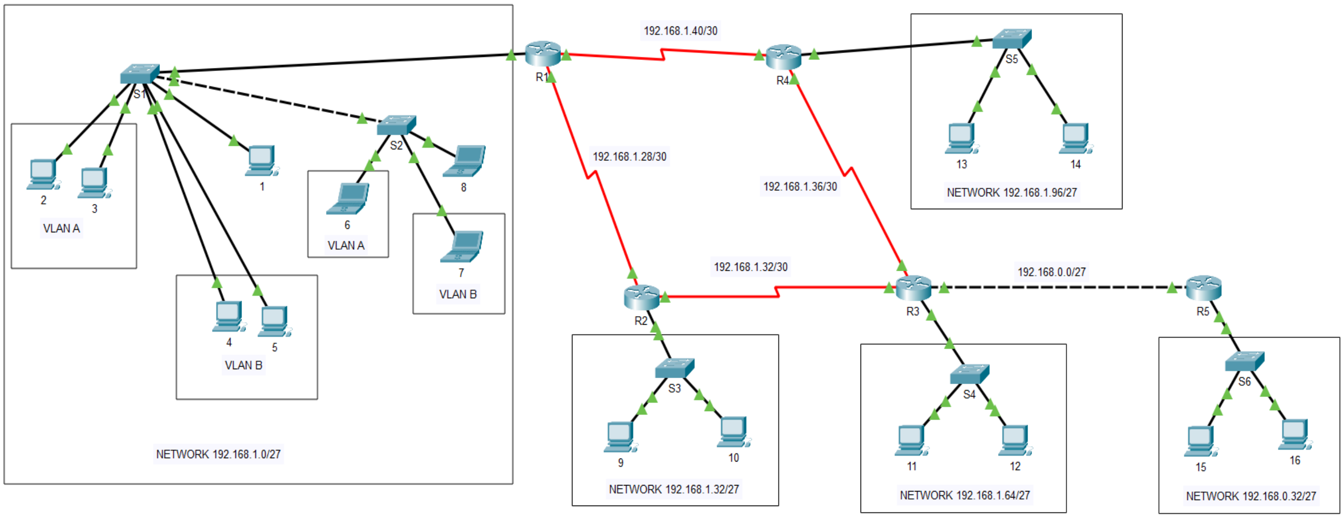
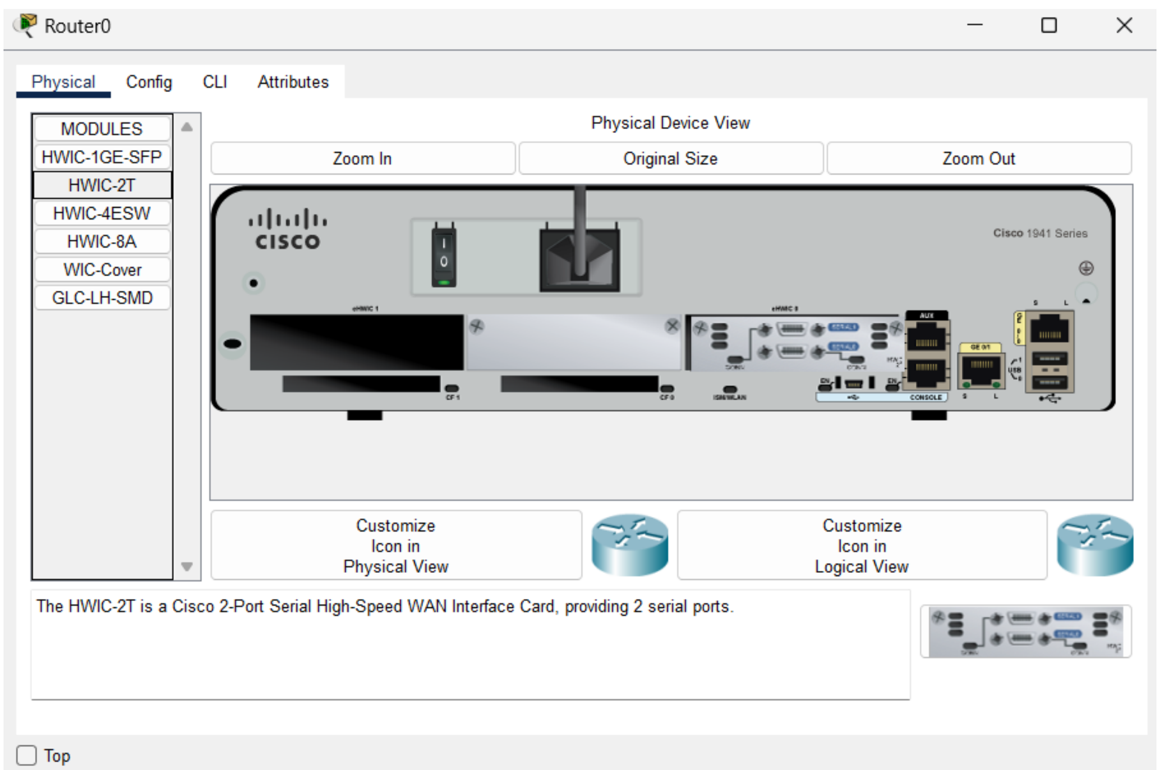
NETWORK CONFIGURATION AND SECURITY IMPLEMENTATION

We have established a network comprising 5 routers interconnected with switches. Each switch is connected to multiple PCs, accommodating up to 30 hosts per switch. The routers are interconnected using Serial DTE connections to ensure reliable communication. All connections, except those between switches which utilize crossover cables, are made using straight-through Ethernet cables. In addition to configuring OSPF, RIP, DHCP services, and securing router access with passwords, VLANs have been deployed across the network. This segmentation optimizes network performance and management by isolating broadcast domains. Robust security measures and efficient traffic management policies complement these configurations, collectively enhancing network reliability and security. We partition the network into 10 subnetworks as shown in the table below.

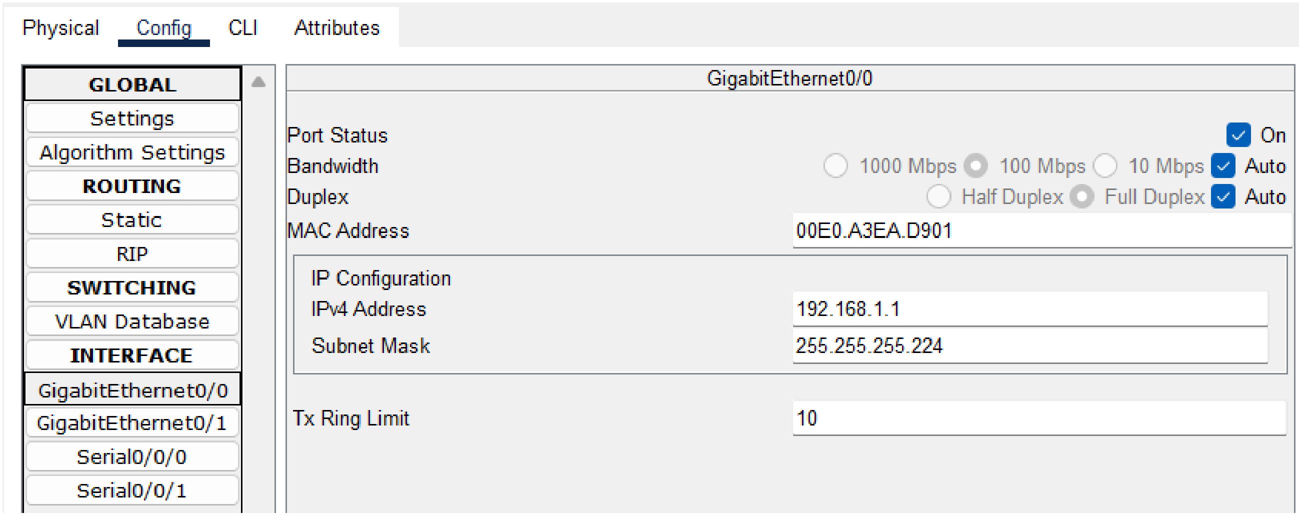
N/W	No. of Hosts	Subnet Mask	Network ID	Valid Hosts	Broadcast ID
N1	30	255.255.255.224	192.168.1.0	192.168.1.1 - 192.168.1.30	192.168.1.31
N2	30	255.255.255.224	192.168.1.32	192.168.1.33 - 192.168.1.62	192.168.1.63
N3	30	255.255.255.224	192.168.1.64	192.168.1.65 - 192.168.1.94	192.168.1.95
N4	30	255.255.255.224	192.168.1.96	192.168.1.97 - 192.168.1.126	192.168.1.127
N5	2	255.255.255.252	192.168.1.128	192.168.1.129 - 192.168.1.130	192.168.1.131
N6	2	255.255.255.252	192.168.1.132	192.168.1.133 - 192.168.1.134	192.168.1.135
N7	2	255.255.255.252	192.168.1.136	192.168.1.137 - 192.168.1.138	192.168.1.139
N8	2	255.255.255.252	192.168.1.140	192.168.1.141 - 192.168.1.142	192.168.1.143
N9	30	255.255.255.224	192.168.0.0	192.168.0.1 - 192.168.0.30	192.168.0.31
N10	30	255.255.255.224	192.168.0.32	192.168.0.33 - 192.168.0.62	192.168.0.63

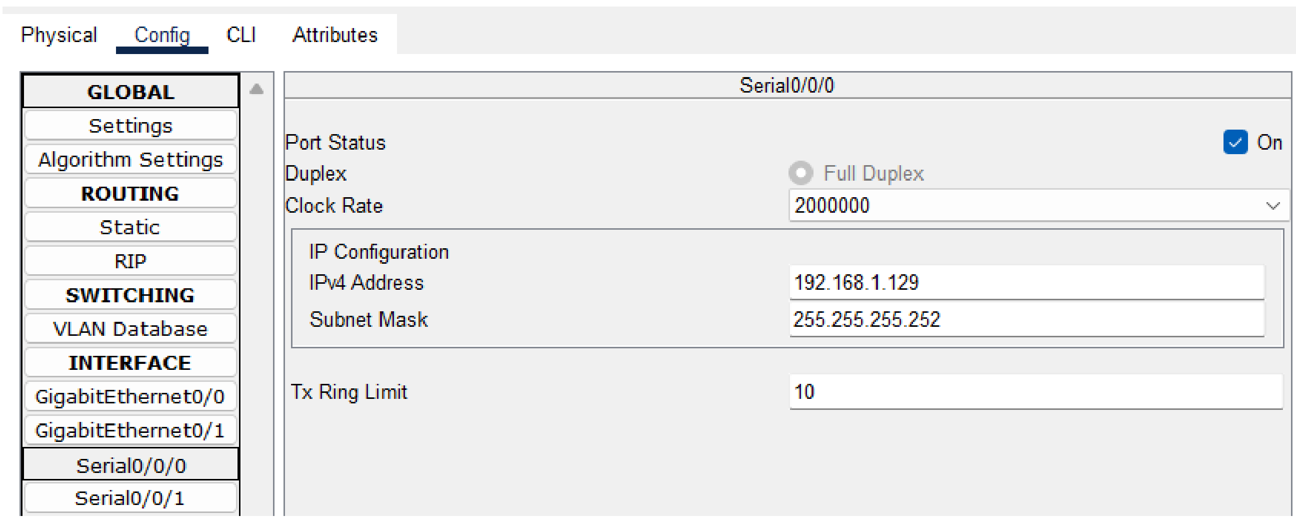


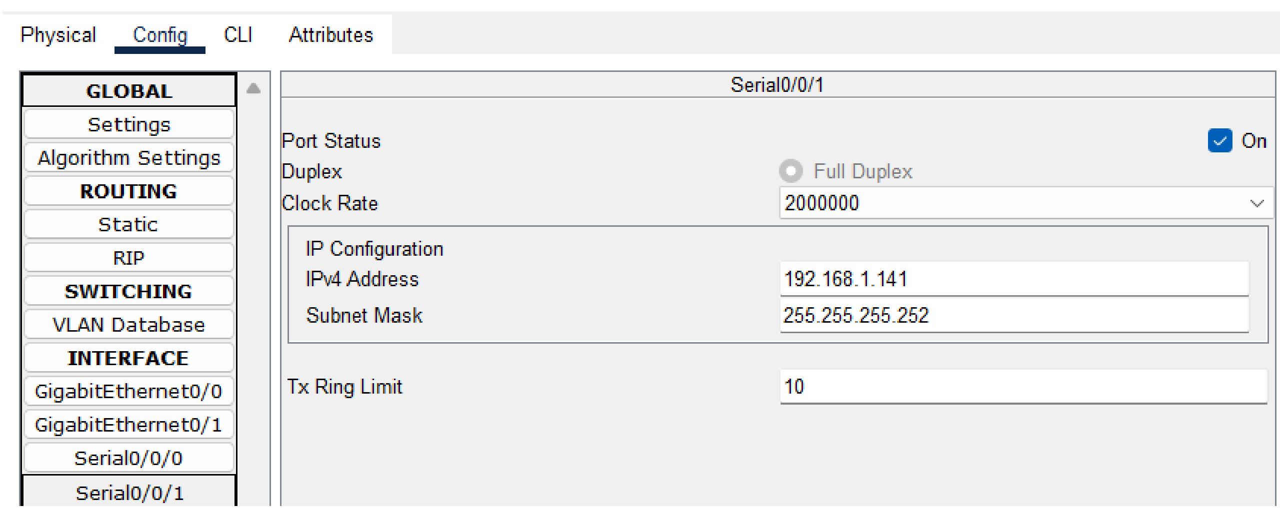
We then physically turned off the router, and turned it on after adding the serial communication module to each of the routers as shown in the figure below.



Then we allocated the valid host addresses to the respective gigabit ethernet interfaces. The addresses with two hosts were added to the respective serial port addresses as shown in the figures below.







Similarly, we configured host addresses for each Gigabit Ethernet interface across all routers according to our network setup. Each router's serial port addresses were also assigned addresses corresponding to their respective host configurations, ensuring consistency and functionality across the network infrastructure.

Then we dynamically allocated the IP addresses to the hosts in each network using DHCP.

In router 1,

Router(config)#ip dhcp pool lab
Router(dhcp-config)#network 192.168.1.0 255.255.255.224
Router(dhcp-config)#default-router 192.168.1.1

In router 2,

Router(config)#ip dhcp pool lab
Router(dhcp-config)#network 192.168.1.32 255.255.255.224
Router(dhcp-config)#default-router 192.168.1.33

In router 3,

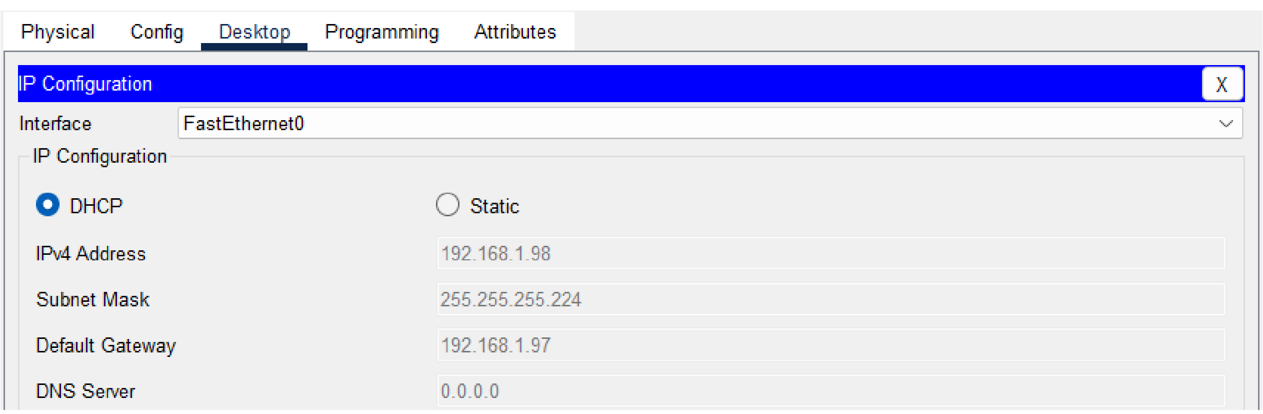
Router(config)#ip dhcp pool lab
Router(dhcp-config)#network 192.168.1.64 255.255.255.224
Router(dhcp-config)#default-router 192.168.1.65

In router 4,

Router(config)#ip dhcp pool lab
Router(dhcp-config)#network 192.168.1.96 255.255.255.224
Router(dhcp-config)#default-router 192.168.1.97

In router 5,

Router(config)#ip dhcp pool lab
Router(dhcp-config)#network 192.168.0.32 255.255.255.224
Router(dhcp-config)#default-router 192.168.0.33



We configured VLANs in a network consisting of Router1, which is connected to two switches. Switch1 has five PCs connected, with two PCs assigned to VLAN A and two PCs assigned to VLAN B. The remaining PC on Switch1 is not part of any VLAN. Switch2, also connected to Router1, has two PCs, with one PC assigned to VLAN A and the other to VLAN B. Also, we enable trunk mode to allow traffic from multiple VLANs (VLAN A and VLAN B) to pass between Switch1 and Switch2 over a single physical connection. This enables devices in the same VLAN but connected to different switches to communicate seamlessly.

In switch 1,

Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name A
Switch(config-vlan)# vlan 20
Switch(config-vlan)# name B
Switch(config-vlan)# exit

Switch(config)# int range fa0/1 -fa0/5
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config)# int range fa0/6 -fa0/10
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config)# int range fa0/23
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/24, Gig0/1, Gig0/2
10   A                                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5
20   B                                active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10
```

In switch 2,

Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name A
Switch(config-vlan)# vlan 20
Switch(config-vlan)# name B
Switch(config-vlan)# exit

Switch(config)# int range fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config)# int range fa0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config)# int range fa0/23
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, 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
                                                Fa0/24, Gig0/1, Gig0/2
10   A                                active    Fa0/1
20   B                                active    Fa0/2
```

We have implemented various security measures across our routers. Router1 now uses encrypted passwords for enhanced security. Router2 has also been configured with encrypted passwords. In addition to this, Router3 has a console password set up to restrict access further, while Router4 has a password configured specifically for telnet access. These steps aim to bolster our network's overall security posture.

First, we setup **unencrypted password** in router 1,

Router> enable
Router# configure terminal
Router(config)# enable password password1
Router(config)# exit

Router>enable
Password:
Router#sh run
Building configuration...
Current configuration : 933 bytes
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
enable password password1

Then, we setup **encrypted password** in router 2,

Router> enable
Router# configure terminal
Router(config)# enable secret password2
Router(config)# exit

Router>enable
Password:
Router#sh run
Building configuration...
Current configuration : 957 bytes
version 15.1
no service timestamps log datetime msec

no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
*enable secre*t 5 1mERr$30voUYZTo/LCMhf7ue69/0

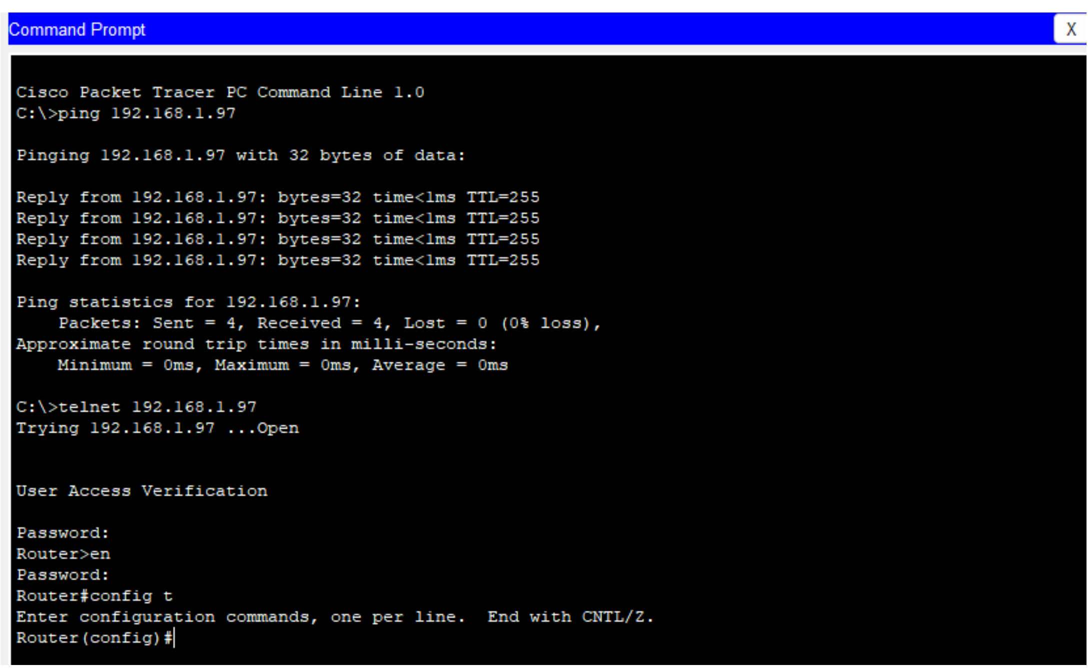
Similarly, we setup **console password** in router 3,

Router> enable
Router# configure terminal
Router(config)# line console 0
Router(config)# password password3
Router(config)# login
Router(config)# exit
User Access Verification
Password:
Router>

Lastly, we setup **telnet password** in router 4,

Router> enable
Router# configure terminal
Router(config)# line vty 0
Router(config)# password password4
Router(config)# login
Router(config)# exit

Before setting up Telnet, direct physical access to network devices like routers was required for configuration and management. After setting up Telnet, remote access becomes possible, allowing administrators to manage devices from any location on the network, thereby improving flexibility and operational efficiency.



We then used RIP to dynamically route the communication path among PCs in different sub-networks for Routers 1, 2, 3 and 4.

In router 1,

Router enable
Router# config t
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 192.168.0.0
Router(config-router)# network 192.168.0.128
Router(config-router)# network 192.168.0.140

In router 2,

Router enable
Router# config t
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 192.168.0.32
Router(config-router)# network 192.168.0.128
Router(config-router)# network 192.168.0.132

In router 3,

Router enable
Router# config t
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 192.168.0.64
Router(config-router)# network 192.168.0.132
Router(config-router)# network 192.168.0.136

In router 4,

Router enable
Router# config t
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 192.168.0.96
Router(config-router)# network 192.168.0.136
Router(config-router)# network 192.168.0.140

For Routers 3 and 5, we used OSPF to achieve dynamic routing between PCs in different sub-networks.

In router 3,

Router#enable
Router#config t
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.64 0.0.0.31 area 0
Router(config-router)#network 192.168.1.132 0.0.0.3 area 0
Router(config-router)#network 192.168.1.136 0.0.0.3 area 0
Router(config-router)#network 192.168.0.0 0.0.0.31 area 0

In router 5,

Router#enable
Router#config t
Router(config)#router ospf 1
Router(config-router)#network 192.168.0.0 0.0.0.31 area 0
Router(config-router)#network 192.168.0.32 0.0.0.31 area 0

To redistribute routes between OSPF and RIP, choose Router 3, which is connected to both the OSPF and RIP networks. Configure Router 3 to exchange routing information by enabling both OSPF and RIP on it and setting up route redistribution between the two protocols.

Router> enable
Router# configure terminal
Router(config)# router ospf 1
Router(config-router)# redistribute rip subnets
Router(config-router)# exit
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# redistribute OSPF 1 metric 1

CONCLUSION

In our network setup, we implemented VLANs for efficient traffic segmentation and enabled trunking between switches to facilitate seamless communication across VLANs. Dynamic IP allocation via DHCP streamlined address management, while rigorous security measures, including encrypted passwords and access restrictions on routers, bolstered network integrity. Routing was managed through RIP for simpler configurations across most routers, complemented by OSPF for more complex topologies on selected routers. This comprehensive approach ensures robust performance, scalability, and security, meeting both current operational needs and future network expansion requirements effectively.

SCREENSHOTS

- Ping from VLAN A to VLAN A

```
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 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- Ping from VLAN B to VLAN A

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- Tracing route from pc 1 to pc 15

```
C:\>ping 192.168.0.33

Pinging 192.168.0.33 with 32 bytes of data:

Reply from 192.168.0.33: bytes=32 time=18ms TTL=252
Reply from 192.168.0.33: bytes=32 time=13ms TTL=252
Reply from 192.168.0.33: bytes=32 time=2ms TTL=252
Reply from 192.168.0.33: bytes=32 time=18ms TTL=252

Ping statistics for 192.168.0.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 18ms, Average = 12ms

C:\>tracert 192.168.0.33

Tracing route to 192.168.0.33 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.1.1
  2   0 ms      1 ms      1 ms      192.168.1.130
  3   1 ms      0 ms      1 ms      192.168.1.138
  4   0 ms      0 ms      1 ms      192.168.0.33

Trace complete.
```

- Tracing route from pc 16 to pc 13

```
C:\>ping 192.168.1.99

Pinging 192.168.1.99 with 32 bytes of data:

Reply from 192.168.1.99: bytes=32 time=2ms TTL=125
Reply from 192.168.1.99: bytes=32 time=12ms TTL=125
Reply from 192.168.1.99: bytes=32 time=17ms TTL=125
Reply from 192.168.1.99: bytes=32 time=1ms TTL=125

Ping statistics for 192.168.1.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 17ms, Average = 8ms

C:\>tracert 192.168.1.99

Tracing route to 192.168.1.99 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.0.33
  2   0 ms      0 ms      0 ms      192.168.0.2
  3   1 ms      15 ms     1 ms      192.168.1.137
  4   1 ms      0 ms      1 ms      192.168.1.99

Trace complete.
```

- Tracing route from pc 13 to pc 8

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=12ms TTL=126
Reply from 192.168.1.3: bytes=32 time=2ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 12ms, Average = 4ms

C:\>tracert 192.168.1.3

Tracing route to 192.168.1.3 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.1.97
  2   0 ms      1 ms      1 ms      192.168.1.141
  3   0 ms      0 ms      0 ms      192.168.1.3

Trace complete.
```

- Using telnet for remote access

```
Cisco Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.1.97
Trying 192.168.1.97 ...Open


User Access Verification

Password:
Router>en
Password:
Router#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.97            -   000B.BEC5.3901  ARPA   GigabitEthernet0/0
Internet  192.168.1.98          123   0001.6428.AE83  ARPA   GigabitEthernet0/0
Internet  192.168.1.99          123   00E0.F9AB.3BBA  ARPA   GigabitEthernet0/0
Router#
```