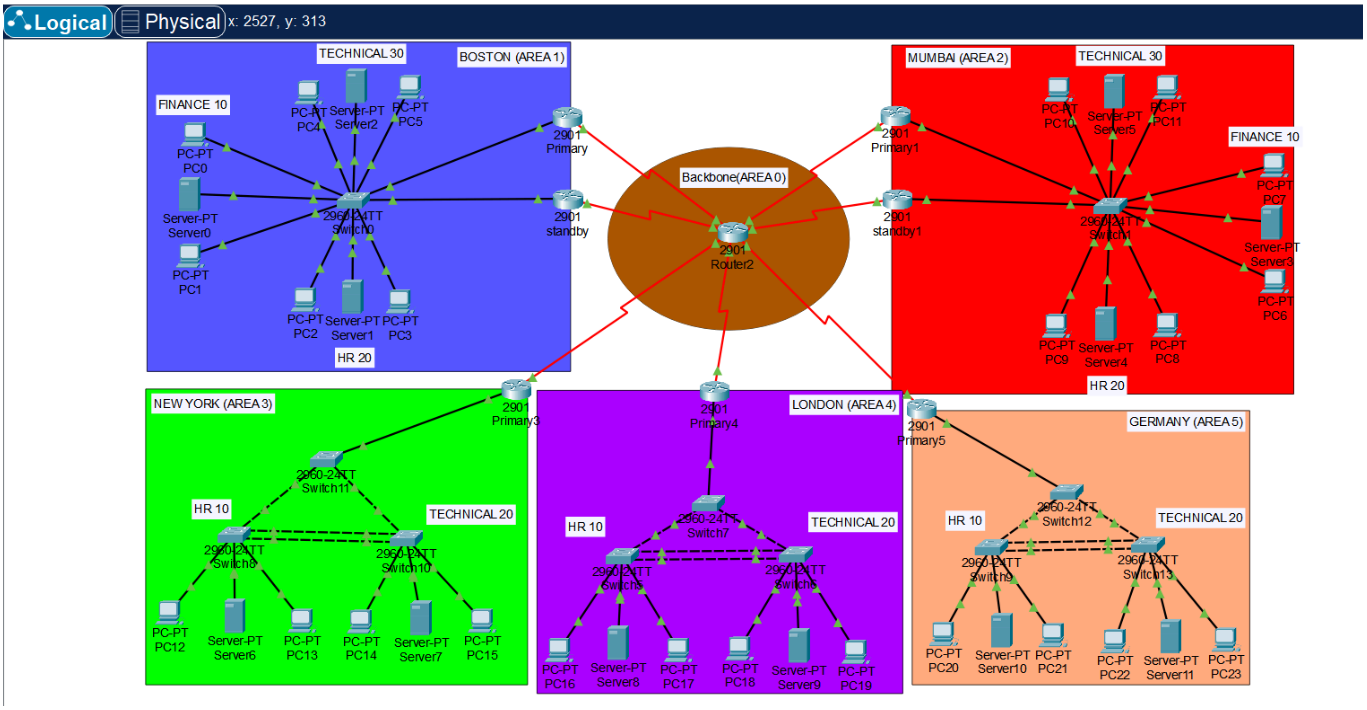


INTRODUCTION:

This project aims to design and implement a secure and efficient enterprise network for an organization with offices spread across multiple geographic locations. The network incorporates key functionalities such as routing, switching, security protocols, and redundancy to ensure reliable communication, high availability, and strong security across all departments and sites.

The organization operates from five locations: Boston, Mumbai, New York, London, and Germany. Each office has distinct departmental needs, including Finance, Technical, and HR. The primary objective is to create a scalable network infrastructure that facilitates seamless inter-office and intra-department communication while enforcing stringent security measures to safeguard sensitive data and prevent unauthorized access.

Hierarchical Structure:

- **Core Layer**: Handles WAN connections and inter-office routing.
- **Distribution Layer**: Includes switches for inter-VLAN routing and redundancy.
- **Access Layer**: Contains switches managing end-user devices.

Design Overview:

- The network employs a partial mesh topology for inter-office communication, ensuring redundancy and efficient routing paths.
- Each office has distinct VLANs segregated for Finance, HR, and Technical departments.
- Dynamic routing protocols (OSPF and EIGRP) ensure scalability and fast convergence.
- HSRP provides high availability for critical devices, with rapid failover configurations.

VLAN TABLE:

LOCATION	DEPARTMENT	VLAN	IP ALLOCATION
BOSTON	FINANCE	10	192.168.1.0/28
	HR	20	192.168.1.16/28
	TECHNICAL	30	192.168.1.32/28
MUMBAI	FINANCE	10	192.168.2.0/28
	HR	20	192.168.2.16/28
	TECHNICAL	30	192.168.2.32/28
NEWYORK	HR	10	192.168.3.0/28
	TECHNICAL	20	192.168.3.16/28
LONDON	HR	10	192.168.4.0/28
	TECHNICAL	20	192.168.4.16/28
GERMANY	HR	10	192.168.5.0/28
	TECHNICAL	20	192.168.5.16/28

Cost of Network:

S.No	LIST OF NETWORK DEVICES	QUANTITY	COST PER 1 QTY	TOTAL COST
1.	CISCO ROUTER 2901	8	590$	4720$
2.	CISCO SWITCH 2960	11	150$	1650$
3.	DHCP SERVER	5	500$	2500$
4.	SERIAL DCE CABLE	-	3.5$ PER FEET	3.5$ (estimate)
5.	COPPER STRAIGHT THRU CABLE	-	0.6$ PER FEET	0.6$ (estimate)

6.	COPPER CROSSOVER CABLE	-	1.7$ PER FEET	1.7$ (estimate)
			TOTAL:	8875.8$

DHCP:

1. BOSTON:

CREATING A DHCP POOL:

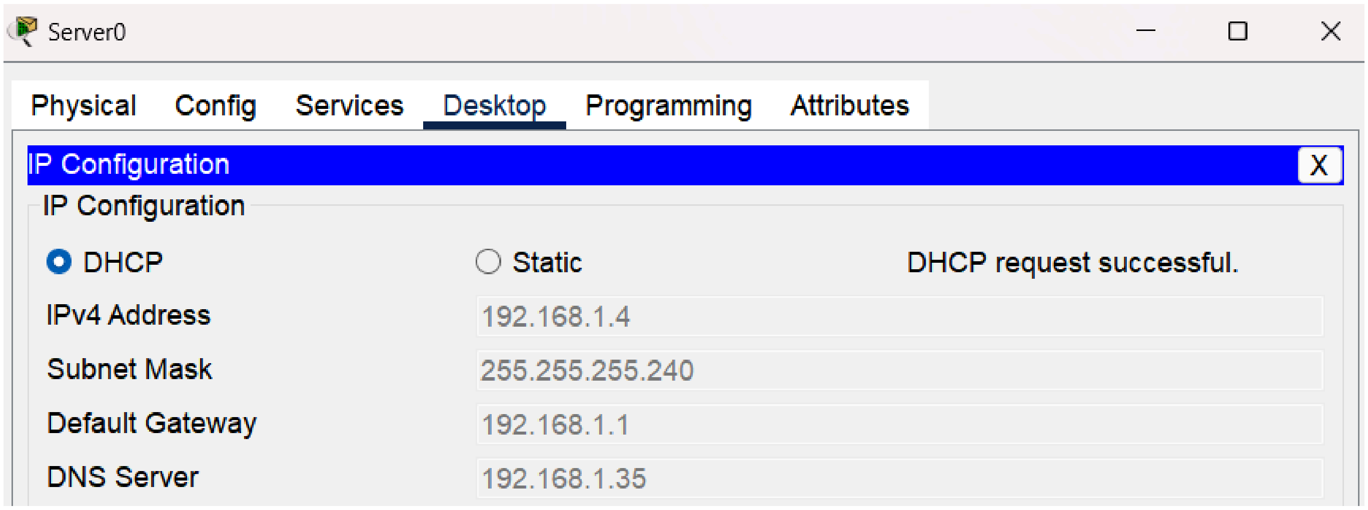
DHCP

Interface	FastEthernet0
Service	On (selected) / Off
Pool Name	serverPool
Default Gateway	192.168.1.1
DNS Server	192.168.1.35
Start IP Address :	192 . 168 . 1 . 2
Subnet Mask:	255 . 255 . 255 . 240
Maximum Number of Users :	10
TFTP Server:	0.0.0.0
WLC Address:	0.0.0.0

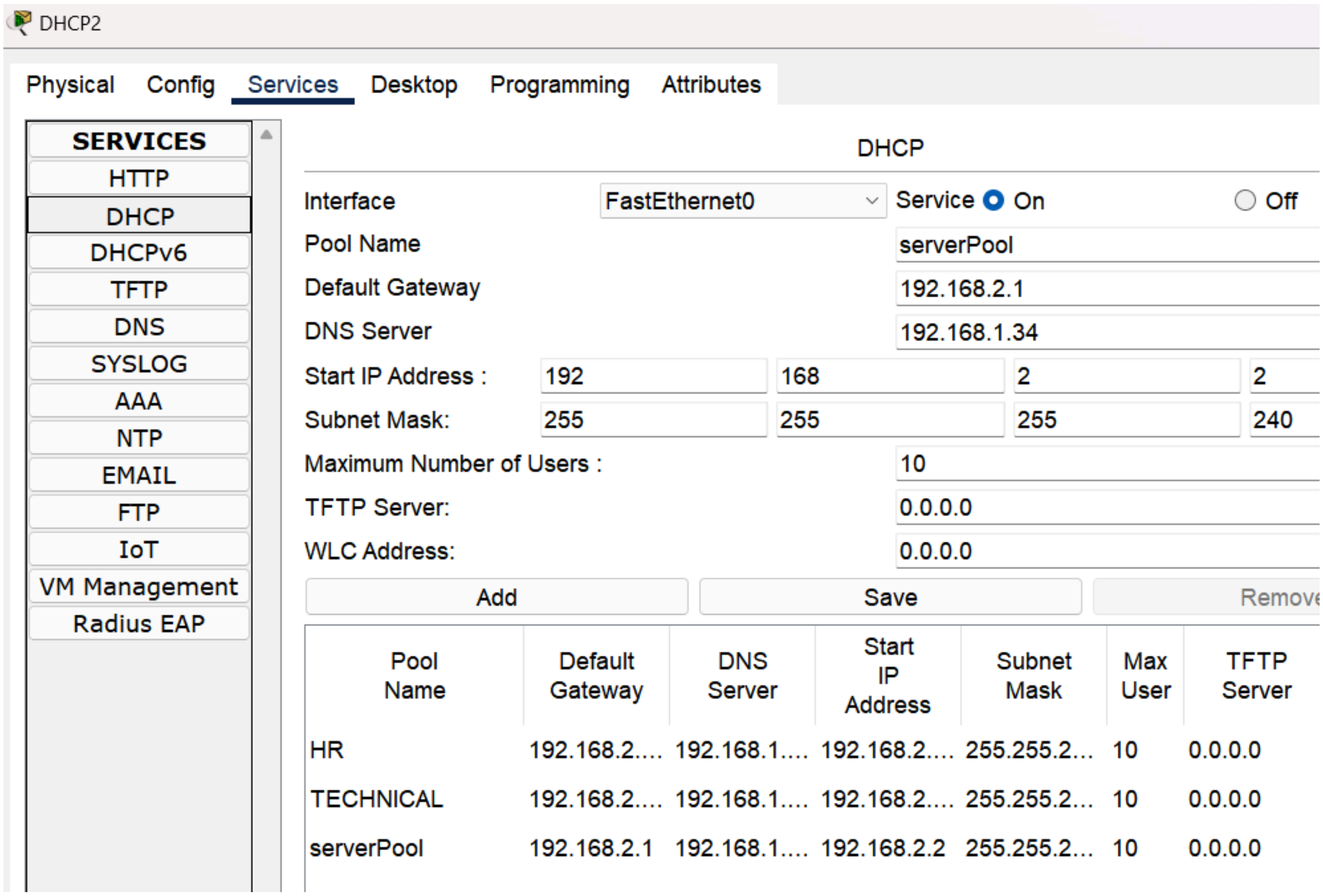
Add | Save | Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server
serverPool	192.168.1.1	192.168.1.35	192.168.1.2	255.255.25...	10	0.0.0.0
HR	192.168.1.17	192.168.1.35	192.168.1.18	255.255.25...	10	0.0.0.0
TECHNICAL	192.168.1.33	192.168.1.35	192.168.1.36	255.255.25...	10	0.0.0.0

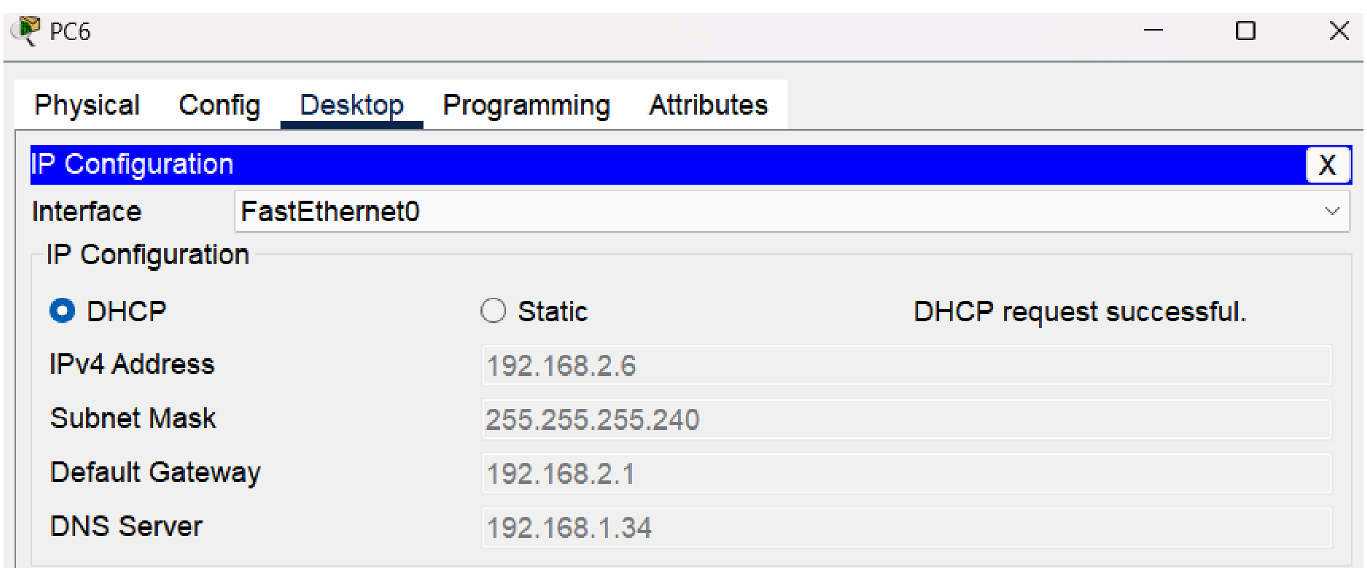
RESULT:


Server0
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
DHCP request successful.
IPv4 Address
192.168.1.4
Subnet Mask
255.255.255.240
Default Gateway
192.168.1.1
DNS Server
192.168.1.35

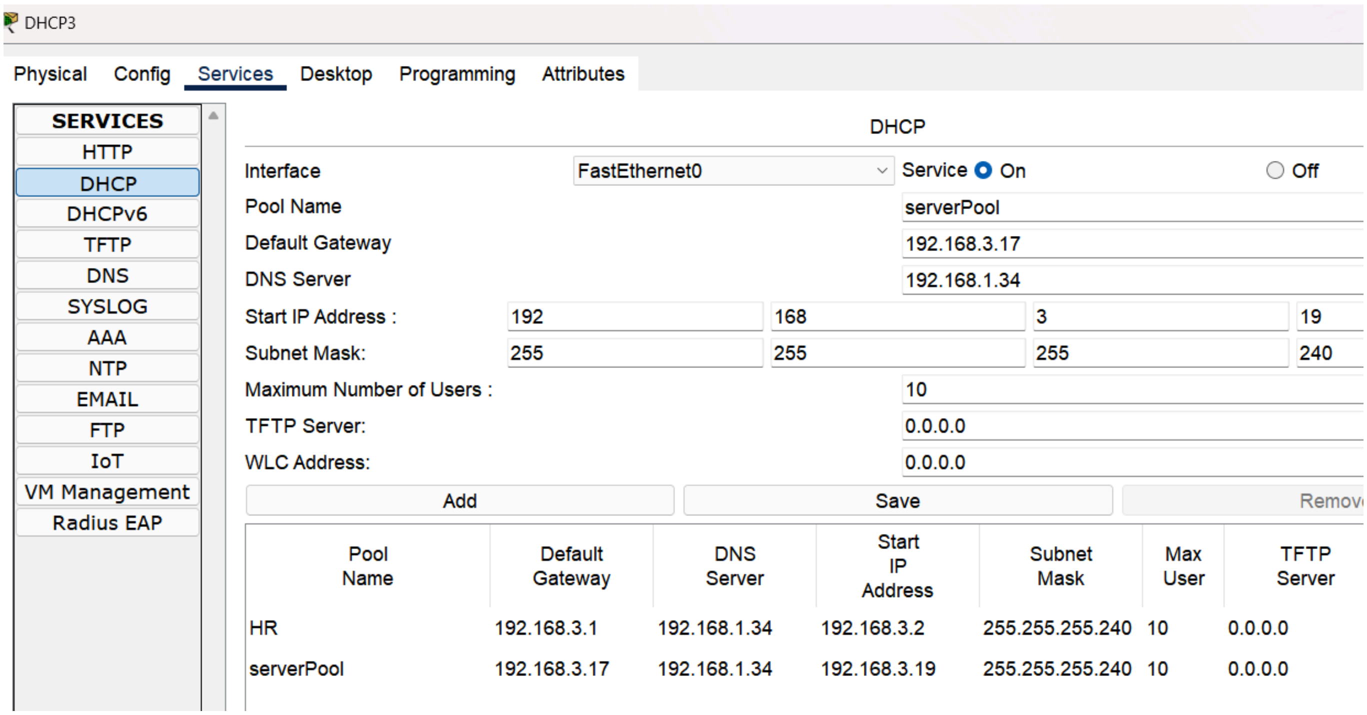
2. MUMBAI:


DHCP2
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
DHCP
Interface
FastEthernet0
Service
On
Off
Pool Name
serverPool
Default Gateway
192.168.2.1
DNS Server
192.168.1.34
Start IP Address :
192
168
2
2
Subnet Mask:
255
255
255
240
Maximum Number of Users :
10
TFTP Server:
0.0.0.0
WLC Address:
0.0.0.0
Add
Save
Remove
Pool Name
Default Gateway
DNS Server
Start IP Address
Subnet Mask
Max User
TFTP Server
HR
192.168.2....
192.168.1....
192.168.2....
255.255.2...
10
0.0.0.0
TECHNICAL
192.168.2....
192.168.1....
192.168.2....
255.255.2...
10
0.0.0.0
serverPool
192.168.2.1
192.168.1....
192.168.2.2
255.255.2...
10
0.0.0.0

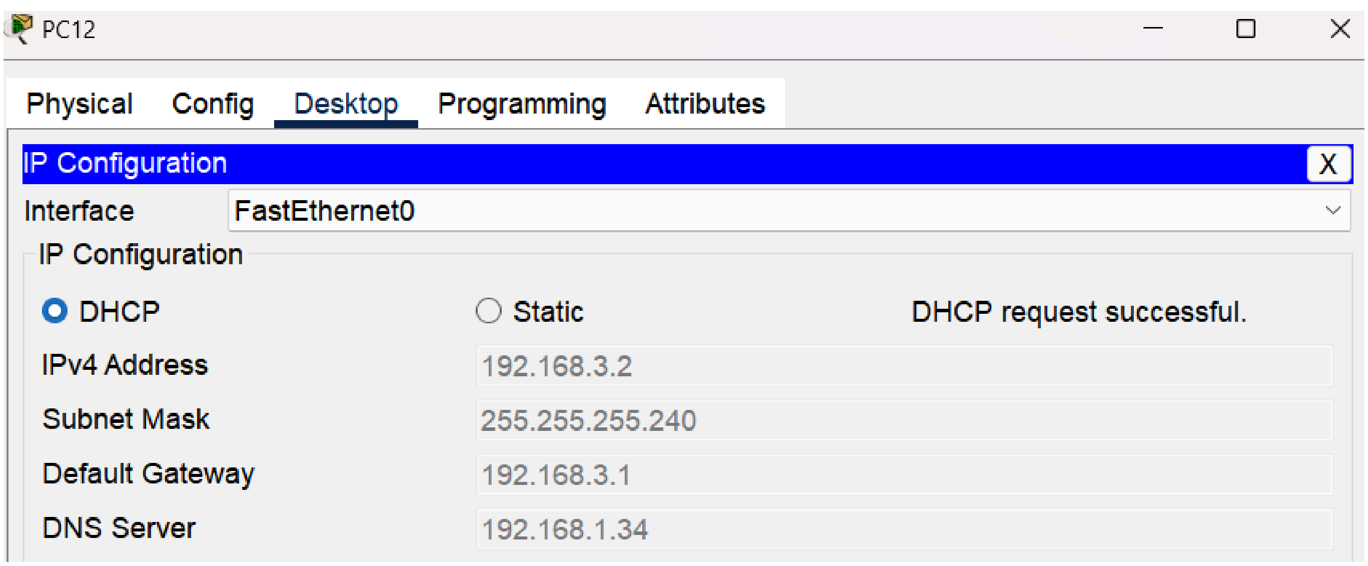
RESULT:


PC6
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
DHCP request successful.
IPv4 Address
192.168.2.6
Subnet Mask
255.255.255.240
Default Gateway
192.168.2.1
DNS Server
192.168.1.34

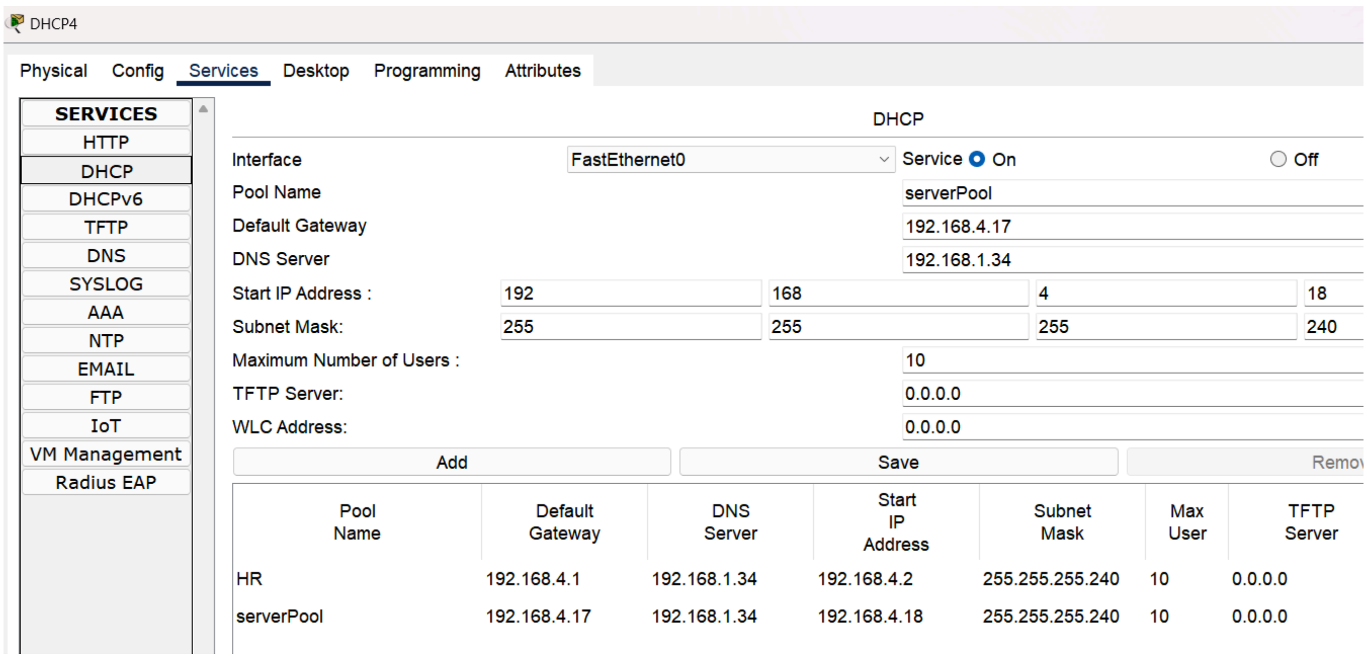
3. NEW YORK:



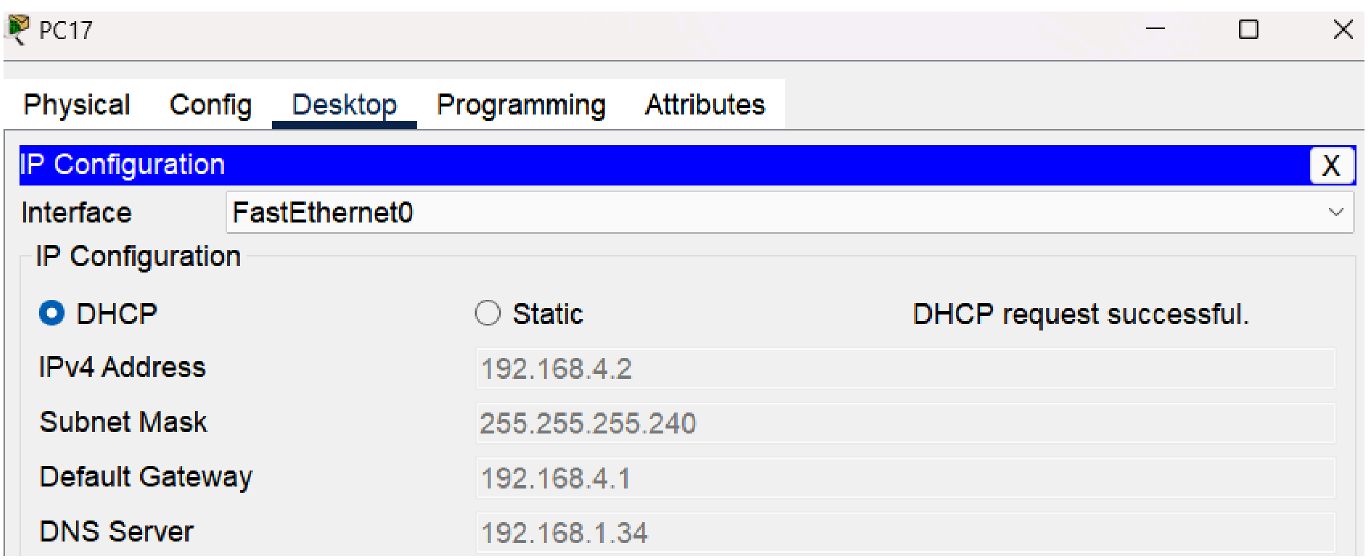
RESULT:



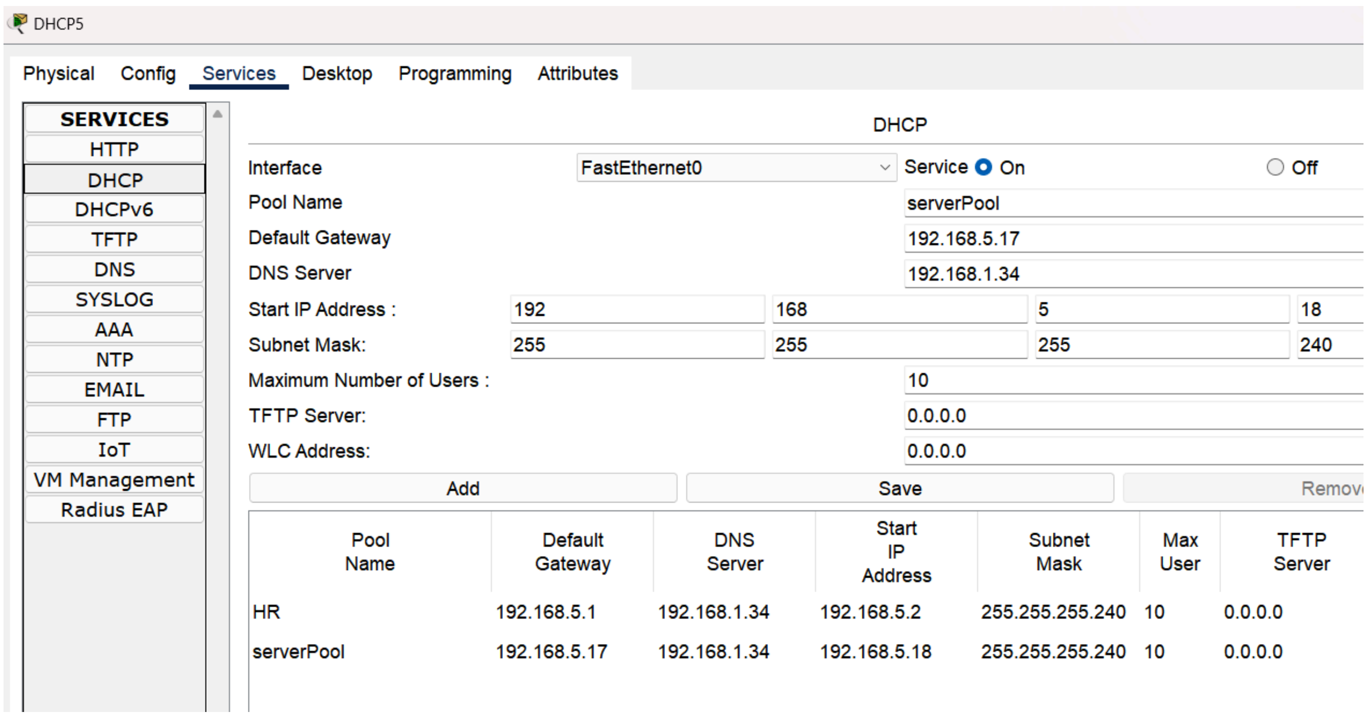
4. LONDON:



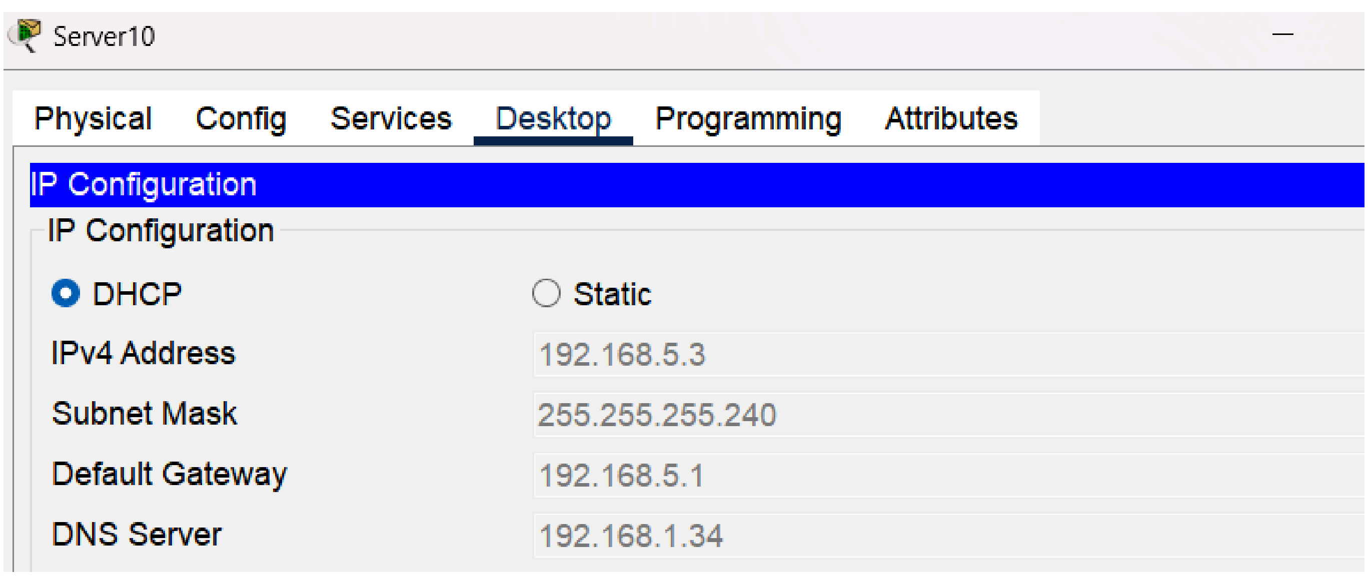
RESULT:



5. GERMANY:



RESULT:



DHCP (Dynamic Host Configuration Protocol):

- Purpose: DHCP servers were configured in each location to dynamically assign IP addresses to devices in their respective VLANs.
- How It Was Done:
  - A DHCP pool was created for each VLAN.
  - ip dhcp excluded-address was used to reserve static IPs for important devices (e.g., routers, servers).
  - Relay agents (ip helper-address) were configured on router subinterfaces to forward DHCP requests to the server.
- Verification:
  - Devices received IP addresses dynamically.
  - Used ‘show ip dhcp binding’ to verify assigned leases

OSPF (Open Shortest Path First):

- **Purpose**: OSPF was configured as the dynamic routing protocol to allow hierarchical interconnectivity between all routers across different locations.
- **How It Was Done**:
  - OSPF Areas were created (e.g., Area 1 for Boston, Area 2 for Mumbai).
  - Each router was assigned to its respective area.
  - The network command was used to advertise networks in OSPF.
  - A backbone (Area 0) was configured to interconnect all other areas.
- **Verification**:
  - Checked adjacency with the ‘show ip ospf neighbor’ command.
  - Routes were verified using ‘show ip route ospf.

OSPF:
AREA 1: (BOSTON-PRIMARY)

```
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.15 area 1
 network 192.168.1.16 0.0.0.15 area 1
 network 192.168.1.32 0.0.0.15 area 1
 network 192.168.6.0 0.0.0.3 area 0
```

AREA 1: (BOSTON-STANDBY)

```
router ospf 1
 router-id 1.1.1.2
 log-adjacency-changes
 network 192.168.1.0 0.0.0.15 area 1
 network 192.168.1.16 0.0.0.15 area 1
 network 192.168.1.32 0.0.0.15 area 1
 network 192.168.6.4 0.0.0.3 area 0
```

AREA 2: (MUMBAI-PRIMARY)

```
router ospf 1
 router-id 2.2.2.1
 log-adjacency-changes
 network 192.168.2.0 0.0.0.15 area 2
 network 192.168.2.16 0.0.0.15 area 2
 network 192.168.2.32 0.0.0.15 area 2
 network 192.168.6.8 0.0.0.3 area 0
```

AREA 2: (MUMBAI-STANDBY)

```
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 network 192.168.2.0 0.0.0.15 area 2
 network 192.168.2.16 0.0.0.15 area 2
 network 192.168.2.32 0.0.0.15 area 2
 network 192.168.6.12 0.0.0.3 area 0
```

AREA 3: (NEW YORK)

```
router ospf 1
 router-id 3.3.3.1
 log-adjacency-changes
 network 192.168.3.0 0.0.0.15 area 3
 network 192.168.3.16 0.0.0.15 area 3
 network 192.168.6.16 0.0.0.3 area 0
```

AREA 4: (LONDON)

```
router ospf 1
 router-id 4.4.4.1
 log-adjacency-changes
 network 192.168.4.0 0.0.0.15 area 4
 network 192.168.4.16 0.0.0.15 area 4
 network 192.168.6.20 0.0.0.3 area 0
```

AREA 5: (GERMANY)

```
router ospf 1
 router-id 5.5.5.1
 log-adjacency-changes
 network 192.168.5.0 0.0.0.15 area 5
 network 192.168.5.16 0.0.0.15 area 5
 network 192.168.6.24 0.0.0.3 area 0
```

AREA 0 : (BACKBONE)

```
router ospf 1
 router-id 0.0.0.1
 log-adjacency-changes
 network 192.168.6.0 0.0.0.3 area 0
 network 192.168.6.4 0.0.0.3 area 0
 network 192.168.6.8 0.0.0.3 area 0
 network 192.168.6.12 0.0.0.3 area 0
 network 192.168.6.16 0.0.0.3 area 0
 network 192.168.6.20 0.0.0.3 area 0
 network 192.168.6.24 0.0.0.3 area 0
```

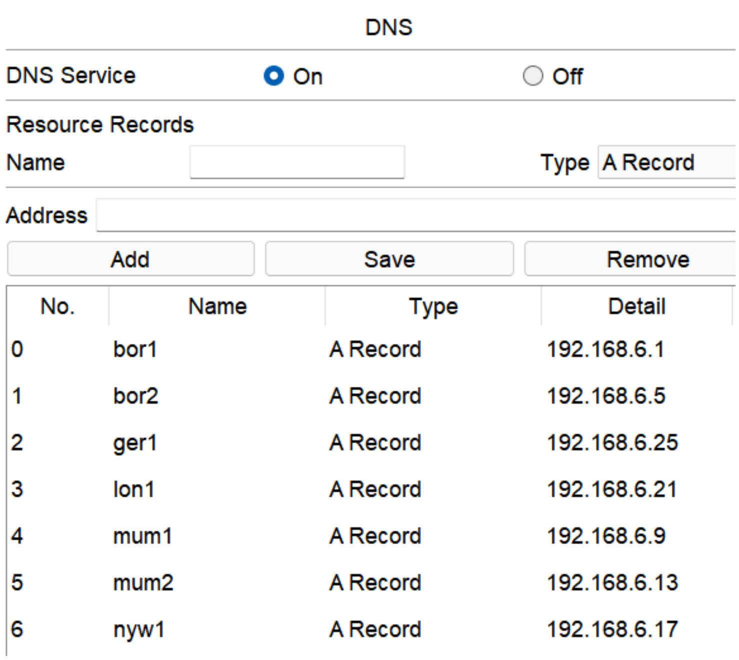
This routing table confirms that:

1. **All Subnets Are Advertised:**
   Networks like 192.168.1.0/28 (Boston) and 192.168.2.0/28 (Mumbai) are present, showing proper OSPF area connectivity.
2. **Inter-Area Communication is Enabled:**
   Routes marked as ‘IA’ confirm that inter-area routing is functioning, and ABRs are advertising routes between OSPF areas.

3. **Redundancy Through Multiple Paths:**
   Each subnet has multiple entries (via different next hops), showing the availability of redundant paths for improved reliability.

DNS (Domain Name System):

- **Purpose**: DNS allows devices to resolve hostnames to IP addresses for easier management and communication.
- **How It Was Done**:
  - A DNS server was configured with an entry for each router using their hostname and IP.
  - The ip name-server command was used to set the DNS server IP on all devices.
- **Verification**:
  - Hostnames were resolved to IPs using the ping hostname command.



No.	Name	Type	Detail
0	bor1	A Record	192.168.6.1
1	bor2	A Record	192.168.6.5
2	ger1	A Record	192.168.6.25
3	lon1	A Record	192.168.6.21
4	mum1	A Record	192.168.6.9
5	mum2	A Record	192.168.6.13
6	nyw1	A Record	192.168.6.17

Result:

```
C:\>ping ger1

Pinging 192.168.6.25 with 32 bytes of data:

Reply from 192.168.6.25: bytes=32 time=2ms TTL=253
Reply from 192.168.6.25: bytes=32 time=14ms TTL=253
Reply from 192.168.6.25: bytes=32 time=16ms TTL=253
Reply from 192.168.6.25: bytes=32 time=7ms TTL=253

Ping statistics for 192.168.6.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 16ms, Average = 9ms
```

EIGRP (Enhanced Interior Gateway Routing Protocol):

- **Purpose**: EIGRP was used between the Boston and Mumbai HQ routers as a secondary dynamic routing protocol.
- **How It Was Done**:
  - EIGRP was enabled with an Autonomous System (AS) number (router eigrp 100).
  - Network statements were added to advertise directly connected subnets and loopbacks.
  - Authentication was implemented to secure EIGRP messages.
- **Verification**:
  - Verified neighbors using show ip eigrp neighbors.
  - Checked advertised routes using ‘show ip eigrp topology’

Boston:

```
router eigrp 100
 eigrp router-id 1.1.1.1
 passive-interface GigabitEthernet0/0.10
 passive-interface GigabitEthernet0/0.20
 passive-interface GigabitEthernet0/0.30
 network 192.168.1.0 0.0.0.15
 network 10.10.10.0 0.0.0.3
 network 192.168.6.0 0.0.0.3
 network 192.168.0.1 0.0.0.0
interface Loopback0
 ip address 192.168.0.1 255.255.255.255
```

Mumbai:

```
router eigrp 100
 passive-interface GigabitEthernet0/0.10
 passive-interface GigabitEthernet0/0.20
 passive-interface GigabitEthernet0/0.30
 network 192.168.2.0 0.0.0.15
 network 192.168.6.0 0.0.0.15
 network 10.10.10.0 0.0.0.3
 network 192.168.0.2 0.0.0.0


interface Loopback0
 ip address 192.168.0.2 255.255.255.255
```

```
BOR1>en
BOR1#show ip eigrp topology
IP-EIGRP Topology Table for AS 100/ID(1.1.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.10.10.0/30, 1 successors, FD is 26880000
         via Connected, Tunnel0
P 192.168.0.1/32, 1 successors, FD is 128256
         via Connected, Loopback0
P 192.168.0.2/32, 1 successors, FD is 27008000
         via 10.10.10.2 (27008000/128256), Tunnel0
P 192.168.1.0/28, 1 successors, FD is 28160
         via Connected, GigabitEthernet0/0.10
P 192.168.2.0/28, 1 successors, FD is 26882560
         via 10.10.10.2 (26882560/28160), Tunnel0
P 192.168.6.0/24, 1 successors, FD is 2169856
         via Connected, Serial0/0/0
BOR1#
```

```
MUM1>en
MUM1#show ip eigrp topology
IP-EIGRP Topology Table for AS 100/ID(192.168.0.2)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.10.10.0/30, 1 successors, FD is 26880000
         via Connected, Tunnel0
P 192.168.0.1/32, 1 successors, FD is 27008000
         via 10.10.10.1 (27008000/128256), Tunnel0
P 192.168.0.2/32, 1 successors, FD is 128256
         via Connected, Loopback0
P 192.168.1.0/28, 1 successors, FD is 26882560
         via 10.10.10.1 (26882560/28160), Tunnel0
P 192.168.2.0/28, 1 successors, FD is 28160
         via Connected, GigabitEthernet0/0.10
P 192.168.6.0/24, 1 successors, FD is 2169856
         via Connected, Serial0/0/0
MUM1#
```

ACL:

The Access Control List (ACL) configuration is implemented to enforce the following security policies:

1. **Finance department isolation:** Prevent unauthorized access to the Finance VLAN from other departments.
2. **Finance department intercommunication:** Allow communication between Finance departments in Boston and Mumbai.
3. **Intra-department communication:** Permit communication between devices within the same department.
4. **Controlled external access:** Restrict or allow access to external networks based on specific rules.

ACL Design

1. Inbound ACLs

Inbound ACLs were applied to the interfaces connecting the Finance VLANs. These control incoming traffic to Finance VLANs to enforce the required policies.

- **Deny statements** block access from other departments (e.g., New York, London, Germany) to the Boston Finance VLAN (192.168.1.0/28).
- **Permit statements** allow intercommunication between Boston Finance and Mumbai Finance VLANs.
- **Default deny** ensures no other traffic is allowed to reach the Boston Finance VLAN.
- **Final permit** is included to allow other non-finance-related traffic.

2. Outbound ACLs

Outbound ACLs manage traffic leaving the Finance VLANs to ensure Finance devices can access other departments or external networks as needed.

- **Permit statements** allow Mumbai Finance VLAN (192.168.2.0/28) to communicate with Boston Finance and any other destinations.

Implementation Steps

1. **Apply the Inbound ACL:**
   - Applied to the interface receiving traffic destined for the Finance VLAN.
2. **Apply the Outbound ACL:**
   - Applied to the interface handling traffic leaving the Finance VLAN.

Verification:

1. **show access-lists:**
   - Used to monitor hit counts and verify if the ACL is being applied correctly.
2. **show ip interface:**
   - Confirmed the correct application of ACLs on the respective interfaces.

```
BOR1#show access-lists
Extended IP access list FINANCE_INBOUND
    10 deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.15
    20 deny ip 192.168.4.0 0.0.0.255 192.168.1.0 0.0.0.15
    30 deny ip 192.168.5.0 0.0.0.255 192.168.1.0 0.0.0.15
    40 permit ip 192.168.2.0 0.0.0.15 192.168.1.0 0.0.0.15
    50 permit ip 192.168.1.0 0.0.0.15 any (866 match(es))
    60 deny ip any 192.168.1.0 0.0.0.15
    70 permit ip any any (7 match(es))
Extended IP access list FINANCE_OUTBOUND
    10 permit ip 192.168.1.0 0.0.0.15 any
    20 permit ip 192.168.2.0 0.0.0.15 any (17 match(es))
```

1. **PortFast Configuration:**
    - PortFast was enabled on all access ports connected to host devices.
    - This feature allows ports to bypass the spanning-tree states (Listening and Learning) and transition directly to the Forwarding state, reducing the time required for host devices to connect to the network.
      spanning-tree portfast
2. **BPDU Guard Configuration:**
    - BPDU Guard was enabled on the same ports to protect the network from receiving Bridge Protocol Data Units (BPDUs) from host devices.
    - If a BPDU is received on a PortFast-enabled port, the port is automatically disabled, preventing rogue switches or misconfigured devices from causing loops or network instability.
      spanning-tree bpduguard enable
3. **Applied on Access Ports:**
    - The configurations were implemented on all access ports connected to end-user devices across all switches in the network.

Verification:

- The command **show running-config** was used to verify the configuration of PortFast and BPDU Guard on the designated ports.

Outcome:

- **Rapid Connectivity:** Host devices were able to connect to the network immediately after powering on, reducing downtime and improving user experience.

- **Improved Security:** The network was protected from rogue switches and misconfigurations, ensuring stability and preventing Layer 2 loops.
- **Optimized Performance:** With PortFast and BPDU Guard enabled, the network achieved faster and more secure host connectivity, aligning with the project's goal of creating a robust and efficient enterprise network.

```
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 3
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0010.1103.3369
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 3
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0030.F24D.36C6
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 3
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0090.21DA.D09E
 spanning-tree portfast
 spanning-tree bpduguard enable
```

TAKEAWAY QUESTIONS:

1. Open Shortest Path First (OSPF) is a robust and widely used link-state routing protocol designed for large, scalable networks. It creates a comprehensive topology map by exchanging Link State Advertisements (LSAs) among routers and computes the shortest paths using Dijkstra's algorithm. OSPF operates within areas, which reduces the complexity of route management and isolates changes to specific sections of the network. Supporting features like equal-cost load balancing, authentication, and route summarization make OSPF highly efficient. Unlike distance-vector protocols, OSPF converges quickly and provides precise control over routing metrics. Its hierarchical structure minimizes routing overhead, making it ideal for enterprise-level deployments.
2. OSPF is considered better than RIP for modern networks due to its scalability, efficiency, and advanced features. While RIP uses hop count as its sole metric with a maximum limit of 15 hops, OSPF considers bandwidth, ensuring better path selection. OSPF also converges significantly faster than RIP, making it more suitable for large and dynamic environments. RIP's frequent updates can lead to high bandwidth usage, while OSPF's event-triggered updates are more resource-efficient. Additionally, OSPF supports large

networks with hierarchical area designs, while RIP lacks such segmentation. For enterprises requiring reliability and performance, OSPF is the preferred choice.

3. The area concept in OSPF allows large networks to be divided into smaller, manageable domains, reducing complexity and improving efficiency. By segmenting the network, the protocol limits the scope of link-state advertisements (LSAs), minimizing routing overhead. This design also enhances stability by isolating topology changes to specific areas, preventing widespread disruptions. Intra-area routing remains straightforward, while inter-area communication is handled through Area 0, the backbone. Area segmentation simplifies route summarization and optimizes resource utilization, making OSPF highly scalable. This modular approach ensures efficient operation in enterprise networks with complex topologies.
4. In OSPF, Area 0 serves as the backbone and is essential for inter-area routing. All other areas must connect directly or indirectly to Area 0, ensuring efficient routing and a loop-free design. The backbone facilitates communication between non-adjacent areas, centralizing inter-area traffic for better control. Configuring a unified backbone minimizes routing overhead and simplifies network management. It also ensures stability by maintaining a predictable and hierarchical structure. This backbone-centric approach is critical for large and distributed networks, as it prevents routing loops and maintains optimal path selection.
5. OSPF uses five main message types to establish and maintain routing: Hello, DBD (Database Description), LSR (Link State Request), LSU (Link State Update), and LSAck (Link State Acknowledgment). Hello packets identify and maintain neighbors. DBD packets provide a summary of link-state databases between neighbors. LSRs request specific database entries, while LSUs carry updates about topology changes. LSAscks confirm the receipt of LSUs, ensuring reliable communication. These message types work together to create and maintain an accurate and synchronized view of the network, enabling OSPF to respond quickly to topology changes.
6. The network’s security and redundancy measures were designed to ensure robust protection and high availability. Access Control Lists (ACLs) restricted inter-department communication, safeguarding sensitive departments like Finance. Port Security limited the number of MAC addresses per switch port, mitigating unauthorized access and MAC flooding attacks. HSRP was deployed for gateway redundancy, ensuring uninterrupted network access during router failures. EtherChannel with LACP aggregated multiple physical links, enhancing both redundancy and bandwidth. Spanning Tree Protocol (STP) prevented Layer 2 loops, while BPDU Guard secured ports from rogue switch connections. These measures ensured a secure and resilient network.
7. Spanning Tree Protocol (STP) eliminates Layer 2 loops by selectively blocking redundant paths, ensuring only one active path exists to each network segment. It elects a root bridge and calculates the shortest path to it for all devices, placing other links in a blocking state. When topology changes occur, STP dynamically recalculates the paths, activating previously blocked links if necessary. This prevents broadcast storms and

ensures network stability. Rapid Spanning Tree Protocol (RSTP) improves on traditional STP with faster convergence times, making it ideal for modern networks with stringent uptime requirements.

8. STP (Spanning Tree Protocol) creates a single spanning-tree instance for the entire network, which can be inefficient for VLANs. PVSTP (Per VLAN Spanning Tree Protocol) runs a separate STP instance for each VLAN, optimizing traffic flow for VLAN-specific needs but consuming more resources. MSTP (Multiple Spanning Tree Protocol) groups multiple VLANs into a single spanning-tree instance, balancing efficiency and resource utilization. MSTP is ideal for larger networks requiring scalability and VLAN traffic optimization. Each protocol addresses specific network requirements, with MSTP offering the most advanced and flexible solution.

TEST PLAN:

Test VLAN:

- Verify VLAN assignments using the show vlan brief command on all switches.
- Test device connectivity within the same VLAN using ping.
- Ensure VLAN trunking across switches is functional by using the show interfaces trunk command.
- Validate inter-VLAN communication through a router or Layer 3 switch and check if it complies with ACL restrictions.

```
BOS-SW0#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/10, Fa0/11, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
10   FINANCE                          active    Fa0/1, Fa0/2, Fa0/3
20   HR                               active    Fa0/4, Fa0/5, Fa0/6
30   Technical                        active    Fa0/7, Fa0/8, Fa0/9
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

```
MUM-SW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
10   FINANCE                          active    Fa0/1, Fa0/2, Fa0/3
20   HR                               active    Fa0/4, Fa0/5, Fa0/6
30   TECHNICAL                        active    Fa0/7, Fa0/8, Fa0/9
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

NYW ROOT SWITCH:

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
10   HR                               active
20   Technical                        active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

NYW VLAN 10 SWITCH:

```
Switch#sh VLAN brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   HR                               active    Fa0/1, Fa0/2, Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

NYW VLAN 20 SWITCH:

```
Switch#SH VLAN BRIEF

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
20   Technical                        active    Fa0/1, Fa0/2, Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

LON ROOT SWITCH:

```
Switch#Show VLAN BRIEF

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
10   HR                               active
20   Technical                        active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

LON VLAN 10 SWITCH:

```
Switch#show VLAN brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   HR                               active    Fa0/1, Fa0/2, Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

LON VLAN 20 SWITCH:

```
Switch#SHOW VLAN BRIEF

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
20   Technical                        active    Fa0/1, Fa0/2, Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

GER ROOT SWITCH

```
Switch#Show VLAN BRIEF

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
10   HR                               active
20   Technical                        active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

GER VLAN 10 SWITCH:

```
Switch#show VLAN brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   HR                               active    Fa0/1, Fa0/2, Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

GER VLAN 20 SWITCH:

```
Switch#SHOW VLAN BRIEF

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
20   Technical                        active    Fa0/1, Fa0/2, Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Test Routing Protocol:

- Check OSPF/EIGRP neighbor relationships using show ip ospf neighbor and show ip eigrp neighbors.
- Verify the routing table with show ip route to ensure all expected routes are present.
- Simulate a link failure and observe how routing protocols dynamically reroute traffic.
- Test connectivity between offices using ping and traceroute.

BOSTON PRIMARY ROUTER:

```
BOR1#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.2           0   2WAY/DROTHER    00:00:34    192.168.1.18    GigabitEthernet0/0.20
1.1.1.2           0   2WAY/DROTHER    00:00:33    192.168.1.34    GigabitEthernet0/0.30
1.1.1.2           0   2WAY/DROTHER    00:00:34    192.168.1.2     GigabitEthernet0/0.10
0.0.0.1           0   FULL/  -        00:00:33    192.168.6.2     Serial0/0/0
BOR1#
```

BOSTON STANDBY ROUTER:

```
BOR2#SHOW IP OSPF NEIGHBOR


Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   2WAY/DROTHER    00:00:36    192.168.1.1     GigabitEthernet0/0.10
1.1.1.1           0   2WAY/DROTHER    00:00:36    192.168.1.17    GigabitEthernet0/0.20
1.1.1.1           0   2WAY/DROTHER    00:00:36    192.168.1.33    GigabitEthernet0/0.30
0.0.0.1           0   FULL/  -        00:00:37    192.168.6.6     Serial0/0/0
BOR2#
```

MUMBAI PRIMARY ROUTER:

```
MUM1#SHOW IP OSPF NEIGHBOR


Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   2WAY/DROTHER    00:00:32    192.168.2.2     GigabitEthernet0/0.10
2.2.2.2           0   2WAY/DROTHER    00:00:31    192.168.2.18    GigabitEthernet0/0.20
2.2.2.2           0   2WAY/DROTHER    00:00:32    192.168.2.34    GigabitEthernet0/0.30
0.0.0.1           0   FULL/  -        00:00:32    192.168.6.10    Serial0/0/0
```

MUMBAI STANDBY ROUTER:

```
MUM2#SHOW IP OSPF NEIGHBOR


Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.1           0   2WAY/DROTHER    00:00:35    192.168.2.17    GigabitEthernet0/0.20
2.2.2.1           0   2WAY/DROTHER    00:00:35    192.168.2.33    GigabitEthernet0/0.30
2.2.2.1           0   2WAY/DROTHER    00:00:35    192.168.2.1     GigabitEthernet0/0.10
0.0.0.1           0   FULL/  -        00:00:35    192.168.6.14    Serial0/0/0
MUM2#
```

NEW-YORK ROUTER:

```
NYW1#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
0.0.0.1           0   FULL/  -        00:00:39    192.168.6.18    Serial0/0/0
NYW1#
```

LONDON ROUTER:

```
LON1#SHOW IP OSPF NEIGHBOR


Neighbor ID     Pri   State           Dead Time   Address         Interface
0.0.0.1           0   FULL/  -        00:00:37    192.168.6.22    Serial0/0/0
LON1#
```

GERMANY ROUTER:

```
GER1#SHOW IP OSPF NEIGHBOR


Neighbor ID     Pri   State           Dead Time   Address         Interface
0.0.0.1           0   FULL/  -        00:00:34    192.168.6.26    Serial0/0/0
GER1#
```

BACKBONE ROUTER:

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:32    192.168.6.1     Serial0/0/0
5.5.5.1           0   FULL/  -        00:00:33    192.168.6.25    Serial0/3/0
3.3.3.1           0   FULL/  -        00:00:32    192.168.6.17    Serial0/2/0
2.2.2.2           0   FULL/  -        00:00:33    192.168.6.13    Serial0/1/1
1.1.1.2           0   FULL/  -        00:00:39    192.168.6.5     Serial0/0/1
2.2.2.1           0   FULL/  -        00:00:39    192.168.6.9     Serial0/1/0
4.4.4.1           0   FULL/  -        00:00:32    192.168.6.21    Serial0/2/1
```

EIGRP:

FOR BOSTON:

```
BOR1#show ip EIGRP neighbor
IP-EIGRP neighbors for process 100
H   Address         Interface      Hold Uptime    SRTT   RTO   Q   Seq
                                   (sec)          (ms)         Cnt Num
0   10.10.10.2      Tun0           13   01:35:46  40     1000  0   17
```

FOR MUMBAI:

```
MUM1#SHOW IP EIGRP NEIGHBOR
IP-EIGRP neighbors for process 100
H   Address         Interface      Hold Uptime    SRTT   RTO   Q   Seq
                                   (sec)          (ms)         Cnt Num
0   10.10.10.1      Tun0           10   01:36:21  40     1000  0   16
```

CHECK IP ROUTE:

BOSTON:

```
BOR1#SHOW IP ROUTE
Codes: L - local, C - connected, S - static, 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 192.168.6.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.10.10.0/30 is directly connected, Tunnel0
L       10.10.10.1/32 is directly connected, Tunnel0
     192.168.0.0/32 is subnetted, 2 subnets
C       192.168.0.1/32 is directly connected, Loopback0
D       192.168.0.2/32 [90/27008000] via 10.10.10.2, 01:37:58, Tunnel0
     192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
C       192.168.1.0/28 is directly connected, GigabitEthernet0/0.10
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0.10
C       192.168.1.16/28 is directly connected, GigabitEthernet0/0.20
L       192.168.1.17/32 is directly connected, GigabitEthernet0/0.20
C       192.168.1.32/28 is directly connected, GigabitEthernet0/0.30
L       192.168.1.33/32 is directly connected, GigabitEthernet0/0.30
     192.168.2.0/28 is subnetted, 3 subnets
D       192.168.2.0/28 [90/26882560] via 10.10.10.2, 01:31:28, Tunnel0
O IA    192.168.2.16/28 [110/129] via 192.168.6.2, 01:37:48, Serial0/0/0
O IA    192.168.2.32/28 [110/129] via 192.168.6.2, 01:37:48, Serial0/0/0
     192.168.3.0/28 is subnetted, 2 subnets
O IA    192.168.3.0/28 [110/129] via 192.168.6.2, 01:37:48, Serial0/0/0
O IA    192.168.3.16/28 [110/129] via 192.168.6.2, 01:37:48, Serial0/0/0
     192.168.4.0/28 is subnetted, 2 subnets
O IA    192.168.4.0/28 [110/129] via 192.168.6.2, 01:37:48, Serial0/0/0
O IA    192.168.4.16/28 [110/129] via 192.168.6.2, 01:37:48, Serial0/0/0
     192.168.5.0/28 is subnetted, 2 subnets
O IA    192.168.5.0/28 [110/129] via 192.168.6.2, 01:37:38, Serial0/0/0
O IA    192.168.5.16/28 [110/129] via 192.168.6.2, 01:37:38, Serial0/0/0
     192.168.6.0/24 is variably subnetted, 8 subnets, 3 masks
C       192.168.6.0/24 is directly connected, Serial0/0/0
L       192.168.6.1/32 is directly connected, Serial0/0/0
O       192.168.6.4/30 [110/128] via 192.168.6.2, 01:37:48, Serial0/0/0
O       192.168.6.8/30 [110/128] via 192.168.6.2, 01:37:48, Serial0/0/0
O       192.168.6.12/30 [110/128] via 192.168.6.2, 01:37:48, Serial0/0/0
O       192.168.6.16/30 [110/128] via 192.168.6.2, 01:37:48, Serial0/0/0
O       192.168.6.20/30 [110/128] via 192.168.6.2, 01:37:48, Serial0/0/0
O       192.168.6.24/30 [110/128] via 192.168.6.2, 01:37:48, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 192.168.6.2
```

BOSTON STANDBY ROUTER:

```
BOR2#SHOW IP ROUTE
Codes: L - local, C - connected, S - static, 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 192.168.6.6 to network 0.0.0.0

     192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
C       192.168.1.0/28 is directly connected, GigabitEthernet0/0.10
L       192.168.1.2/32 is directly connected, GigabitEthernet0/0.10
C       192.168.1.16/28 is directly connected, GigabitEthernet0/0.20
L       192.168.1.18/32 is directly connected, GigabitEthernet0/0.20
C       192.168.1.32/28 is directly connected, GigabitEthernet0/0.30
L       192.168.1.34/32 is directly connected, GigabitEthernet0/0.30
     192.168.2.0/28 is subnetted, 3 subnets
O IA    192.168.2.0/28 [110/129] via 192.168.6.6, 01:21:32, Serial0/0/0
O IA    192.168.2.16/28 [110/129] via 192.168.6.6, 01:21:32, Serial0/0/0
O IA    192.168.2.32/28 [110/129] via 192.168.6.6, 01:21:32, Serial0/0/0
     192.168.3.0/28 is subnetted, 2 subnets
O IA    192.168.3.0/28 [110/129] via 192.168.6.6, 01:21:32, Serial0/0/0
O IA    192.168.3.16/28 [110/129] via 192.168.6.6, 01:21:32, Serial0/0/0
     192.168.4.0/28 is subnetted, 2 subnets
O IA    192.168.4.0/28 [110/129] via 192.168.6.6, 01:21:32, Serial0/0/0
O IA    192.168.4.16/28 [110/129] via 192.168.6.6, 01:21:32, Serial0/0/0
     192.168.5.0/28 is subnetted, 2 subnets
O IA    192.168.5.0/28 [110/129] via 192.168.6.6, 01:21:32, Serial0/0/0
O IA    192.168.5.16/28 [110/129] via 192.168.6.6, 01:21:32, Serial0/0/0
     192.168.6.0/24 is variably subnetted, 8 subnets, 3 masks
C       192.168.6.0/24 is directly connected, Serial0/0/0
O       192.168.6.4/30 [110/128] via 192.168.6.6, 01:21:32, Serial0/0/0
L       192.168.6.5/32 is directly connected, Serial0/0/0
O       192.168.6.8/30 [110/128] via 192.168.6.6, 01:21:32, Serial0/0/0
O       192.168.6.12/30 [110/128] via 192.168.6.6, 01:21:32, Serial0/0/0
O       192.168.6.16/30 [110/128] via 192.168.6.6, 01:21:32, Serial0/0/0
O       192.168.6.20/30 [110/128] via 192.168.6.6, 01:21:32, Serial0/0/0
O       192.168.6.24/30 [110/128] via 192.168.6.6, 01:21:32, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 192.168.6.6
```

MUMBAI PRIMARY ROUTER:

```
MUM1#SHOW IP ROUTE
Codes: L - local, C - connected, S - static, 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 are
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.6.10 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.10.10.0/30 is directly connected, Tunnel0
L       10.10.10.2/32 is directly connected, Tunnel0
     192.168.0.0/32 is subnetted, 2 subnets
D       192.168.0.1/32 [90/27008000] via 10.10.10.1, 01:40:44, Tunnel0
C       192.168.0.2/32 is directly connected, Loopback0
     192.168.1.0/28 is subnetted, 3 subnets
D       192.168.1.0/28 [90/26882560] via 10.10.10.1, 01:22:08, Tunnel0
O IA    192.168.1.16/28 [110/129] via 192.168.6.10, 01:22:33, Serial0/0/0
O IA    192.168.1.32/28 [110/129] via 192.168.6.10, 01:22:33, Serial0/0/0
     192.168.2.0/24 is variably subnetted, 6 subnets, 2 masks
C       192.168.2.0/28 is directly connected, GigabitEthernet0/0.10
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0.10
C       192.168.2.16/28 is directly connected, GigabitEthernet0/0.20
L       192.168.2.17/32 is directly connected, GigabitEthernet0/0.20
C       192.168.2.32/28 is directly connected, GigabitEthernet0/0.30
L       192.168.2.33/32 is directly connected, GigabitEthernet0/0.30
     192.168.3.0/28 is subnetted, 2 subnets
O IA    192.168.3.0/28 [110/129] via 192.168.6.10, 01:40:29, Serial0/0/0
O IA    192.168.3.16/28 [110/129] via 192.168.6.10, 01:40:29, Serial0/0/0
     192.168.4.0/28 is subnetted, 2 subnets
O IA    192.168.4.0/28 [110/129] via 192.168.6.10, 01:40:29, Serial0/0/0
O IA    192.168.4.16/28 [110/129] via 192.168.6.10, 01:40:29, Serial0/0/0
     192.168.5.0/28 is subnetted, 2 subnets
O IA    192.168.5.0/28 [110/129] via 192.168.6.10, 01:40:29, Serial0/0/0
O IA    192.168.5.16/28 [110/129] via 192.168.6.10, 01:40:29, Serial0/0/0
     192.168.6.0/24 is variably subnetted, 8 subnets, 3 masks
C       192.168.6.0/24 is directly connected, Serial0/0/0
O       192.168.6.4/30 [110/128] via 192.168.6.10, 01:40:39, Serial0/0/0
O       192.168.6.8/30 [110/128] via 192.168.6.10, 01:40:39, Serial0/0/0
L       192.168.6.9/32 is directly connected, Serial0/0/0
O       192.168.6.12/30 [110/128] via 192.168.6.10, 01:40:39, Serial0/0/0
O       192.168.6.16/30 [110/128] via 192.168.6.10, 01:40:39, Serial0/0/0
O       192.168.6.20/30 [110/128] via 192.168.6.10, 01:40:39, Serial0/0/0
O       192.168.6.24/30 [110/128] via 192.168.6.10, 01:40:39, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 192.168.6.10
```

MUMBAI STANDBY ROUTER:

```
MUM2#SHOW IP ROUTE
Codes: L - local, C - connected, S - static, 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

     192.168.1.0/28 is subnetted, 3 subnets
O IA    192.168.1.0/28 [110/129] via 192.168.6.14, 01:23:23, Serial0/0/0
O IA    192.168.1.16/28 [110/129] via 192.168.6.14, 01:23:23, Serial0/0/0
O IA    192.168.1.32/28 [110/129] via 192.168.6.14, 01:23:23, Serial0/0/0
     192.168.2.0/24 is variably subnetted, 6 subnets, 2 masks
C       192.168.2.0/28 is directly connected, GigabitEthernet0/0.10
L       192.168.2.2/32 is directly connected, GigabitEthernet0/0.10
C       192.168.2.16/28 is directly connected, GigabitEthernet0/0.20
L       192.168.2.18/32 is directly connected, GigabitEthernet0/0.20
C       192.168.2.32/28 is directly connected, GigabitEthernet0/0.30
L       192.168.2.34/32 is directly connected, GigabitEthernet0/0.30
     192.168.3.0/28 is subnetted, 2 subnets
O IA    192.168.3.0/28 [110/129] via 192.168.6.14, 01:41:24, Serial0/0/0
O IA    192.168.3.16/28 [110/129] via 192.168.6.14, 01:41:24, Serial0/0/0
     192.168.4.0/28 is subnetted, 2 subnets
O IA    192.168.4.0/28 [110/129] via 192.168.6.14, 01:41:24, Serial0/0/0
O IA    192.168.4.16/28 [110/129] via 192.168.6.14, 01:41:24, Serial0/0/0
     192.168.5.0/28 is subnetted, 2 subnets
O IA    192.168.5.0/28 [110/129] via 192.168.6.14, 01:41:14, Serial0/0/0
O IA    192.168.5.16/28 [110/129] via 192.168.6.14, 01:41:14, Serial0/0/0
     192.168.6.0/24 is variably subnetted, 8 subnets, 3 masks
C       192.168.6.0/24 is directly connected, Serial0/0/0
O       192.168.6.4/30 [110/128] via 192.168.6.14, 01:41:24, Serial0/0/0
O       192.168.6.8/30 [110/128] via 192.168.6.14, 01:41:24, Serial0/0/0
O       192.168.6.12/30 [110/128] via 192.168.6.14, 01:41:24, Serial0/0/0
L       192.168.6.13/32 is directly connected, Serial0/0/0
O       192.168.6.16/30 [110/128] via 192.168.6.14, 01:41:24, Serial0/0/0
O       192.168.6.20/30 [110/128] via 192.168.6.14, 01:41:24, Serial0/0/0
O       192.168.6.24/30 [110/128] via 192.168.6.14, 01:41:24, Serial0/0/0
```

NEW-YORK ROUTER:

```
NYW1#SHOW IP ROUTE
Codes: L - local, C - connected, S - static, 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 192.168.6.18 to network 0.0.0.0

     192.168.1.0/28 is subnetted, 3 subnets
O IA    192.168.1.0/28 [110/129] via 192.168.6.18, 01:24:06, Serial0/0/0
O IA    192.168.1.16/28 [110/129] via 192.168.6.18, 01:24:06, Serial0/0/0
O IA    192.168.1.32/28 [110/129] via 192.168.6.18, 01:24:06, Serial0/0/0
     192.168.2.0/28 is subnetted, 3 subnets
O IA    192.168.2.0/28 [110/129] via 192.168.6.18, 01:42:07, Serial0/0/0
O IA    192.168.2.16/28 [110/129] via 192.168.6.18, 01:42:07, Serial0/0/0
O IA    192.168.2.32/28 [110/129] via 192.168.6.18, 01:42:07, Serial0/0/0
     192.168.3.0/24 is variably subnetted, 4 subnets, 2 masks
C       192.168.3.0/28 is directly connected, GigabitEthernet0/0.10
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0.10
C       192.168.3.16/28 is directly connected, GigabitEthernet0/0.20
L       192.168.3.17/32 is directly connected, GigabitEthernet0/0.20
     192.168.4.0/28 is subnetted, 2 subnets
O IA    192.168.4.0/28 [110/129] via 192.168.6.18, 01:42:07, Serial0/0/0
O IA    192.168.4.16/28 [110/129] via 192.168.6.18, 01:42:07, Serial0/0/0
     192.168.5.0/28 is subnetted, 2 subnets
O IA    192.168.5.0/28 [110/129] via 192.168.6.18, 01:41:57, Serial0/0/0
O IA    192.168.5.16/28 [110/129] via 192.168.6.18, 01:41:57, Serial0/0/0
     192.168.6.0/24 is variably subnetted, 8 subnets, 3 masks
C       192.168.6.0/24 is directly connected, Serial0/0/0
O       192.168.6.4/30 [110/128] via 192.168.6.18, 01:42:07, Serial0/0/0
O       192.168.6.8/30 [110/128] via 192.168.6.18, 01:42:07, Serial0/0/0
O       192.168.6.12/30 [110/128] via 192.168.6.18, 01:42:07, Serial0/0/0
O       192.168.6.16/30 [110/128] via 192.168.6.18, 01:42:07, Serial0/0/0
L       192.168.6.17/32 is directly connected, Serial0/0/0
O       192.168.6.20/30 [110/128] via 192.168.6.18, 01:42:07, Serial0/0/0
O       192.168.6.24/30 [110/128] via 192.168.6.18, 01:42:07, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 192.168.6.18
```

LONDON ROUTER:

```
LON1#SHOW IP ROUTE
Codes: L - local, C - connected, S - static, 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 192.168.6.22 to network 0.0.0.0

     192.168.1.0/28 is subnetted, 3 subnets
O IA    192.168.1.0/28 [110/129] via 192.168.6.22, 01:24:49, Serial0/0/0
O IA    192.168.1.16/28 [110/129] via 192.168.6.22, 01:24:49, Serial0/0/0
O IA    192.168.1.32/28 [110/129] via 192.168.6.22, 01:24:49, Serial0/0/0
     192.168.2.0/28 is subnetted, 3 subnets
O IA    192.168.2.0/28 [110/129] via 192.168.6.22, 01:42:51, Serial0/0/0
O IA    192.168.2.16/28 [110/129] via 192.168.6.22, 01:42:51, Serial0/0/0
O IA    192.168.2.32/28 [110/129] via 192.168.6.22, 01:42:51, Serial0/0/0
     192.168.3.0/28 is subnetted, 2 subnets
O IA    192.168.3.0/28 [110/129] via 192.168.6.22, 01:42:51, Serial0/0/0
O IA    192.168.3.16/28 [110/129] via 192.168.6.22, 01:42:51, Serial0/0/0
     192.168.4.0/24 is variably subnetted, 4 subnets, 2 masks
C       192.168.4.0/28 is directly connected, GigabitEthernet0/0.10
L       192.168.4.1/32 is directly connected, GigabitEthernet0/0.10
C       192.168.4.16/28 is directly connected, GigabitEthernet0/0.20
L       192.168.4.17/32 is directly connected, GigabitEthernet0/0.20
     192.168.5.0/28 is subnetted, 2 subnets
O IA    192.168.5.0/28 [110/129] via 192.168.6.22, 01:42:40, Serial0/0/0
O IA    192.168.5.16/28 [110/129] via 192.168.6.22, 01:42:40, Serial0/0/0
     192.168.6.0/24 is variably subnetted, 8 subnets, 3 masks
C       192.168.6.0/24 is directly connected, Serial0/0/0
O       192.168.6.4/30 [110/128] via 192.168.6.22, 01:42:51, Serial0/0/0
O       192.168.6.8/30 [110/128] via 192.168.6.22, 01:42:51, Serial0/0/0
O       192.168.6.12/30 [110/128] via 192.168.6.22, 01:42:51, Serial0/0/0
O       192.168.6.16/30 [110/128] via 192.168.6.22, 01:42:51, Serial0/0/0
O       192.168.6.20/30 [110/128] via 192.168.6.22, 01:42:51, Serial0/0/0
L       192.168.6.21/32 is directly connected, Serial0/0/0
O       192.168.6.24/30 [110/128] via 192.168.6.22, 01:42:51, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 192.168.6.22
```

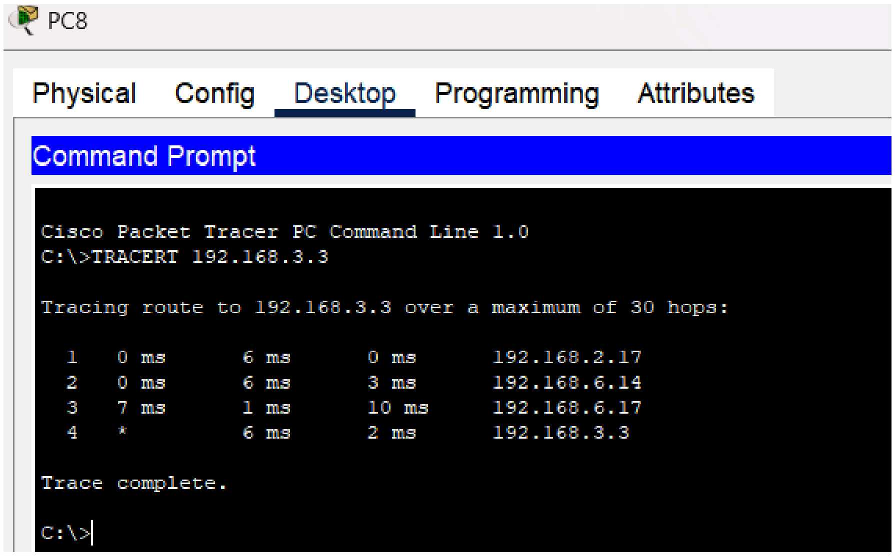
GERMANY ROUTER:

```
GER1#SHOW IP ROUTE
Codes: L - local, C - connected, S - static, 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 192.168.6.26 to network 0.0.0.0

     192.168.1.0/28 is subnetted, 3 subnets
O IA    192.168.1.0/28 [110/129] via 192.168.6.26, 01:25:32, Serial0/0/0
O IA    192.168.1.16/28 [110/129] via 192.168.6.26, 01:25:32, Serial0/0/0
O IA    192.168.1.32/28 [110/129] via 192.168.6.26, 01:25:32, Serial0/0/0
     192.168.2.0/28 is subnetted, 3 subnets
O IA    192.168.2.0/28 [110/129] via 192.168.6.26, 01:43:33, Serial0/0/0
O IA    192.168.2.16/28 [110/129] via 192.168.6.26, 01:43:33, Serial0/0/0
O IA    192.168.2.32/28 [110/129] via 192.168.6.26, 01:43:33, Serial0/0/0
     192.168.3.0/28 is subnetted, 2 subnets
O IA    192.168.3.0/28 [110/129] via 192.168.6.26, 01:43:33, Serial0/0/0
O IA    192.168.3.16/28 [110/129] via 192.168.6.26, 01:43:33, Serial0/0/0
     192.168.4.0/28 is subnetted, 2 subnets
O IA    192.168.4.0/28 [110/129] via 192.168.6.26, 01:43:33, Serial0/0/0
O IA    192.168.4.16/28 [110/129] via 192.168.6.26, 01:43:33, Serial0/0/0
     192.168.5.0/24 is variably subnetted, 4 subnets, 2 masks
C       192.168.5.0/28 is directly connected, GigabitEthernet0/0.10
L       192.168.5.1/32 is directly connected, GigabitEthernet0/0.10
C       192.168.5.16/28 is directly connected, GigabitEthernet0/0.20
L       192.168.5.17/32 is directly connected, GigabitEthernet0/0.20
     192.168.6.0/24 is variably subnetted, 8 subnets, 3 masks
C       192.168.6.0/24 is directly connected, Serial0/0/0
O       192.168.6.4/30 [110/128] via 192.168.6.26, 01:43:33, Serial0/0/0
O       192.168.6.8/30 [110/128] via 192.168.6.26, 01:43:33, Serial0/0/0
O       192.168.6.12/30 [110/128] via 192.168.6.26, 01:43:33, Serial0/0/0
O       192.168.6.16/30 [110/128] via 192.168.6.26, 01:43:33, Serial0/0/0
O       192.168.6.20/30 [110/128] via 192.168.6.26, 01:43:33, Serial0/0/0
O       192.168.6.24/30 [110/128] via 192.168.6.26, 01:43:33, Serial0/0/0
L       192.168.6.25/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 192.168.6.26
```

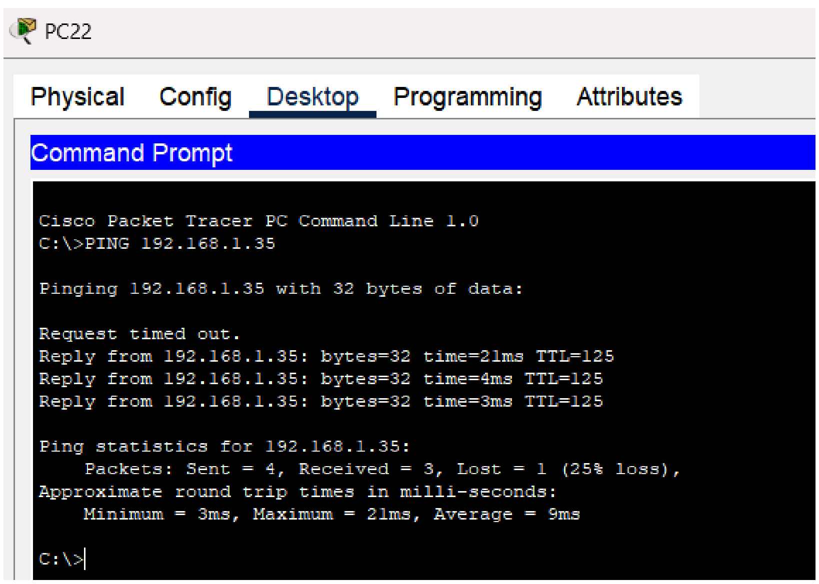
BACKBONE ROUTER:

```
Router>EN
Router#SHOW IP ROUTE
Codes: L - local, C - connected, S - static, 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

     192.168.1.0/28 is subnetted, 3 subnets
O IA    192.168.1.0/28 [110/65] via 192.168.6.5, 01:26:55, Serial0/0/1
                       [110/65] via 192.168.6.1, 01:26:20, Serial0/0/0
O IA    192.168.1.16/28 [110/65] via 192.168.6.5, 01:26:55, Serial0/0/1
                        [110/65] via 192.168.6.1, 01:26:20, Serial0/0/0
O IA    192.168.1.32/28 [110/65] via 192.168.6.5, 01:26:55, Serial0/0/1
                        [110/65] via 192.168.6.1, 01:26:20, Serial0/0/0
     192.168.2.0/28 is subnetted, 3 subnets
O IA    192.168.2.0/28 [110/65] via 192.168.6.13, 01:45:01, Serial0/1/1
                       [110/65] via 192.168.6.9, 01:44:51, Serial0/1/0
O IA    192.168.2.16/28 [110/65] via 192.168.6.13, 01:45:01, Serial0/1/1
                        [110/65] via 192.168.6.9, 01:44:51, Serial0/1/0
O IA    192.168.2.32/28 [110/65] via 192.168.6.13, 01:45:01, Serial0/1/1
                        [110/65] via 192.168.6.9, 01:44:51, Serial0/1/0
     192.168.3.0/28 is subnetted, 2 subnets
O IA    192.168.3.0/28 [110/65] via 192.168.6.17, 01:45:01, Serial0/2/0
O IA    192.168.3.16/28 [110/65] via 192.168.6.17, 01:45:01, Serial0/2/0
     192.168.4.0/28 is subnetted, 2 subnets
O IA    192.168.4.0/28 [110/65] via 192.168.6.21, 01:45:01, Serial0/2/1
O IA    192.168.4.16/28 [110/65] via 192.168.6.21, 01:45:01, Serial0/2/1
     192.168.5.0/28 is subnetted, 2 subnets
O IA    192.168.5.0/28 [110/65] via 192.168.6.25, 01:45:01, Serial0/3/0
O IA    192.168.5.16/28 [110/65] via 192.168.6.25, 01:45:01, Serial0/3/0
     192.168.6.0/24 is variably subnetted, 14 subnets, 2 masks
C       192.168.6.0/30 is directly connected, Serial0/0/0
L       192.168.6.2/32 is directly connected, Serial0/0/0
C       192.168.6.4/30 is directly connected, Serial0/0/1
L       192.168.6.6/32 is directly connected, Serial0/0/1
C       192.168.6.8/30 is directly connected, Serial0/1/0
L       192.168.6.10/32 is directly connected, Serial0/1/0
C       192.168.6.12/30 is directly connected, Serial0/1/1
L       192.168.6.14/32 is directly connected, Serial0/1/1
C       192.168.6.16/30 is directly connected, Serial0/2/0
L       192.168.6.18/32 is directly connected, Serial0/2/0
C       192.168.6.20/30 is directly connected, Serial0/2/1
L       192.168.6.22/32 is directly connected, Serial0/2/1
C       192.168.6.24/30 is directly connected, Serial0/3/0
L       192.168.6.26/32 is directly connected, Serial0/3/0
```

```
C:\>TRACERT 192.168.4.3

Tracing route to 192.168.4.3 over a maximum of 30 hops:

  1   0 ms      1 ms      0 ms      192.168.1.33
  2   0 ms      5 ms      11 ms     192.168.6.2
  3   1 ms      1 ms      3 ms      192.168.6.21
  4   *         1 ms      9 ms      192.168.4.3

Trace complete.

C:\>
```



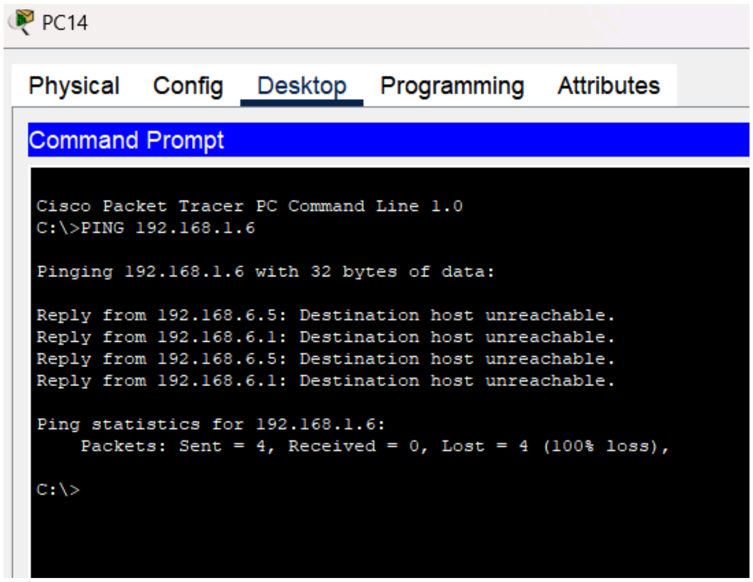

```
Cisco Packet Tracer PC Command Line 1.0
C:\>TRACERT 192.168.3.3

Tracing route to 192.168.3.3 over a maximum of 30 hops:

  1   0 ms      6 ms      0 ms      192.168.2.17
  2   0 ms      6 ms      3 ms      192.168.6.14
  3   7 ms      1 ms      10 ms     192.168.6.17
  4   *         6 ms      2 ms      192.168.3.3

Trace complete.

C:\>
```




```
Cisco Packet Tracer PC Command Line 1.0
C:\>PING 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.35: bytes=32 time=21ms TTL=125
Reply from 192.168.1.35: bytes=32 time=4ms TTL=125
Reply from 192.168.1.35: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 21ms, Average = 9ms

C:\>
```

Test Security Plan:

- Validate ACLs by attempting connections from unauthorized departments to Finance and ensure they are blocked.




```
Cisco Packet Tracer PC Command Line 1.0
C:\>PING 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.6.5: Destination host unreachable.
Reply from 192.168.6.1: Destination host unreachable.
Reply from 192.168.6.5: Destination host unreachable.
Reply from 192.168.6.1: Destination host unreachable.

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

- Confirm BPDU Guard functionality by sending a BPDU from a connected device and observing the port status.

```
BOS-SW0#show spanning-tree interface FastEthernet0/2 detail


Port 2 (FastEthernet0/2) of VLAN0010 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.2
  Designated root has priority 32778, address 000A.F340.5E59
  Designated bridge has priority 32778, address 000A.F340.5E59
  Designated port id is 128.2, designated path cost 19
  Timers: message age 16, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  The port is in the portfast mode
  Link type is point-to-point by default
```

Test Redundancy Plan:

1. HSRP (Hot Standby Router Protocol):

Purpose:
HSRP was implemented in the Boston and Mumbai offices to ensure **redundancy and high availability**. This configuration enables one router to act as the primary (active) device and the other as the backup (standby). If the primary router fails, the standby router takes over seamlessly, ensuring network continuity.

How It Was Done:

1. **Assign HSRP Group**:
    - Each router was assigned an **HSRP group ID** (e.g., Group 1 for Boston Finance VLAN).
2. **Virtual IP Address**:
    - A **virtual IP** was configured, which serves as the default gateway for devices within the VLAN (e.g., 192.168.1.14 for Boston Finance).
3. **Priority and Preemption**:
    - The active router was configured with a **higher priority** (e.g., priority 110), ensuring it becomes and remains the active router.
    - **Preemption** was enabled to allow the higher-priority router to reclaim its role as the active router after recovery.
4. **Timers**:
    - Custom **hello** and **hold timers** were set (standby 1 timers 2 6) for faster failover.
5. **Standby Configuration**:
    - The secondary router was configured as the standby device, ready to take over when the active router becomes unavailable.

Verification Command:
1. show standby

BOSTON Primary Router Configuration:

```
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.1.1 255.255.255.240
 ip helper-address 192.168.1.35
 ip ospf priority 0
 ip access-group FINANCE_INBOUND in
 ip access-group FINANCE_OUTBOUND out
 standby version 2
 standby 1 ip 192.168.1.14
 standby 1 priority 110
 standby 1 preempt
 standby 1 timers 2 6
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.1.17 255.255.255.240
 ip helper-address 192.168.1.35
 ip ospf priority 0
 standby version 2
 standby 2 ip 192.168.1.30
 standby 2 priority 110
 standby 2 preempt
 standby 2 timers 2 6
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.1.33 255.255.255.240
 ip helper-address 192.168.1.35
 ip ospf priority 0
 standby version 2
 standby 3 ip 192.168.1.46
 standby 3 priority 110
 standby 3 preempt
 standby 3 timers 2 6
```

BOSTON Standby router Configuration:

```
BOR2#sh standby
GigabitEthernet0/0.10 - Group 1 (version 2)
  State is Standby
    10 state changes, last state change 00:00:35
  Virtual IP address is 192.168.1.14
  Active virtual MAC address is 0000.0C9F.F001
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)
  Hello time 2 sec, hold time 6 sec
    Next hello sent in 1.172 secs
  Preemption enabled
  Active router is 192.168.1.1, priority 110 (expires in 4 sec)
    MAC address is 0000.0C9F.F001
  Standby router is local
  Priority 100 (default 100)
  Group name is hsrp-Gig-1 (default)
GigabitEthernet0/0.20 - Group 2 (version 2)
  State is Standby
    12 state changes, last state change 00:00:35
  Virtual IP address is 192.168.1.30
  Active virtual MAC address is 0000.0C9F.F002
    Local virtual MAC address is 0000.0C9F.F002 (v2 default)
  Hello time 2 sec, hold time 6 sec
    Next hello sent in 1.726 secs
  Preemption enabled
  Active router is 192.168.1.17, priority 110 (expires in 4 sec)
    MAC address is 0000.0C9F.F002
  Standby router is local
  Priority 100 (default 100)
  Group name is hsrp-Gig-2 (default)
GigabitEthernet0/0.30 - Group 3 (version 2)
  State is Standby
    9 state changes, last state change 00:00:37
  Virtual IP address is 192.168.1.46
  Active virtual MAC address is 0000.0C9F.F003
    Local virtual MAC address is 0000.0C9F.F003 (v2 default)
  Hello time 2 sec, hold time 6 sec
    Next hello sent in 1.407 secs
  Preemption enabled
  Active router is 192.168.1.33, priority 110 (expires in 5 sec)
    MAC address is 0000.0C9F.F003
  Standby router is local
  Priority 100 (default 100)
  Group name is hsrp-Gig-3 (default)
```

MUMBAI Primary Router Configuration:

```
MUM1#sh standby
GigabitEthernet0/0.10 - Group 1 (version 2)
  State is Active
    23 state changes, last state change 00:07:01
  Virtual IP address is 192.168.2.14
  Active virtual MAC address is 0000.0C9F.F001
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)
  Hello time 2 sec, hold time 6 sec
    Next hello sent in 0.047 secs
  Preemption enabled
  Active router is local
  Standby router is unknown, priority 100
  Priority 110 (configured 110)
  Group name is hsrp-Gig-1 (default)
GigabitEthernet0/0.20 - Group 2 (version 2)
  State is Active
    23 state changes, last state change 00:06:51
  Virtual IP address is 192.168.2.30
  Active virtual MAC address is 0000.0C9F.F002
    Local virtual MAC address is 0000.0C9F.F002 (v2 default)
  Hello time 2 sec, hold time 6 sec
    Next hello sent in 1.633 secs
  Preemption enabled
  Active router is local
  Standby router is unknown, priority 100
  Priority 110 (configured 110)
  Group name is hsrp-Gig-2 (default)
GigabitEthernet0/0.30 - Group 3 (version 2)
  State is Active
    21 state changes, last state change 00:06:51
  Virtual IP address is 192.168.2.46
  Active virtual MAC address is 0000.0C9F.F003
    Local virtual MAC address is 0000.0C9F.F003 (v2 default)
  Hello time 2 sec, hold time 6 sec
    Next hello sent in 1.239 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 110 (configured 110)
  Group name is hsrp-Gig-3 (default)
```

MUMBAI Standby Router Configuration:

```
MUM2>en
MUM2#sh standby
GigabitEthernet0/0.10 - Group 1
  State is Active
    9 state changes, last state change 00:03:55
  Virtual IP address is 192.168.2.14
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (v1 default)
  Hello time 2 sec, hold time 6 sec
    Next hello sent in 0.302 secs
  Preemption enabled
  Active router is local
  Standby router is unknown, priority 110
  Priority 100 (default 100)
  Group name is hsrp-Gig-1 (default)
GigabitEthernet0/0.20 - Group 2
  State is Active
    8 state changes, last state change 00:03:53
  Virtual IP address is 192.168.2.30
  Active virtual MAC address is 0000.0C07.AC02
    Local virtual MAC address is 0000.0C07.AC02 (v1 default)
  Hello time 2 sec, hold time 6 sec
    Next hello sent in 0.36 secs
  Preemption enabled
  Active router is local
  Standby router is unknown, priority 110
  Priority 100 (default 100)
  Group name is hsrp-Gig-2 (default)
GigabitEthernet0/0.30 - Group 3
  State is Active
    7 state changes, last state change 00:03:54
  Virtual IP address is 192.168.2.46
  Active virtual MAC address is 0000.0C07.AC03
    Local virtual MAC address is 0000.0C07.AC03 (v1 default)
  Hello time 2 sec, hold time 6 sec
    Next hello sent in 1.368 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 100 (default 100)
  Group name is hsrp-Gig-3 (default)
```

2. Rapid Spanning Tree Protocol (RSTP):

Purpose:
RSTP was implemented to enhance network redundancy, prevent Layer 2 loops, and ensure faster convergence, minimizing downtime during topology changes.

Implementation:

- **Configuration:**
  - Enabled **Rapid Per-VLAN Spanning Tree Protocol (PVST+)** for each VLAN.
  - Configured **spanning-tree mode rapid-pvst** for optimal performance and failover.
- **Bridge Priorities:**
  - Assigned specific priorities to designate root bridges for VLANs (e.g., Boston switch as the root for VLAN 10, 20, and 30).
- **PortFast and BPDU Guard:**
  - Enabled **PortFast** on access ports to bypass learning/listening states for quicker connectivity.
  - Enabled **BPDU Guard** to block rogue devices sending BPDUs.
- **Redundant Links:**
  - Configured redundant uplinks, ensuring only one active link per path, with rapid failover for link failures.

Outcome:

- Faster recovery from changes, efficient path utilization, loop prevention, and improved stability across all locations.

```
MUM-SW1>en
MUM-SW1#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     00D0.BC23.DE8E
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00D0.BC23.DE8E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/10           Desg FWD 19        128.10   P2p
Fa0/11           Desg FWD 19        128.11   P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     00D0.BC23.DE8E
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     00D0.BC23.DE8E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/10           Desg FWD 19        128.10   P2p
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/11           Desg FWD 19        128.11   P2p
```

```
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    32788
             Address     00D0.BC23.DE8E
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     00D0.BC23.DE8E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/10           Desg FWD 19        128.10   P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/11           Desg FWD 19        128.11   P2p

VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    32798
             Address     00D0.BC23.DE8E
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32798  (priority 32768 sys-id-ext 30)
             Address     00D0.BC23.DE8E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/9            Desg FWD 19        128.9    P2p
Fa0/10           Desg FWD 19        128.10   P2p
Fa0/7            Desg FWD 19        128.7    P2p
Fa0/8            Desg FWD 19        128.8    P2p
Fa0/11           Desg FWD 19        128.11   P2p
```

Test Bonus:

1.Enable SSH Between All Routers Using Hostnames

Purpose:
SSH was enabled for secure communication and management of routers across the network.

Implementation:

- Configured an SSH version 2 server on each router using ip ssh version 2.
- Assigned hostnames and mapped them to IP addresses with the ip host command.
- Defined a domain name using ip domain-name.
- Created user credentials with privilege levels using username <name> privilege 15 secret <password>.
- Enabled SSH on vty lines with login local and transport input ssh.

Outcome:
Administrators could securely manage routers using SSH and hostnames, ensuring encrypted communication.

Username: admin

Password: Cisco123

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin GER1

Trying 192.168.6.25 ...
Password:


GER1#
```

2. Configure a VPN Tunnel Between Boston and Mumbai HQs

Purpose:
A VPN tunnel was implemented to securely connect the two HQs, ensuring encrypted communication over the internet.

Implementation:

- Used GRE (Generic Routing Encapsulation) to establish a tunnel.
- Configured tunnel source and tunnel destination on both routers.
- Assigned IP addresses to the tunnel interfaces.

Outcome:

The VPN tunnel provided secure, encrypted connectivity between the Boston and Mumbai HQs.

```
interface Tunnel0
 ip address 10.10.10.1 255.255.255.252
 mtu 1476
 tunnel source Serial0/0/0
 tunnel destination 192.168.6.9
```

```
BOR1#show ip interface brief | include Tunnel
Tunnel0                10.10.10.1      YES manual up                    up
```

```
interface Tunnel0
 ip address 10.10.10.2 255.255.255.252
 mtu 1476
 tunnel source Serial0/0/0
 tunnel destination 192.168.6.1
```

```
MUM1#show ip interface brief | include Tunnel
Tunnel0                10.10.10.2      YES manual up                    up
```

3. EtherChannel with LACP (Link Aggregation Control Protocol)

Purpose:
EtherChannel with LACP was used to combine multiple physical links into a single logical link, increasing bandwidth, ensuring redundancy, and improving fault tolerance. LACP dynamically negotiated link inclusion in the bundle and provided seamless failover in case of link failures.

Implementation:

1. Configured EtherChannel on trunk links between switches and routers using the **channel-group** command.
2. Set LACP mode to **active or passive** for dynamic negotiation.
3. Enabled trunking on the logical Port-Channel interface to support VLAN traffic.
4. LACP managed link operations based on their status and adjusted the bundle during failures.

Verification:
The **show etherchannel summary** command confirmed the operational status of the EtherChannel bundle and displayed active links with protocol (LACP).

Outcome:

1. **Increased Bandwidth:** Aggregated multiple physical links for higher throughput.
2. **Improved Redundancy:** Ensured uninterrupted traffic during link failures.
3. **Optimized Traffic Flow:** Reduced congestion through load-balancing algorithms

IN NEWYORK SWITCH:

```
interface Port-channel1
 switchport mode trunk
```

```
interface FastEthernet0/5
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/6
 switchport trunk allowed vlan 10,20
 switchport mode trunk
 channel-group 1 mode active
```

```
Switch#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------

1      Po1(SU)           LACP   Fa0/5(P) Fa0/6(P)
Switch#
```

4. Defend MAC Flooding Attack

Purpose:
MAC flooding attacks aim to overload a switch's MAC address table, forcing it to broadcast all traffic and potentially expose sensitive data. Port Security was implemented to prevent such attacks.

Implementation:

- Configured switchport port-security on access ports.
- Limited the number of MAC addresses learned on a port using switchport port-security maximum.
- Enabled sticky MAC learning with switchport port-security mac-address sticky to dynamically bind MAC addresses.
- Set the violation mode to restrict to drop unauthorized traffic and log violations.

Outcome:
This defense mechanism prevented MAC flooding attacks by limiting the number of MAC addresses, ensuring only legitimate devices could connect, and protecting against unauthorized access.

```
BOS-SW0>EN
BOS-SW0#SHOW PORT-SECURITY
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
        Fa0/1        3          1                0         Restrict
        Fa0/2        3          1                0         Restrict
        Fa0/3        3          1                0         Restrict
        Fa0/4        3          1                0         Restrict
        Fa0/5        3          1                0         Restrict
        Fa0/6        3          1                0         Restrict
        Fa0/7        3          1                0         Restrict
        Fa0/8        3          1                0         Restrict
        Fa0/9        3          1                0         Restrict
```

Concepts Learned

This project enhanced understanding of complex enterprise networking concepts such as VLAN configuration, dynamic routing protocols like OSPF and EIGRP, and advanced security measures. Practical exposure to redundancy protocols like HSRP and RSTP was invaluable for improving network reliability. Configuring EtherChannel and GRE VPN tunnels strengthened knowledge of link aggregation and secure inter-office connectivity. The importance of ACLs for segmenting network traffic and preventing unauthorized access was emphasized, along with hands-on experience in debugging and troubleshooting network configurations.

Conclusion

The project successfully designed and implemented a secure, scalable, and redundant enterprise network for a geographically distributed organization. By leveraging VLANs, routing protocols, and security mechanisms, seamless communication was achieved across multiple departments and locations while maintaining strict access controls. Redundancy plans ensured high availability, and the implementation of advanced protocols like RSTP and EtherChannel improved network performance. Overall, this project provided valuable insights into the practical application of theoretical networking concepts, preparing for real-world scenarios in enterprise environments.