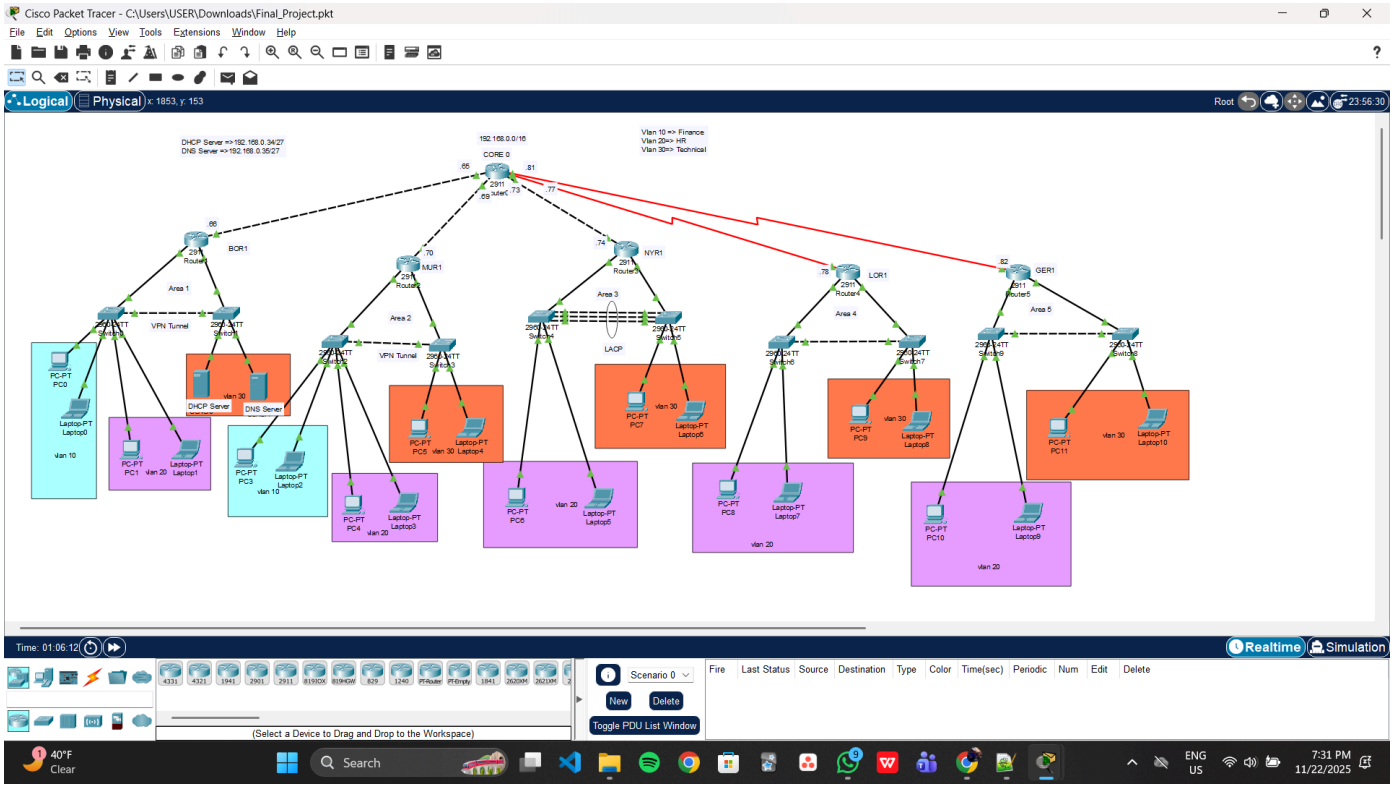
Answers:

1.) Network Diagram:



My network connects five major locations:

*. Boston(BOR1)

*. Mumbai(MUR1)

*. New York(NYR1)

*. London(LOR1)

*. Germany(GER1)

Boston and Mumbai are the head offices so they have 3 departments(Finance, HR, Technical) and others have 2 departments(HR and Technical) and head offices are connected by a GRE tunnel for direct communication. I used Vlans to separate departments and OSPF across the routers for routing across the entire topology and DHCP and DNS servers are in the technical department of boston.Departments vlan allocation:

*. Finance(vlan 10)

*. HR(vlan 20)

*. Technical(vlan 30).

According to the ACLs rules, Finance department pcs can ping each other and also they have an ability to access other departments but departments are restricted to access finance department.

2.) Architecture:

*. Core Layer Router : It has a core 0 router which is a backbone for all routers and it is connected with point to point network type links and running OSPF.

*. Distribution Layer Router: There are total 5 routers that have sub-interfaces to handle inter-vlan routing and they also act as a DHCP relay agent to get IP addresses for their end devices.

*. Access Layer (Switches): Each router will have two access layer switches and they have been connected with trunk ports between them and access ports with the end devices and switches belongs to NYR1 router, I did LACP(Etherchannel) bundling to avoid oversubscription problem in switches.

Router sub-interfaces: G0/1.10 => vlan 10
G0/1.20 => vlan 20
G0/2.30 => vlan 30

*. In boston and mumbai routers and the i used two different interfaces for two different vlans.Each sub-interfaces has its own ips based on subnetting i did and also they are configured with ospf area and acls based on router they are in and each switches have been enabled with port security restrict which will block the unknown mac addresses and also keep the port stable by not shutting down it and each switch will support 802.1Q trunking and have multiple access ports.

Ip allocation in boston(Similar to that i have allocated to Mumbai router also)

*. DHCP server is in vlan 30(Technical department) of BOR1 => 192.168.0.34/34

*. DNS Server => 192.168.0.35/27

*. Vlan 10(G0/1.10) => 192.168.0.1/28

*. Vlan 20(G0/1.20) => 192.168.0.17/28

*. Vlan 30(G0/2.30) => 192.168.0.33/27

To make ip allocation simple these are the addresses with increment on one to the network address and also it will be easy to exclude certain ips while dns configuration.

Configuration in New York(NYR1) :

*. Vlan 20(G0/1.20) => 192.168.0.129/27

*. Vlan 30(G0/2.30) => 192.168.0.161/27

Basically I have planned that the total number of hosts in a single router should be within /26 to meet the requirements, so I subnetted accordingly.

I have configured ssh on each router according to the hostname I have provided in the DNS server and it also has a username and password. We can login into routers from any of the pcs in the network or from any of the routers.

3.)
i.) OSPF is a routing protocol that learns the network by exchanging link information with neighboring routers. They find the shortest path using Dijkstra's algorithm and also they form a connectivity map which is common in each area. They will exchange Link State Advertisements(LSA) until they all have a common Link State Database(LSDB).and its metric is cost of the exit interface. Each router will undergo 7 states after enabling ospf to form neighbors with other ospf enabled routers.

ii.) *. OSPF is better than RIP, The main advantage of choosing OSPF is the best is because of metric, RIP uses HOP as a metric and it doesn't care about interface speed. The interface with higher speed and the interface with lower will be the same if we are using RIP as a routing protocol.

*. OSPF supports multiple areas for cleaner design and routers recover more quickly from link failures. RIP is simple, but too limited for modern enterprise Networks.

iii.) The main purpose of having multiple areas concept in ospf is to reduce the routing table size in the individual router and also for every change in the network, they have to update their LSDB for that they have to share LSA often. If it is a single and large area, LSA flooding will happen often.
It also improved the stability of router because CPU load is being decreased and it also keeps local changes inside each area.

iv.) OSPF requires all other areas to connect to Area 0 because this rule keeps routing simple, avoid loops and it ensures all areas can communicate efficiently and it act as a gate way to the outer network, If any packet from the outer network wants to communicate inside the network it will first contact area 0 router. Area 0 acts like the SPINE of the network.

v.) Hello- It is used to find neighbors and maintain adjacencies between the routers.
DBD(Database Description)- It gives short summaries of link-state databases
LSR(Link State Requests)- It is used to ask neighbor routers for missing information.
LSU(Link State Update)- It sends full updates to routers.
LSAck(Link State Acknowledgement)- after receiving an update, it is a confirming receipt.
These are all the messages keep all routers Synzhronized.

vi.) Security and Plan:
*. Vlan segmentation. It will restrict other departments to see their information because each vlan will be in different subnets.
*. ACLs will block unauthorized access.
*. SSh for router management.
*. Port security on switches to stop MAC flooding attack.
*. DHCP and DNS Servers are placed in a port security enabled switches to avoid risk of attacks.

*. LACP bundling on NYR1 to avoid oversubscription problem.
*. HSRP for gateway failover.
*. GRE tunneling between headquarters.
*. Multiple OSPF Areas for stability

vii.) Generally when switches are interconnected with each other with multiple link it will create a broadcast storm. STP will block the extra links so only one active path exists. If any of the active link fails STP opens the blocked link automatically and put that in a forwarding state.

To blocking a particular port, it will undergo multiple elections.
*. Root Bridge Election (the switch which has lower bridge id). After election For every 2 seconds it will STP BPDUs out of its designated ports which will have root bridge information.
*. Root port election (This port will receive the stp bpdus sent by the root bridge and each switch have one root port)
*. Forwarding port election(Used to forward the stp bpdu, the port that fails in forwarding port election will the blocking port)

viii.) STP - It is the first version used in older networks and it will create one spanning tree instance for entire switch network, even if we have many vlans. For all vlans it will have same blocked and forwarding port.

PVSTP(Per-vlan spanning tree)- It will create a separate instance for every vlan. We can allocate each vlan different primary and secondary root bridge. It will load balance efficiently because vlans can be spread across links.

MSTP(Multiple Spanning Tree Protocol)- It is designed for bif networks where pvstp becomes too heavy. It let us group several vlans into a single stp instance. It reduces Overhead because instead of 30 STP calculations, we might have to run only 3 instances.

4.) i. VLAN Testing
*. Checking by using (“SHOW VLAN BREIF”). screenshot taken from BOR1 switches.

```
Switch#
Switch#sho
Switch#show vl
Switch#show vlan br
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   VLAN0010                         active    Fa0/2, Fa0/3
20   VLAN0020                         active    Fa0/5, Fa0/6
30   VLAN0030                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

```
Switch#show vla
Switch#show vlan b
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active    Fa0/3, Fa0/4
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

*. Inspecting Trunk ports using (“SHOW INTERFACES TRUNK”)

```
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#show in
Switch#show interfaces t
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/4       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       10,20,30
Fa0/4       10,20,30

Port        Vlans allowed and active in management domain
Fa0/1       10,20,30
Fa0/4       10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,20,30
Fa0/4       10,20,30

Switch#
```

```
Switch#show interfaces t
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/2       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       10,20,30
Fa0/2       10,20,30

Port        Vlans allowed and active in management domain
Fa0/1       10,20,30
Fa0/2       10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,20,30
Fa0/2       10,20,30

Switch#
```

*. Pinging in same vlan.

```
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 192.168.0.5

Pinging 192.168.0.5 with 32 bytes of data:

Reply from 192.168.0.5: bytes=32 time<1ms TTL=128
Reply from 192.168.0.5: bytes=32 time<1ms TTL=128
Reply from 192.168.0.5: bytes=32 time<1ms TTL=128
Reply from 192.168.0.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

*. Pinging across the vlan.

```
C:\>
C:\>ping 192.168.0.173

Pinging 192.168.0.173 with 32 bytes of data:

Reply from 192.168.0.173: bytes=32 time<1ms TTL=125
Reply from 192.168.0.173: bytes=32 time<1ms TTL=125
Reply from 192.168.0.173: bytes=32 time<1ms TTL=125
Reply from 192.168.0.173: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.0.173:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>
```

ii.) Routing protocol testing:

*. To check ospf neighbors(“SHOW IP OSPF NEIGHBIOR”) BOR1

```
BOR1#
BOR1#show ip os
BOR1#show ip ospf n
BOR1#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:37    192.168.1.65    GigabitEthernet0/0
BOR1#
```

From CORE 0:

```
CORE0#show ip os
CORE0#show ip ospf n
CORE0#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.2           0   FULL/  -        00:00:35    192.168.1.66    GigabitEthernet0/0
2.2.2.2           0   FULL/  -        00:00:33    192.168.1.70    GigabitEthernet0/1
3.3.3.3           0   FULL/  -        00:00:36    192.168.1.74    GigabitEthernet0/2
4.4.4.4           0   FULL/  -        00:00:36    192.168.1.78    Serial0/3/0
5.5.5.5           0   FULL/  -        00:00:37    192.168.1.82    Serial0/3/1
CORE0#
```

Copy Paste

*. Verifying Routing tables(SHOW IP ROUTE) CORE)

```
CORE0#
CORE0#show ip ro
CORE0#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

     192.168.0.0/24 is variably subnetted, 10 subnets, 2 masks
O IA    192.168.0.0/28 [110/2] via 192.168.1.66, 03:29:51, GigabitEthernet0/0
O IA    192.168.0.16/28 [110/2] via 192.168.1.66, 03:29:51, GigabitEthernet0/0
O IA    192.168.0.32/27 [110/2] via 192.168.1.66, 03:29:51, GigabitEthernet0/0
O IA    192.168.0.64/28 [110/2] via 192.168.1.70, 03:30:01, GigabitEthernet0/1
O IA    192.168.0.80/28 [110/2] via 192.168.1.70, 03:30:01, GigabitEthernet0/1
O IA    192.168.0.96/27 [110/2] via 192.168.1.70, 03:30:01, GigabitEthernet0/1
O IA    192.168.0.128/27 [110/2] via 192.168.1.74, 02:59:13, GigabitEthernet0/2
O IA    192.168.0.160/27 [110/2] via 192.168.1.74, 02:59:13, GigabitEthernet0/2
O IA    192.168.0.192/27 [110/65] via 192.168.1.78, 03:30:01, Serial0/3/0
O IA    192.168.0.224/27 [110/65] via 192.168.1.78, 03:30:01, Serial0/3/0
     192.168.1.0/24 is variably subnetted, 12 subnets, 3 masks
O IA    192.168.1.0/27 [110/65] via 192.168.1.82, 03:30:01, Serial0/3/1
O IA    192.168.1.32/27 [110/65] via 192.168.1.82, 03:30:01, Serial0/3/1
C       192.168.1.64/30 is directly connected, GigabitEthernet0/0
L       192.168.1.65/32 is directly connected, GigabitEthernet0/0
C       192.168.1.68/30 is directly connected, GigabitEthernet0/1
L       192.168.1.69/32 is directly connected, GigabitEthernet0/1
C       192.168.1.72/30 is directly connected, GigabitEthernet0/2
L       192.168.1.73/32 is directly connected, GigabitEthernet0/2
C       192.168.1.76/30 is directly connected, Serial0/3/0
L       192.168.1.77/32 is directly connected, Serial0/3/0
C       192.168.1.80/30 is directly connected, Serial0/3/1
L       192.168.1.81/32 is directly connected, Serial0/3/1

CORE0#
```

From BOR1

```
BOR1#
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 not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.100.100.0/30 is directly connected, Tunnel10
L       10.100.100.1/32 is directly connected, Tunnel10
     192.168.0.0/24 is variably subnetted, 13 subnets, 3 masks
C       192.168.0.0/28 is directly connected, GigabitEthernet0/1.10
L       192.168.0.1/32 is directly connected, GigabitEthernet0/1.10
C       192.168.0.16/28 is directly connected, GigabitEthernet0/1.20
L       192.168.0.17/32 is directly connected, GigabitEthernet0/1.20
C       192.168.0.32/27 is directly connected, GigabitEthernet0/2.30
L       192.168.0.33/32 is directly connected, GigabitEthernet0/2.30
O IA    192.168.0.64/28 [110/3] via 192.168.1.65, 03:31:20, GigabitEthernet0/0
O IA    192.168.0.80/28 [110/3] via 192.168.1.65, 03:31:20, GigabitEthernet0/0
O IA    192.168.0.96/27 [110/3] via 192.168.1.65, 03:31:20, GigabitEthernet0/0
O IA    192.168.0.128/27 [110/3] via 192.168.1.65, 03:00:47, GigabitEthernet0/0
O IA    192.168.0.160/27 [110/3] via 192.168.1.65, 03:00:47, GigabitEthernet0/0
O IA    192.168.0.192/27 [110/66] via 192.168.1.65, 03:31:30, GigabitEthernet0/0
O IA    192.168.0.224/27 [110/66] via 192.168.1.65, 03:31:30, GigabitEthernet0/0
     192.168.1.0/24 is variably subnetted, 8 subnets, 3 masks
O IA    192.168.1.0/27 [110/66] via 192.168.1.65, 03:31:30, GigabitEthernet0/0
O IA    192.168.1.32/27 [110/66] via 192.168.1.65, 03:31:30, GigabitEthernet0/0
C       192.168.1.64/30 is directly connected, GigabitEthernet0/0
L       192.168.1.66/32 is directly connected, GigabitEthernet0/0
O       192.168.1.68/30 [110/2] via 192.168.1.65, 03:31:30, GigabitEthernet0/0
O       192.168.1.72/30 [110/2] via 192.168.1.65, 03:31:30, GigabitEthernet0/0
O       192.168.1.76/30 [110/65] via 192.168.1.65, 03:31:30, GigabitEthernet0/0
O       192.168.1.80/30 [110/65] via 192.168.1.65, 03:31:30, GigabitEthernet0/0

BOR1#
```

*. Ping across the network

```
C:\>
C:\>ping 192.168.0.173

Pinging 192.168.0.173 with 32 bytes of data:

Reply from 192.168.0.173: bytes=32 time<1ms TTL=125
Reply from 192.168.0.173: bytes=32 time<1ms TTL=125
Reply from 192.168.0.173: bytes=32 time<1ms TTL=125
Reply from 192.168.0.173: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.0.173:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>
```

vi.) Bonus testing:

*. Testing Tunnel(“Show interface tunnel 10”)

```
BOR1#show interfaces tu
BOR1#show interfaces tunnel 10
Tunnel10 is up, line protocol is up (connected)
  Hardware is Tunnel
  Internet address is 10.100.100.1/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 192.168.1.66 (GigabitEthernet0/0), destination 192.168.1.70
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
      0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out

BOR1#
```

*. Ssh Testing(“ssh -l barath bor1”)

```
MUR1>
MUR1>
MUR1>en
MUR1#
MUR1#
MUR1#ssh -l barath bor1
Translating "bor1"...domain server (192.168.0.35)
Trying 192.168.1.66 ...
Password:



BOR1#
```

*. Portchannel Testing(“SHOW ETHERCHANNEL SUMMARY”)

```
Switch#show eth
Switch#show etherchannel su
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   Fa0/2(P) Fa0/5(P) Fa0/6(P)
Switch#
```

*. Port Security Testing (“SHOW PORT-SECURITY INTERFACE FA0/1”)

```
Switch#show port-security in
Switch#show port-security interface f
Switch#show port-security interface fastEthernet 0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 10
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0002.17EE.BCE6:10
Security Violation Count   : 0

Switch#
```

*. DNS server Name testing (“Ping bor1”)

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping bor1

Pinging 192.168.1.66 with 32 bytes of data:

Reply from 192.168.1.66: bytes=32 time<1ms TTL=253
Reply from 192.168.1.66: bytes=32 time<1ms TTL=253
Reply from 192.168.1.66: bytes=32 time<1ms TTL=253
Reply from 192.168.1.66: bytes=32 time<1ms TTL=253

Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

V.) *. During the projects i have learnt so many concepts both theoretically and practically and I have learned to build the network in a structured way.

*. I learnt various protocols and concepts like OSPF, HSRP, DHCP, DNS, ACLS, Port security, Intervlan routing and basic flow of packets in the network.

*. In addition to that i have learnt GRE tunneling which is new for me. Overall, the project improved my understanding of real- world enterprise networking.

iii.) Security Testing:

*. Ping From hr department ACL should block

```
C:\>ping 192.168.0.5

Pinging 192.168.0.5 with 32 bytes of data:

Reply from 192.168.1.66: Destination host unreachable.
Reply from 192.168.1.66: Destination host unreachable.
Reply from 192.168.1.66: Destination host unreachable.
Reply from 192.168.1.66: Destination host unreachable.

Ping statistics for 192.168.0.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

*. Ping from finance it should succeed.

```
C:\>ping 192.168.0.165

Pinging 192.168.0.165 with 32 bytes of data:

Reply from 192.168.0.165: bytes=32 time<1ms TTL=125
Reply from 192.168.0.165: bytes=32 time<1ms TTL=125
Reply from 192.168.0.165: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.0.165:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

Control-C
```

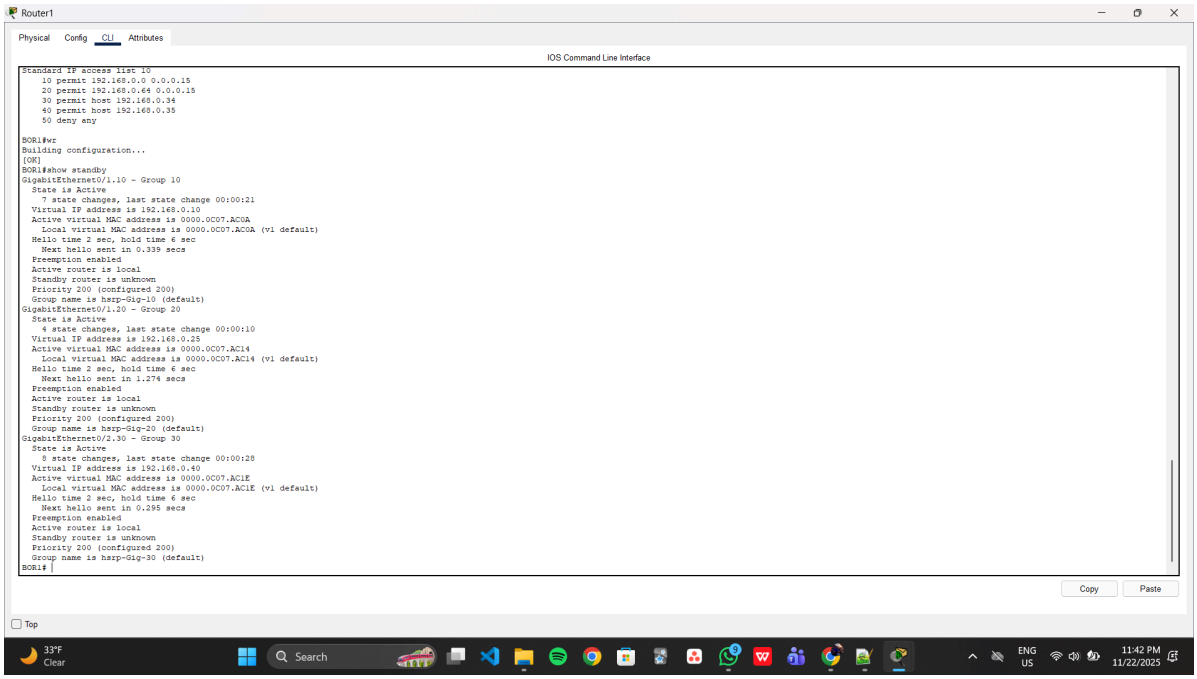
*. Port security(I have already attached screen shot in bonus testing)

*. To check access lists(“SHOW ACCESS-LISTS”)

```
BOR1#show
BOR1#show acc
BOR1#show access-lists
Standard IP access list 10
    10 permit 192.168.0.0 0.0.0.15
    20 permit 192.168.0.64 0.0.0.15
    30 permit host 192.168.0.34
    40 permit host 192.168.0.35
    50 deny any

BOR1#
```

4.) Redundancy plan testing(Show Standby):



*. As I have already used OSPF, Each router will learn every available path in the network, not just one.

Conclusion:

*. This project brought together almost all key topics in networking . I learned to design a clean, scalable and secure multi office network.

*. Implementing GRE tunnels also showed how companies maintain stable inter-office communication.

*. Overall, this project Strengthened both my technical knowledge and my confidence in building large scale networks and resemble real enterprise environments.