SIES College of Arts, Science & Commerce
RISE WITH EDUCATION
NAAC REACCREDITED - 'A' GRADE
ISO 9001 : 2008

S.I.E.S College of Arts, Science and Commerce (Empowered Autonomous)
Sion(W), Mumbai – 400 022.

CERTIFICATE

This is to certify that Miss/Mr Ansari Abu Fahad Ashfaque Ahmed Roll No. FMCS2526096 has successfully completed the necessary course of experiments in the subject of **Software Defined Networking** during the academic year **2025 – 2026** complying with the requirements of **University of Mumbai**, for the course of MSC **CS [Semester- I].**

Asst. Prof. In-Charge
MS. JESICA D'CRUZ

Examination date:

Examiner's Signature & Date: College Seal

Head of Department
DR. MANOJ SINGH

INDEX

Sr. No	Date	Topic
1	12-Aug-2025	Implement IPv4 ACLs 1. Standard 2. Extended
2	14-Aug-2025	Implement SPAN Technologies (Switch Port Analyzer)
3	19-Aug-2025	Implement Inter-VLAN Routing
4	26-Aug-2025	Implement RIP protocol
5	04-Sep-2025	OSPF Implementation 1. Implement Single-Area OSPFv2 2. Implement multi-Area OSPFv2 3. OSPFv2 Route Summarization
6	11-Sep-2025	Implement BGP Communities 1. Implement EBGP 2. Implement IBGP
7.	25-Sep-2025	Implement IPsec Site-to-Site VPNs connections
8	09-Oct-2025	Demonstrate Multilayer switch-based Networking

PRACTICAL NO:1

AIM: Implement IPv4 ACLs
1. Standard
2. Extended

DESCRIPTION:

Access Control Lists (ACLs)

An **Access Control List (ACL)** is a set of rules used in networking devices (like routers) to **control traffic**. ACLs work by permitting or denying packets based on criteria such as source IP, destination IP, protocol, or port numbers. They are used for **traffic filtering, network security, and restricting access**

Uses of ACL:

- Improves network security by restricting unwanted traffic.
- Can allow or block traffic based on:
  - Source IP address
  - Destination IP address
  - Protocol (TCP, UDP, ICMP, etc.)
  - Port numbers
- Helps in traffic management and access restriction.

1) Standard

Standard ACL:

A **Standard Access Control List (ACL)** is the simplest ACL type in Cisco networking. It filters traffic based only on the **source IP address** of the packet. Standard ACLs use numbers **1–99 (or 1300–1999)** and are generally applied **close to the destination** network. They cannot filter by destination address, protocol, or port number.

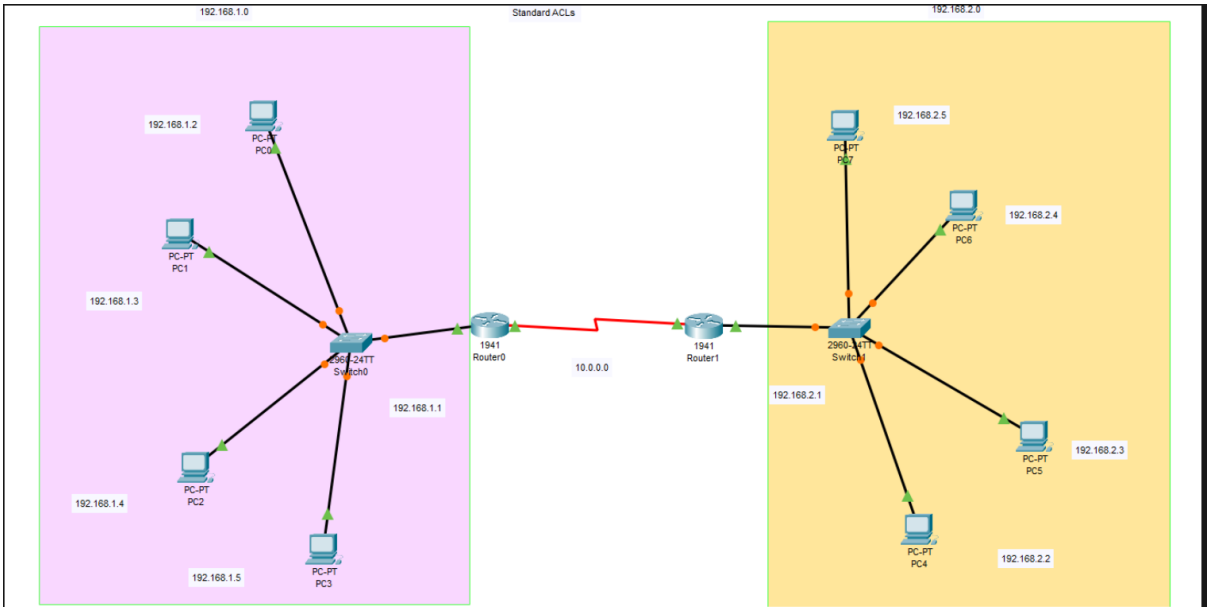
Command format:

ACCESS-LIST <NUMBER> PERMIT / DENY <SOURCE> <WILDCARD-MASK>

After creation, it must be applied to a router interface using:

IP ACCESS-GROUP <NUMBER> IN / OUT

Topology:



Configuration:

1) PC Configuration Table
Go to PC / Desktop / Ip Configuration
Cable Name: Copper Straight-Through

Tables:

PC	IP Address	Subnet Mask	Default Gateway
PC0	192.168.1.2	255.255.255.0	192.168.1.1
PC1	192.168.1.3	255.255.255.0	192.168.1.1
PC2	192.168.1.4	255.255.255.0	192.168.1.1
PC3	192.168.1.5	255.255.255.0	192.168.1.1
PC4	192.168.2.2	255.255.255.0	192.168.2.1
PC5	192.168.2.3	255.255.255.0	192.168.2.1
PC6	192.168.2.4	255.255.255.0	192.168.2.1
PC7	192.168.2.5	255.255.255.0	192.168.2.1

2) Router Configuration Table
Go to Router / Config:
Cable Name: Serial DTE
Add this '**HWIC-2T'** Each Router (HWIC-2T = High-Speed WAN Interface Card (2T = 2 Serial Ports)

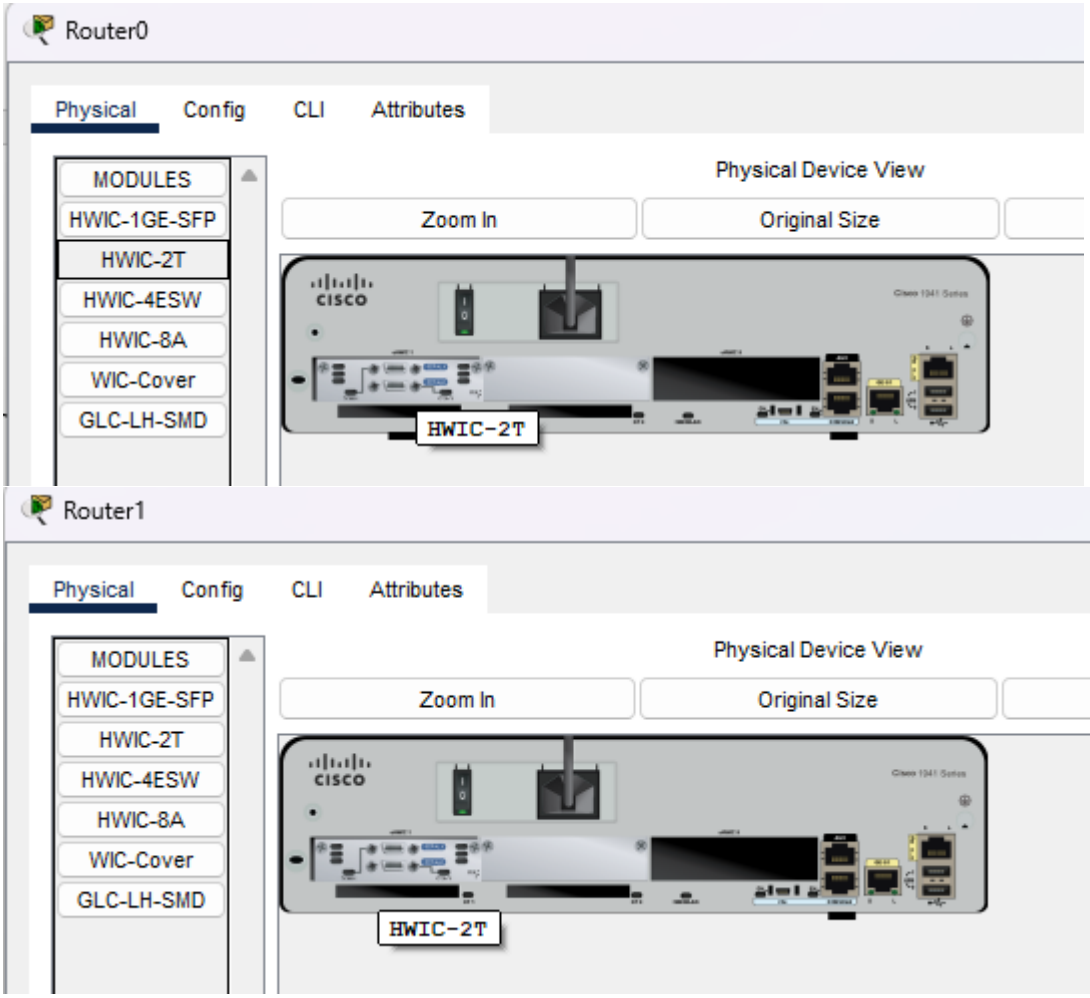


Table:

Router	Interface	IP Address	Subnet Mask
Router 0	FastEthernet0/0	192.168.1.1	255.255.255.0
	Serial0/1/0	10.0.0.1	255.255.255.0
Router 1	FastEthernet0/0	192.168.2.1	255.255.255.0
	Serial0/1/1	10.0.0.2	255.255.255.0

CLI Mode:
Go to Router / CLI
Deny Right LAN (192.168.2.0) from accessing Left LAN
Code:

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname left(router1)
left(router1)(config)#access-list 1 deny 192.168.2.0 0.0.0.255
left(router1)(config)#access-list 1 permit any
left(router1)(config)#int g0/0
left(router1)(config-if)#ip access-group 1 in
left(router1)(config-if)#ex
left(router1)(config)#
```

Output:
Effect:

- PC4–PC7 → PC0–PC3 ❌ (blocked)
- PC0–PC3 → PC4–PC7 ✅ (allowed, since reply traffic is still permitted)

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

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.

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

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

2) Extended

Extended ACL

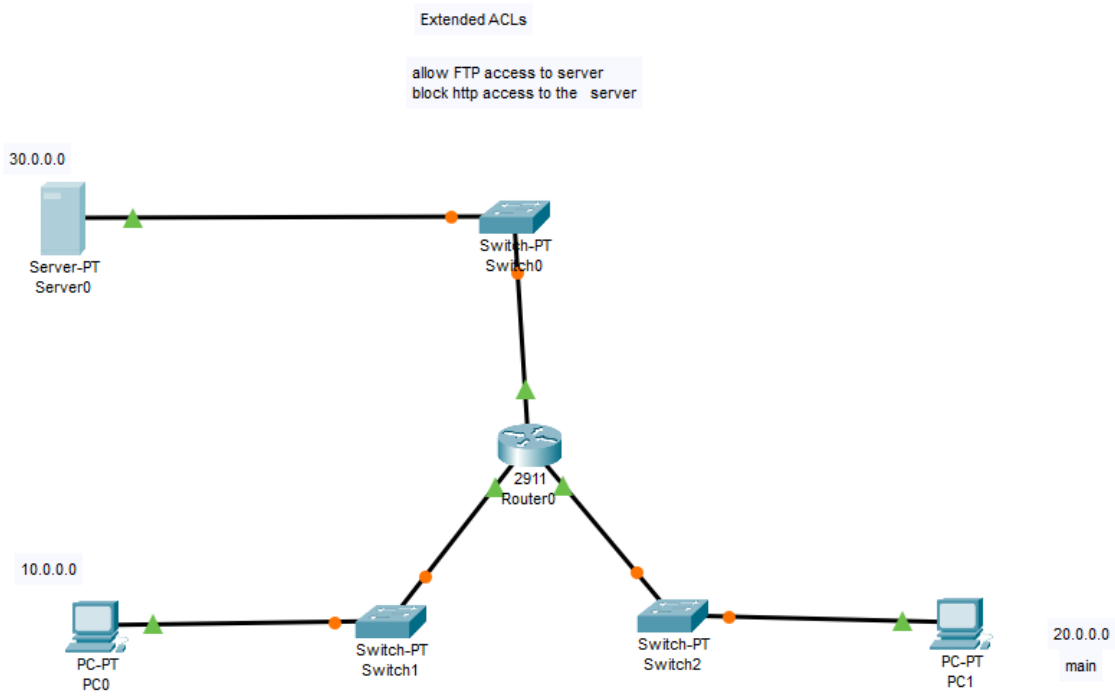
An **Extended Access Control List (ACL)** is a type of ACL that provides more detailed traffic filtering compared to Standard ACLs. Unlike Standard ACLs (which filter only by source IP), Extended ACLs can filter packets based on:

- Source IP address
- Destination IP address
- Protocol type (IP, TCP, UDP, ICMP, etc.)
- Port numbers (e.g., HTTP – 80, FTP – 21, Telnet – 23)

Number Range:

- 100–199 and 2000–2699

Topology:



Configuration Table:

PC: Go to PC / Desktop / Ip Configuration
Server: Go to Server / Desktop / Ip Configuration
Router: Go To Router / Config
Cable Name: Copper Straight-through

Table:

Device	Interface	IP Address	Subnet Mask
PC0	NIC	10.0.0.2	255.0.0.0
PC1	NIC	20.0.0.2	255.0.0.0
Server0	NIC	30.0.0.2	255.0.0.0

Device	Interface	IP Address	Subnet Mask
Router0	G0/0	10.0.0.1	255.0.0.0
	G0/1	20.0.0.1	255.0.0.0
	G0/2	30.0.0.1	255.0.0.0

CLI Mode
Go to Router / CLI

1

Code:

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 permit tcp any host 30.0.0.2 eq ftp
Router(config)#access-list 100 deny tcp any host 30.0.0.2 eq 80
Router(config)#access-list 100 permit ip any any
Router(config)#int g 0/2
Router(config-if)#ip access-group 100 in
Router(config-if)#
```

From PC0 (10.0.0.2) → Server (30.0.0.2):

- ping 30.0.0.2 → ✓ Works
- ftp 30.0.0.2 → ✓ Works (FTP allowed)
- http://30.0.0.2 in browser → ❌ Blocked

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 30.0.0.2

Pinging 30.0.0.2 with 32 bytes of data:

Request timed out.
Reply from 30.0.0.2: bytes=32 time<1ms TTL=127
Reply from 30.0.0.2: bytes=32 time<1ms TTL=127
Reply from 30.0.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 30.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ftp 30.0.0.2
Trying to connect...30.0.0.2
Connected to 30.0.0.2
220- Welcome to PT Ftp server
Username:MSc cs\
```

2) ✅ Allow **HTTP** access to the server (30.0.0.0 network → Server0).
❌ Block **FTP** access to the server.
Code:

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 120 deny tcp 20.0.0.0 0.0.0.255 host 30.0.0.2 eq 21
Router(config)#access-list 120 permit ip any any
Router(config)#interface gig0/1
Router(config-if)#ip access-group 120 in
Router(config-if)#ex
Router(config)#
```

Output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 30.0.0.2
Trying to connect...30.0.0.2

%Error opening ftp://30.0.0.2/ (Timed out)
.



(Disconnecting from ftp server)
```

Practical No: 02

Aim: Implement SPAN Technologies (Switch Port Analyzer)

Description:

What is SPAN?

- SPAN is a feature on Cisco switches that allows you to monitor traffic on one or more switch ports (source ports) and copy that traffic to another port (the destination port).
- The destination port is usually connected to a network analyser, IDS/IPS, or Wireshark PC for traffic capture and troubleshooting.

Why Use SPAN?

- Network monitoring → Capture and analyze live traffic.
- Security analysis → Monitor suspicious packets.
- Performance troubleshooting → Debug latency, packet drops, or errors.
- IDS/IPS integration → Send mirrored traffic to security appliances.

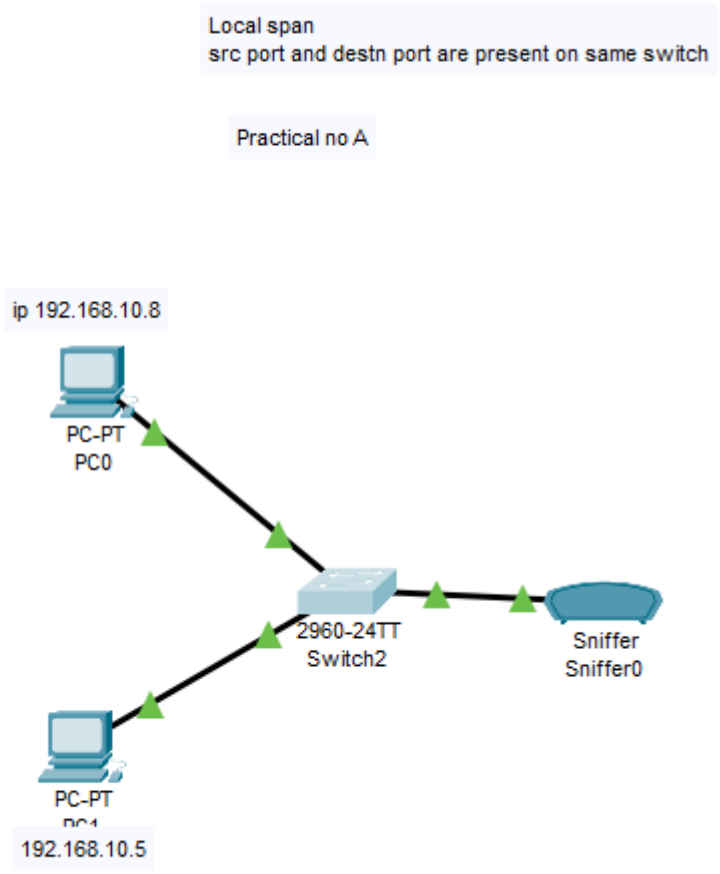
There Two Type of Span
1) Local Span
2) Remote Span

1) Local Span

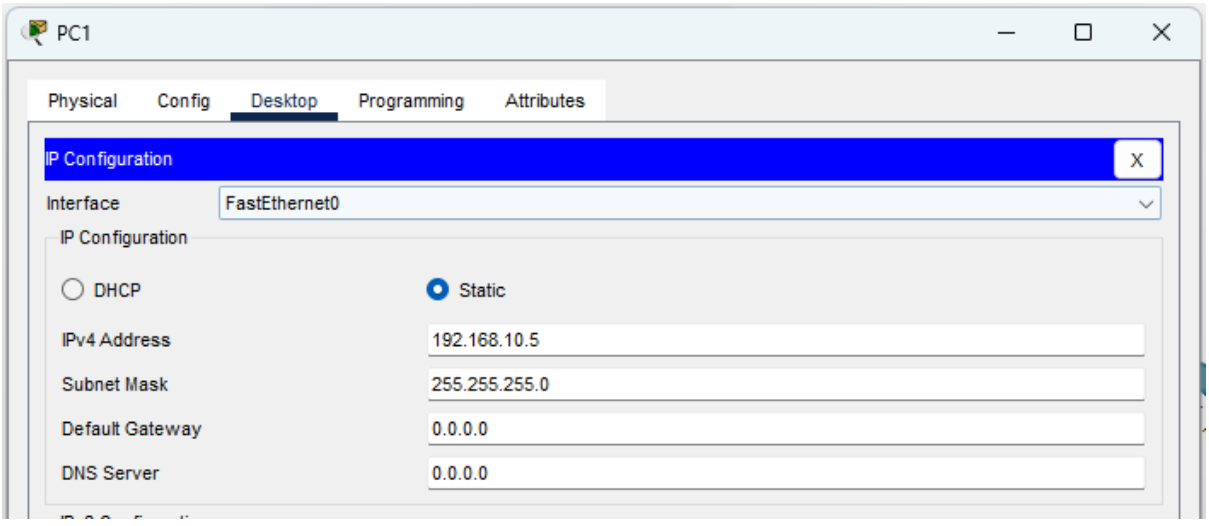
Local SPAN (Switch Port Analyzer):

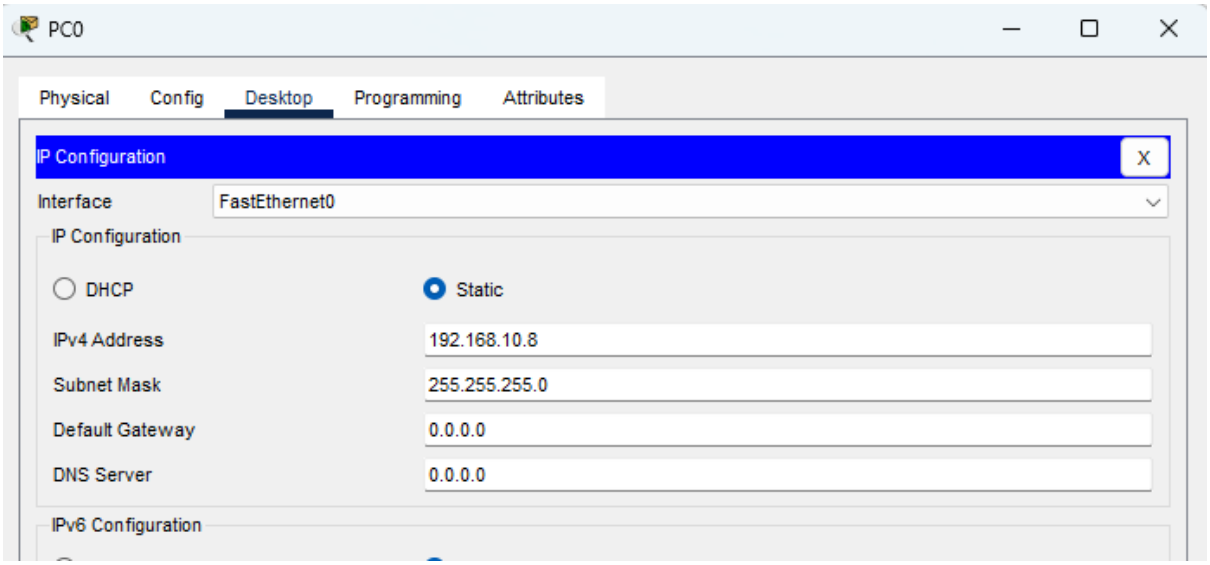
- In Local SPAN, both the source port (where traffic originates) and the destination port (where traffic is mirrored) are present on the same switch.
- It is used to capture and analyze traffic directly without affecting the original communication.
- A sniffer or analyzer tool connected to the destination port can observe all the packets from the source port.

Topology:



PC0 = connected on Fa0/1
PC1 = connected on Fa0/2
Sniffer0 = connected on Fa0/3 (destination port)

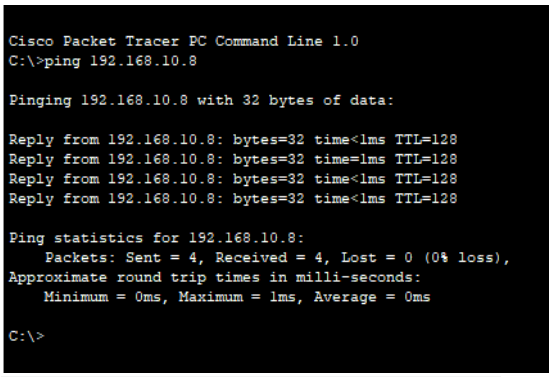


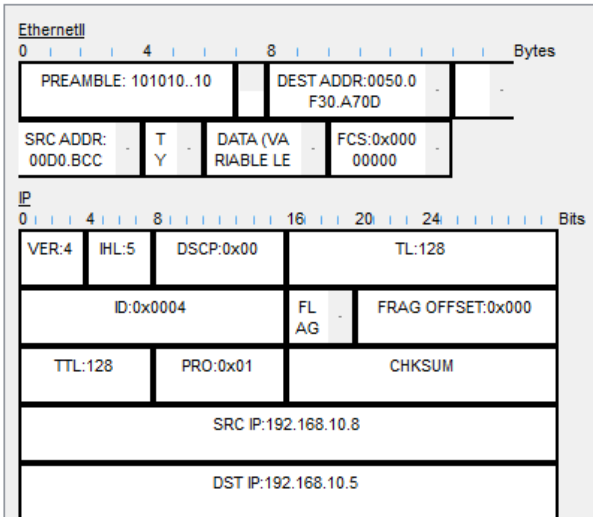


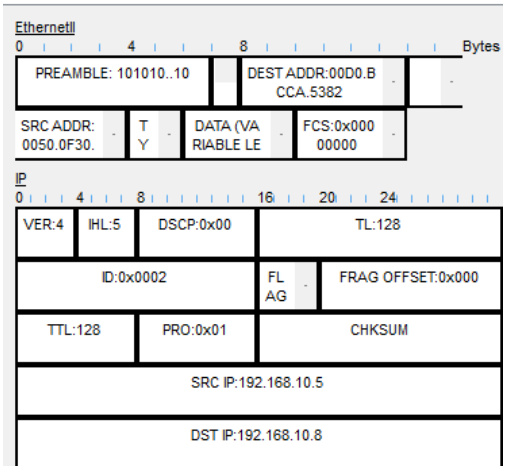
CLI mode:
Go to Switch / CLI

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#monitor session 1 source interface fa0/1
Switch(config)#monitor session 1 source interface fa0/2
Switch(config)#monitor session 1 destination interface fa0/3
Switch(config)#ex
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sh monitor
Session 1
---------
Type                   : Local Session
Description            : -
Source Ports           :
    Both               : Fa0/2,Fa0/1
Destination Ports      : Fa0/3
    Encapsulation      : Native
          Ingress      : Disabled
```

Output:







Now your sniffer will capture all traffic between PC0 ↔ PC1 without interrupting them.

2) Remote Span

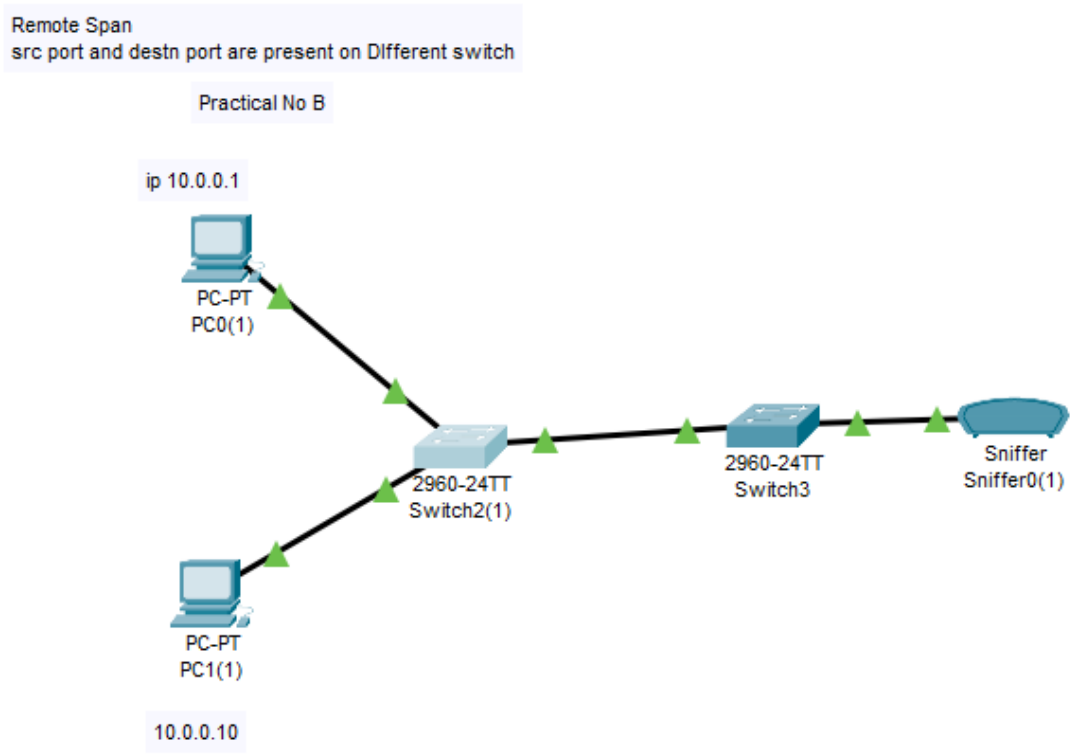
Description – Remote SPAN (RSPAN)

Remote SPAN is an advanced feature of SPAN (Switch Port Analyzer) that allows you to monitor traffic from source ports on one switch and send a copy of that traffic to a sniffer/monitoring device connected to another switch. Unlike Local SPAN, where the source and destination are on the same switch, RSPAN uses a special VLAN (RSPAN VLAN) to carry mirrored traffic across multiple switches.

Purpose:

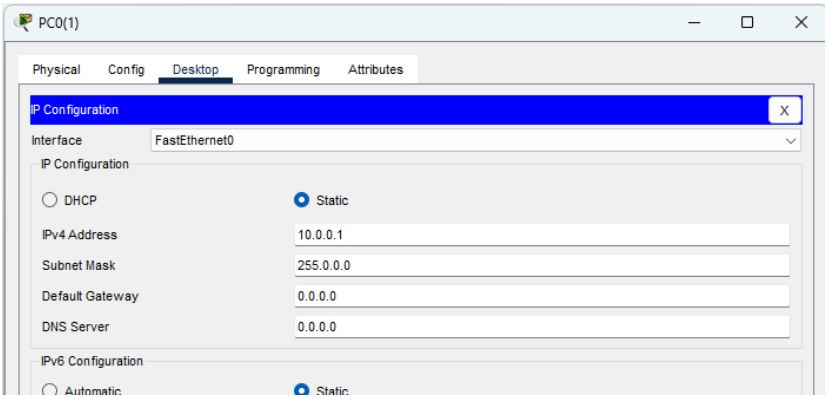
- To capture and analyze network traffic remotely when the sniffer/IDS (Intrusion Detection System) is not physically on the same switch.
- Useful for centralized monitoring in large networks

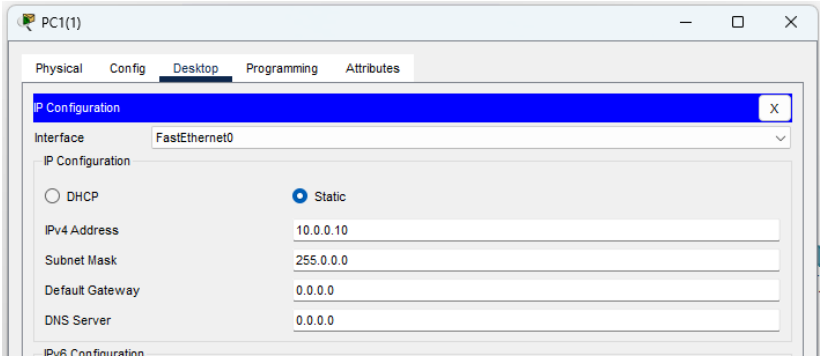
Topology:



Configuration:
Go to PC / Desktop / Ip configuration

PC Configuration:





Switches Configuration

Switch1:

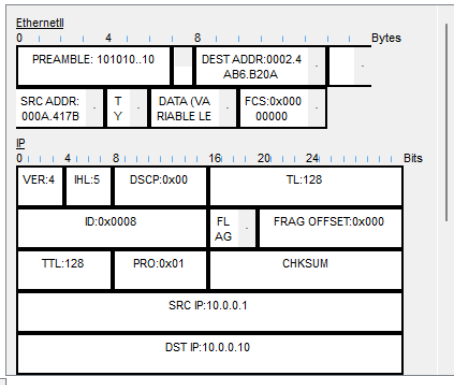
```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 999
Switch(config-vlan)#remote-span
Switch(config-vlan)#ex
Switch(config)#monitor session 1 source f0/1
                                        ^
% Invalid input detected at '^' marker.

Switch(config)#monitor session 1 source int f0/1
Switch(config)#monitor session 1 destination remote vlan 999 reflector-port int f0/24
                                                                            ^
% Invalid input detected at '^' marker.

Switch(config)#monitor session 1 destination remote vlan 999 reflector-port f0/24
Switch(config)#ex
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

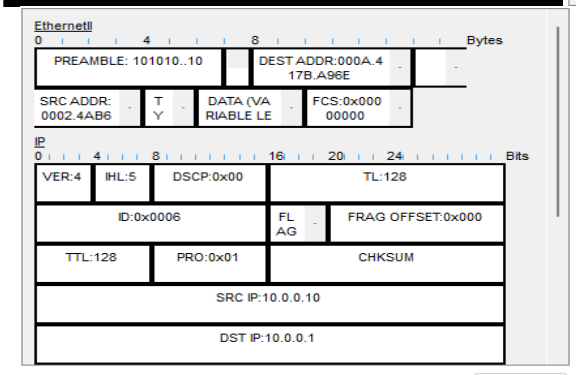
Switch 2:

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#monitor session 1 source remote vlan 999
Switch(config)#monitor session 1 destination int f0/2
Switch(config)#ex
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
```

Output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.10

Pinging 10.0.0.10 with 32 bytes of data:

Reply from 10.0.0.10: bytes=32 time<1ms TTL=128
Reply from 10.0.0.10: bytes=32 time<1ms TTL=128
Reply from 10.0.0.10: bytes=32 time<1ms TTL=128
Reply from 10.0.0.10: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```





Practical No: 03

Aim: implement Inter-VLAN Routing

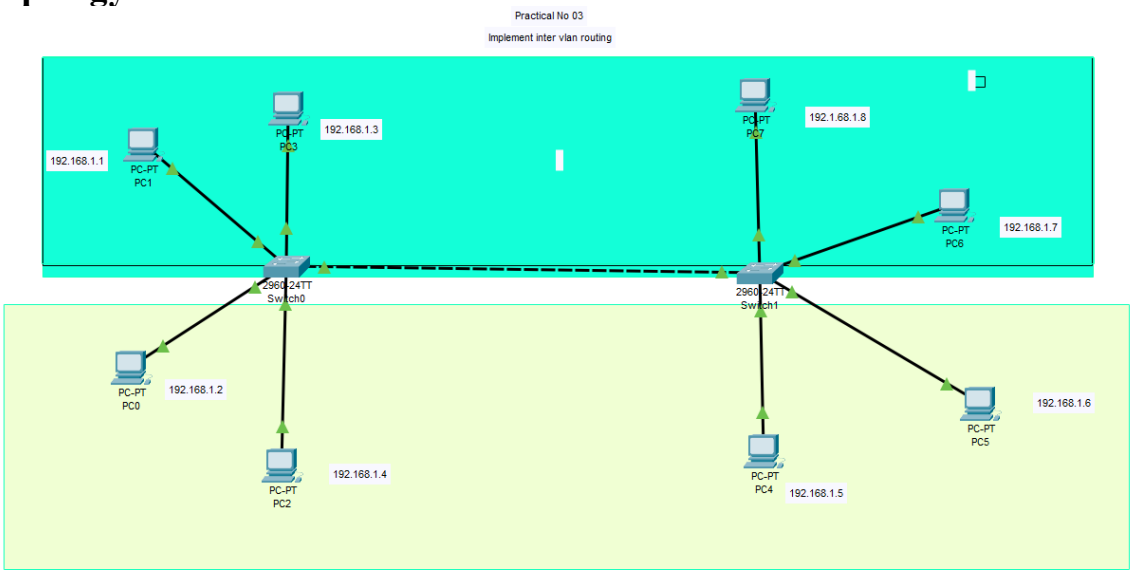
Definition:
Inter-VLAN Routing is the process of allowing communication between devices that are in different VLANs (Virtual Local Area Networks).
Since VLANs separate network traffic at Layer 2 (Data Link Layer), routers or Layer 3 switches are needed to route packets between them at Layer 3 (Network Layer).

Description:
In a switched network, VLANs are used to segment the network into smaller broadcast domains. However, devices in different VLANs cannot communicate directly.
To enable communication between these VLANs, Inter-VLAN Routing is implemented.
There are two common methods:

1. Router-on-a-Stick: A single router interface is divided into multiple sub-interfaces, each configured for a different VLAN.
2. Layer 3 Switch (Multilayer Switch): The switch performs routing internally using Switch Virtual Interfaces (SVIs).

This setup improves network organization, security, and performance while still allowing necessary communication between VLANs.

Topology:

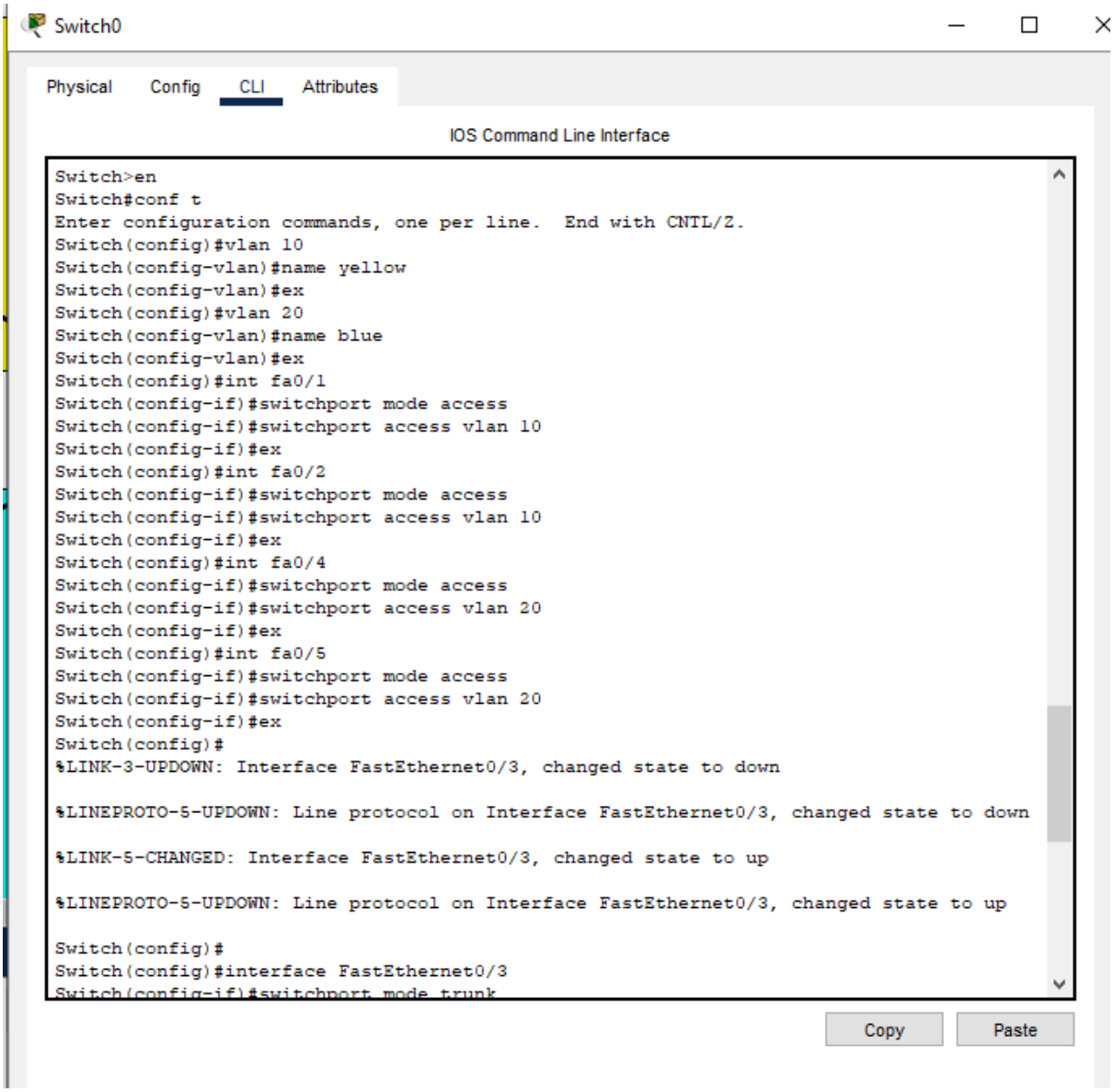


Configuration:

1) PC Configuration
Go to PC / Desktop / IP Configuration:

Device	Switch	Switch Port	VLAN	IP Address	Mask	Default Gateway
PC0	Switch0	Fa0/2	10	192.168.1.1	255.255.255.0	192.168.1.254
PC1	Switch0	Fa0/1	10	192.168.1.2	255.255.255.0	192.168.1.254
PC2	Switch0	Fa0/4	20	192.168.2.1	255.255.255.0	192.168.2.254
PC3	Switch0	Fa0/5	20	192.168.2.2	255.255.255.0	192.168.2.254
PC4	Switch1	Fa0/1	20	192.168.2.3	255.255.255.0	192.168.2.254
PC5	Switch1	Fa0/2	20	192.168.2.4	255.255.255.0	192.168.2.254
PC6	Switch1	Fa0/3	10	192.168.1.3	255.255.255.0	192.168.1.254
PC7	Switch1	Fa0/4	10	192.168.1.4	255.255.255.0	192.168.1.254

2) Switch Configuration (Switch0)



```
Switch(config)#
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
```

Copy Paste

3) Switch Configuration (Switch0)

Switch1

Physical Config CLI Attributes

IOS Command Line Interface

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name yellow
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name blue
Switch(config-vlan)#ex
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#ex
Switch(config)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#ex
Switch(config)#int fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#ex
Switch(config)#int fa0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#ex
Switch(config)#int fa0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#ex
Switch(config)#
```

Copy Paste

Top

Output:

Scenario 0

New Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC0	PC7	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC4	PC1	ICMP		0.000	N	1	(edit)	(delete)

Practical No: 04

Aim: Implement RIP protocol

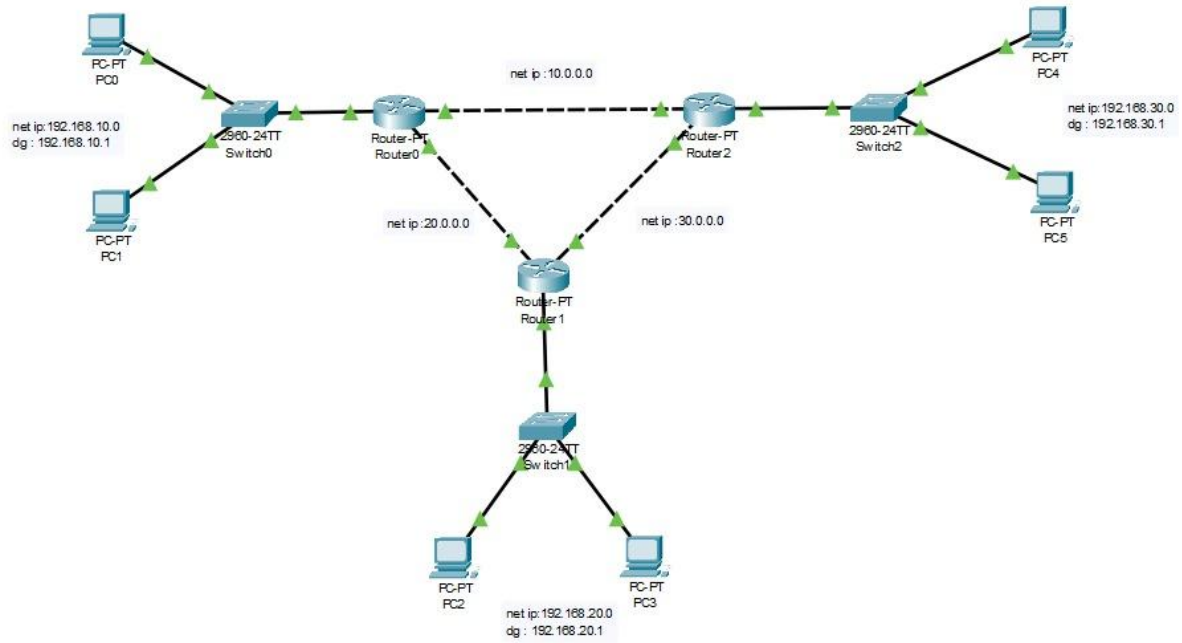
Definition:
RIP (Routing Information Protocol) is a **distance-vector routing protocol** used to enable routers to share information about network paths.
It determines the best route to a destination network based on the **hop count** (the number of routers a packet passes through).

Description:
RIP is one of the oldest dynamic routing protocols that automatically updates and maintains routing tables in a network.
Routers using RIP periodically exchange their routing tables with neighbouring routers every **30 seconds**.
The route with the **lowest hop count** (up to a maximum of 15 hops) is considered the best path.
There are two main versions:

- **RIP version 1 (RIPv1):** Classful, does not support subnet masks.
- **RIP version 2 (RIPv2):** Classless, supports subnet masks, authentication, and multicasting.

RIP helps simplify network configuration and ensures routers can dynamically adjust routes when network topology changes.

Topology:



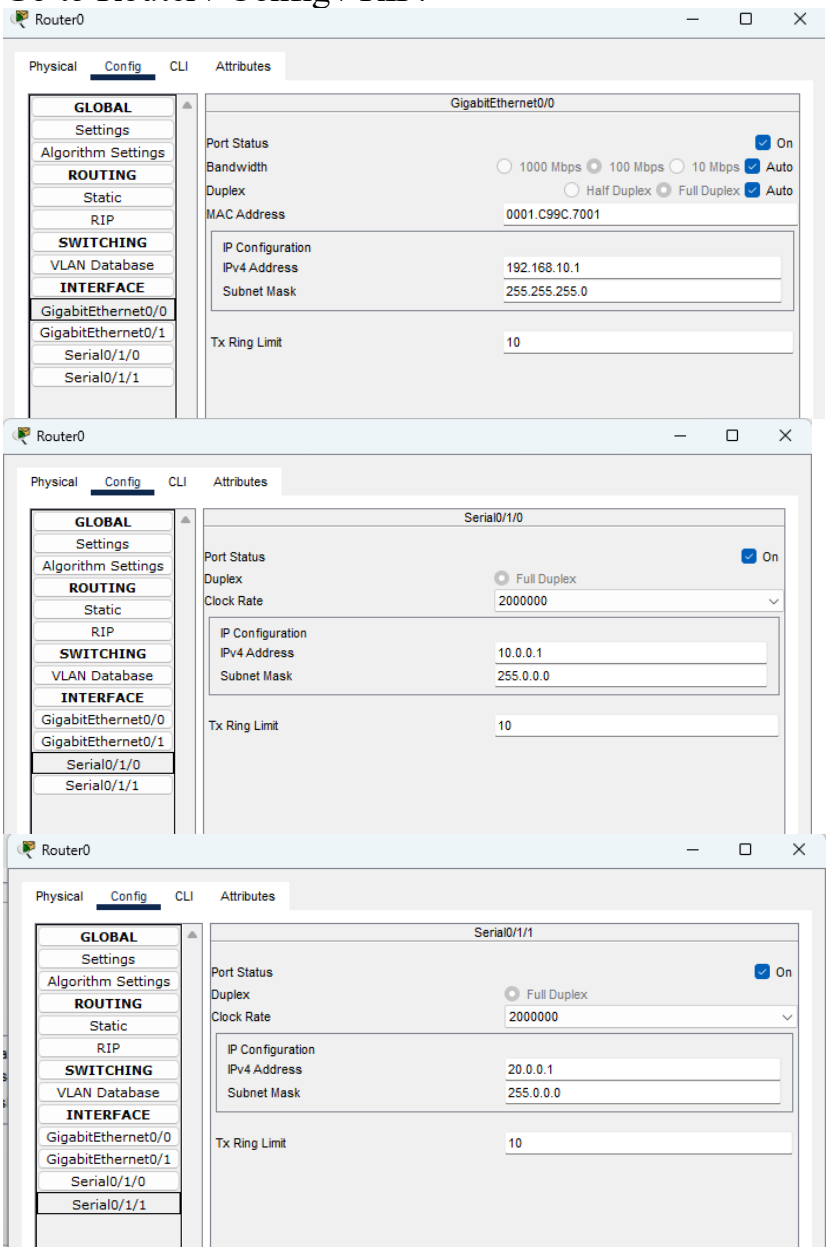
Configuration:
1) PC Configuration
Go to PC / Desktop / IP Configuration:

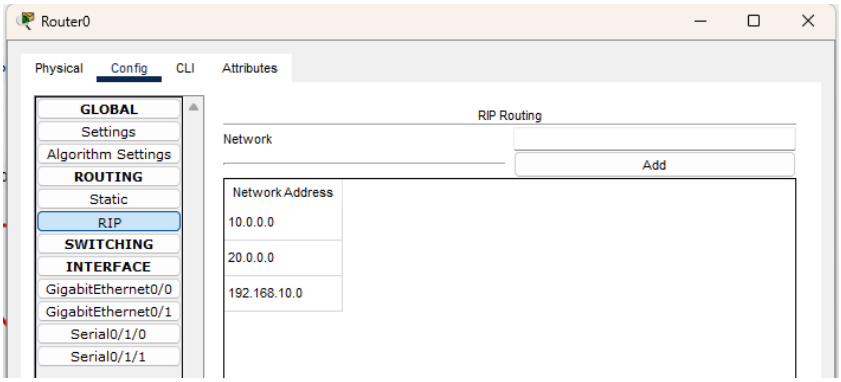
PC	IP Address	Subnet Mask	Default Gateway
PC0	192.168.10.2	255.255.255.0	192.168.10.1
PC1	192.168.10.3	255.255.255.0	192.168.10.1
PC2	192.168.20.2	255.255.255.0	192.168.20.1
PC3	192.168.20.3	255.255.255.0	192.168.20.1
PC4	192.168.30.2	255.255.255.0	192.168.30.1
PC5	192.168.30.3	255.255.255.0	192.168.30.1

2) Switch Configuration:

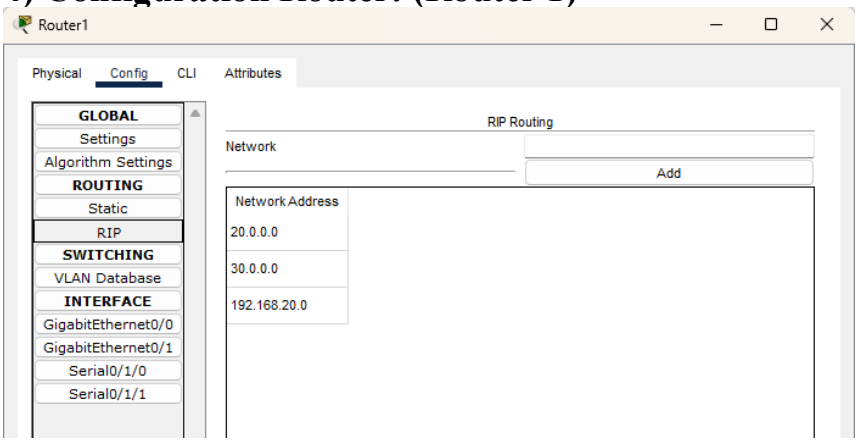
Go to Switch / Config:

Go to Router / Config / RIP:

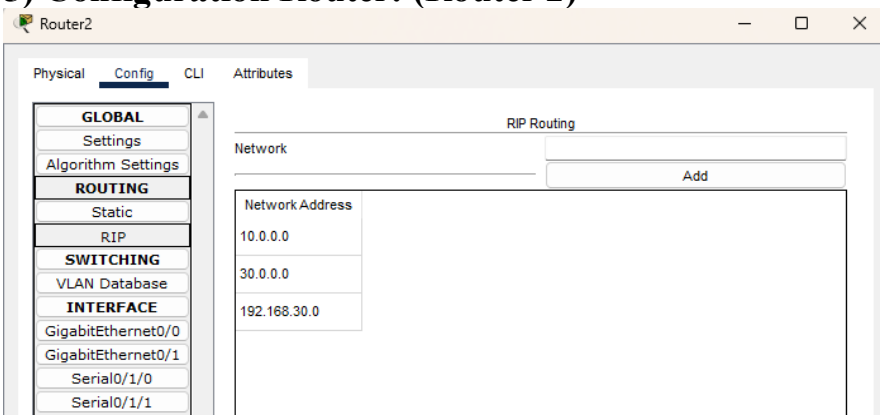




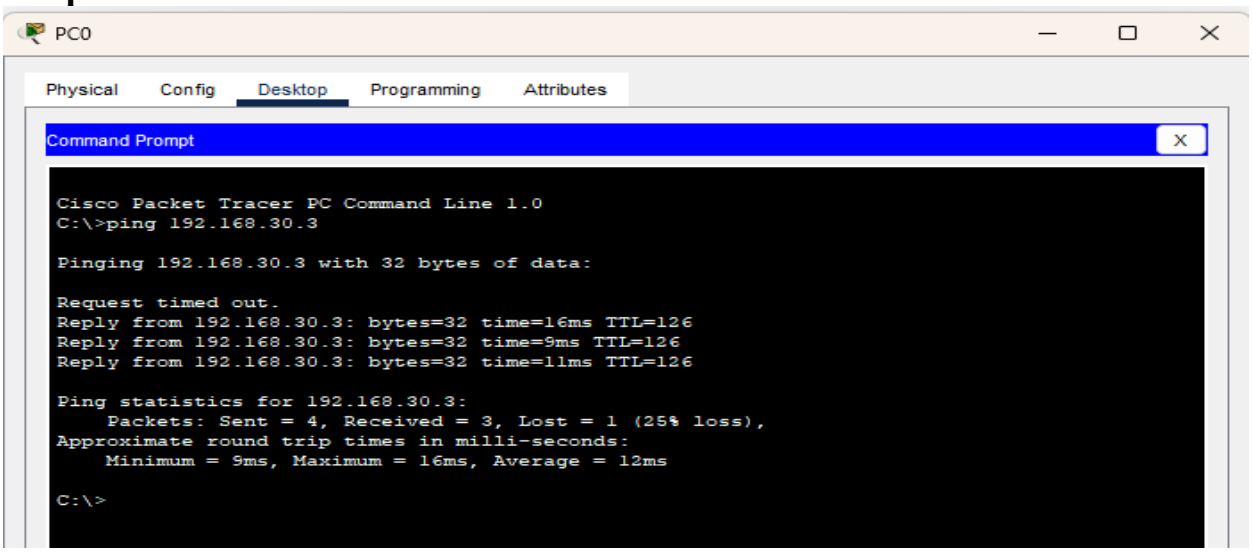
4) Configuration Router: (Router 1)



5) Configuration Router: (Router 2)



Output:



Practical No: 05

Aim:
To implement OSPF (Open Shortest Path First) protocol in:

1. Single-Area OSPFv2
2. Multi-Area OSPFv2

Definition:
OSPF (Open Shortest Path First) is a link-state dynamic routing protocol used to find the shortest and most efficient path to each network using the Dijkstra algorithm.
It shares link-state information between routers instead of entire routing tables and organizes networks into areas to improve scalability.

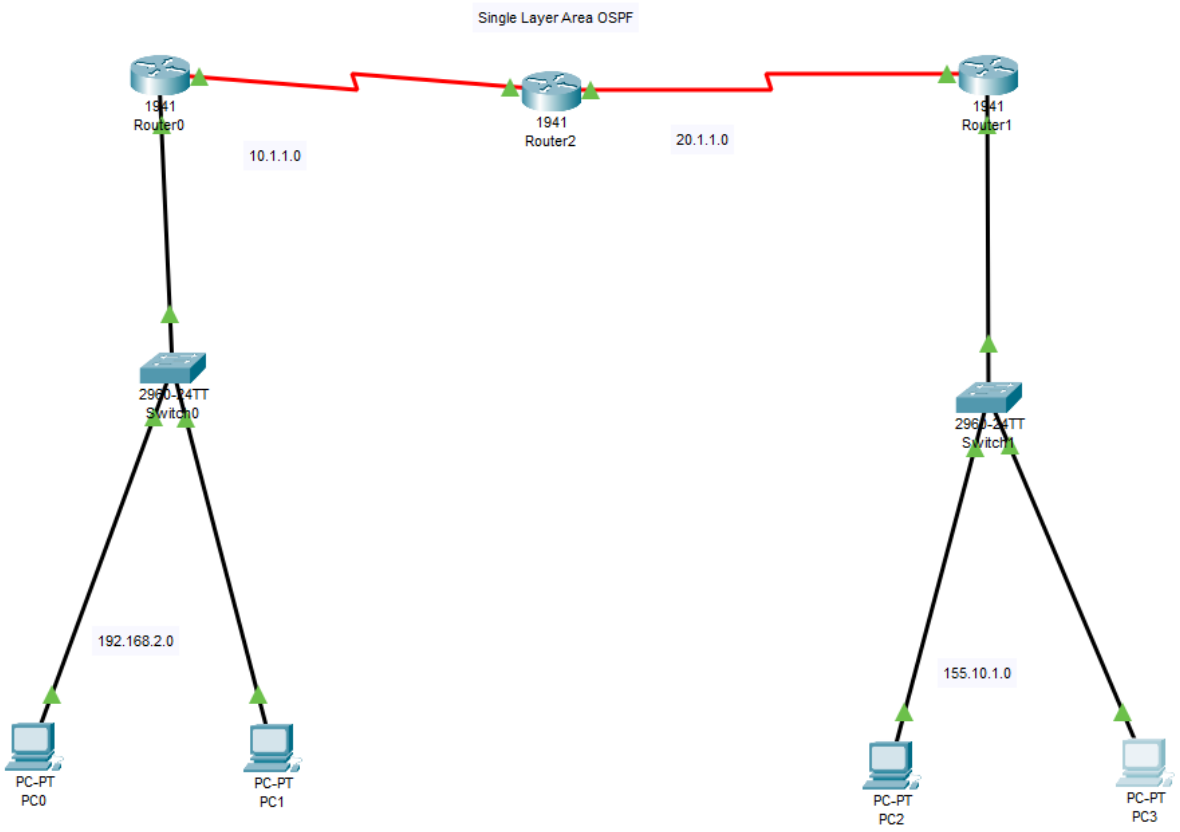
Description:

- OSPFv2 is used for IPv4 networks.
- It divides the network into areas to reduce routing overhead.
- The main area (backbone) is called Area 0.
- Each router shares information about its directly connected networks.
- OSPF uses cost (based on bandwidth) as its metric — the lower the cost, the better the path.
- It quickly updates routes when a link fails, providing fast convergence

1) Single Layer OSPF 1

Definition:
Single-Area OSPFv2 is a routing protocol configuration in which all routers belong to one common area (Area 0).
It uses the link-state routing method to exchange routing information and build a complete map of the network within that area.
This setup is simple, easy to manage, and suitable for small to medium-sized networks where network design is not too complex.

Topology:



Configuration:

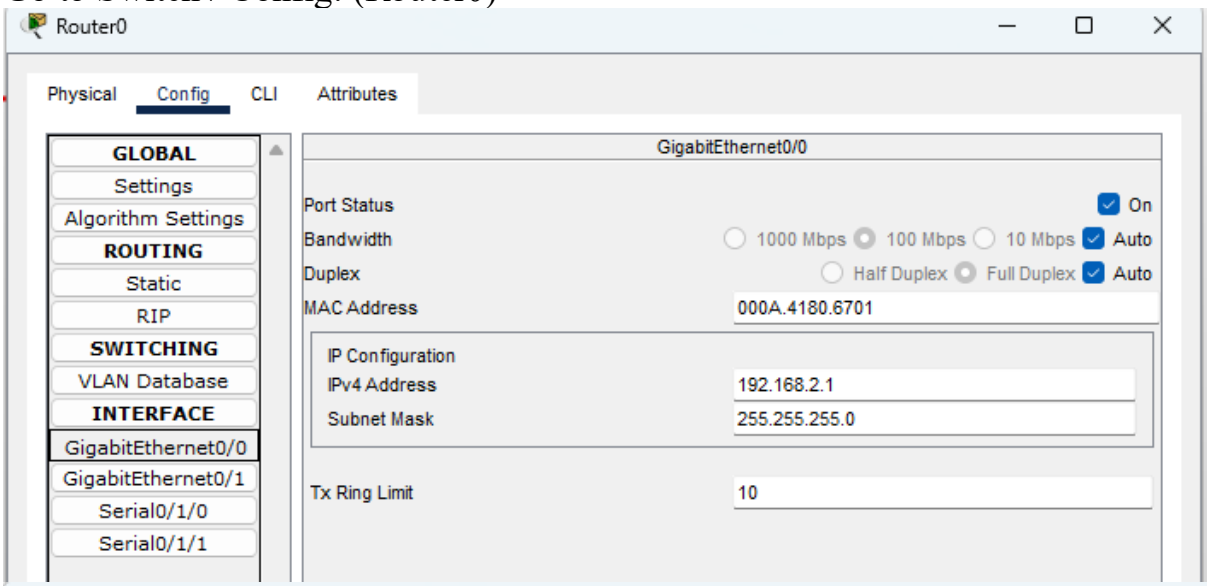
1) PC Configuration

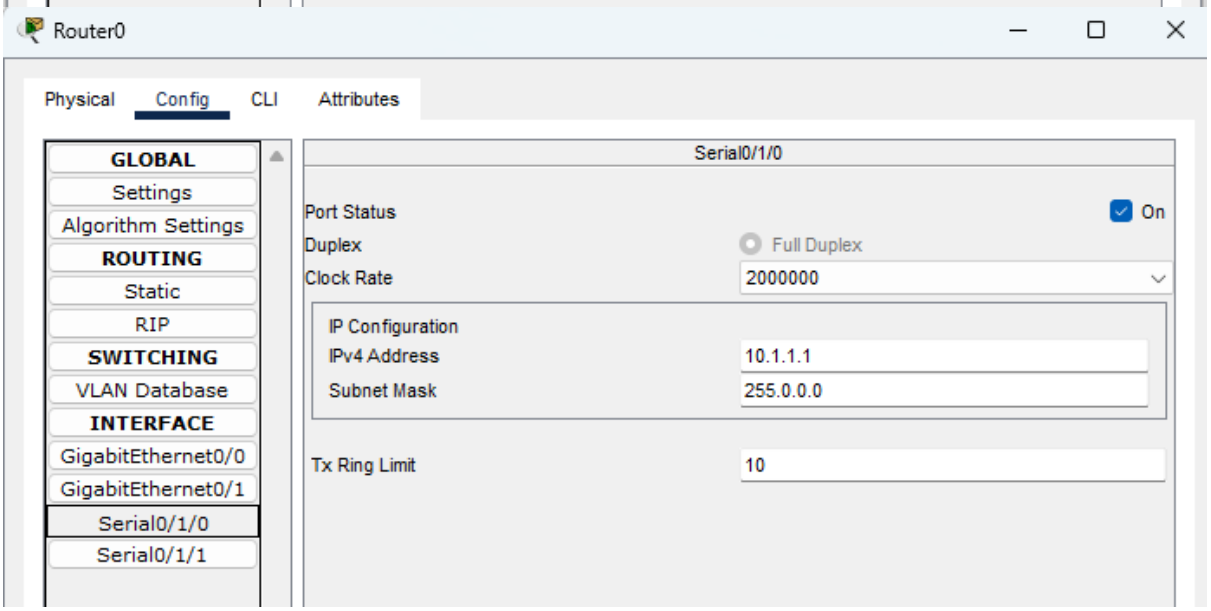
Go to PC / Desktop / IP Configuration:

PC	IP Address	Subnet Mask	Default Gateway
PC0	192.168.2.2	255.255.255.0	192.168.2.1
PC1	192.168.2.3	255.255.255.0	192.168.2.1
PC2	155.10.1.2	255.255.0.0	155.10.1.1
PC3	155.10.1.3	255.255.0.0	155.10.1.1

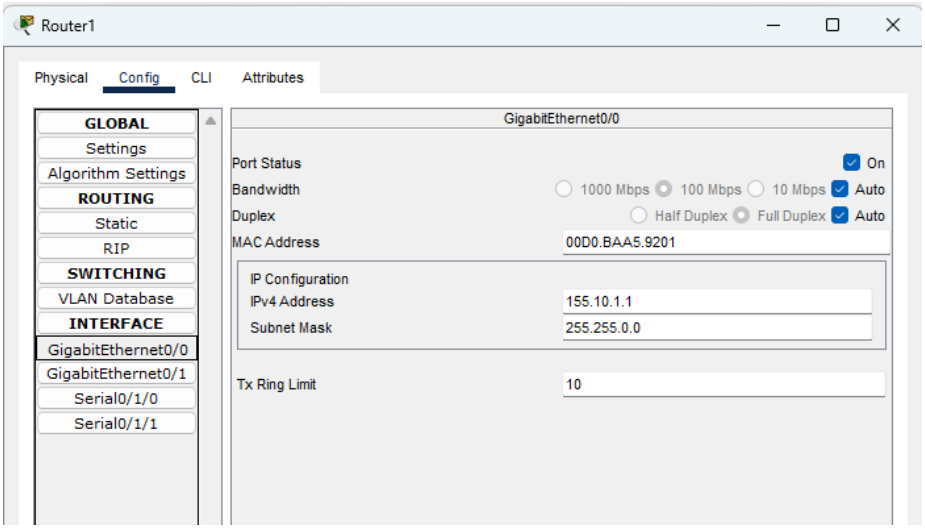
2) Switch Configuration:

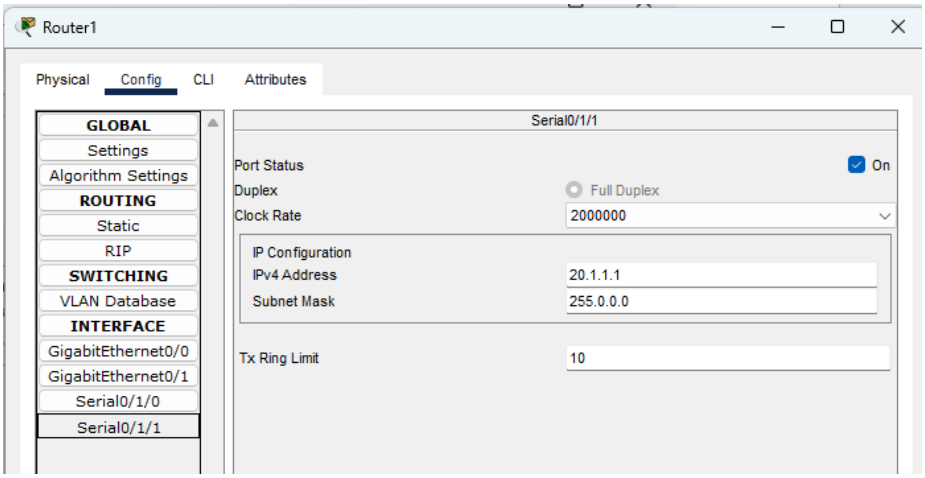
Go to Switch / Config: (Router0)



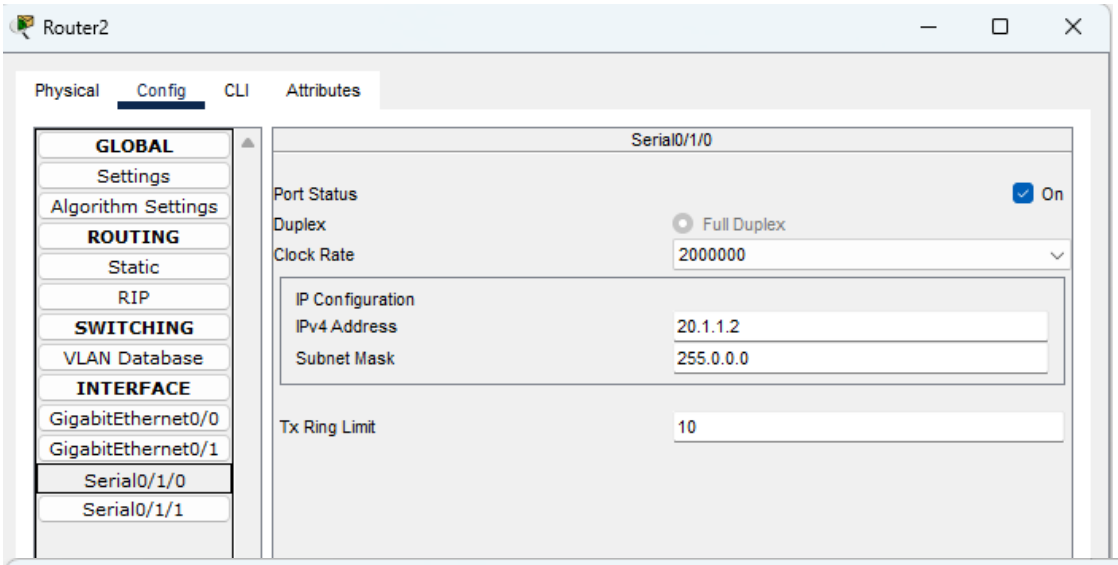


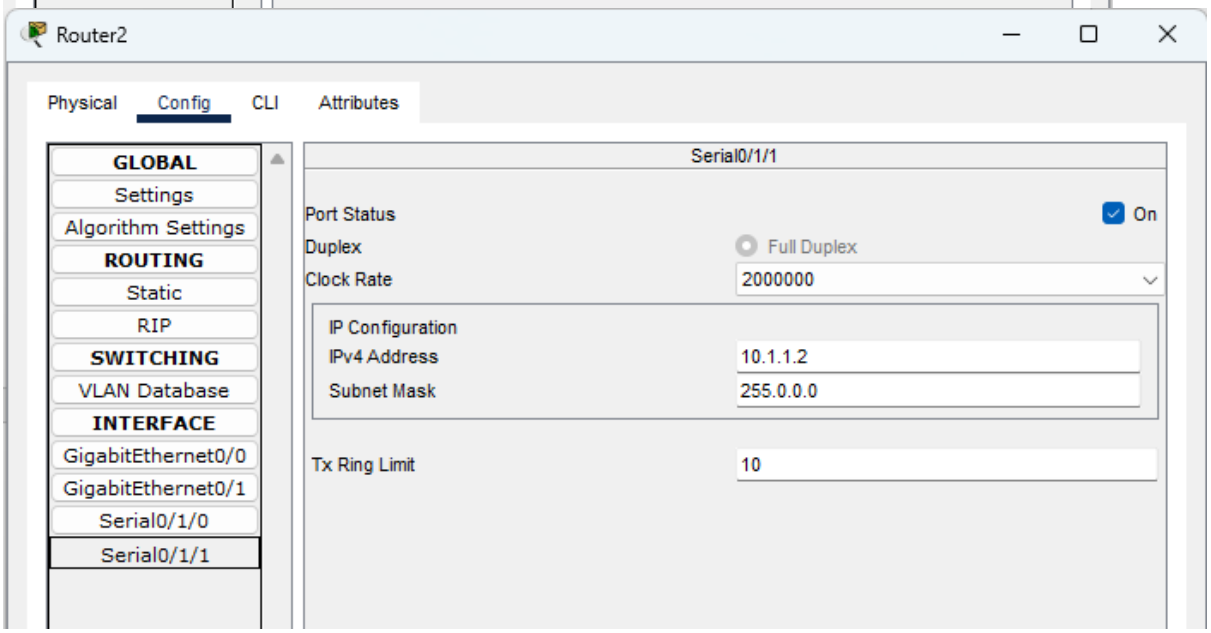
Router1:




Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/1
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
20.1.1.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10

Router 2:


Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
20.1.1.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10


Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/1
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
10.1.1.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10

3) CLI mode (Router0):

Go to Router0 / CLI:

4) CLI mode (Router1):

Go to Router1 / CLI:

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 155.10.0.0 0.0.0.255 area 0
Router(config-router)#network 20.1.1.0 0.0.0.255 area 0
Router(config-router)#ex
Router(config)#
```

4) CLI mode (Router2):

Go to Router2 / CLI:

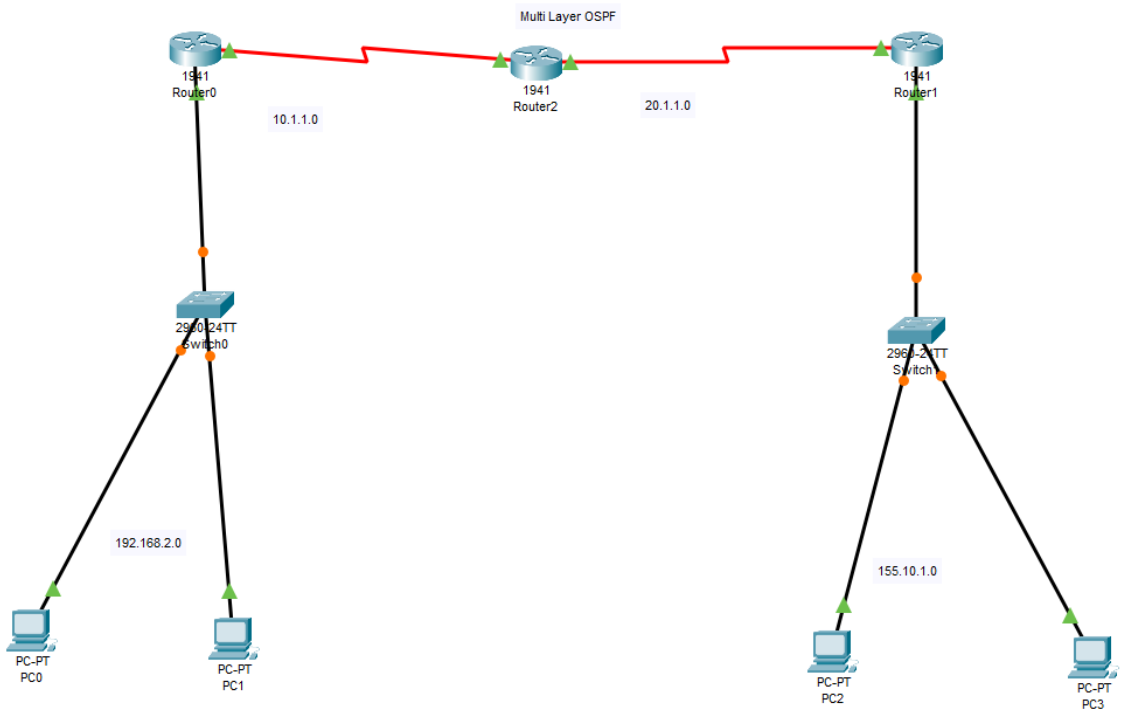
```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#network 10.1.1.0 0.0.0.255 area 0
                  ^
% Invalid input detected at '^' marker.

Router(config)#router ospf 1
Router(config-router)#network 10.1.1.0 0.0.0.255 area 0
Router(config-router)#network 20.1.1.0 0.0.0.255 area 0
Router(config-router)#ex
Router(config)#
```

```
^C
C:\>ping 155.10.1.2

Pinging 155.10.1.2 with 32 bytes of data:

Request timed out.
Reply from 155.10.1.2: bytes=32 time=25ms TTL=125
Reply from 155.10.1.2: bytes=32 time=21ms TTL=125
Reply from 155.10.1.2: bytes=32 time=2ms TTL=125

Ping statistics for 155.10.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 25ms, Average = 16ms

C:\>
```

2) Multi-Layer OSPF

Definition: Multi-Area OSPFv2:
Multi-Area OSPF (Open Shortest Path First) is a hierarchical routing design where the network is divided into multiple areas to optimize routing performance.
Each area has its own topology database, which reduces CPU load and routing table size.
The Backbone Area (Area 0) connects all other areas, called non-backbone areas (Area 1, Area 2, etc.).

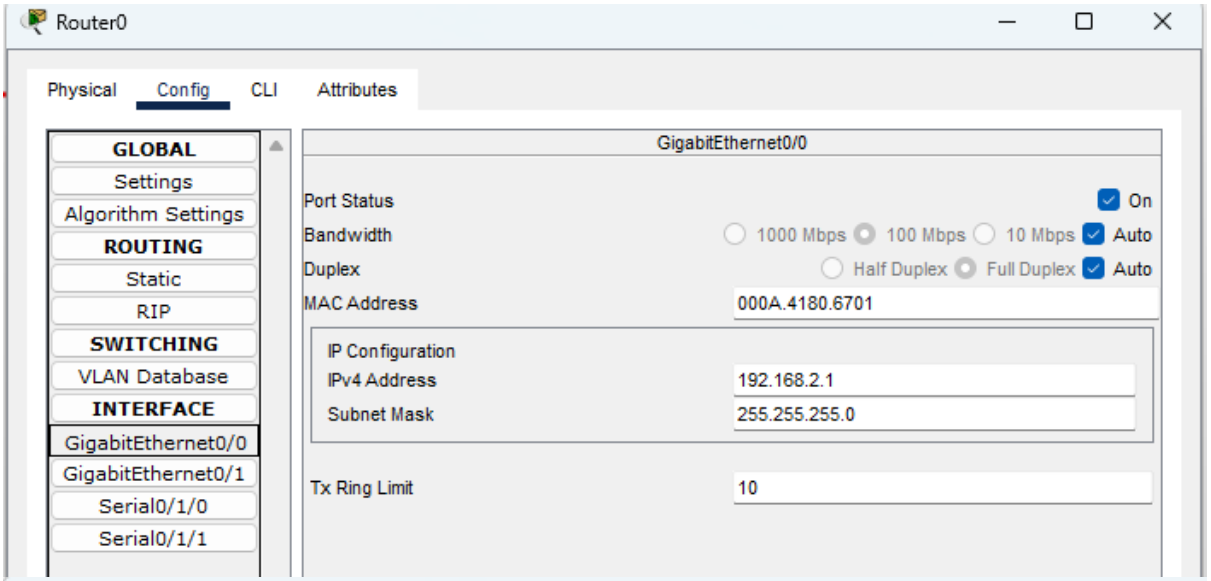
Topology:

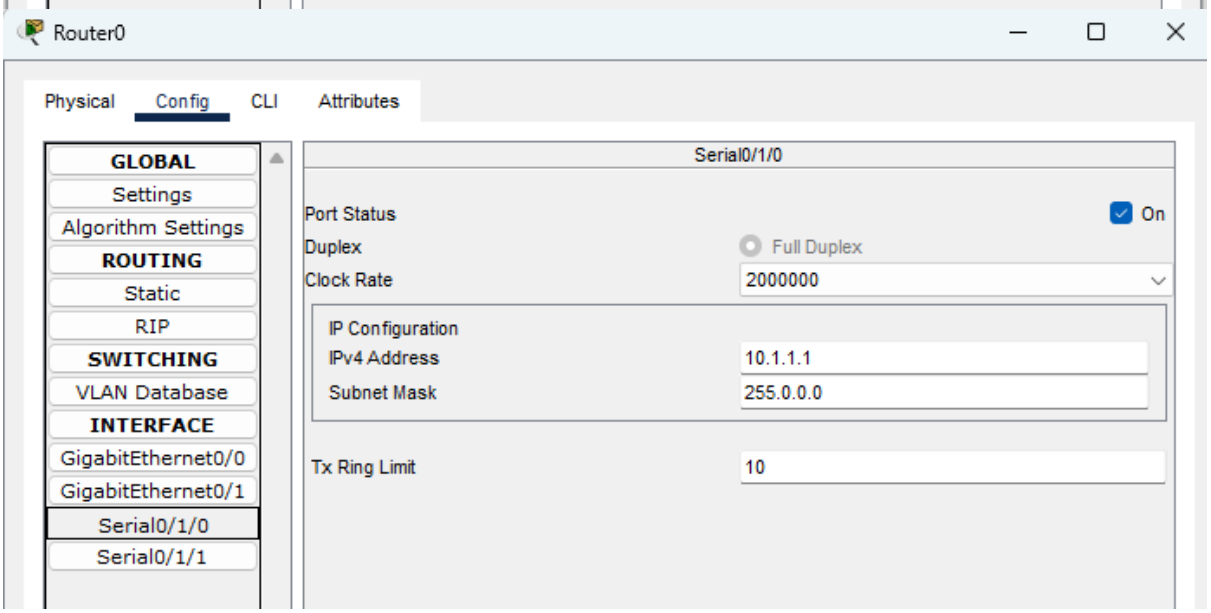


Configuration:
1) PC Configuration
Go to PC / Desktop / IP Configuration:

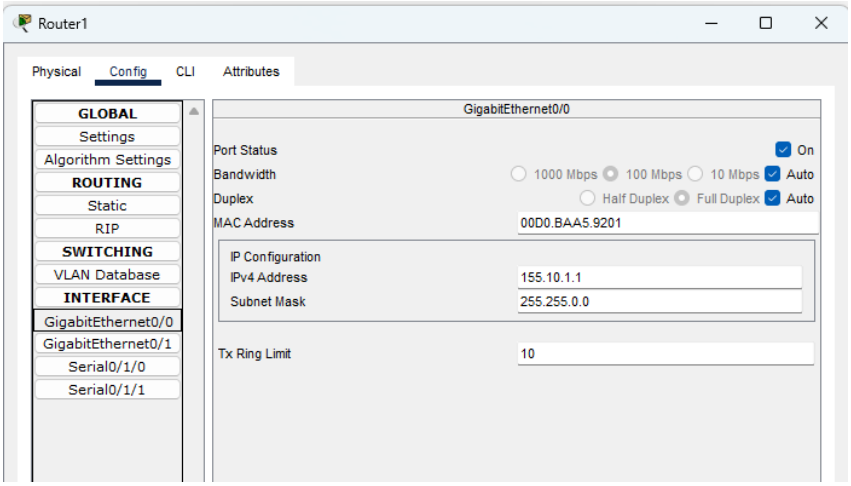
PC	IP Address	Subnet Mask	Default Gateway
PC0	192.168.2.2	255.255.255.0	192.168.2.1
PC1	192.168.2.3	255.255.255.0	192.168.2.1
PC2	155.10.1.2	255.255.0.0	155.10.1.1
PC3	155.10.1.3	255.255.0.0	155.10.1.1

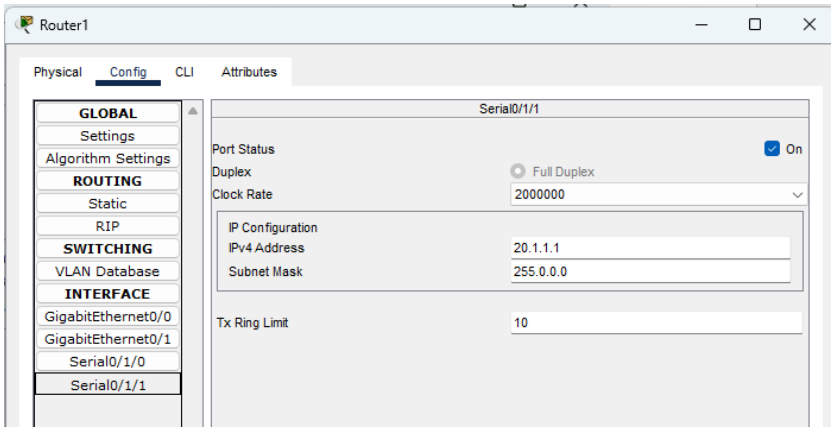
2) Switch Configuration:
Go to Switch / Config: (Router0)


Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
000A.4180.6701
IP Configuration
IPv4 Address
192.168.2.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10

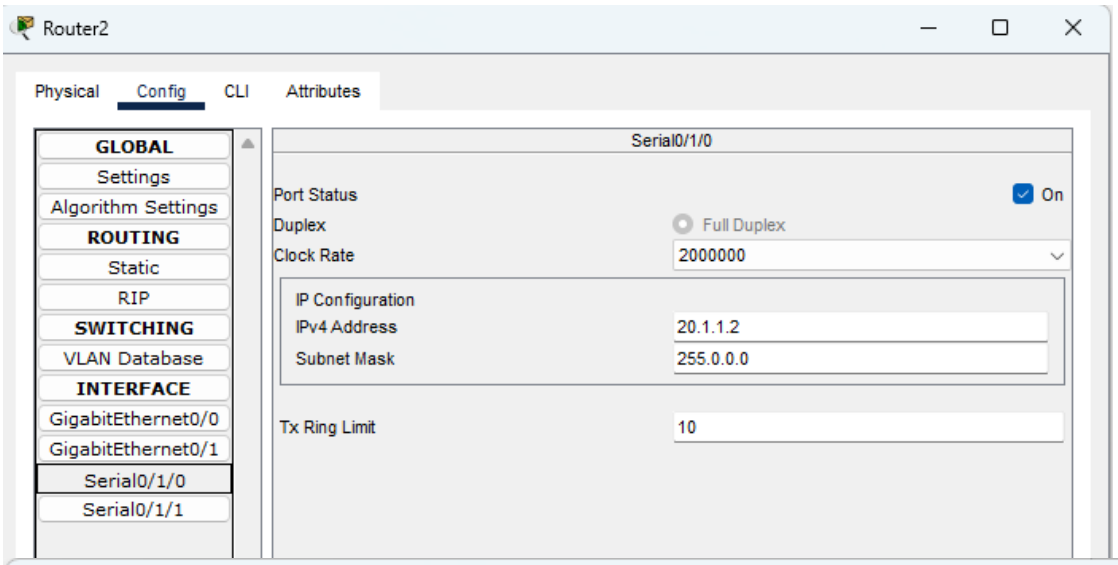

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
10.1.1.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10

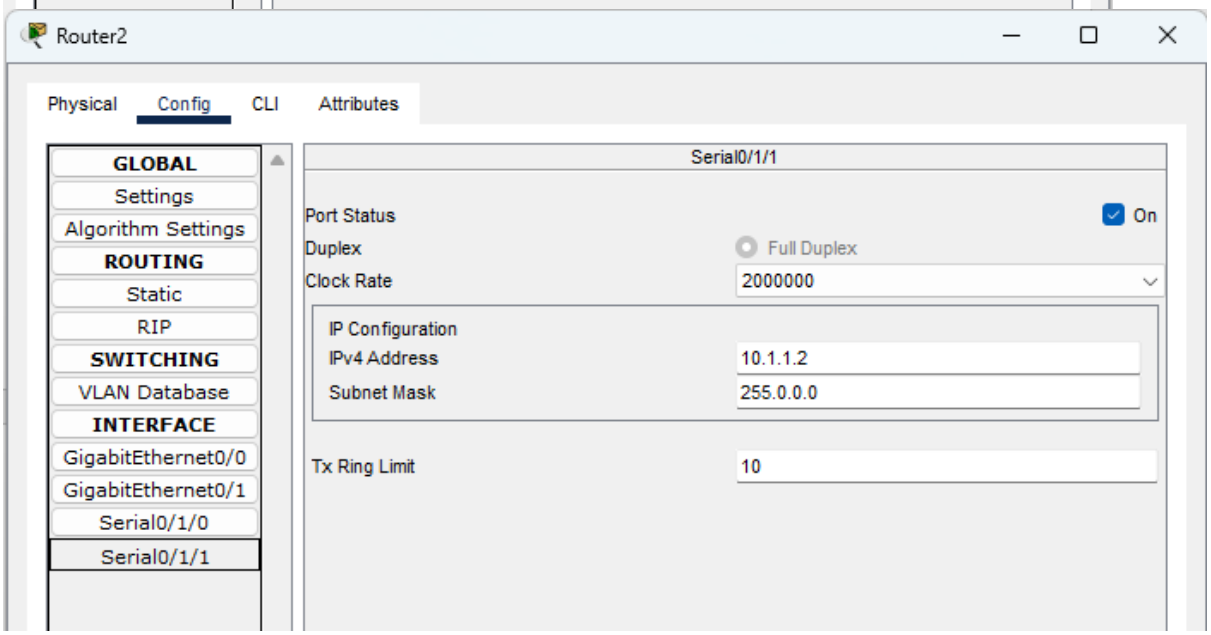
Router1:


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00D0.BAA5.9201
IP Configuration
IPv4 Address
155.10.1.1
Subnet Mask
255.255.0.0
Tx Ring Limit
10


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/1
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
20.1.1.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10

Router 2:


Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
20.1.1.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10


Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/1
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
10.1.1.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10

CLI mode (Router0):

Go to Router0 / CLI:

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router(config-router)#network 10.1.1.0 0.255.255.255 area 0
Router(config-router)#ex
Router(config)#
```

4) CLI mode (Router1):

Go to Router1 / CLI:

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 155.10.1.0 0.255.255 area 1
                                         ^
% Invalid input detected at '^' marker.

Router(config-router)#network 155.10.1.0 0.0.255.255 area 1
Router(config-router)#network 20.1.1.0 0.255.255.255 area 1
Router(config-router)#ex
Router(config)#
```

4) CLI mode (Router2):

Go to Router2 / CLI:

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 10.1.1.0 0.255.255.255 area 0
Router(config-router)#network 20.1.1.0 0.255.255.255 area 1
Router(config-router)#ex
Router(config)#
```

```
^C
C:\>ping 155.10.1.2

Pinging 155.10.1.2 with 32 bytes of data:

Request timed out.
Reply from 155.10.1.2: bytes=32 time=25ms TTL=125
Reply from 155.10.1.2: bytes=32 time=21ms TTL=125
Reply from 155.10.1.2: bytes=32 time=2ms TTL=125

Ping statistics for 155.10.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 25ms, Average = 16ms

C:\>
```

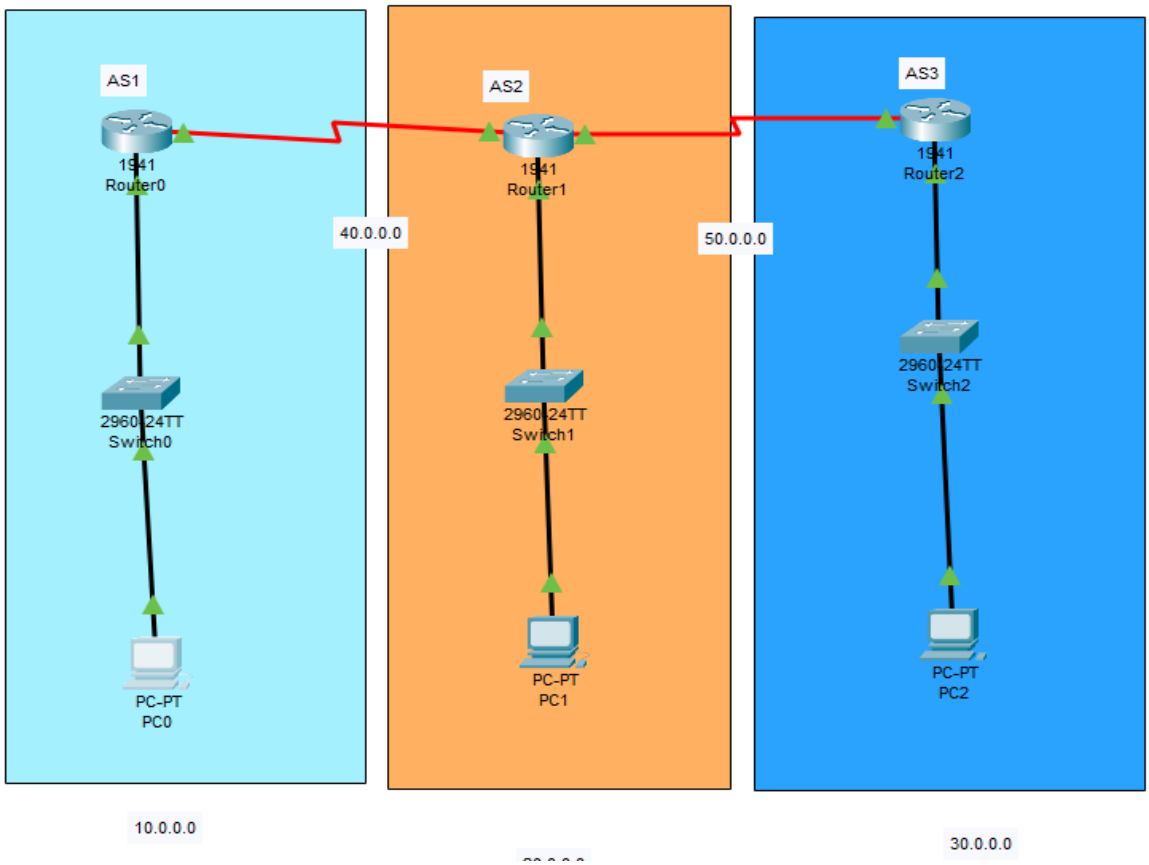
Practical No: 06

Aim: Implement BGP Communities
1. Implement EBGP
2. Implement IBGP

What is BGP (Border Gateway Protocol)?

- **BGP** is a **path-vector routing protocol** used to exchange routing information **between different autonomous systems (AS)**.
- It is the **protocol of the Internet** — all ISPs use BGP to communicate.
- BGP identifies each network using a unique **Autonomous System Number (ASN)**.

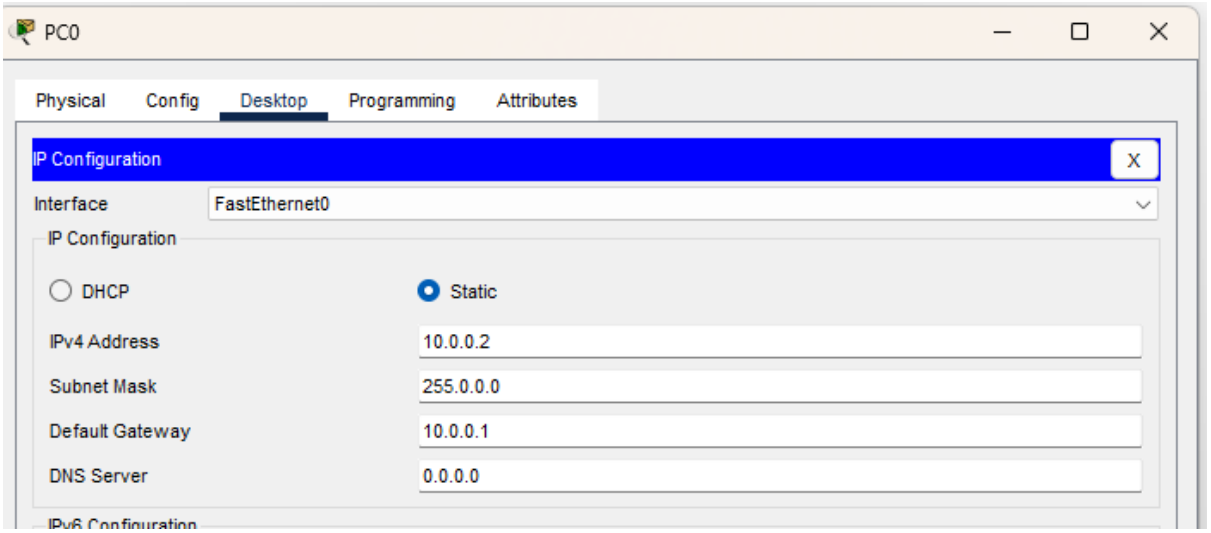
Topology:

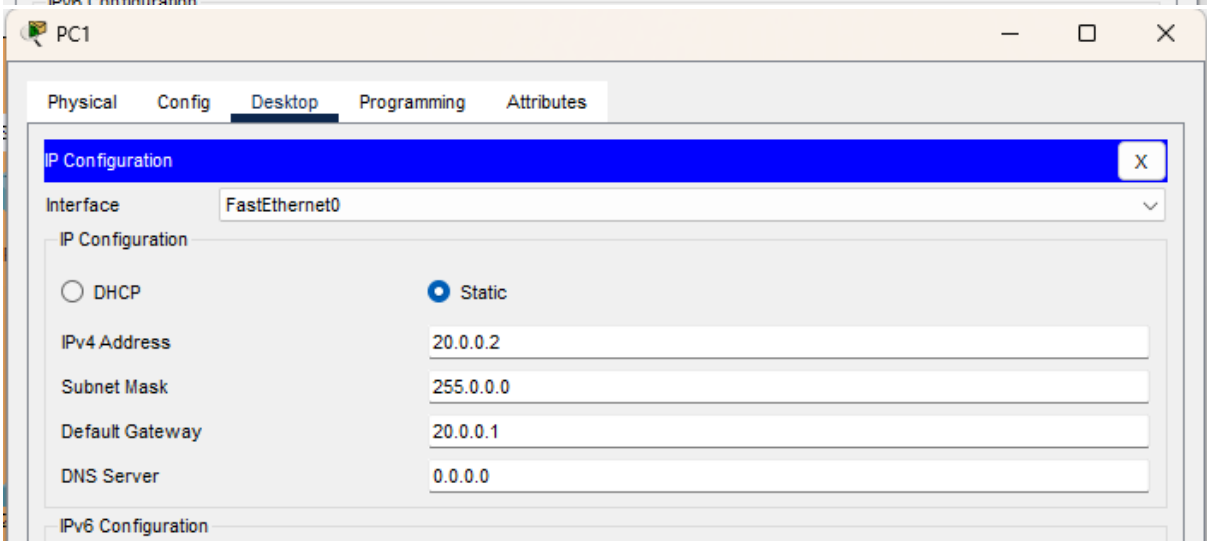


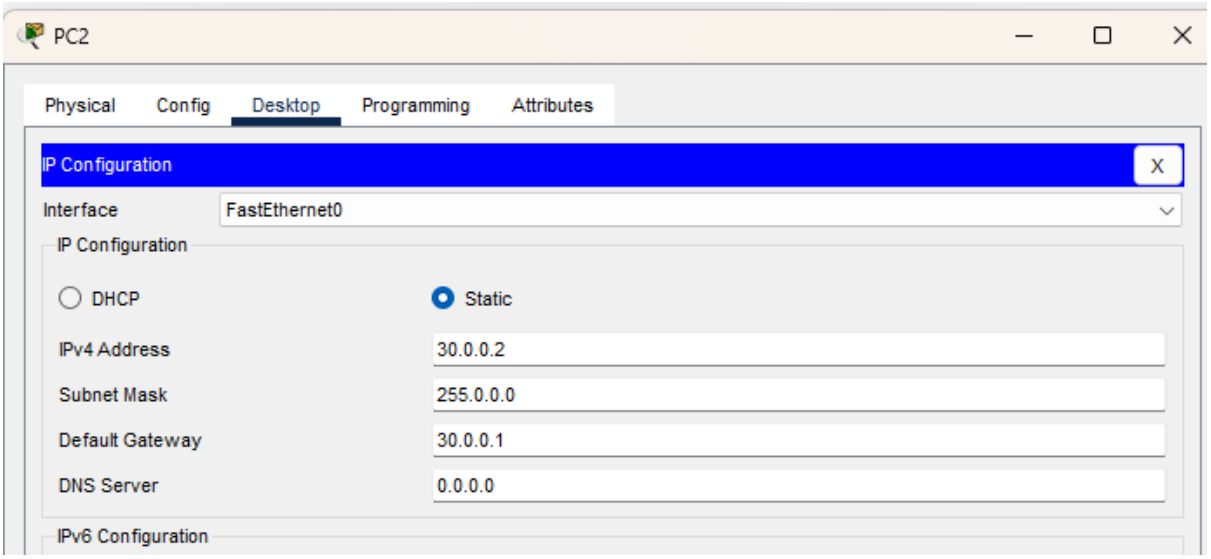
Configuration:

PC Configuration

Go to PC / Desktop / IP Configuration

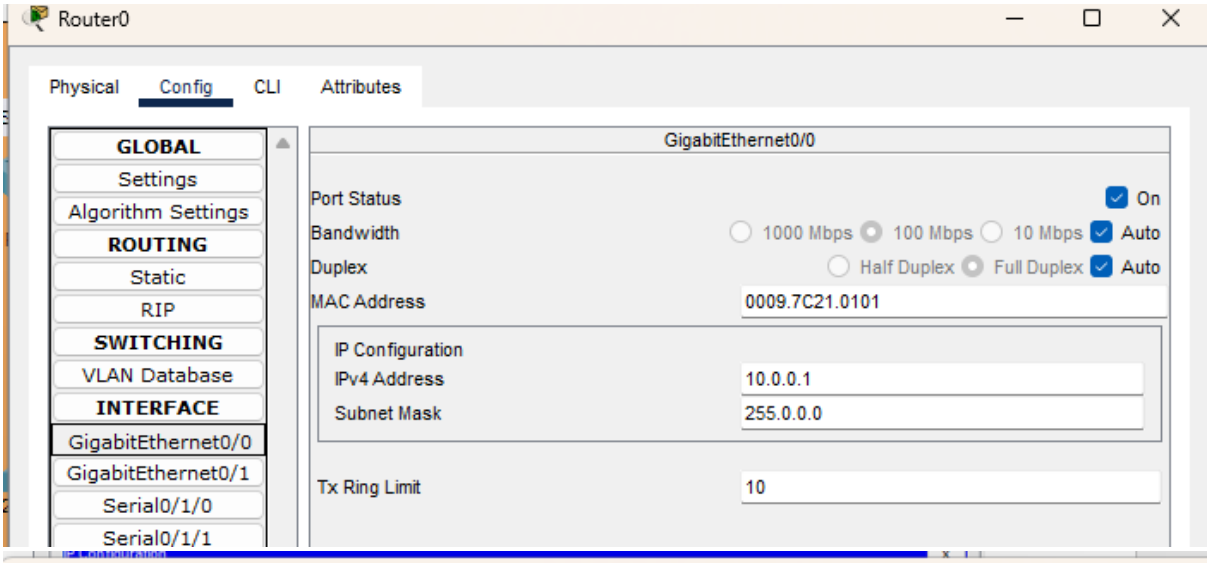

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
10.0.0.2
Subnet Mask
255.0.0.0
Default Gateway
10.0.0.1
DNS Server
0.0.0.0

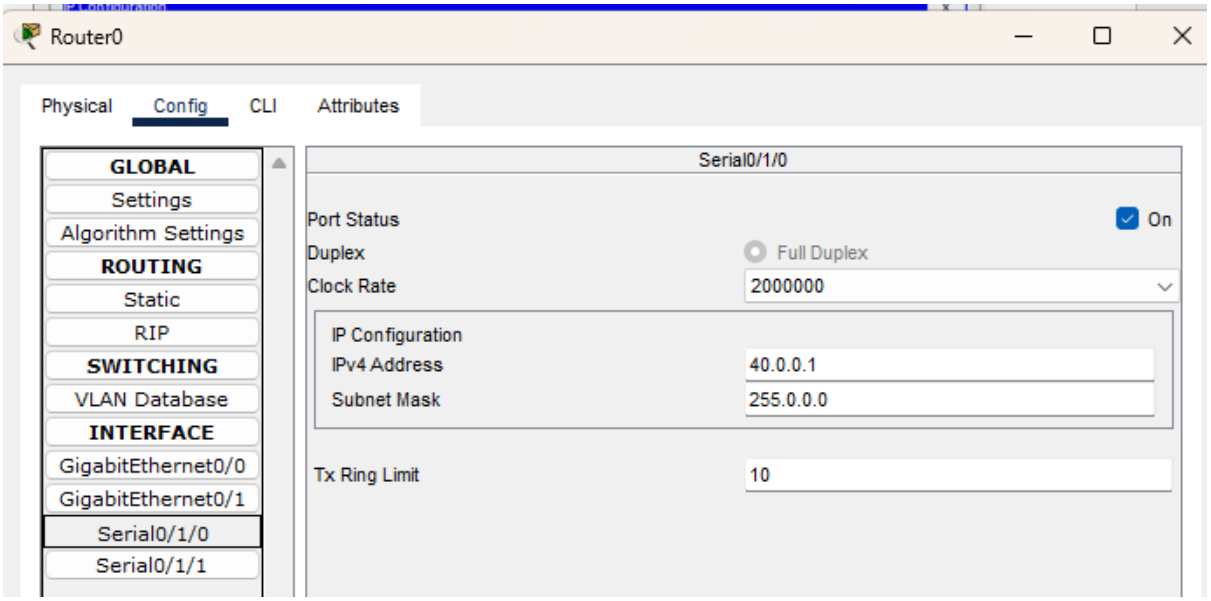

PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
20.0.0.2
Subnet Mask
255.0.0.0
Default Gateway
20.0.0.1
DNS Server
0.0.0.0
IPv6 Configuration


PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
30.0.0.2
Subnet Mask
255.0.0.0
Default Gateway
30.0.0.1
DNS Server
0.0.0.0
IPv6 Configuration

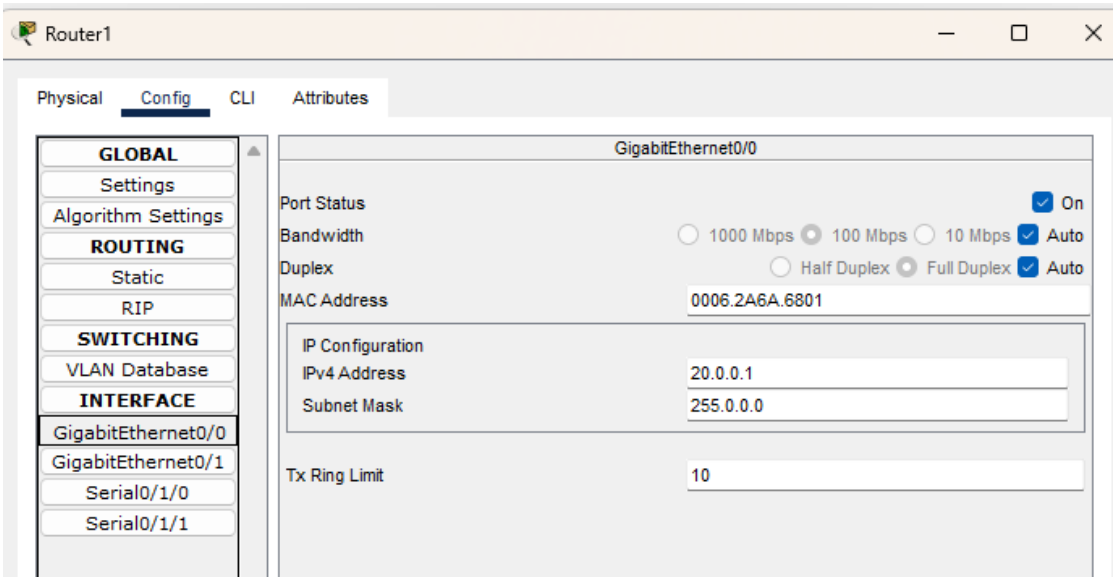
Router Configuration:

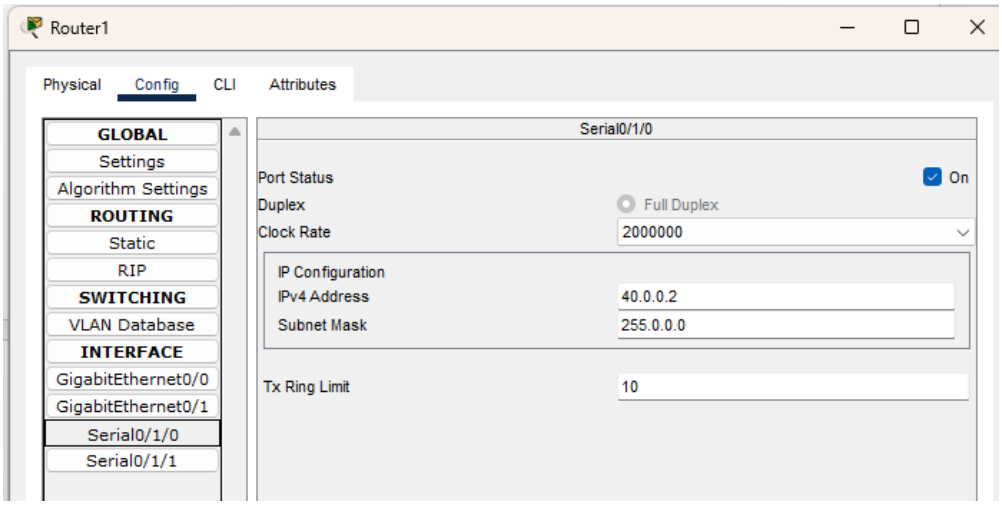
Go to Router / Config

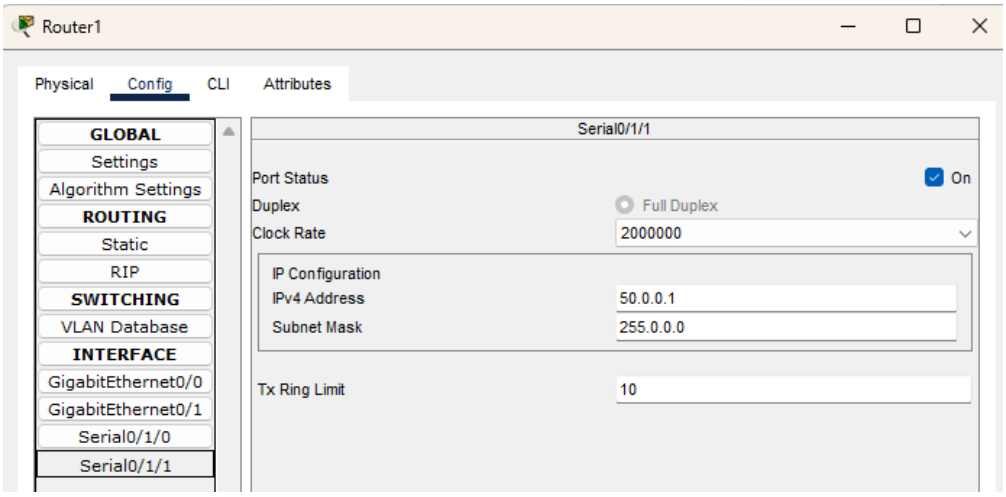




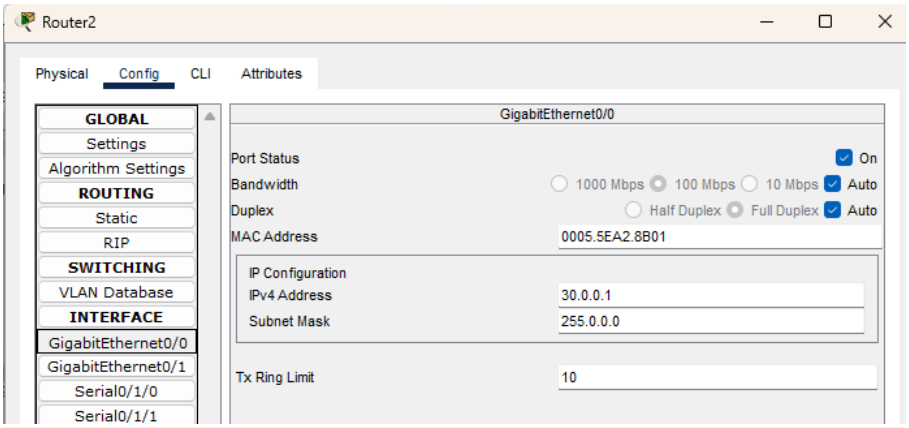
Router1:

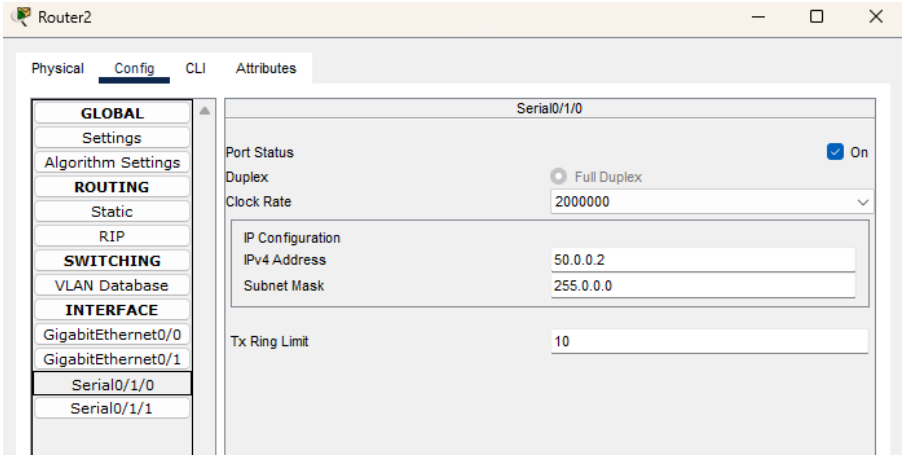



Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
40.0.0.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/1
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
50.0.0.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10

Router2:


Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0005.5EA2.8B01
IP Configuration
IPv4 Address
30.0.0.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10


Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
50.0.0.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10

CLI Mode

Router0

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router bgp 1
Router(config-router)# network 40.0.0.0
Router(config-router)# network 10.0.0.0
Router(config-router)# neighbor 40.0.0.2 remote-as 2
Router(config-router)#ex
Router(config)#
```

Router1:

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router bgp 2
Router(config-router)# network 50.0.0.0
Router(config-router)# network 20.0.0.0
Router(config-router)# network 40.0.0.0
Router(config-router)# network 40.0.0.1 remote-as 1
                                        ^
% Invalid input detected at '^' marker.

Router(config-router)#neighbor 40.0.0.1 remote-as 1
Router(config-router)#neighbor 50.0.0.2 remote-as 3
Router(config-router)#ex
```

Router 2:

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router bgp 3
Router(config-router)#network 50.0.0.0
Router(config-router)#network 30.0.0.0
Router(config-router)#neighbor 50.0.0.1 remote-as 2
Router(config-router)#ex
```

Output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 30.0.0.2

Pinging 30.0.0.2 with 32 bytes of data:

Request timed out.
Reply from 30.0.0.2: bytes=32 time=20ms TTL=125
Reply from 30.0.0.2: bytes=32 time=28ms TTL=125
Reply from 30.0.0.2: bytes=32 time=32ms TTL=125

Ping statistics for 30.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 32ms, Average = 26ms

C:\>
```

Practical No: 07

Aim: Implement IPsec Site-to-Site VPNs connections

What is IPsec VPN?

IPsec (Internet Protocol Security) is a protocol suite that provides secure communication over an untrusted network (like the Internet) by encrypting and authenticating IP packets.

It is used to build Virtual Private Networks (VPNs) — secure tunnels between distant networks.

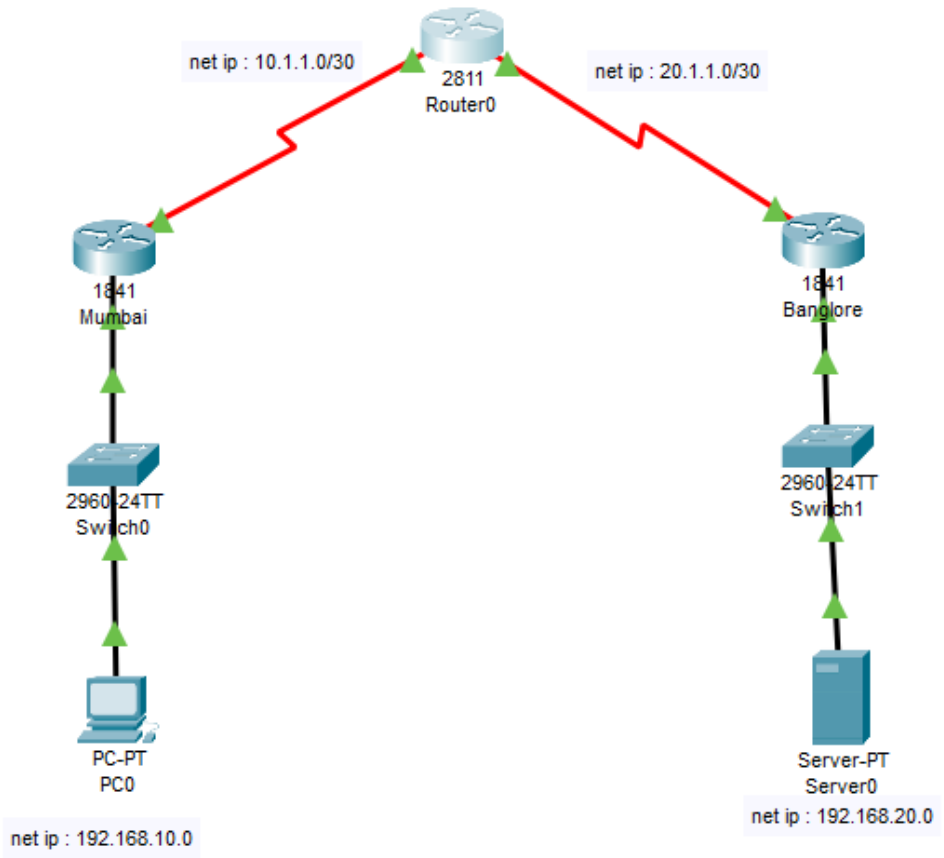
What is a Site-to-Site VPN?

A Site-to-Site VPN connects entire networks (LAN-to-LAN) over the Internet securely.

Example:

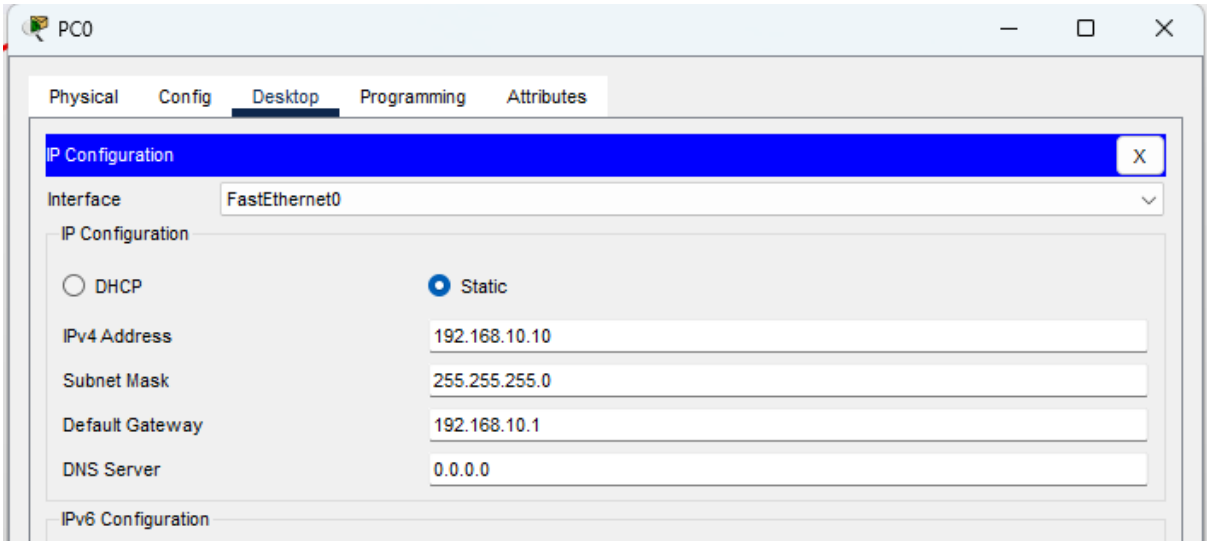
- Head Office (LAN 1) ↔ Branch Office (LAN 2)
- Both sites use routers/firewalls to establish an encrypted tunnel over the Internet using IPsec

Topology:

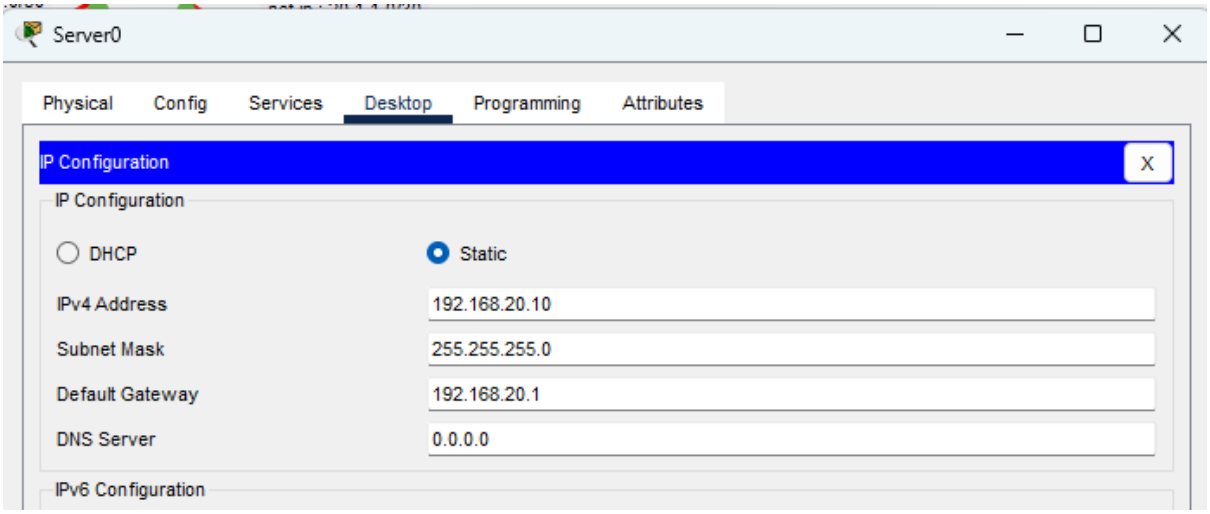


Configuration:

PC Configuration:

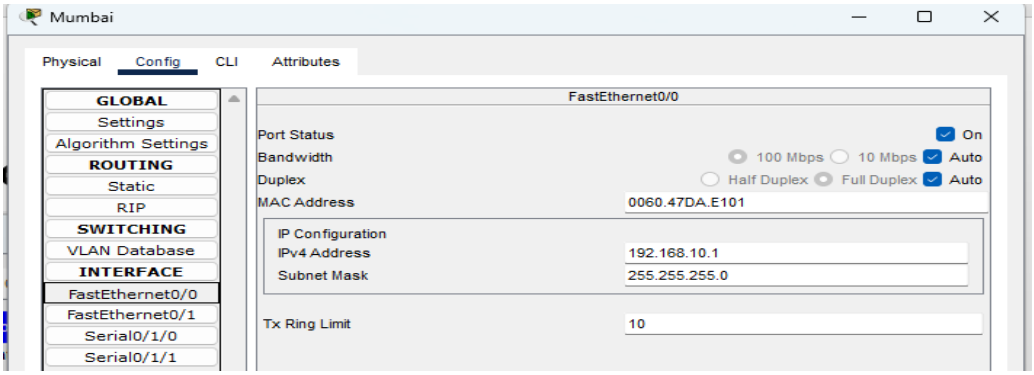


Server Configuration:

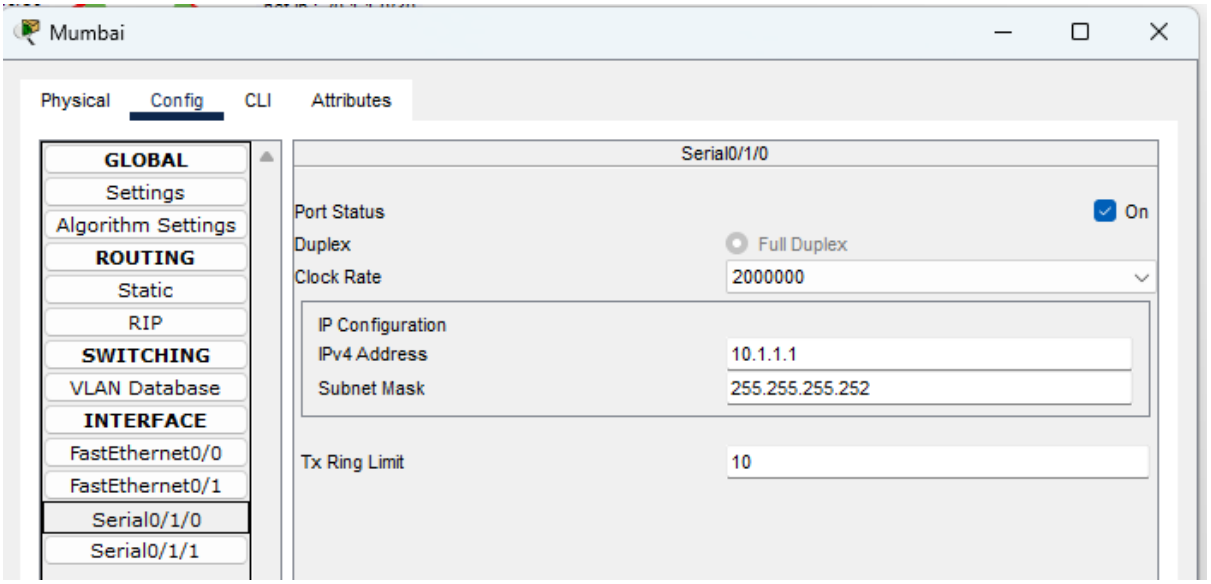


Router Configuration:(Mumbai)

Interface FastEthernet0/0:

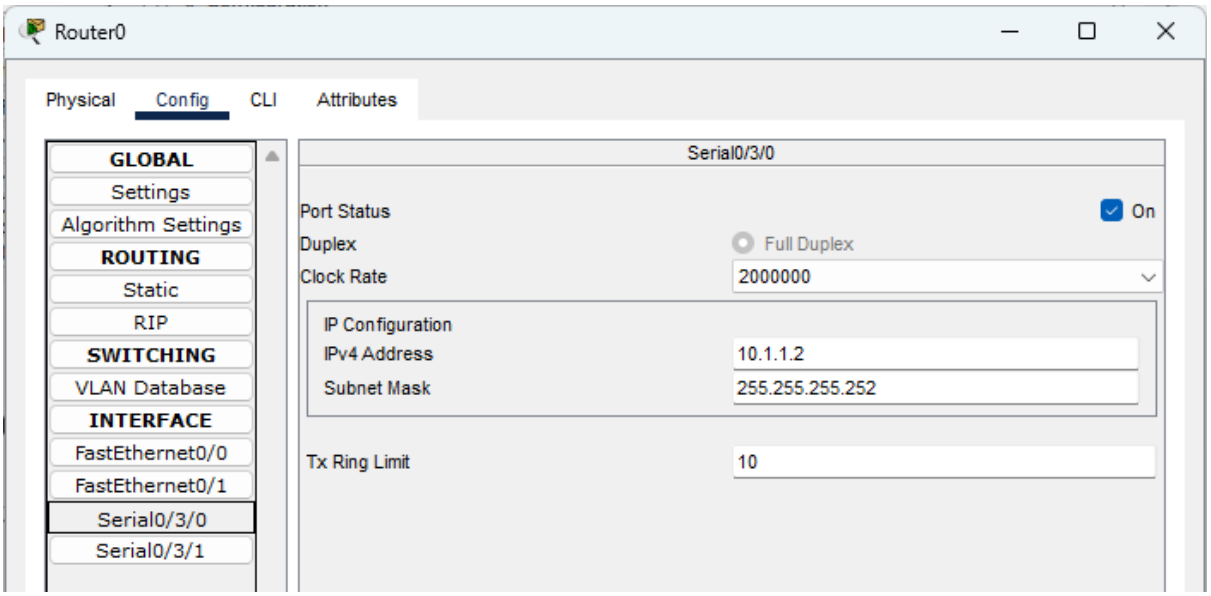


Interface Serial0/1/0:

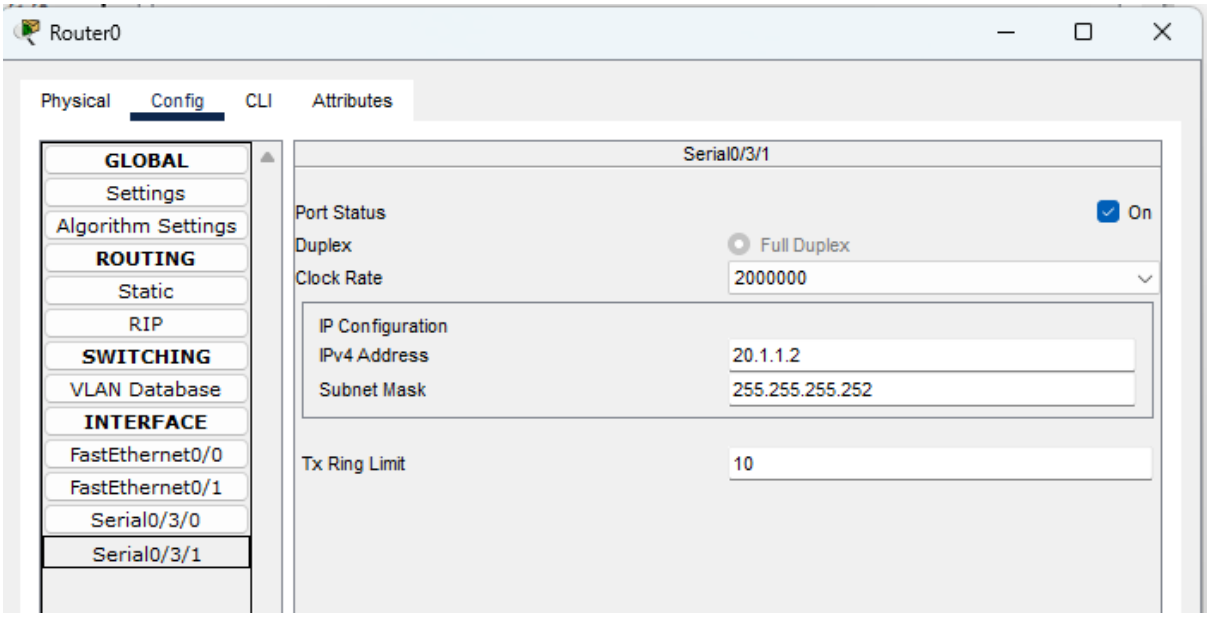


Router Configuration: (Router0)

Interface Serial0/3/0:

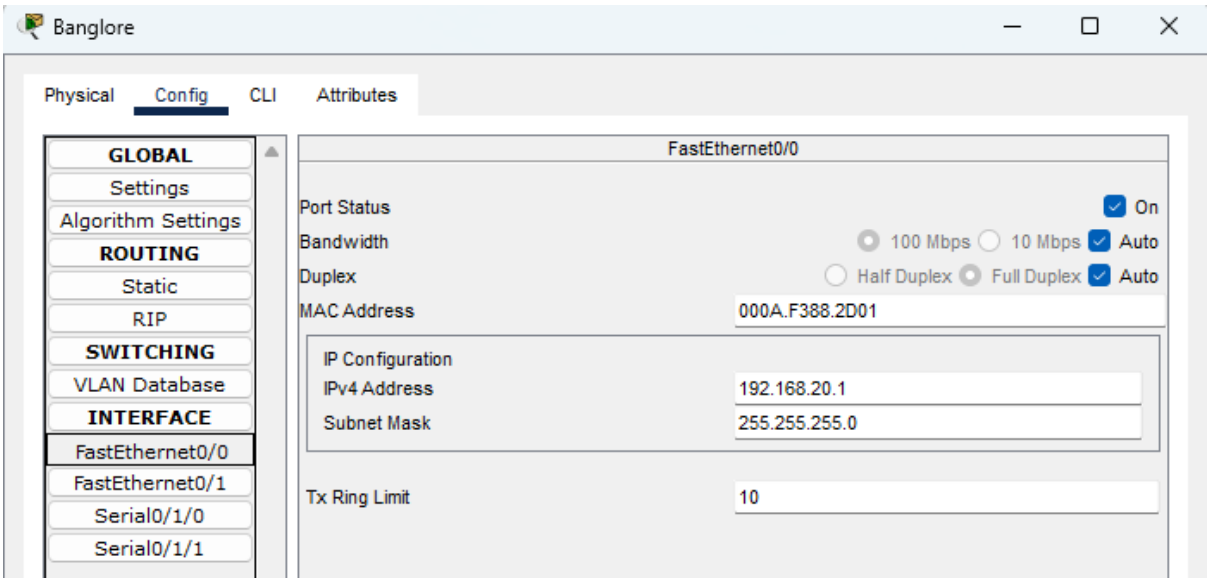


Interface Serial0/3/1:

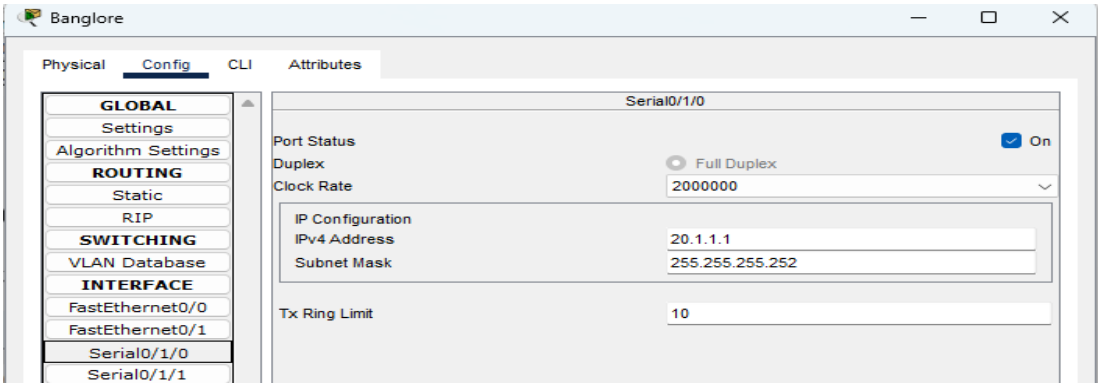


Router Configuration: (Bangalore)

Interface FastEthernet0/0:



Interface Serial0/1/0:



CLI Mode:

Router (Mumbai):

```
mumbai>en
mumbai#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
mumbai(config)#ip access-list extended VPN
mumbai(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
mumbai(config-ext-nacl)#ex
mumbai(config)#crypto isakmp policy 1
mumbai(config-isakmp)#encryption aes
mumbai(config-isakmp)#hash sha
mumbai(config-isakmp)#authentication pre-share
mumbai(config-isakmp)#group 2
mumbai(config-isakmp)#lifetime 86400
mumbai(config-isakmp)#ex
mumbai(config)#crypto isakmp key TimiGate address 20.1.1.2
mumbai(config)#crypto ipsec transform-set TGSET esp-aes esp-sha-hmac
mumbai(config)#crypto map TGMAP 1 ipsec-isakmp
mumbai(config-crypto-map)# set peer 20.1.1.2
mumbai(config-crypto-map)# set transform-set TGSET
mumbai(config-crypto-map)# match address VPN
mumbai(config-crypto-map)#interface Serial0/1/0
mumbai(config-if)# crypto map TGMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
mumbai(config-if)#end
mumbai#
%SYS-5-CONFIG_I: Configured from console by console

mumbai#wr
Building configuration...
[OK]
```

Router (Bangalore):

```
banglore>en
banglore#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
banglore(config)#crypto isakmp policy 1
banglore(config-isakmp)# encryption aes
banglore(config-isakmp)# hash sha
banglore(config-isakmp)# hash sha
banglore(config-isakmp)# authentication pre-share
banglore(config-isakmp)# group 2
banglore(config-isakmp)# lifetime 86400
banglore(config-isakmp)#exit
banglore(config)#crypto isakmp key TimiGate address 10.1.1.2
banglore(config)#crypto ipsec transform-set TGSET esp-aes esp-sha-hmac
banglore(config)#crypto map TGMAP 1 ipsec-isakmp
banglore(config-crypto-map)# set peer 10.1.1.2
banglore(config-crypto-map)# set transform-set TGSET
banglore(config-crypto-map)# match address VPN
banglore(config-crypto-map)#interface Serial0/1/0
banglore(config-if)# crypto map TGMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
banglore(config-if)#end
banglore#
%SYS-5-CONFIG_I: Configured from console by console

banglore#wr
Building configuration...
[OK]
```

From PC:

```
C:\>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:

Reply from 192.168.20.10: bytes=32 time=19ms TTL=126
Reply from 192.168.20.10: bytes=32 time=19ms TTL=126
Reply from 192.168.20.10: bytes=32 time=22ms TTL=126
Reply from 192.168.20.10: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 22ms, Average = 15ms
```

From Server:

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=19ms TTL=254
Reply from 192.168.10.1: bytes=32 time=4ms TTL=254
Reply from 192.168.10.1: bytes=32 time=21ms TTL=254
Reply from 192.168.10.1: bytes=32 time=2ms TTL=254

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 21ms, Average = 11ms

C:\>
```

Practical No: 08

Aim: Demonstrate Multilayer switch-based Networking

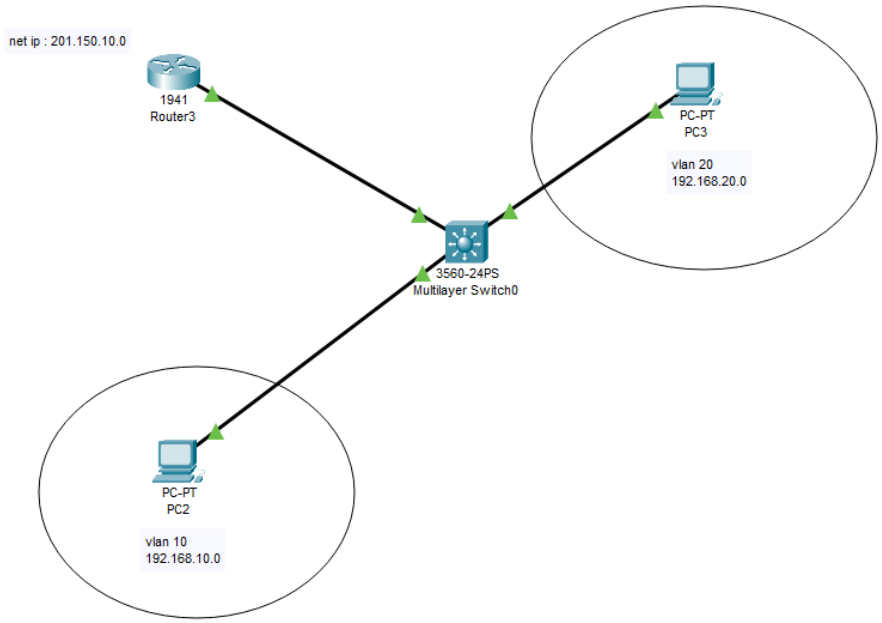
Description:

A multilayer switch (MLS) works at both Layer 2 (Switching) and Layer 3 (Routing) of the OSI model.
It can create VLANs and also route between them without using a separate router — using SVI (Switch Virtual Interfaces).

Key Features:

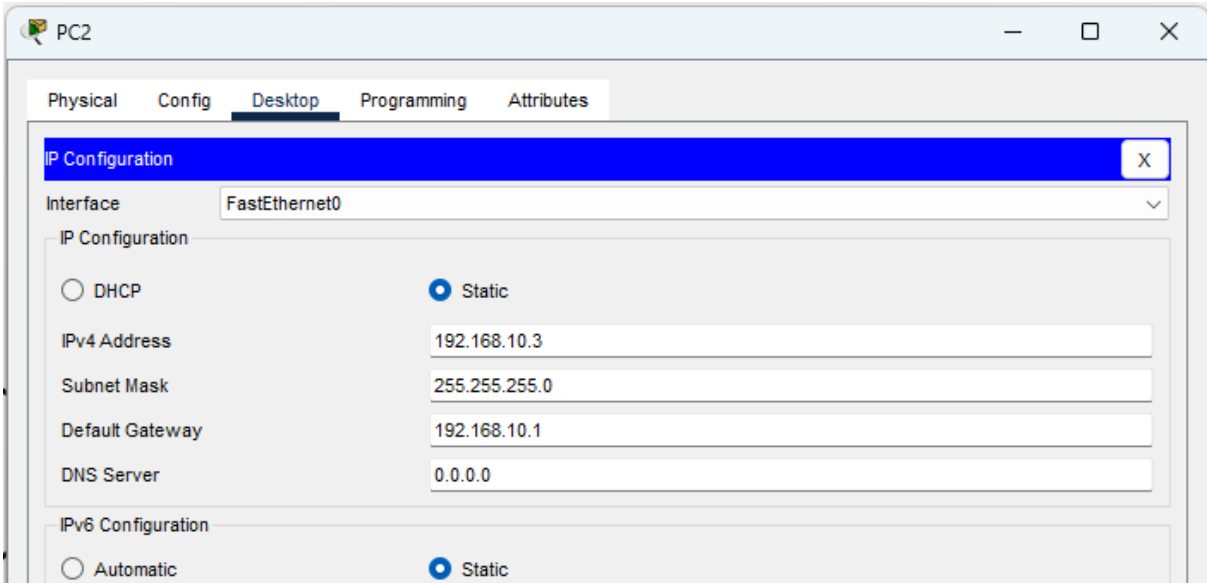
- Performs both switching and routing functions
- Supports VLAN segmentation
- Uses SVI for inter-VLAN routing
- Provides high performance and reduced latency

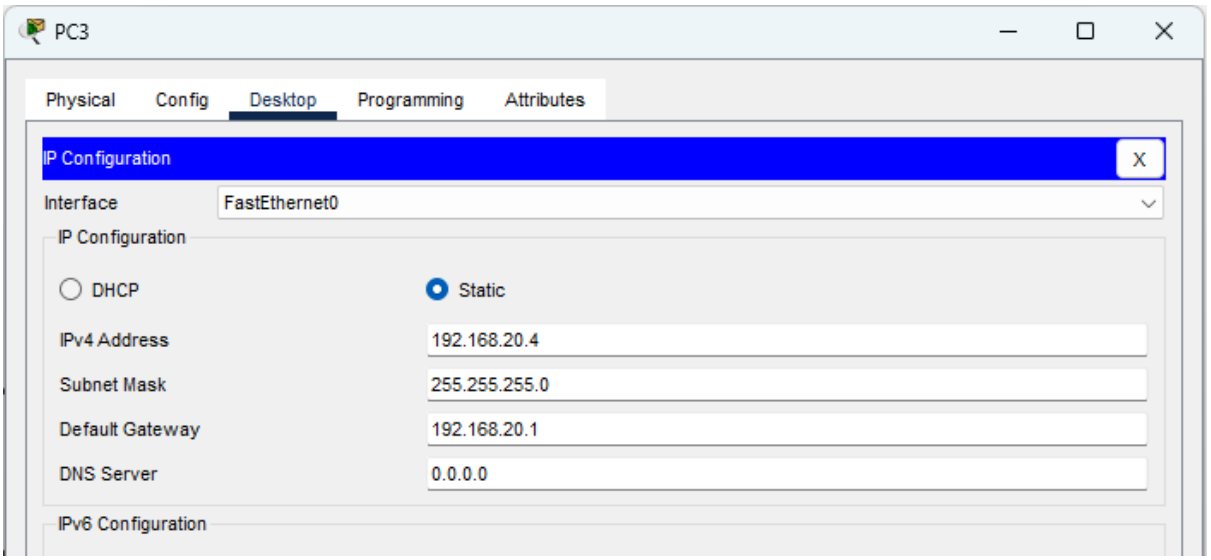
Topology:



Configuration:

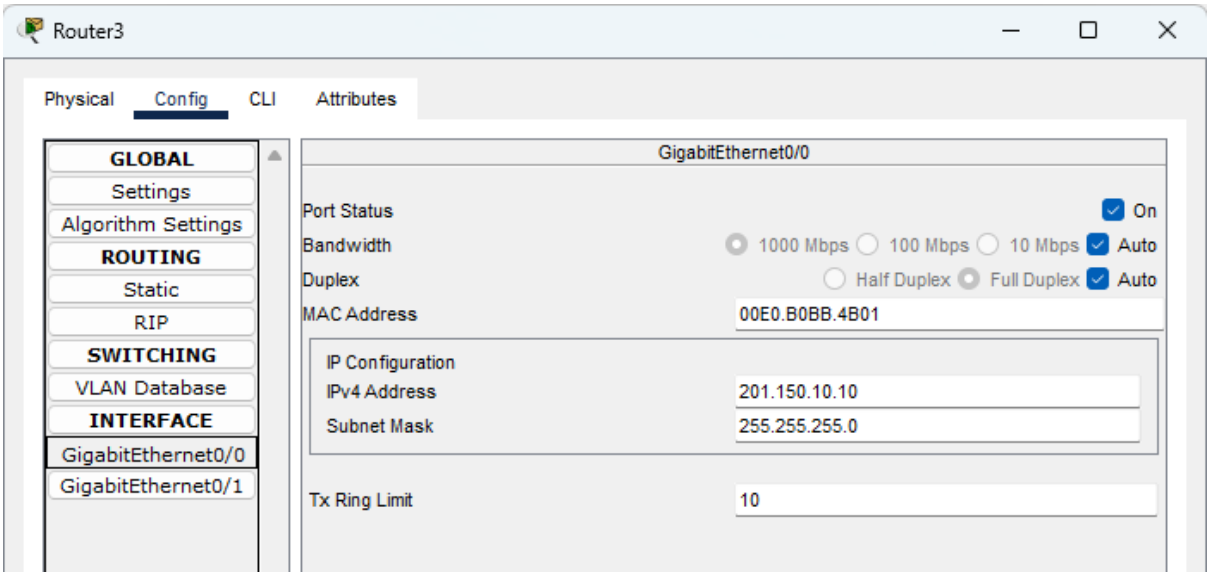
PC Configuration:





Router Configuration:

Interface FastEthernet0/0:



CLI Mode:

Multi-Layer Switch0:

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastEthernet0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#ex
Switch(config)#interface fastEthernet0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#ex
Switch(config)#ip routing
Switch(config)#interface vlan 10
Switch(config-if)#ip address 192.168.10.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#ex
Switch(config)#interface vlan 20
Switch(config-if)#ip address 192.168.20.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#ex
Switch(config)#
```

Output:

From PC2:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.4

Pinging 192.168.20.4 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.4: bytes=32 time<1ms TTL=127
Reply from 192.168.20.4: bytes=32 time<1ms TTL=127
Reply from 192.168.20.4: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

From PC2:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time<1ms TTL=127
Reply from 192.168.10.3: bytes=32 time<1ms TTL=127
Reply from 192.168.10.3: bytes=32 time<1ms TTL=127
Reply from 192.168.10.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```