PROJECT REPORT

DATA NETWORKING_TELE_5330

CISCO PACKET TRACER

MANIK KUMAR 001063023

1. DESIGN

1.1 High Level Network Diagram

Below is an overview diagram of the network created in Packet Tracer.

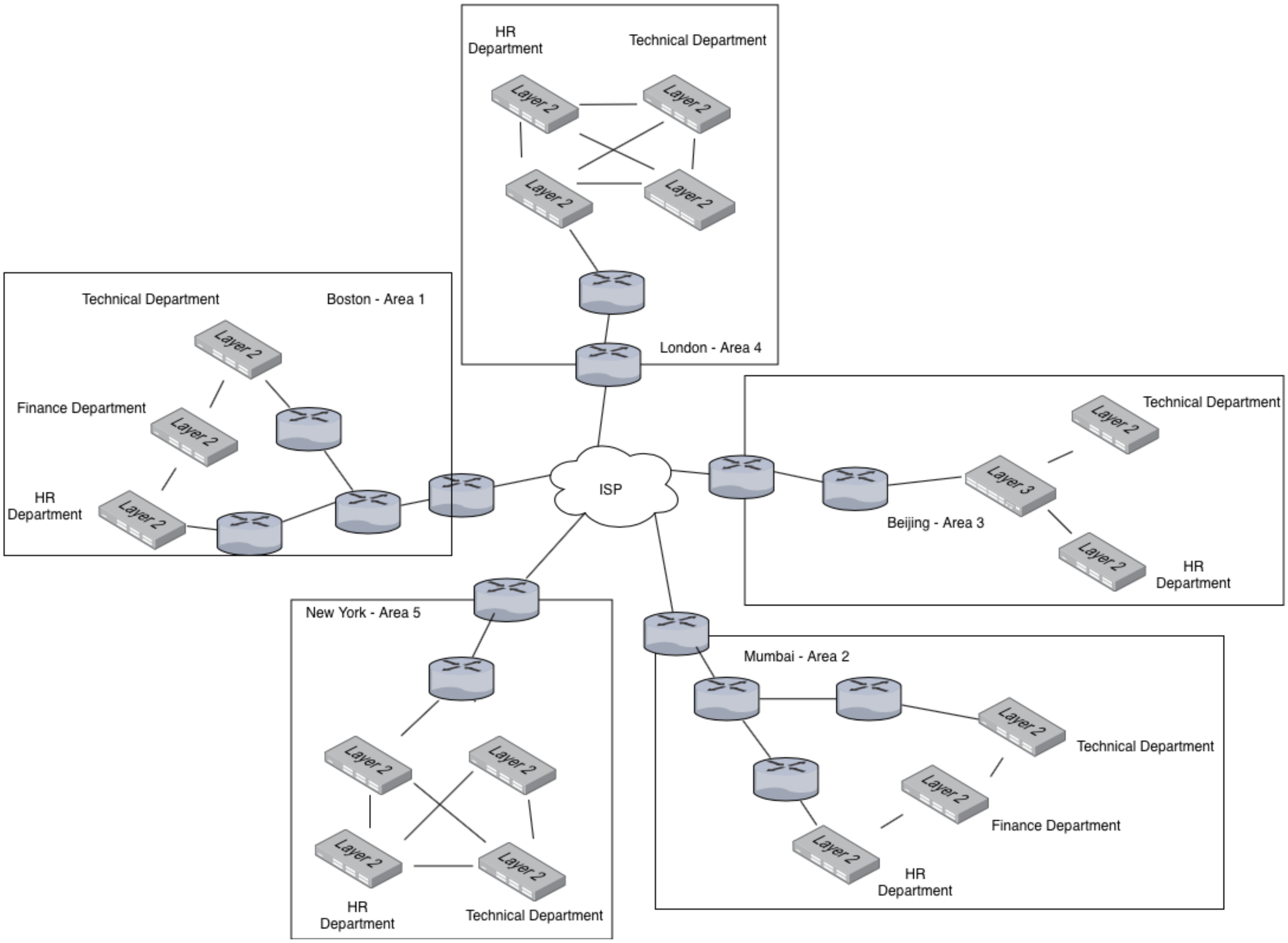


Figure 1: Network Overview

1.2 Equipment Used and Cost

Area Border Routers : Cisco ISR 4451 – X/K9

Internal Office Routers : Cisco 2911/K9

Layer 2 Switches : Cisco 2960X – 24PS

Layer 3 Switches : Cisco 3560 – 24PS

Model	Cost(Approx.)[1]
ISR4451	USD 6000
2911/K9	USD 1800
2960X	USD 800
3560	USD 1700

2. NETWORK OPTIMIZATION AND DETAILED ARCHITECTURE

2.1 Cost Optimization of Network

Assigned Budget to HQ cities : USD 20k.

Assigned Budget to other cities : USD 15k.

2.1.1 Internal Office Routers

For internal office edge router use I decided to go with a Cisco 2911 router, although it’s an older model but it’s optimized for edge router usage and is reliable and fast enough to easily support up-to 500 devices.

2.1.2 Area Border Routers

For ABR usage I decided to use a much powerful and newer model, Cisco 4451 router. Given it would be the router an office will receive its connection from, it was required that it’s reliable and has enough bandwidth. *(Note: Cisco Pkt Tracer did not have a 4451 simulation, hence I used a generic router and spec’d it according to a 4451)*

2.1.3 Switches

I decided to go with a 24 Port Cisco 2940 Layer 2 Switches and a Layer 3 Cisco 3560 Switch to be used in Beijing.

2.1.4 Costing

In Boston and Mumbai HQ locations, we used:

2x 2911 Routers

3x 2960 Switches

1x 4451 Router

Total : 11,200 USD out of 20,000 USD

In New York and London, we used:

1x 2911 Routers

4x 2960 Switches

1x 4451 Routers

Total: 11,000 USD out of 15,000 USD

In Beijing we used:

1x 2911 Router

2x 2960 Switches

1x 3560 Switches

1x 4451 Router

Total: 11,100 USD out of 15,000 USDD

Hence, we're well under budget everywhere. We can easily add more switches to expand to have to more users on the network with our remaining budge

2.2 Detailed Network Architecture

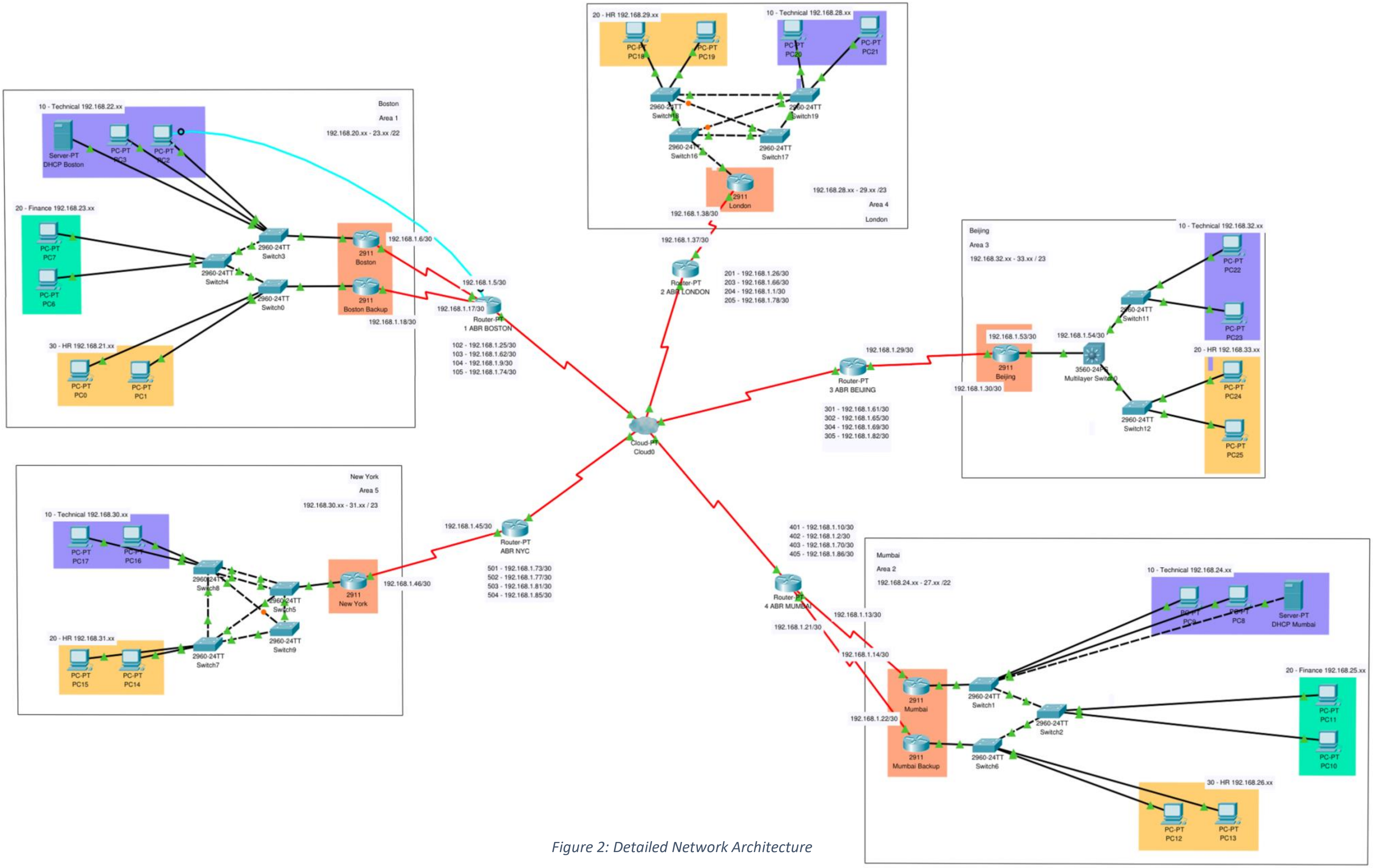


Figure 2: Detailed Network Architecture

2.2.1 Detailed Network Architecture Explained

The organization network architecture has the following important key features:

- **OSPF**

  OSPF is a routing protocol which uses Link-State Routing Algorithm. All routers in the network run OSPF routing protocol with areas on it.
  Boston is Area 1,
  Mumbai is Area 0,
  Beijing is Area 3,
  London is Area 4,
  New York is Area 5,
  And the rest of the underlying network is Area 0.

- **Frame Relay**

  All the ABR routers connect to an ISP, which is emulated by a cloud. This ISP then runs a frame relay service which relays the data from a certain location to another.

- **HSRP**

  HSRP is a router redundancy service, which groups two routers and makes them act like one via a virtual IP, in case of a router failure, the data link seamlessly moves from one HSRP router to another.

  Both 2911 routers in both HQ locations run HSRP on them.

- **DHCP Servers**

  There are two DHCP servers in our network. One is hosted in Boston’s technical department and the other in Mumbai’s technical department.

- **VLANs**

  Mumbai and Boston both have 3 VLANs, one for each department.

  VLAN 10 for Technical.
  VLAN 20 for Finance.
  VLAN 30 for HR.

  All other cities have 2 VLANs, one for each department.

  VLAN 10 for Technical.
  VLAN 20 for HR.

2.3 Assignment of IP address

Each office required 250 employees. And an IP redundancy of 85%.

That means, the required IP addresses are 250 + 250*0.80 = 463 IP addresses.

Closest network we can create with wasting the least number of addresses a /23 network.

In the cities we only have 2 VLANS I decided on using a /23 network with two /24 subnets in it:

New York : Entire network is on 192.168.30.xx – 192.168.31.xx /23

VLAN 10 is on 192.168.30.xx / 24 - *Technical*

VLAN 20 is on 192.168.31.xx / 24 - *HR*

London : Entire network is on 192.168.28.xx – 192.168.29.xx /23

VLAN 10 is on 192.168.28.xx / 24 - *Technical*

VLAN 20 is on 192.168.29.xx / 24 - *HR*

Beijing : Entire network is on 192.168.32.xx – 192.168.33.xx /23

VLAN 10 is on 192.168.32.xx / 24 - *Technical*

VLAN 20 is on 192.168.33.xx / 24 - *HR*

For the HQ locations we have 3 VLANS and for best practice I choose an entire /24 subnet for each VLAN which means we cannot contain all the required IP addresses for the networks in a /23 network, hence a move to /22 network was required.

Although this move wastes a lot more IP addresses, it was preferred better than using common DHCP pools, this also gives us a lot more capability for extension in future.

Boston : Entire network is on 192.168.20.xx – 192.168.23.xx /22

VLAN 10 is on 192.168.23.xx / 24 - *Technical*

VLAN 20 is on 192.168.24.xx / 24 - *Finance*

VLAN 30 is on 192.168.21.xx / 24 - *HR*

Mumbai : Entire network is on 192.168.24.xx – 192.168.27.xx /22

VLAN 10 is on 192.168.24.xx / 24 - *Technical*

VLAN 20 is on 192.168.26.xx / 24 - *Finance*

VLAN 30 is on 192.168.26.xx / 24 - *HR*

2.4 Individual Headquarters Office Networks

Boston

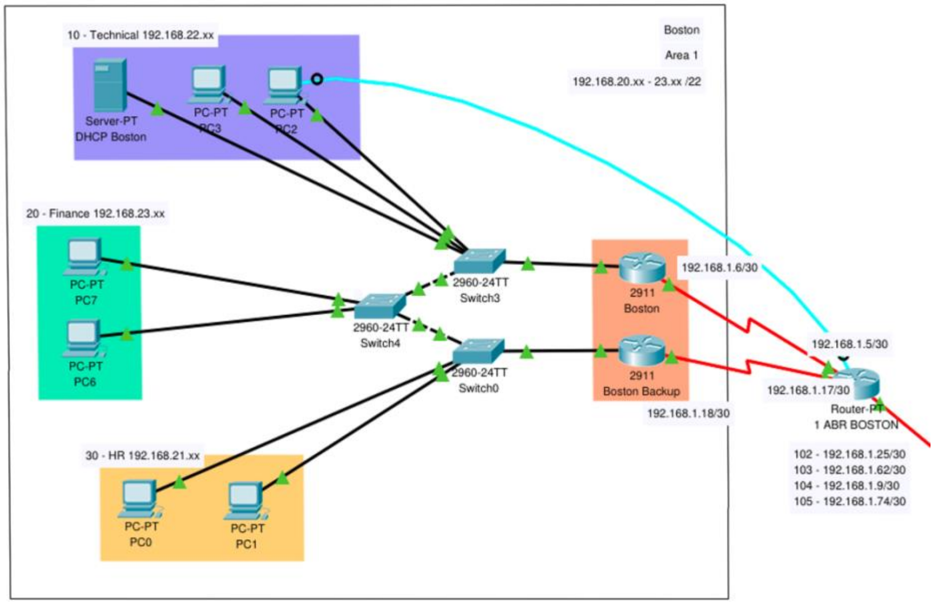


Figure 3: Boston Architecture

Above is the network architecture of Boston.

Boston is OSPF area 1, which starts from the Boston's ABR router. The ABR router connects to two internal company 2911 routers which are configured to have HSRP running on them. The ABR router can only be accessed by the Technical department of Boston and has access limitations when tried to be accessed by anywhere else.

As we can see, each department gets its own switch which runs the departments VLAN.

Mumbai

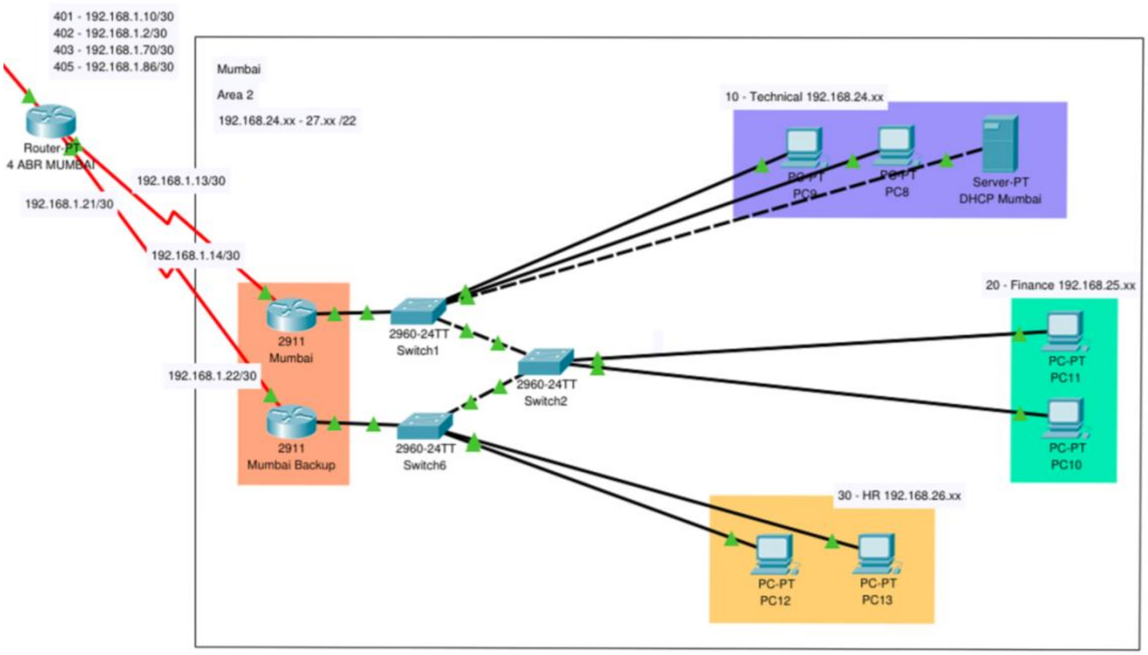


Figure 4: Mumbai Architecture

Similarly, to the Boston HQ, the Mumbai has two internal routers running HSRP which are connected to by the Mumbai's ABR router via two serial links. Similar to Boston, each department gets its own VLAN, which runs the departments VLAN.

3. TAKEAWAY QUESTIONS

3.1 About OSPF Protocol

3.1.1 Is RIPv2 better or OSPF?

The main difference between OSPF and RIPv2 is that RIP keeps track of only its closest neighboring routers, while OSPF sends and exchanges messages once setup to analyze all possible paths to find the shortest possible path.

To answer if OSPF is better than RIPv2, it's not a straightforward answer, technically speaking yes, it does offer the added benefit of always talking the shortest possible path over RIP but that is at an added overhead. So, there are possible scenarios where RIPv2 would actually be the preferred choice over the OSPF[3].

Usually big and convoluted networks prefer to use OSPF over RIP, because the added overhead isn't that much when compared to the overhead of not talking the shortest path possible. And, smaller networks like a home network would prefer to use RIP because there aren't really that many possible hops to cause a significant delay anyways.

So overall, I'd say OSPF is a technically superior routing protocol, but it still doesn't supersede RIP and both the routing protocols are used based on different requirements.

3.1.2 Why does OSPF need the concept of areas?

OSPF uses Link State Advertisements (LSA) to check and report on its neighbor's network address and their state. Each OSPF router send and receives these LSA messages and then aggregates them to create a routing table, as you can imagine the more the routers that exist on the network, the bigger the routing table a router would have to keep.

Areas were introduced to OSPF to rid routers of the problem of keeping humongous routing tables. With areas, an OSPF router only has to keep a routing list of routers in its own area, and for the times when a packet has to be sent to some other area, it keeps track of the shortest path to that particular area as well. Areas helped OSPF routers to avoid going through intensive task of going through a huge routing table each time a packet goes through it, helping the overall network be a lot more efficient.

3.1.2 Why do we configure the backbone area 0?

People often miss out that OSPF uses Distance-Vector Protocol in addition to the Link State Protocol as well. In OSPF with areas, OSPF uses Distance Vector to route from an area to another. And with Distance-Vector Protocols, there exists a "counting to infinity" problem[2], that is why OSPF requires all the areas to connect to the area 0 forming this star like topology.

Using the backbone area 0, OSPF prevents inter-area routing loops by implementing a split-horizon mechanism allowing ABRs to gain access to the backbone by only Summary-LSAs derived from the intra-area routes, and limiting ABRs' SPF calculation to consider only Summary-LSAs in the backbone area's link-state database.

3.1.3 Different types of LSAs in OSPF?

LSA Type 1: Packets sent between the routers between the same area, which do not leave the area. Packets sent to describe its own interfaces.

LSA Type 2: Packets sent by the designated router to describe all the routers connected to it directly.

LSA Type 3: Packets generated by Area Border Router to describe it's directly connected area.

LSA Type 4: These are the LSAs which broadcast the presence of an ABSR in other areas.

LSA Type 5: Messages generated by an ABSR to advertise external redistributed routes.

LSA Type 6: LSA type 6 messages were designed for Multicast OSPF, a protocol that allows for multicast routing through OSPF.

LSA Type 7: Packets used by some areas which do not allow externally distributed routes to go through the area.

LSA Type 8: Type 8 packets are packets redefined packets designed to carry IPv6 Information through OSPF.

LSA Type 9, **10, 11:** The last three LSA Types exist to allow us to extend the capabilities of OSPF based on our network's requirements. They can carry data and information in them about things which OSPF doesn't necessarily care about.

3.2 How does STP avoids looping?

Spanning Tree protocols looks for possible loops that may occur in a network and blocks redundant links. STP when it finds a redundant port, it shuts it down.[4]

When more than one link is connected to the root bridge(Switch), only one of them is used and all others are blocked. STP assigns a root bridge a designation port, which is a port the said root bridge will use to forward packets and then it assigns root port, which is a port that is used for receiving packets. On how STP decides whether to block which port, it decides based on a number of factors like Bandwidth, Path cost etc.

3.3 Difference between STP, PVSTP AND MSTP.

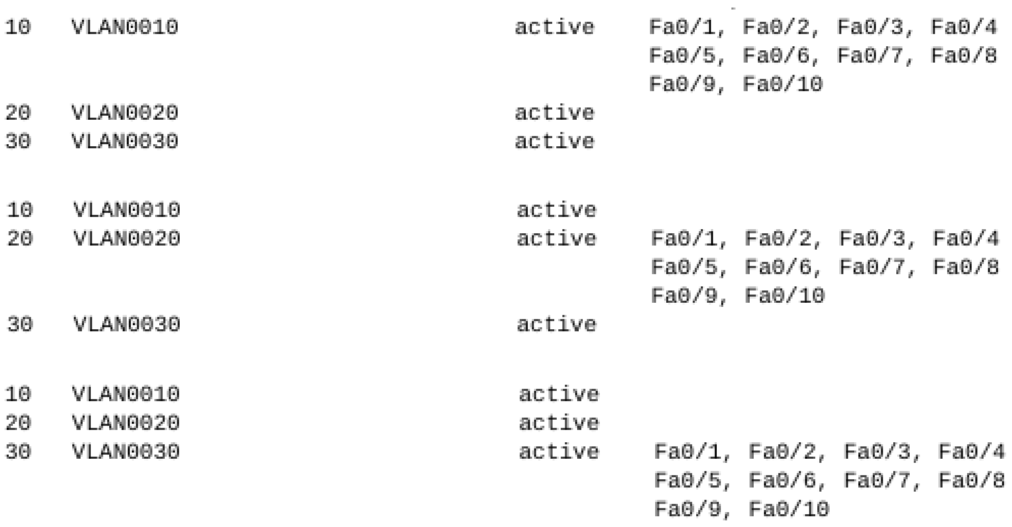
STP	PVSTP	MSTP
Uses a single instance on all ports on the switched network.	Uses separate instances of STP for every virtual LAN.	Uses multiple STP instances but can map multiple VLANS to the same instance
STP doesn't support load balancing as it decides a single port to use in advance	Supports Load balancing, can dynamically use more than one port, as it runs multiple instances of STP.	Supports Load balancing, and alternate routes can be selected like PVSTP.
Very light on resources and minimal overhead.	Requires a lot of resources and introduces overhead.	Uses more recourses than STP but fewer recourses than PVSTP

4. TESTING

4.1 VLANs

First step in testing our VLANs is to check if they exist properly. (Note: This testing was done in Boston).

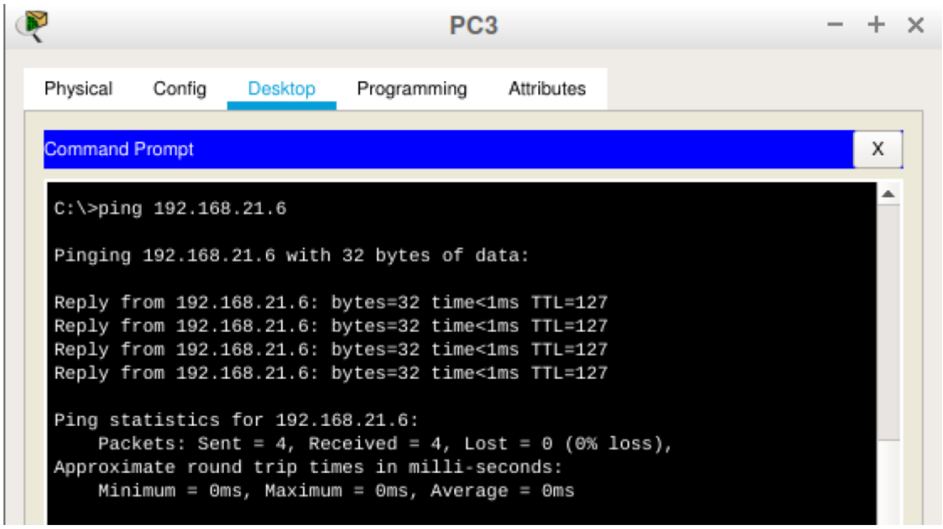
Output from the three switches :



```
10   VLAN0010                         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10
20   VLAN0020                         active
30   VLAN0030                         active

10   VLAN0010                         active
20   VLAN0020                         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10
30   VLAN0030                         active

10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10
```

Figure 5: VLANs exiting on switches

We can observe the three VLANs exist in the switches, and now to check if we can ping from a VLAN to another. (Note: If the connections between the switches are on trunking and they allow the three VLANs, only then the ping will go through)



```
C:\>ping 192.168.21.6

Pinging 192.168.21.6 with 32 bytes of data:

Reply from 192.168.21.6: bytes=32 time<1ms TTL=127
Reply from 192.168.21.6: bytes=32 time<1ms TTL=127
Reply from 192.168.21.6: bytes=32 time<1ms TTL=127
Reply from 192.168.21.6: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.21.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

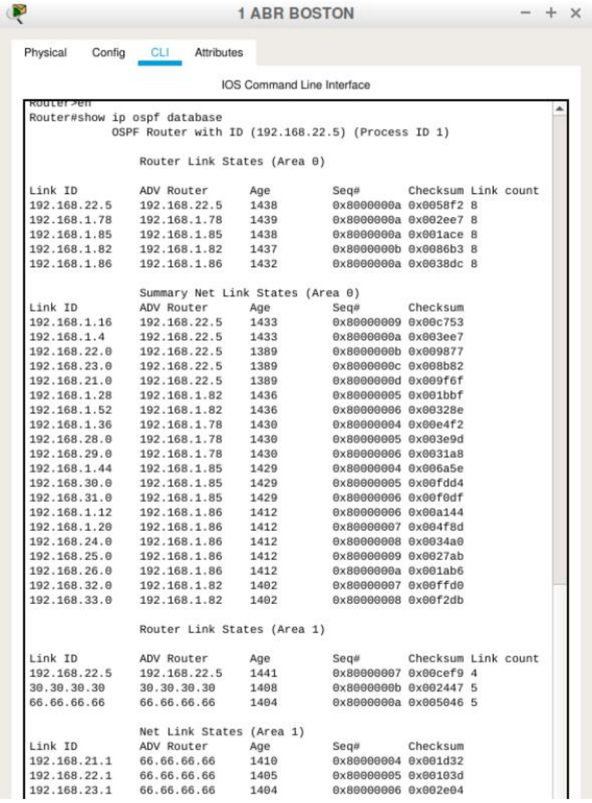
Figure 6: Ping to another VLAN

Pinging from PC3 in the VLAN 10(refer back to our Boston Architecture) to 192.168.21.6 which is in VLAN 30. We're able to do it successfully hence our Inter-VLAN routing is working perfectly.

4.2 Routing Protocols

In this section we’ll be testing if our routing protocol i.e. OSPF works properly.

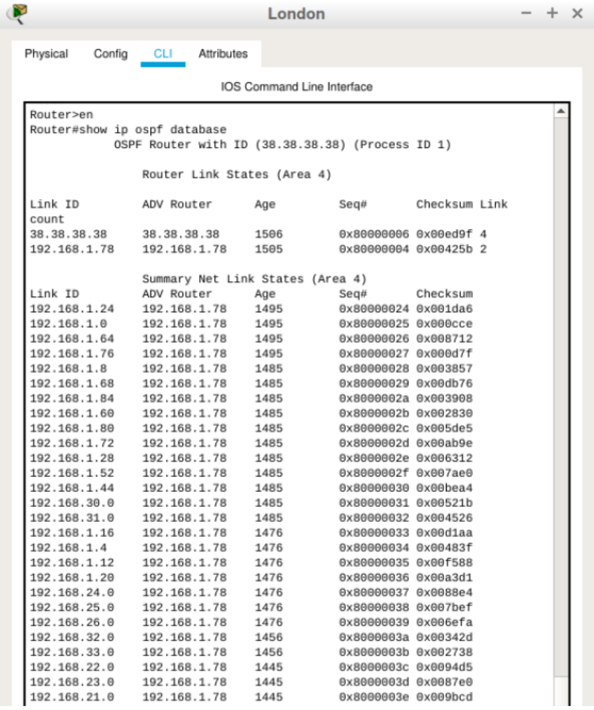
After configuring the OSPF with areas on every router we’ll try and look at the OSPF Database on multiple routers to confirm the Database exists and is correct and then we’ll try to ping across the network.



```
Router>en
Router#show ip ospf database
            OSPF Router with ID (192.168.22.5) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
192.168.22.5    192.168.22.5    1438        0x8000000a 0x0058f2 8
192.168.1.78    192.168.1.78    1439        0x8000000a 0x002ee7 8
192.168.1.85    192.168.1.85    1438        0x8000000a 0x001ace 8
192.168.1.82    192.168.1.82    1437        0x8000000b 0x0086b3 8
192.168.1.86    192.168.1.86    1432        0x8000000a 0x0038dc 8

                Summary Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.1.16    192.168.22.5    1433        0x80000009 0x00c753
192.168.1.4     192.168.22.5    1433        0x8000000a 0x003ee7
192.168.22.0    192.168.22.5    1389        0x8000000b 0x009877
192.168.23.0    192.168.22.5    1389        0x8000000c 0x008b82
192.168.21.0    192.168.22.5    1389        0x8000000d 0x009f6f
192.168.1.28    192.168.1.82    1436        0x80000005 0x001bbf
192.168.1.52    192.168.1.82    1436        0x80000006 0x00328e
192.168.1.36    192.168.1.78    1430        0x80000004 0x00e4f2
192.168.28.0    192.168.1.78    1430        0x80000005 0x003e9d
192.168.29.0    192.168.1.78    1430        0x80000006 0x0031a8
192.168.1.44    192.168.1.85    1429        0x80000004 0x006a5e
192.168.30.0    192.168.1.85    1429        0x80000005 0x00fdd4
192.168.31.0    192.168.1.85    1429        0x80000006 0x00f0df
192.168.1.12    192.168.1.86    1412        0x80000006 0x00a144
192.168.1.20    192.168.1.86    1412        0x80000007 0x004f8d
192.168.24.0    192.168.1.86    1412        0x80000008 0x0034a0
192.168.25.0    192.168.1.86    1412        0x80000009 0x0027ab
192.168.26.0    192.168.1.86    1412        0x8000000a 0x001ab6
192.168.32.0    192.168.1.82    1402        0x80000007 0x00ffd0
192.168.33.0    192.168.1.82    1402        0x80000008 0x00f2db

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link count
192.168.22.5    192.168.22.5    1441        0x80000007 0x00cef9 4
30.30.30.30     30.30.30.30     1408        0x8000000b 0x002447 5
66.66.66.66     66.66.66.66     1404        0x8000000a 0x005046 5

                Net Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.21.1    66.66.66.66     1410        0x80000004 0x001d32
192.168.22.1    66.66.66.66     1405        0x80000005 0x00103d
192.168.23.1    66.66.66.66     1404        0x80000006 0x002e04
```

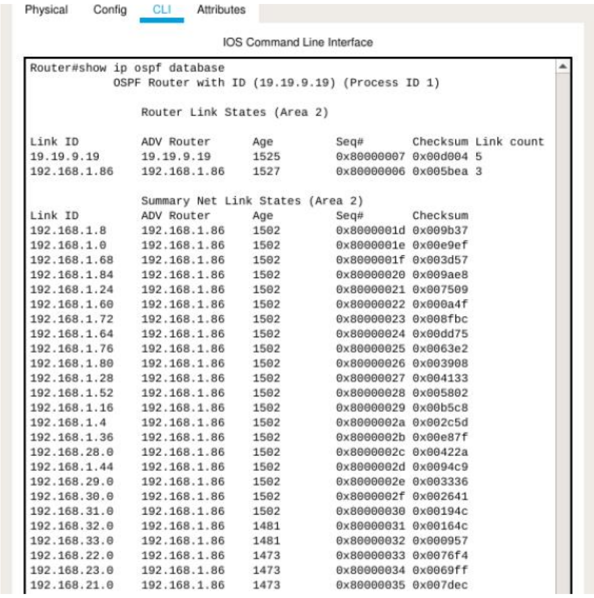
Figure 9: ABR Boston routing table

As we can see, the routing tables exist in each of the selected routers. Now to try and ping from Boston to Mumbai and London(Referring back to how I assigned IP addresses).



```
Router>en
Router#show ip ospf database
            OSPF Router with ID (38.38.38.38) (Process ID 1)

                Router Link States (Area 4)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
38.38.38.38     38.38.38.38     1506        0x80000006 0x00ed9f 4
192.168.1.78    192.168.1.78    1505        0x80000004 0x00425b 2

                Summary Net Link States (Area 4)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.1.24    192.168.1.78    1495        0x80000024 0x001da6
192.168.1.0     192.168.1.78    1495        0x80000025 0x000cce
192.168.1.64    192.168.1.78    1495        0x80000026 0x008712
192.168.1.76    192.168.1.78    1495        0x80000027 0x000d7f
192.168.1.8     192.168.1.78    1485        0x80000028 0x003857
192.168.1.68    192.168.1.78    1485        0x80000029 0x00db76
192.168.1.84    192.168.1.78    1485        0x8000002a 0x003908
192.168.1.60    192.168.1.78    1485        0x8000002b 0x002830
192.168.1.80    192.168.1.78    1485        0x8000002c 0x005de5
192.168.1.72    192.168.1.78    1485        0x8000002d 0x00ab9e
192.168.1.28    192.168.1.78    1485        0x8000002e 0x006312
192.168.1.52    192.168.1.78    1485        0x8000002f 0x007ae0
192.168.1.44    192.168.1.78    1485        0x80000030 0x00bea4
192.168.30.0    192.168.1.78    1485        0x80000031 0x00521b
192.168.31.0    192.168.1.78    1485        0x80000032 0x004526
192.168.1.16    192.168.1.78    1476        0x80000033 0x00d1aa
192.168.1.4     192.168.1.78    1476        0x80000034 0x00483f
192.168.1.12    192.168.1.78    1476        0x80000035 0x00f588
192.168.1.20    192.168.1.78    1476        0x80000036 0x00a3d1
192.168.24.0    192.168.1.78    1476        0x80000037 0x0088e4
192.168.25.0    192.168.1.78    1476        0x80000038 0x007bef
192.168.26.0    192.168.1.78    1476        0x80000039 0x006efa
192.168.32.0    192.168.1.78    1456        0x8000003a 0x00342d
192.168.33.0    192.168.1.78    1456        0x8000003b 0x002738
192.168.22.0    192.168.1.78    1445        0x8000003c 0x0094d5
192.168.23.0    192.168.1.78    1445        0x8000003d 0x0087e0
192.168.21.0    192.168.1.78    1445        0x8000003e 0x009bcd
```

Figure 7: London OSPF routing table



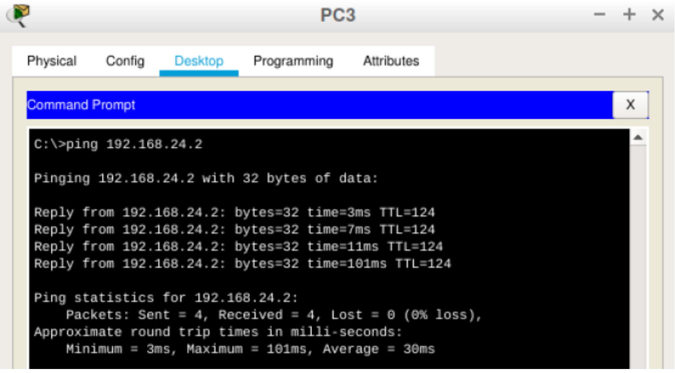
```
Router#show ip ospf database
            OSPF Router with ID (19.19.9.19) (Process ID 1)

                Router Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum Link count
19.19.9.19      19.19.9.19      1525        0x80000007 0x00d004 5
192.168.1.86    192.168.1.86    1527        0x80000006 0x005bea 3

                Summary Net Link States (Area 2)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.1.8     192.168.1.86    1502        0x8000001d 0x009b37
192.168.1.0     192.168.1.86    1502        0x8000001e 0x00e9ef
192.168.1.68    192.168.1.86    1502        0x8000001f 0x003d57
192.168.1.84    192.168.1.86    1502        0x80000020 0x009ae8
192.168.1.24    192.168.1.86    1502        0x80000021 0x007509
192.168.1.60    192.168.1.86    1502        0x80000022 0x000a4f
192.168.1.72    192.168.1.86    1502        0x80000023 0x008fbc
192.168.1.64    192.168.1.86    1502        0x80000024 0x00dd75
192.168.1.76    192.168.1.86    1502        0x80000025 0x0063e2
192.168.1.80    192.168.1.86    1502        0x80000026 0x003908
192.168.1.28    192.168.1.86    1502        0x80000027 0x004133
192.168.1.52    192.168.1.86    1502        0x80000028 0x005802
192.168.1.16    192.168.1.86    1502        0x80000029 0x00b5c8
192.168.1.4     192.168.1.86    1502        0x8000002a 0x002c5d
192.168.1.36    192.168.1.86    1502        0x8000002b 0x00e87f
192.168.28.0    192.168.1.86    1502        0x8000002c 0x00422a
192.168.1.44    192.168.1.86    1502        0x8000002d 0x0094c9
192.168.29.0    192.168.1.86    1502        0x8000002e 0x003336
192.168.30.0    192.168.1.86    1502        0x8000002f 0x002641
192.168.31.0    192.168.1.86    1502        0x80000030 0x00194c
192.168.32.0    192.168.1.86    1481        0x80000031 0x00164c
192.168.33.0    192.168.1.86    1481        0x80000032 0x000957
192.168.22.0    192.168.1.86    1473        0x80000033 0x0076f4
192.168.23.0    192.168.1.86    1473        0x80000034 0x0069ff
192.168.21.0    192.168.1.86    1473        0x80000035 0x007dec
```

Figure 8: Mumbai OSPF routing table

To show OSPF working and being table to deliver packets as expectedly we’re considering two scenarios:

1. Pinging from PC3 from VLAN10 in Boston to 192.168.24.2 in VLAN10 in Mumbai office.
2. Pinging from PC3 from VLAN18 in London to 192.168.21.6 in VLAN30 in Boston.

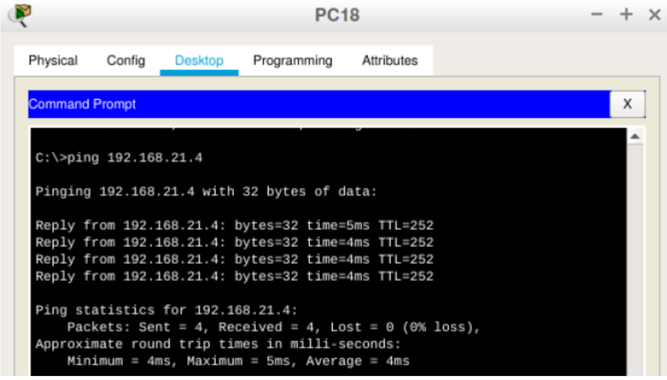
Case 1: Succeeded, we're able to ping!



```
C:\>ping 192.168.24.2

Pinging 192.168.24.2 with 32 bytes of data:

Reply from 192.168.24.2: bytes=32 time=3ms TTL=124
Reply from 192.168.24.2: bytes=32 time=7ms TTL=124
Reply from 192.168.24.2: bytes=32 time=11ms TTL=124
Reply from 192.168.24.2: bytes=32 time=101ms TTL=124

Ping statistics for 192.168.24.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 101ms, Average = 30ms
```

Figure 10: Ping Success

Case 2: Succeeded, we're able to ping!



```
C:\>ping 192.168.21.4

Pinging 192.168.21.4 with 32 bytes of data:

Reply from 192.168.21.4: bytes=32 time=5ms TTL=252
Reply from 192.168.21.4: bytes=32 time=4ms TTL=252
Reply from 192.168.21.4: bytes=32 time=4ms TTL=252
Reply from 192.168.21.4: bytes=32 time=4ms TTL=252

Ping statistics for 192.168.21.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5ms, Average = 4ms
```

Figure 11: Ping Success

Hence, we can conclude that our OSPF is working properly.

4.3 Redundancy Testing

4.3.1 Router Redundancy

For routing redundancy we're using HSRP protocol, Hot Standby Router Protocol allows for multiple router to form a congregation for fault tolerance. The group of routers would have a virtual IP address and if a link of a router goes down another would take over.

We're using HSRP in Mumbai and Boston offices.

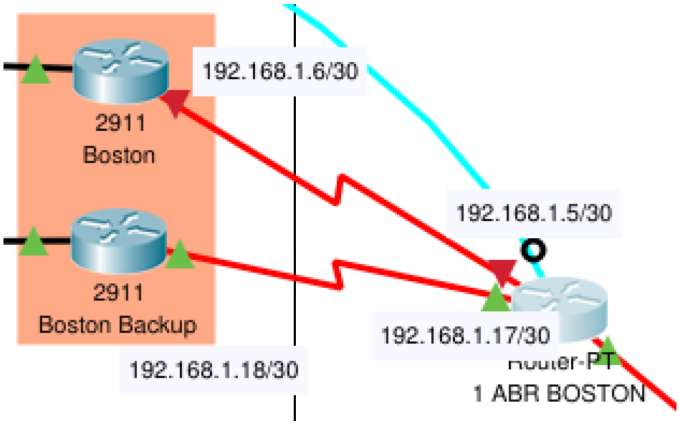


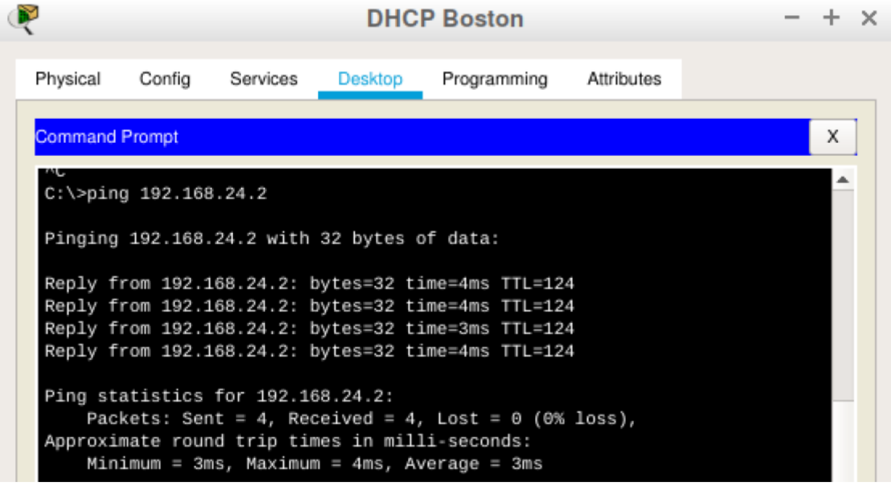
Figure 12: Boston's HSRP

To test the HSRP working correctly we'll take down the link from the active router and then try to access the outside network from one of the devices in the network. As we can see from the picture only 'Boston Backup' has an active connection.

Opening up the cli on the Boston Backup Router, we get the following message

```
%HSRP-6-STATECHANGE: GigabitEthernet0/0.10 Grp 1 state Standby -> Active

%HSRP-6-STATECHANGE: GigabitEthernet0/0.20 Grp 1 state Standby -> Active

%HSRP-6-STATECHANGE: GigabitEthernet0/0.30 Grp 1 state Standby -> Active
```

Which means the state of the Backup router changed to Active.



```
^C
C:\>ping 192.168.24.2

Pinging 192.168.24.2 with 32 bytes of data:

Reply from 192.168.24.2: bytes=32 time=4ms TTL=124
Reply from 192.168.24.2: bytes=32 time=4ms TTL=124
Reply from 192.168.24.2: bytes=32 time=3ms TTL=124
Reply from 192.168.24.2: bytes=32 time=4ms TTL=124

Ping statistics for 192.168.24.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

Figure 13: HSRP Success

So, we can see that we're still able to ping outside the network hence out HSRP is working.

4.3.1 Switch Redundancy

Switch Redundancy here refers to each switch in our office access to other switches via multiple paths so if one of the paths goes down it still has 1 or more path to choose from.

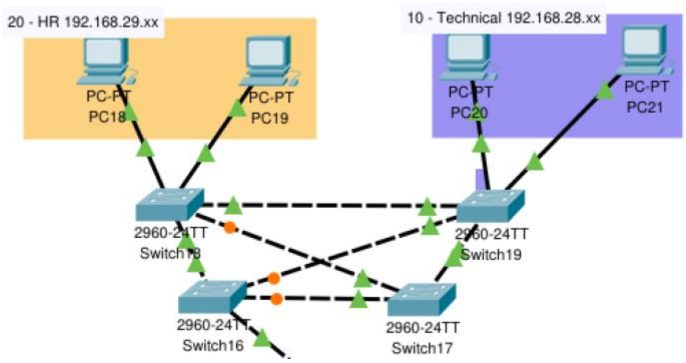


Figure 14: Switch Redundancy

The picture shows the switch redundancy in its original form. Now let's get rid of one of the connections and see if the devices can still connect to its router.

As we can see now that we've deleted one of the links. Now let's ping to the network router.

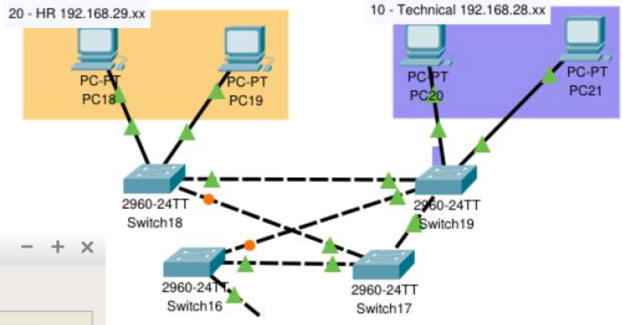
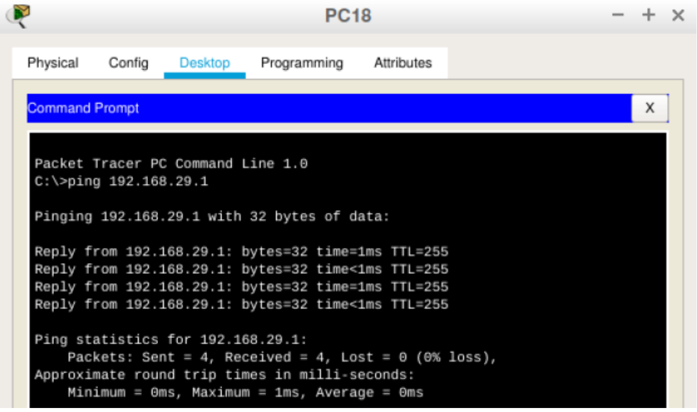


Figure 15: Switch Redundancy

As we can see, the PC18 is still able to ping to its routers sub-interface. we can conclude that Switch Redundancy is working in our network.



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.29.1

Pinging 192.168.29.1 with 32 bytes of data:

Reply from 192.168.29.1: bytes=32 time=1ms TTL=255
Reply from 192.168.29.1: bytes=32 time<1ms TTL=255
Reply from 192.168.29.1: bytes=32 time=1ms TTL=255
Reply from 192.168.29.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.29.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

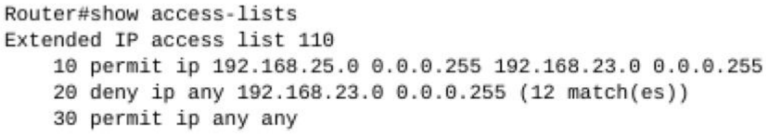
Figure 16: Ping with Switch Redundancy

4.4 Access Control Testing

4.4.1 Access Control on Finance Department

We were required to place a set of restrictions in the Finance Department. That is to block access to Finance Department from all other departments but both Finance Departments should be able to access each other.

Here's how the access List in Boston look

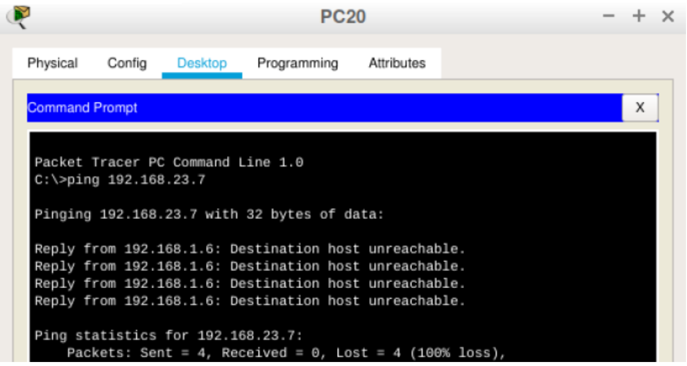


```
Router#show access-lists
Extended IP access list 110
    10 permit ip 192.168.25.0 0.0.0.255 192.168.23.0 0.0.0.255
    20 deny ip any 192.168.23.0 0.0.0.255 (12 match(es))
    30 permit ip any any
```

Figure 18: Boston's Access Lists

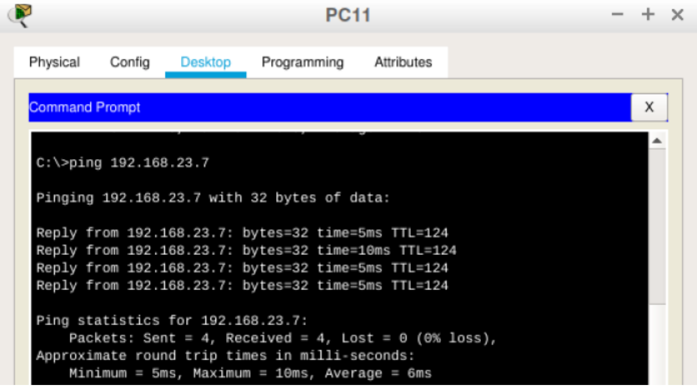
When I try to ping from the Mumbai's finance department, this is what we get

Figure 17: Ping from Finance



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.23.7

Pinging 192.168.23.7 with 32 bytes of data:

Reply from 192.168.1.6: Destination host unreachable.
Reply from 192.168.1.6: Destination host unreachable.
Reply from 192.168.1.6: Destination host unreachable.
Reply from 192.168.1.6: Destination host unreachable.

Ping statistics for 192.168.23.7:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

and then when I try to ping from any other department this is what we get

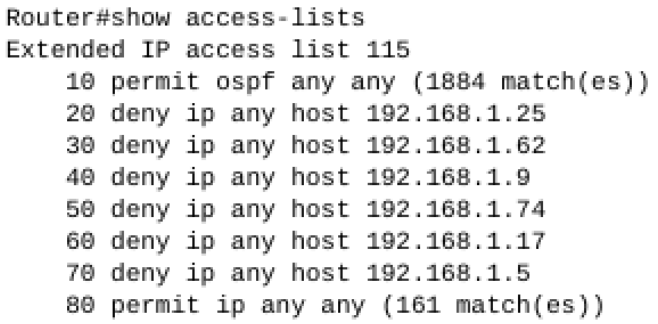


```
C:\>ping 192.168.23.7

Pinging 192.168.23.7 with 32 bytes of data:

Reply from 192.168.23.7: bytes=32 time=5ms TTL=124
Reply from 192.168.23.7: bytes=32 time=10ms TTL=124
Reply from 192.168.23.7: bytes=32 time=5ms TTL=124
Reply from 192.168.23.7: bytes=32 time=5ms TTL=124

Ping statistics for 192.168.23.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 10ms, Average = 6ms
```

Figure 19: Ping from somewhere else

4.4.2 Access Control on Boston's ABSR

To block access to Boston's ABSR I added an access list which blocks all the incoming traffic which has a destination address of one of the ABSRs sub-interfaces



```
Router#show access-lists
Extended IP access list 115
    10 permit ospf any any (1884 match(es))
    20 deny ip any host 192.168.1.25
    30 deny ip any host 192.168.1.62
    40 deny ip any host 192.168.1.9
    50 deny ip any host 192.168.1.74
    60 deny ip any host 192.168.1.17
    70 deny ip any host 192.168.1.5
    80 permit ip any any (161 match(es))
```

And to allow access from Boston's Technical department added a hardware connection to the router through the console cable.

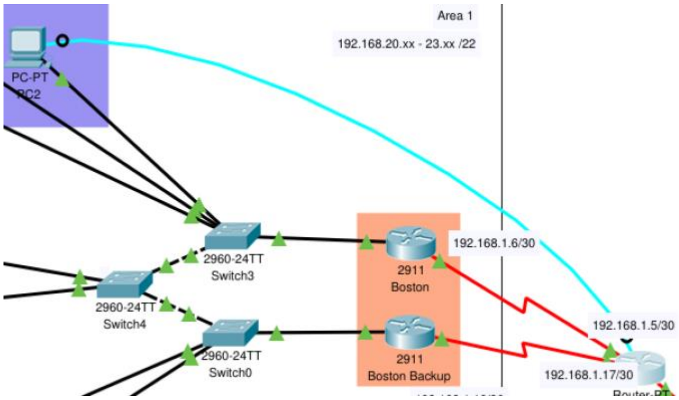
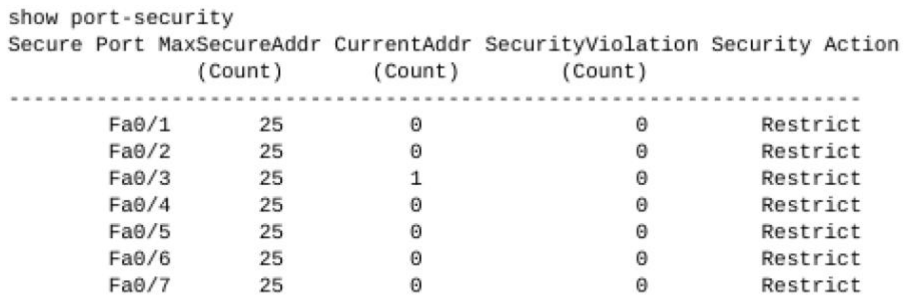


Figure 20: Access Control on Boston ABR

4.5 Mac Flooding Testing

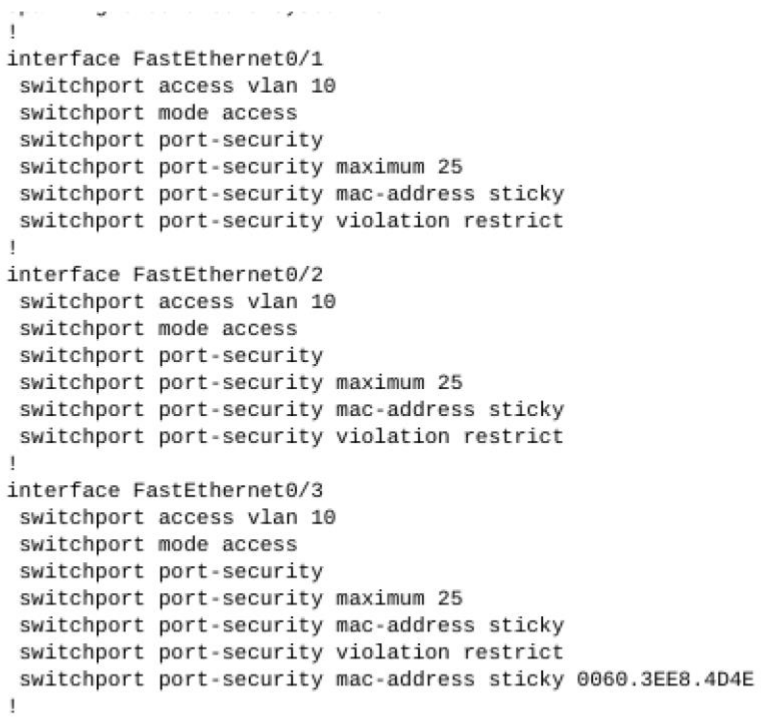
To Defend against MAC Flooding, I used port security measures provided by Cisco.

Where maximum Mac addresses that are allowed are set to 25 and Mac sticky is enabled for the port-security feature to update dynamically.



```
show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
        Fa0/1       25          0                 0         Restrict
        Fa0/2       25          0                 0         Restrict
        Fa0/3       25          1                 0         Restrict
        Fa0/4       25          0                 0         Restrict
        Fa0/5       25          0                 0         Restrict
        Fa0/6       25          0                 0         Restrict
        Fa0/7       25          0                 0         Restrict
```

Figure 21: Port Security List

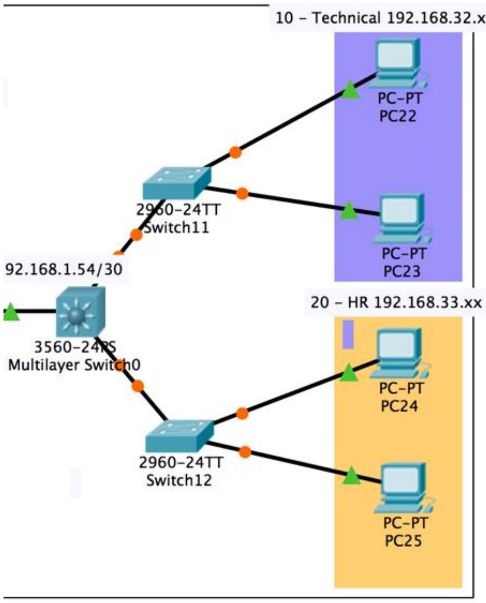


```
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 25
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 25
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 25
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0060.3EE8.4D4E
!
```

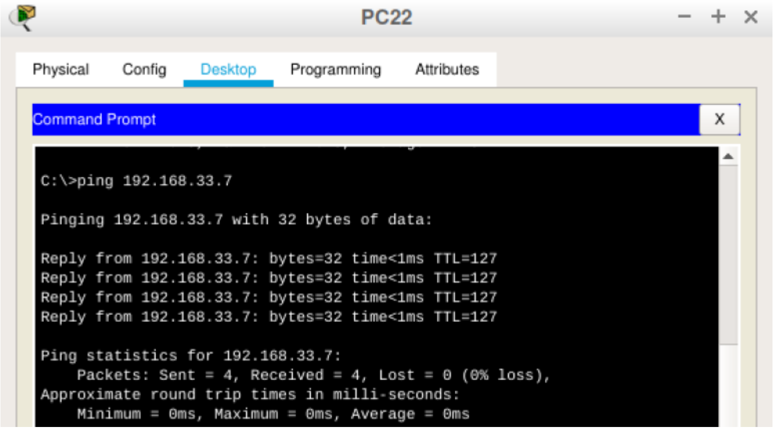
Figure 22: Port Security Settings

4.5 Addons

4.5.1 Inter-VLAN routing via Layer 3 Switch



Pinging from Technical to HR



```
C:\>ping 192.168.33.7

Pinging 192.168.33.7 with 32 bytes of data:

Reply from 192.168.33.7: bytes=32 time<1ms TTL=127
Reply from 192.168.33.7: bytes=32 time<1ms TTL=127
Reply from 192.168.33.7: bytes=32 time<1ms TTL=127
Reply from 192.168.33.7: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.33.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

We’re able to pin, hence we can conclude the inter-VLAN routing is working.

5. CONCEPTS LEARNING DURING THE PROJECT

- **Routing Concepts**

Distance Vector Protocols: These are the protocols which only store information from their immediate neighbors. Ex: RIP

Link-State Protocols: These are the protocols which construct a map of the given network and uses that to calculate the shortest possible path.

OSPF: OSPF is usually referred to as a Link-State Protocol but it is a hybrid between the two, because OSPF uses distance vector protocol to route between the two areas. OSPF also include a concept of areas which is usually used to create more efficient routing in a network.

Frame-Relay: Frame-Relay is a cost-efficient data transmission system between WAN and LAN. Frame-Relay puts data in a Frame and leaves any error data correction to the endpoints, which helps speed up the data transmission rates.

- **Subnetting**

Subnetting refers to the practice of dividing up a network into two or more smaller networks. It’s usually done to increase efficiency(for example by wasting less IP addresses) and decreases the size of the broadcast domain.

- **Access Control**

Access Control refers to denying or permitting a certain set of people from accessing something on a network. Access Control is an integral part of an organizations network because often there exists situations where you don’t want a certain department to access another.

- **Redundancy Requirements**

In an organizational network, some integral networking gear going down can have catastrophic results. Which is why redundancy is the really important.

HSRP: HSRP protocol allows for two or more routers to be grouped together to provide a failover, a redundant router.

Switch Redundancy: Like Router redundancy, a switch redundancy can be provided with simply connecting a switch to multiple other switches, which will further connect to a router. Providing multiple links to a switch to access the outside network from in case one of them fail.

- **Security Requirements**

  Security Requirements refer to the cyber security part of the network design process. It's an important requirement for an organizational network usually. The common practices involve disabling access to the edge and border routers for most and limit to only certain devices inside the network. Another common practice is to limit the maximum number of mac addresses on a switched network, which helps avoid mac flooding attacks.

- **Networking Addons**

  VLANs: VLANs are virtual networks created within a network. Most switches and routers offer a service to create VLANs, VLANs can work as independent networks like normal LANs but can be created virtually i.e. the devices do not need to be connected directly to each other.

  EtherChannel: EtherChannel refers to combining one or more ports/links on a switch or a router and make them act like a single connection. This is usually done to increase the bandwidth of the link.

  STP: STP refers to the spanning tree protocol, a protocol which helps avoids loops in a network and stopping the packets from looping in the network, saving resources.

  DHCP: DHCP is a protocol which can dynamically assign IP addresses to a bunch of end devices.

6. CONCLUSION

To conclude, I simulated an organizational network in this project which used plenty of real-world applications, protocols and methodologies. I ended up learning and using protocols like OSPF, Frame-Relay, STP, etc. to simulate this network.

I also learned and understood the importance of redundancy of various kinds network equipment in a network, especially in an organization. I also understood why network security is another thing to take care of while designing a network, because the internet in itself wasn't designed to be a secure way of communicating, we need to add and implement security protocols as we desire.

In the end, I created a realistic organizational network with a realistic budget.

REFERENCES

[1]. Costing reference of all the network Equipment. www.router-switch.com/.

[2]. RFC 3509. Section 1.2. https://tools.ietf.org/search/rfc3509#section-1.2

[3] Keith Ward. May 4th, 2019. RIP up your dynamic routing with OSPF.

[4]. Charlie Schluting. Aug 14th, 2007. Networking 101: Understanding Spanning Tree.