High level Network Topology: -   
A computer screen shot of a computer

Description automatically generated

Network Optimization: - IP Subnetting

Boston

Differentiating Vlan so assign virtual ip address.

vlan 10 192.168.0.30

Vlan 20 192.168.0.62

Vlan 30 192.168.0.94

Vlan 10 - HR 192.168.0.2 - HR 192.168.0.30 255.255.255.224

DG - HR 192.168.0.1

NA - 192.168.0.0

BA - 192.168.0.31

Vlan 20 - Tech 192.168.0.35 - 192.168.0.63 255.255.255.224

DG - 192.168.0.33

NA - 192.168.0.32

BA - 192.168.0.64

DHCP static IP - 192.168.0.34

Vlan 30 - Finance 192.168.0.66 - 192.168.0.95 255.255.255.224

DG - 192.168.0.65

NA - 192.168.0.64

BA - 192.168.0.96

Mumbai

Differentiating Vlan so assign virtual ip address

vlan 40 192.168.1.30

Vlan 50 192.168.1.62

Vlan 60 192.168.1.94

Vlan 40 - HR 192.168.1.2 - HR 192.168.1.30 255.255.255.224

DG - 192.168.1.1

NA - 192.168.1.0

BA - 192.168.1.31

Vlan 50 - Tech 192.168.1.35 - 192.168.1.63 255.255.255.224

DG - 192.168.1.33

NA - 192.168.1.32

BA - 192.168.1.64

DHCP static IP - 192.168.1.34

Vlan 60 - Finance 192.168.1.66 - 192.168.1.95 255.255.255.224

DG - 192.168.1.65

NA - 192.168.1.64

BA - 192.168.1.96

London

Vlan 10 - HR 192.168.2.2 - HR 192.168.2.30 255.255.255.224

DG - 192.168.2.1

NA - 192.168.2.0

BA - 192.168.2.31

Vlan 20 - Tech 192.168.2.35 - 192.168.2.63 255.255.255.224

DG - 192.168.2.33

NA - 192.168.2.32

BA - 192.168.2.64

DHCP static IP - 192.168.2.34

New York

Vlan 10 - HR 192.168.3.2 - HR 192.168.3.30 255.255.255.224

DG - 192.168.3.1

NA - 192.168.3.0

BA - 192.168.3.31

Vlan 20 - Tech 192.168.3.35 - 192.168.3.63 255.255.255.224

DG - 192.168.3.33

NA - 192.168.3.32

BA - 192.168.3.64

DHCP static IP - 192.168.3.34

Germany

Vlan 10 - HR 192.168.4.2 - HR 192.168.4.30 255.255.255.224

DG - 192.168.4.1

NA - 192.168.4.0

BA - 192.168.4.31

Vlan 20 - Tech 192.168.4.35 - 192.168.4.63 255.255.255.224

DG - 192.168.4.33

NA - 192.168.4.32

BA - 192.168.4.64

DHCP static IP - 192.168.4.34

VPN tunneling

192.168.6.0/27

192.168.6.4 - Boston side

192.168.6.6 - Mumbai side

4 PC's

1 DHCP server

1 2960-24 TT switch

BUDGET:

7 - ISR 4321 Router + 1 - 2901 Router = 7 x 3300+ 870 = 23970

2 - Multilayer switch + 9 - 2960 switch = 2 x 1500+ 9 x 1500 = 16500

24 - PC 24 x 1000 = 24000

5 - Server = 5 x 2000 = 10000

Total Cost 74,470

**TAKEAWAY QUESTIONS:  
1)**  
A scalable link-state routing system called OSPF (Open Shortest Path First) uses Dijkstra's algorithm and a cost metric depending on link bandwidth to determine the shortest paths. It facilitates effective address usage by supporting classless routing with VLSM and CIDR. OSPF is a hierarchical design that optimizes routing by connecting all areas to a backbone (Area 0). Areas can be NSSA (allowing limited external routes), regular, stubby (limiting external routes), or completely stubby (blocking external and inter-area routes). OSPF routers can be classified as ASBRs (connected to external networks), ABRs (connecting multiple areas), or internal (single area).

Link-State Advertisements (LSAs), such as Type 1 (router), Type 2 (network), Type 3 (inter-area), Type 4 (ASBR summary), Type 5 (external), and Type 7 (NSSA), are used to transmit routing information. Point-to-point, broadcast, and non-broadcast networks are among the network types that OSPF supports. In multi-access networks, DRs and BDRs are used to reduce overhead. By using states like Down, Init, 2-Way, **ExStart**, Exchange, Loading, and Full, it creates neighbor relationships and guarantees synchronized link-state databases.

The cost can be modified for faster networks by dividing the reference bandwidth (by default 100 Mbps) by the link bandwidth. OSPF offers scalability, load balancing over equal-cost pathways, secure updates with authentication, quick convergence, and effective resource usage through multicast updates. It is perfect for big, intricate networks because of these capabilities.

2)   
Because of its features, scalability, and efficiency, OSPF is superior to RIP for contemporary networks. OSPF allows vast networks with no hop limit, hierarchical design, and precise cost-based metrics, whereas RIP is only allowed to make 15 hops and use a basic hop count measure. Whereas RIP depends on slower periodic updates, OSPF uses event-driven updates to converge more quickly and reduce traffic. OSPF is better suited for complicated, secure applications because it provides enhanced security through authentication. OSPF is the recommended option for medium-to-large, scalable networks, while RIP is simpler to set up and appropriate for smaller networks.  
  
3)   
In large networks, OSPF's area concept enhances scalability, efficiency, and stability. By summarizing routes, it minimizes costs by limiting LSA propagation, isolates topology changes to avoid network-wide disruptions, and reduces the size of routing tables. Areas facilitate logical network design, optimize resource utilization, and guarantee effective routing through the backbone area (Area 0). OSPF can effectively manage complicated networks thanks to this topology.  
  
4)   
To centralize routing, guarantee effective route exchange, and facilitate scalability in big networks, OSPF's Area 0 is set up as the backbone. It enables the sharing of routing information across areas and connects all other areas, either directly or via virtual links. This centralized topology enforces inter-area communication through the backbone, reducing the complexity of routing tables and preventing routing loops. Additionally, by summarizing routing data prior to its transmission across areas, Area 0 optimizes network efficiency and enables OSPF to scale. The OSPF protocol definition mandates the backbone design in order to guarantee uniformity and interoperability among various network devices. All things considered, Area 0 is the essential component of OSPF's hierarchical structure, offering a reliable, well-structured, and effective routing framework for big and complicated networks.  
  
5)   
**Different types of messages exchanged in OSPF:**

1. **Hello Packet** - Routers utilize this communication to learn about one another and establish a connection. It assists routers in determining which other routers are in the vicinity and prepared to provide routing data.
2. **Database Description packet** - This is how routers exchange summaries of their routing data. Without relaying all the information, it informs nearby routers of what they know about the network.
3. **Link-State Request (LSR) packet** - A router sends this request to request the precise data it requires from a neighbor if it detects that it is lacking some information.
4. **Link-State Update (LSU) packet** - The actual routing information is contained in this message. To maintain synchronization, routers communicate updated routing information after receiving a request.
5. **Link-State Acknowledgement packet (LSAck)** - A router replies with this message to verify that it has successfully received the updated data (LSU).

6)   
Security Plan:

1) Inter-Departmental Access Control:

- Finance department is isolated from all the other departments, but it can access the Technical, HR and Finance departments in the same location and other locations.

- Other departments have restricted access to finance department but they can access and talk with each other.

2) VLAN Implementation:

- Network segmentation using VLANs improves security by separating departmental traffic.

- Trunk ports only permit essential VLANs, minimizing possible attack surfaces.

3) SSH Configuration:

- SSH is set up on all network routers for remote management, which increases security compared to less secure protocols like Telnet. You can use "admin" as the username and "pass@123" as the password to do so.

4) Port Security

- All host-connected ports have BPDU guard turned on to stop unwanted switches from joining the network.

5) VPN Tunnel

- The Boston and Mumbai headquarters are connected via a VPN tunnel, guaranteeing safe communication between these vital locations.

6) MAC Flooding Defense

- At the Boston facility, precautions are taken to guard against MAC flooding assaults, shielding the network from this frequent security risk.

Redundancy Plan:

1) HSRP Implementation

- For the Boston and Mumbai offices, Hot Standby Router Protocol (HSRP) is set up to provide router redundancy.

- For quicker failover, the hello timer is set to 2 seconds and held at 6 seconds.

2) Rapid Spanning Tree Protocol (RSTP)

- In order to provide rapid convergence in the event of link outages, RSTP is implemented for the offices in Germany, London, and New York.

3) Switch Redundancy

- To remove single points of failure, redundant switches are installed in offices in Germany, London, and New York.

4) Multiple OSPF Areas   
 - Because the network is separated into several OSPF regions, it is more stable and the effects of failures in one area on the network are lessened.  
 - Area 1 – Boston, Area 2 – Mumbai, Area 3 – London, Area 4 – New York, Area 5 – Germany, Area 0 – Backbone (Core)

7)   
By guaranteeing that there is only one active link between switches and maintaining backup paths for dependability, the Spanning Tree Protocol (STP) helps networks avoid loops. The Root Bridge, which serves as the network's hub, is chosen first by STP. The best (cheapest) path to the Root Bridge is then determined by each switch, and the port that offers it is designated as the Root Port. The designated port is the port that routes traffic to every network segment. To prevent loops, any redundant paths are blocked; however, in the event that an active path fails, STP recalculates and activates a blocked path to keep the network stable and loop-free. In the event of a failure, this procedure enables network redundancy and recovery.  
  
8)   
STP: Since STP builds a single spanning tree for the network as a whole, all VLANs use the same path for data forwarding. Because it doesn't offer precise control over the traffic in each VLAN, it is less effective but simpler in networks with several VLANs.

PVSTP: By creating a distinct spanning tree for every VLAN, PVSTP gives each VLAN greater control and makes better use of its network paths. However, it is more sophisticated than STP and uses more resources because each VLAN requires its own tree.

MSTP: By grouping VLANs into fewer spanning tree instances, MSTP enhances scalability and efficiency. It is perfect for big networks since it requires fewer spanning trees than PVSTP, but it is more difficult to set up and maintain.

TEST PLAN: -   
  
Test Vlan: -   
This is for Boston Location similarly can be done for other locations as well.  
1) show vlan brief – to check for vlan ids, names and ports associated with each vlan configured.

A screenshot of a computer

Description automatically generated

2) show interfaces trunk – run this command on the switch to get information if the trunk ports are properly configured or not.  
A screenshot of a computer

Description automatically generated  
  
3) ping one pc from vlan 10 to vlan 20 to check inter-vlan routing:   
 Here I am pinging a PC in the Technical department from the HR department   
 A screenshot of a computer

Description automatically generated

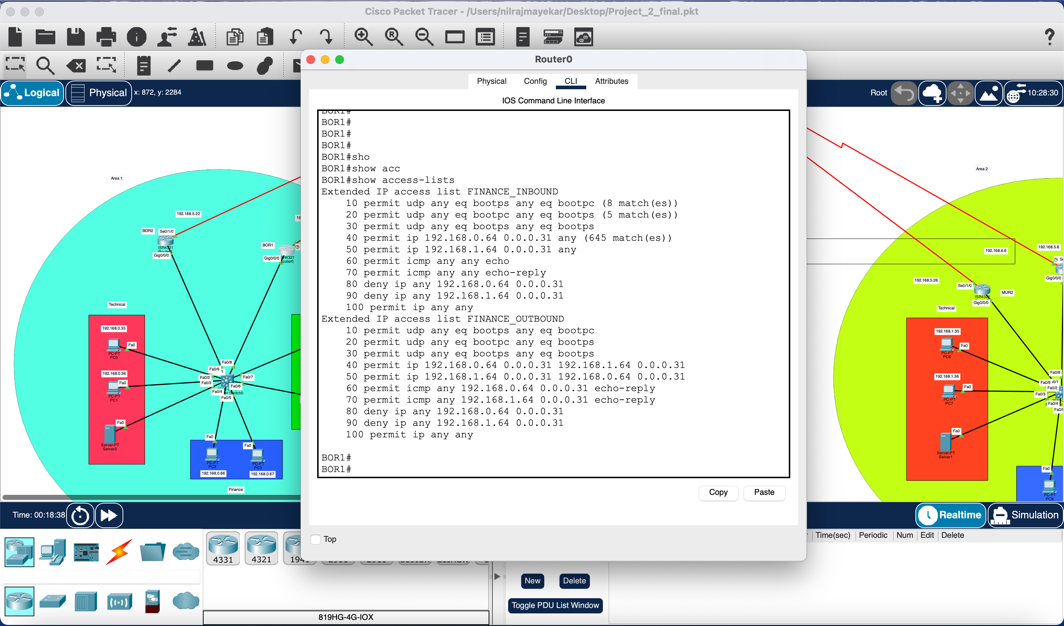
Test Routing protocol: -   
1) show ip ospf – to verify correct area assignments for each interface.  
Here I am sharing for Boston which is my Area 1 and has router id 1.1.1.1  
A screenshot of a computer

Description automatically generated  
  
2) show ip ospf neighbor – to confirm neighbor relationships are established.  
You can see that the routers participating are neither DR or BDR  
A screenshot of a computer

Description automatically generated

3) ping a computer from one ospf location to another to show case OSPF routing  
I am pinging a PC in HR department in London from Technical department in Boston  
A screenshot of a computer

Description automatically generated

Test Security Plan: -  
1) For the ACL implemented: -   
- show access-lists (To see the configured ACL’s on the router), below is for Boston, we have implemented on Boston and Mumbai main and back routers. Similarly we can see configurations for other routers as well.  


- ping a PC in Finance department from tech department it should restrict the access as below  
A screenshot of a computer

Description automatically generated

- ping a PC from Finance to Tech department it should be accessible  
A computer screen shot of a computer

Description automatically generated

- ping a PC from Tech to HR it should be accessible  
A screenshot of a computer

Description automatically generated

2) BPDU guard on ports  
- show spanning-tree summary will show on which interfaces the Bpdu guard is enabled  
A screenshot of a computer

Description automatically generated

Test Redundancy Plan: -   
1) Test Rapid STP and swith redundancy: -   
- First disable on of the interfaces here I have disabled for London location Fa0/3 and the interface Fa0/4 should be enabled as below

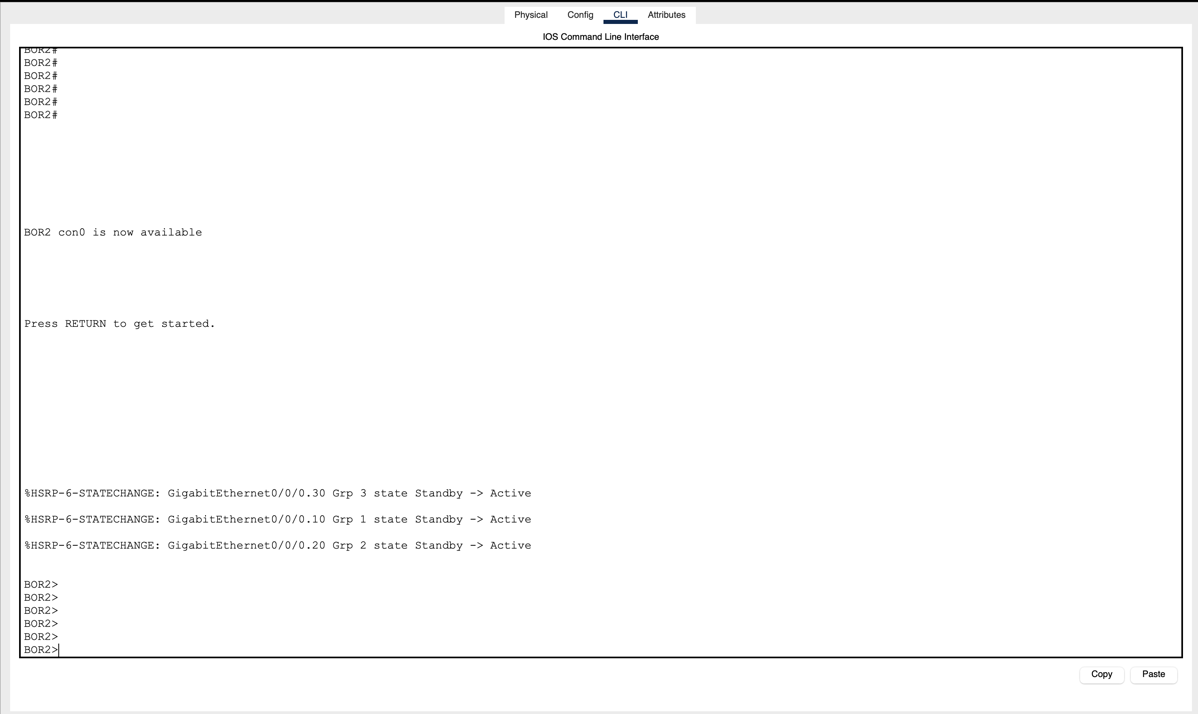
A screenshot of a computer

Description automatically generated  
  
- ping PC from Tech to HR it should work  
A screenshot of a computer

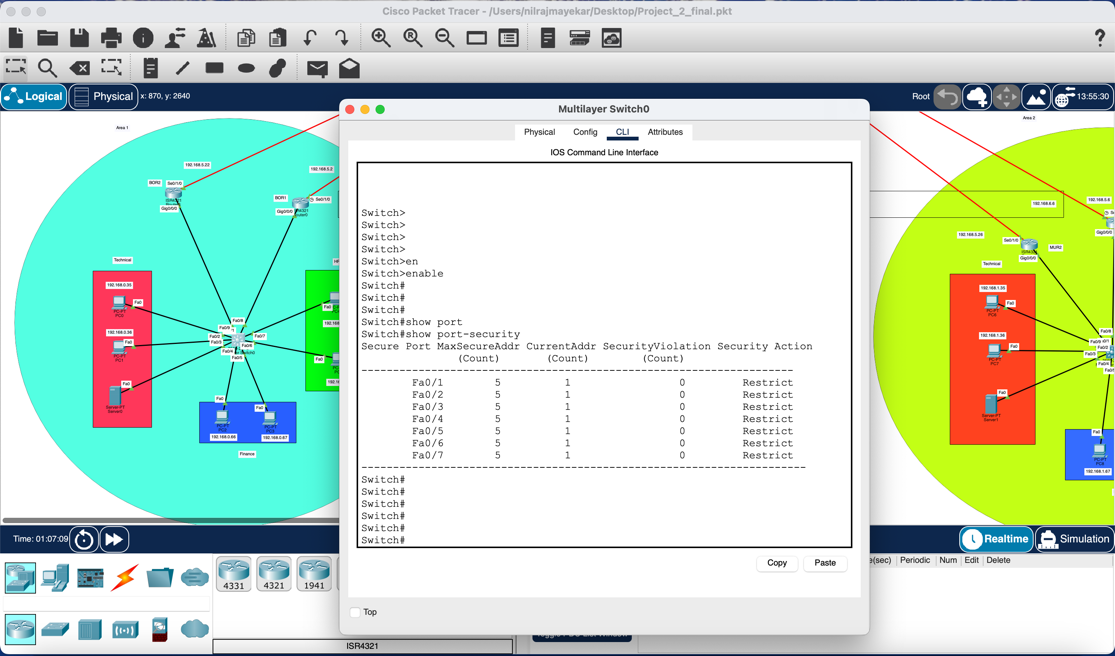
Description automatically generated

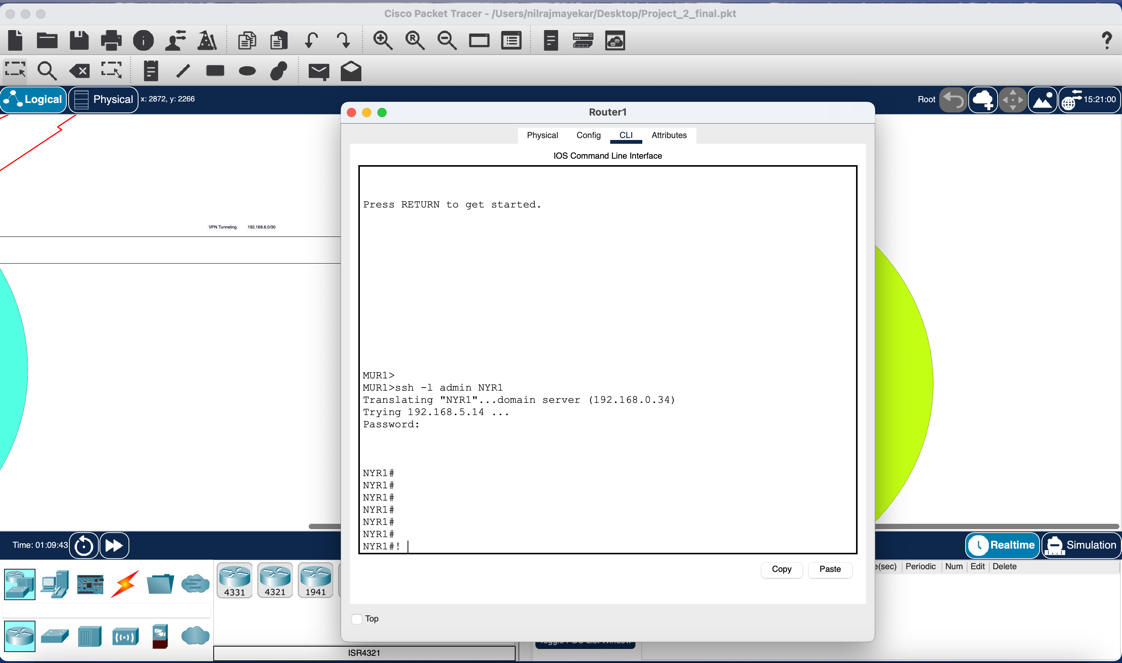
- show spanning tree should show the spanning-tree topology  
A screenshot of a computer

Description automatically generated

Test HSRP: -   
- Put the main router interface down that should make the backup router go active which is BOR2  


- Ping from one PC to another PC to check if working  
A screenshot of a computer

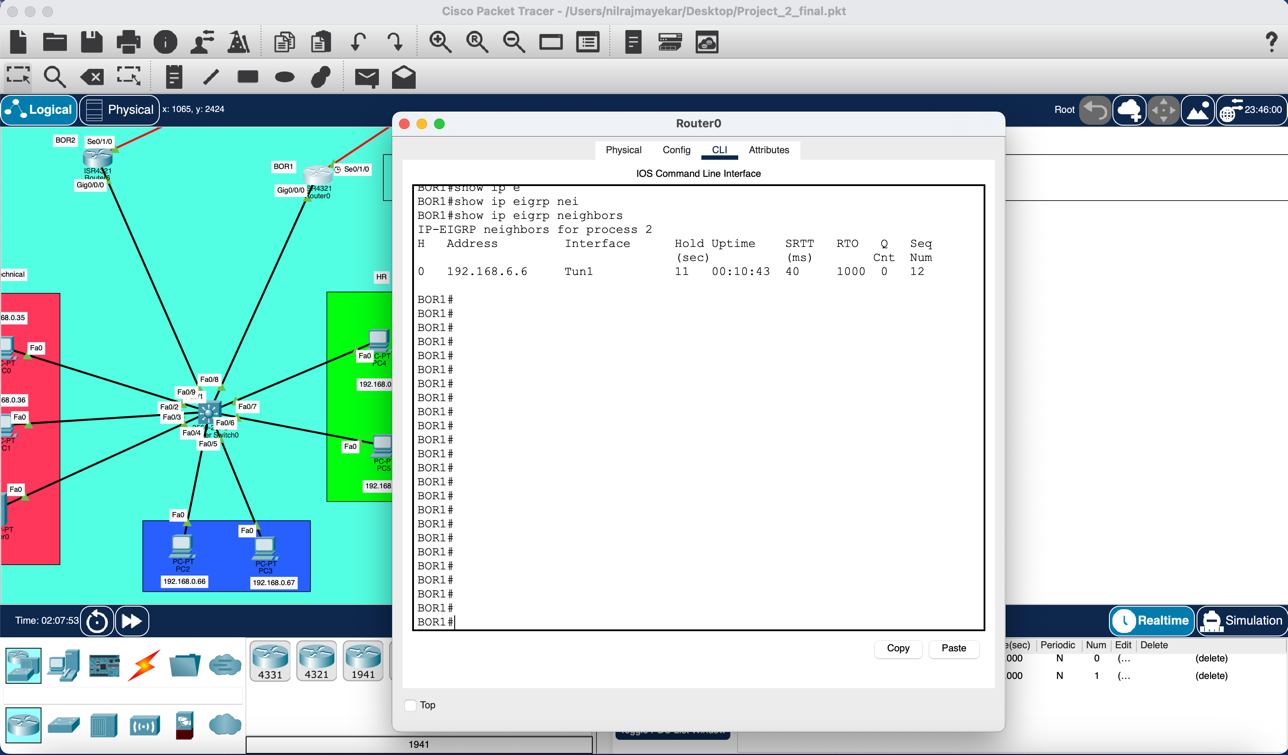
Description automatically generated  
  
  
  
Test Mac flooding attack: -   
- show port-security will show the port security configurations done on the switch  


Test SSH configuration: -   
- Run the command ssh -l admin NYR1 on Mumbai main router MUR1, should be able to successfully ssh into the NYR1 router after entering the password “pass@123”  


Test VPN tunneling: -  
- Configured a VPN tunneling between Mumbai and Boston, so with Boston end Ip address being 192.168.6.4 and the Mumbai side Ip address being 192.168.6.6, to test we can ping from Boston to Mumbai from the end devices to the end ip and the result should be as below  
A screenshot of a computer

Description automatically generated

Test EIGRP: -   
- show ip protocol command to check if eigrp is configured or not  
A screenshot of a computer

Description automatically generated  
  
- show ip eigrp neighbors – will show neighbors configured here I am showing for Boston main router.  


CONCEPTS LEARNED: -

1) Sub netting of IP addresses.   
2) Area concept of OSPF.  
3) Spanning Tree protocol (STP)  
4) Rapid Spanning Tree protocol (RSTP)  
5) Hot standby routing protocol (HSRP)  
6) Defending mac flooding attack.  
7) Enabling SSH into routers for remote management.  
8) VPN tunneling  
9) IP assignment through DHCP server.

CONCLUSION: -

For this project, a small firm with offices in Boston, Mumbai, New York, London, and Germany needed a multi-location network designed and put into place. The network architecture called for setting up VLANs for department segregation, implementing OSPF routing with various areas, and subnetting the 192.168.0.0/16 address space to offer 50 usable IPs per office. Setting up DHCP and DNS servers, installing security mechanisms like HSRP and Rapid STP, and isolating the Finance department while granting it access to other departments were among the essential requirements. The project includes extra responsibilities including setting up VPN tunnels and protecting against MAC flooding assaults, with a focus on network optimization and redundancy. I acquired useful skills in network design, IP addressing, routing protocols, security implementation, and troubleshooting from this practical experience. The project reaffirmed the significance of methodical planning, striking a balance between functionality and security, and developing scalable network solutions. It also emphasized how important thorough testing and documentation are when implementing networks. All things considered, this project prepared me for upcoming difficulties in network administration and design by giving me a useful chance to apply theoretical networking principles to a simulated real-world setting.