposed Network Design:



Cost of Network Equipment:

Sr. No.	Equipment	Cost
1	Cisco 1841 router (12)	$565*$12 = $6780
2	Cisco switch 2960 (11)	$150*$11 = $1650
3	DHCP Server (5)	$500*$5 = $2500
4	Copper straight through cable	$0.6 per inch
5	Copper cross over cable	$1.9 per inch
6	Serial DCE	$3 per feet

Data link connection identifier: 24*5 = $120

Total network equipment cost: $6780 + $1650 + $2500 + $120 = **$11,050**

2. NETWORK OPTIMIZATION

- I have designed 5 offices of one company which has 2 headquarters Boston and Mumbai and 3 sub offices London, New York and Beijing. For headquarters I have used one switch and implemented different VLANs to reduce the equipment cost and implemented HSRP for both the headquarters if one link goes down traffic can go from another link. I have implemented switch redundancy for New York, Beijing and London. If one switch goes down traffic can go from another switch. I have implemented BPDUguard and port fast. BPDUguard blocked another port if we connect that port to another equipment. I have used routers in backbone area tried to configure minimum number of routers to cut down the cost of the network.

Detailed Architecture:

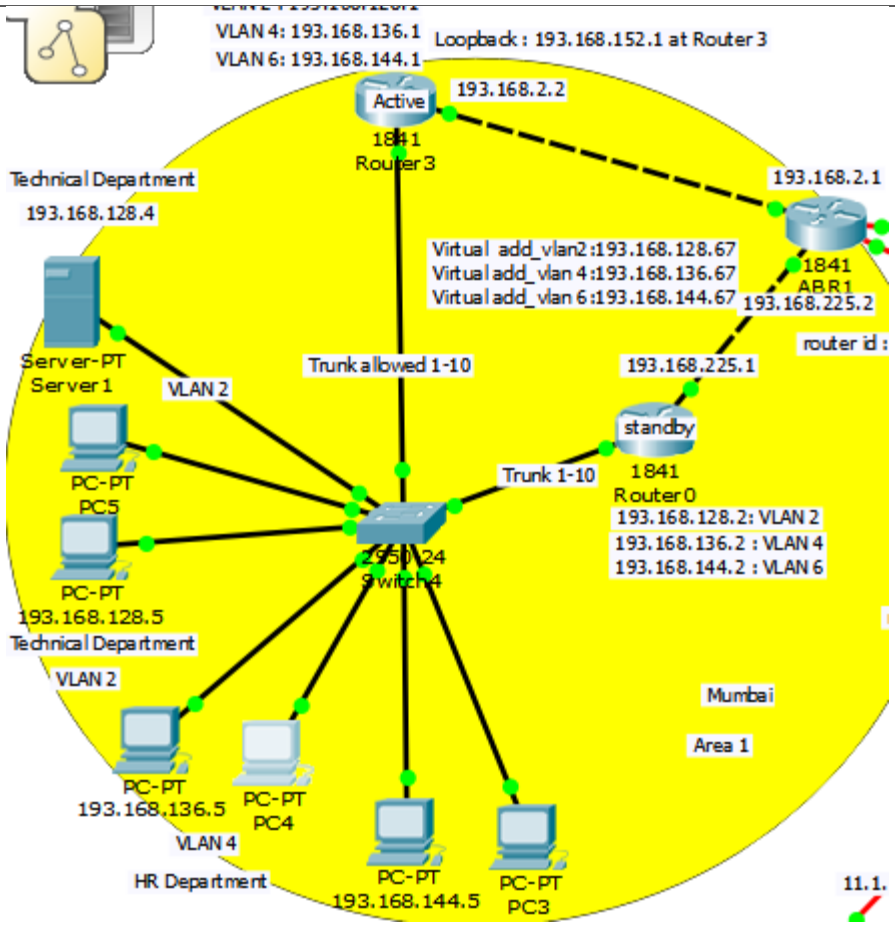
Network is in 5 locations:
1. Boston(headquarter)
2. Mumbai(headquarter)
3. London
4. New York
5. Beijing

VLAN and IP subnets

VLAN	Department	Boston	Mumbai
2	Technical	193.168.32.0/24	193.168.128.0/24
4	HR	193.168.40.0/24	193.168.136.0/24
6	Finance	193.168.48.0/24	193.168.144.0/24

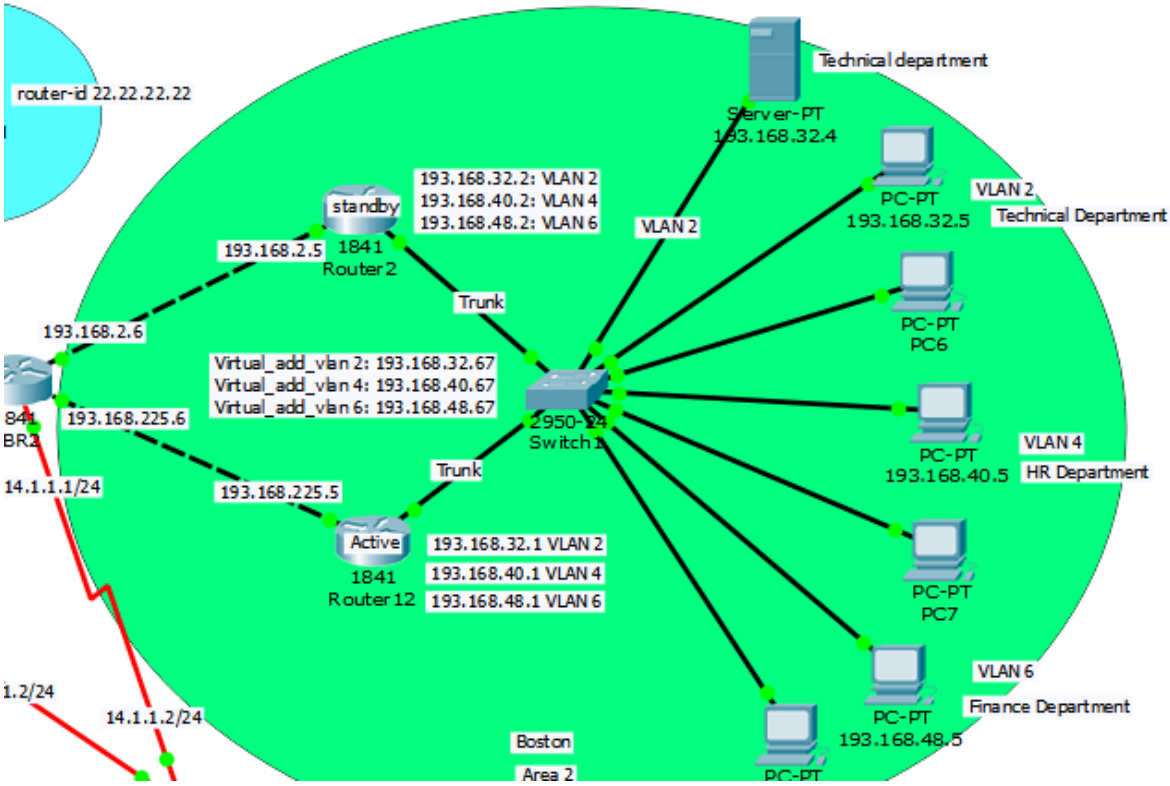
VLAN	Department	London	New York	Beijing
2	Technical	193.168.160.0/24	193.168.64.0/24	193.168.96.0/24
4	HR	193.168.168.0/24	193.168.72.0/24	193.168.104.0/24

Location 1: Mumbai



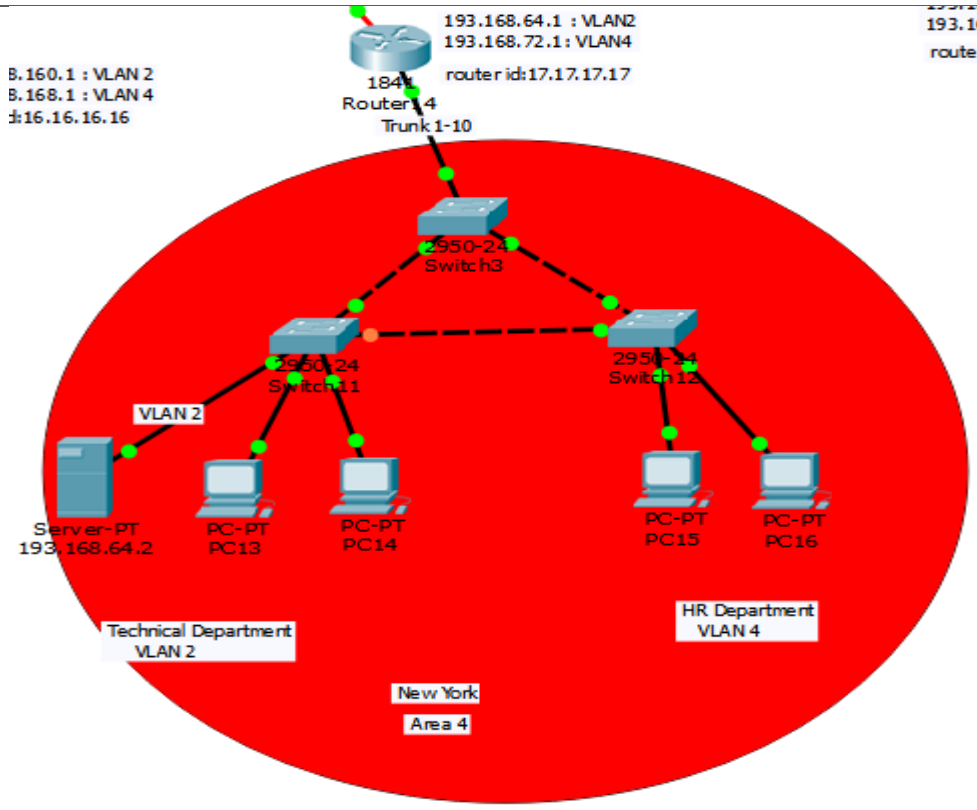
- Implemented HSRP
- Implemented OSPF
- 3 different department Technical, HR and Finance in 3 different VLANs 2,4 and 6
- Implemented in one single switch
- Implemented DHCP using server which is in technical department
- Created 3 sub interfaces to provide IP addresses in 3 different VLANs using DHCP

Location 2: Boston



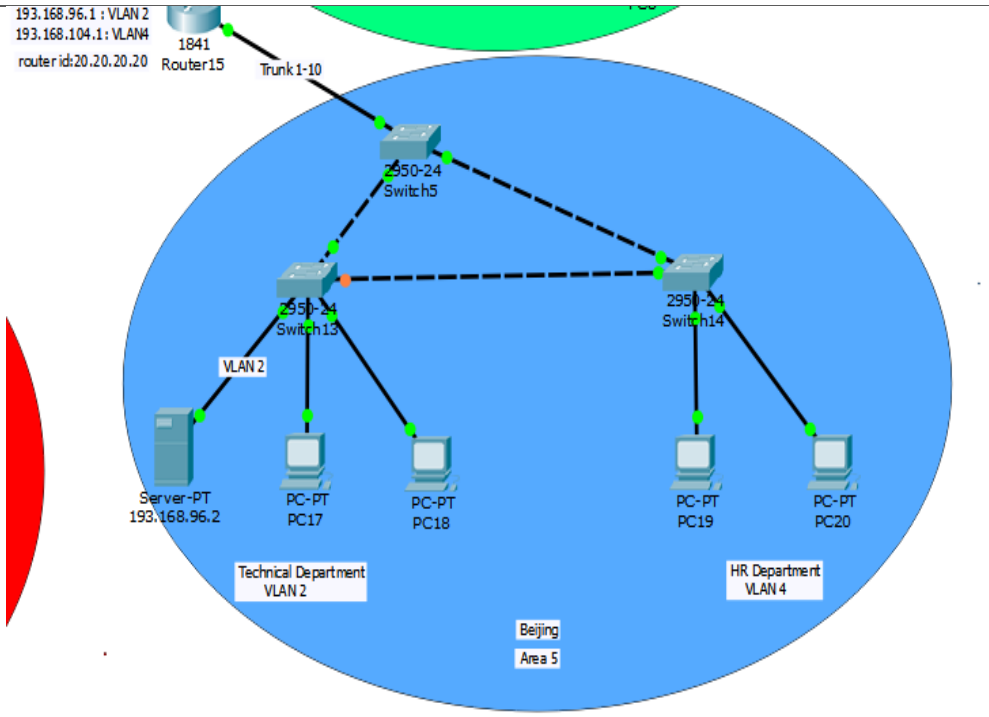
- Implemented HSRP
- Implemented OSPF
- 3 different department Technical, HR and Finance in 3 different VLANs 2,4 and 6
- Implemented in one single switch
- Implemented DHCP using server which is in technical department
- Created 3 sub interfaces to provide IP addresses in 3 different VLANs using DHCP

Location 3: New York



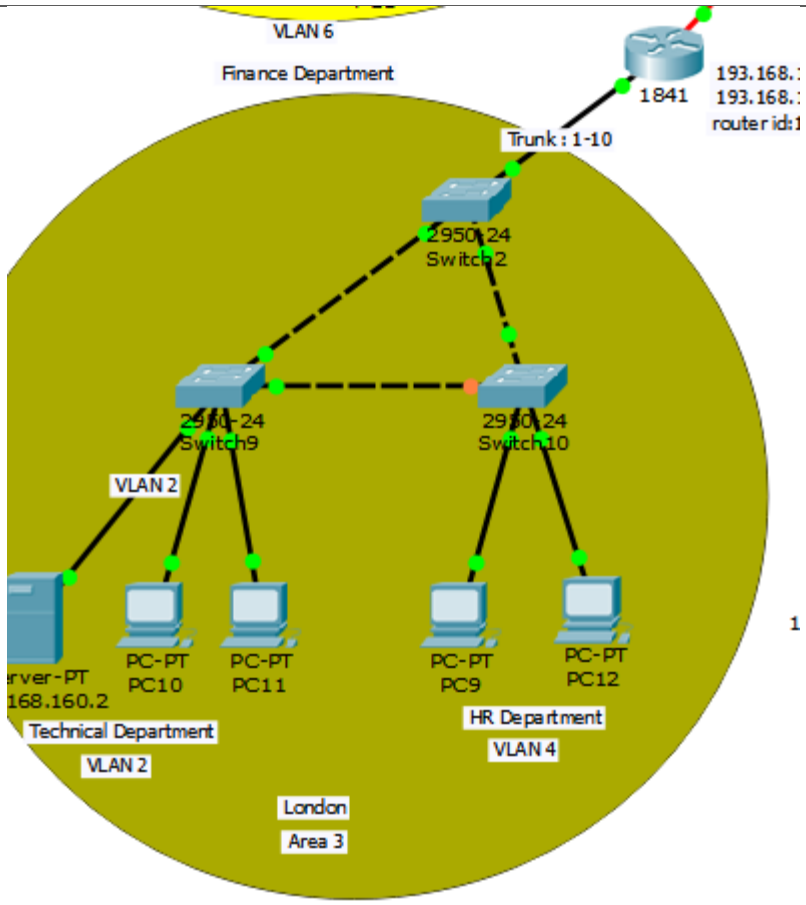
- Implemented RSTP
- Implemented switch redundancy
- Implemented OSPF
- 2 departments Technical and HR in VLAN 2 and 4
- Created 2 sub interface in router to give IP address using DHCP
- Server is in technical department in VLAN 2

Location 4: Beijing



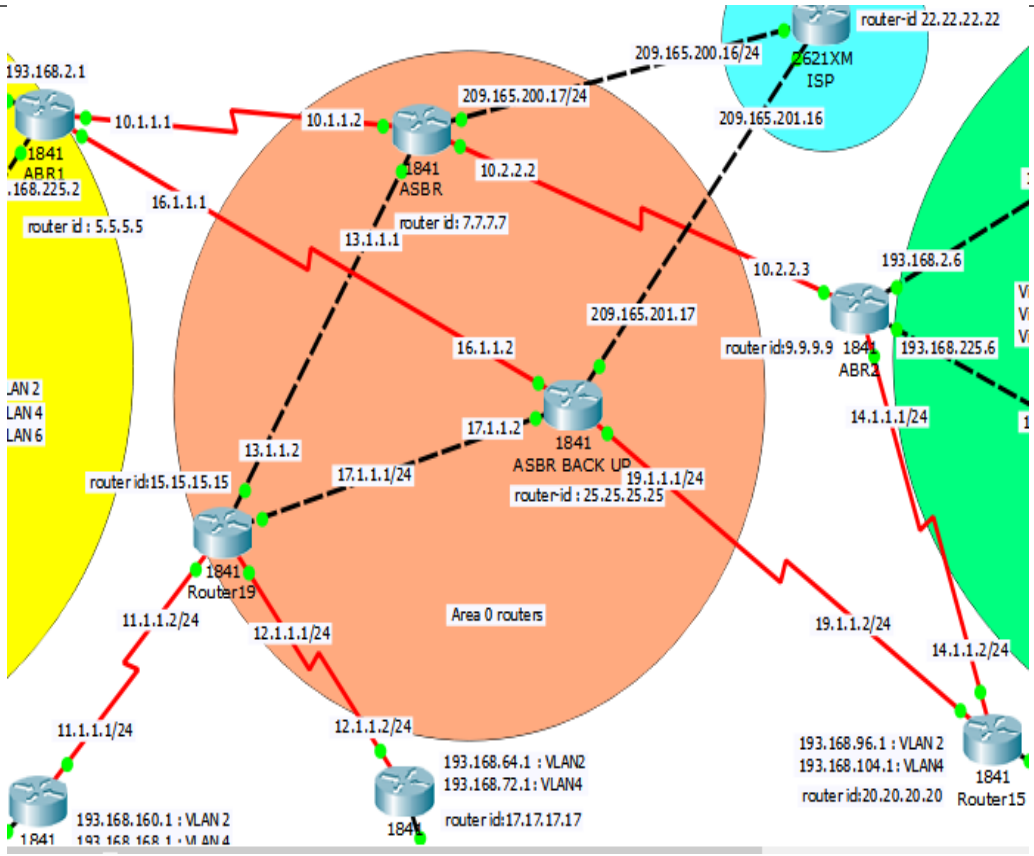
- Implemented RSTP
- Implemented switch redundancy
- Implemented OSPF
- 2 departments Technical and HR in VLAN 2 and 4
- Created 2 sub interface in router to give IP address using DHCP
- Server is in technical department in VLAN 2

Location 5: London



- Implemented RSTP
- Implemented switch redundancy
- Implemented OSPF
- 2 departments Technical and HR in VLAN 2 and 4
- Created 2 sub interface in router to give IP address using DHCP
- Server is in technical department in VLAN 2

Area 0 routers:



- Boundary routers of Mumbai and Boston connected to ASBR
- Boundary routers of London and New York connected to area 0 routers
- Boundary router of Beijing is connected to Boundary router of Boston because I have implemented considering both the location is near which will help us to cut down the cost
- I have also set up the backup router if ASBR is down then traffic can go from ASBR backup

Assignment of IP addresses

Source	destination	network	Subnet mask
Mumbai R1	ABR 1	193.168.2.0	255.255.255.0
ABR 1	ASBR 1	10.1.1.0	255.255.255.0
ASBR 1	ABR 2	10.2.2.0	255.255.255.0
ABR 2	Boston R1	193.168.225.0	255.255.255.0
ASBR 1	Area 0 router	13.1.1.0	255.255.255.0
Area 0 router	Lodnon boundary router	11.1.1.0	255.255.255.0
Area 0 router	New York boundary router	12.1.1.0	255.255.255.0

ABR 2	Beijing boundary router	14.1.1.0	255.255.255.0
Mumbai R1(router on stick)	switch	193.168.128.0 193.168.136.0 193.168.144.0	255.255.255.0
Boston R1(router on stick)	switch	193.168.32.0 193.168.40.0 193.168.48.0	255.255.255.0
London R1(router on stick)	switch	193.168.160.0 193.168.168.0	255.255.255.0
New York R1(router on stick)	switch	193.168.64.0 193.168.72.0	255.255.255.0
Beijing R1(router on stick)	switch	193.168.96.0 193.168.104.0	255.255.255.0

3. TAKEAWAY QUESTIONS

1.

- RIP is a distance vector protocol in which router sends routing information to neighbor in every 30 seconds.
- In OSPF every router sends its external link and state information it's all router and generates a shortest path tree
- OSPF is better than RIP in following ways:
- In RIP updates are periodic where in OSPF updates are triggered
- RIP has a hop count of 15 which can be used in small networks where as in OSPF there is no limitation of hop count
- OSPF provides better information because it contains Link state database which consist of cost information and link information
- when we run OSPF and RIP on the same network, we can see that the Administrative value(A.D.) (decides the routes) is more for RIP than OSPF. It means OSPF is preferred

2.

- OSPF network is divided in small domains called areas. An area contains small networks, routers and links
- In each area, a router must maintain a database for its own area for collecting all information related to that area
- frequent LSA-LSU link state resulted into high bandwidth utilization, high memory and processing power utilization
- OSPF summarize the path and gives us the best possible path. Therefore, the area concept will reduce the complexity of OSPF
- Hence, the main benefit of creating areas is reduction in the number of routes to propagate which included all filtering and synchronization information

3.
   - The backbone area 0 connects all the different areas of the network
   - If we want to send packet from area 1 to area 3 then area 1 pass its information to its boundary router and boundary router pass all this information to area 0 and then the packet will reach to area 3
   - Only single area can act as a backbone area otherwise there will be conflicts which route to choose
   - Hence, OSPF designers decided to designate the backbone area as area 0, which is the beginning and this number cannot be configured. And, any non-zero numbered area is considered as a regular area and the working becomes simpler

4.
   - Type 1: Router: a router sends this to describe neighbors and its interfaces.
   - Type 2: Network: it is generated by designated router (DR) for multi-access networks
   - Type 3: summary: summarize information about one area to update other are
   - Type 4: summary ASBR: it is sent by a border router that has sent a Type 5 LSA to describe how to get to that border router via the internal network.
   - Type 5: AS external: it is sent by a border router to describe external routes
   - Type 6: group membership: it is used in multicast version of Multicast Open Shortest Path First (MOSPF). Most routers no longer support MOSPF.
   - Type 7: NSSA external: NSSA is not-so-stubby-area. OSPF stub areas are those without a direct path to the outside and they do not allow Type 5 LSAs in. All externally bound traffic is routed out through the stub area's boundary router. A NSSA has some limited external routes available and they are advertised within the NSSA using Type 7 LSAs. The NSSA's boundary routers translate Type 7 LSAs into Type 5 LSAs to flood into adjacent areas.
   - Type 8: external attributes: it was used to convey BGP link attributes into an OSPF network, in OSPFv2. In OSPFv3, it has been repurposed to send information about all of the IPv6 address information associated with the local link.

5.
   - Single switch means single point of failure
   - We can create redundant links, but it creates loop in the network
   - Switch forwards broadcast packets to all ports
   - STP block redundant path and prevent loop
   - Switch sends probes into the network called BPDU (bridge protocol data unit) to
   - discover loops.
   - BPDU also helps to elect the core switch of the network called the root bridge.
   - All switches find the best way to reach the root bridge and then block all redundant paths.
   - Switch sends BPDU every 2 seconds.
   - BPDU= bridge priority + MAC = Bridge ID
   - Default bridge priority is 32768
   - Range of bridge priority is 0-65535.
   - Root bridge has lowest bridge ID.

- STP stages are:
  1. Listening
  2. Learning
  3. Forwarding
  4. Blocking

6.

- STP: Used for avoiding loops in network
- PVSTP: Used to separate traffic in multi VLAN network
- MSTP: Multiple instance of spanning tree but not every VLAN is in different instance of spanning-tree

4. TEST PLAN FOR THE NETWORK

- **Test VLAN**

```
Switch>
Switch>en
Switch#show int vlan
% Incomplete command.
Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/10, Fa0/11, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24
2    VLAN0002                          active    Fa0/2, Fa0/3, Fa0/9
4    VLAN0004                          active    Fa0/4, Fa0/5
6    VLAN0006                          active    Fa0/6, Fa0/7
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
4    enet  100004     1500  -      -      -        -    -        0      0
6    enet  100006     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
```

DHCP

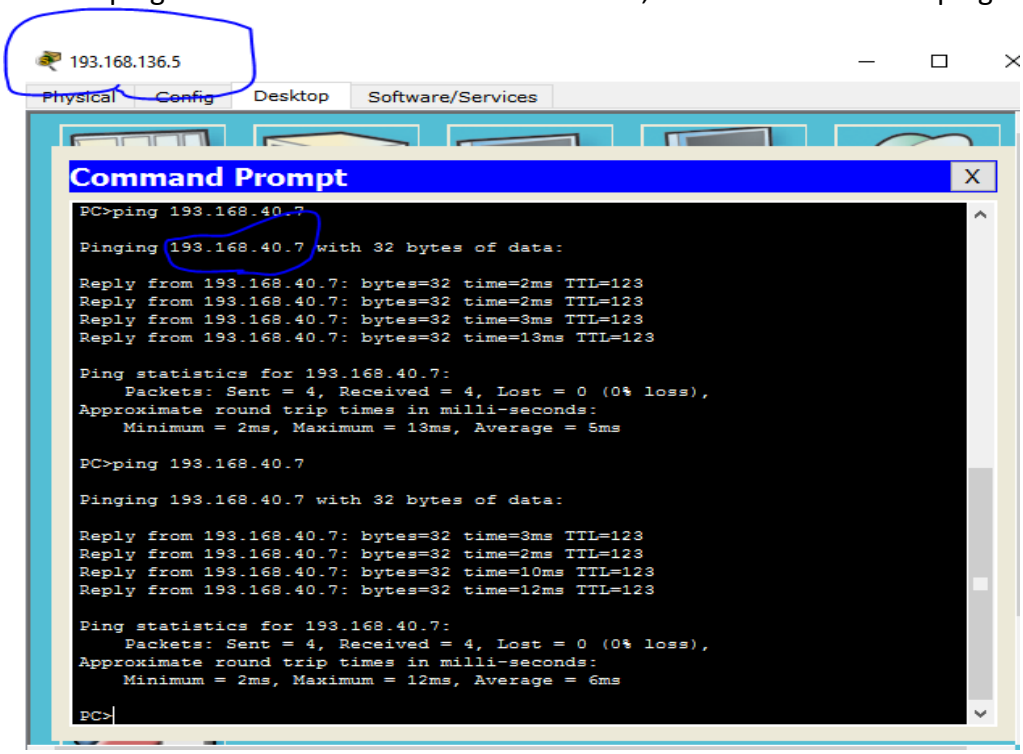
In the above picture you can see that there are three VLAN and each VLAN has 2 ports except VLAN 2 because fa 0/9 is connected to DHCP server it means DHCP server is in technical department.

- **Test routing protocol**

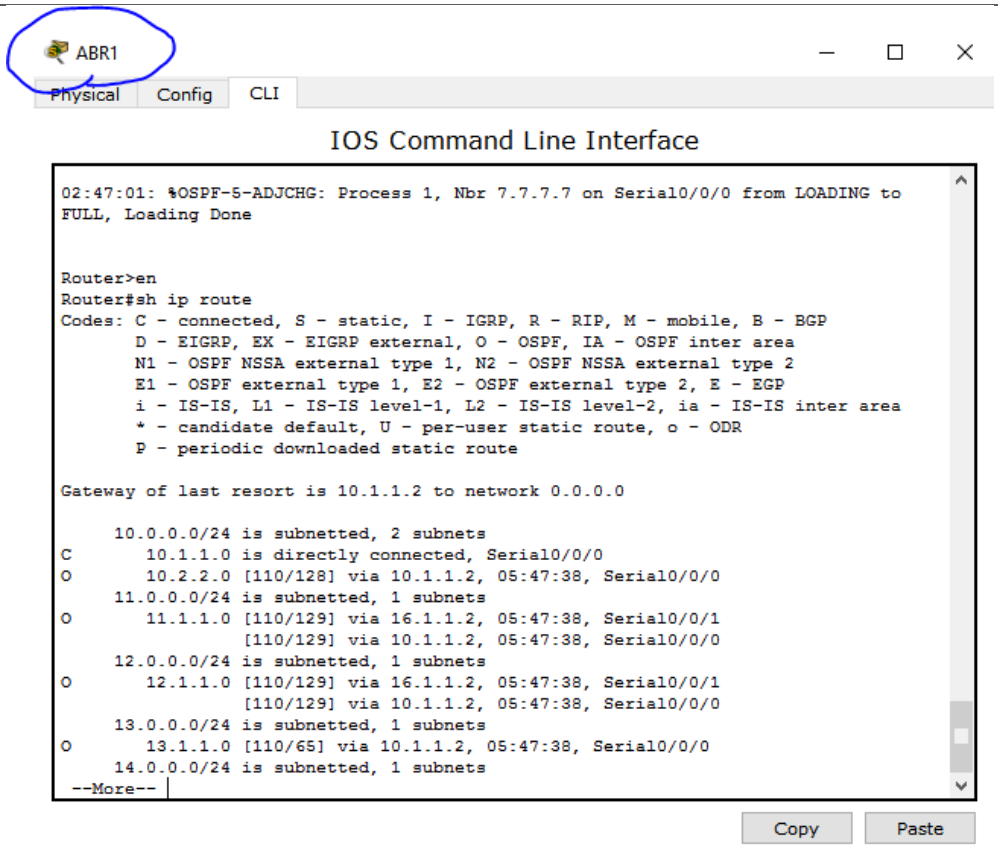
  Configuration of ospf:

```
router ospf 1
 router-id 7.7.7.7
 log-adjacency-changes
 network 10.1.1.0 0.0.0.255 area 0
 network 10.2.2.0 0.0.0.255 area 0
 network 13.1.1.0 0.0.0.255 area 0
 network 209.165.200.0 0.0.0.255 area 0
 default-information originate
```

If we are able to ping from Mumbai's HR Department to Boston's HR department then we can say that OSPF is working
Boston HR department PC's IP: 193.168.136.7
Mumbai HR department PC's IP: 193.168.40.7
And we ping from 193.168.136.7 to 193.168.40.7, below is the result of ping:



Ospf configuration (boundary router Mumbai ABR1):



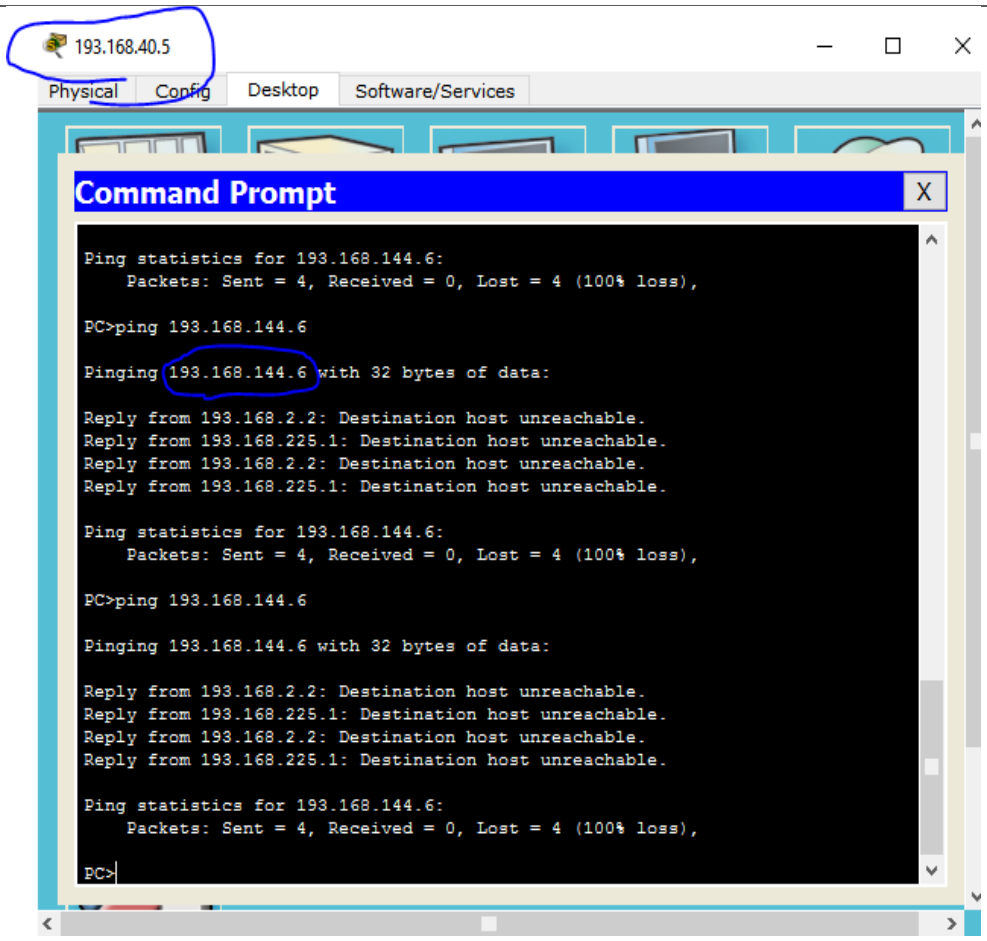
- **Test Security plan**

  I have implemented extended Access list so that no other department can access finance department and finance department can access each other and access all other department.

  Configuration of ACL at London office router:

```
access-list 103 permit icmp any any echo-reply
access-list 103 deny ip 193.168.160.0 0.0.0.255 193.168.144.0 0.0.0.255
access-list 103 deny ip 193.168.160.0 0.0.0.255 193.168.48.0 0.0.0.255
access-list 103 deny ip 193.168.168.0 0.0.0.255 193.168.48.0 0.0.0.255
access-list 103 deny ip 193.168.168.0 0.0.0.255 193.168.144.0 0.0.0.255
access-list 103 permit ip any any
!
!
!
!
!
```

  This extended access list 103 is implemented in sub interface 0/0.2 and 0/0.4, so this list will block all the requests which are going to the finance department of Boston and Mumbai. The same thing I have implemented in all of the offices boundary router. Also, I have implemented BPDUguard. If you connect switchport to some other switch, then the BPDUguard will block the port.



In the above example I have tried to ping from Boston's HR department to Mumbai's Finance department but using ACLs we have blocked that network that is why it is giving destination host unreachable and that reply is coming from the router.

- **Test redundancy plan**

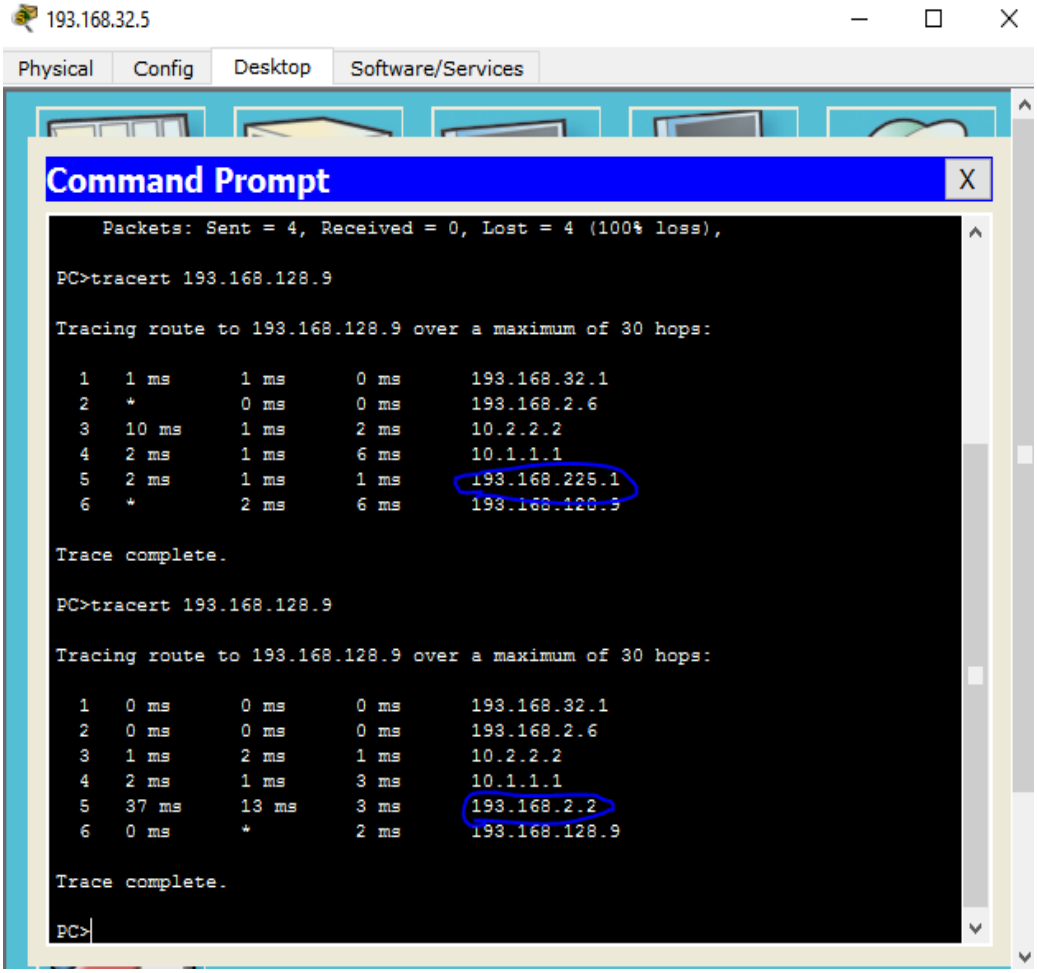
To check redundancy, we turned off the active link of Mumbai office and see whether we can still ping using standby router

HSRP configuration on active router:

```
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip address 193.168.128.1 255.255.255.0
 ip helper-address 193.168.128.4
 standby version 2
 standby 1 ip 193.168.128.67
 standby 1 priority 105
 standby 1 preempt
 standby 1 timers 2 6
 standby 0 track FastEthernet0/1
!
```

HSRP configuration on standby router:

```
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip address 193.168.128.2 255.255.255.0
 ip helper-address 193.168.128.4
 standby version 2
 standby 1 ip 193.168.128.67
```



When we ping from 193.168.32.5(Technical department of Boston) to 193.168.128.9(Technical department of Mumbai):
1. In the above example 193.168.225.1 is showing that we ping through standby router because active router is not on.
2. In the above example 193.168.2.2 is showing that we ping through the active router

- **Test mac flood BPDU guard**

```
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
 switchport port-security maximum 3
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
 switchport port-security maximum 3
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

Implemented port security to defend the mac flooding attack and enable BPDU guard.

- **Control all router in one router**
  I have tried to implement only one control router for this one large network and also implemented one back up router if at all the main router link go down.

5. CONCEPTS LEARNED DURING THE PROJECTS

- OSPF
- HSRP
- VLANs and Trunk
- Access List
- DHCP
- RTP
- RSTP
- IP subnetting

6. CONCLUSION

- Successfully implemented network for 5 offices including 2 head offices and 3 sub offices on Cisco Packet Tracer. We have successfully implemented HSRP, OSPF and ACLS, VLANs and Trunk, RSTP, portfast and BPDUguard**.** We have tried to optimize the network to reduce the cost. We have implemented BPDUguard and ACLs for security purposes.