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 (Access Control List).

A. Standard ACL.
B. Extended ACL.

1. Introduction to ACL

- **ACL (Access Control List)** is a set of rules used to control traffic in and out of a network device like a router or switch. It is used to permit or deny packets based on various conditions.
- ACLs are used in Cisco routers and switches to enhance **network security**, filter traffic, and control access to network resources.
- ACLs can filter traffic based on criteria such as **IP address**, **protocol type**, and **port number**.
- ACLs are applied to **interfaces** and can be configured to affect **inbound or outbound traffic**.
- ACLs help administrators **control network traffic**, **block unauthorized access**, and **enforce security policies**.

---

2. Where ACL is Used

ACLs are typically used in the following scenarios:

- To **allow or block** traffic from specific IP addresses or networks.
- To **enhance network security** by restricting unauthorized access.
- In **firewalls and routers** to define traffic control policies.
- To **filter routing updates** in routing protocols.
- In **Quality of Service (QoS)** to prioritize or limit certain types of traffic.

---

3. Types of ACLs in Cisco

✅ Standard ACL

- Filters traffic based **only on source IP address**.
- Simple and less resource-intensive.
- Typically placed **near the destination**.
- **Numbered Range:**
  - **1 to 99**
- **Example**: access-list 10 permit 192.168.1.0 0.0.0.255

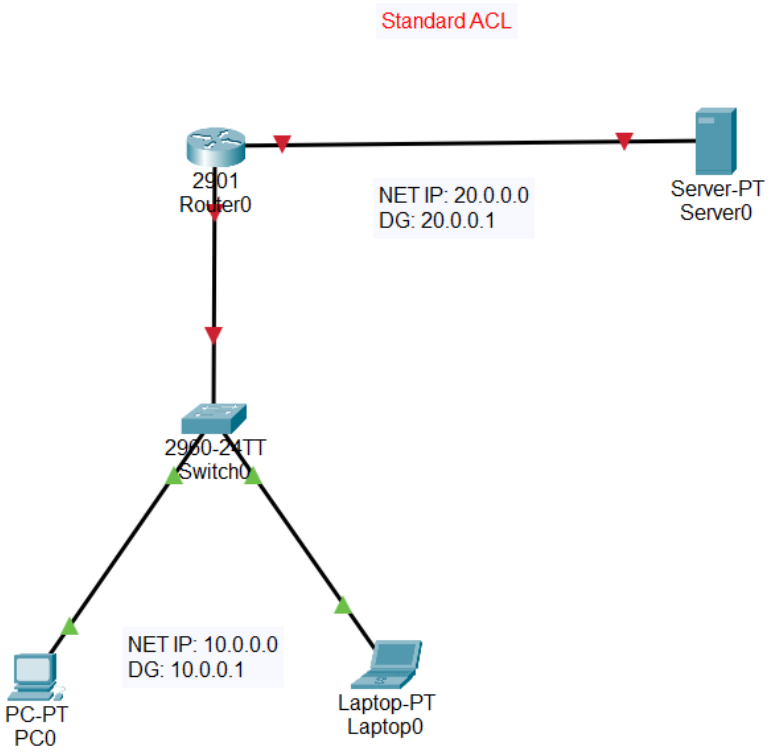
✅ Extended ACL

- Filters traffic based on **source and destination IP addresses**, **protocols (TCP, UDP, ICMP)**, and **port numbers**.
- Provides more granular control.
- Typically placed **near the source**.
- **Numbered Range:**
  - **100 to 199**
- **Example:** access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 80

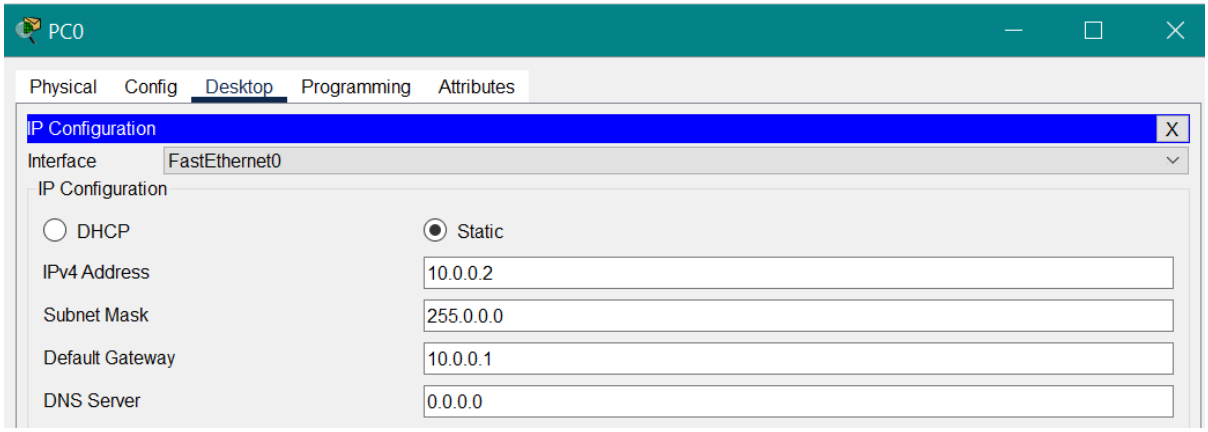
A. Standard ACL.

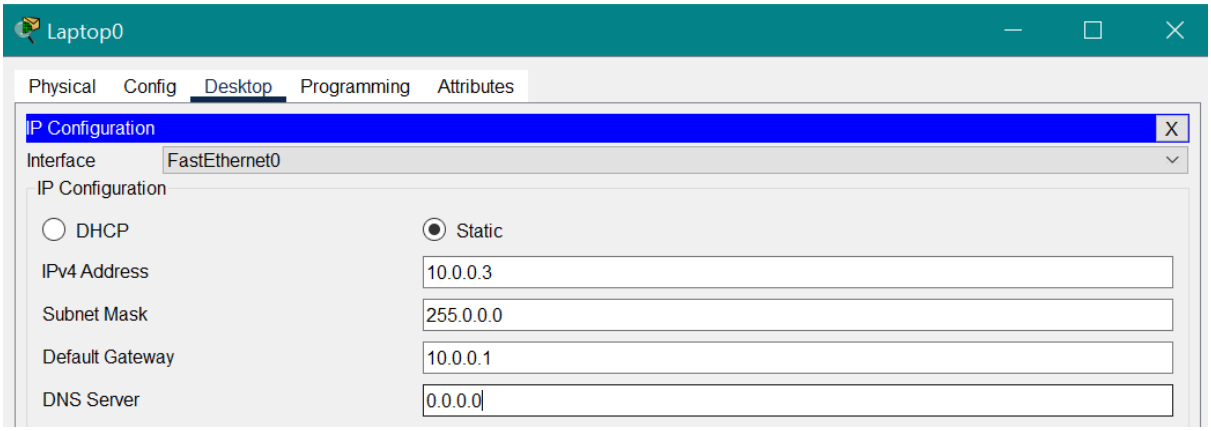
Steps to Configure Standard ACL (Access Control List) on Cisco Packets Tracer:

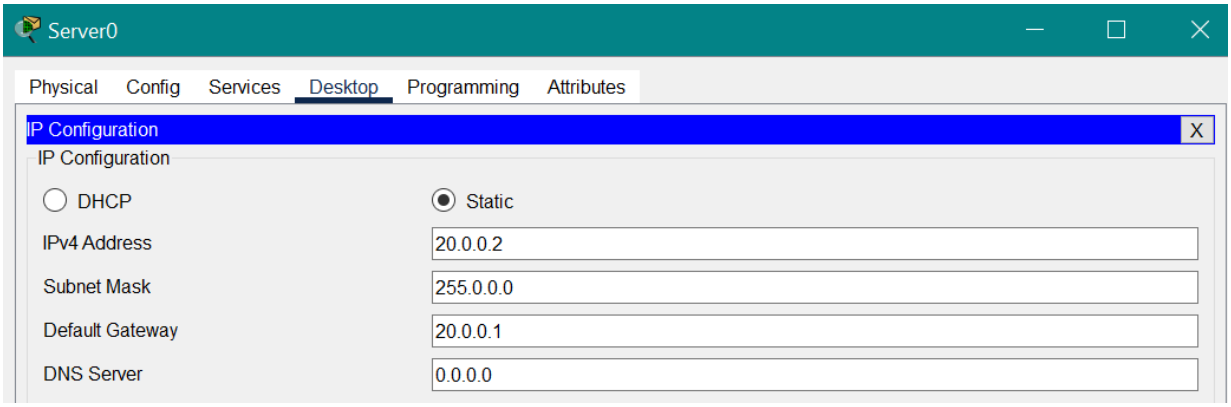
Topology:

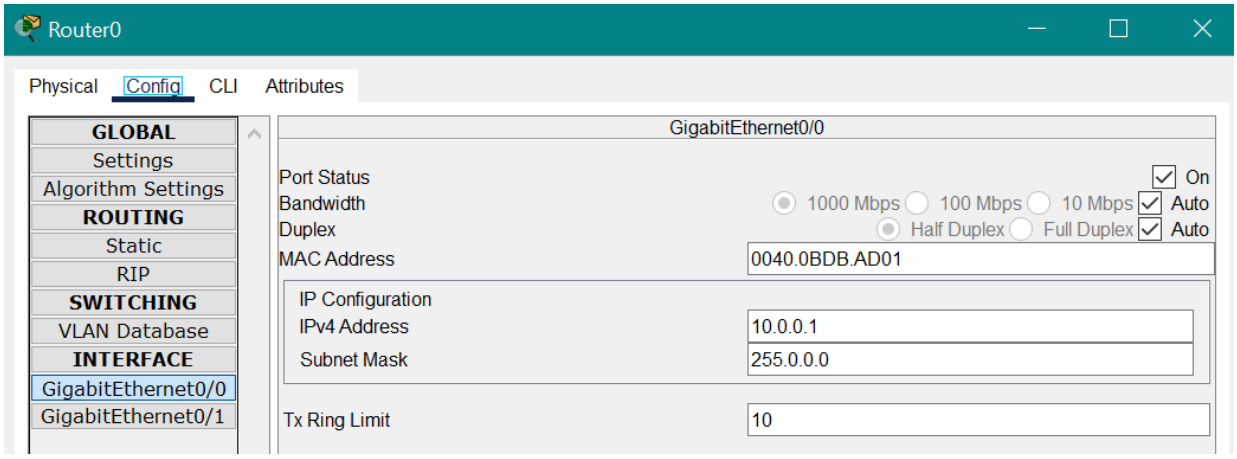


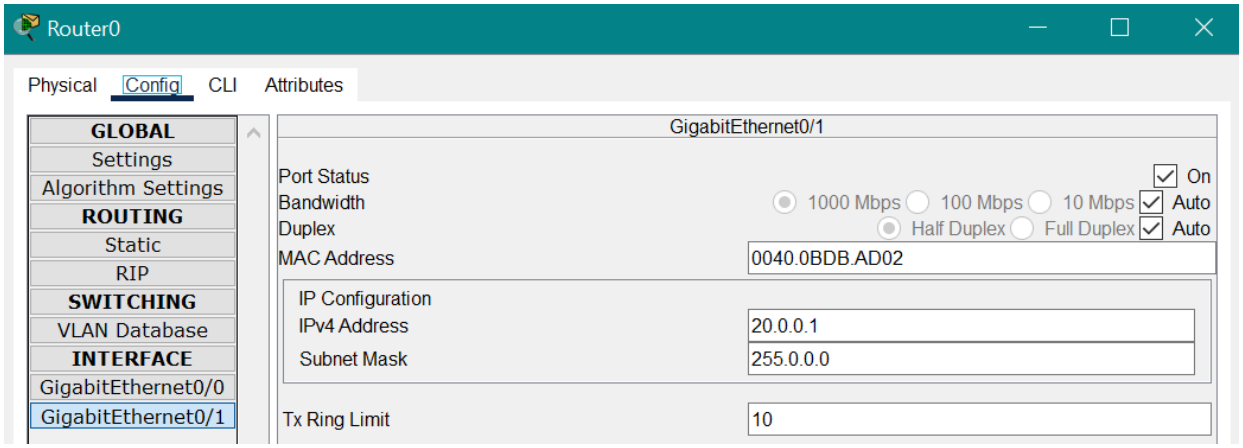
Assigning IP`s:





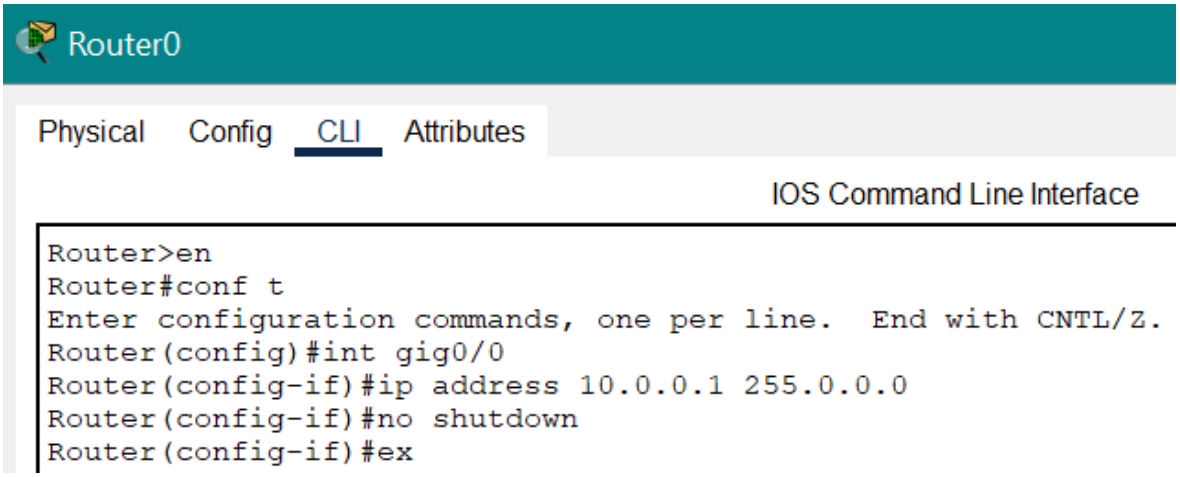






Let's configure the router and create standard ACL to permit or deny traffic Configure Router Interface.

LAN Interface (connected to PC & Laptop)



Server Side Interface

Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig0/1
Router(config-if)#ip address 20.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#ex
Router(config)#
```

Create Standard ACL

Suppose we want to deny Laptop0 (10.0.0.3) from reaching the Server, and allow all other traffic.

Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>EN
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 10 deny 10.0.0.3
Router(config)#access-list 10 permit any
Router(config)#int gig0/1
Router(config-if)#ip access-group 10 out
Router(config-if)#ex
Router(config)#ex
Router#
```

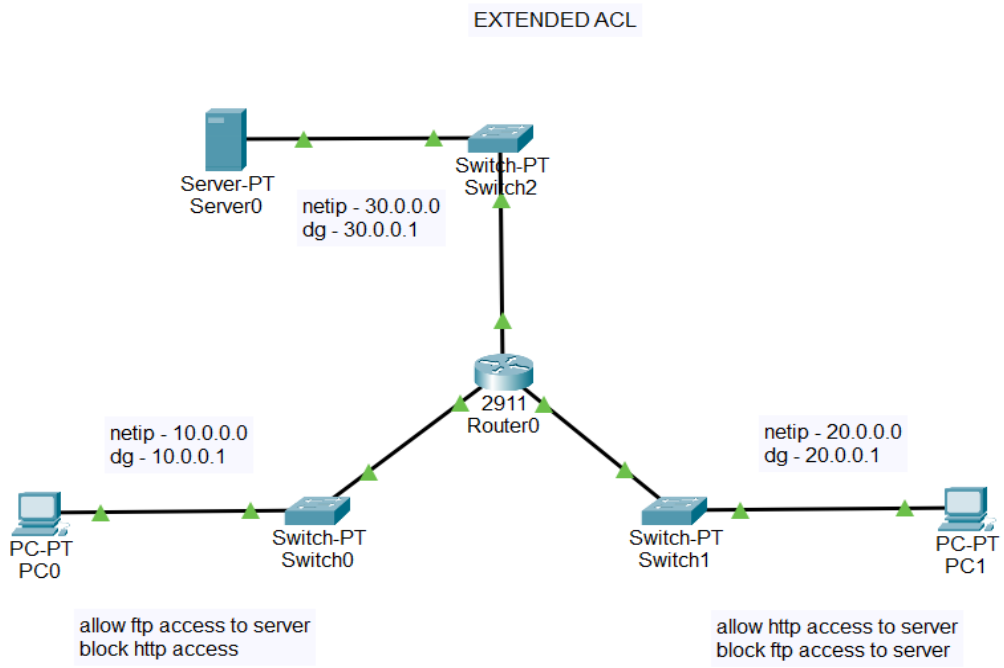
OUTPUT:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Server0	PC0	ICMP		0.000	N	0	(edit)	(delete)
	Failed	Server0	Laptop0	ICMP		0.000	N	1	(edit)	(delete)
	Failed	Laptop0	Server0	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC0	Server0	ICMP		0.000	N	3	(edit)	(delete)

B. Extended ACL.

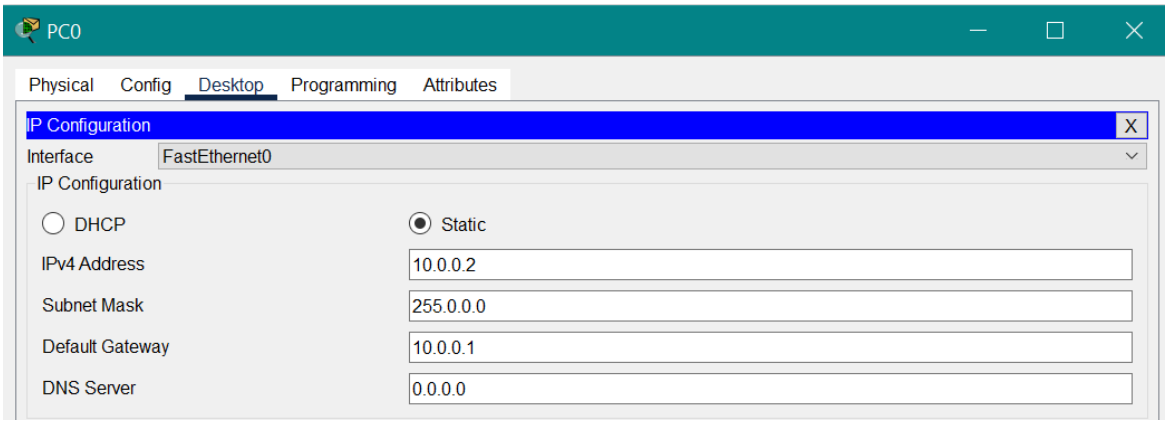
Steps to Configure Extended ACL (Access Control List) on Cisco Packets Tracer:

Topology:

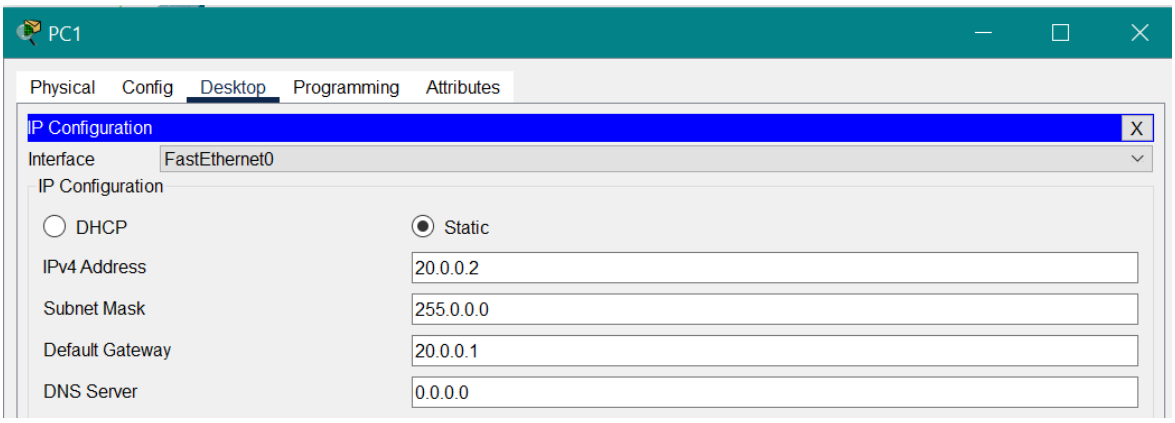


Assigning IP's:

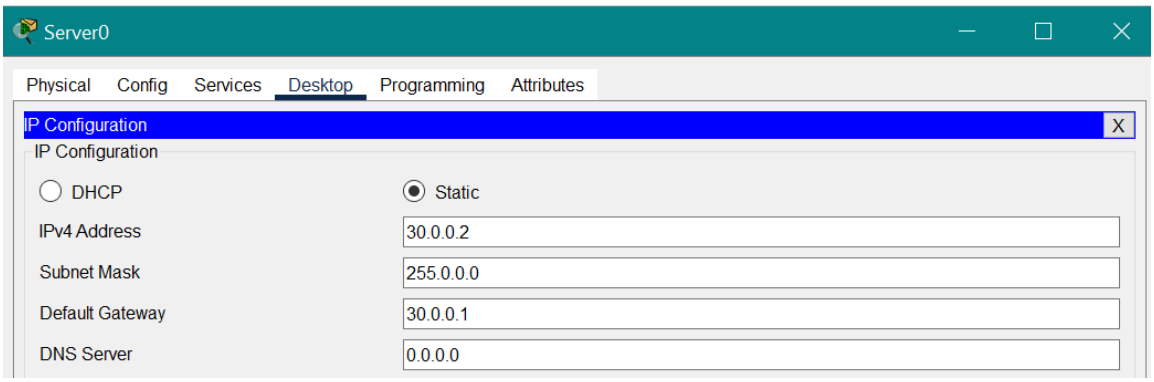
- **PC0**



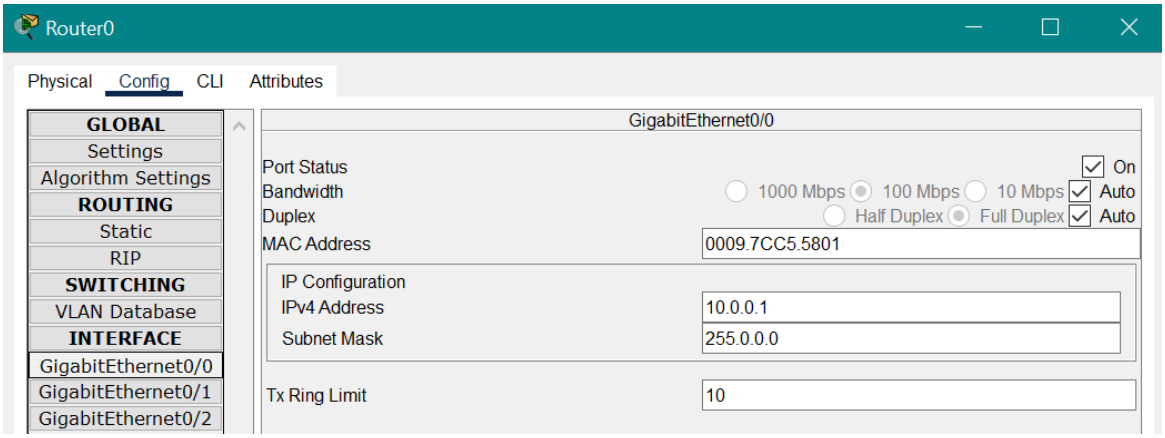
- PC1



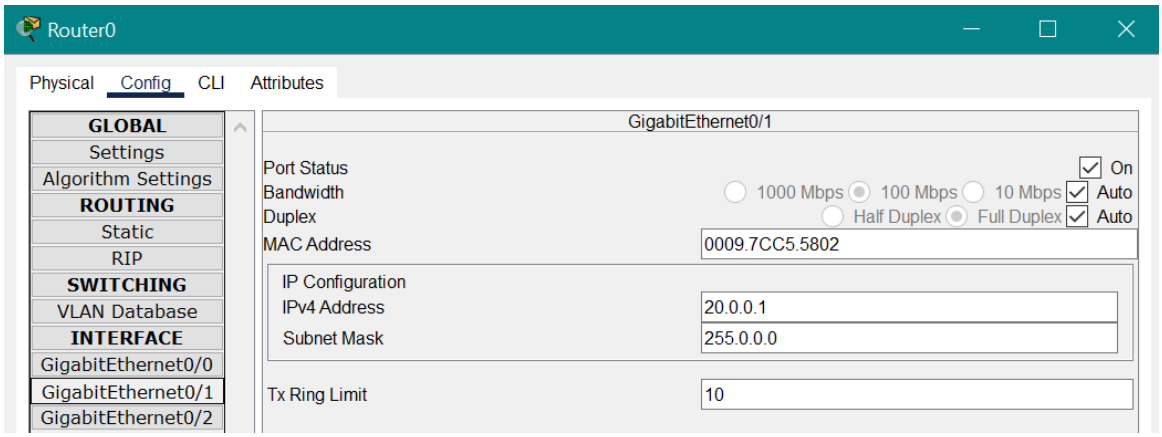
- Server0



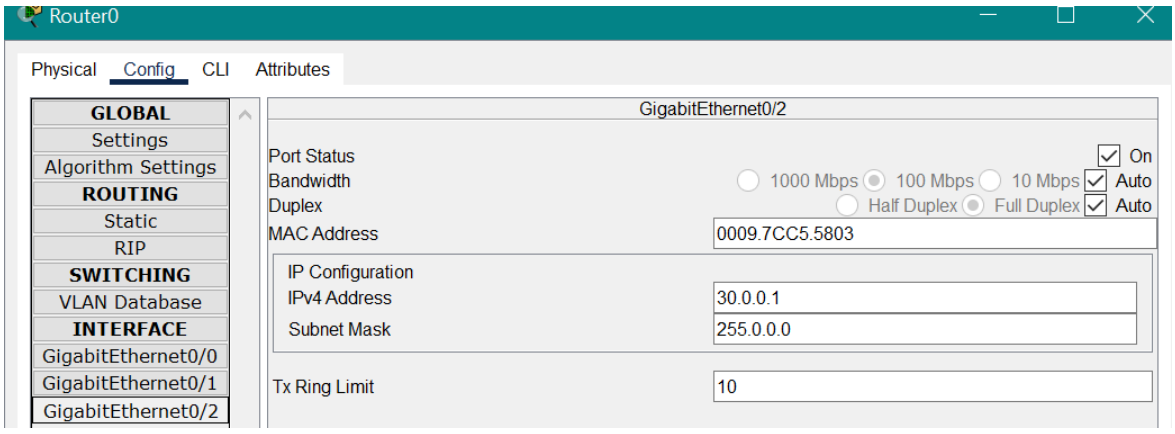
- Gig0/0



- Gig0/1



- Gig0/2



For PC0:

- allow ftp access to server
- block http access

Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 deny tcp 10.0.0.0 0.255.255.255 host 30.0.0.2 eq www
Router(config)#access-list 100 permit ip any any
Router(config)#int gig0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#ex
Router(config)#ex
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#sh access-list
Extended IP access list 100
    10 deny tcp 10.0.0.0 0.255.255.255 host 30.0.0.2 eq www
    20 permit ip any any
```

PC0

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
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:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit

221- Service closing control connection.
C:\>telnet 30.0.0.2 80
Trying 30.0.0.2 ...
% Connection timed out; remote host not responding
C:\>
```

PC0

Physical Config Desktop Programming Attributes

Web Browser

< > URL http://30.0.0.2 Go Stop

Request Timeout

For PC1:

- allow http access to server
- block ftp access to server

Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
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 0.255.255.255 host 30.0.0.2 eq ftp
Router(config)#access-list 120 permit ip any any
Router(config)#int gig0/1
Router(config-if)#ip access-group 120 in
Router(config-if)#ex
Router(config)#ex
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#sh access-list
Extended IP access list 100
    10 deny tcp 10.0.0.0 0.255.255.255 host 30.0.0.2 eq www
    20 permit ip any any
Extended IP access list 120
    10 deny tcp 20.0.0.0 0.255.255.255 host 30.0.0.2 eq ftp
    20 permit ip any any
```

PC1

Physical Config Desktop Programming Attributes

Command Prompt

```
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)



C:\>telnet 30.0.0.2 80
Trying 30.0.0.2 ...Open

[Connection to 30.0.0.2 closed by foreign host]
C:\>
```

PC1

Physical Config Desktop Programming Attributes

Web Browser

< > URL http://30.0.0.2 Go Stop

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

PRACTICAL NO : 2

AIM: Implement **SPAN** Technologies (Switch Port Analyzer).
A. Local Span
B. Remote Span

1. Introduction to Span

- A span is the portion of a communication path or circuit between two points in a telecommunication or computer network.
- A span represents the link or section of transmission line such as copper wire, fiber optic cable, or microwave link that connects switching centers or devices.
- A span is important because it helps in establishing communication, dividing the network into smaller sections, and ensuring reliable data or voice transmission.

---

2. Why Span is Used

- A span is used to connect two exchanges or devices for communication.
- A span is used to divide the communication path into manageable sections for easier maintenance.
- A span is used to ensure efficient and reliable transmission of data or voice.
- A span is used to extend communication over both short and long distances.

---

3. Types of Span

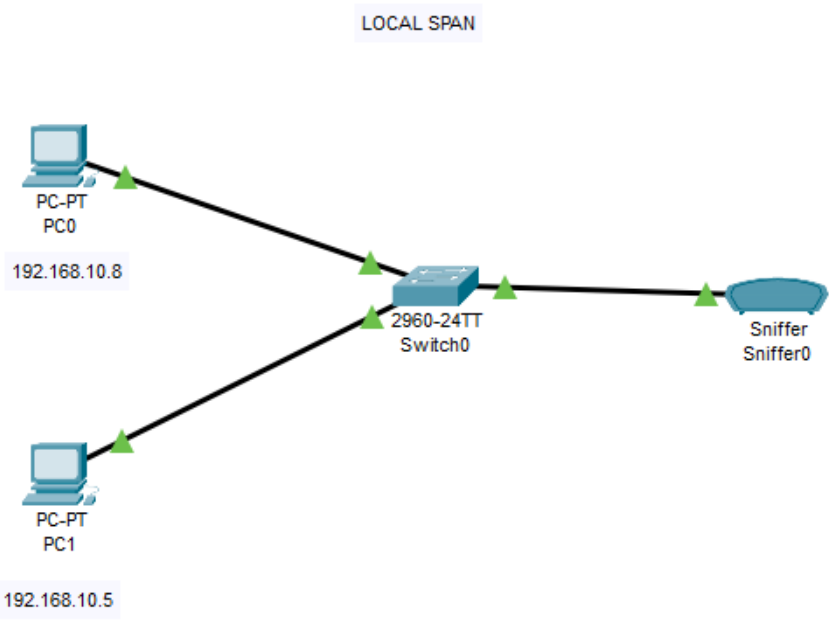
✓ Local Span

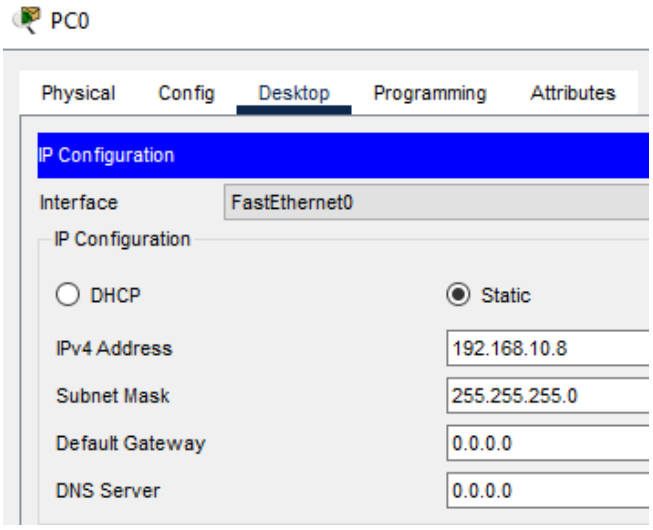
- A local span is the type of span that lies within the same exchange area.
- A local span usually covers only a short distance.
- A local span does not require any long-distance transmission facility.
- For example, two telephones connected in the same city exchange represent a local span.

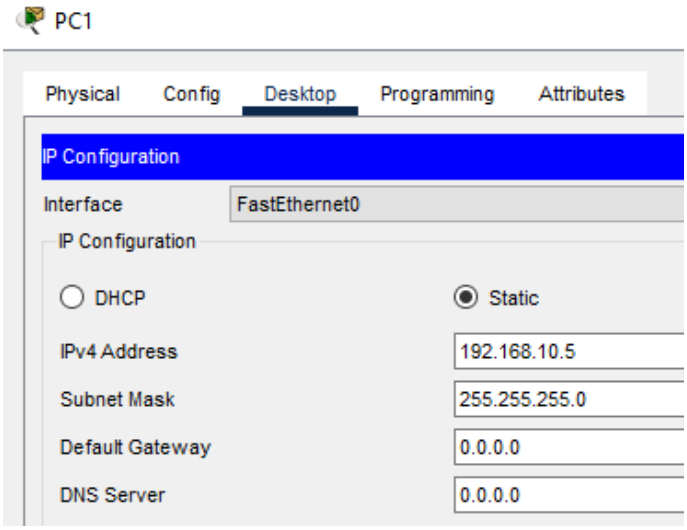
✓ Remote Span

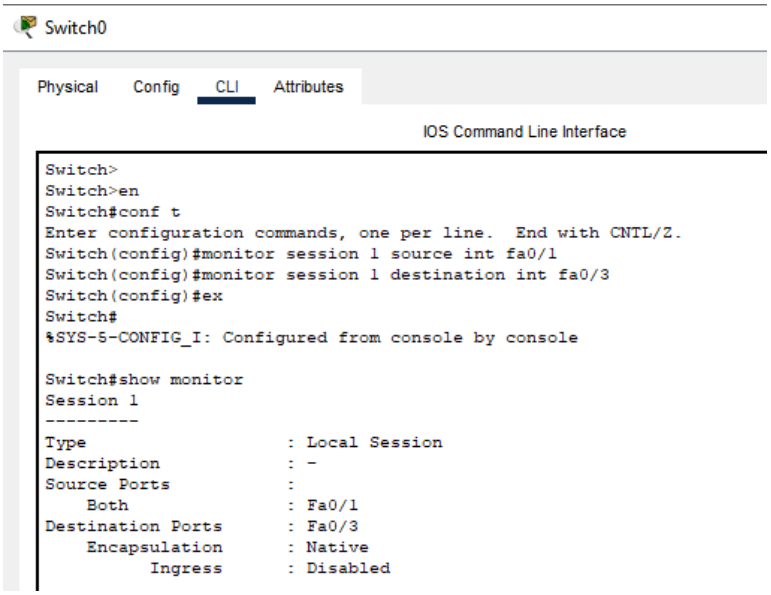
- A remote span is the type of span that connects exchanges or devices in different areas or cities.
- A remote span usually covers a long distance.
- A remote span requires long-distance transmission mediums such as fiber optic cables, microwave links, or satellite communication.
- For example, a telephone call from Delhi to Mumbai represents a remote span.

A) LOCAL SPAN










```
Switch#
Switch#sh monitor session 1 detail
Session 1
---------
Type                   : Local Session
Description            : -
Source Ports           :
    RX Only            : None
    TX Only            : None
    Both               : Fa0/1
Source VLANs           :
    RX Only            : None
    TX Only            : None
    Both               : None
Source RSPAN VLAN      : None
Destination Ports      : Fa0/3
    Encapsulation      : Native
          Ingress      : Disabled
Filter VLANs           : None
Dest RSPAN VLAN        : None
```

.....

OUTPUT:

PC0

Physical Config Desktop Programming Attributes

Command Prompt

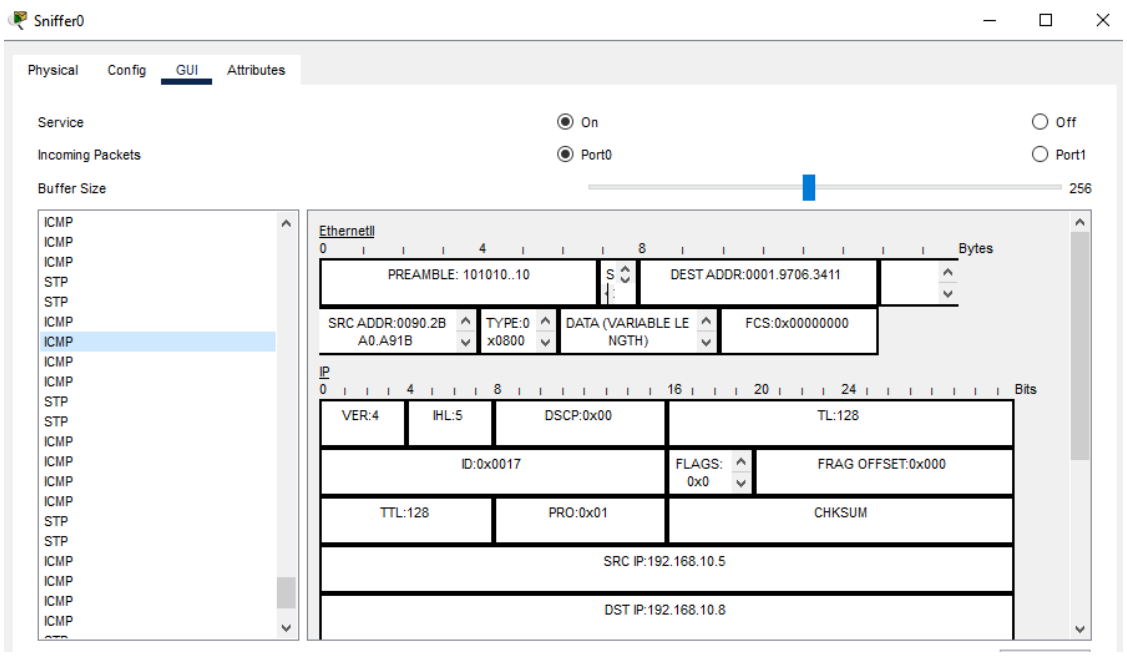
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.5

Pinging 192.168.10.5 with 32 bytes of data:

Reply from 192.168.10.5: bytes=32 time<1ms TTL=128
Reply from 192.168.10.5: bytes=32 time<1ms TTL=128
Reply from 192.168.10.5: bytes=32 time<1ms TTL=128
Reply from 192.168.10.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

PC1

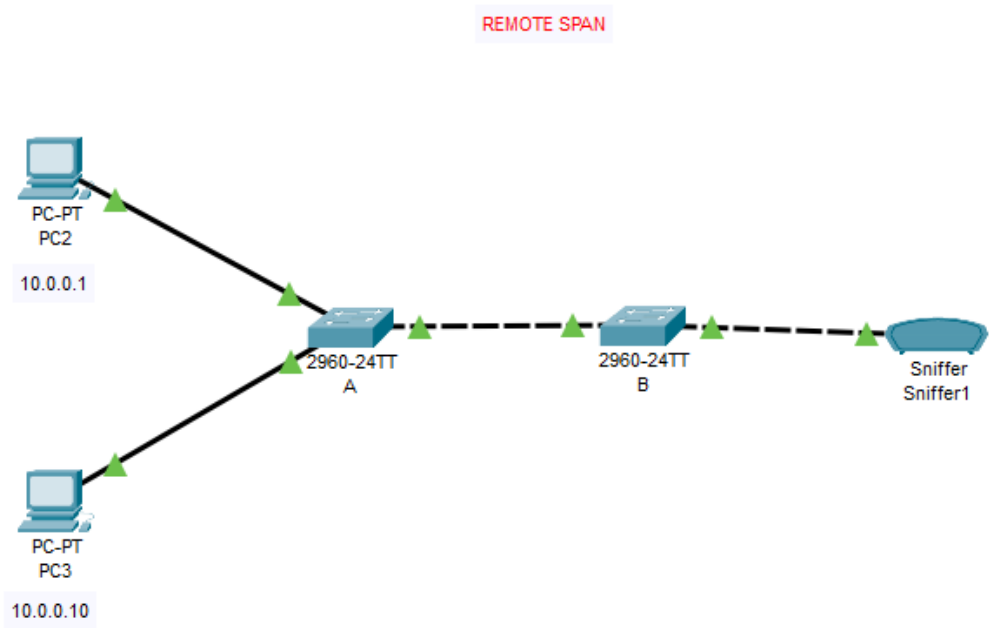
Physical Config Desktop Programming Attributes

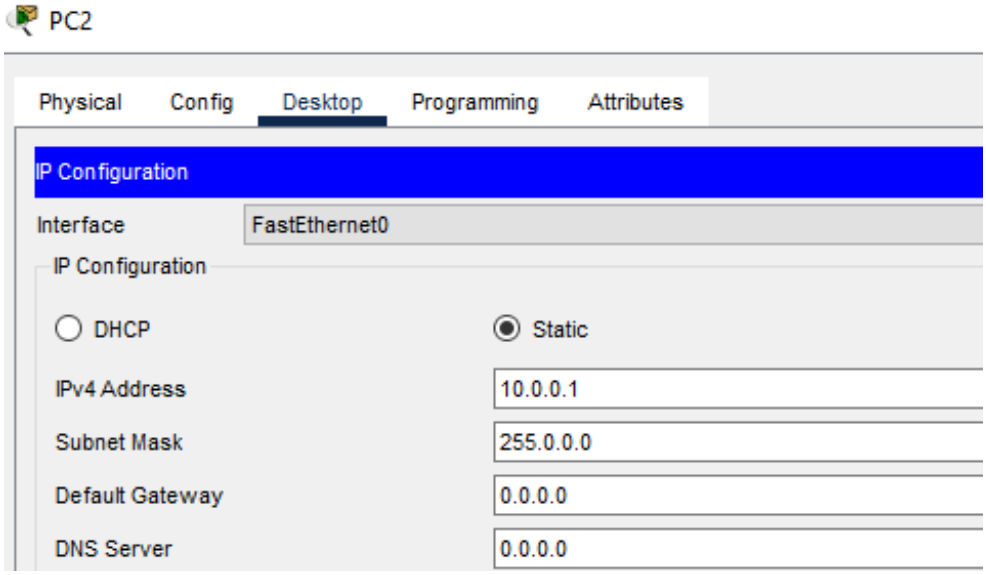
Command Prompt

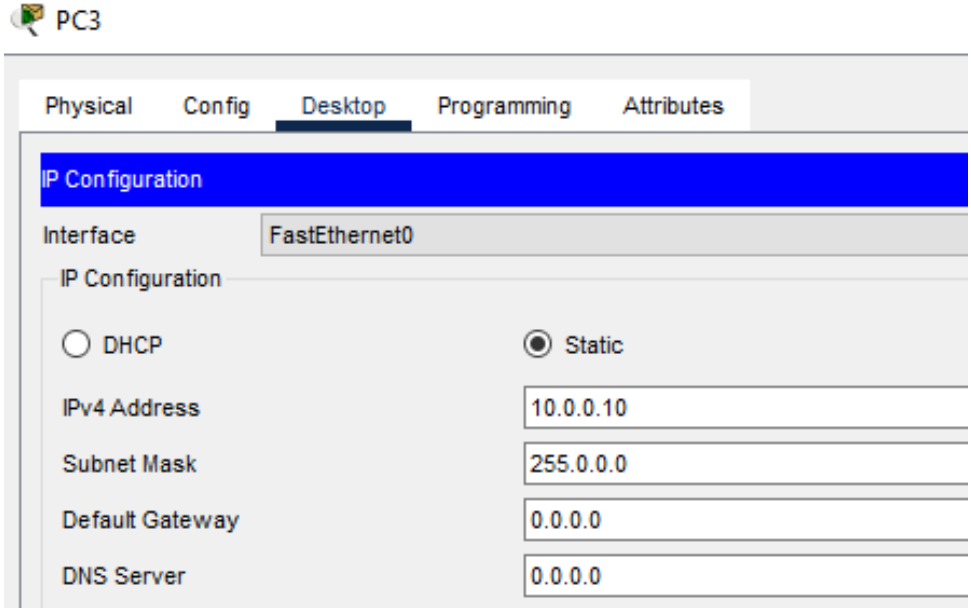
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.8

Pinging 192.168.10.8 with 32 bytes of data:

Reply from 192.168.10.8: bytes=32 time<1ms TTL=128
Reply from 192.168.10.8: bytes=32 time<1ms TTL=128
Reply from 192.168.10.8: bytes=32 time<1ms TTL=128
Reply from 192.168.10.8: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

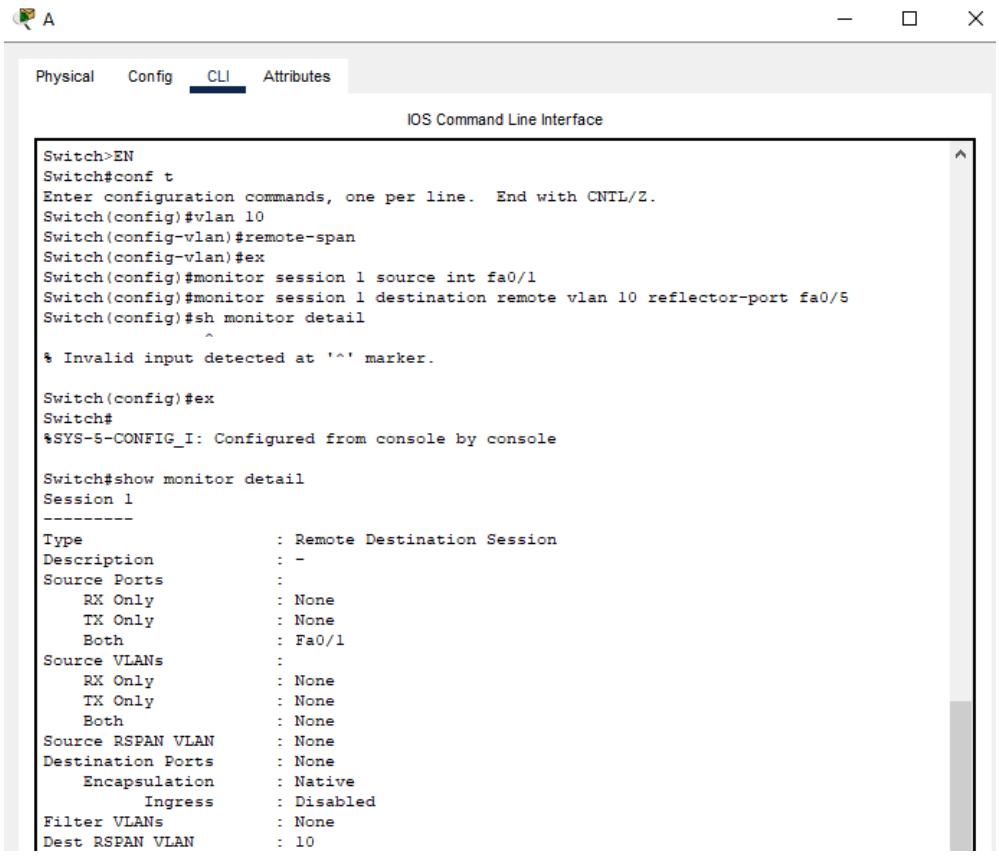


B) REMOTE SPAN:



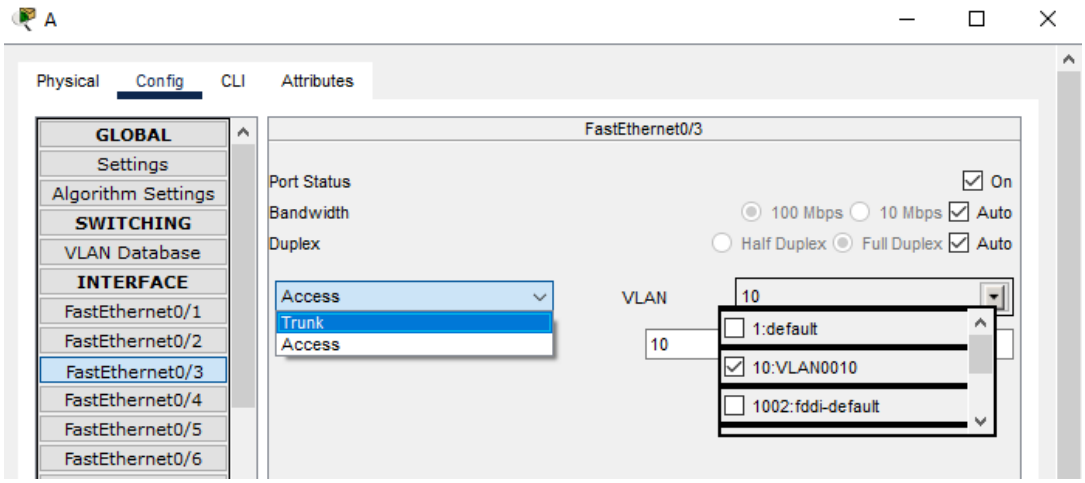


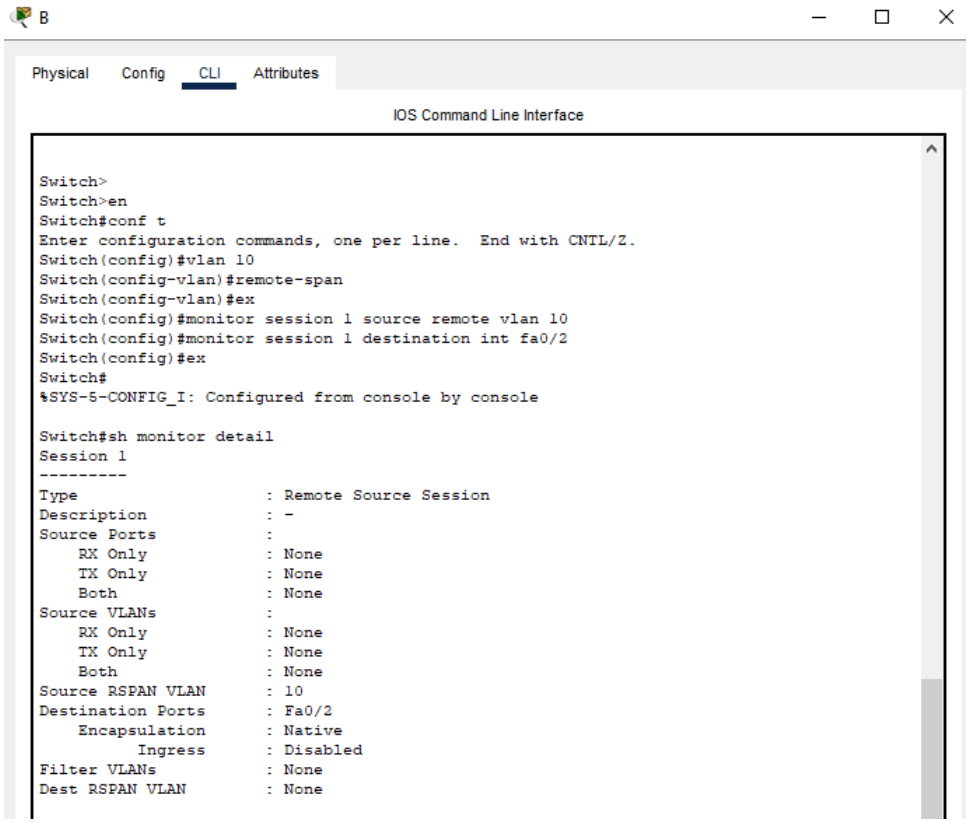




Remove monitor>>no monitor session 1

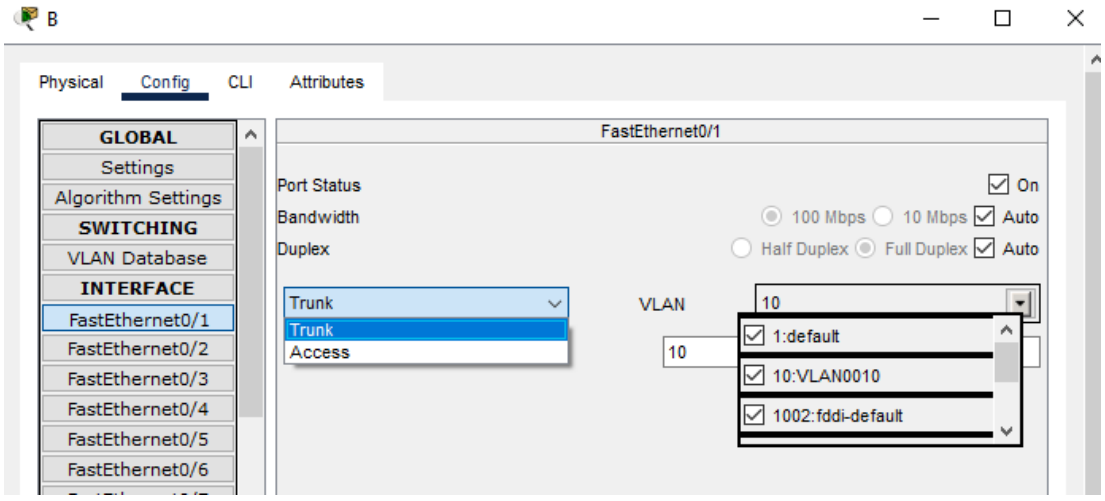
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no monitor session 1
Switch(config)#vlan 10
Switch(config-vlan)#remote-span
Switch(config-vlan)#ex
Switch(config)#monitor session 1 source int fa0/1
Switch(config)#monitor session 1 destination remote vlan 10 reflector-port fa0/5
Switch(config)#ex
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#sh monitor detail





Remove monitor>>no monitor session 1

Switch(config-if)#no monitor session 1
Switch(config)#vlan 10
Switch(config-vlan)#remote-span
Switch(config-vlan)#ex
Switch(config)#monitor session 1 source remote vlan 10
Switch(config)#monitor session 1 destination int fa0/2
Switch(config)#
Switch(config)#ex
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#sh monitor detail



NOTE: If icmp is not available so remove monitor session on both switch and restart the configuration

OUTPUT:

PC3

Physical Config Desktop Programming Attributes

Command Prompt

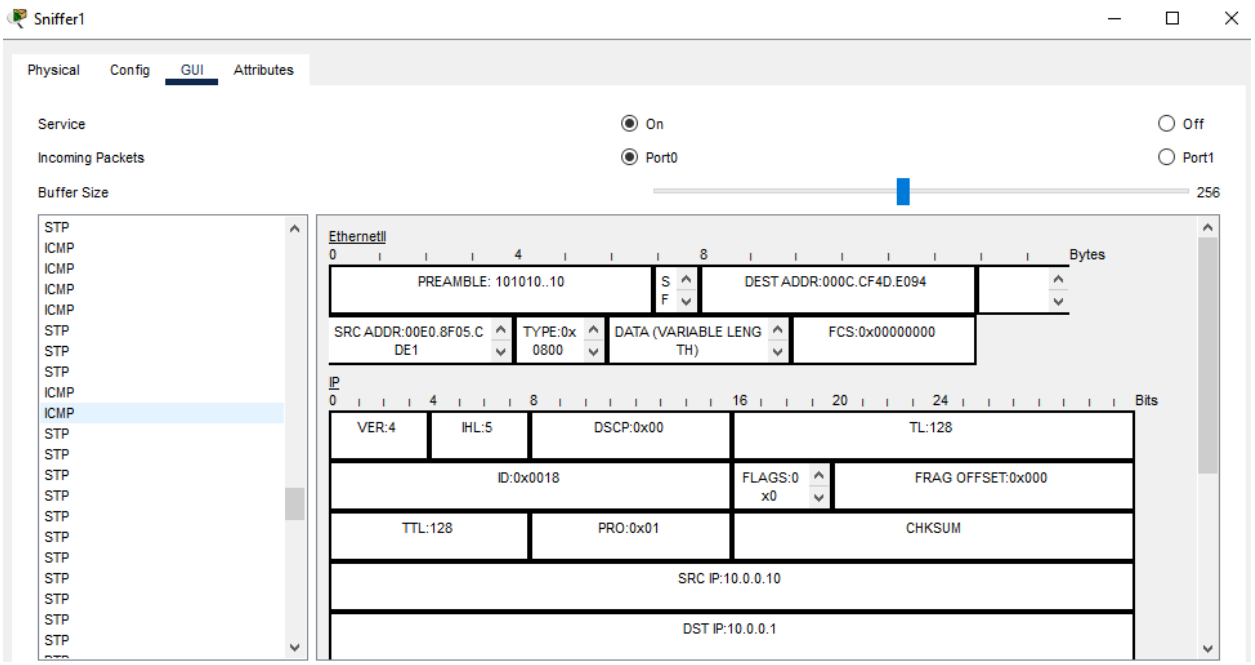
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time=7ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 1ms

C:\>
```

PC2

Physical Config Desktop Programming Attributes

Command Prompt

```
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: 3

AIM: Implement an **Inter-VLAN** Routing.

---

1. Introduction to Inter-VLAN

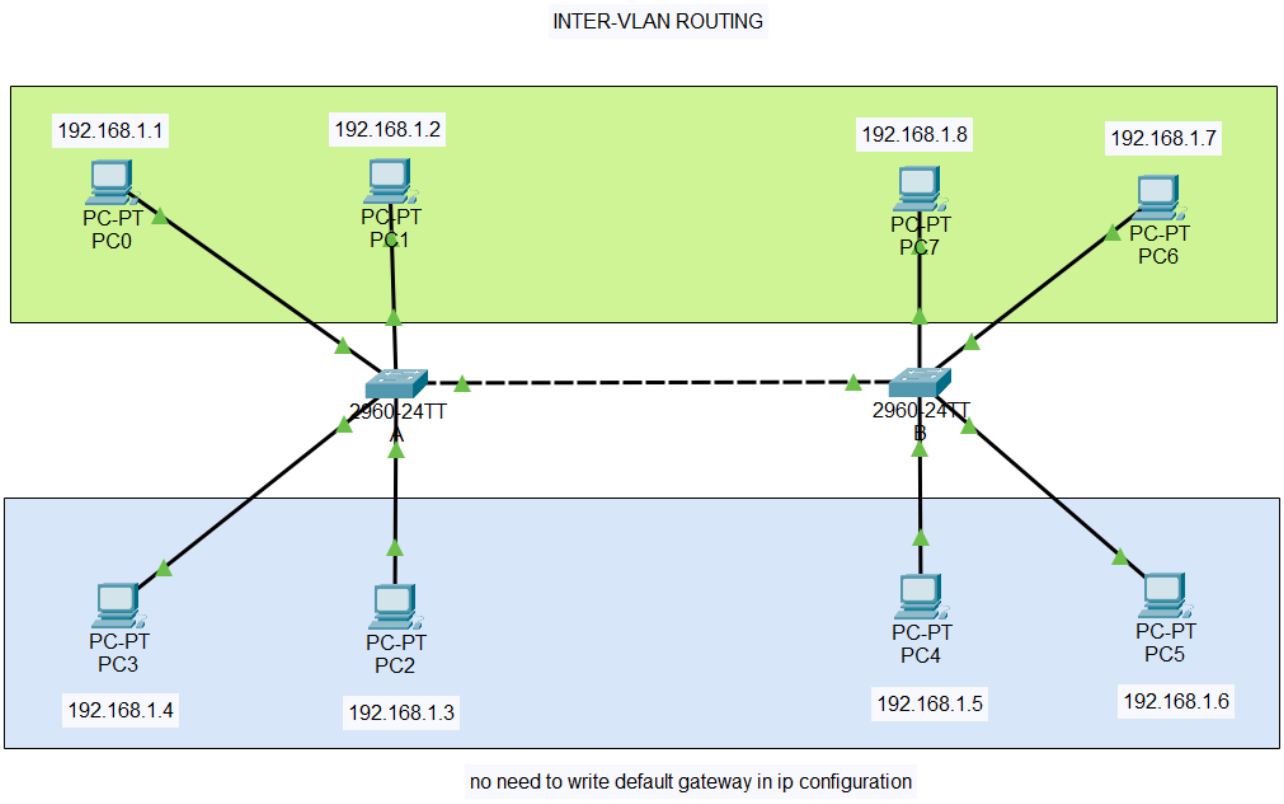
- Inter-VLAN routing is the process of allowing communication between different VLANs within a network.
- Since VLANs are separate broadcast domains, devices in different VLANs cannot communicate with each other without routing.
- Inter-VLAN routing provides a method to connect these VLANs using either a router or a Layer 3 switch.
- It is commonly used in enterprise networks to segment traffic for security and efficiency while still allowing controlled communication between VLANs.

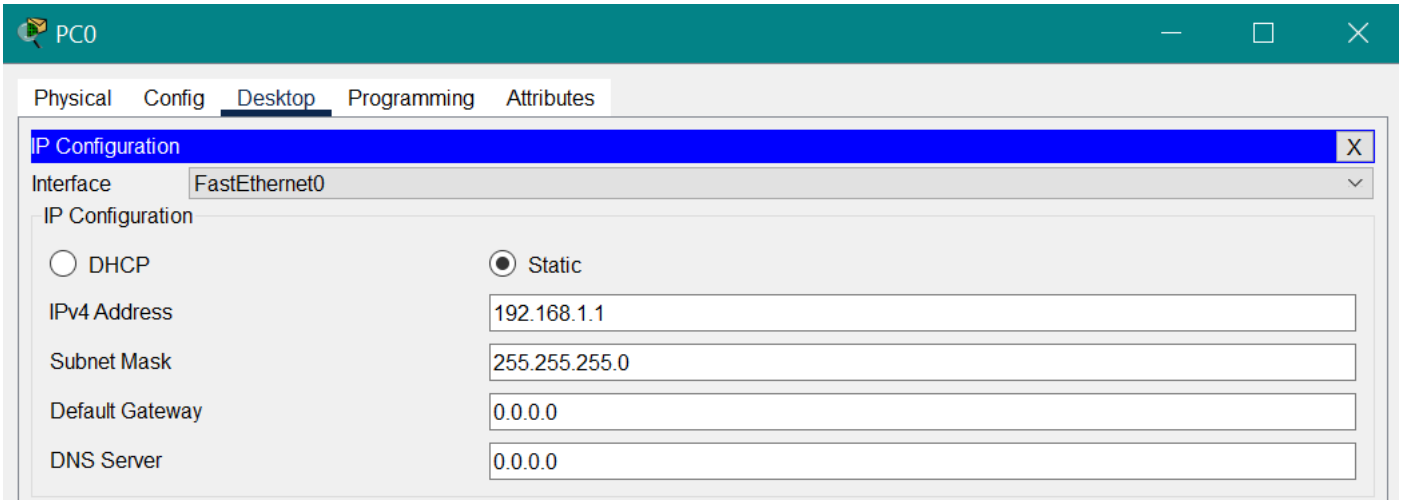
---

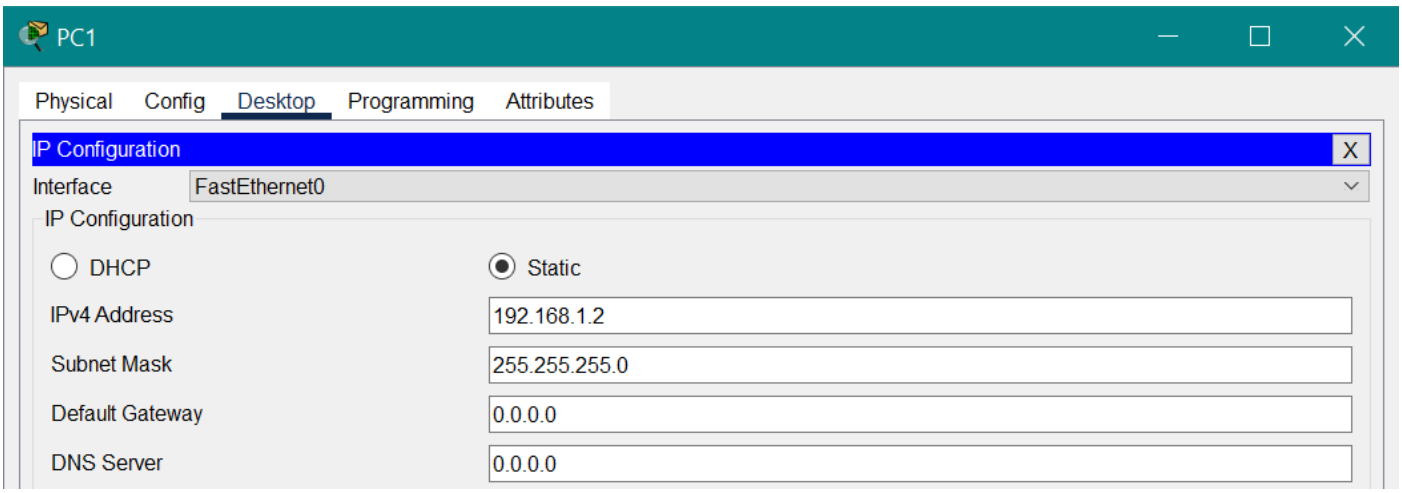
2. Why Inter-VLAN is Used

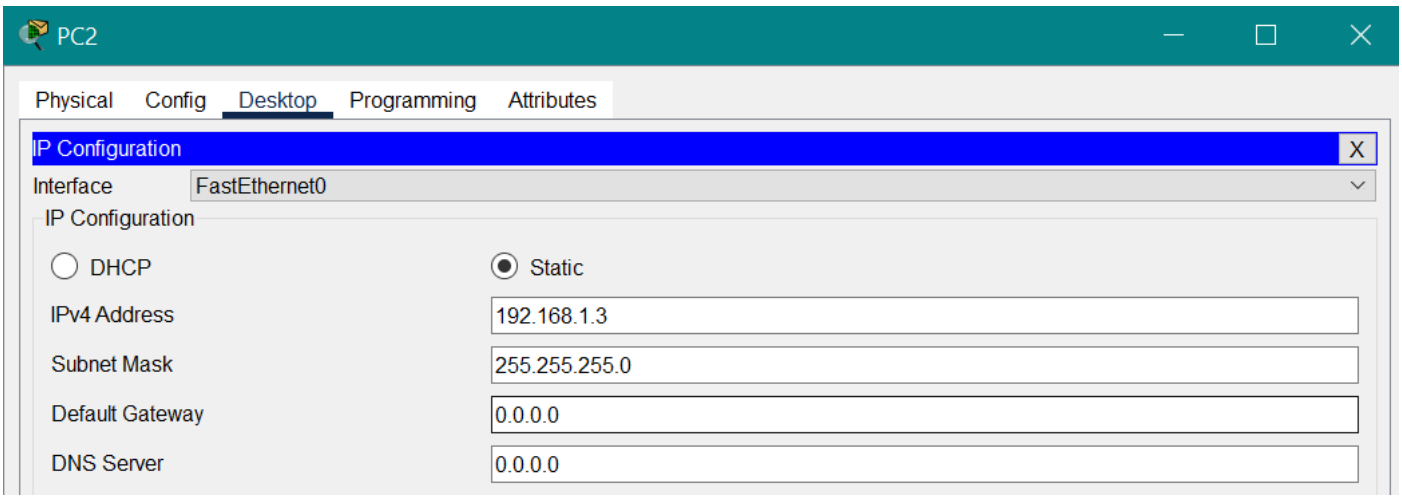
- Inter-VLAN routing is used to enable communication between devices located in different VLANs.
- Inter-VLAN routing is used to provide better security by separating broadcast domains while still allowing required data exchange.
- Inter-VLAN routing is used to optimize network performance by reducing unnecessary broadcast traffic.
- Inter-VLAN routing is used to provide centralized management of routing policies between VLANs.

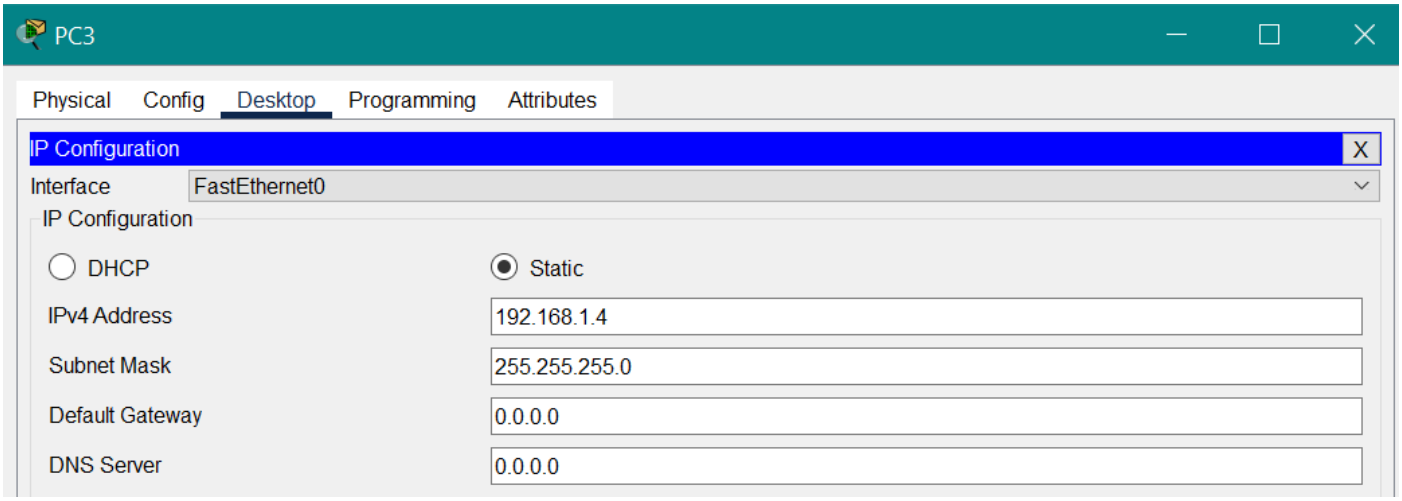
TOPOLOGY:

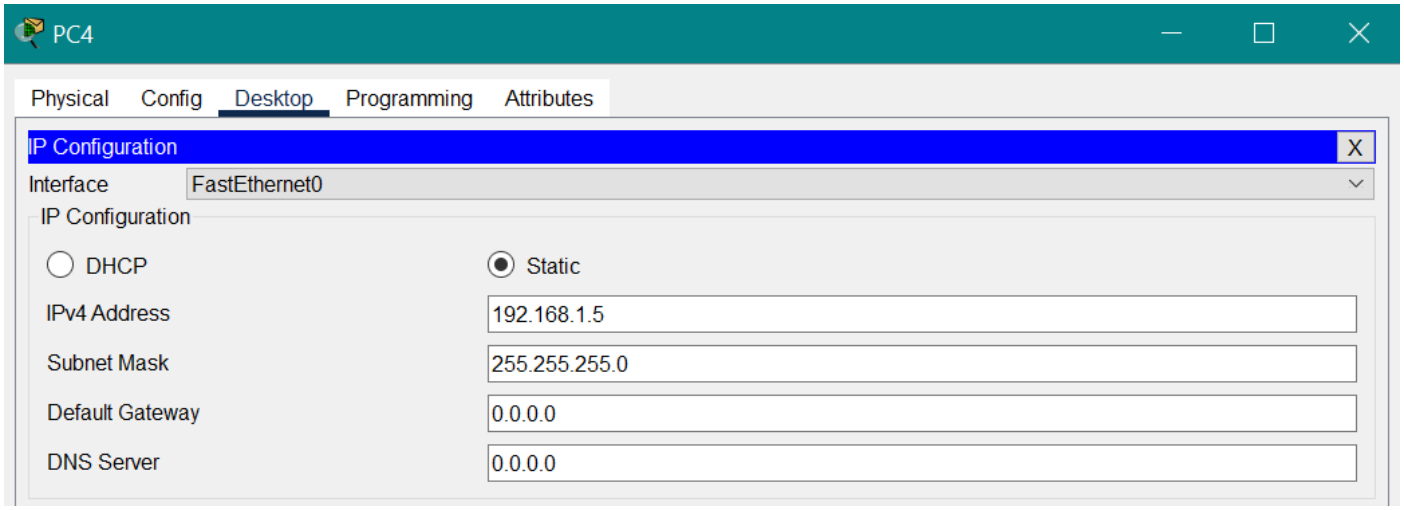


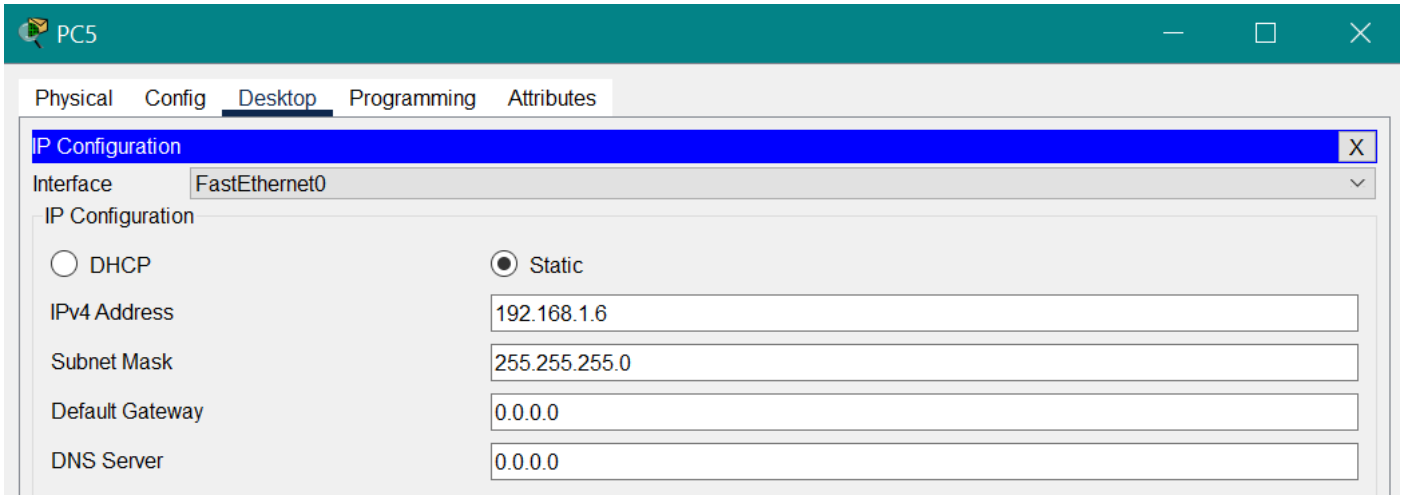

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0

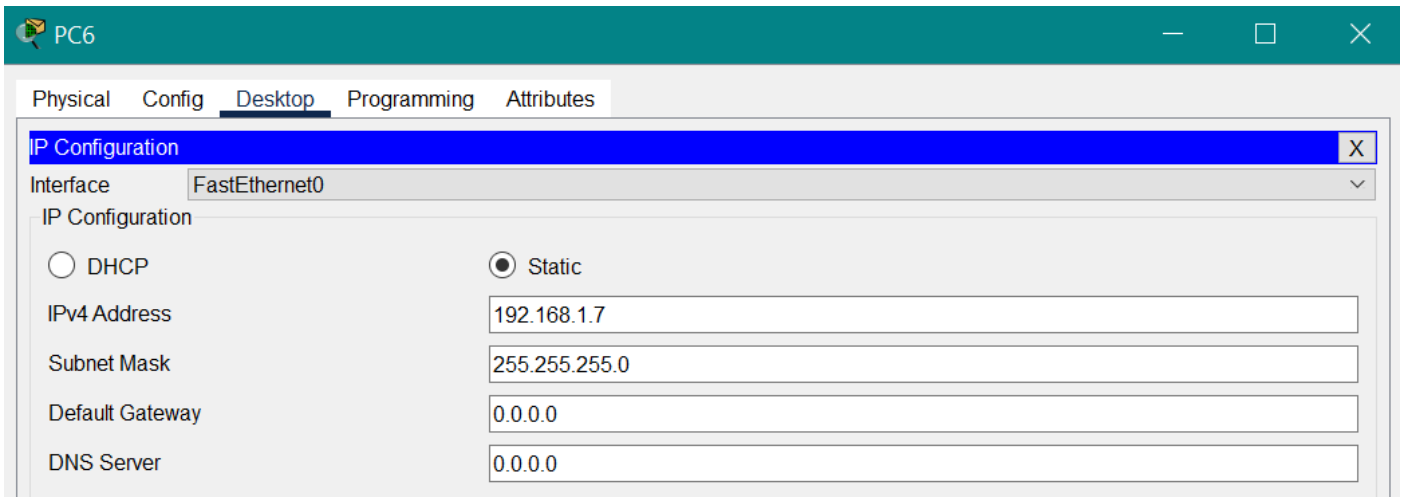

PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0

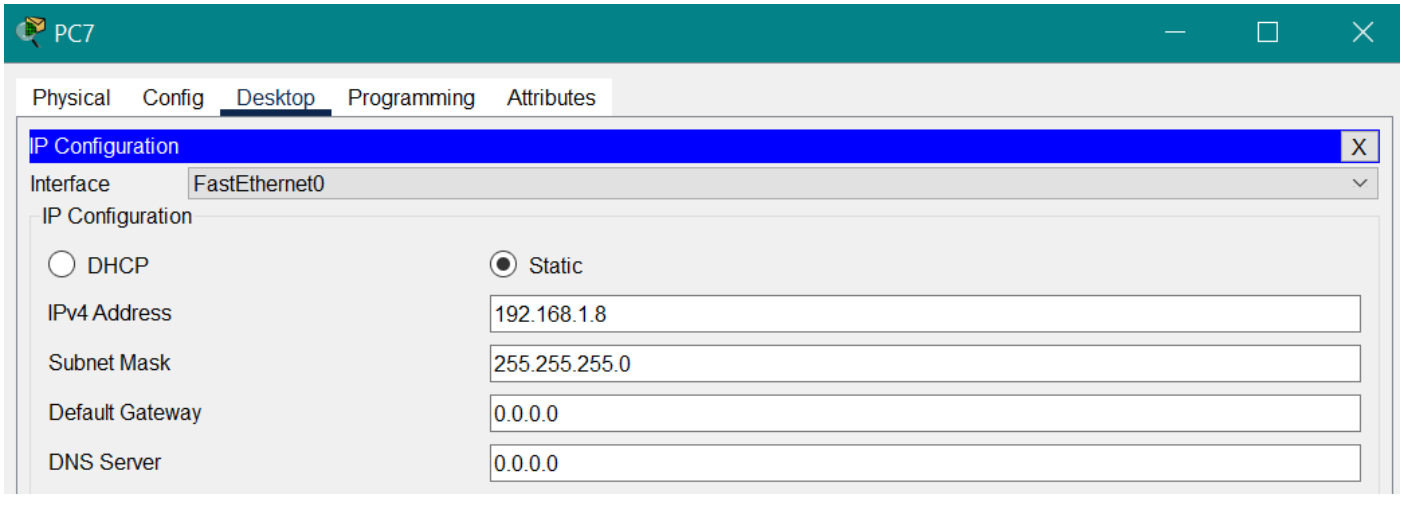

PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0


PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.4
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0


PC4
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.5
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0


PC5
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.6
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0


PC6
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.7
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0


PC7
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.8
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0

A

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)#ex
Switch(config)#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 fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
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 trunk
```

B

Physical Config CLI Attributes

IOS Command Line Interface

```
%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/5 on VLAN0001. Inconsistent port
type.


Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down

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

Switch(config-vlan)#name yellow
Switch(config-vlan)#ex
Switch(config)#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 20
Switch(config-if)#ex
Switch(config)#int fa0/2
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 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 10
Switch(config-if)#ex
Switch(config)#int fa0/5
Switch(config-if)#switchport mode trunk
Switch(config-if)#ex
Switch(config)#
```

OUTPUT:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	PC6	ICMP		0.000	N	0	(edit)
	Failed	PC7	PC2	ICMP		0.000	N	1	(edit)
	Successful	PC3	PC5	ICMP		0.000	N	2	(edit)
	Failed	PC1	PC4	ICMP		0.000	N	3	(edit)

PRACTICAL NO : 4

AIM : Create a Network and Implement a RIP Protocol.

1. Introduction to RIP (Routing Information Protocol)

The **Routing Information Protocol (RIP)** is one of the earliest and simplest **distance-vector routing protocols**, used in small and medium-sized networks to dynamically exchange routing information between routers. RIP uses **hop count** as the metric to determine the shortest path between networks.

---

2. Key Features of RIP

Here are some of the important characteristics that define RIP:

- **Distance Vector Protocol**: RIP uses hop count (number of routers) as its routing metric.
- **Maximum Hop Count: 15**: If a route requires more than 15 hops, it is considered unreachable.
- **Routing Updates Every 30 Seconds**: RIP routers broadcast their full routing table to neighbors every 30 seconds.
- **Uses UDP Port 520**: RIP relies on the User Datagram Protocol (UDP) for communication.
- **Supports RIPv1 and RIPv2**:
  - **RIPv1**: Classful routing, does not support subnet information.
  - **RIPv2**: Classless routing, supports VLSM and subnetting.
- **Simple Configuration**: Very easy to implement in small networks.
- **Slow Convergence**: Takes time to react to network topology changes compared to more modern protocols.
- **Loop Prevention Techniques**: Includes methods like **split horizon**, **route poisoning**, and **hold-down timers** to avoid routing loops.

---

3. Where is RIP Used ?

RIP is typically used in:

- **Small to medium-sized networks** where simplicity is more important than scalability.
- **Lab environments or educational purposes** for learning basic routing concepts.
- Scenarios where **manual route configuration** would be inefficient.

Due to limitations like slow convergence and hop count restrictions, RIP is generally **not recommended** for large or mission-critical networks.

---

4. How RIP Works in a Network Topology

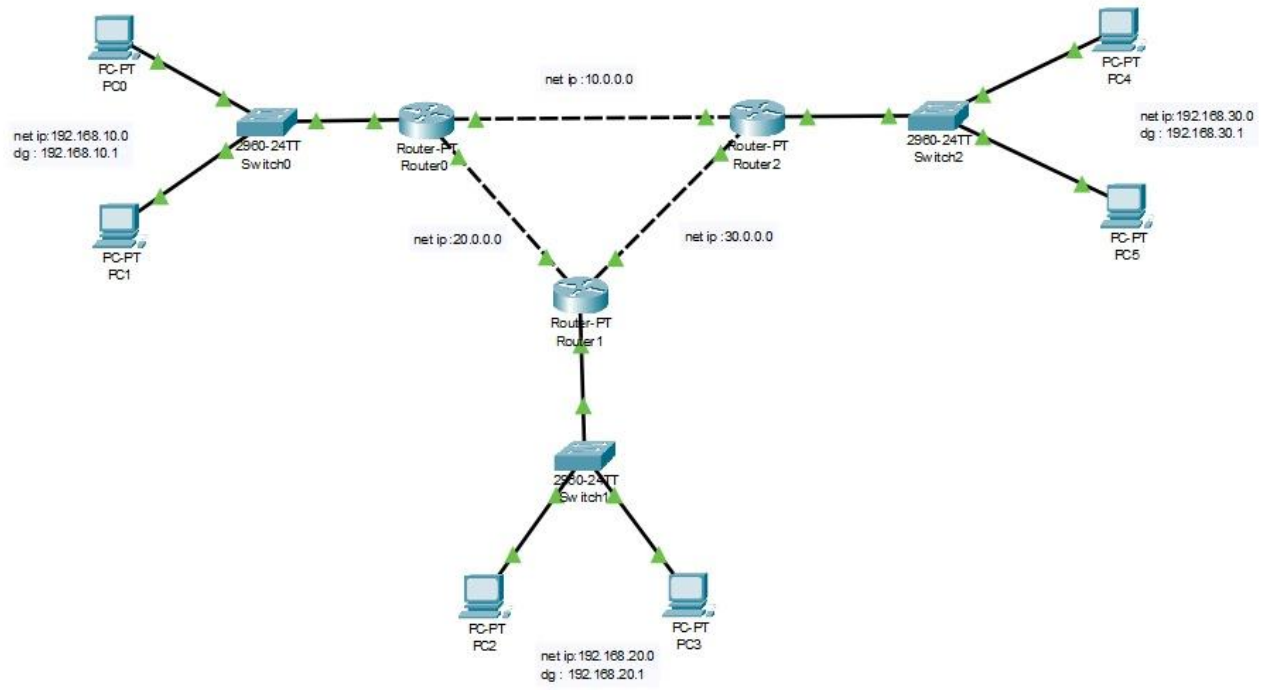
- **Each router** is connected to one or more networks and assigned IP addresses.
- RIP is **enabled on all routers** in the network.
- Routers **advertise their directly connected networks** to neighboring routers using RIP.
- **Routing updates** are automatically sent every **30 seconds** to nearby routers.
- Routers **receive updates**, add new routes to their **routing tables**, and increase the hop count by 1 for each route.
- The process continues until **all routers learn about all networks** in the topology.
- **Data packets** are then forwarded through the shortest path (based on hop count).
- This allows **end devices (PCs)** on different routers to communicate efficiently.

5. Network Design

The network typically includes:

- **Multiple routers** interconnected in a basic topology such as linear, star, or triangular.
- **Switches** connected to router interfaces, serving as access points for end devices.
- **PCs or other end devices** connected to the switches, each assigned an IP address in the same subnet as the router interface.

This setup demonstrates how RIP enables communication between devices across different networks without requiring static route configuration.



6. Used Cable Types For This Network Connection

1. Straight-Through Cable

- **Used for:** Connecting **different types of devices**
- **Examples:**
  - PC ↔ Switch
  - Router ↔ Switch
- **Why:** Maintains the standard pin configuration; suitable for end devices to networking devices.

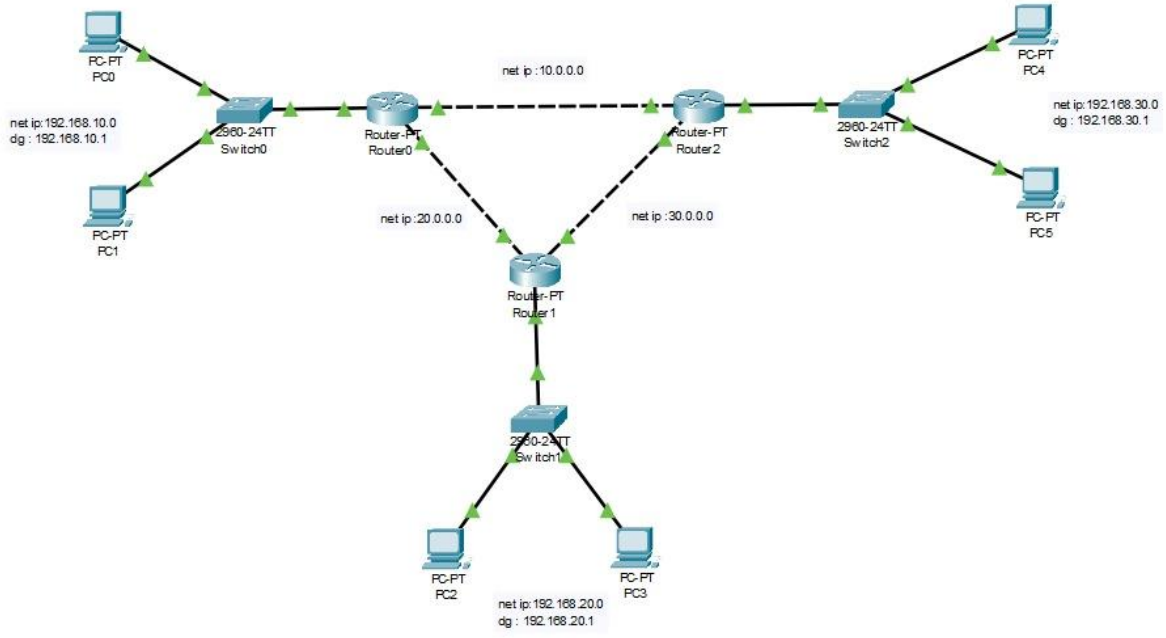
2. Copper Crossover Cable

- **Used for:** Connecting **similar types of devices**
- **Examples:**
  - PC ↔ PC
  - Switch ↔ Switch
  - Router ↔ Router (in older or simulated networks)
- **Why:** Transmit and receive pins are crossed to allow direct communication between similar devices.

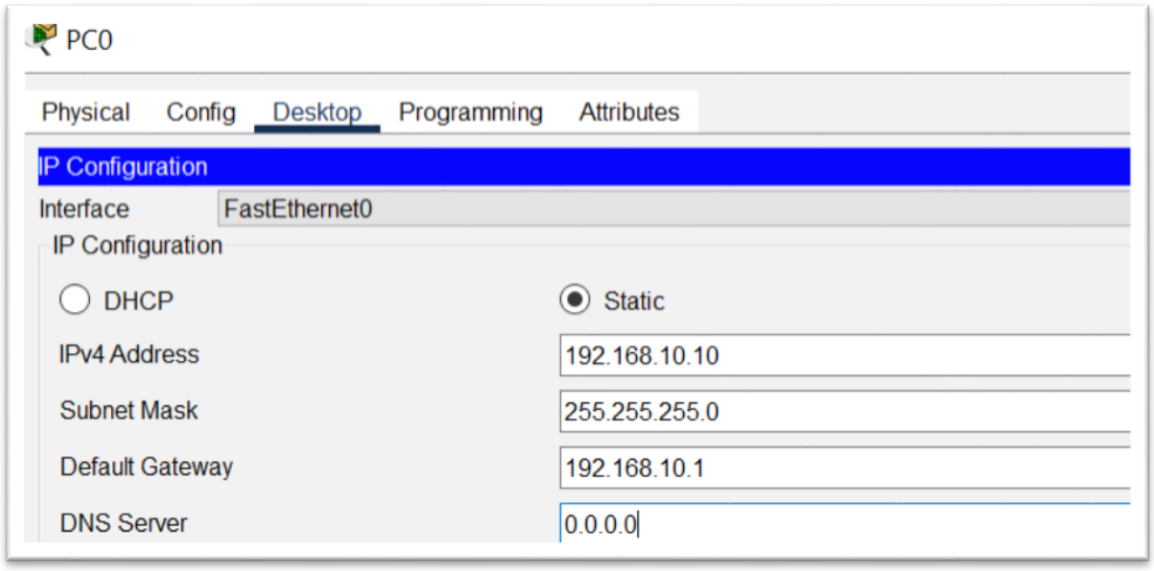
Feature	Straight-Through Cable	Copper Crossover Cable
Purpose	Connects different types of devices	Connects similar types of devices
Typical Use Cases	PC ↔ Switch, Router ↔ Switch	PC ↔ PC, Switch ↔ Switch, Router ↔ Router
Wiring Pattern	Same pin order on both ends	Transmit and receive pairs are crossed
Signal Flow	Transmit pins connect to receive pins	Transmit pins connect to transmit pins
Devices Connected	End devices to networking devices	Networking device to networking device
Modern Device Support	May or may not require auto-MDI/MDIX	Needed if auto-MDI/MDIX not supported
Simulator Use	Used for connecting different devices	Used for connecting similar devices

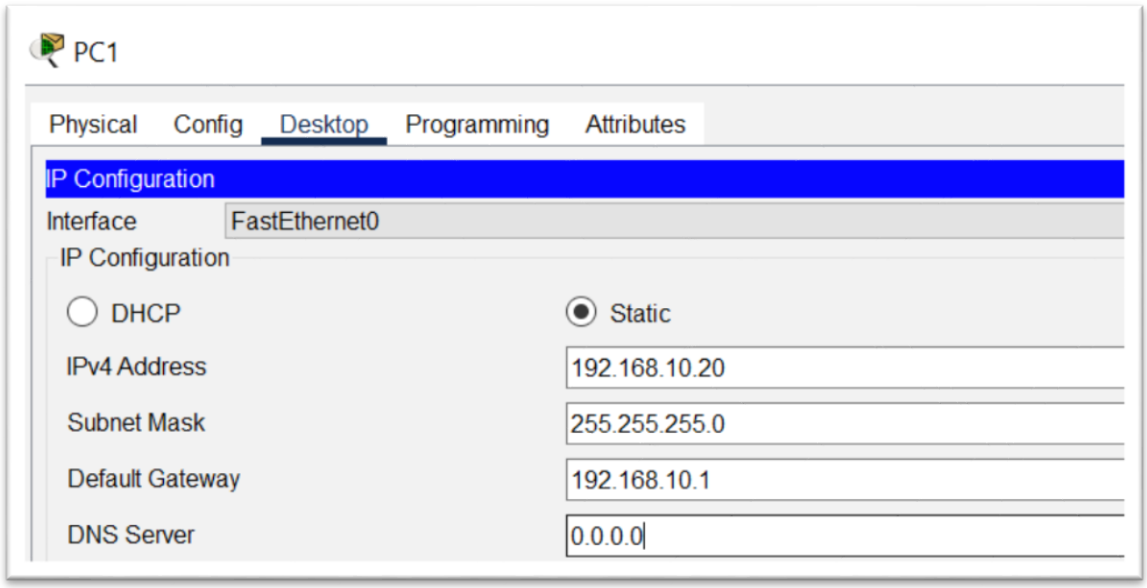
DEVICE	NET-IP	IP ADDRESS	DEFAULT GATEWAY
ROUTER 0	192.168.10.0	192.168.10.1	----
ROUTER 0	10.0.0.0	10.0.0.1	----
ROUTER 0	20.0.0.0	20.0.0.1	----
ROUTER 1	192.168.20.0	192.168.20.1	----
ROUTER 1	20.0.0.0	20.0.0.2	----
ROUTER 1	30.0.0.0	30.0.0.1	----
ROUTER 2	192.168.30.0	192.168.30.1	----
ROUTER 2	10.0.0.0	10.0.0.2	----
ROUTER 2	30.0.0.0	30.0.0.2	----
PC 0	192.168.10.0	192.168.10.10	192.168.10.1
PC1	192.168.10.10	192.168.10.20	192.168.10.1
PC2	192.168.20.0	192.168.20.10	192.168.20.1
PC3	192.168.20.0	192.168.20.20	192.168.20.1
PC4	192.168.30.0	192.168.30.10	192.168.30.1
PC5	192.168.30.0	192.168.30.20	192.168.30.1

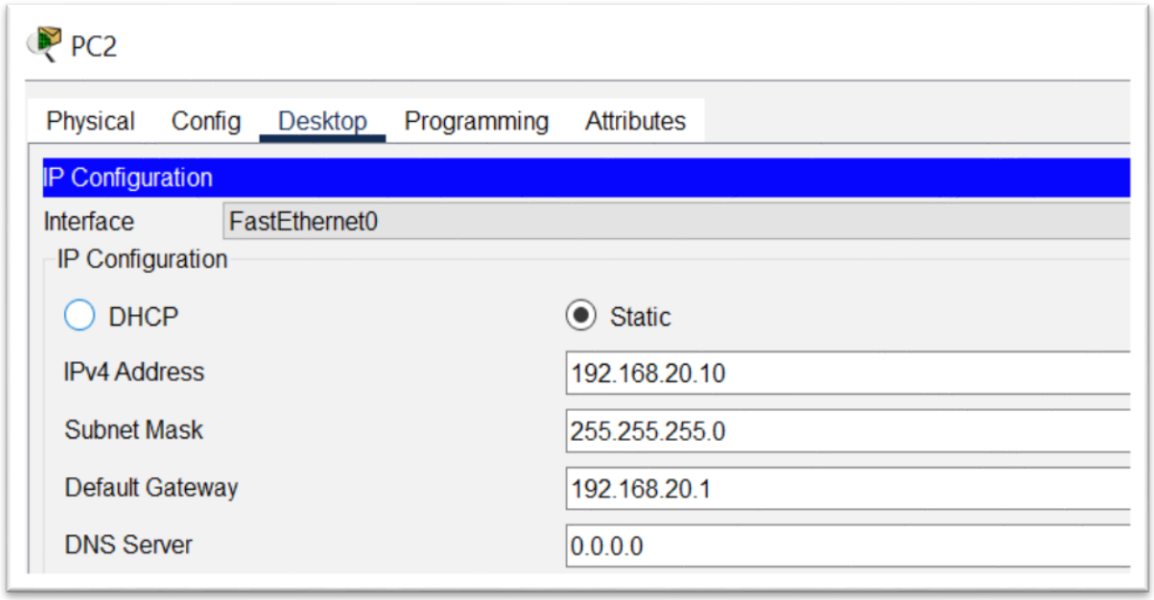
This how the topology look.

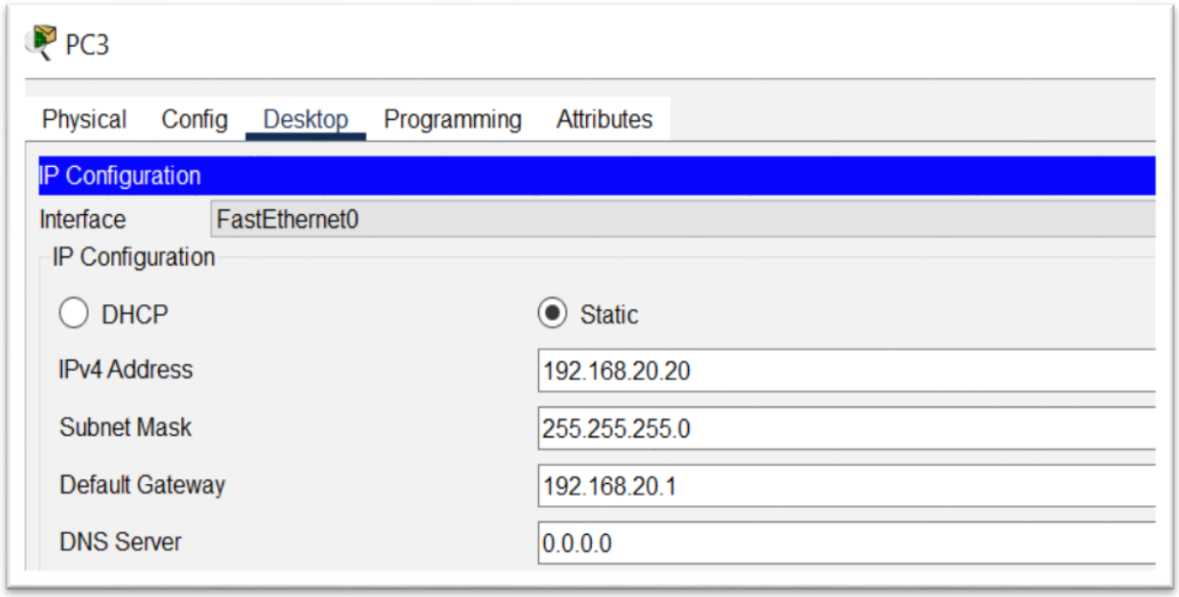


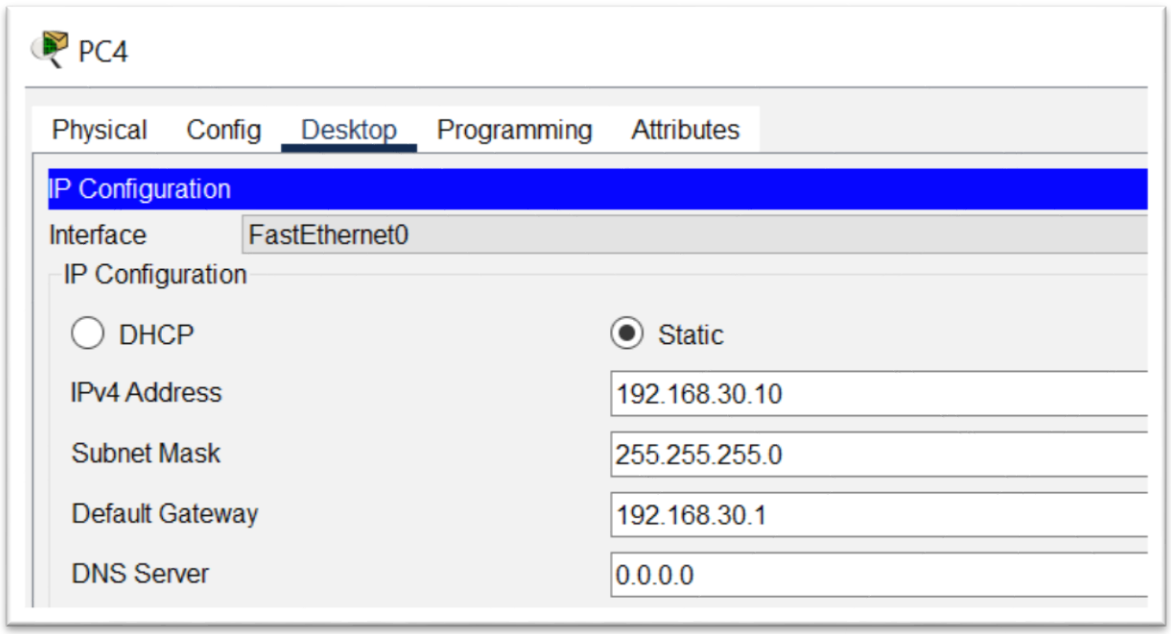
Assigning ip addresses to pc's & routers.

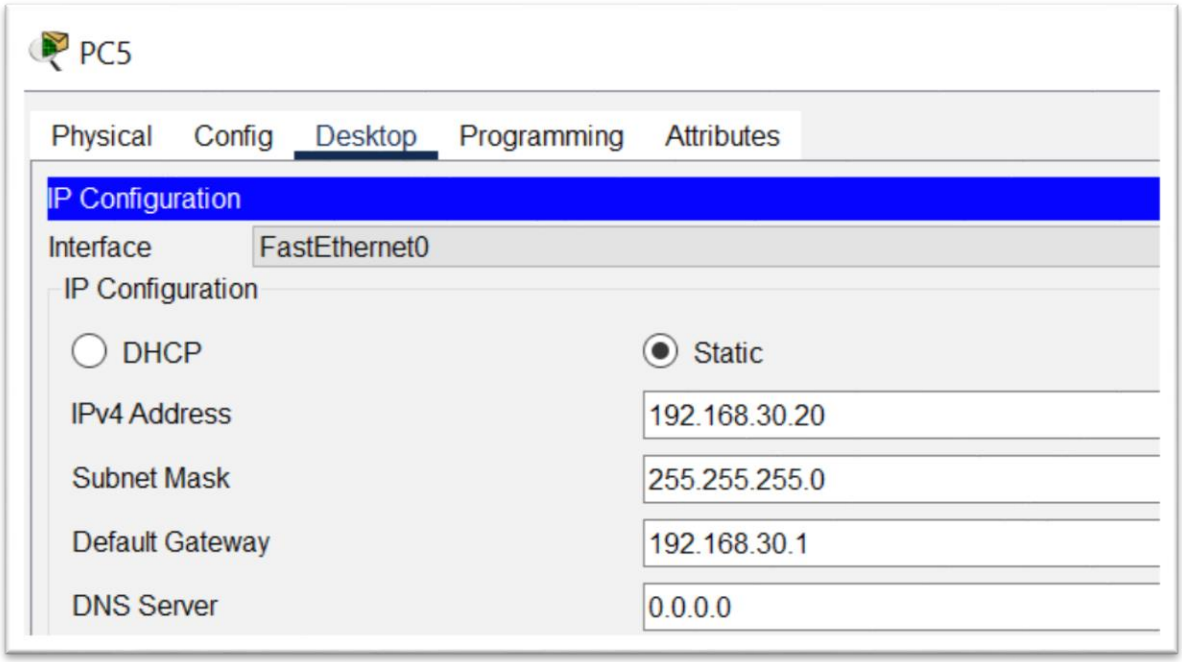




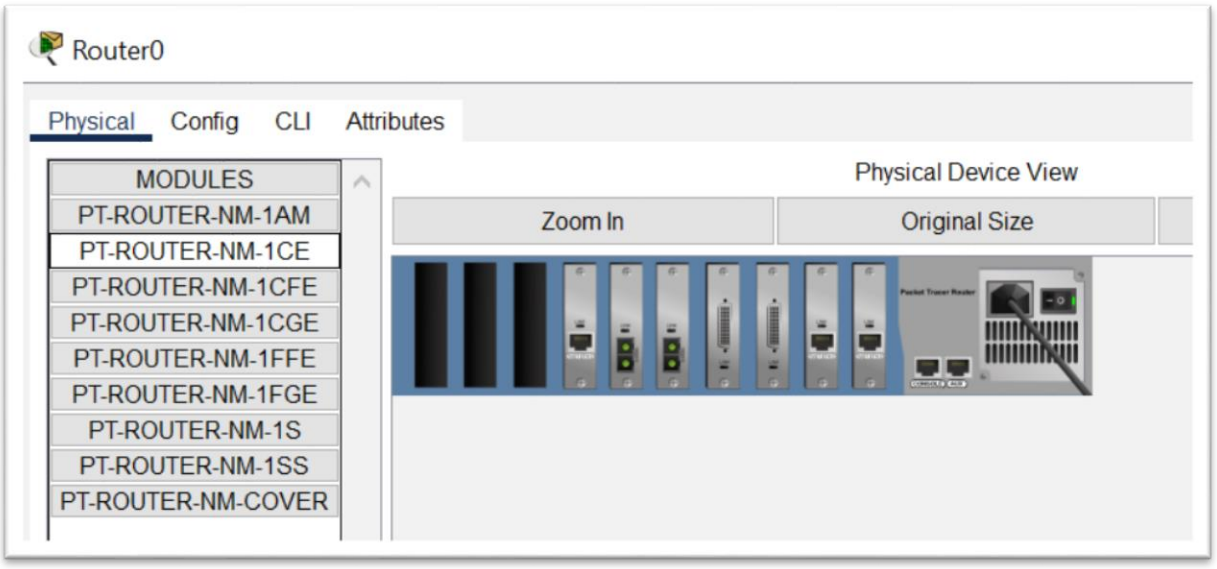


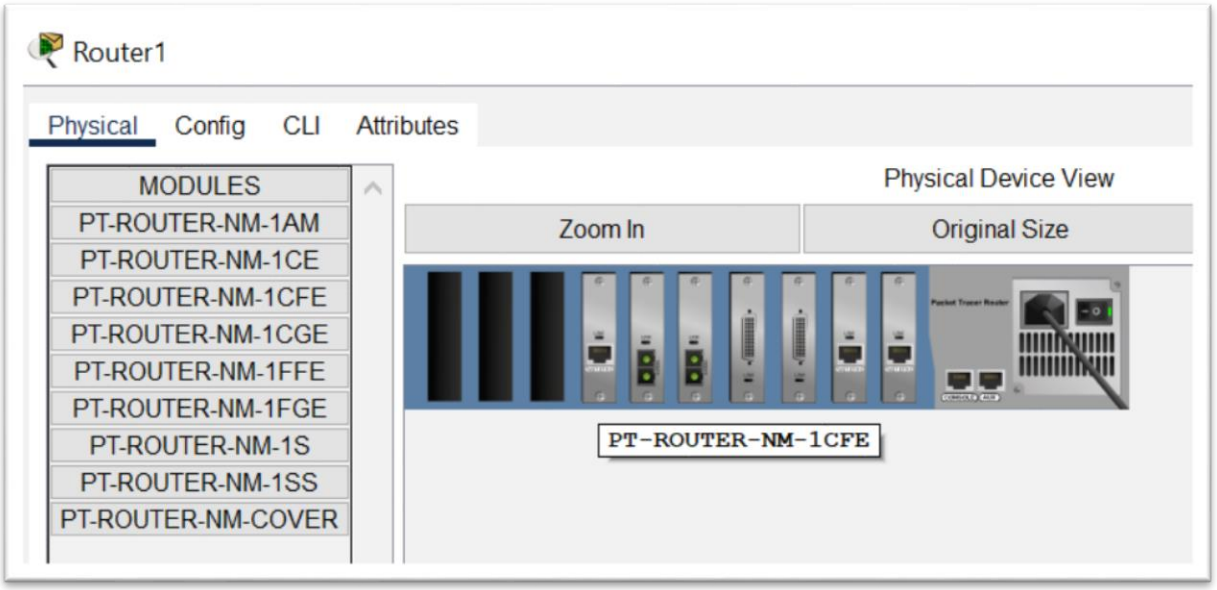

PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.20.20
Subnet Mask
255.255.255.0
Default Gateway
192.168.20.1
DNS Server
0.0.0.0

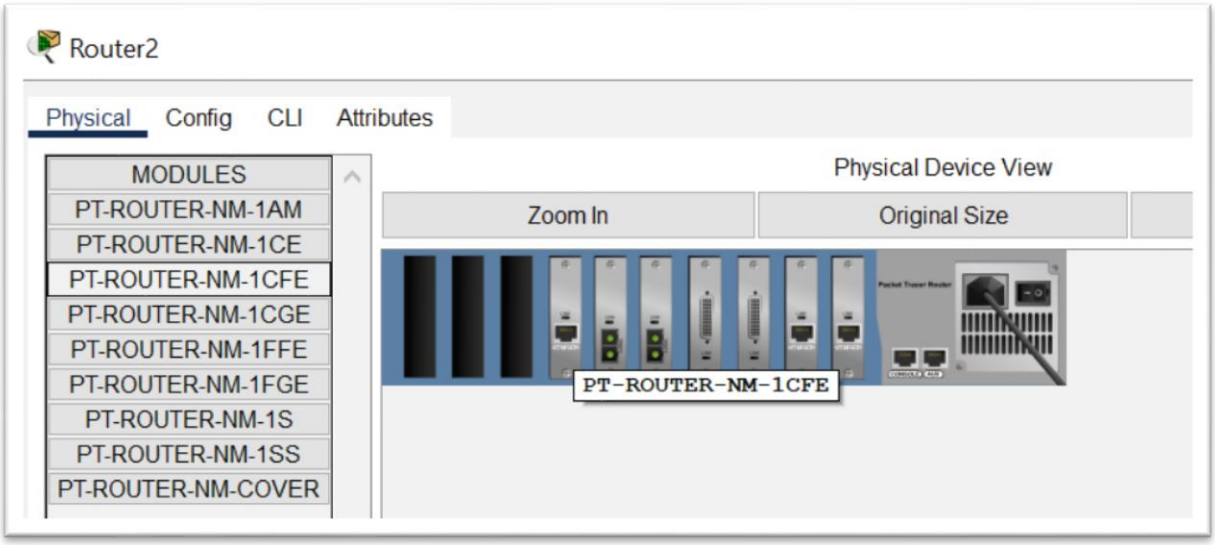

PC4
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.30.10
Subnet Mask
255.255.255.0
Default Gateway
192.168.30.1
DNS Server
0.0.0.0


PC5
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.30.20
Subnet Mask
255.255.255.0
Default Gateway
192.168.30.1
DNS Server
0.0.0.0

For Router connection via Copper Cross-over, Add 1 port Of PT-ROUTER-NM-1CFE to each router.

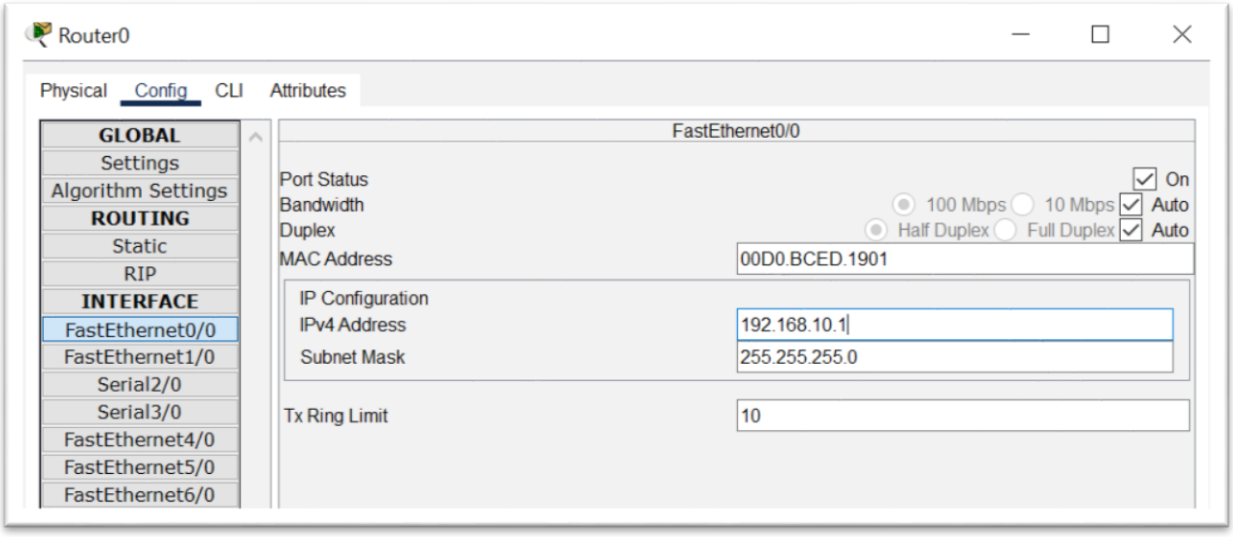




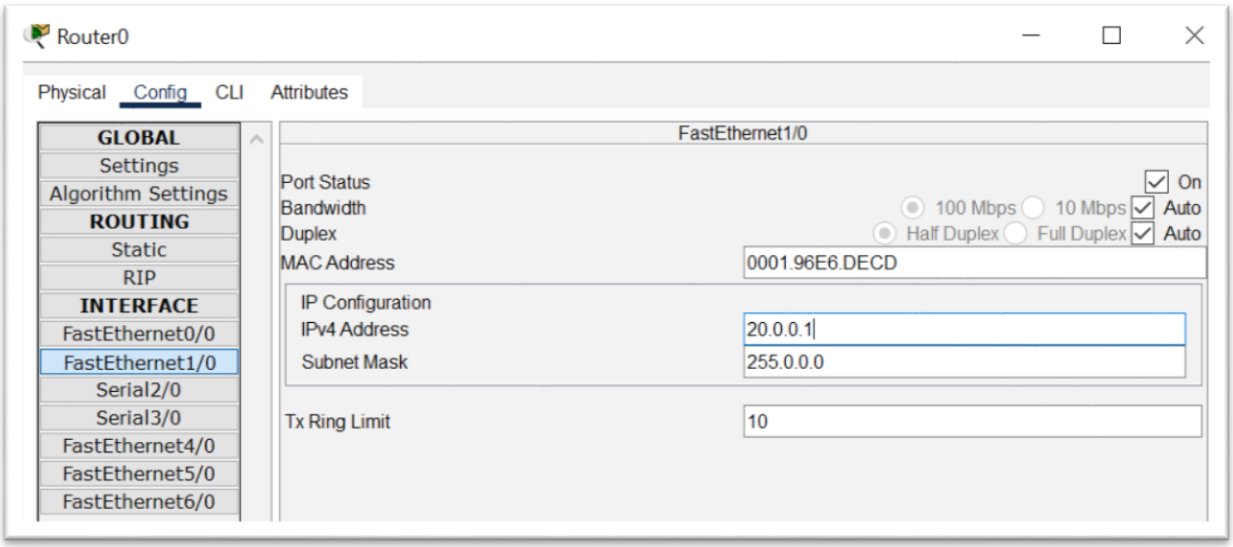


Router 0:

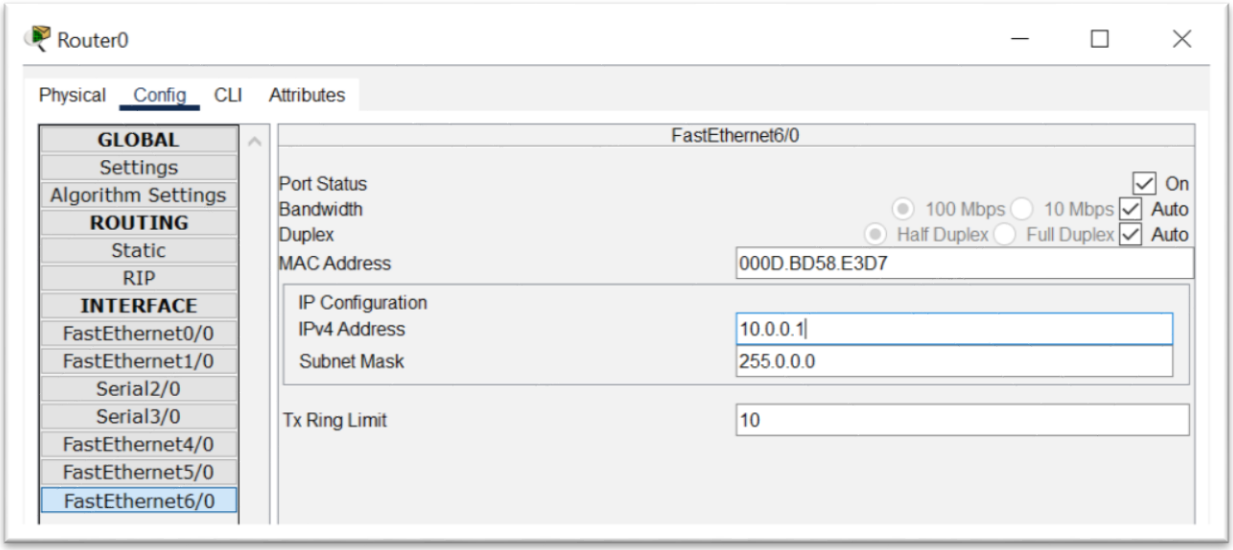
- Fa 0/0



- Fa 1/0

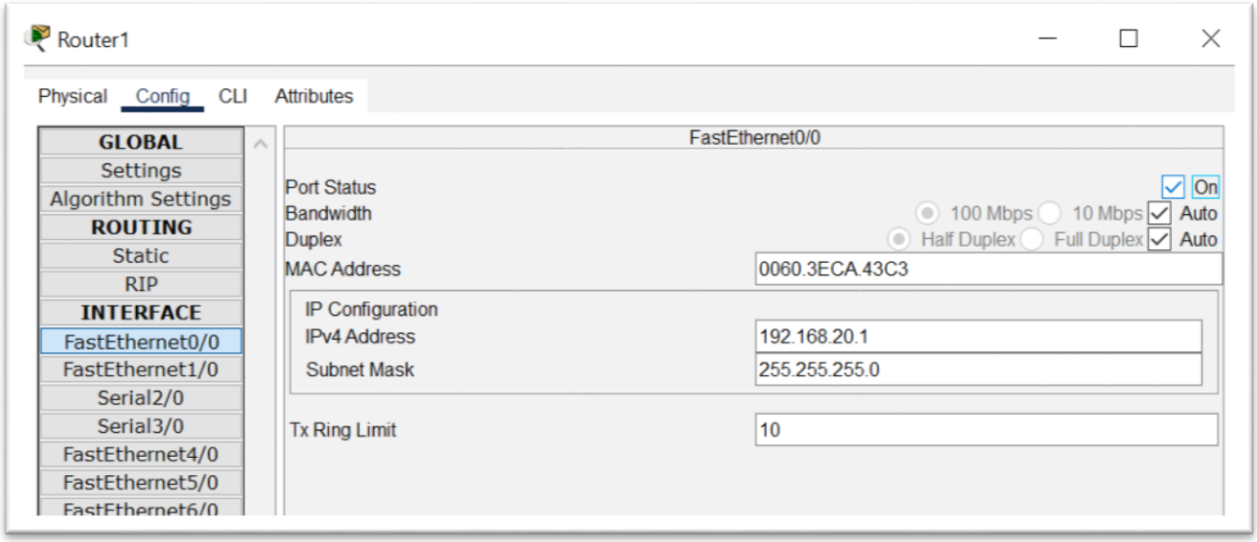


- Fa 6/0

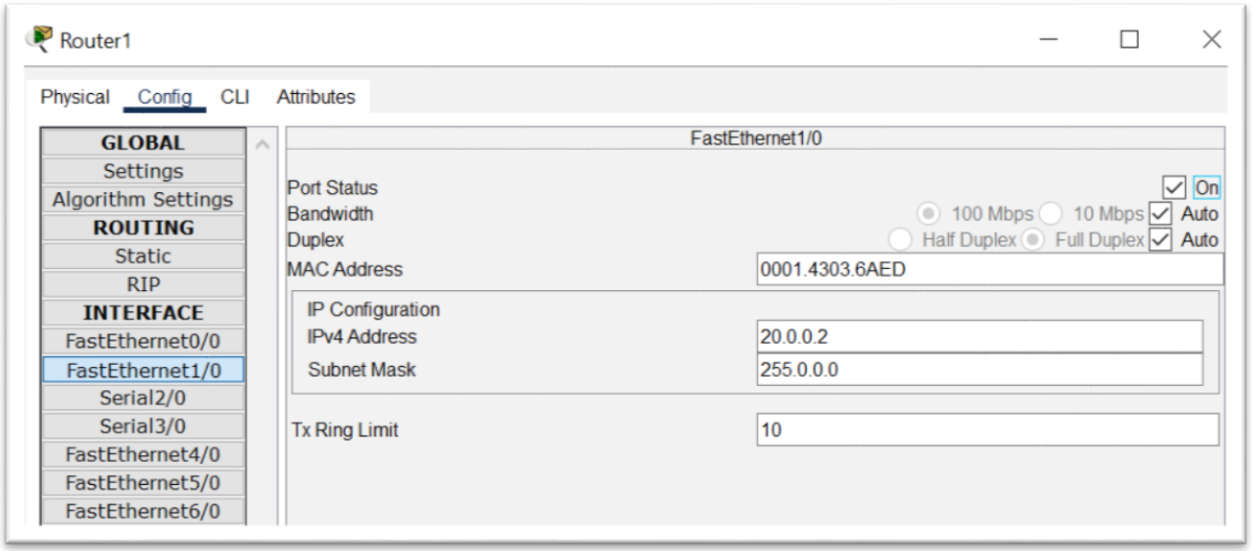


Router 1:

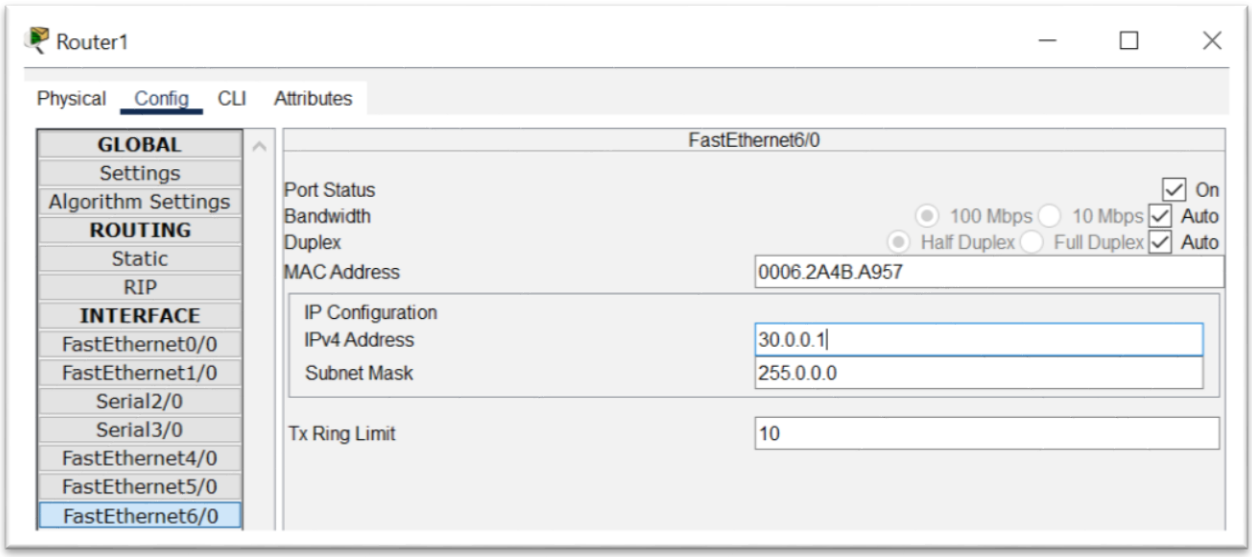
- Fa 0/0



- Fa 1/0

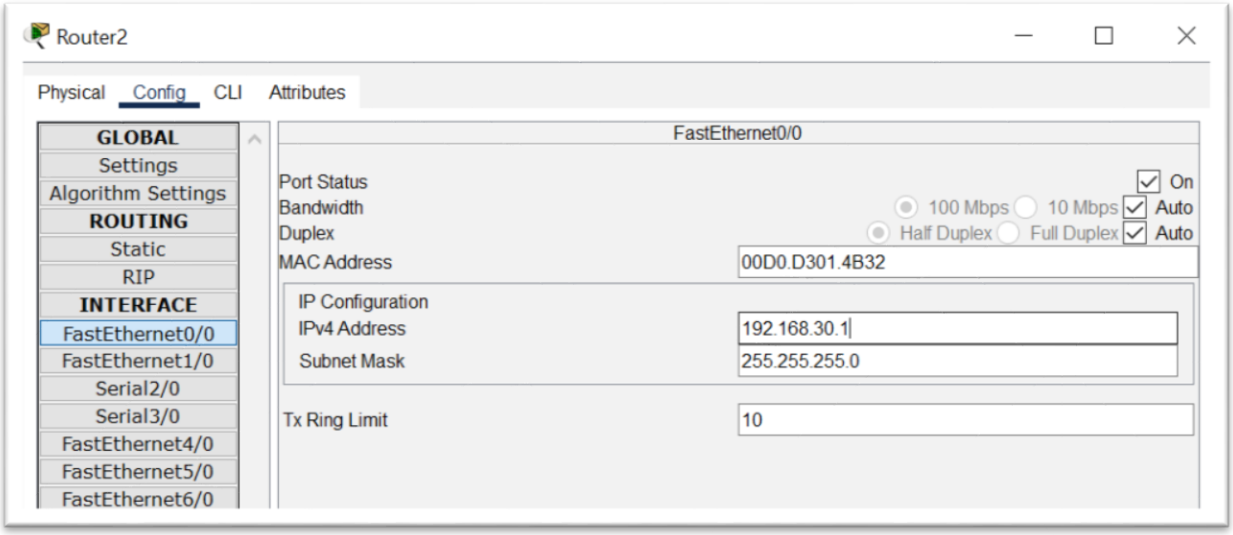


- Fa 6/0

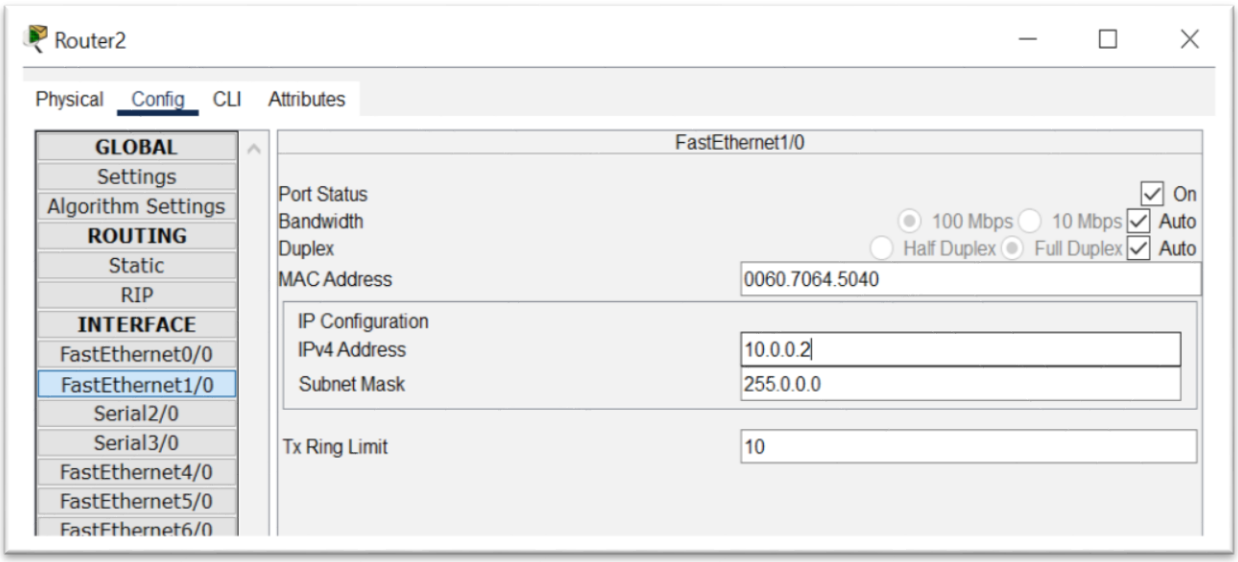


Router 2:

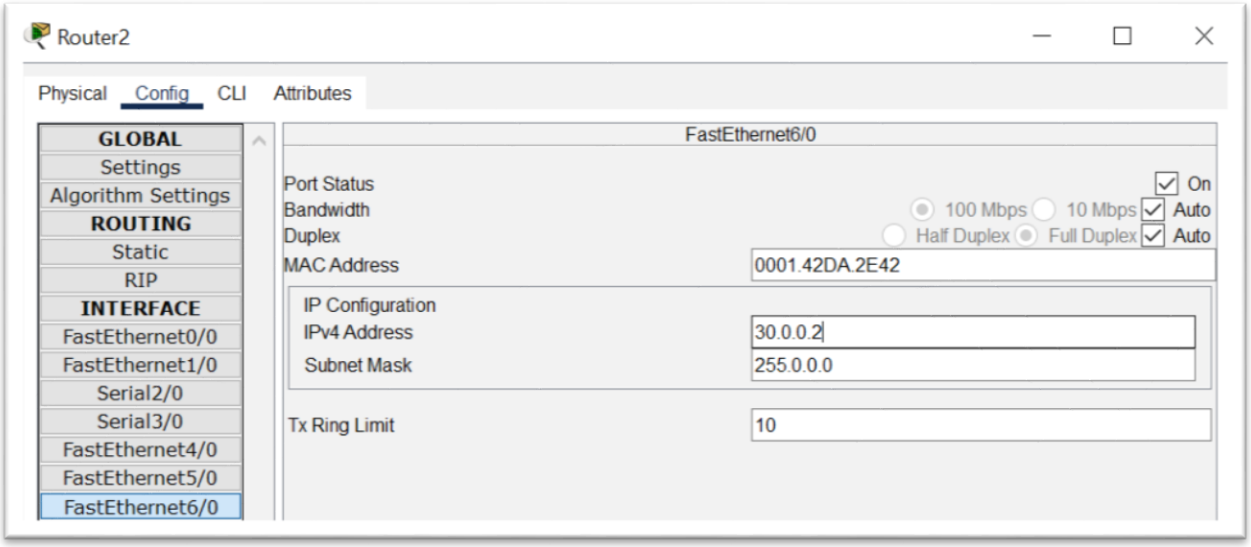
- Fa 0/0



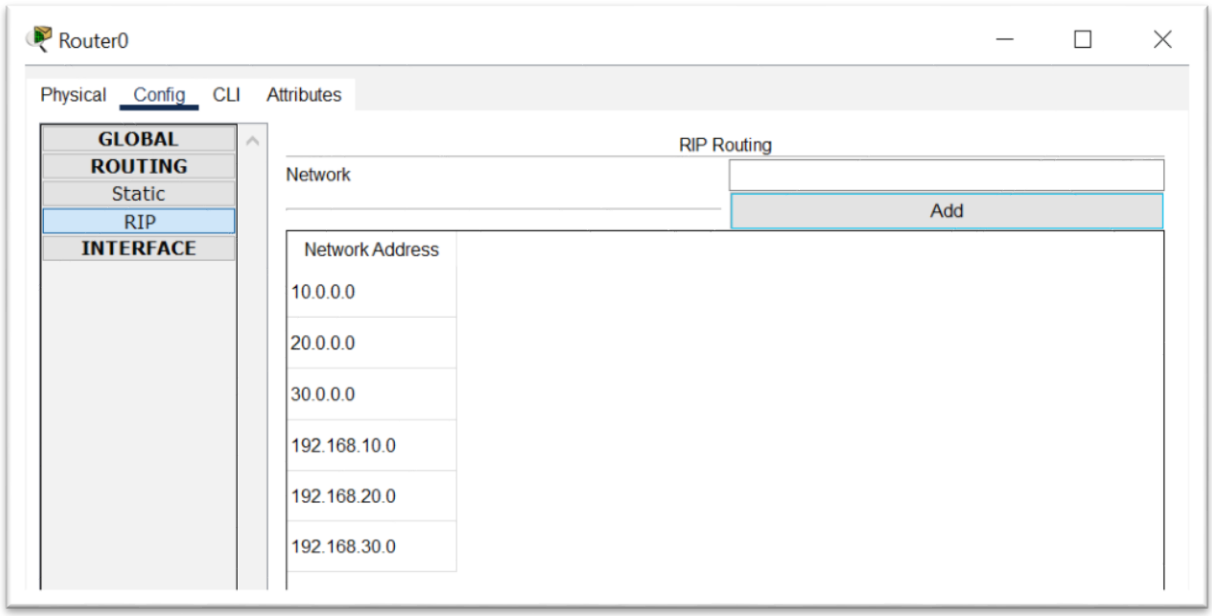
- Fa 1/0

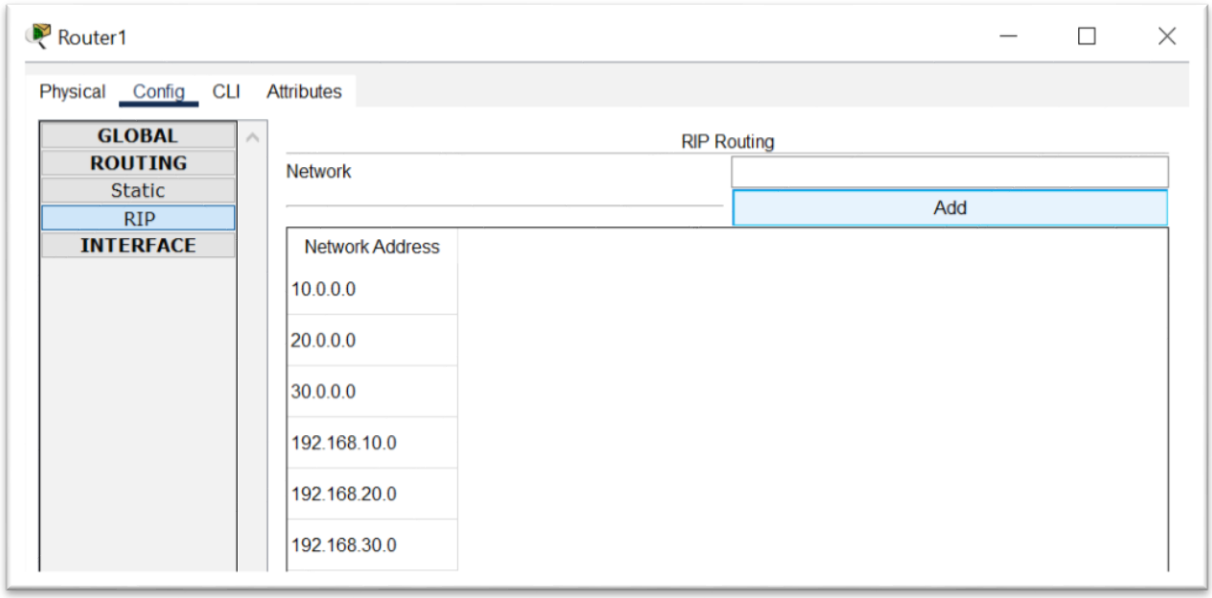


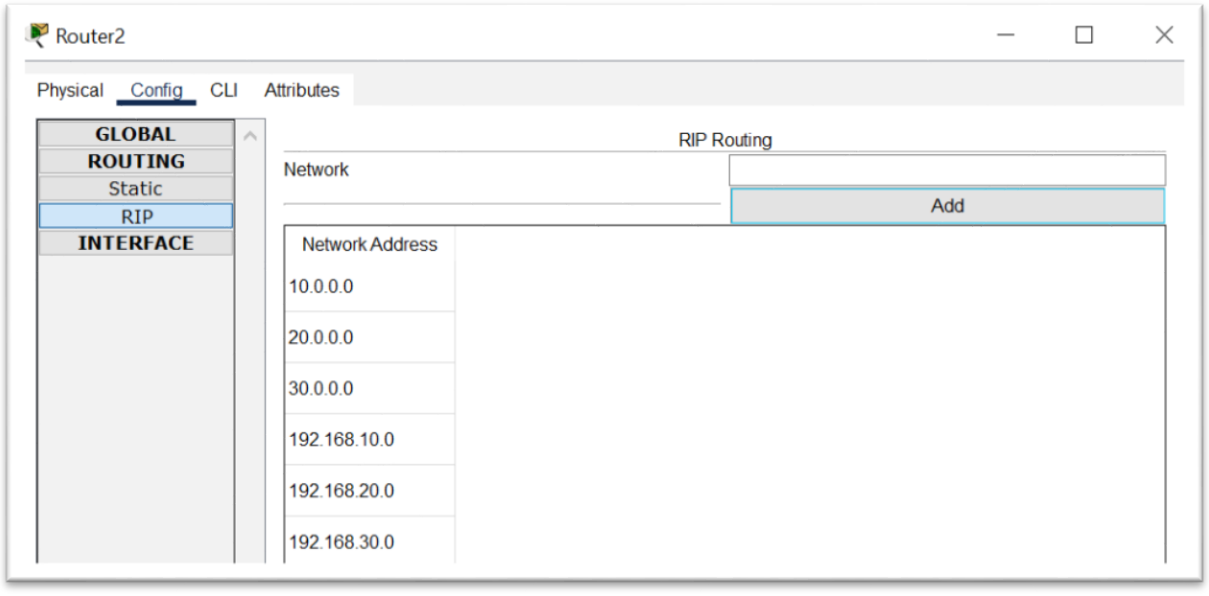
- Fa 6/0



Now Add All 6 Net IP's In Rip Routing .







OUTPUT:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC2	PC4	ICMP		0.000	N	2	(edit)
	Successful	PC3	PC1	ICMP		0.000	N	3	(edit)
	Successful	PC1	PC2	ICMP		2.219	N	4	(edit)
	Successful	PC3	PC5	ICMP		4.218	N	5	(edit)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	PC5	ICMP		0.000	N	0	(edit)
	Successful	PC1	PC4	ICMP		0.000	N	1	(edit)
	Successful	PC2	PC4	ICMP		0.000	N	2	(edit)
	Successful	PC3	PC1	ICMP		0.000	N	3	(edit)

PRACTICAL NO : 5

AIM: OSPF Implementation

- Create a Network to Implement Single-Area & Multi-Area OSPF.

---

1. Introduction to OSPF

- OSPF (Open Shortest Path First) is a dynamic routing protocol used within large and complex IP networks. It allows routers to automatically discover the best path for sending data by building a complete map of the network and selecting the shortest path based on cost (which is calculated using bandwidth).
- OSPF is a link-state routing protocol and is classified as an Interior Gateway Protocol (IGP), meaning it operates within a single autonomous system (AS). It uses Dijkstra's Shortest Path First (SPF) algorithm to compute the most efficient routes.
- Unlike protocols like RIP, which use hop count, OSPF considers link speed, making it more efficient and scalable. It is also an open standard, which means it is supported by many different network device vendors (e.g., Cisco, Juniper).

2. Uses of OSPF

- The idea behind the implementation of OSPF is to decrease or lower the amount of routing traffic and lower the tasks of core routers.
- OSPF supports both IPv4 and IPv6 and supports the classless CIDR addressing system, and is widely used in large enterprise networks.
- OSPF protocol has unlimited hop counts, unlike RIP protocol which has only 15 hops.

3. Basic Operation of OSPF

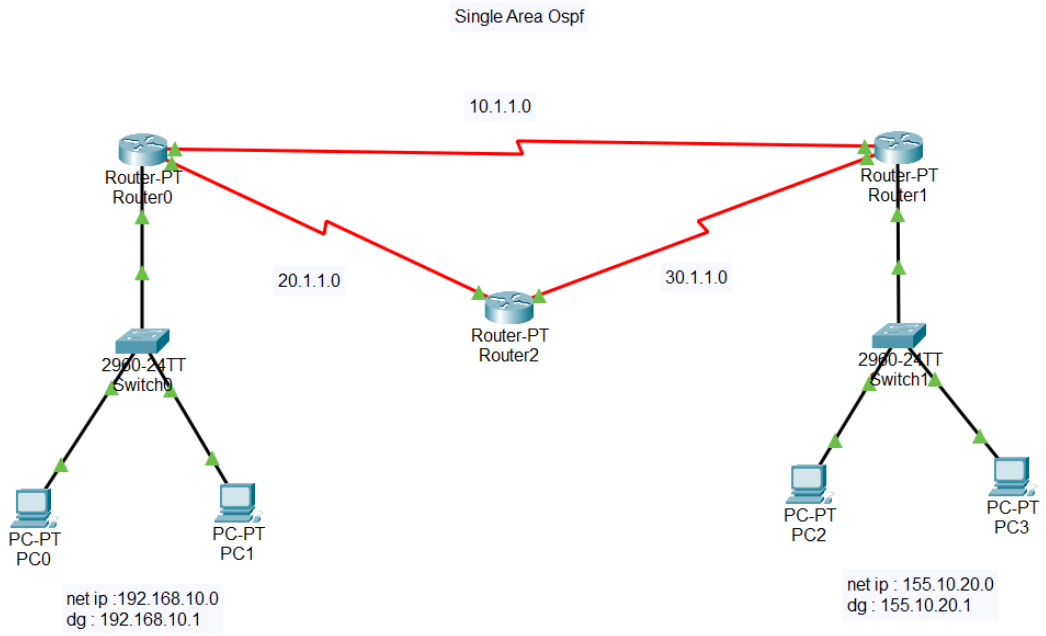
OSPF (Open Shortest Path First) is a link-state routing protocol that dynamically finds the best path for data in an IP network. Here's how it works:

- Neighbor Discovery: OSPF routers send Hello packets to find and establish communication with directly connected routers.
- Adjacency Formation: After verifying compatibility, routers form adjacencies and exchange routing information.
- LSA Exchange: Routers share Link-State Advertisements (LSAs) containing information about their interfaces and neighbors.
- Link-State Database (LSDB): Each router builds a link-state database, which is identical across all routers in the same area.
- SPF Algorithm (Dijkstra's): Routers run the Shortest Path First algorithm to calculate the best paths to all destinations.
- Routing Table Update: The best routes are installed in the routing table, labelled with an "O" for OSPF.

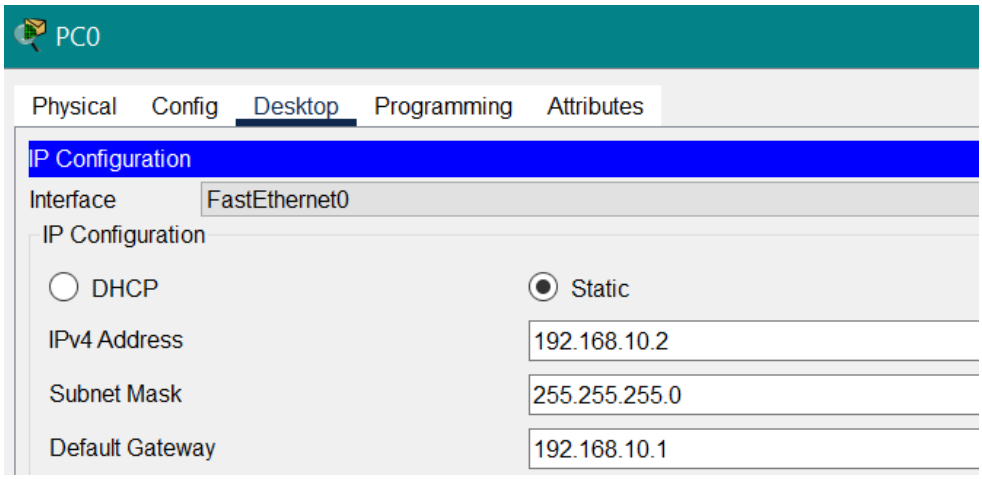
(A) : Create a Network to Implement Single-Area OSPF.

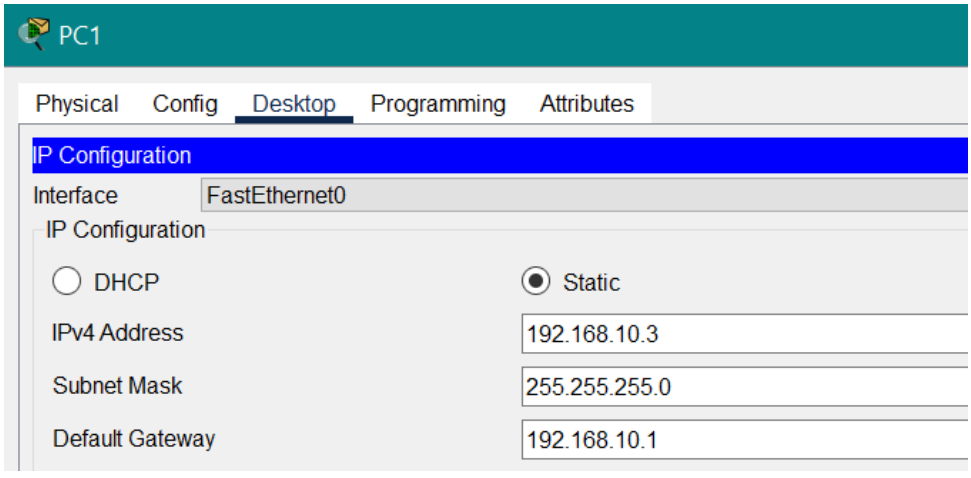
Steps to Configure Single Area OSPF on Cisco Packets Tracer:

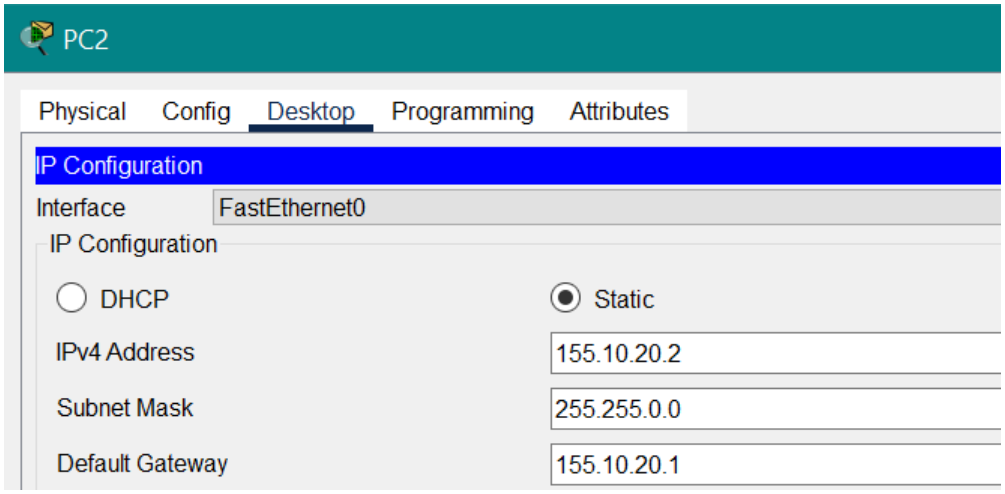
Topology :

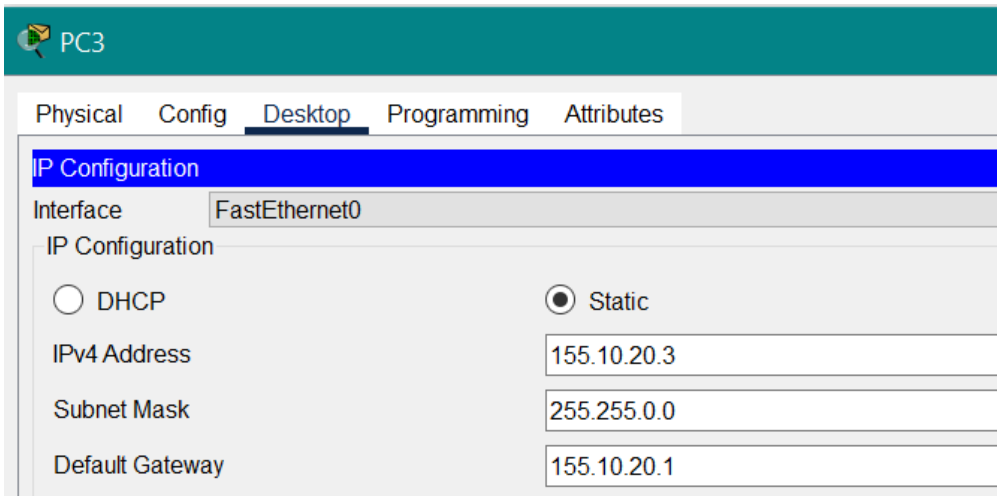


Assigning ip addresses to pc's & routers.

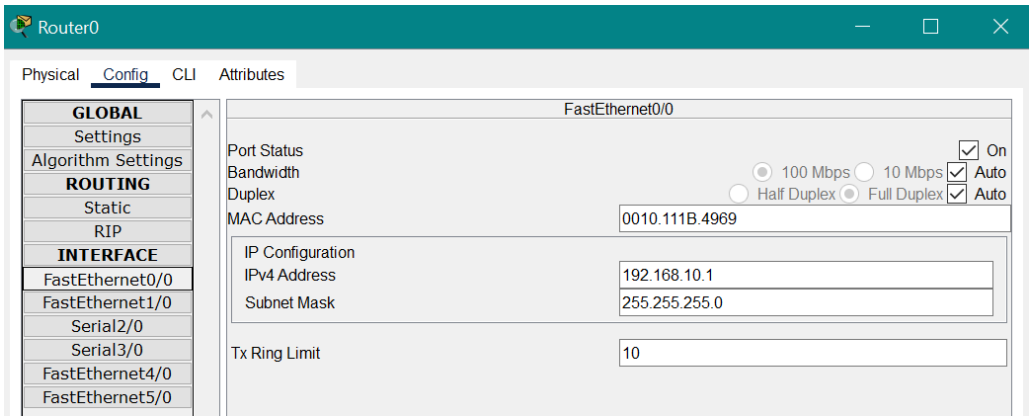


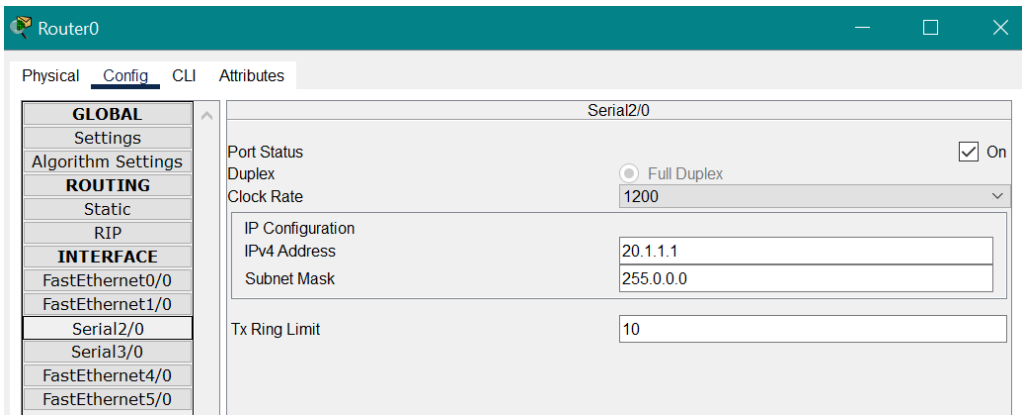


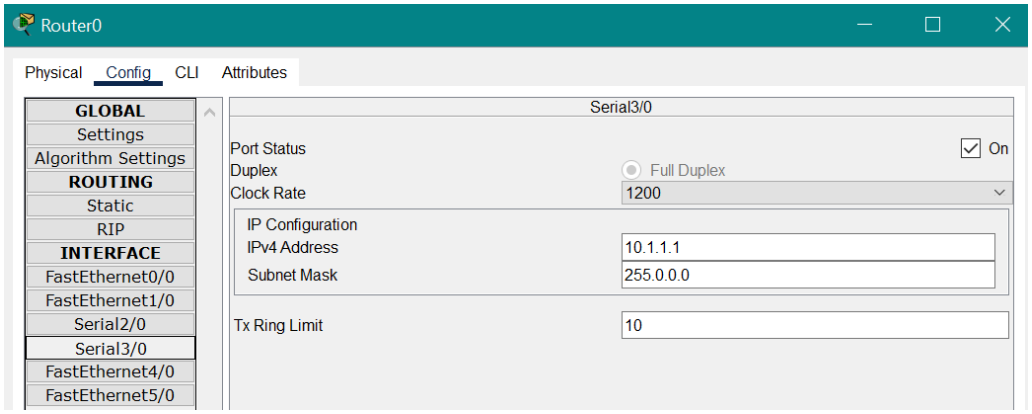

PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
155.10.20.2
Subnet Mask
255.255.0.0
Default Gateway
155.10.20.1


PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
155.10.20.3
Subnet Mask
255.255.0.0
Default Gateway
155.10.20.1

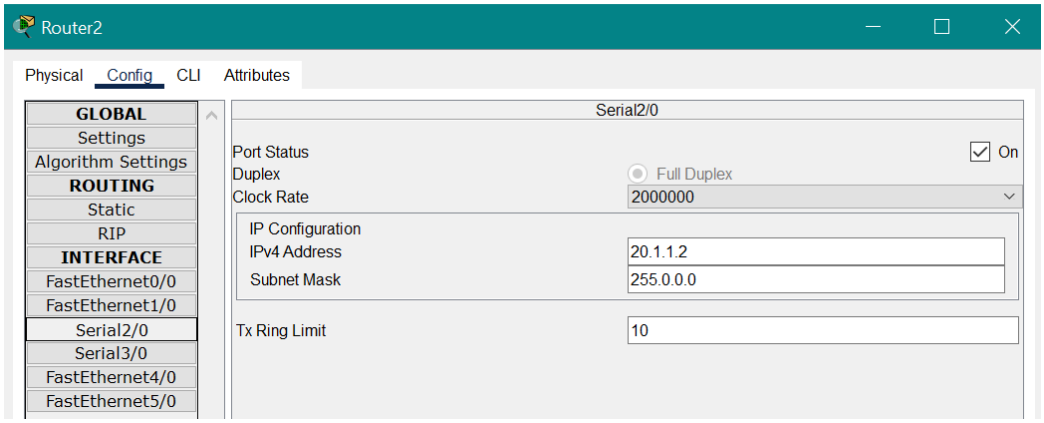
Router 0:

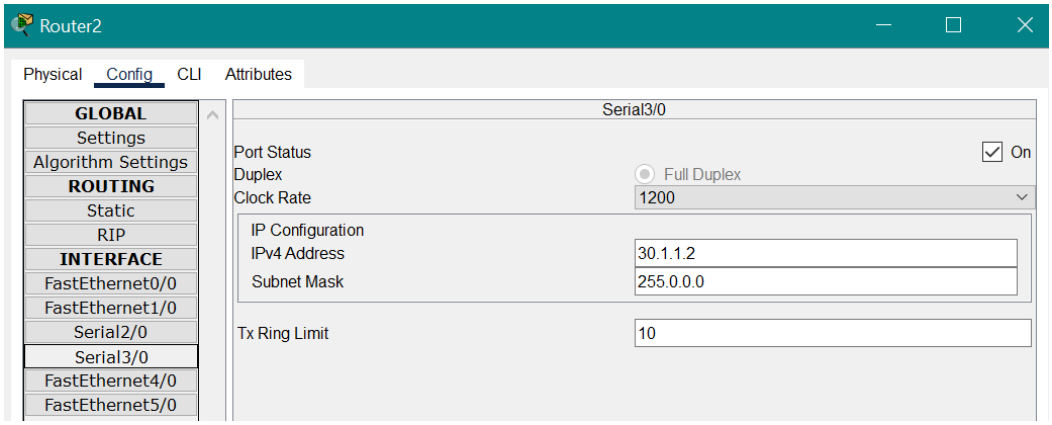

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0010.111B.4969
IP Configuration
IPv4 Address
192.168.10.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10


Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Serial2/0
Port Status
On
Duplex
Full Duplex
Clock Rate
1200
IP Configuration
IPv4 Address
20.1.1.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10

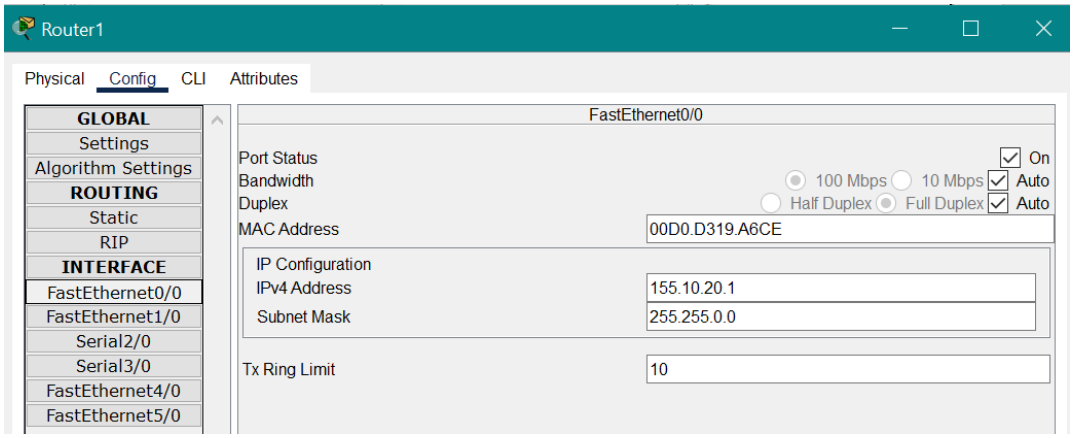


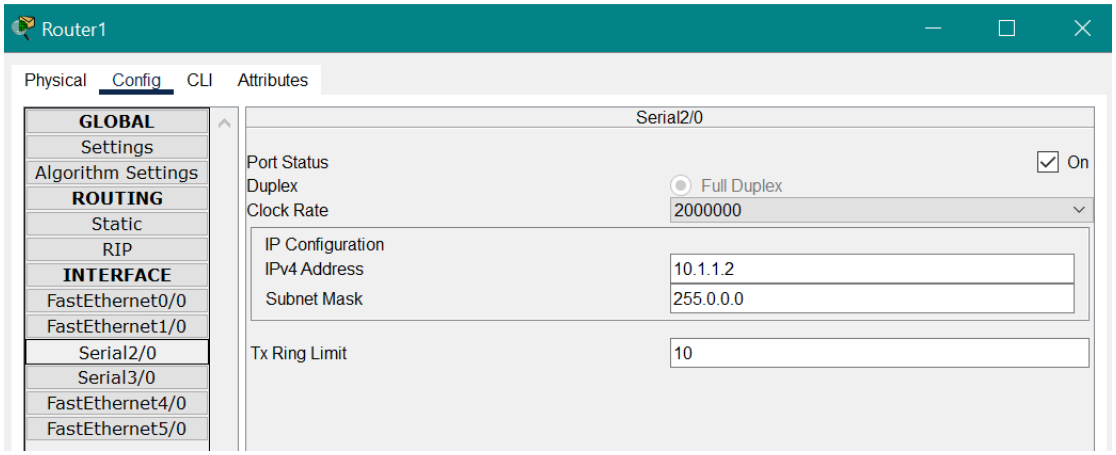
Router 2:

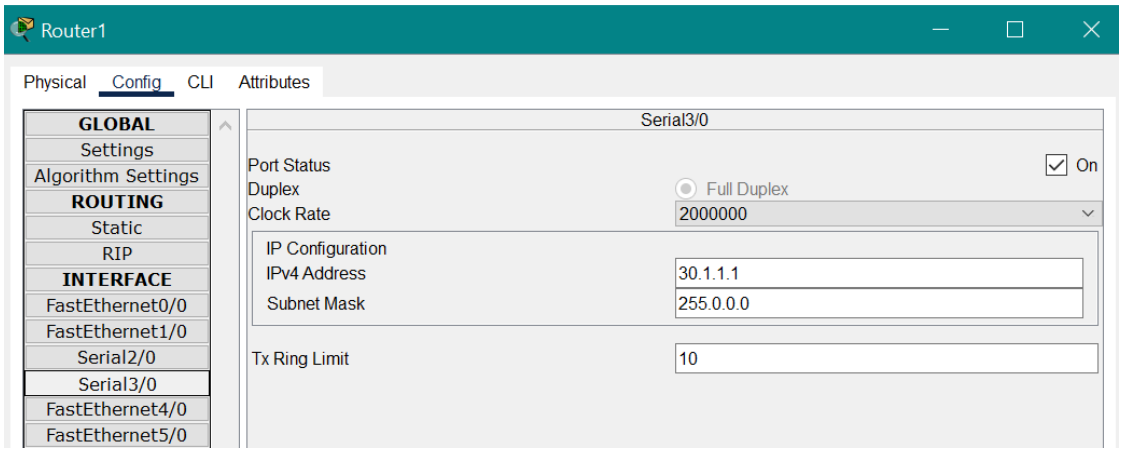




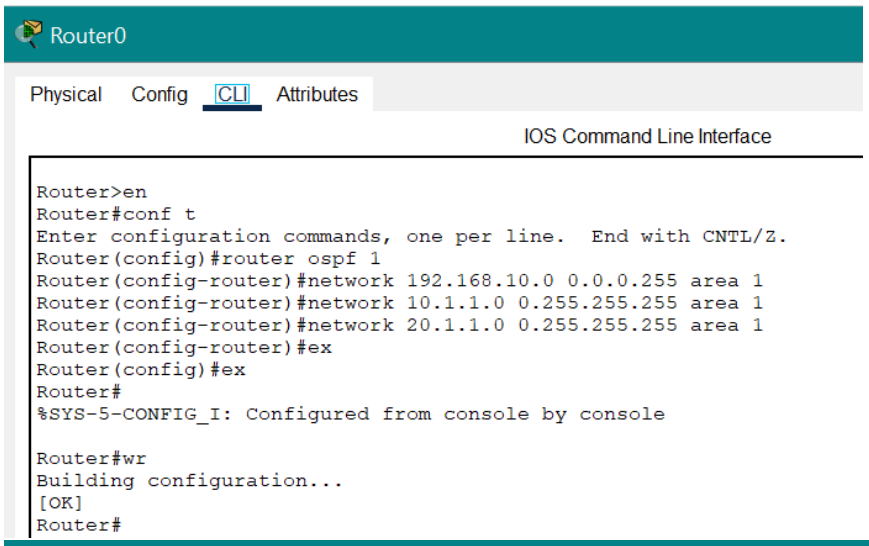
Router 1:

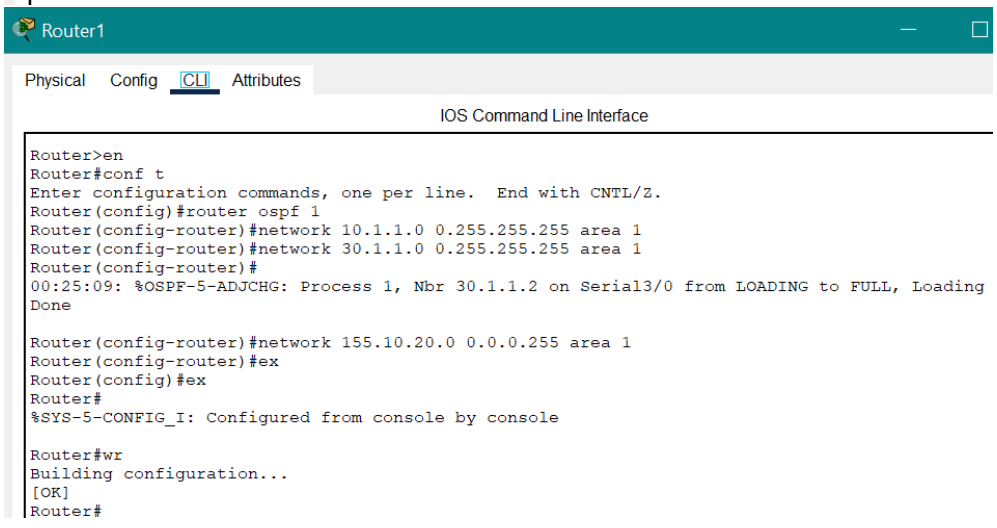


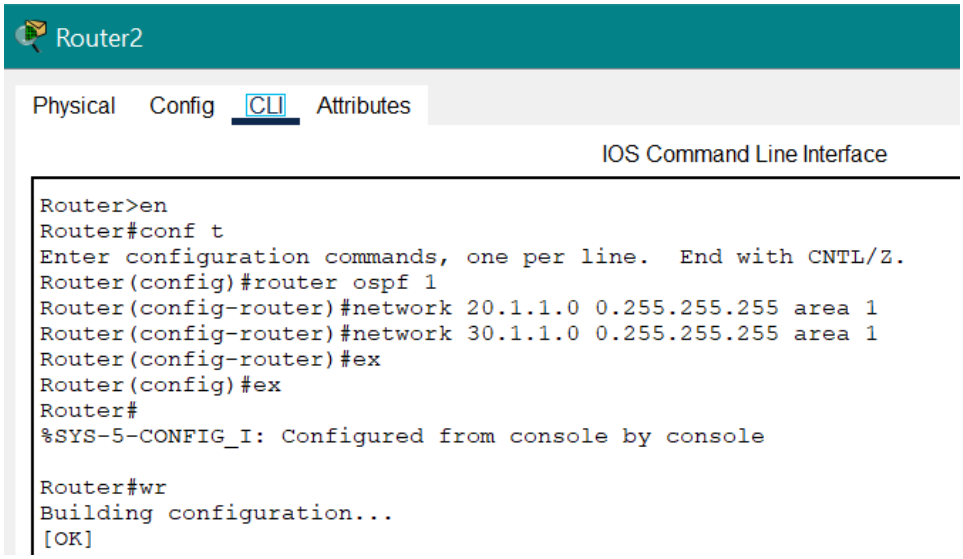




go to CLI mode on each router and type the commands that are given below:







OUTPUT:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	PC2	ICMP		0.000	N	0	(edit)
	Successful	PC0	PC3	ICMP		0.000	N	1	(edit)
	Successful	PC1	PC2	ICMP		0.000	N	2	(edit)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC1	PC3	ICMP		0.000	N	3	(edit)
	Successful	PC2	PC1	ICMP		0.000	N	4	(edit)
	Successful	PC2	PC0	ICMP		0.000	N	5	(edit)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC3	PC1	ICMP		0.000	N	0	(edit)
	Successful	PC3	PC0	ICMP		0.000	N	1	(edit)

(B) : Create a Network to Implement Multi-Area OSPF.

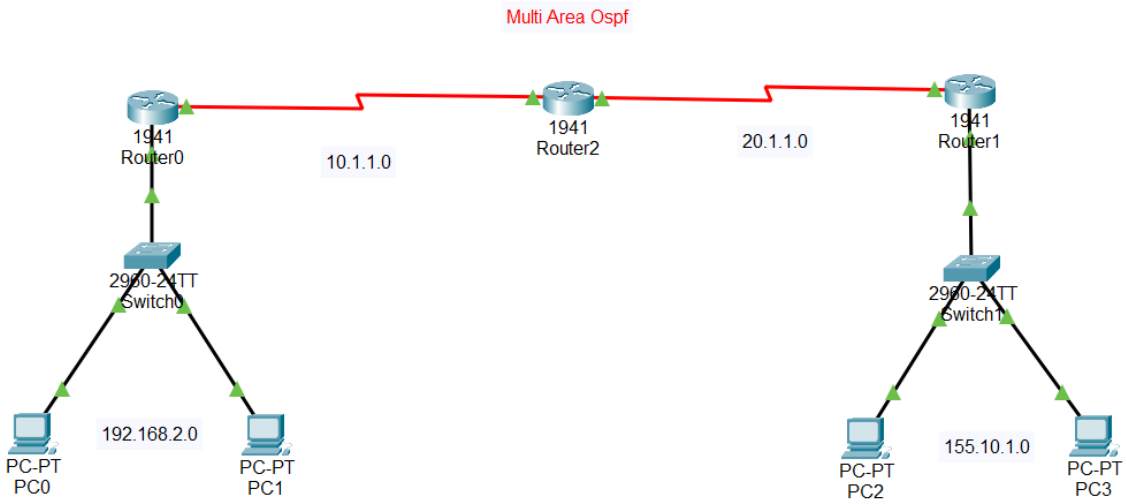
Steps to Configure Multi Area OSPF on Cisco Packets Tracer:

1. Network Design Description:

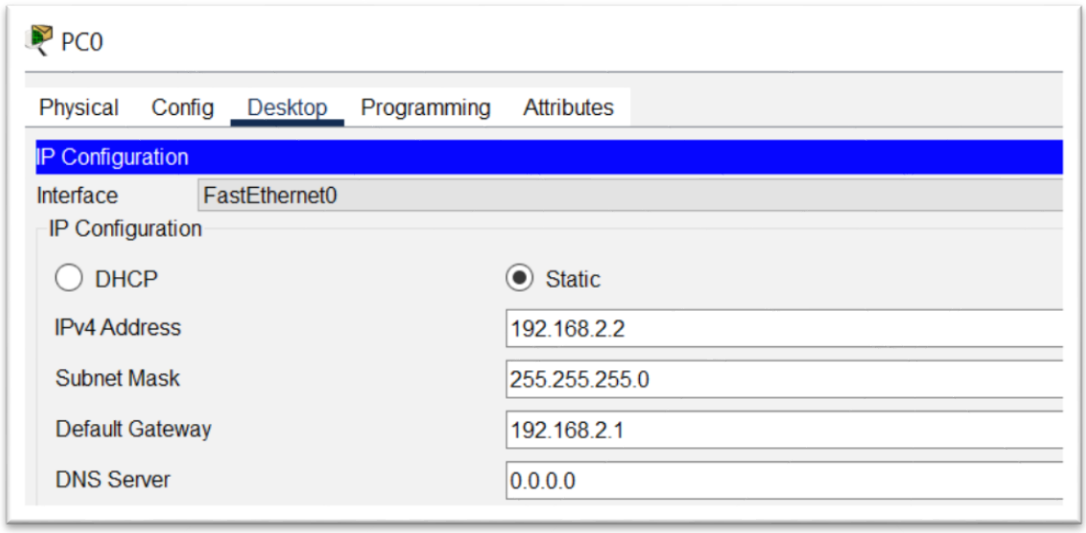
This network consists of three routers, two switches, and four PCs, arranged to demonstrate OSPF routing between multiple network segments. The design includes both LAN and WAN connections, allowing dynamic routing and inter-network communication.

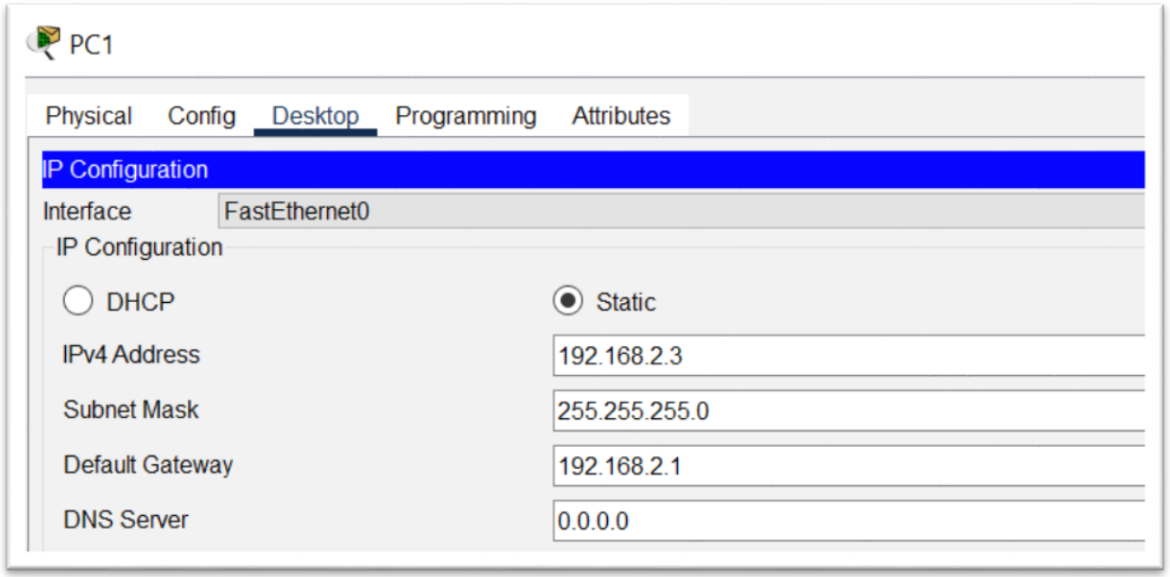
Topology Overview:

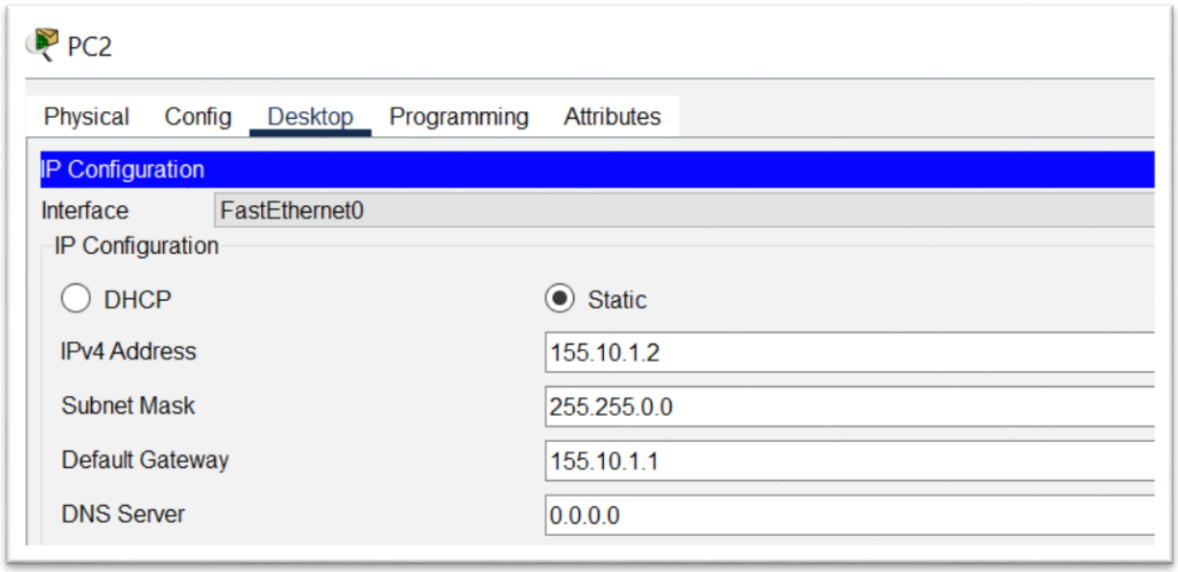
- Router0 is connected to Router2 via a serial link using the subnet 10.1.1.0/24.
- Router2 is connected to Router1 via another serial link using the subnet 20.1.1.0/24.
- Router0 connects to Switch0 via an Ethernet connection, which serves the subnet 192.168.2.0/24.
- Two PCs (PC0 and PC1) are connected to Switch0 in the 192.168.2.0/24 network.
- Router1 connects to Switch1 via an Ethernet connection, which serves the subnet 155.10.1.0/24.
- Two PCs (PC2 and PC3) are connected to Switch1 in the 155.10.1.0/24 network.

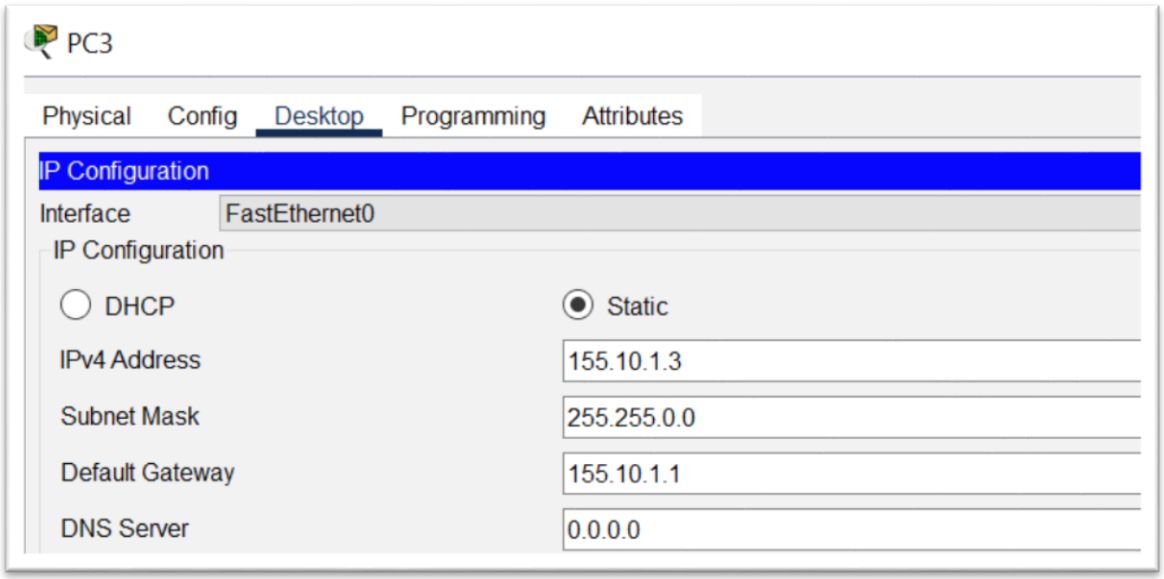


Assigning ip addresses to pc's & routers.

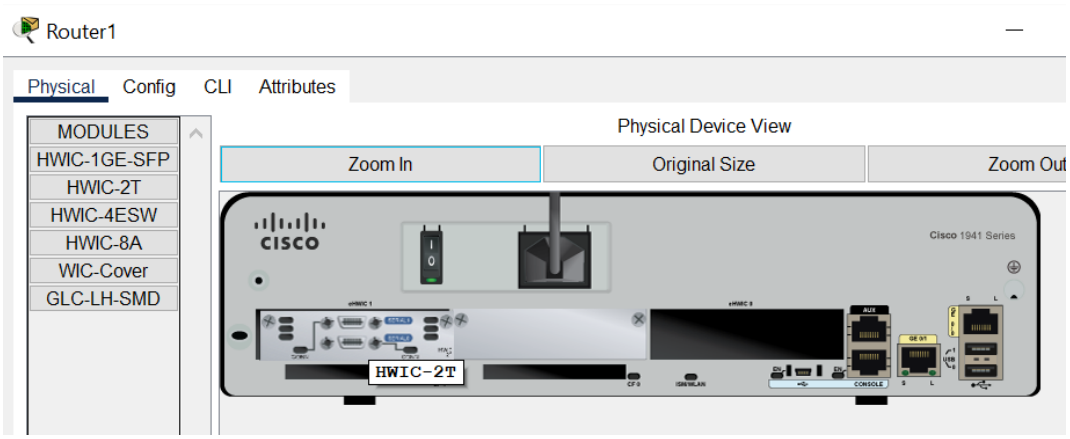


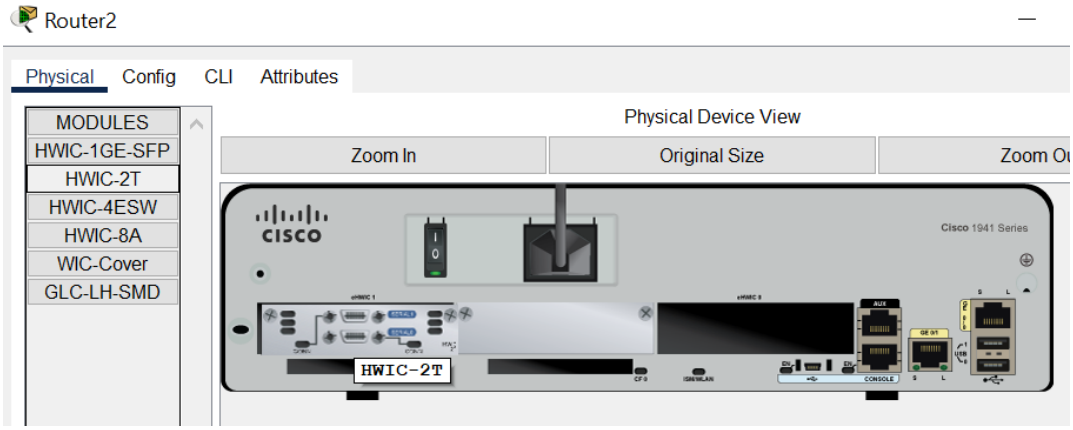

PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.2.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
0.0.0.0


PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
155.10.1.2
Subnet Mask
255.255.0.0
Default Gateway
155.10.1.1
DNS Server
0.0.0.0


PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
155.10.1.3
Subnet Mask
255.255.0.0
Default Gateway
155.10.1.1
DNS Server
0.0.0.0

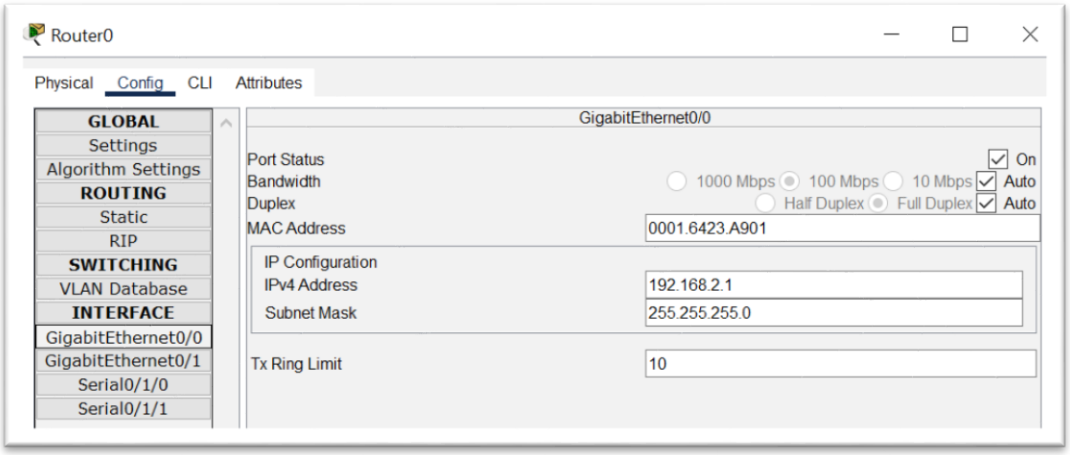
For Router connection via Serial DTE, Add 1 port Of HWIC-2T to each router.



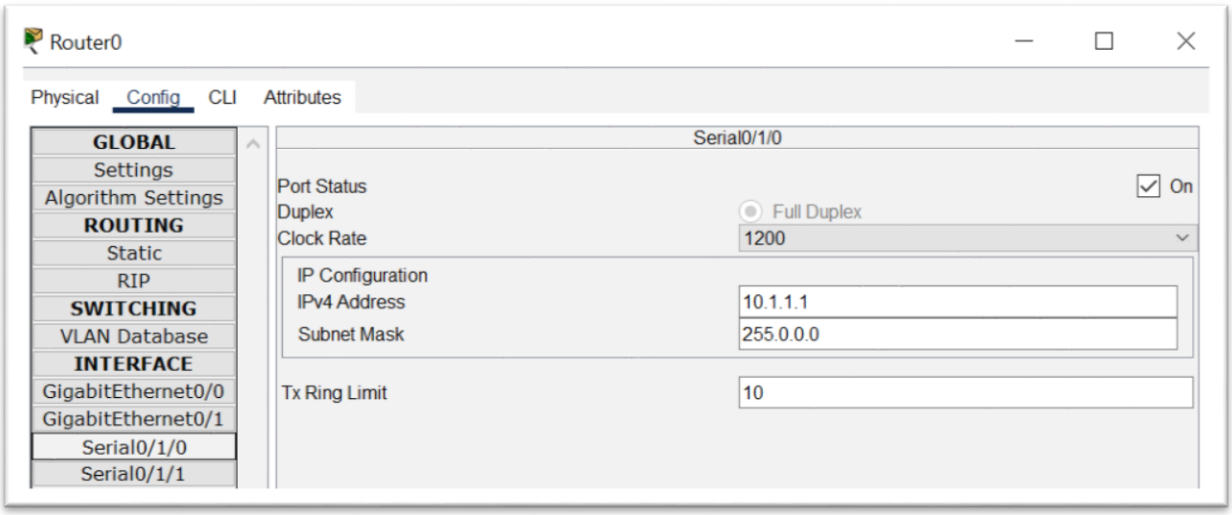


Router 0:

- Gigabit Ethernet 0/0

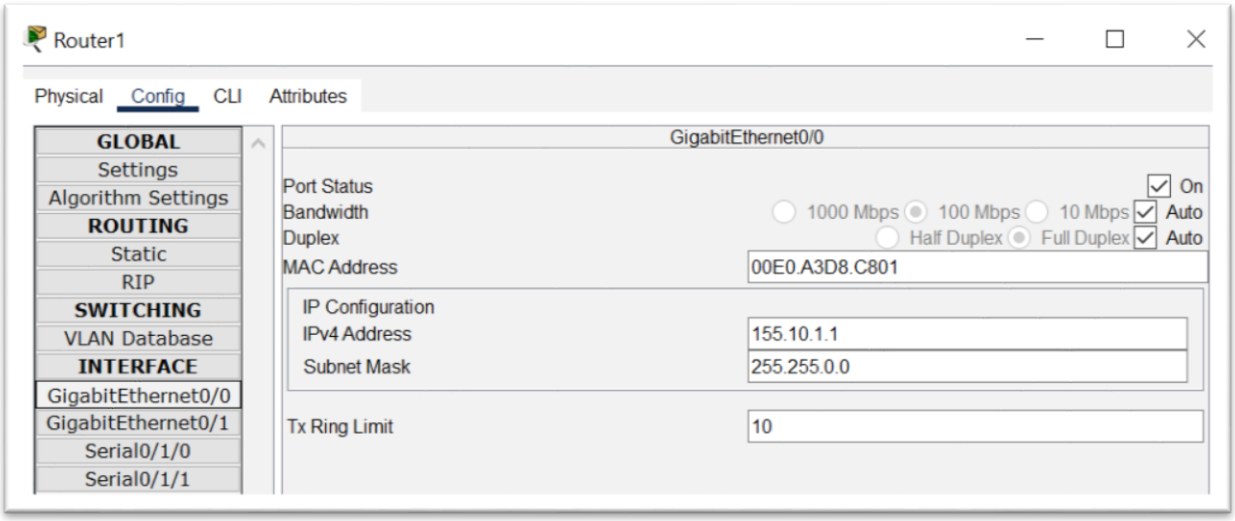


- Serial 0/1/0

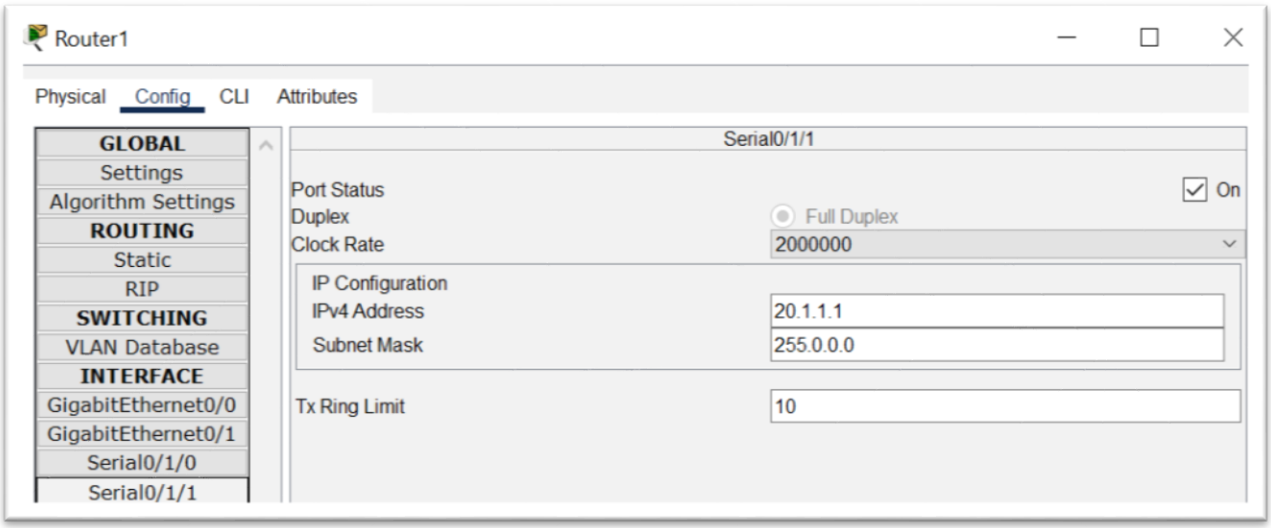


Router 1:

- Gigabit Ethernet 0/0

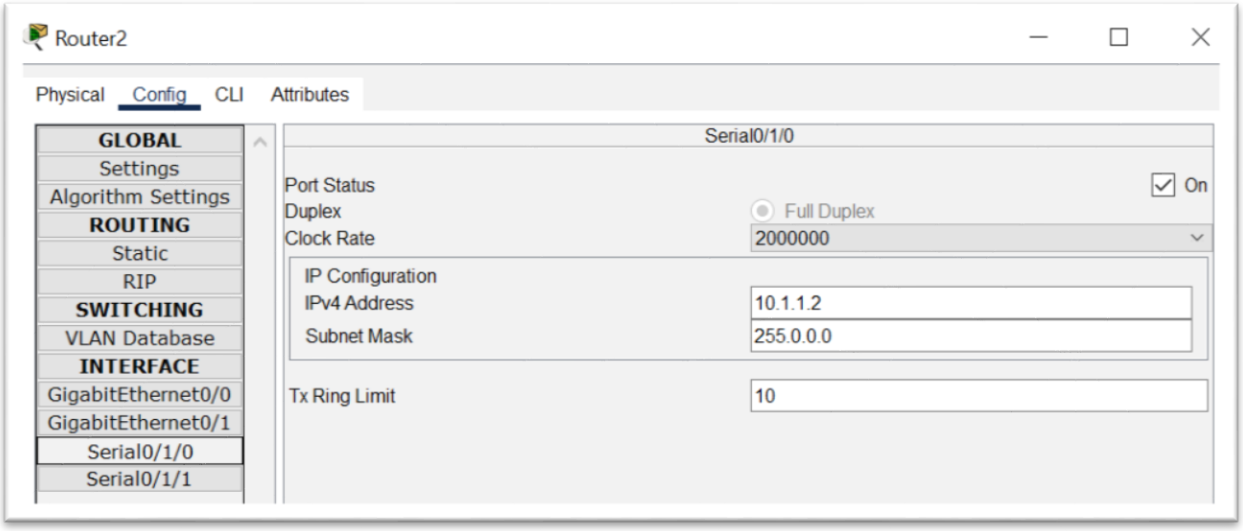


- Serial 0/1/1

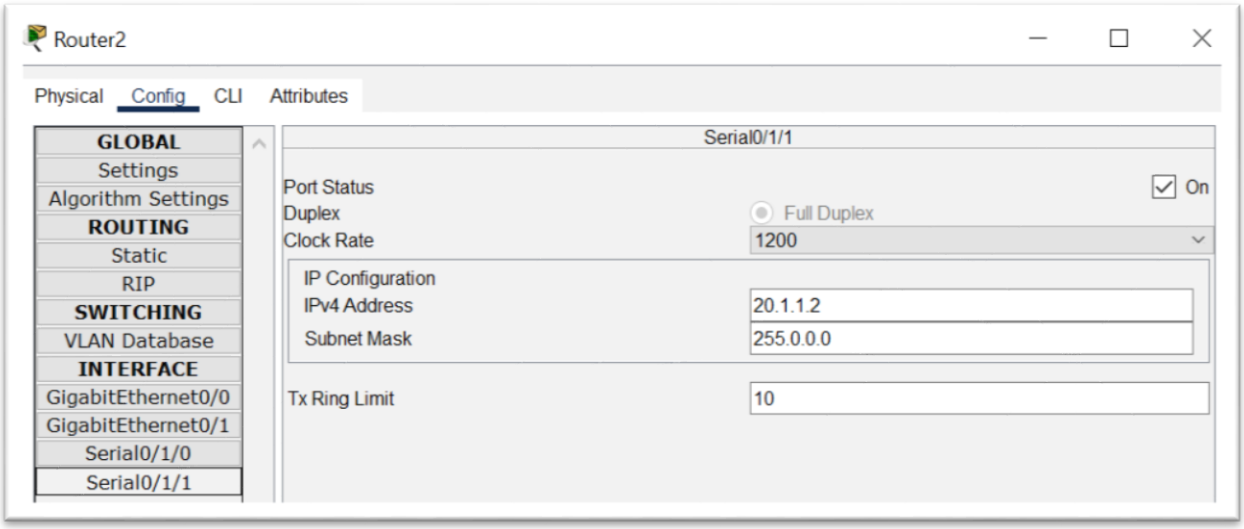


Router 2:

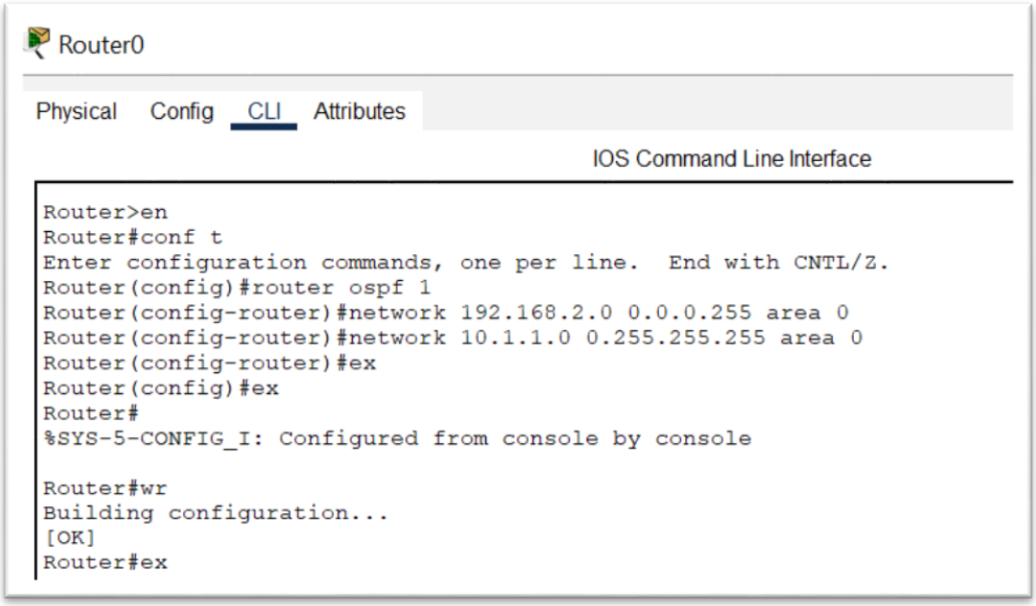
- Serial 0/1/0

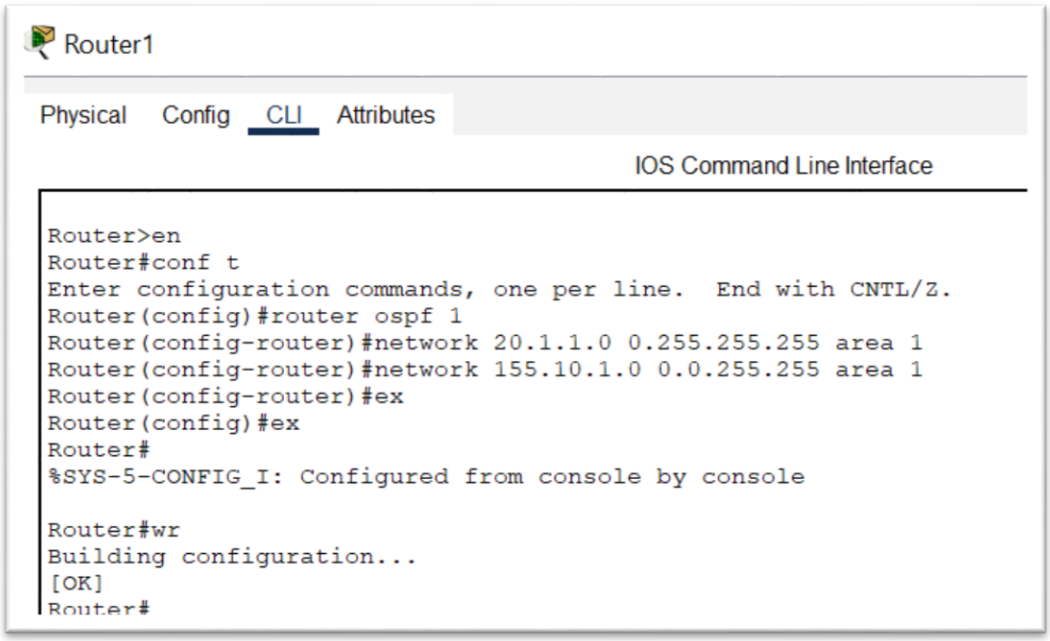


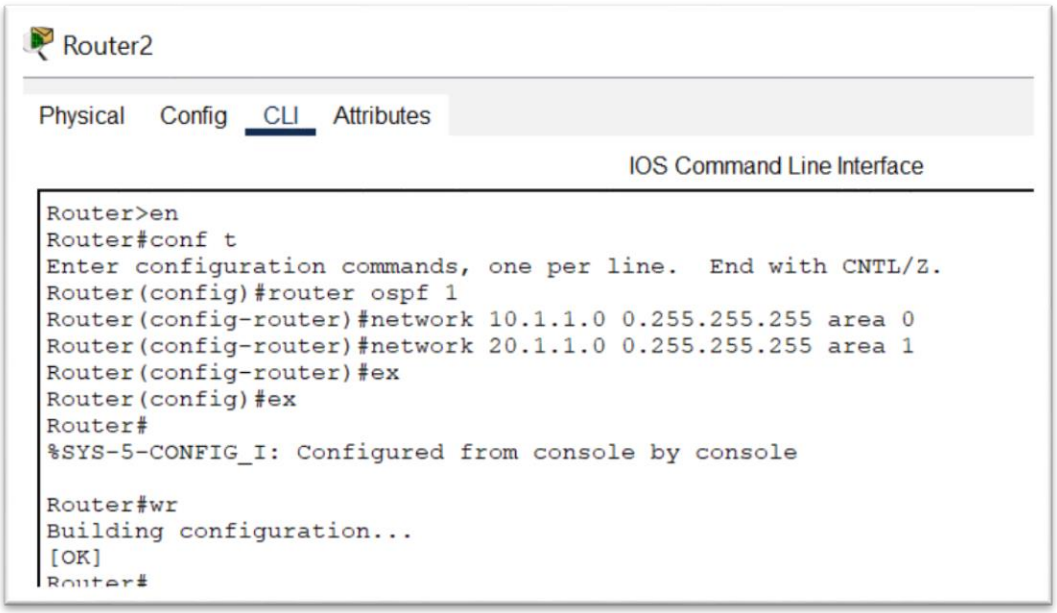
- Serial 0/1/1



go to CLI mode on each router and type the commands that are given below:







OUTPUT:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC2	ICMP		0.000	N	0	(edit)	
	Successful	PC0	PC3	ICMP		0.000	N	1	(edit)	
	Successful	PC1	PC2	ICMP		0.000	N	2	(edit)	
	Successful	PC1	PC3	ICMP		0.000	N	3	(edit)	

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC2	PC1	ICMP		0.000	N	0	(edit)	
	Successful	PC2	PC0	ICMP		0.000	N	1	(edit)	
	Successful	PC3	PC1	ICMP		0.000	N	2	(edit)	
	Successful	PC3	PC0	ICMP		0.000	N	3	(edit)	

PRACTICAL NO : 6

AIM : Create a Network and Implement a **BGP Protocol**.

1. Introduction to BGP

- BGP (Border Gateway Protocol) is a path vector routing protocol used to exchange routing and reachability information between autonomous systems (ASes) on the Internet. It is the protocol that makes the Internet work by connecting different organizations' networks together.
- BGP is classified as an Exterior Gateway Protocol (EGP) because it operates between different autonomous systems, unlike Interior Gateway Protocols (IGPs) such as OSPF or RIP that operate within a single AS.
- BGP uses TCP (Transmission Control Protocol) port 179 for establishing reliable communication between peers (BGP routers).
- BGP makes routing decisions based on path attributes, such as AS path, next-hop, and various policy rules, rather than simply selecting the shortest path like OSPF.
- BGP is a policy-based routing protocol, allowing network administrators to set rules and policies to control routing decisions and traffic flow.
-

2. Where is BGP Used : BGP is typically used in:

- Large enterprise networks connected to multiple ISPs (multi-homing).
- Internet Service Providers (ISPs) to exchange routing information with other ISPs and organizations.
- Data centers and cloud networks requiring policy-based and scalable routing.
- Backbone networks where global Internet routing decisions are made.
- Due to its complexity, BGP is not suitable for small networks or environments where automatic and simple routing is preferred.

3. Key features of BGP include

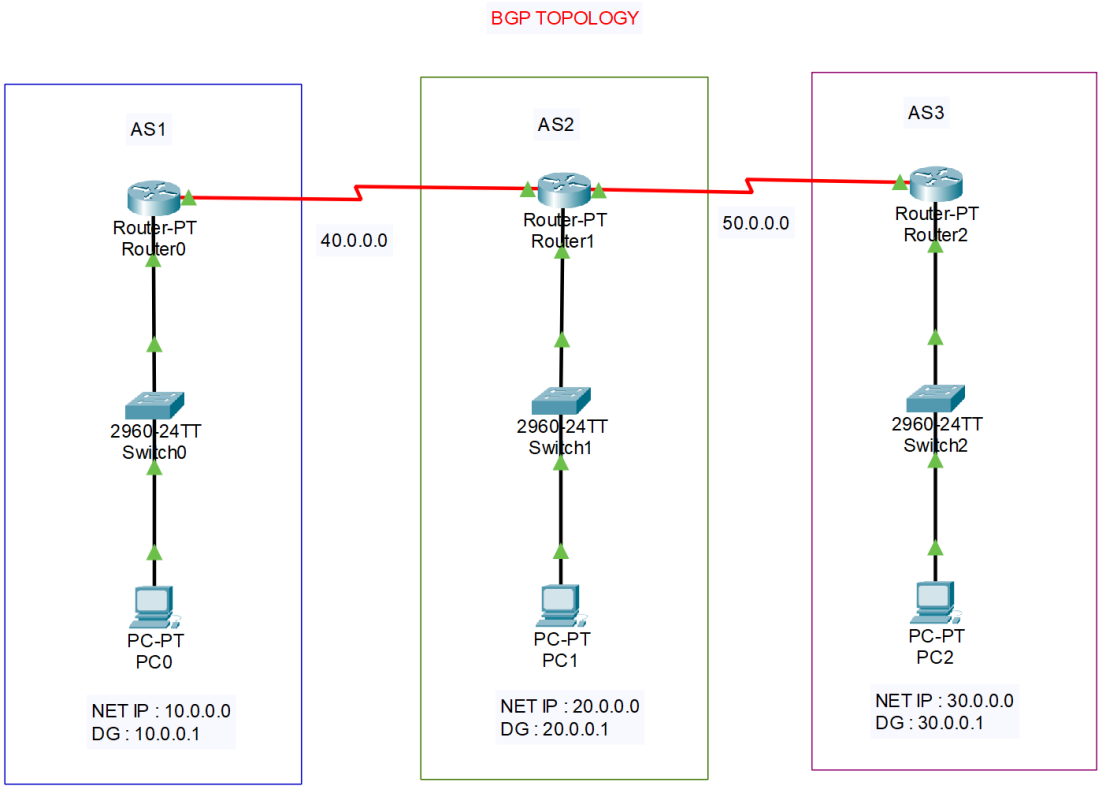
- Scalability: Handles large routing tables, making it ideal for global Internet use.
- Policy Control: Supports complex routing policies using AS-path filters, prefix lists, and route maps.
- Loop Prevention: Uses AS-path to prevent routing loops by tracking route history across ASes.
- Path Vector Protocol: Maintains AS path to select the best route based on policy and topology.
- Route Aggregation: Summarizes multiple IP prefixes into a single route to reduce table size.

4. How BGP Works in a Network Topology

- Each BGP router (peer) is configured with a list of neighbor routers to establish sessions.
- BGP is enabled manually on routers requiring external or policy-based routing.
- Peer Establishment: BGP routers establish TCP connections using port 179 and exchange Open messages.
- Routing Information Exchange: Once the session is up, routers exchange Update messages that carry network prefixes and path attributes.
- Best Path Selection: Routers use BGP's decision algorithm considering AS path, local preference, MED, origin, and other attributes.
- Updates and Withdrawals: Routers send updates for new routes and withdrawal messages for unreachable routes. Forwarding: Packets are forwarded based on the best path selected by BGP.

The process ensures that all routers across different autonomous systems can make informed routing decisions and maintain consistent Internet-wide connectivity.

Steps to Configure BGP (Border Gateway Protocol) on Cisco Packets Tracer:



Network Design and Connections for BGP Topology

1. Network Overview

This network consists of three Autonomous Systems (AS1, AS2, and AS3). Each AS has its own router, switch, and PC. The routers in each AS connect to each other to form a BGP (Border Gateway Protocol) network for routing between different autonomous systems.

2. Components in Each AS

- Router: Each AS has one router that runs BGP to exchange routing information with routers in other ASes.
- Switch: Connects the router to the PCs within the local AS.
- PC: End device connected to the switch, representing hosts within each network.

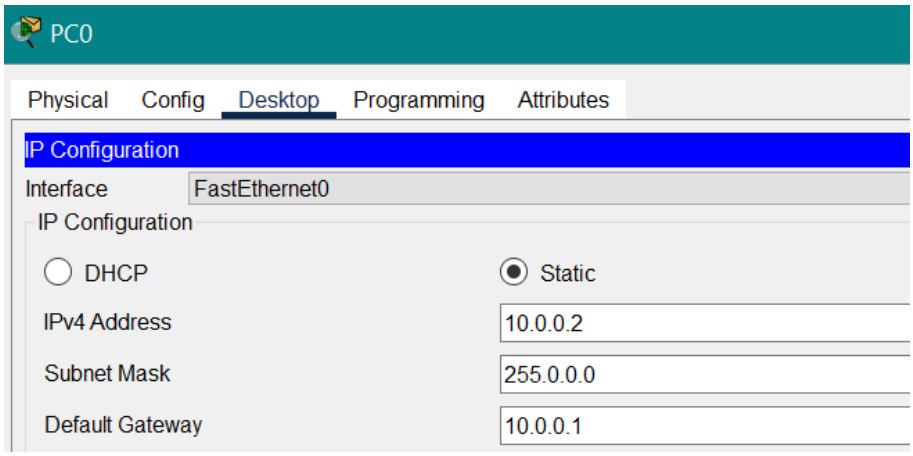
3. IP Addressing Scheme

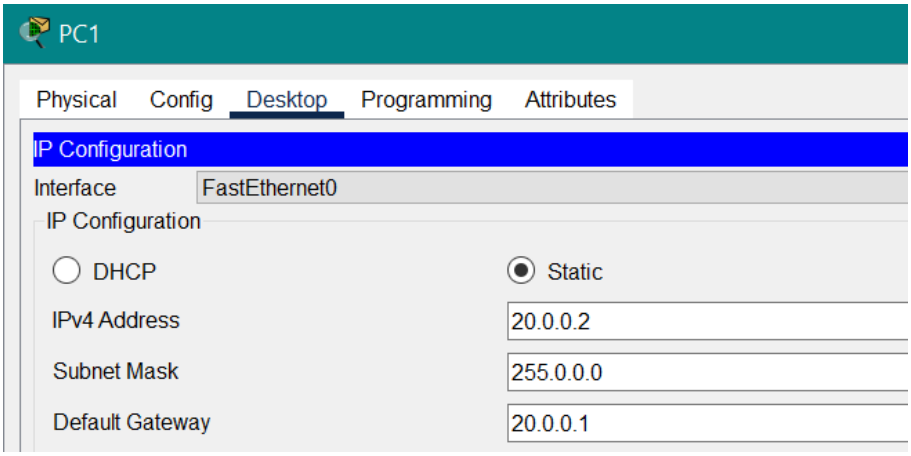
- Each AS has a unique subnet for its local network:
    1. AS1: 10.0.0.0/24
    2. AS2: 20.0.0.0/24
    3. AS3: 30.0.0.0/24
- PCs have IP addresses within their respective subnets, and their default gateway is set to the router's local IP.
- The routers are connected through point-to-point links with IP addresses on separate subnets:
    1. Link between AS1 and AS2: 40.0.0.0/30
    2. Link between AS2 and AS3: 50.0.0.0/30

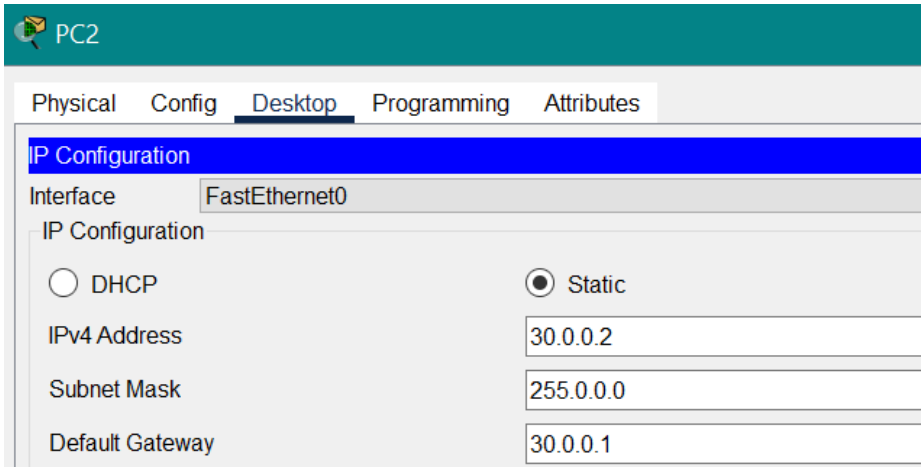
4. Physical Connections and Cable Types

- PC to Switch: Connected using a straight-through cable to allow communication within the LAN.
- Switch to Router: Connected using a straight-through cable to link the LAN to the router.
- Router to Router (WAN links): Connected using either a cross-over cable or serial cable, forming inter-AS links used for BGP peering.

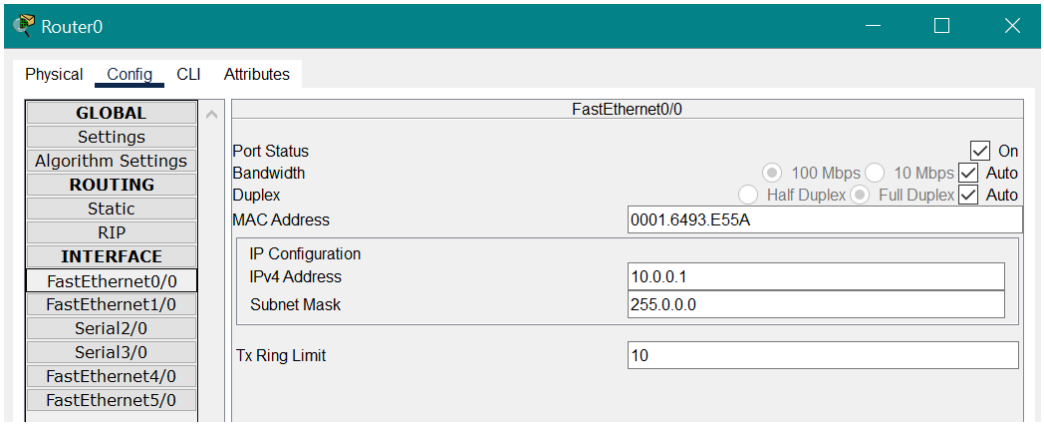
Assigning ip addresses to pc's & routers.

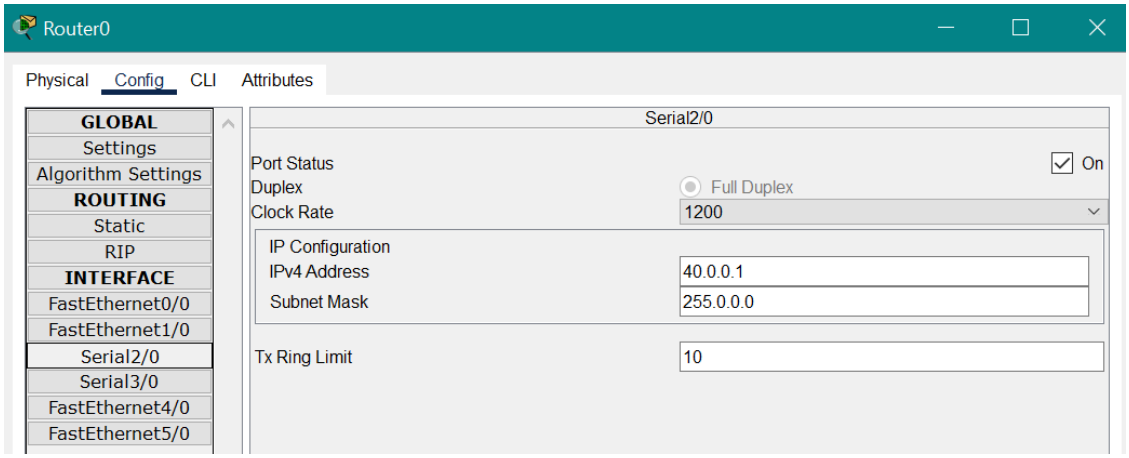




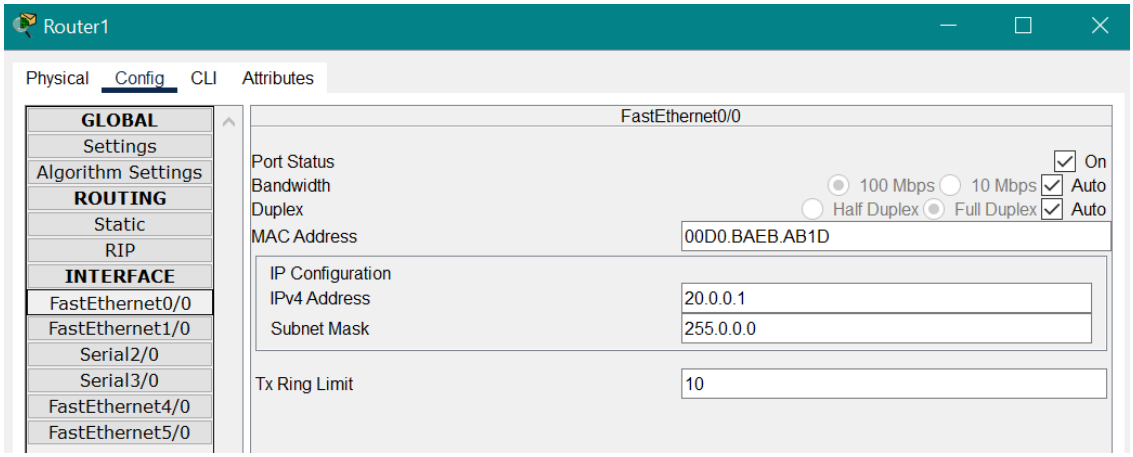


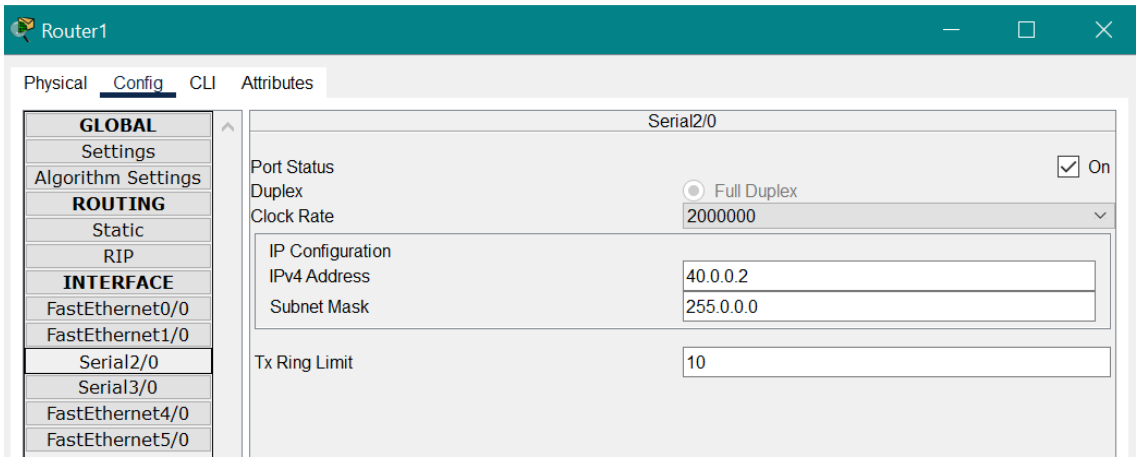
Router 0:

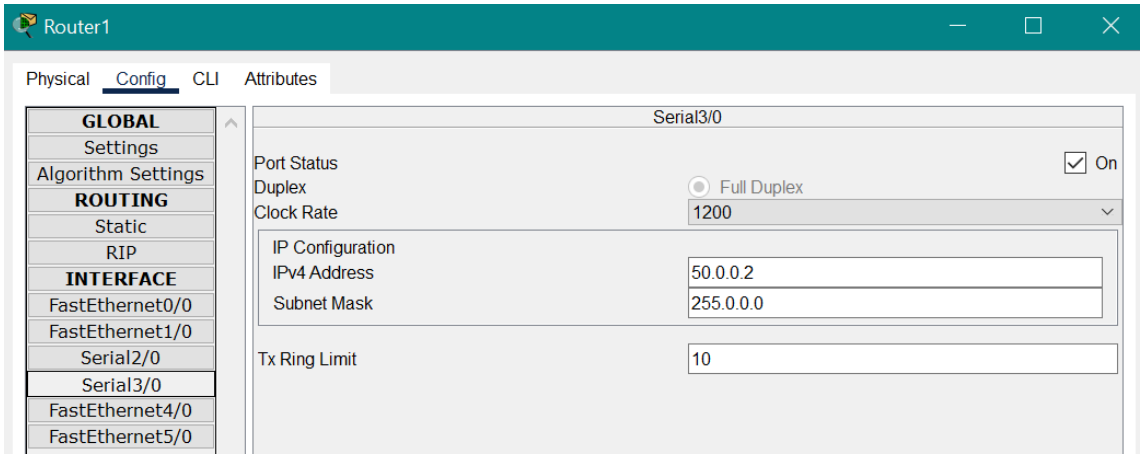



Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Serial2/0
Port Status
On
Duplex
Full Duplex
Clock Rate
1200
IP Configuration
IPv4 Address
40.0.0.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10

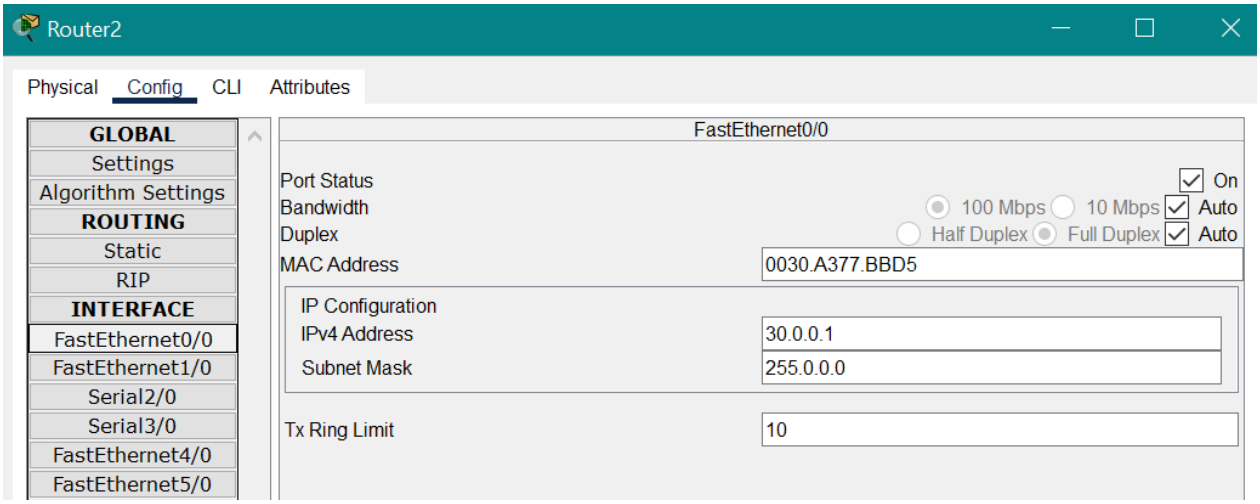
Router 1:

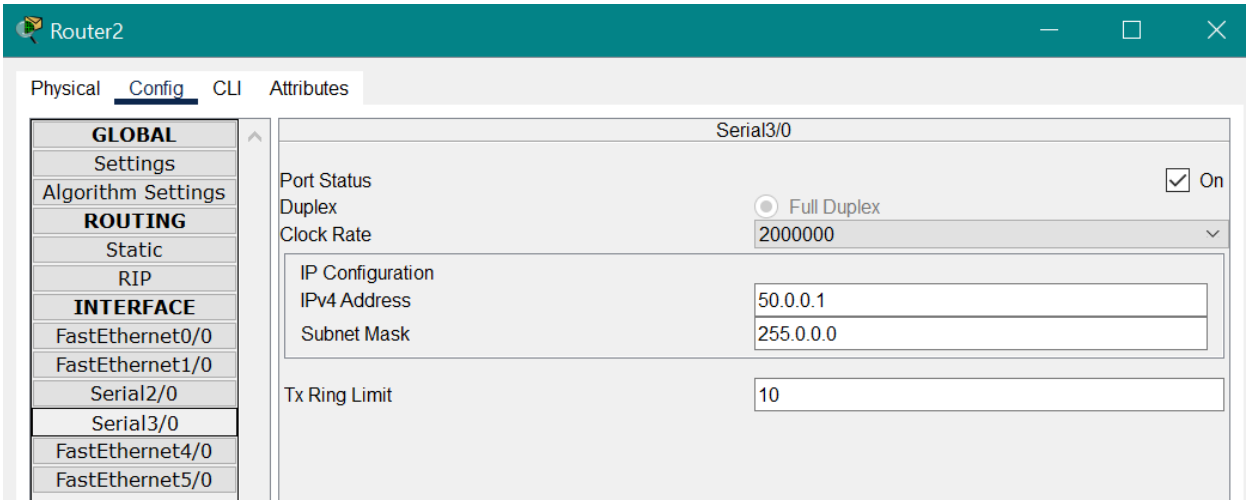

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00D0.BAEB.AB1D
IP Configuration
IPv4 Address
20.0.0.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Serial2/0
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

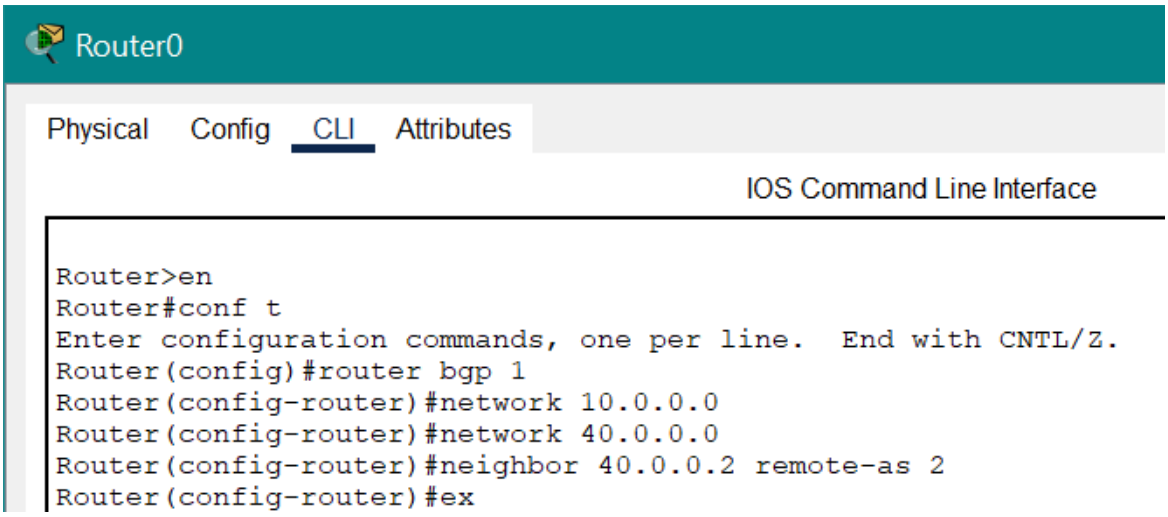

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Serial3/0
Port Status
On
Duplex
Full Duplex
Clock Rate
1200
IP Configuration
IPv4 Address
50.0.0.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10

Router 2:





Go to CLI mode on each router and type the commands that are given below:



Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router bgp 2
Router(config-router)#network 40.0.0.0
Router(config-router)#network 20.0.0.0
Router(config-router)#network 50.0.0.0
Router(config-router)#neighbor 40.0.0.1 remote-as 1
Router(config-router)#%BGP-5-ADJCHANGE: neighbor 40.0.0.1 Up

Router(config-router)#neighbor 50.0.0.1 remote-as 3
Router(config-router)#%BGP-5-ADJCHANGE: neighbor 50.0.0.1 Up

Router(config-router)#ex
Router(config)#
```

Router2

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router bgp 3
Router(config-router)#network 30.0.0.0
Router(config-router)#network 50.0.0.0
Router(config-router)#neighbor 50.0.0.2 remote-as 2
Router(config-router)#ex
```

OUTPUT:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	PC1	ICMP		0.000	N	0	(edit)
	Successful	PC0	PC2	ICMP		0.000	N	1	(edit)
	Successful	PC1	PC0	ICMP		0.000	N	2	(edit)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC1	PC2	ICMP		0.000	N	3	(edit)
	Successful	PC2	PC0	ICMP		0.000	N	4	(edit)
	Successful	PC2	PC1	ICMP		0.000	N	5	(edit)

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.

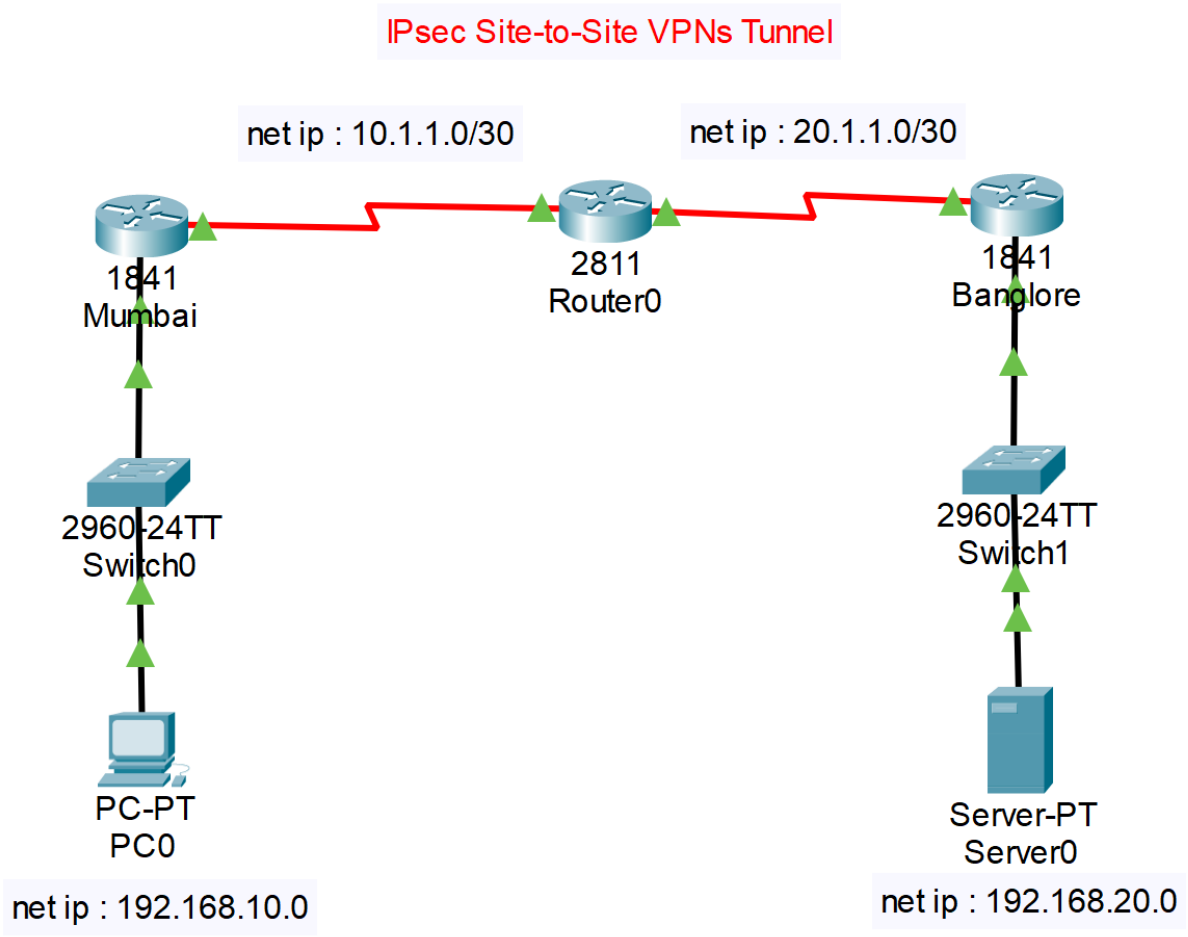
What is a Site-to-Site VPN?

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

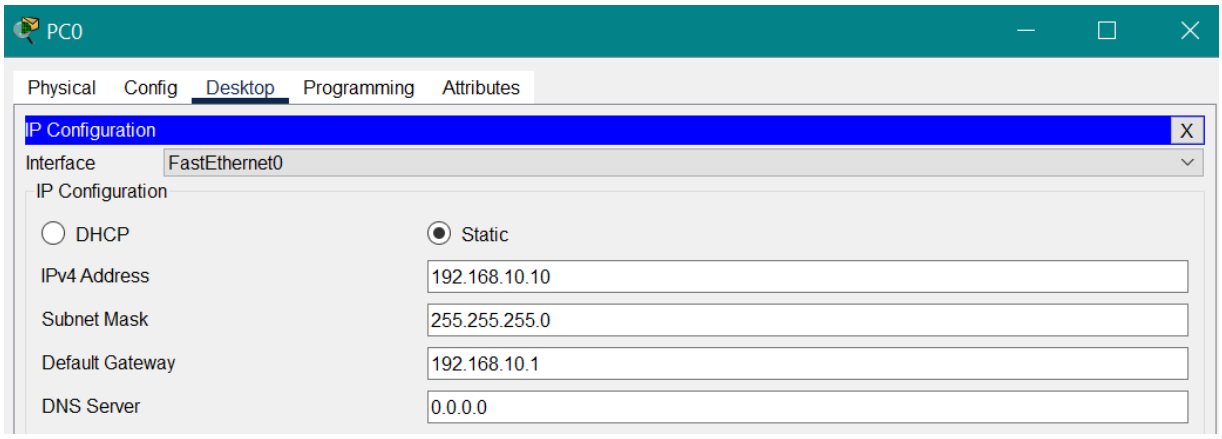
Example:

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

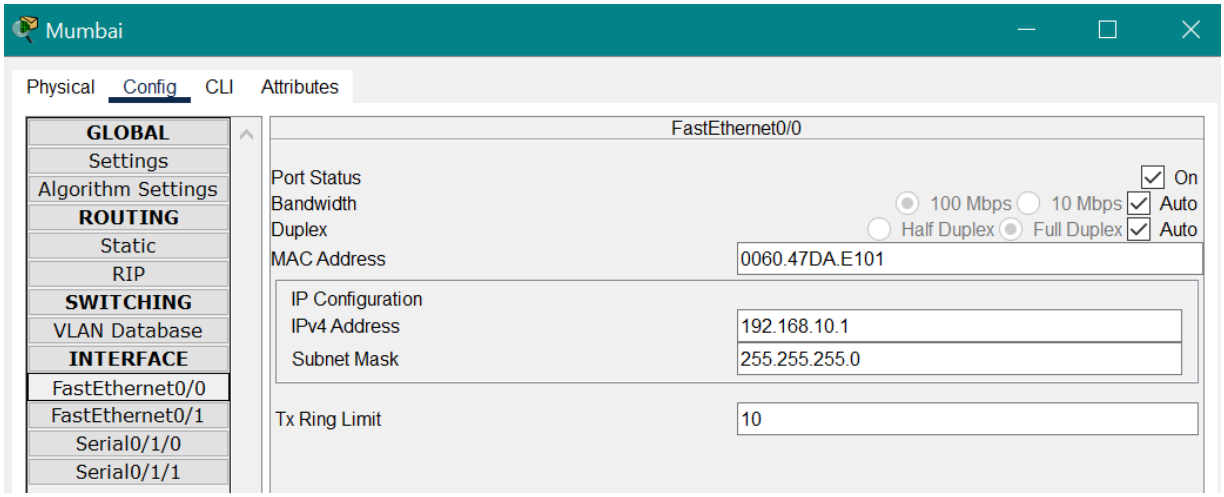
Topology:

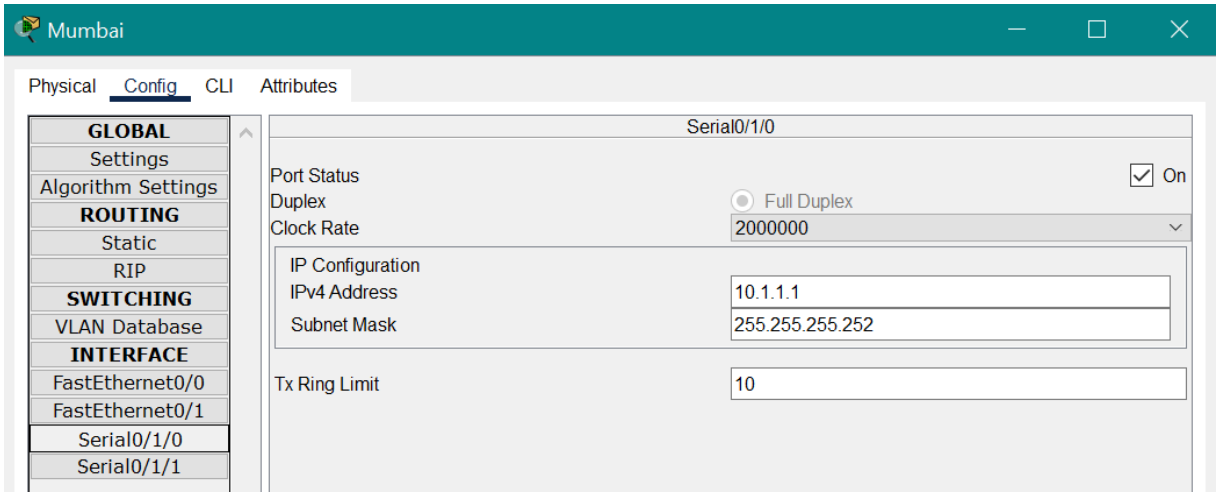


PC Configuration:

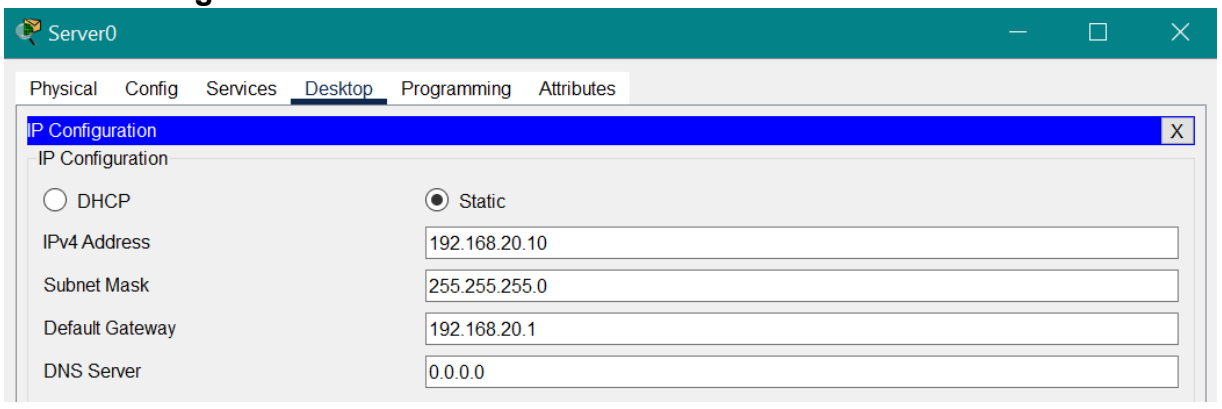


Router Configuration:(Mumbai)

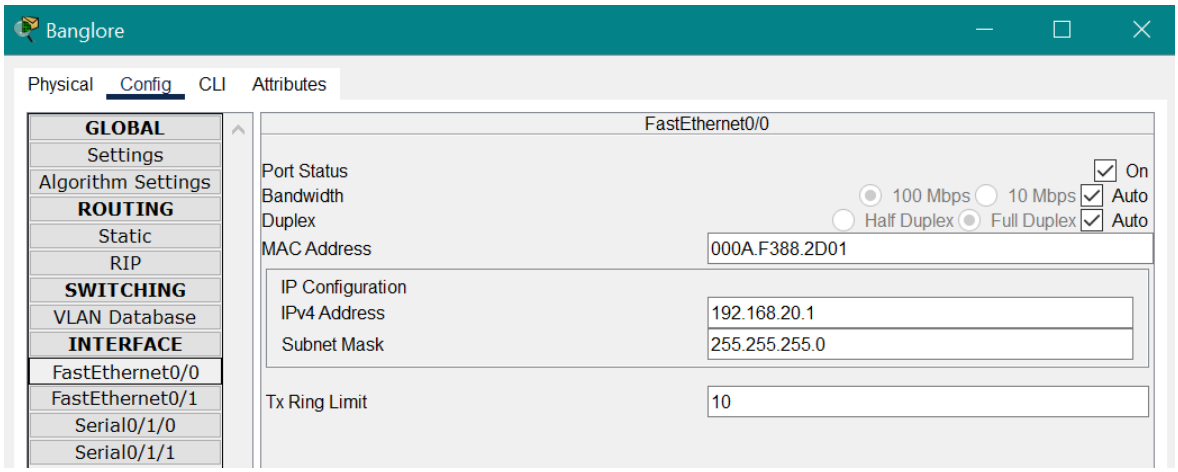


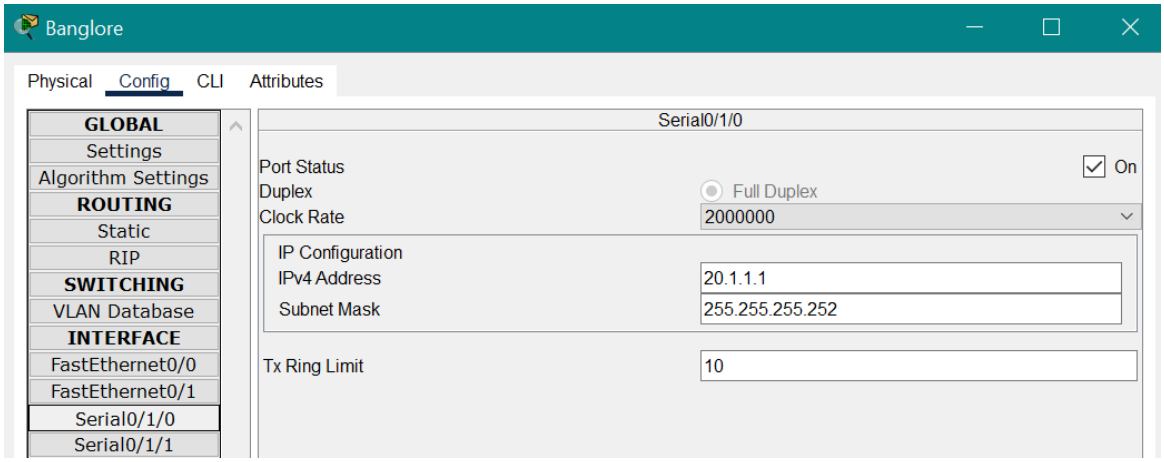


Server Configuration:

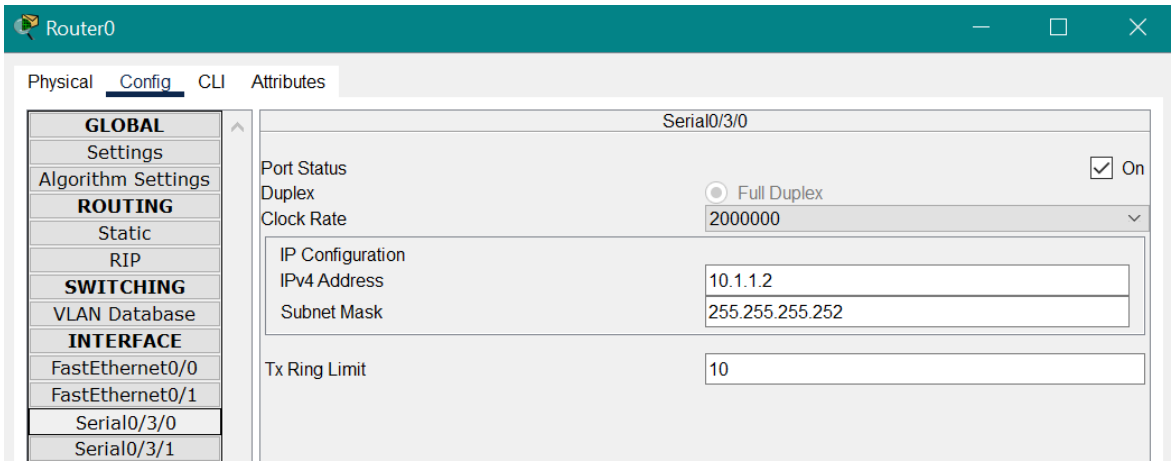


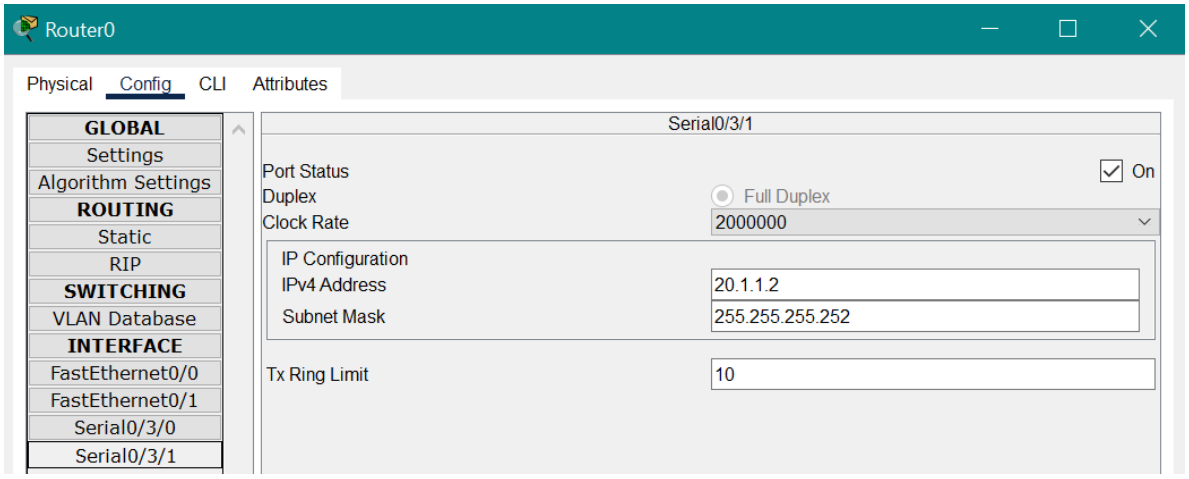
Router Configuration: (Bangalore)





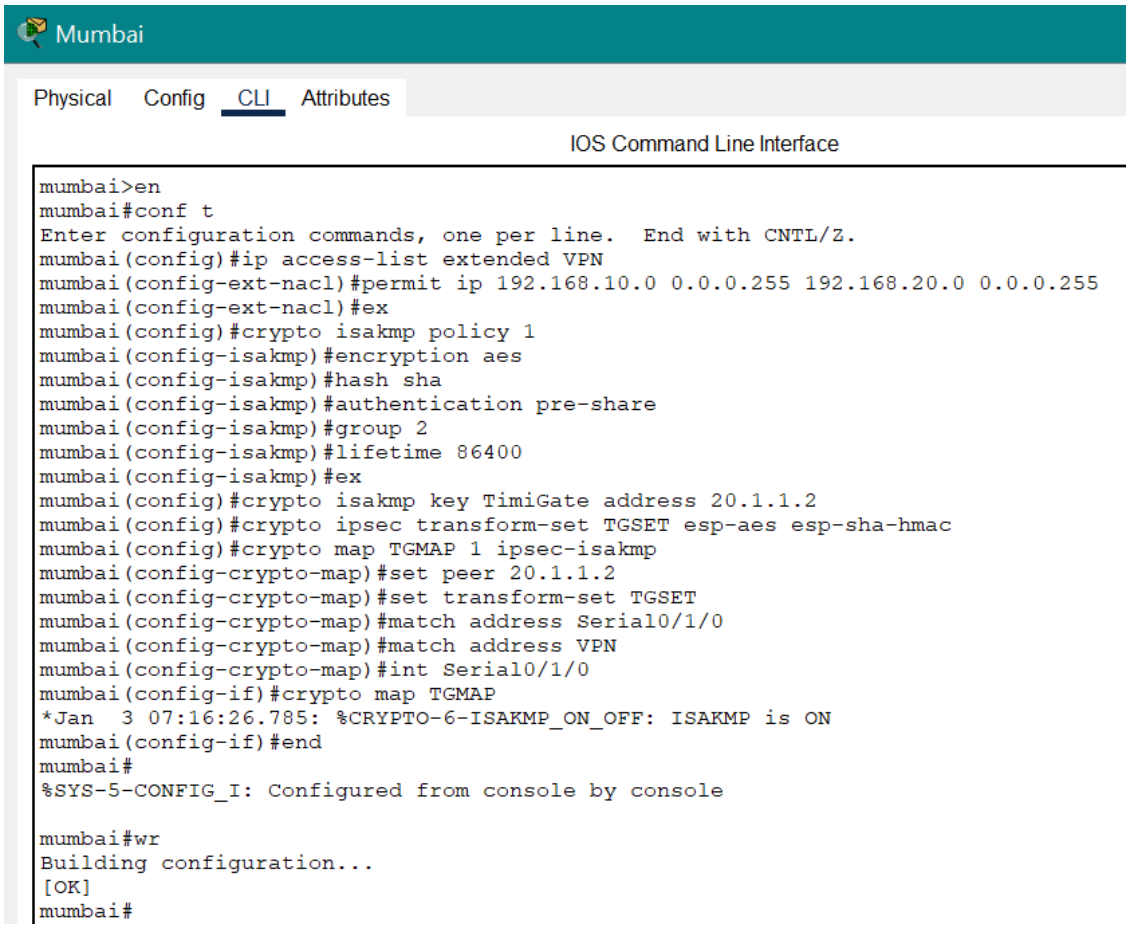
Router Configuration: (Router0)



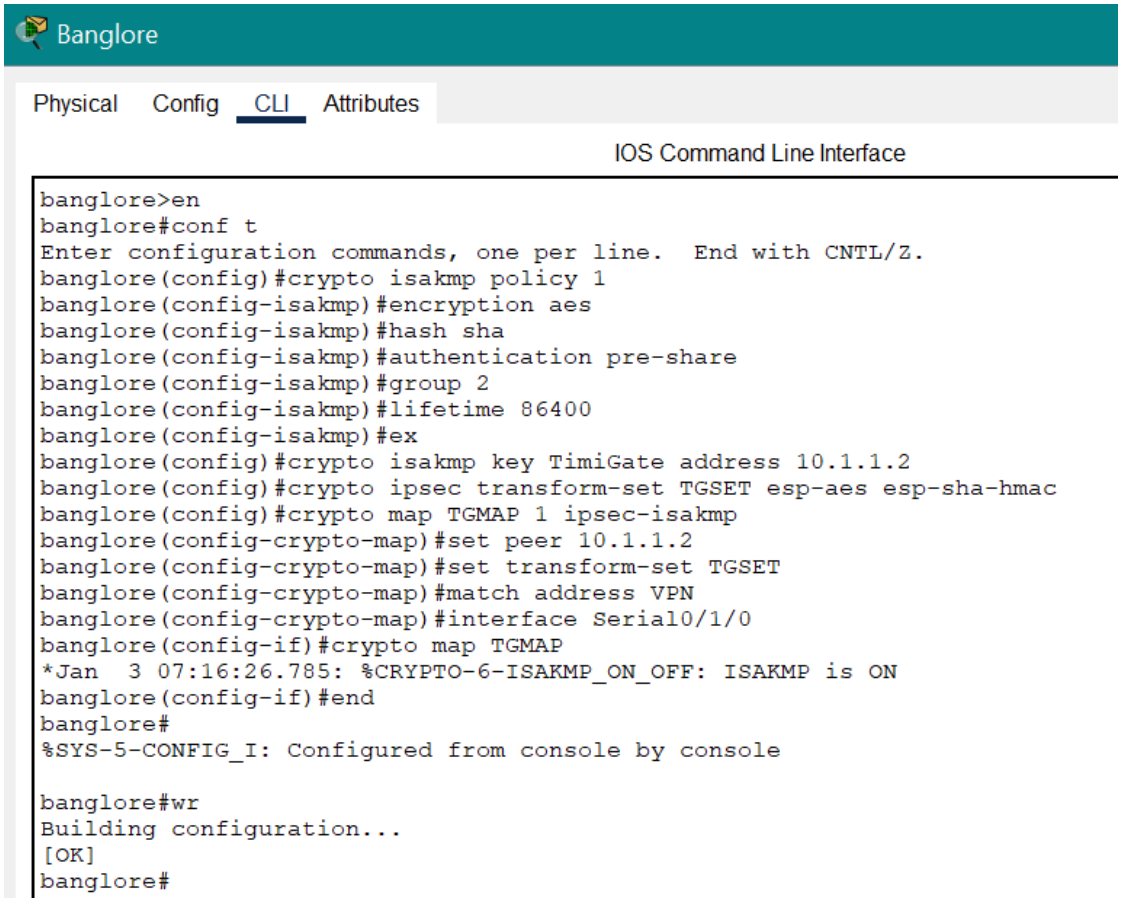


CLI Mode:

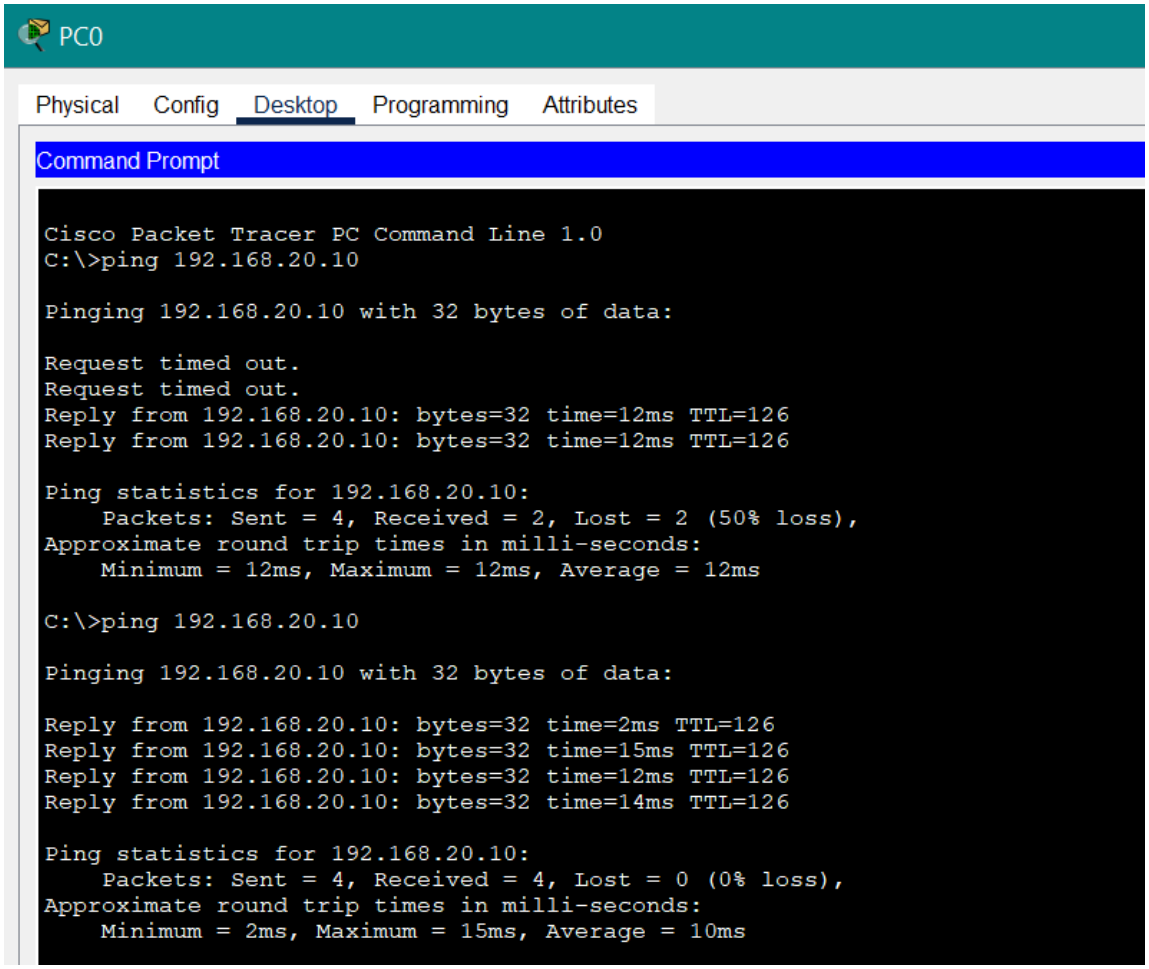
Router (Mumbai):

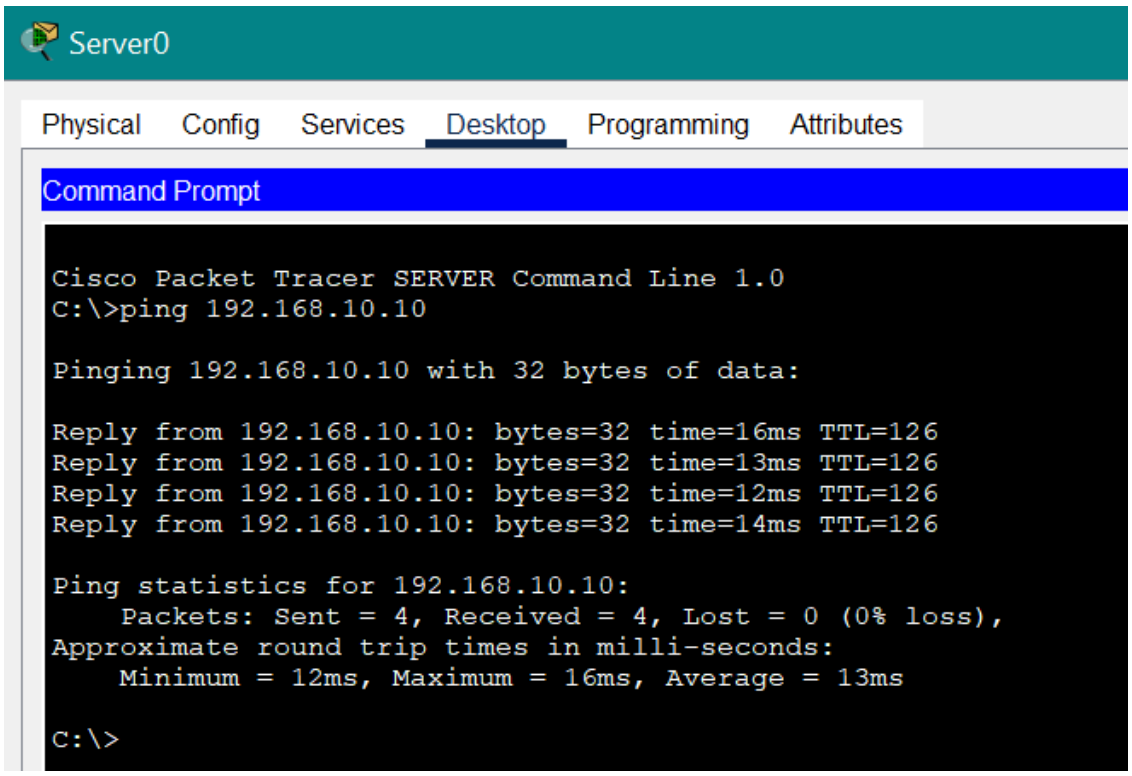


Router (Bangalore):



OUTPUT:


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.10
Pinging 192.168.20.10 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.20.10: bytes=32 time=12ms TTL=126
Reply from 192.168.20.10: bytes=32 time=12ms TTL=126
Ping statistics for 192.168.20.10:
Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
Minimum = 12ms, Maximum = 12ms, Average = 12ms
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=2ms TTL=126
Reply from 192.168.20.10: bytes=32 time=15ms TTL=126
Reply from 192.168.20.10: bytes=32 time=12ms TTL=126
Reply from 192.168.20.10: bytes=32 time=14ms 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 = 15ms, Average = 10ms


Server0
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.10.10
Pinging 192.168.10.10 with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time=16ms TTL=126
Reply from 192.168.10.10: bytes=32 time=13ms TTL=126
Reply from 192.168.10.10: bytes=32 time=12ms TTL=126
Reply from 192.168.10.10: bytes=32 time=14ms TTL=126
Ping statistics for 192.168.10.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 12ms, Maximum = 16ms, Average = 13ms
C:\>

Practical No: 8

Aim – Demonstrate multilayer switch based networking.

Multilayer Switch

- It is a network switching technology that works on **both Layer 2 (Data Link Layer)** and **Layer 3 (Network Layer)** of the OSI model.
- A **multilayer switch** combines the functions of a **switch and a router** in one device.
- It can **forward frames** based on MAC addresses (Layer 2) and **route packets** based on IP addresses (Layer 3).
- Commonly used for **inter-VLAN routing** within large networks.
- Provides **high-speed routing** using hardware instead of software like traditional routers.

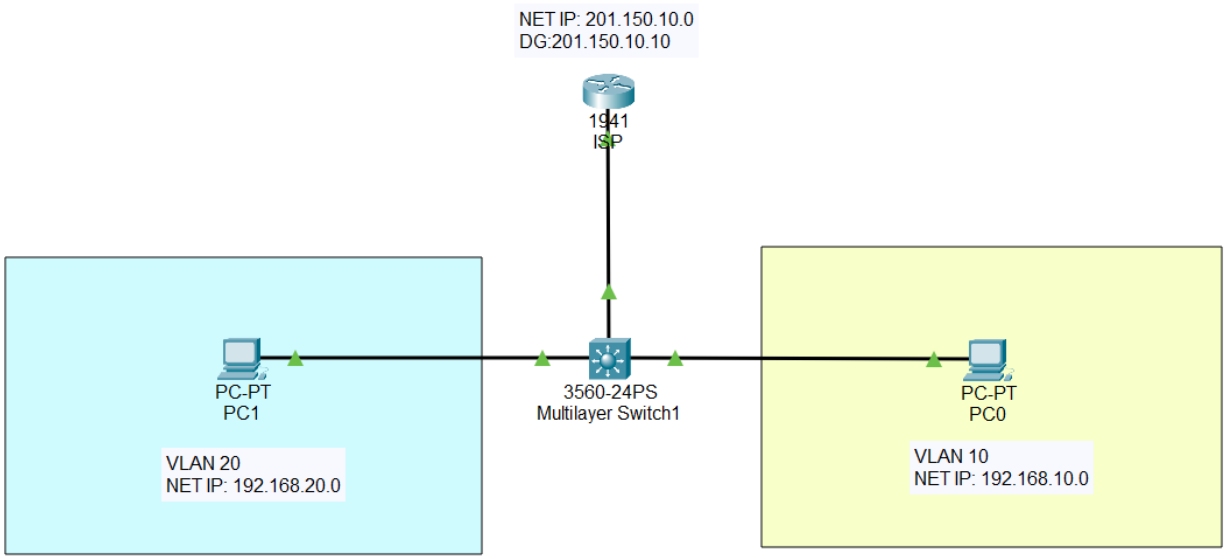
Why We Use It:

- To **increase network speed and performance**.
- To **reduce latency** by handling routing inside the switch.
- To **simplify network design** (no need for separate routers).
- To **enable inter-VLAN communication** efficiently.
- To **improve scalability and traffic management** in enterprise networks.

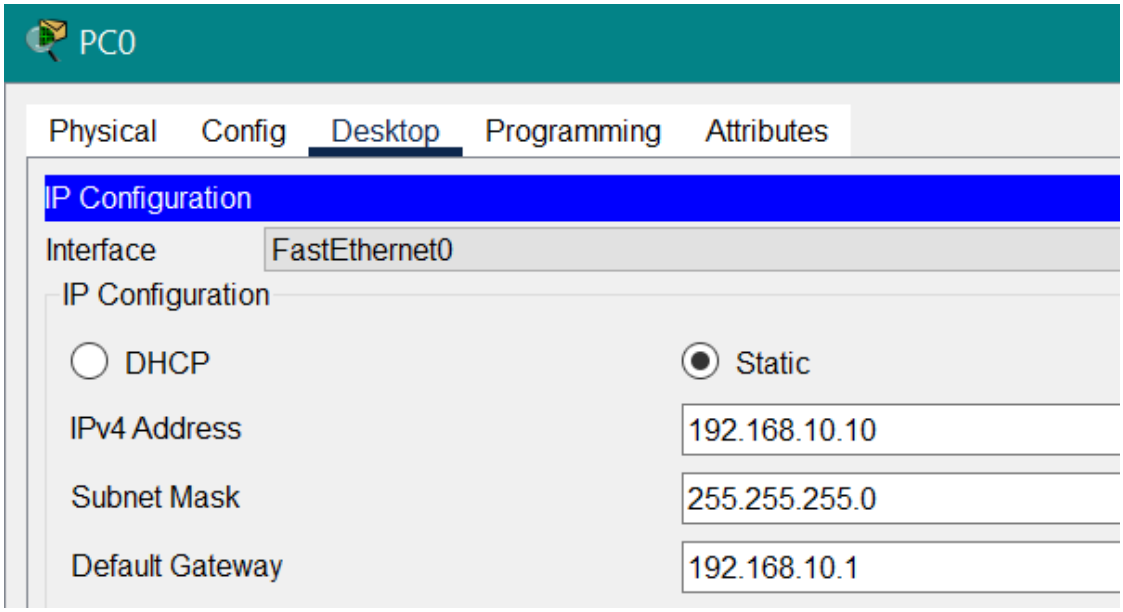
How Multilayer Switching Works in a Network Topology:

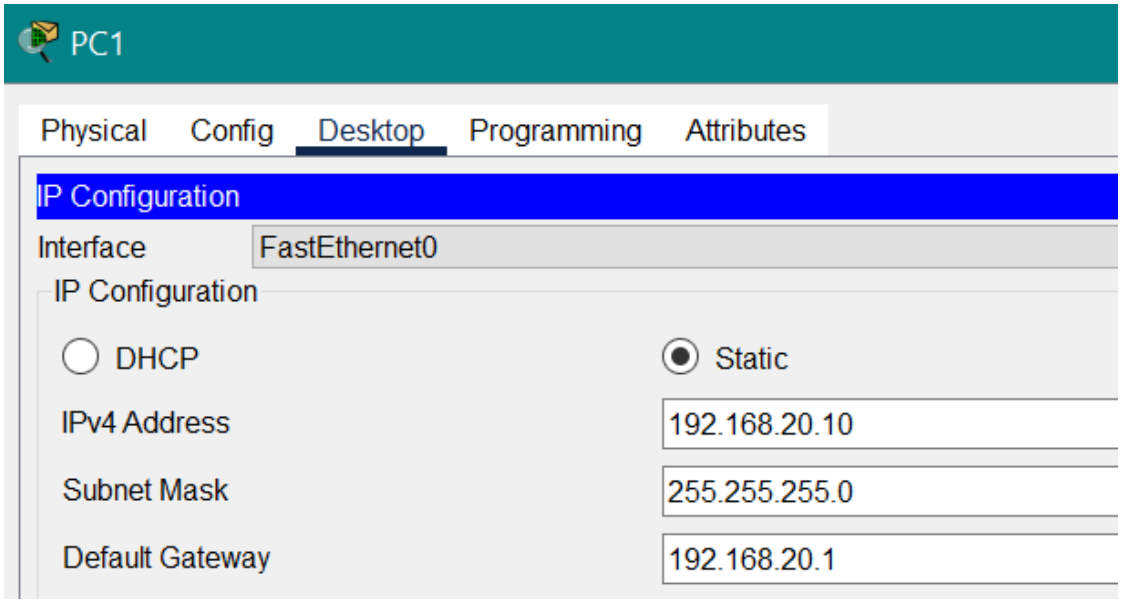
- Works at **Layer 2 and Layer 3** of the OSI model.
- **Switches** data within VLANs using MAC addresses.
- **Routes** data between VLANs using IP addresses.
- Uses **hardware-based routing** for high speed.
- Placed at the **core or distribution layer** of the network.
- Provides **fast inter-VLAN communication** and better performance.

Network Topology

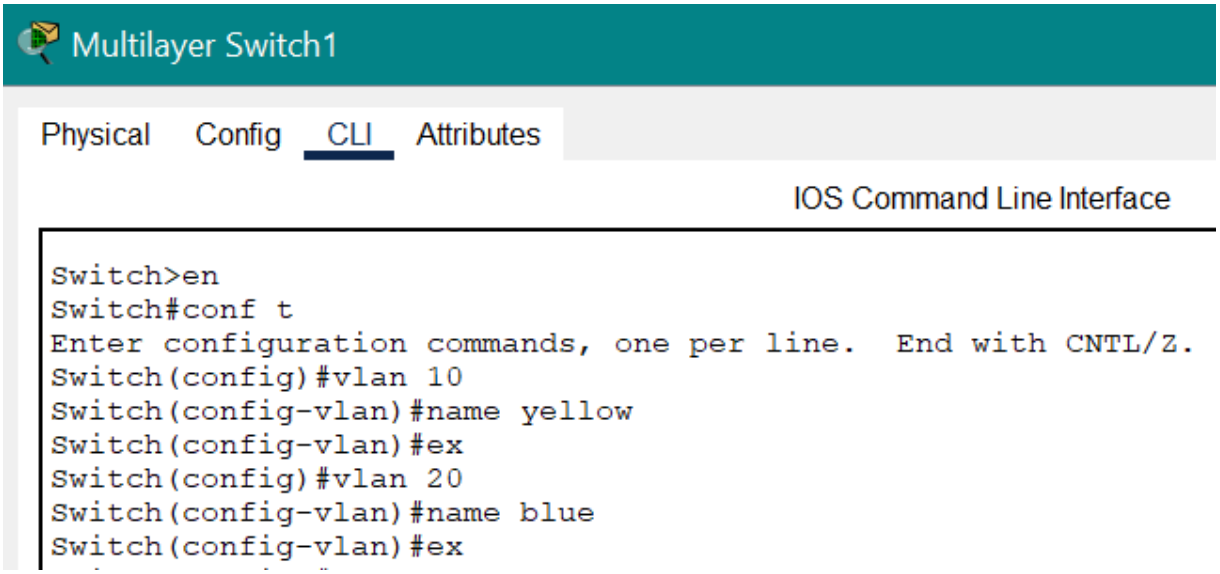


Assigning IP`s as show in topology:





Now to configure both pc on switch, we set up 2 vlan first, namely



Now we will enable switchport access for both the vlan .

```
Switch(config)#int f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#ex
Switch(config)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#ex
```

Now add the ip address of PC to the switch & Enable the routing of multilayer switch

Multilayer Switch1

Physical Config CLI Attributes

IOS Command Line Interface

```
Switch(config)#int vlan 10
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

Switch(config-if)#ip address 192.168.10.1 255.255.255.0
Switch(config-if)#ex
Switch(config)#int vlan 20
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up

Switch(config-if)#ip address 192.168.20.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#ex
Switch(config)#ip routing
```

Lastly add the router's IP address -

Multilayer Switch1

Physical Config CLI Attributes

IOS Command Line Interface

```
Switch(config)#int gig0/1
Switch(config-if)#no switchport
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Switch(config-if)#ip address 201.105.10.101 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#ex
Switch(config)#ip default-gateway 201.105.10.10
```

OUTPUT:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	PC0	ICMP		0.000	N	0	(edit)	
	Successful	PC0	PC1	ICMP		0.000	N	1	(edit)	
	Successful	Multila...	PC0	ICMP		0.000	N	2	(edit)	
	Successful	Multila...	PC1	ICMP		0.000	N	3	(edit)	