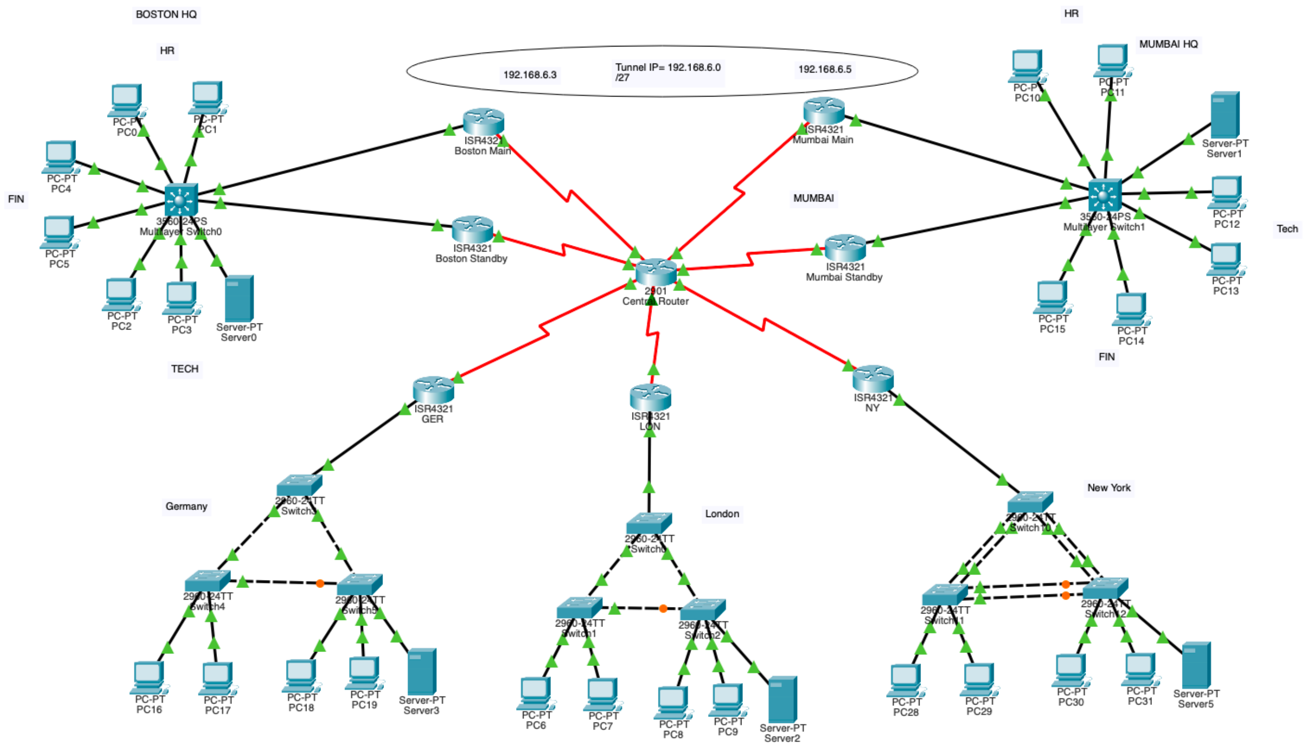
PROJECT DESIGN



Network Optimization

Boston:

HR: 192.168.0.0/27

TECHNICAL: 192.168.0.32/27

FINANCE: 192.168.0.64/27

2 ISR 4321 Routers with HWIC-2T module installed

6 PC's

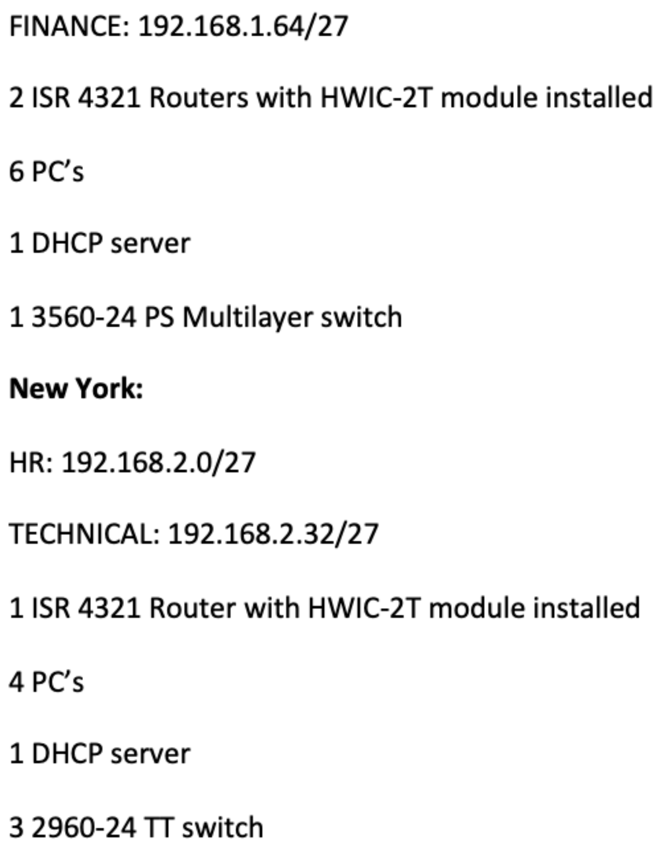
1 server (DNS& DHCP included)

1 3560-24 PS Multilayer switch

Mumbai:

HR: 192.168.1.0/27

TECHNICAL: 192.168.1.32/27



FINANCE: 192.168.1.64/27

2 ISR 4321 Routers with HWIC-2T module installed

6 PC's

1 DHCP server

1 3560-24 PS Multilayer switch

New York:

HR: 192.168.2.0/27

TECHNICAL: 192.168.2.32/27

1 ISR 4321 Router with HWIC-2T module installed

4 PC's

1 DHCP server

3 2960-24 TT switch

Germany:

HR: 192.168.3.0/27

TECHNICAL: 192.168.3.32/27

4 PC's

1 DHCP server

1 ISR 4321 Router with HWIC-2T module installed

1 2960-24 TT switch

London:

HR: 192.168.4.0/27

TECHNICAL: 192.168.4.32/27

1 ISR 4321 Router with HWIC-2T module installed

4 PC's

1 DHCP server

1 2960-24 TT switch

BUDGET:

7*ISR 4321 Router + 1* 2901 Router = 7*3300+ 870 = 23970

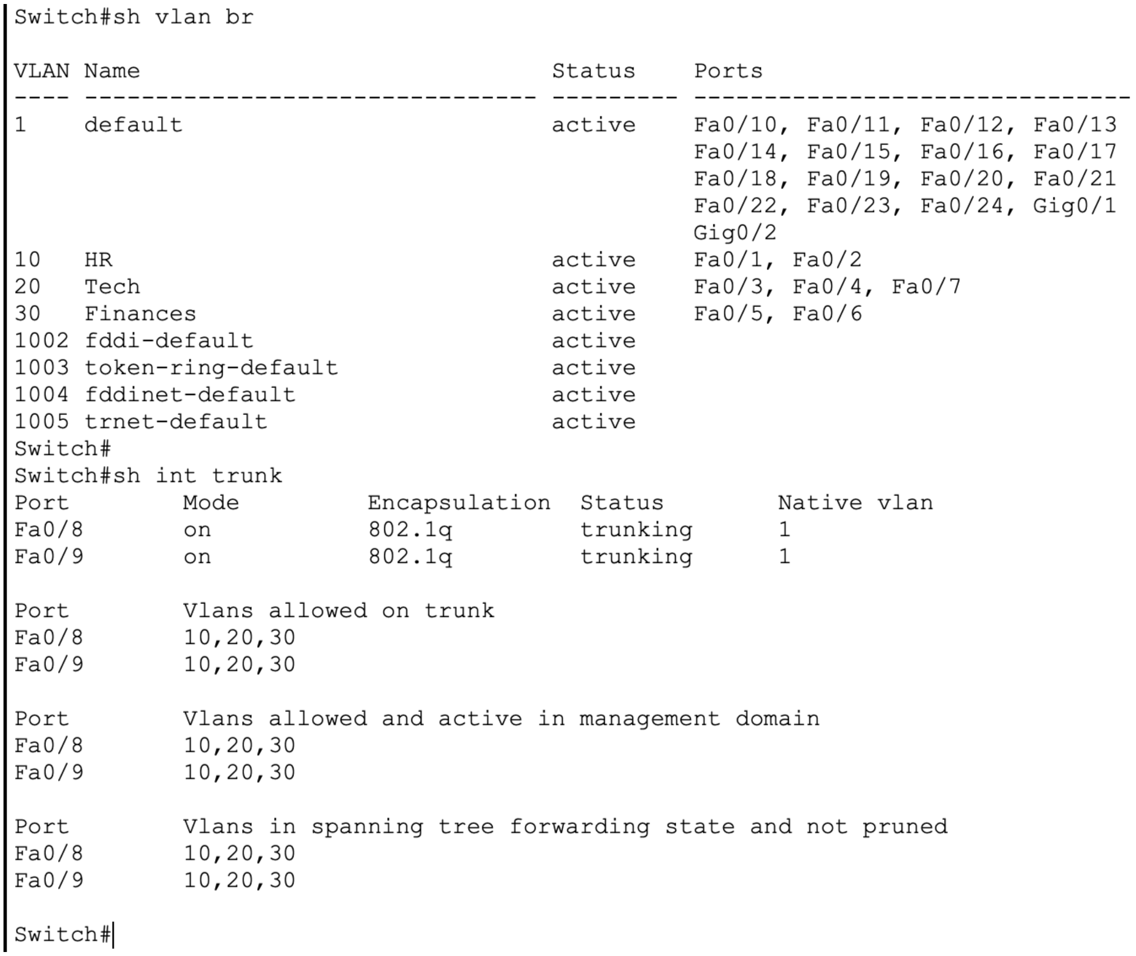
2* Multilayer switch + 9 * 2960 switch = 2*1500+ 9*1500 = 16500

24* PC = 24*1000 = 24000

5* Server = 5*2000 = 10000

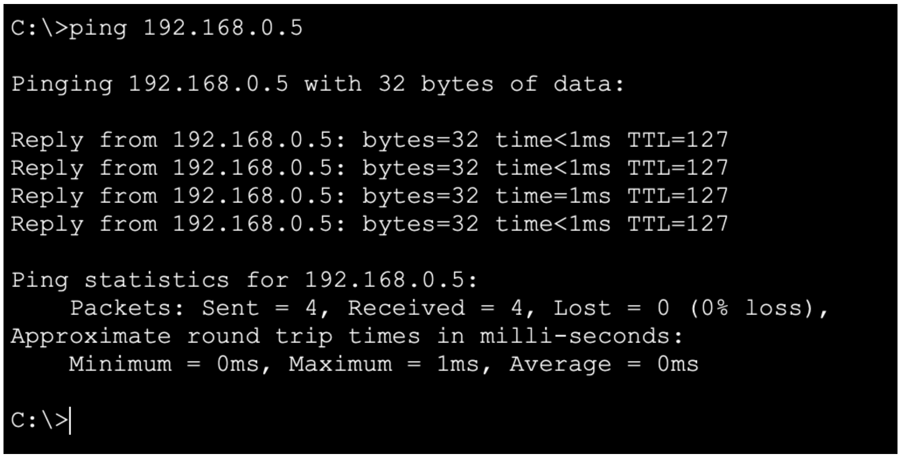
Total Cost = 74,470

Testing VLANs



```
Switch#sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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
20   Tech                             active    Fa0/3, Fa0/4, Fa0/7
30   Finances                         active    Fa0/5, Fa0/6
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
Switch#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/8       on           802.1q         trunking      1
Fa0/9       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/8       10,20,30
Fa0/9       10,20,30

Port        Vlans allowed and active in management domain
Fa0/8       10,20,30
Fa0/9       10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/8       10,20,30
Fa0/9       10,20,30

Switch#
```

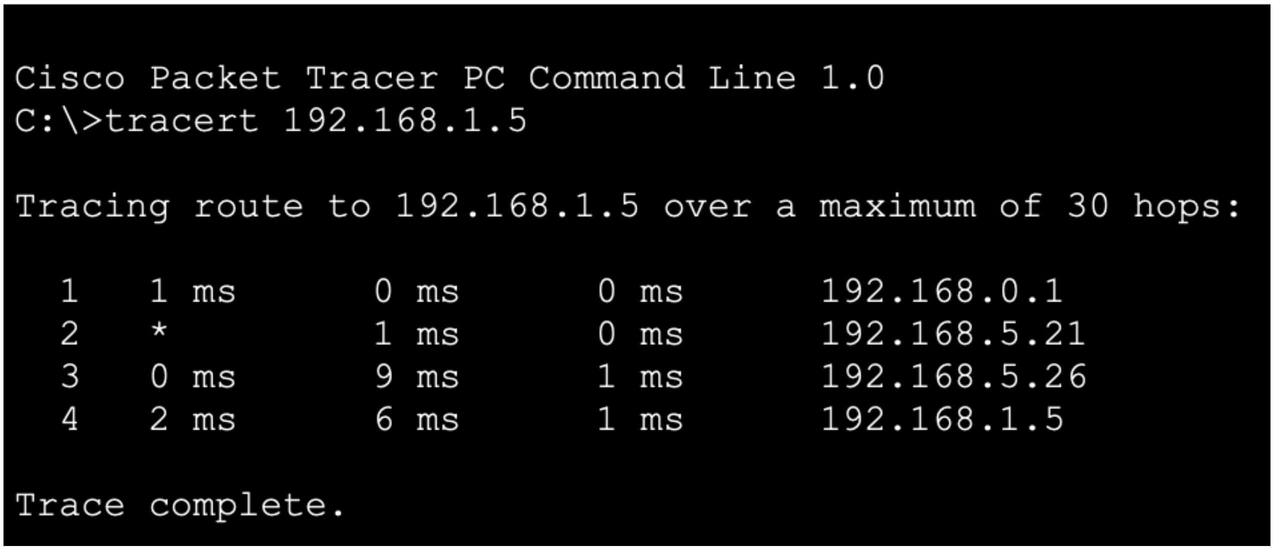
Pinging from Finance to Hr both are on different VLANS



```
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=127
Reply from 192.168.0.5: bytes=32 time<1ms TTL=127
Reply from 192.168.0.5: bytes=32 time=1ms TTL=127
Reply from 192.168.0.5: bytes=32 time<1ms TTL=127

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 = 1ms, Average = 0ms

C:\>
```

Testing Routing Protocol

OSPF



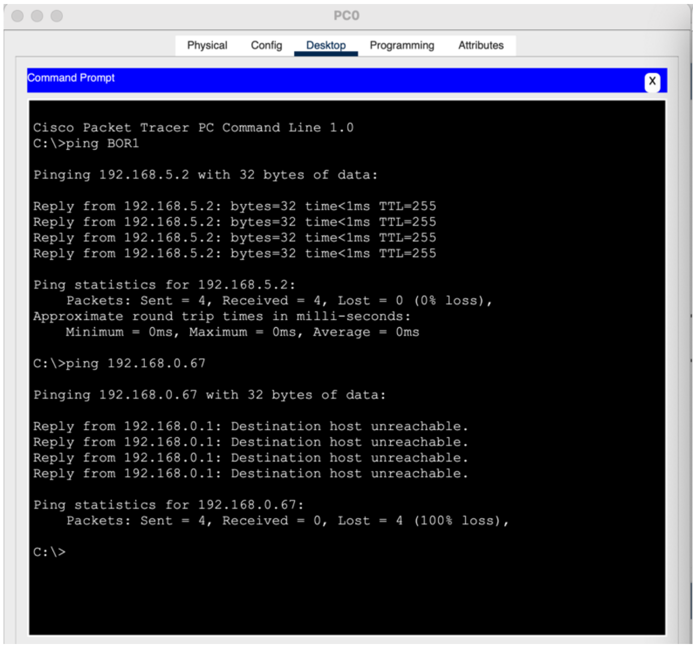
```
Cisco Packet Tracer PC Command Line 1.0
C:\>tracert 192.168.1.5

Tracing route to 192.168.1.5 over a maximum of 30 hops:

  1   1 ms      0 ms      0 ms      192.168.0.1
  2   *         1 ms      0 ms      192.168.5.21
  3   0 ms      9 ms      1 ms      192.168.5.26
  4   2 ms      6 ms      1 ms      192.168.1.5

Trace complete.
```

```
CNTRL#sh ip ospf neigh


Neighbor ID     Pri   State           Dead Time   Address
Interface
1.1.1.1           0   FULL/  -        00:00:37    192.168.5.2
Serial0/0/0
2.2.2.2           0   FULL/  -        00:00:36    192.168.5.6
Serial0/0/1
5.5.5.5           0   FULL/  -        00:00:37    192.168.5.18
Serial0/1/0
4.4.4.4           0   FULL/  -        00:00:37    192.168.5.14
Serial0/1/1
3.3.3.3           0   FULL/  -        00:00:37    192.168.5.10
Serial0/2/0
7.7.7.7           0   FULL/  -        00:00:37    192.168.5.22
Serial0/3/0
8.8.8.8           0   FULL/  -        00:00:37    192.168.5.26
Serial0/3/1
```

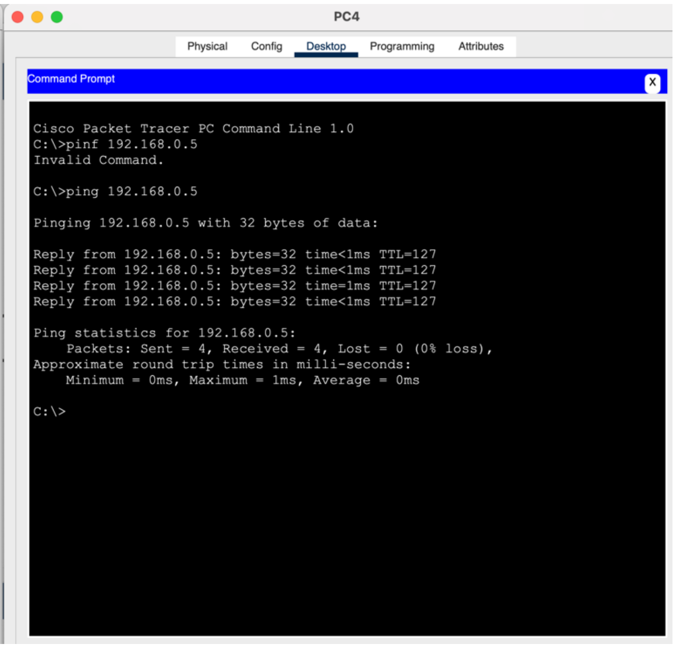
EIGRP is Mentioned In BONUS Part

Test security plan

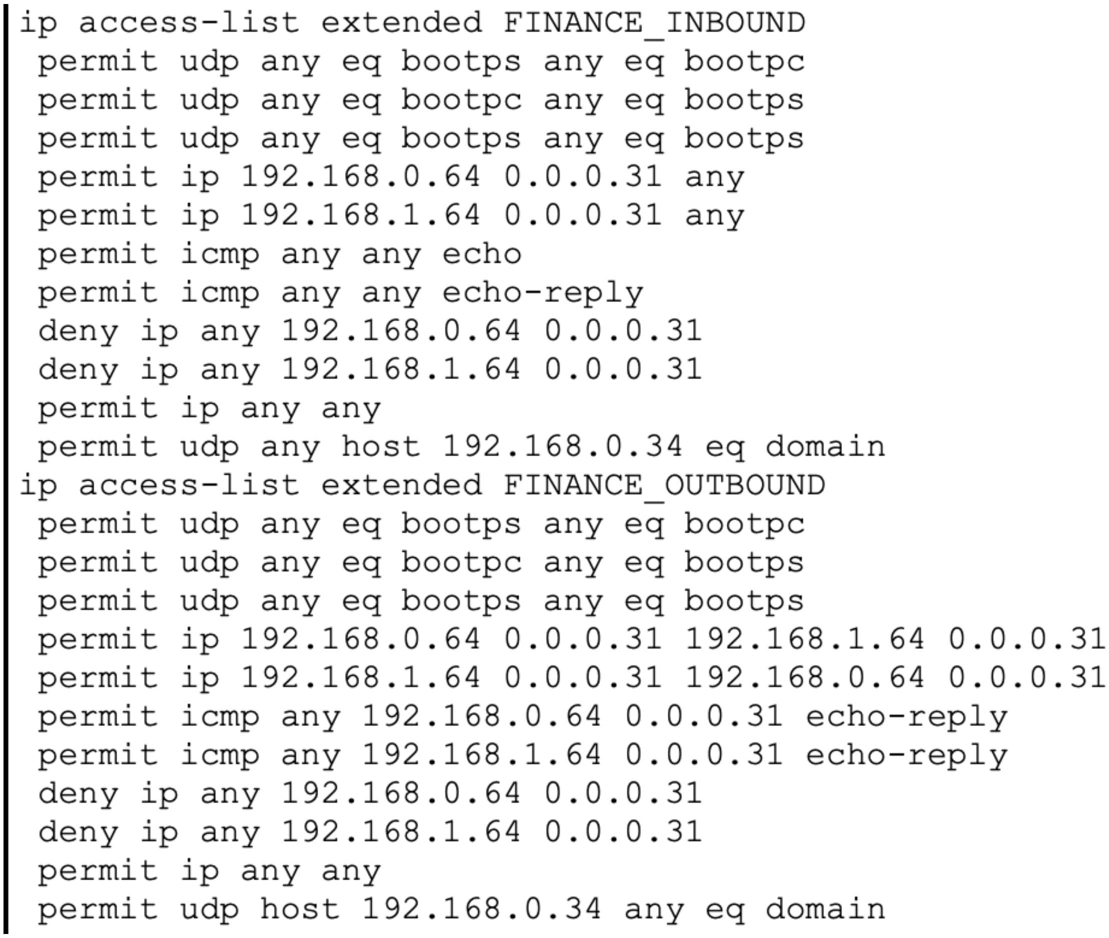
Here I pinged HR to Finance and Finance to HR we can see that when HR pc sends a packet to Finance Pc packet drops and it's not reachable



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping BOR1

Pinging 192.168.5.2 with 32 bytes of data:

Reply from 192.168.5.2: bytes=32 time<1ms TTL=255
Reply from 192.168.5.2: bytes=32 time<1ms TTL=255
Reply from 192.168.5.2: bytes=32 time<1ms TTL=255
Reply from 192.168.5.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.5.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.0.67

Pinging 192.168.0.67 with 32 bytes of data:

Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.

Ping statistics for 192.168.0.67:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

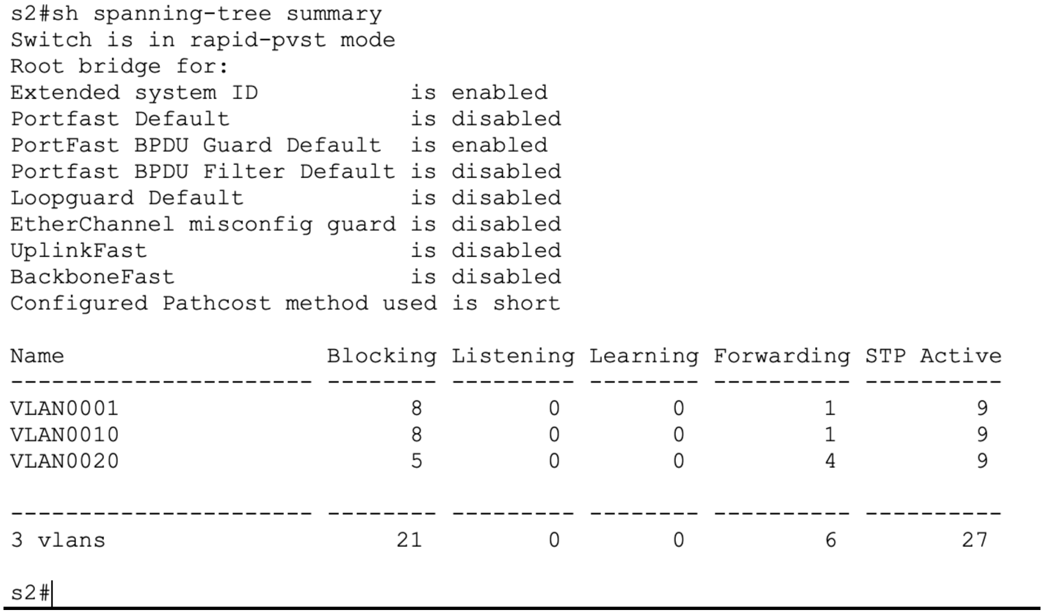


```
Cisco Packet Tracer PC Command Line 1.0
C:\>pinf 192.168.0.5
Invalid Command.

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=127
Reply from 192.168.0.5: bytes=32 time<1ms TTL=127
Reply from 192.168.0.5: bytes=32 time=1ms TTL=127
Reply from 192.168.0.5: bytes=32 time<1ms TTL=127

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 = 1ms, Average = 0ms

C:\>
```



```
ip access-list extended FINANCE_INBOUND
 permit udp any eq bootps any eq bootpc
 permit udp any eq bootpc any eq bootps
 permit udp any eq bootps any eq bootps
 permit ip 192.168.0.64 0.0.0.31 any
 permit ip 192.168.1.64 0.0.0.31 any
 permit icmp any any echo
 permit icmp any any echo-reply
 deny ip any 192.168.0.64 0.0.0.31
 deny ip any 192.168.1.64 0.0.0.31
 permit ip any any
 permit udp any host 192.168.0.34 eq domain
ip access-list extended FINANCE_OUTBOUND
 permit udp any eq bootps any eq bootpc
 permit udp any eq bootpc any eq bootps
 permit udp any eq bootps any eq bootps
 permit ip 192.168.0.64 0.0.0.31 192.168.1.64 0.0.0.31
 permit ip 192.168.1.64 0.0.0.31 192.168.0.64 0.0.0.31
 permit icmp any 192.168.0.64 0.0.0.31 echo-reply
 permit icmp any 192.168.1.64 0.0.0.31 echo-reply
 deny ip any 192.168.0.64 0.0.0.31
 deny ip any 192.168.1.64 0.0.0.31
 permit ip any any
 permit udp host 192.168.0.34 any eq domain
```

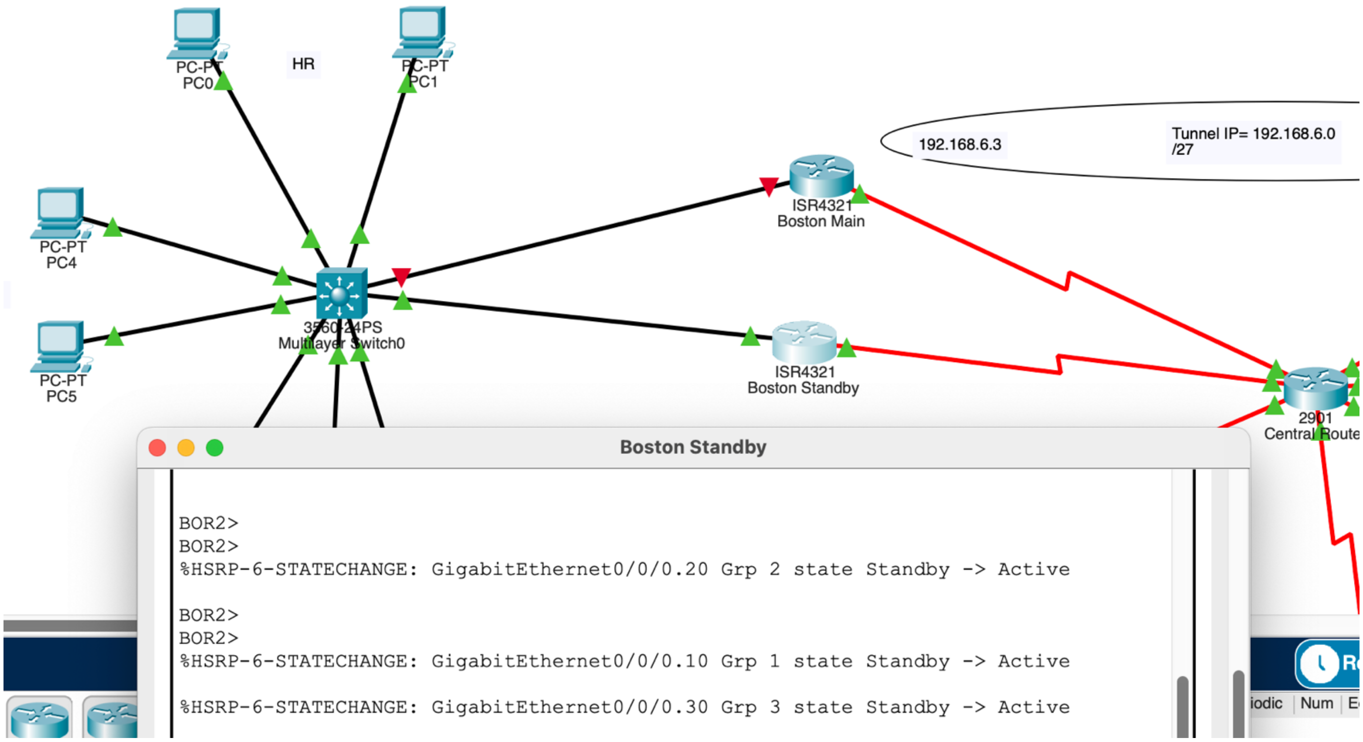
Enable Port fast and BPDU guard on all the ports that are connected to the host machine



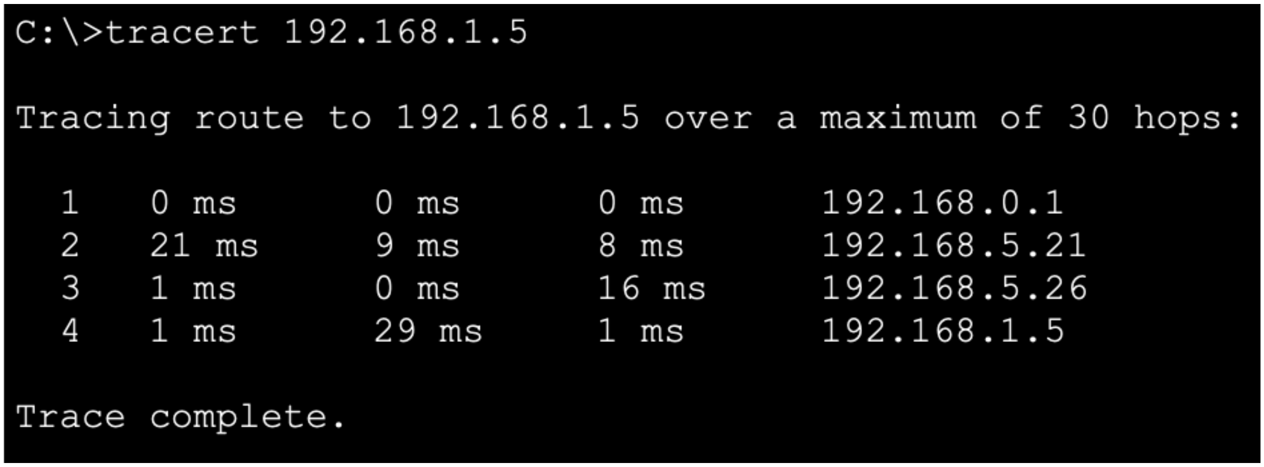
```
s2#sh spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for:
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                     8         0        0          1          9
VLAN0010                     8         0        0          1          9
VLAN0020                     5         0        0          4          9

---------------------- -------- --------- -------- ---------- ----------
3 vlans                     21         0        0          6         27

s2#
```

Test redundancy plan

When a Router Fails the Backup Router Becomes Active Configured Using HSRP. Here we turned off the main router we can see the backup router became active



```
BOR2>
BOR2>
%HSRP-6-STATECHANGE: GigabitEthernet0/0/0.20 Grp 2 state Standby -> Active

BOR2>
BOR2>
%HSRP-6-STATECHANGE: GigabitEthernet0/0/0.10 Grp 1 state Standby -> Active

%HSRP-6-STATECHANGE: GigabitEthernet0/0/0.30 Grp 3 state Standby -> Active
```

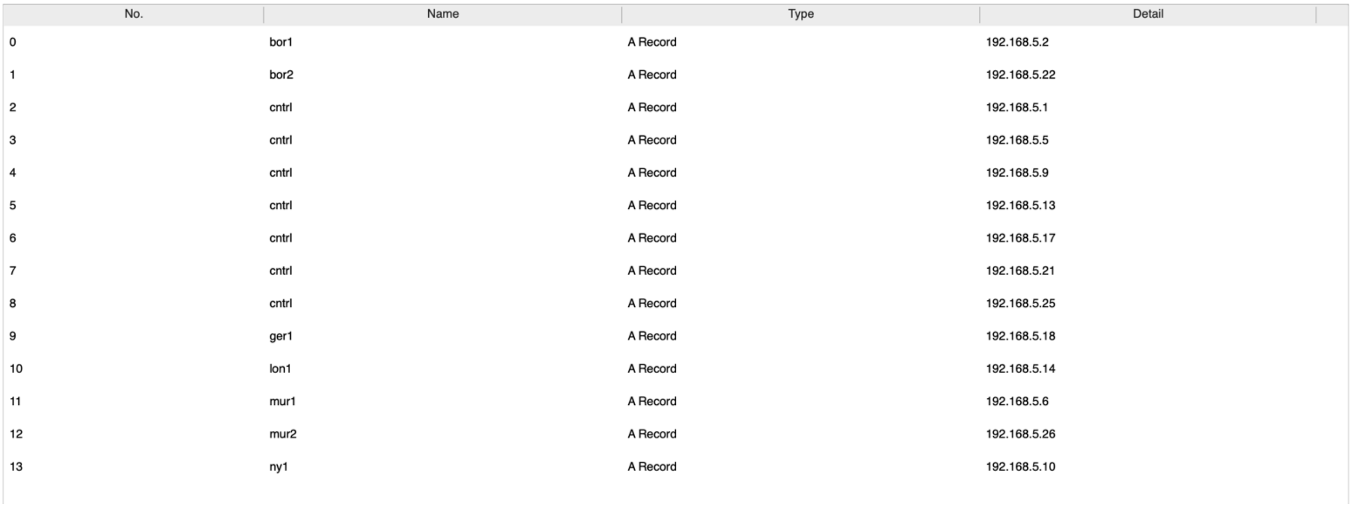


```
C:\>tracert 192.168.1.5

Tracing route to 192.168.1.5 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.0.1
  2   21 ms     9 ms      8 ms      192.168.5.21
  3   1 ms      0 ms      16 ms     192.168.5.26
  4   1 ms      29 ms     1 ms      192.168.1.5

Trace complete.
```

Implement Rapid STP and switch redundancy for Germany, London, and New York office

```
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    24586
             Address     0001.9744.1EC0
             Cost        12
             Port        27(Port-channel2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28682  (priority 28672 sys-id-ext 10)
             Address     00D0.FFB6.3935
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po2              Root FWD 12        128.27   Shr
Po3              Altn BLK 12        128.28   Shr

VLAN0020
  Spanning tree enabled protocol rstp
  Root ID    Priority    24596
             Address     0001.9744.1EC0
             Cost        12
             Port        27(Port-channel2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28692  (priority 28672 sys-id-ext 20)
             Address     00D0.FFB6.3935
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Po2              Root FWD 12        128.27   Shr
Po3              Altn BLK 12        128.28   Shr
```

DNS Server



No.	Name	Type	Detail
0	bor1	A Record	192.168.5.2
1	bor2	A Record	192.168.5.22
2	cntrl	A Record	192.168.5.1
3	cntrl	A Record	192.168.5.5
4	cntrl	A Record	192.168.5.9
5	cntrl	A Record	192.168.5.13
6	cntrl	A Record	192.168.5.17
7	cntrl	A Record	192.168.5.21
8	cntrl	A Record	192.168.5.25
9	ger1	A Record	192.168.5.18
10	lon1	A Record	192.168.5.14
11	mur1	A Record	192.168.5.6
12	mur2	A Record	192.168.5.26
13	ny1	A Record	192.168.5.10

BONUS

Defend against MAC flooding attack

MAC flooding attack targets a switch by overwhelming its MAC table, forcing it to act like a hub

a. Enable port security, which limits the total number of addresses a switch learns, & if a limit is passed, told to do something (shut down…)

i. switchport port-security

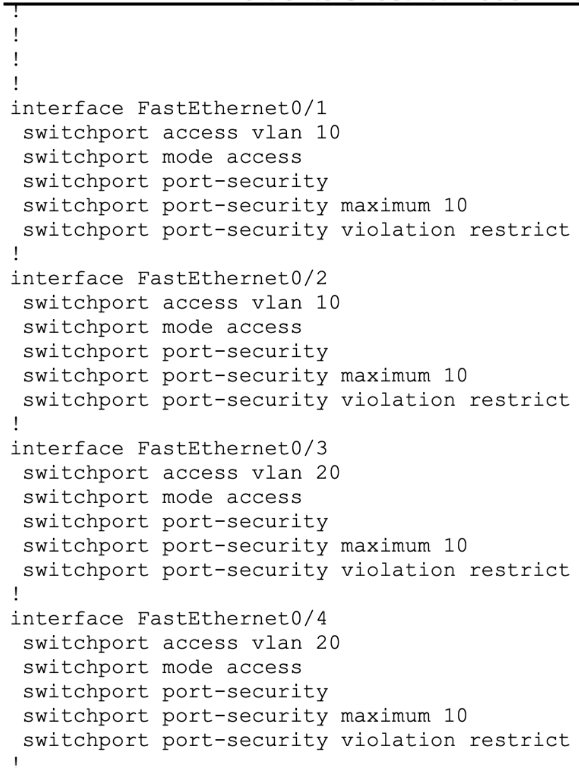
1. Enables port security on the interface

ii. switchport port-security maximum 10

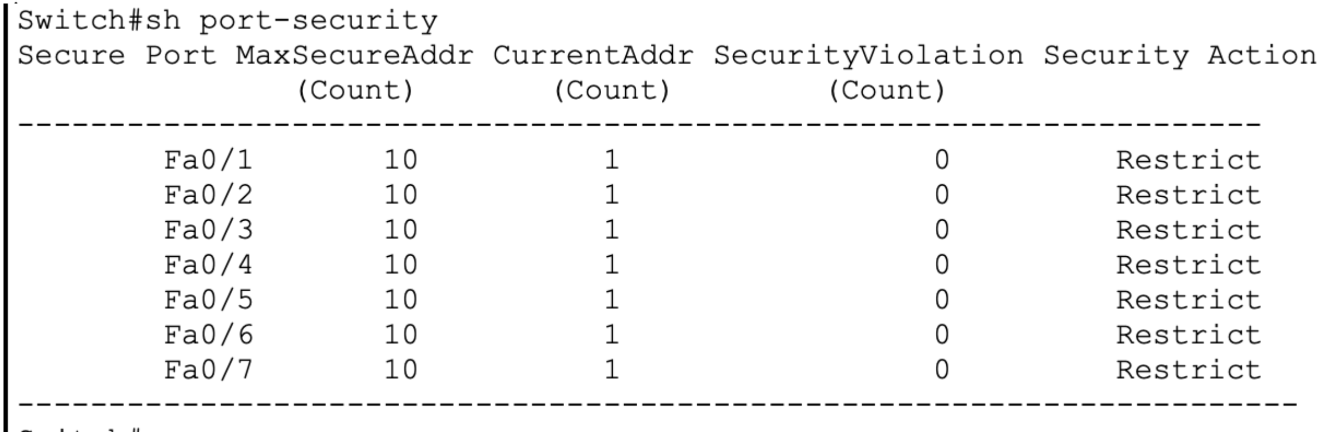
1. Limits the number of dynamically learned MAC addresses to two

iii. switchport port security violation restrict

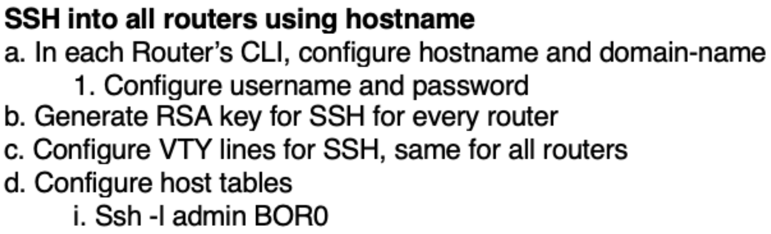
1. Port enters restrict mode *if* specific violations are found



```
!
!
!
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 10
 switchport port-security violation restrict
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 10
 switchport port-security violation restrict
!
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security maximum 10
 switchport port-security violation restrict
!
interface FastEthernet0/4
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security maximum 10
 switchport port-security violation restrict
!
```

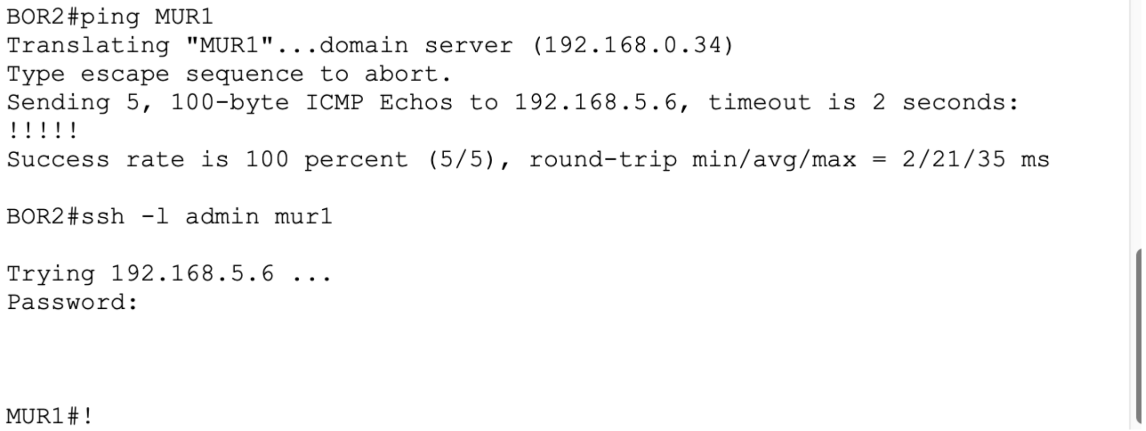


```
Switch#sh port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)          (Count)
----------------------------------------------------------------------
        Fa0/1        10           1                 0         Restrict
        Fa0/2        10           1                 0         Restrict
        Fa0/3        10           1                 0         Restrict
        Fa0/4        10           1                 0         Restrict
        Fa0/5        10           1                 0         Restrict
        Fa0/6        10           1                 0         Restrict
        Fa0/7        10           1                 0         Restrict
------------------------------------------------------------------------
Switch#
```

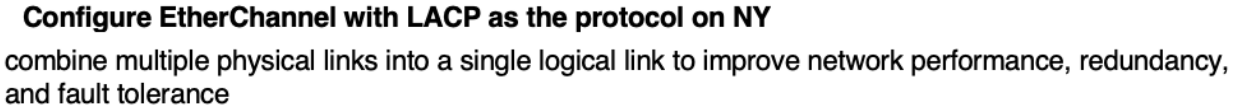


SSH into all routers using hostname

a. In each Router's CLI, configure hostname and domain-name
  1. Configure username and password
b. Generate RSA key for SSH for every router
c. Configure VTY lines for SSH, same for all routers
d. Configure host tables
  i. Ssh -l admin BOR0

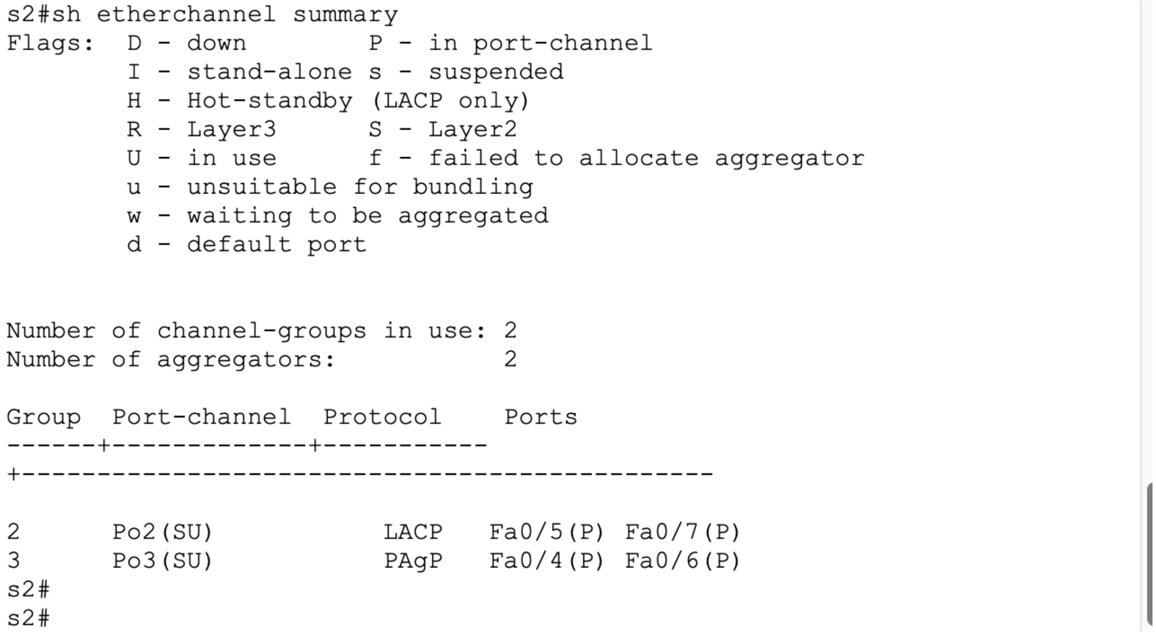


```
BOR2#ping MUR1
Translating "MUR1"...domain server (192.168.0.34)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/21/35 ms

BOR2#ssh -l admin mur1

Trying 192.168.5.6 ...
Password:



MUR1#!
```



Configure EtherChannel with LACP as the protocol on NY

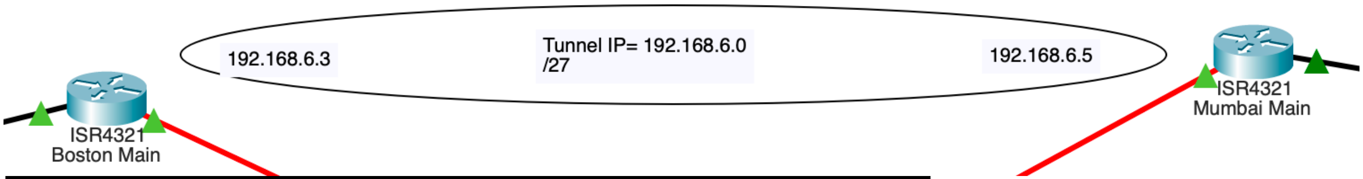
combine multiple physical links into a single logical link to improve network performance, redundancy, and fault tolerance

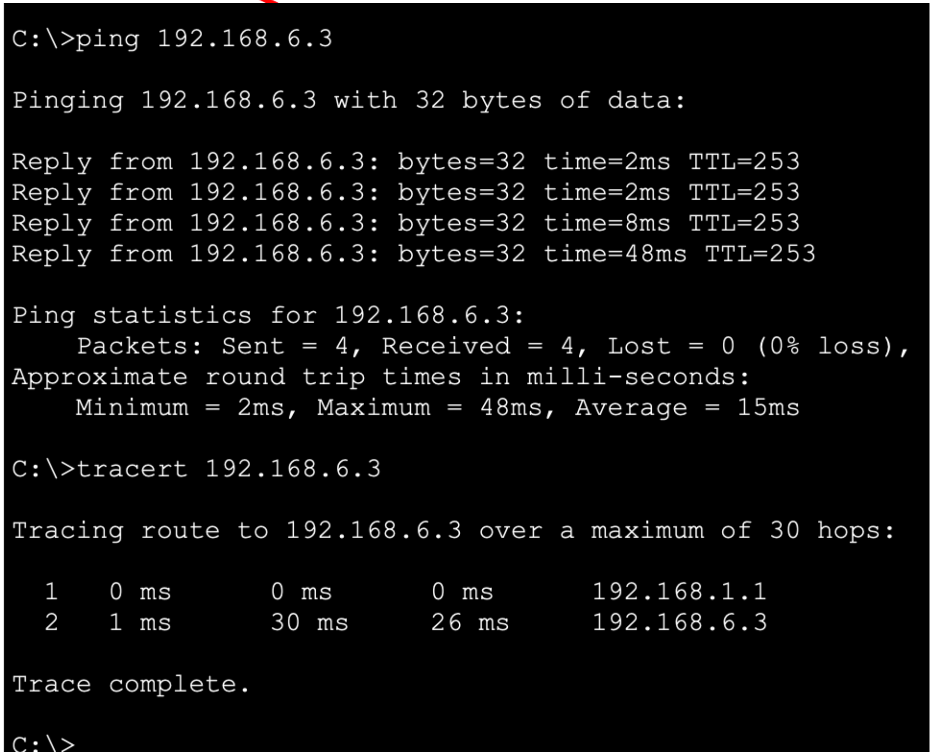


```
s2#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

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

2      Po2(SU)           LACP   Fa0/5(P) Fa0/7(P)
3      Po3(SU)           PAgP   Fa0/4(P) Fa0/6(P)
s2#
s2#
```

Configure VPN tunnel between 2 HQs Boston & Mumbai

used to create a secure, private communication channel over a public or untrusted network



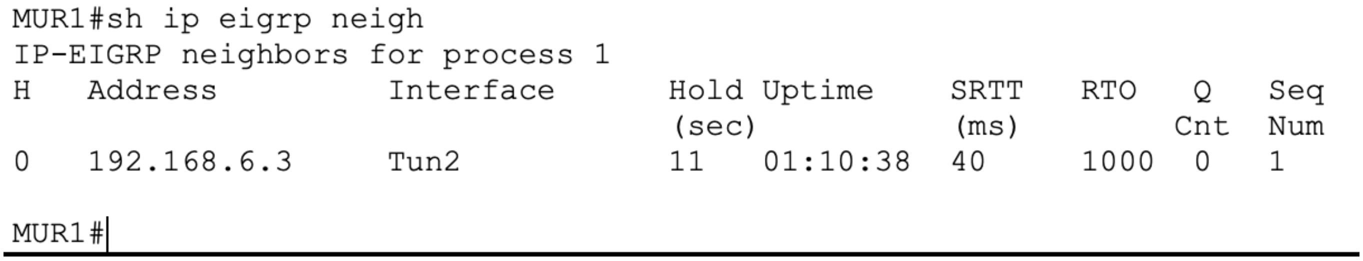


```
C:\>ping 192.168.6.3

Pinging 192.168.6.3 with 32 bytes of data:

Reply from 192.168.6.3: bytes=32 time=2ms TTL=253
Reply from 192.168.6.3: bytes=32 time=2ms TTL=253
Reply from 192.168.6.3: bytes=32 time=8ms TTL=253
Reply from 192.168.6.3: bytes=32 time=48ms TTL=253

Ping statistics for 192.168.6.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 48ms, Average = 15ms

C:\>tracert 192.168.6.3

Tracing route to 192.168.6.3 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.1.1
  2   1 ms      30 ms     26 ms     192.168.6.3

Trace complete.

C:\>
```

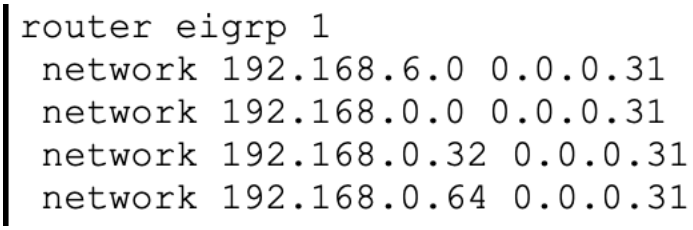
Configure EIGRP on these 2 routers

used on a VPN tunnel to optimize routing within the network and ensure seamless communication between connected sites.

s



```
MUR1#sh ip eigrp neigh
IP-EIGRP neighbors for process 1
H   Address          Interface        Hold Uptime    SRTT    RTO   Q    Seq
                                      (sec)          (ms)          Cnt  Num
0   192.168.6.3      Tun2             11   01:10:38  40      1000  0    1

MUR1#
```



```
router eigrp 1
 network 192.168.6.0 0.0.0.31
 network 192.168.0.0 0.0.0.31
 network 192.168.0.32 0.0.0.31
 network 192.168.0.64 0.0.0.31
```

Conclusion:

This project successfully implements a comprehensive enterprise network topology that integrates modern networking technologies to ensure scalability, security, and high availability.

Key takeaways include:

1 . **Efficient Network Design**:

- VLANs for isolating Finance, HR, and technical departments, enhancing security and traffic management.
- Subnetting for optimized IP address allocation.

Dynamic Routing Protocols:

- OSPF for inter-area routing and EIGRP for enhanced convergence and flexibility in certain offices.
- VPN tunnels for secure communication between offices over public networks.

High Availability and Redundancy:

- HSRP ensures seamless router failover in case of a primary router failure.
- STP prevents Layer 2 loops in redundant link scenarios.
- LACP in the London office ensures efficient load balancing and link aggregation for critical operations.

Automation and Security:

- DHCP automates IP address assignments.
- ACLs regulate traffic flow, permitting or denying communication based on organizational policies.
- SSH enables secure remote login and management of routers, improving administrative efficiency while maintaining security.

This network topology ensures a robust, efficient, and secure infrastructure capable of meeting the demands of a dynamic and scalable enterprise environment.