Index

Sr No	Practical	Date	Sign
1	Using, linux-terminal or Windows-cmd, execute following networking commands and note the output: ping, traceroute, netstat, arp, ipconfig, Getmac, hostname, NSLookUp, SystemInfo	20/12/23	
2	Using Packet Tracer, create a basic network of two computers using appropriate network wire through Static IP address allocation and verify connectivity	03/01/24	
3	Using Packet Tracer, create a basic network of one server and two computers using appropriate network wire. Use Dynamic IP address allocation and show connectivity	10/01/24	
4	Using Packet Tracer, create a basic network of one server and two computers and two mobile / movable devices using appropriate network wire. And verify the connectivity	24/01/24	
5	Using Packet Tracer, Implement Static Routing, create a network with three routers with and each router associated network will have minimum three PC. Show Connectivity	07/02/24	
6	Using Packet Tracer, Implement RIP, create a network with three routers with and each router associated network will have minimum three PC. Show Connectivity	21/02/24	
7	Using Packet Tracer, create a network and implement Simple Area and MultiArea OSPF. Show Connectivity	28/02/24	
8	Using Packet Tracer, create a network with three routers with BGP and each router associated network will have minimum three PC. Show Connectivity	13/03/24	

Practical No 1

Aim: Using, linux-terminal or Windows-cmd, execute following networking commands and note the output: ping, traceroute, netstat, arp, ipconfig, Getmac, hostname, NSLookUp, SystemInfo

Theory:

1) ping: ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol network. It is available for virtually all operating systems that have networking capability, including most embedded network administration software

2) traceroute: The traceroute command (tracert) is a utility designed for displaying the time it takes for a packet of information to travel between a host system and the final destination system. This command returns a list of the hops that the data packets take along their path along their way to the destination

3) netstat: The netstat provides statistics about all active connections so you that we can find out which computers or networks a PC is connected to
Some of the netstat commands commonly used are
i) netstat -in command
This netstat function shows the state of all configured interfaces.

ii) netstat -a command
The netstat -a command shows the state of all sockets.

iii) netstat -s
The netstat -s command shows statistics for each protocol (while the netstat -p command shows the statistics for the specified protocol).

4) arp: The ARP (Address Resolution Protocol) commands are used to view, display, or modify the details/information in an ARP table/cache.
Some of the common arp commands are as follows
i) arp -a: This command is used to display the ARP table for a particular IP address. It also shows all the entries of the ARP cache or table.

5) ipconfig: ipconfig (Internet Protocol CONFIGuration) is used to display and manage the IP address assigned to the machine. In Windows, typing ipconfig without any parameters displays the computer's currently assigned IP, subnet mask and default gateway addresses.

6) getmac: Getmac is a Windows command used to display the Media Access Control (MAC) addresses for each network adapter in the computer.

7) hostname: A hostname is a label that is assigned to a device connected to a computer network and it is used to identify the device.

8) NSlookUp: Using this command we can find the corresponding IP address or domain name system record. The user can also enter a command for it to do a reverse DNS lookup and find the host name for an IP address that is specified.

9) SystemInfo: This command is use to display detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties

Commands

1. ping google.com
2. tracert google.com
3. netstat -in
   netstat -a
   netstat -s
4. arp -a
5. ipconfig
6. getmac
7. hostname
8. nslookup google.com
9. systeminfo

Short Explanation \\for viva

1. ping google.com: Checks connectivity to Google's servers.
2. tracert google.com: Traces the route packets take to reach Google's servers.
3. netstat -in: Displays network interfaces and their statistics.
   netstat -a: Shows all active network connections.
   netstat -s: Provides network statistics, such as packet counts.
4. arp -a: Displays the ARP (Address Resolution Protocol) cache.
5. ipconfig: Shows IP configuration details for the system.
6. getmac: Retrieves the MAC (Media Access Control) addresses of network adapters.
7. hostname: Displays the computer's hostname.
8. nslookup google.com: Resolves and displays the IP address of Google's domain.
9. systeminfo: Provides detailed information about the system.

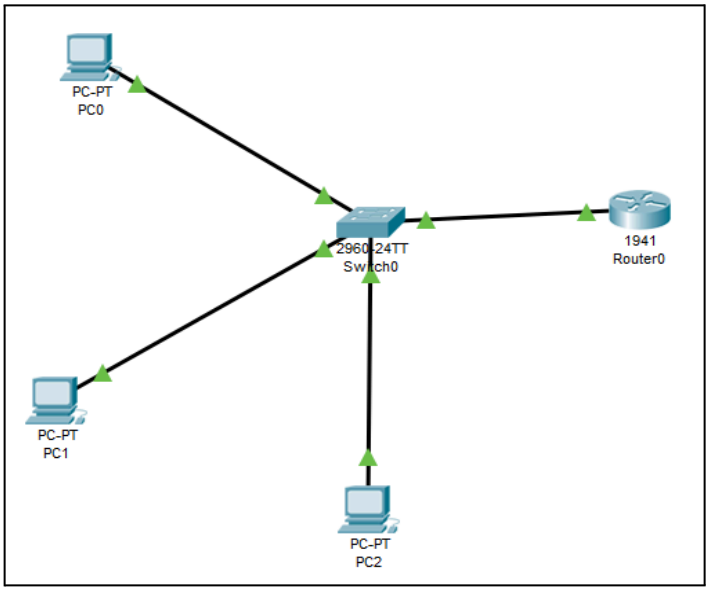
These commands are commonly used for network troubleshooting and system information gathering.

Practical No 2

Aim: Using Packet Tracer, create a basic network of two computers using appropriate network wire through Static IP address allocation and verify connectivity

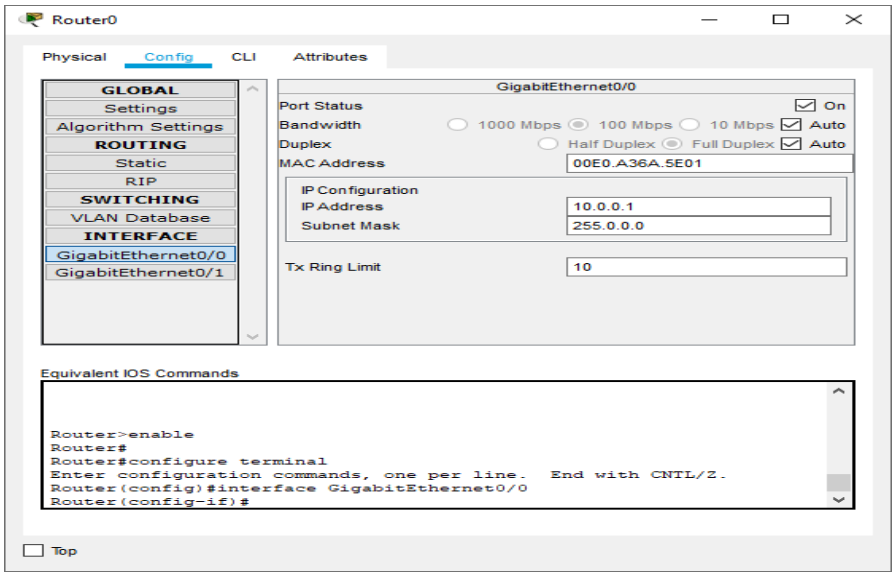
Theory:

We use the following network to verify the connectivity using Cisco packet tracer

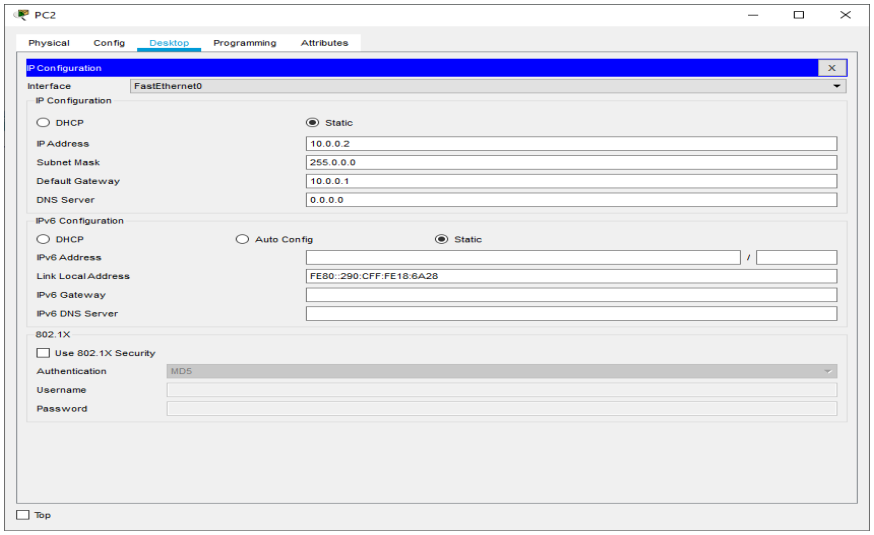


Name	IP ADDRESS	DEFAULT GATEWAY
PC0	10.0.0.4	10.0.0.1
PC1	10.0.0.3	10.0.0.1
PC2	10.0.0.2	10.0.0.1
Router0	GigabitEthernet 0/0 =>10.0.0.1	

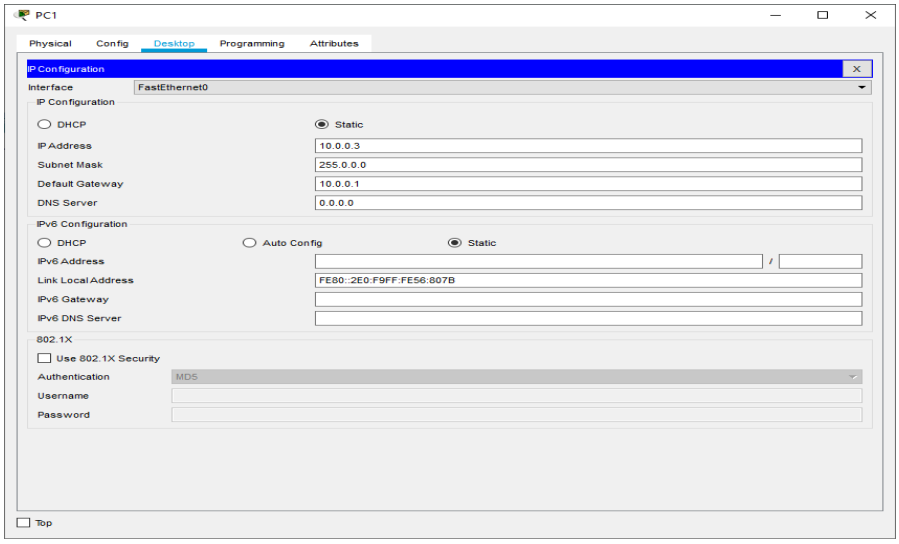
Configure the Router 0:



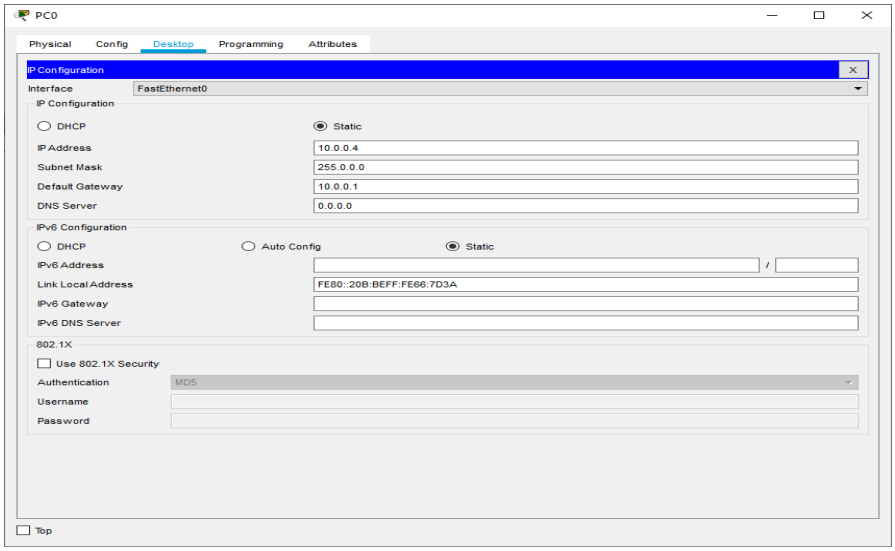
Configure PC2:



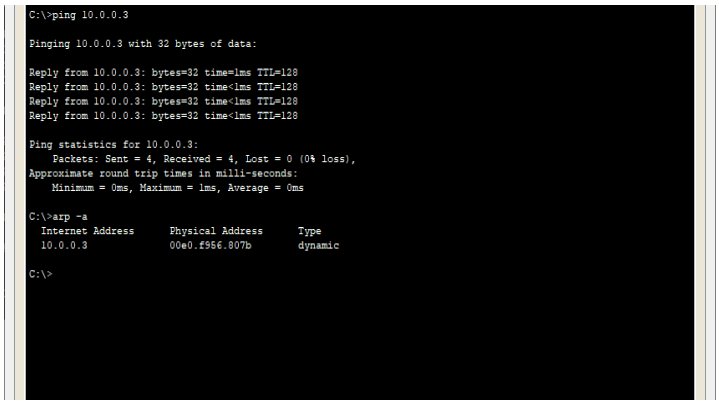
Configure PC1:



Configure PC0:



Next, we type the commands in PC0 ping 10.0.0.3



Practical No 3

Aim: Using Packet Tracer, create a basic network of one server and two computers using appropriate network wire. Use Dynamic IP address allocation and show connectivity

Theory:

For assigning ip addresses dynamically we use the DHCP protocol

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

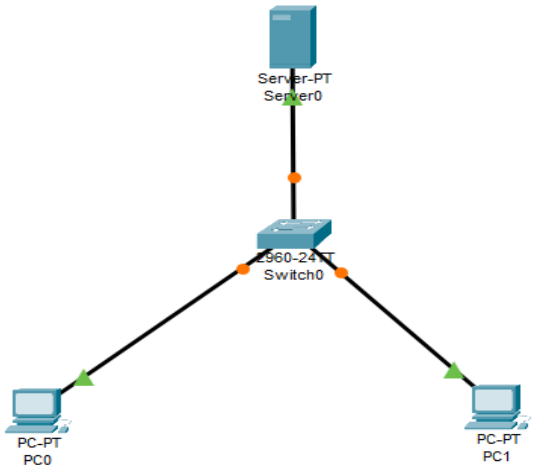
The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it starts up on the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.

DHCP provides the following benefits.

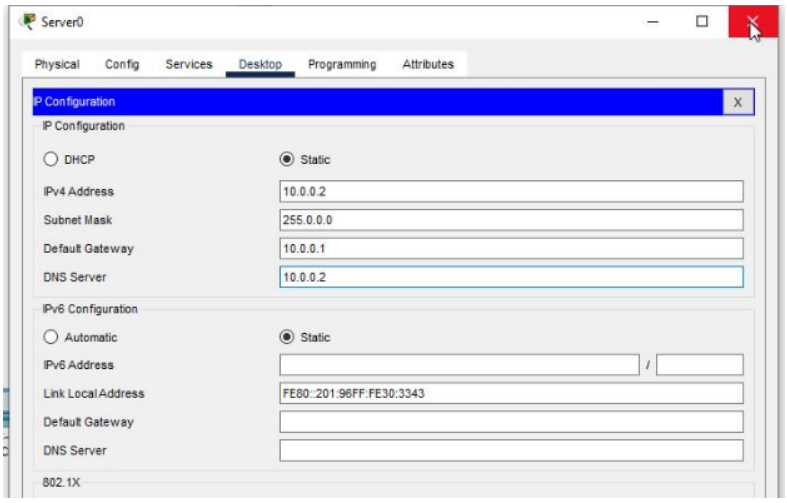
1) Reliable IP address configuration. DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.
2) Reduced network administration. DHCP includes the following features to reduce network administration

   DHCP runs at the application layer of the Transmission Control Protocol/IP (TCP/IP) stack to dynamically assign IP addresses to DHCP clients and to allocate TCP/IP configuration information to DHCP clients. This includes subnet mask information, default gateway IP addresses and domain name system (DNS) addresses.

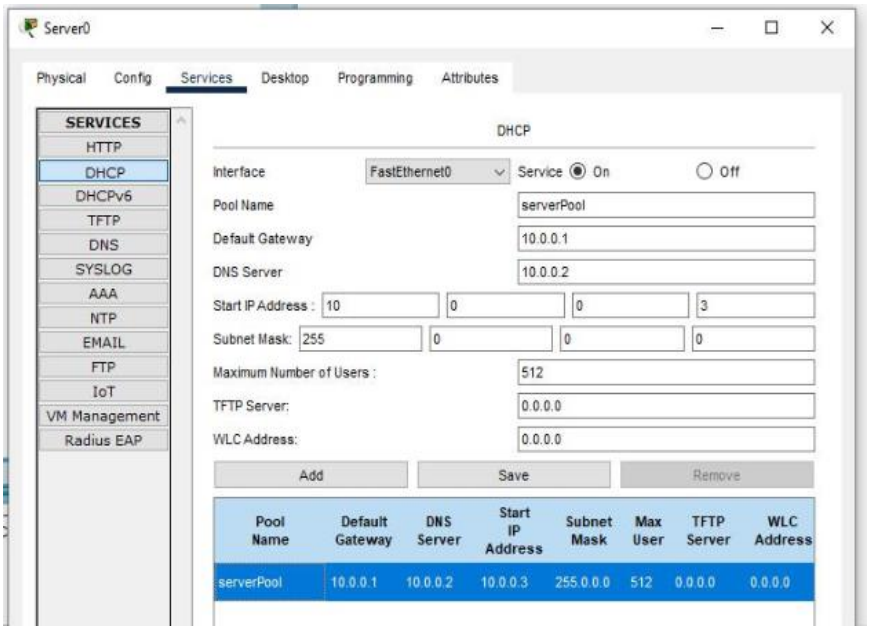
We use the following topology for the present case



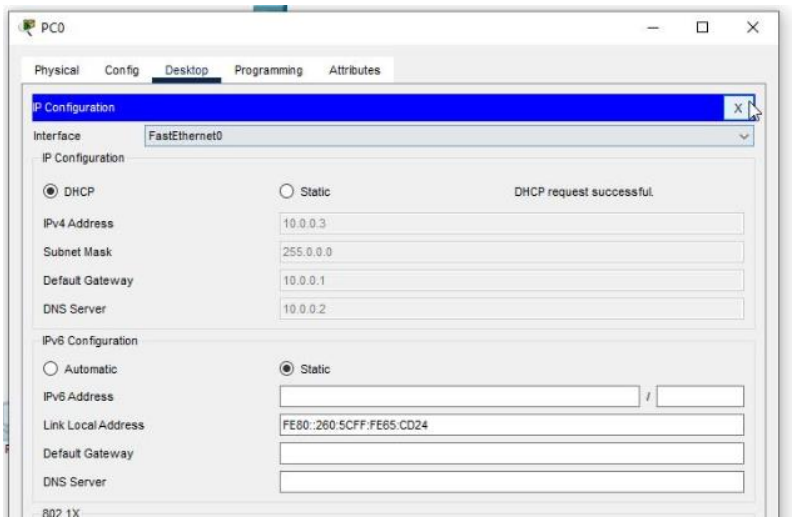
Configuring the Server:

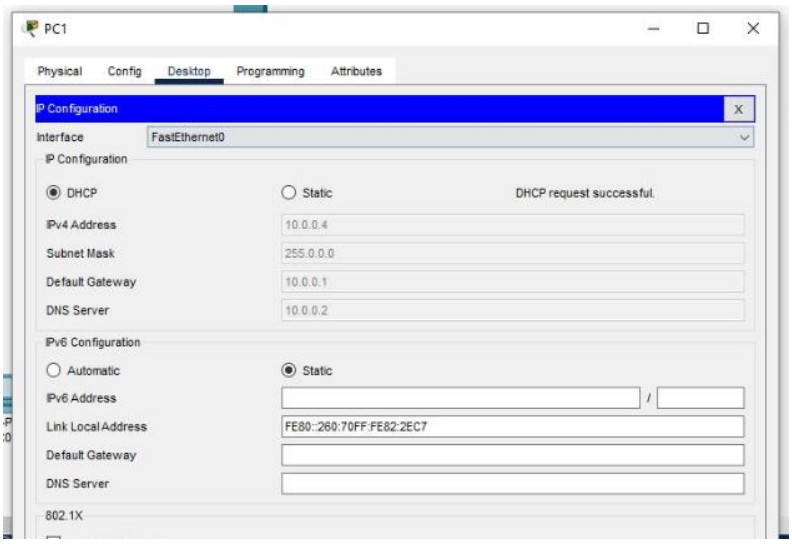


Enabling and setting the DHCP Service on the Server:

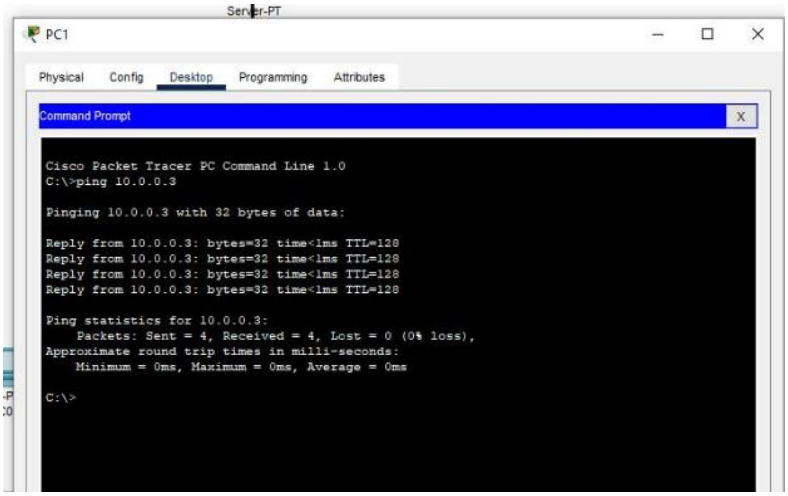


Verifying the Dynamic Addressing on both the PCs:





Checking the connectivity:



Result:

Hence the Connectivity between the PCs has been verified.

Link for the video demonstration of the practical:

https://youtu.be/Jnj8c_15AiE

Practical No 4

Aim: Using Packet Tracer, create a basic network of one server and two computers and two mobile / movable devices using appropriate network wire. And verify the connectivity

Theory:

A Wireless Access Point (WAP) is a networking device that allows wireless-capable devices to connect to a wired network. Instead of using wires and cables to connect every computer or device in the network, installing WAPs is a more convenient, more secure, and cost-efficient alternative.

Setting up a wireless network provides a lot of advantages and benefits for you and your small business.

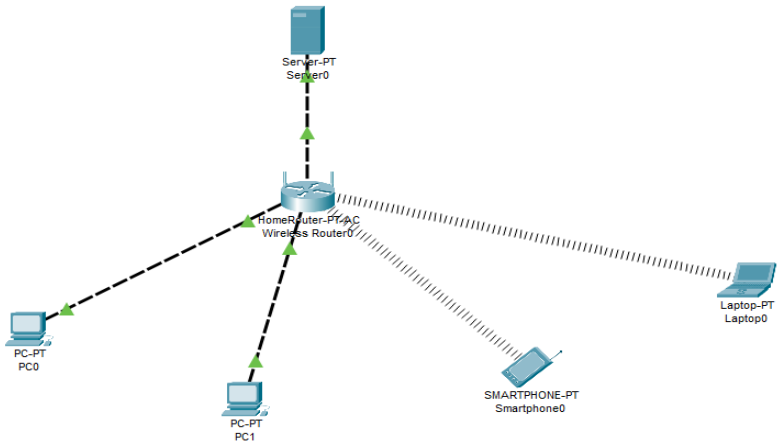
1) It is easier to set up compared to setting up a wired network.
2) It is more convenient to access.
3) It is less complicated to add new users in the network.
4) It gives users more flexibility to stay online even when moving from one area in the office to another.
5) Guest users can have Internet access by just using a password.
6) Wireless network protection can be set up even if the network is visible to the public by configuring maximum wireless security.
7) Segmentation of users, such as guests and employees, is possible by creating Virtual Local Area Networks (VLANs) to protect your network resources and assets.

There are different purposes of setting up a wireless network using a WAP.

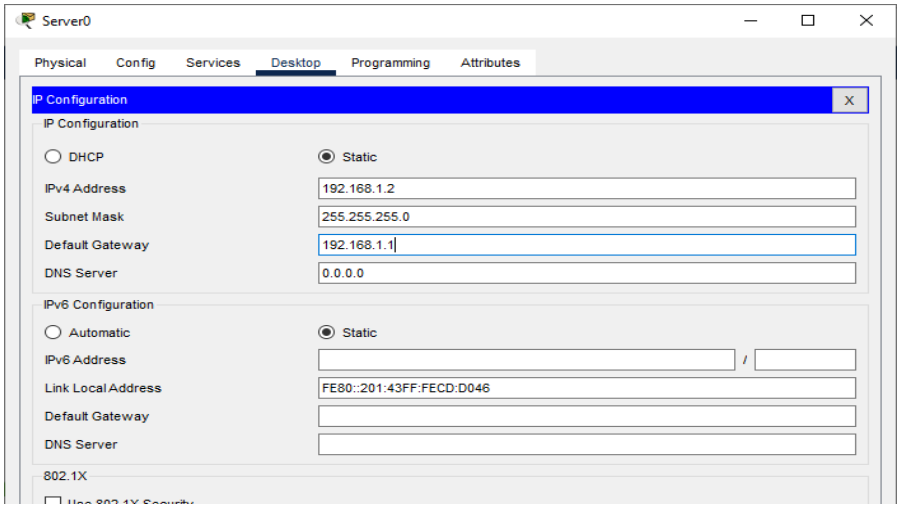
With a WAP, the following can be done:

1) Create a wireless network within your existing wired network.
2) Extend the signal range and strength of your wireless network to provide complete wireless coverage and get rid of dead spots especially in larger office spaces or buildings.
3) Accommodate wireless devices within a wired network.
4) Configure the settings of your wireless access points in one device.

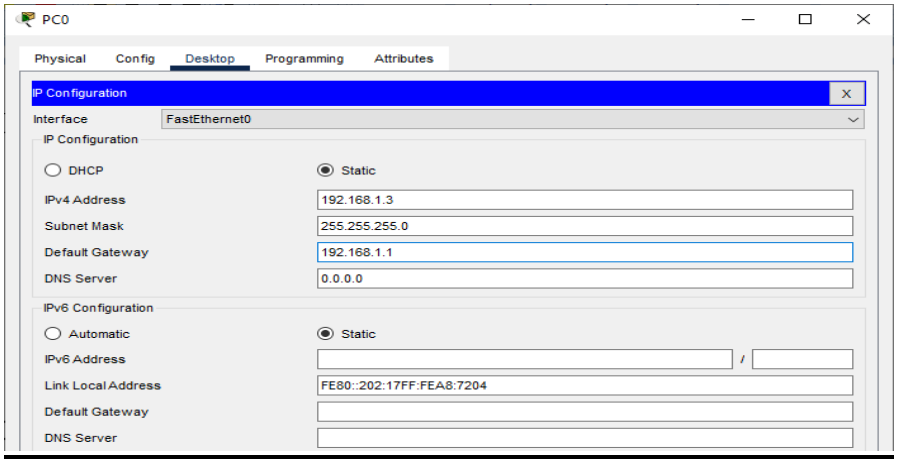
For the present case we use the following topology



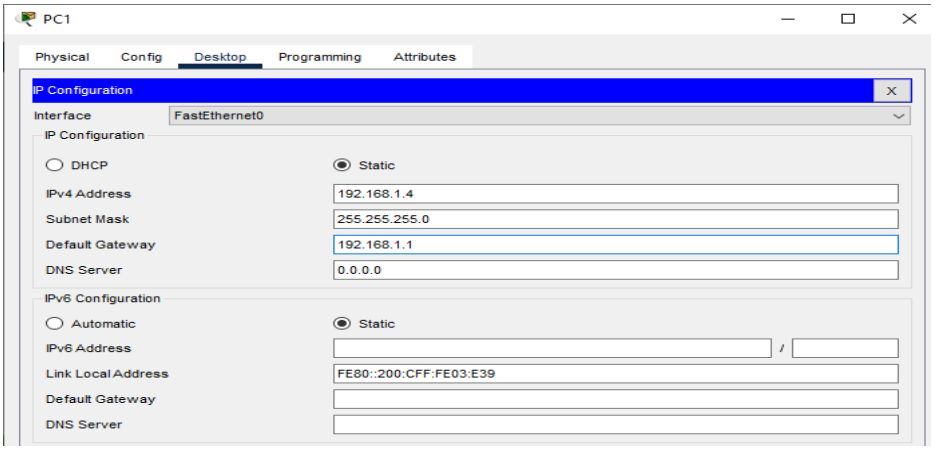
Configure the Server:



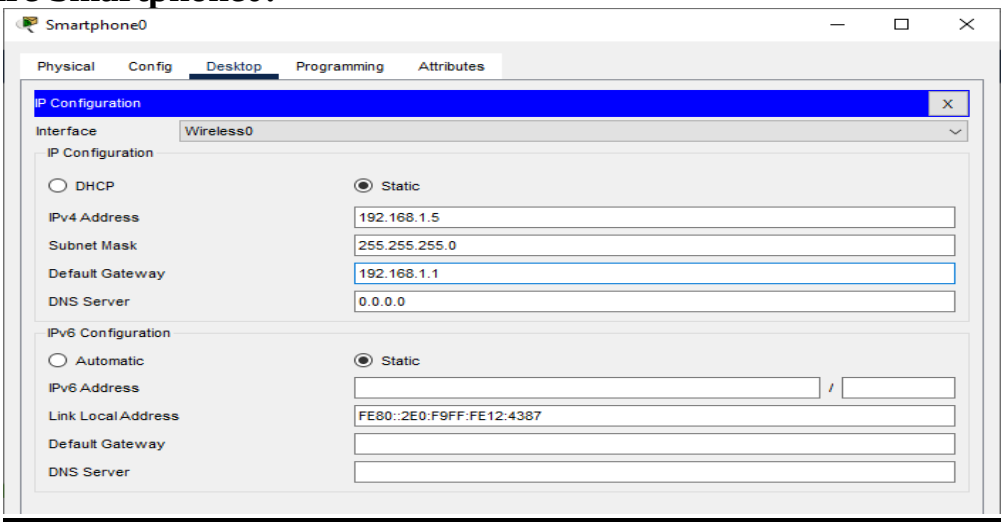
Configure PC0:



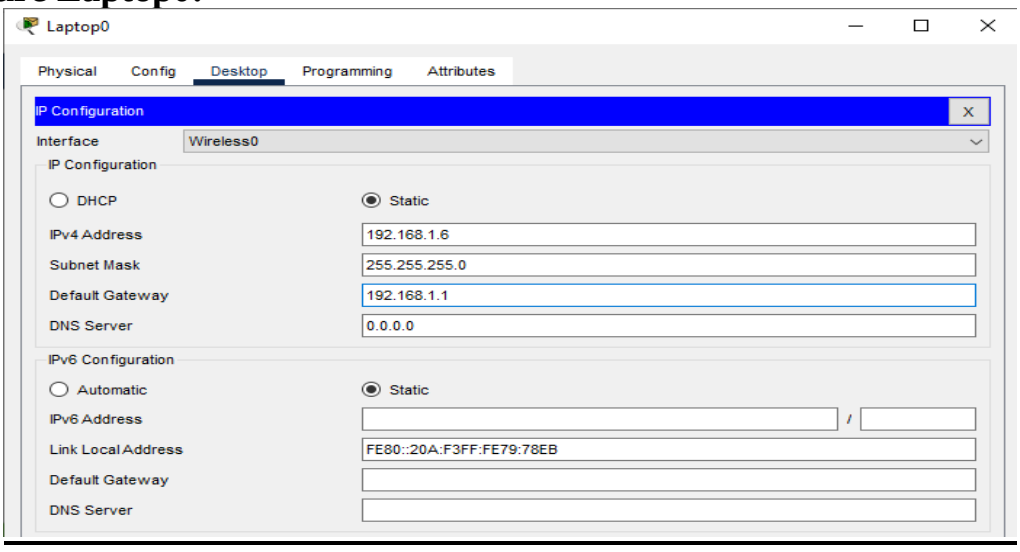
Configure PC1:



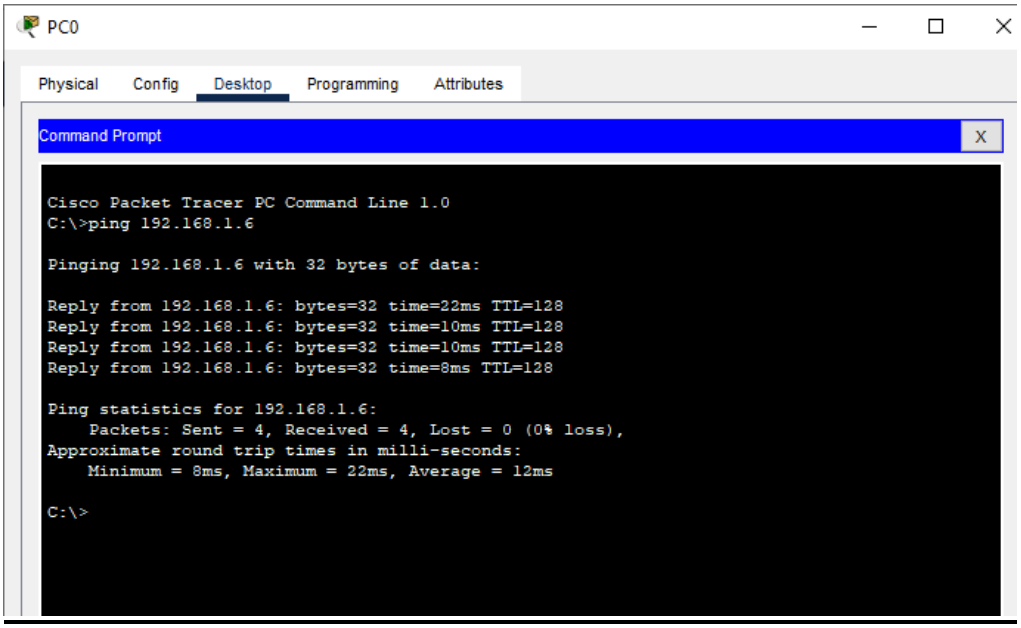
Configure Smartphone0:



Configure Laptop0:



Checking the connectivity (pinging laptop0 from PC0):



Similarly the ping message can be checked for all the devices

Result:

Hence the Connectivity of the network has been verified.

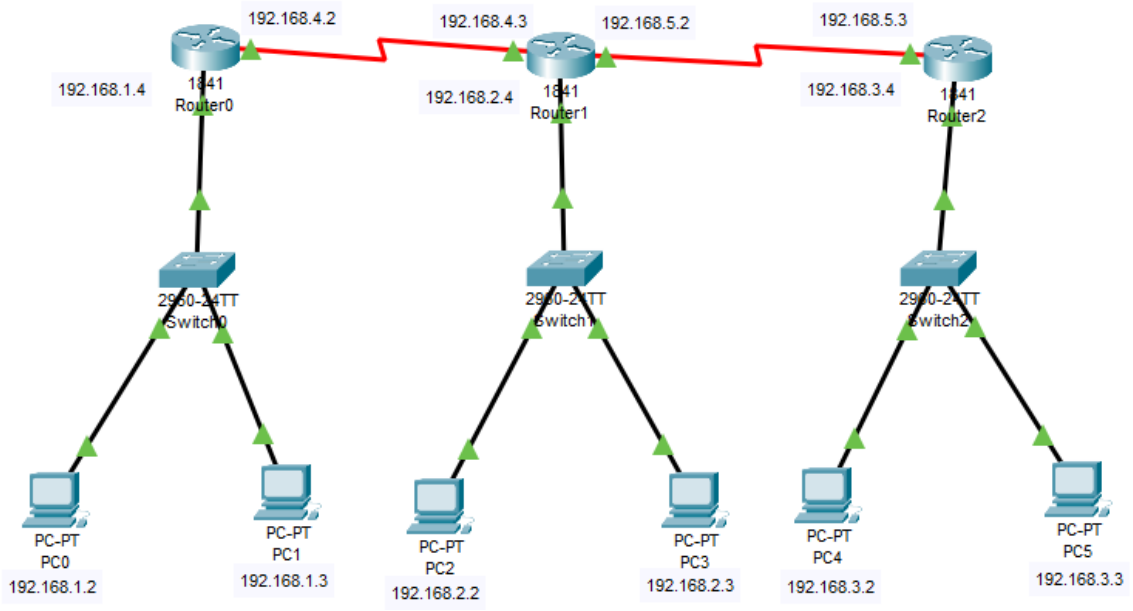
Link for the video demonstration of the practical:

https://youtu.be/zvBKvkY8-nA

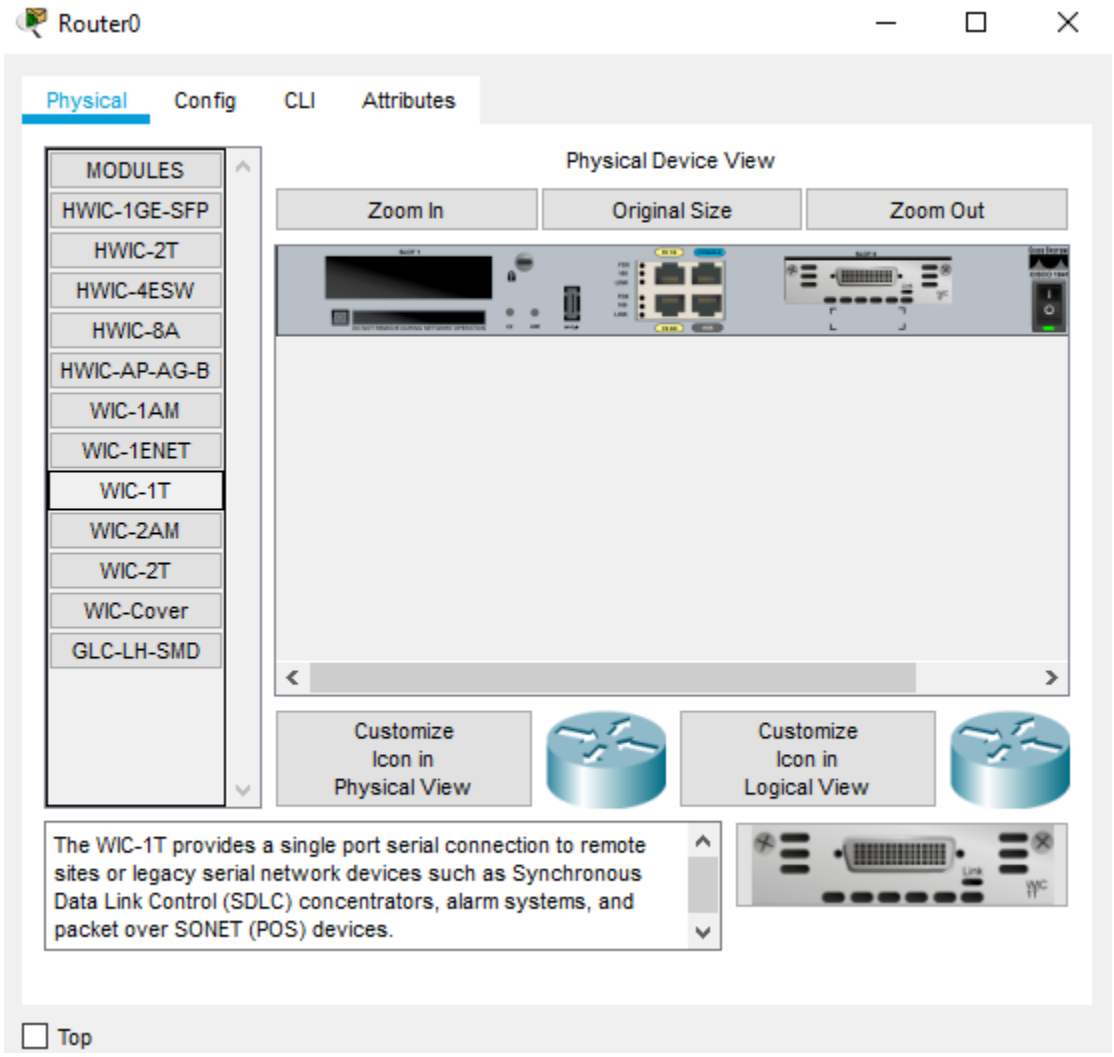
Practical 4

Configure Static Routing

Topology:

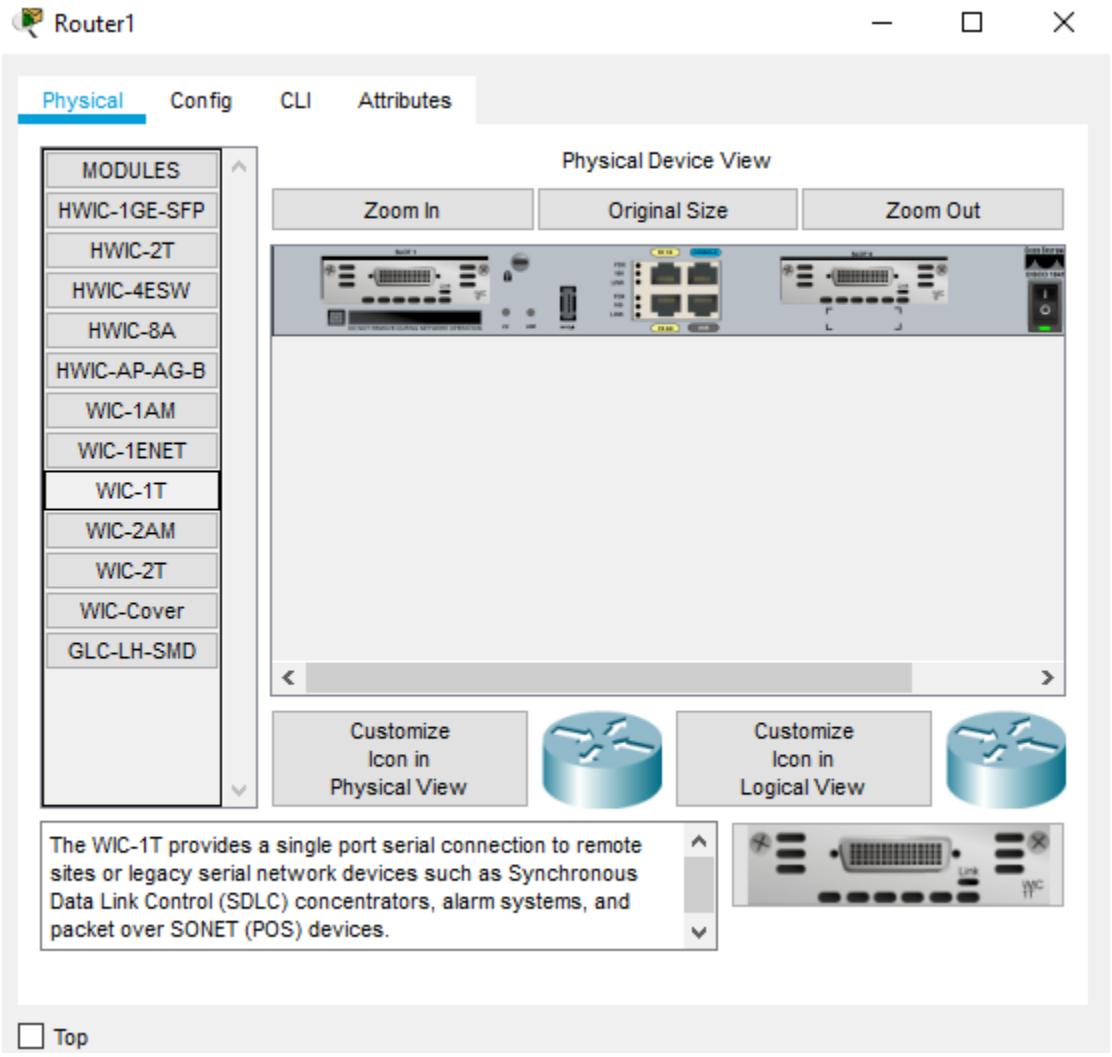


In Router 0
Switch it off
Add one port of WIC-1T
And Switch it on

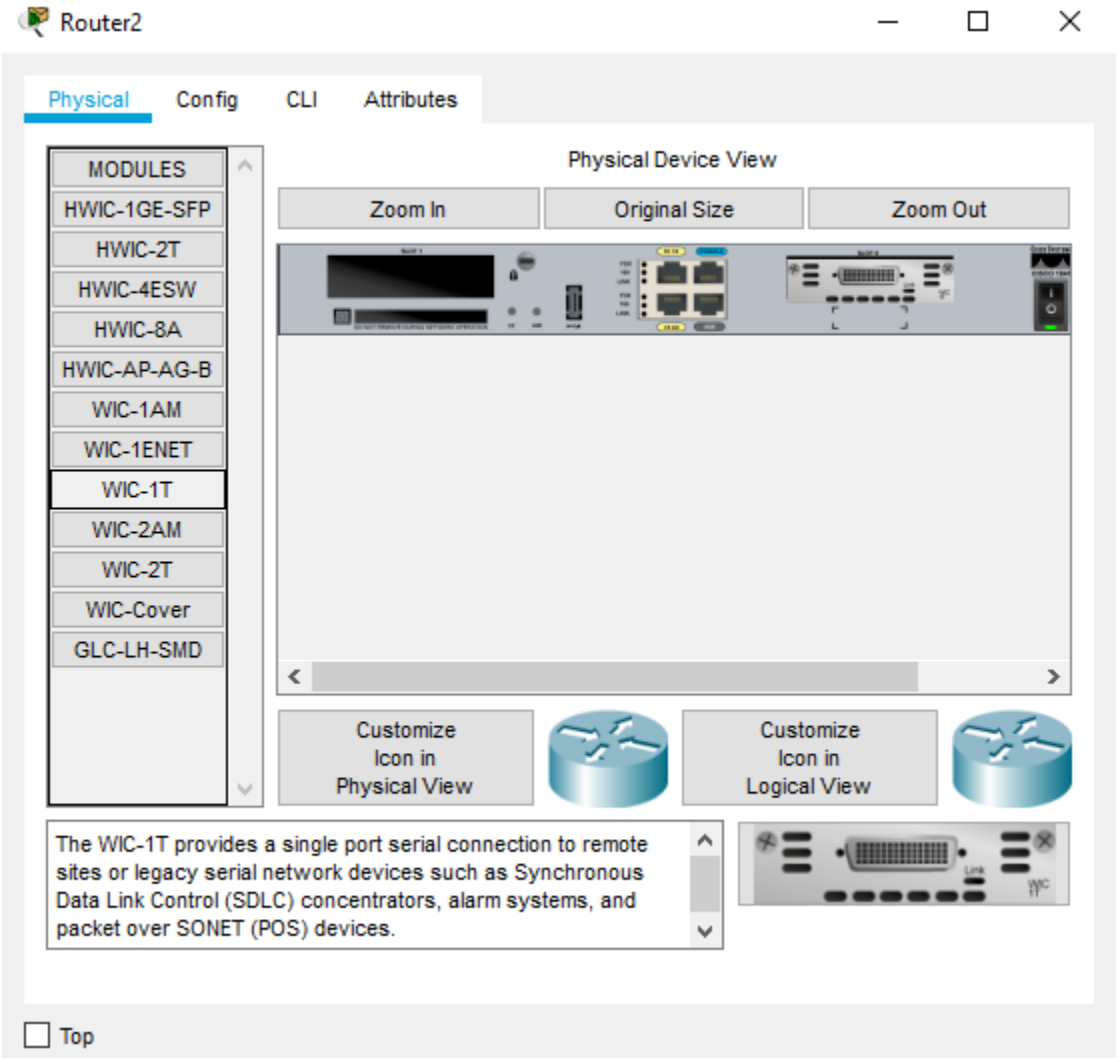


Adding Extra ports to the Routers

In Router 1
Switch it off
Add two port of WIC-1T
And Switch it on



In Router 2
Switch it off
Add one port of WIC-1T
And Switch it on



Configuration

PC No.	IP Address	Default Gateway
PC0	192.168.1.2	192.168.1.4
PC1	192.168.1.3	192.168.1.4
PC2	192.168.2.2	192.168.2.4
PC3	192.168.2.3	192.168.2.4
PC4	192.168.3.2	192.168.3.4
PC5	192.168.3.3	192.168.3.4

Router

Router Number	Port No.	IP Address
Router0	Fa0/0	192.168.1.4
	Se0/0/0	192.168.4.2
Router1	Fa0/0	192.168.2.4
	Se0/0/0	192.168.4.3
	Se0/1/0	192.168.5.2
Router2	Fa0/0	192.168.3.4
	Se0/0/0	192.168.5.3

Static Routing Configuration

Router0

Network	Subnet Mask	Next Hop
192.168.2.0	255.255.255.0	192.168.4.3
192.168.3.0	255.255.255.0	192.168.4.3
192.168.5.0	255.255.255.0	192.168.4.3

Router1

Network	Subnet Mask	Next Hop
192.168.1.0	255.255.255.0	192.168.4.2
192.168.3.0	255.255.255.0	192.168.5.3
192.168.4.0	255.255.255.0	192.168.4.2
192.168.5.0	255.255.255.0	192.168.5.3

Router2

Network	Subnet Mask	Next Hop
192.168.2.0	255.255.255.0	192.168.5.2
192.168.1.0	255.255.255.0	192.168.5.2
192.168.4.0	255.255.255.0	192.168.5.2

Output

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC0	PC5	ICMP		0.000	N	0

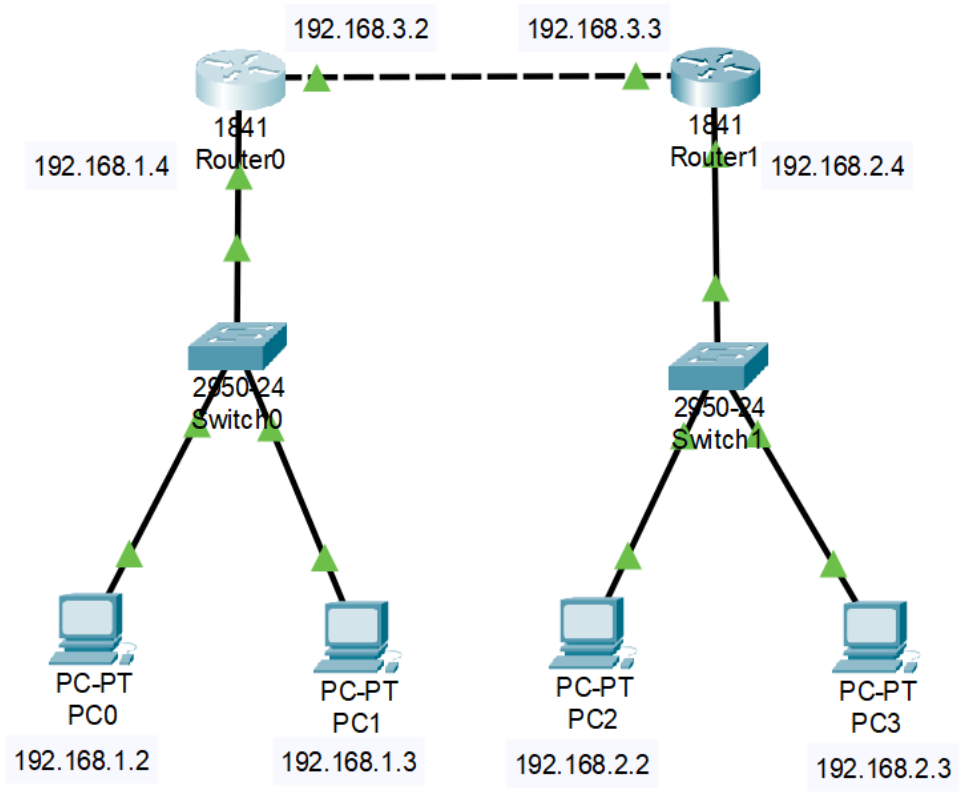
Practical 5

Configuring IP Routing using RIP

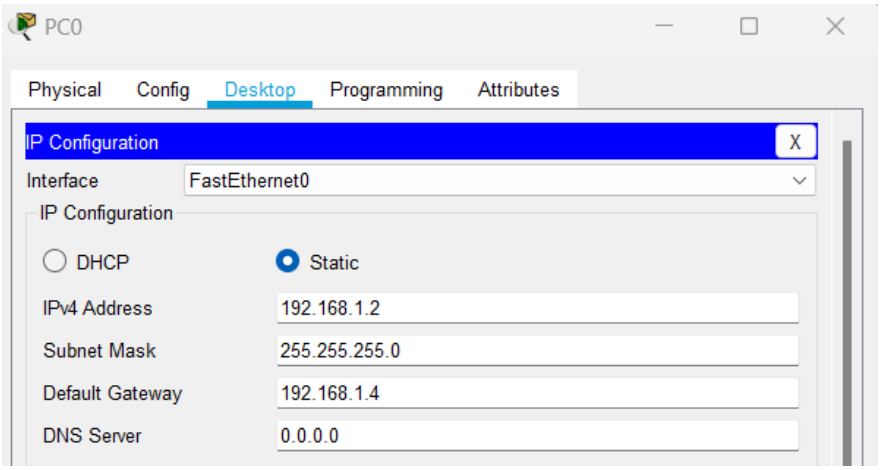
Routing Information Protocol (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network.

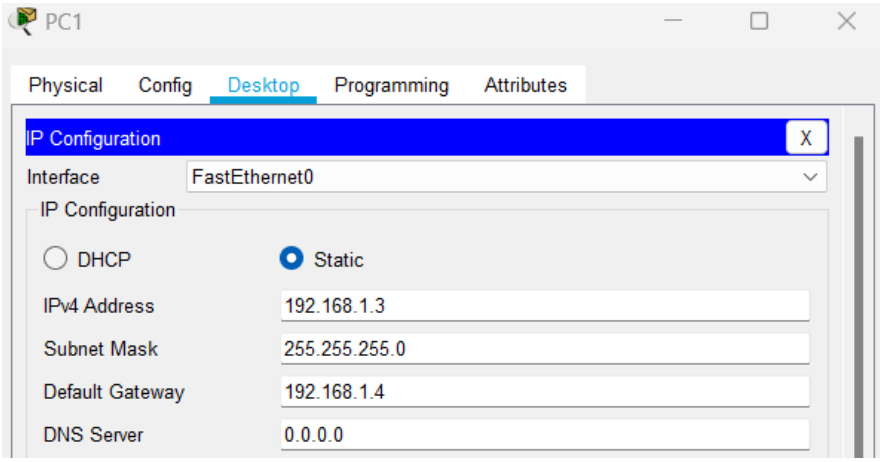
Aim: To Configure IP Rounting using RIP

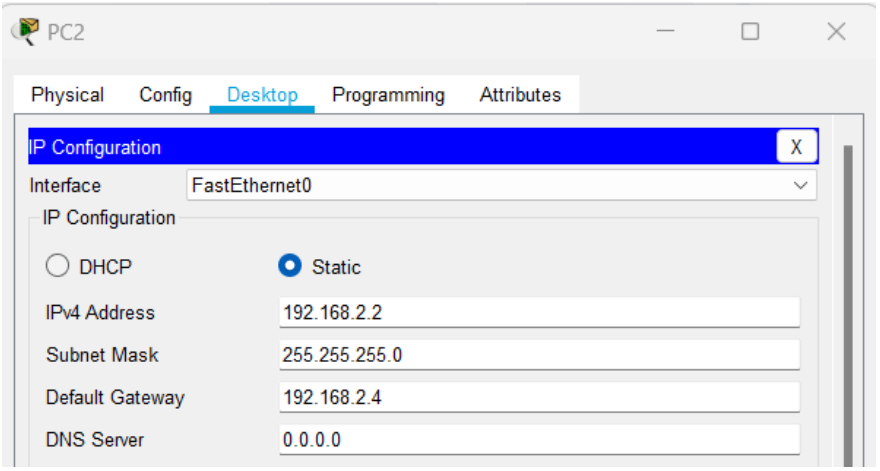
Topology:

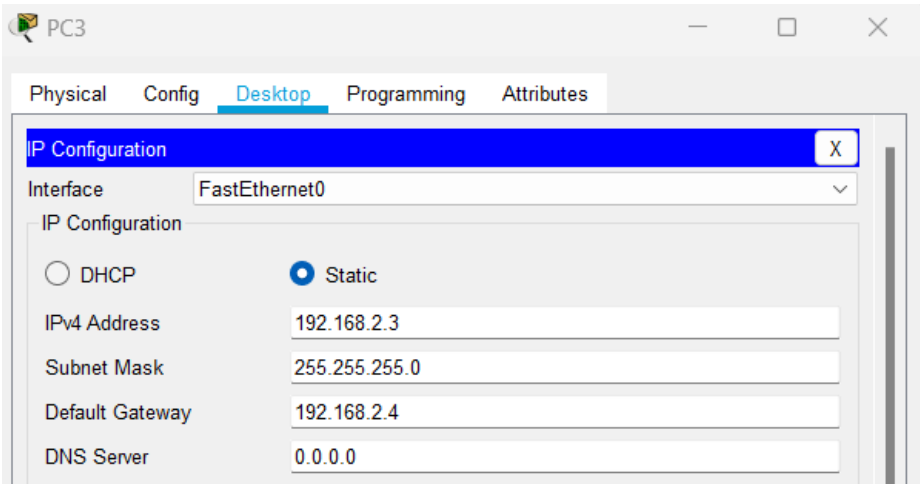


Configuration:
Configuration of PC0, PC1, PC2, PC3


PC0
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
192.168.1.4
DNS Server
0.0.0.0


PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.4
DNS Server
0.0.0.0


PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.2.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.4
DNS Server
0.0.0.0



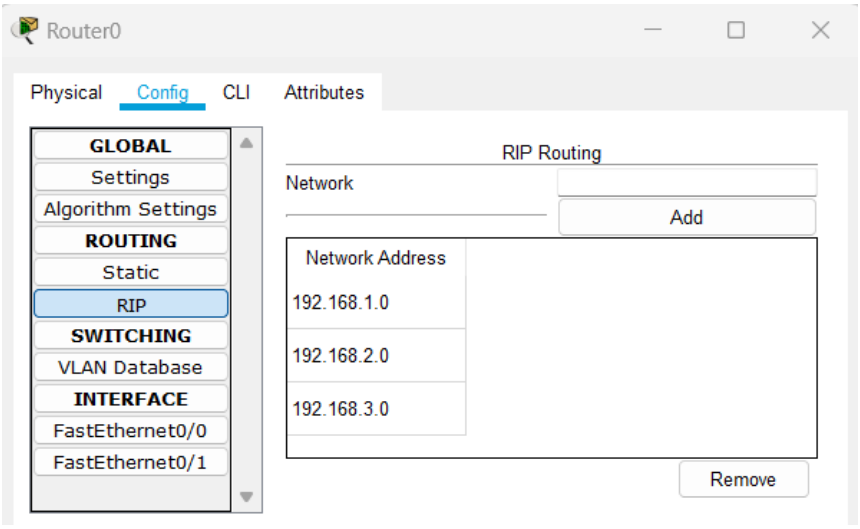
Configuration of Router 0

FastEthernet0/0	192.168.1.4
FastEthernet0/1	192.168.3.2

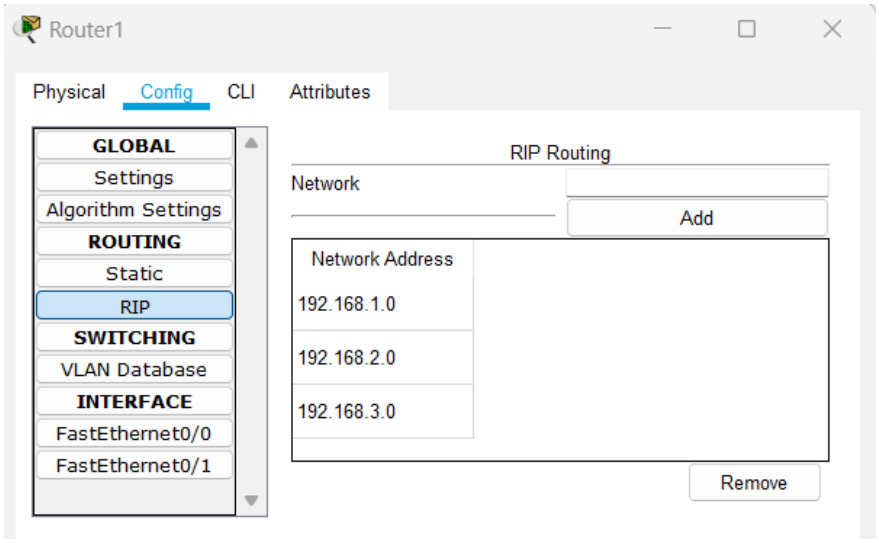
Configuration of Router 1

FastEthernet0/0	192.168.2.4
FastEthernet0/1	192.168.3.3

Configuration of RIP in Router 0



Configuration of RIP in Router 1

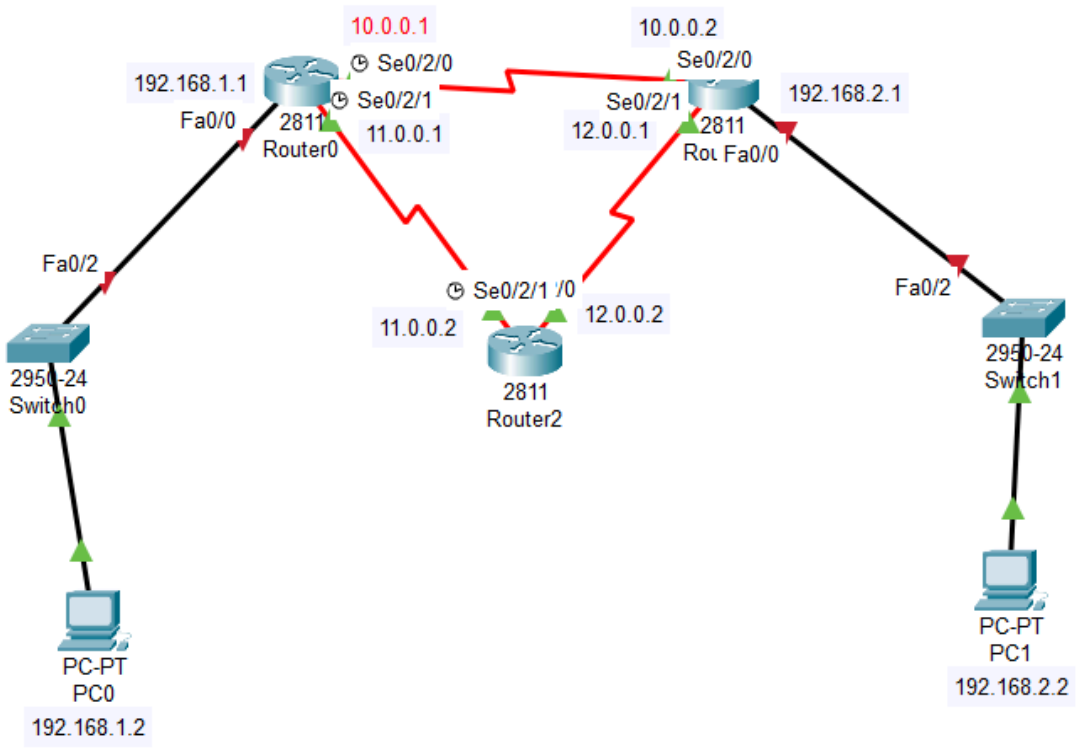


Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	PC3	ICMP		0.000	N	0	(edit)	

Configure simple and multi area ospf

Simple OSPF

Topology



PC Configuration:

PC Name	Ip Address	Default Gateway
PC0	192.168.1.2	192.168.1.1
PC1	192.168.2.2	192.168.2.1

Router 0

FastEthernet0/0	192.168.1.1
Se0/2/0	10.0.0.1
Se0/2/1	11.0.0.1

Router 2

Se0/2/0	12.0.0.2
Se0/2/1	11.0.0.2

Router 1

FastEthernet0/0	192.168.2.1
Se0/2/0	10.0.0.2
Se0/2/1	12.0.0.1

Ospf Configuration
Router 0
enable
conf t
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
network 11.0.0.0 0.255.255.255 area 0
network 192.168.1.0 0.0.0.255 area 0
end
wr

Router 1
router ospf 2
network 10.0.0.0 0.255.255.255 area 0
network 12.0.0.0 0.255.255.255 area 0
network 192.168.2.0 0.0.0.255 area 0

Router 2

router ospf 3
network 11.0.0.0 0.255.255.255 area 0
network 12.0.0.0 0.255.255.255 area 0

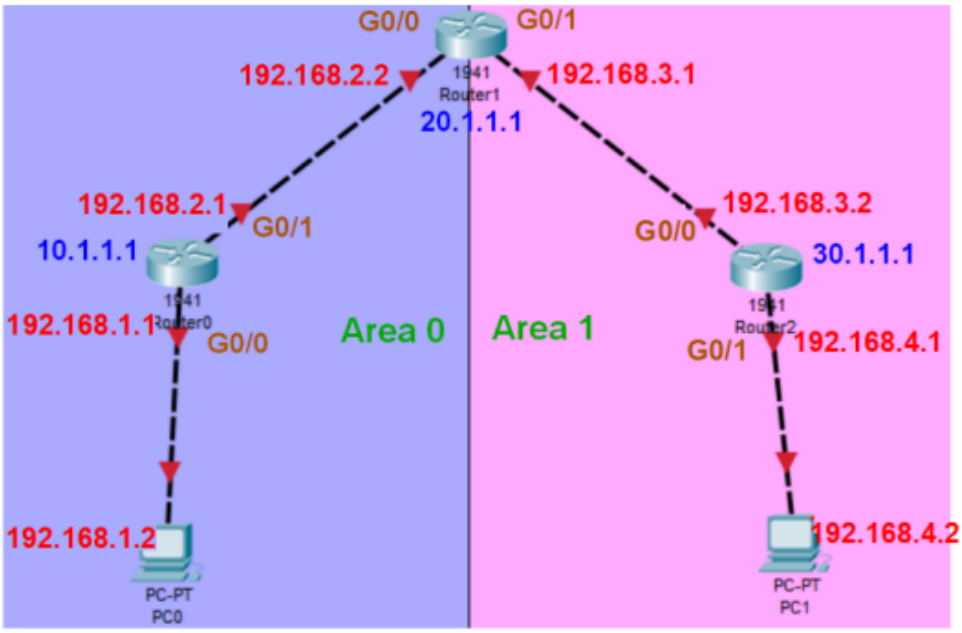
Router 0
sh ip route

pc0 command prompt
ping 192.168.2.2

pc1 command prompt
ping 192.168.1.2

Part b) Multi-area OSPF

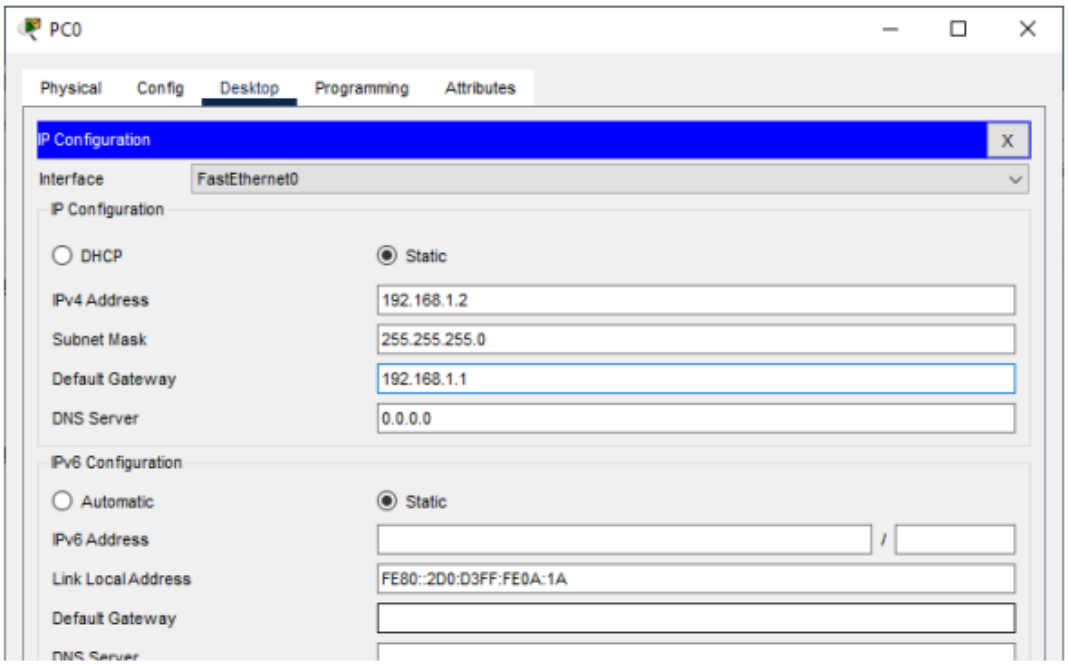
Consider the following topology



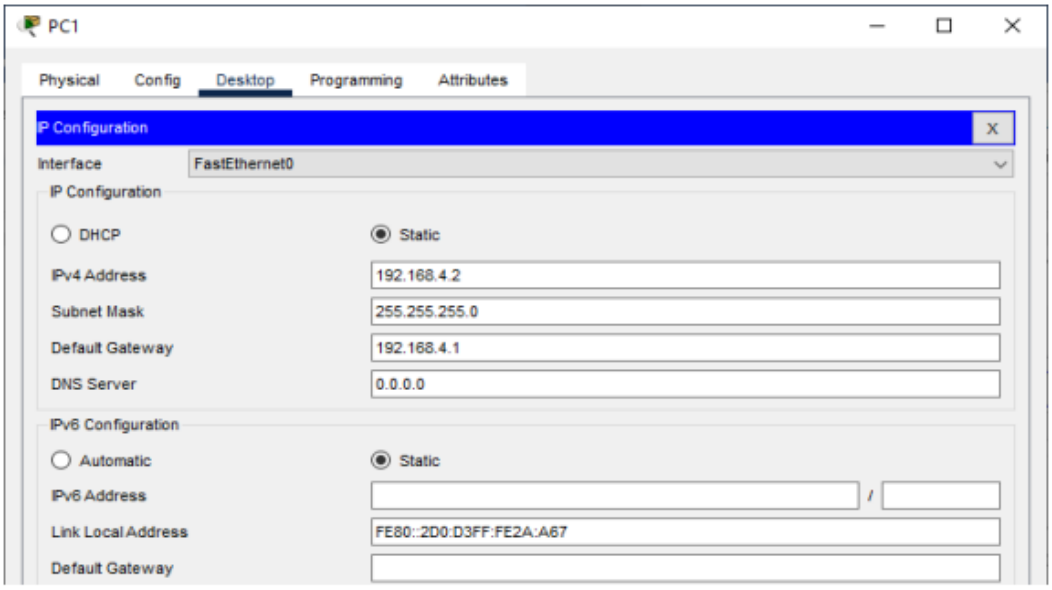
We use the following IP addresses for the given topology

Host	IP Address	Network Address	Network Mask	Wild Card Mask
PC 0	192.168.1.2	192.168.1.0	255.255.255.0	0.0.0.255
PC 1	192.168.4.2	192.168.4.0	255.255.255.0	0.0.0.255
ROUTER 0	G0/0 192.168.1.1	192.168.1.0	255.255.255.0	0.0.0.255
	G0/1 192.168.2.1	192.168.2.0	255.255.255.0	0.0.0.255
	LOOPBACK 10.1.1.1	10.0.0.0	255.0.0.0	0.255.255.255
ROUTER 1	G0/0 192.168.2.2	192.168.2.0	255.255.255.0	0.0.0.255
	G0/1 192.168.3.1	192.168.3.0	255.255.255.0	0.0.0.255
	LOOPBACK 20.1.1.1	20.0.0.0	255.0.0.0	0.255.255.255
ROUTER 2	G0/0 192.168.3.2	192.168.3.0	255.255.255.0	0.0.0.255
	G0/1 192.168.4.1	192.168.4.0	255.255.255.0	0.0.0.255
	LOOPBACK 30.1.1.1	30.0.0.0	255.0.0.0	0.255.255.255

Configuring PC0



Configuring PC1



Configuring Router0

```
Router>enable
Router#
Router#configure terminal
Router(config)#
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
Router(config)#interface loopback 0
Router(config-if)#
Router(config-if)#ip address 10.1.1.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

Configuring Router1

```
Router>enable
Router#
Router#configure terminal
Router(config)#
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#
Router(config-if)#ip address 192.168.2.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
Router(config)#interface loopback 0
Router(config-if)#
Router(config-if)#ip address 10.1.1.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
Router(config)#interface loopback 0
Router(config-if)#
Router(config-if)#ip address 20.1.1.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

Configuring Router2

```
Router>enable
Router#
Router#configure terminal
Router(config)#
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#
Router(config-if)#ip address 192.168.3.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#
Router(config-if)#ip address 192.168.4.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

```
Router(config)#interface loopback 0
Router(config-if)#
Router(config-if)#ip address 30.1.1.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

Configuring Router0 for OSPF

```
Router(config)#
Router(config)#router ospf 1
Router(config-router)#
Router(config-router)#network 192.168.1.0 255.255.255.0 area 0
Router(config-router)#network 192.168.2.0 255.255.255.0 area 0
Router(config-router)#exit
```

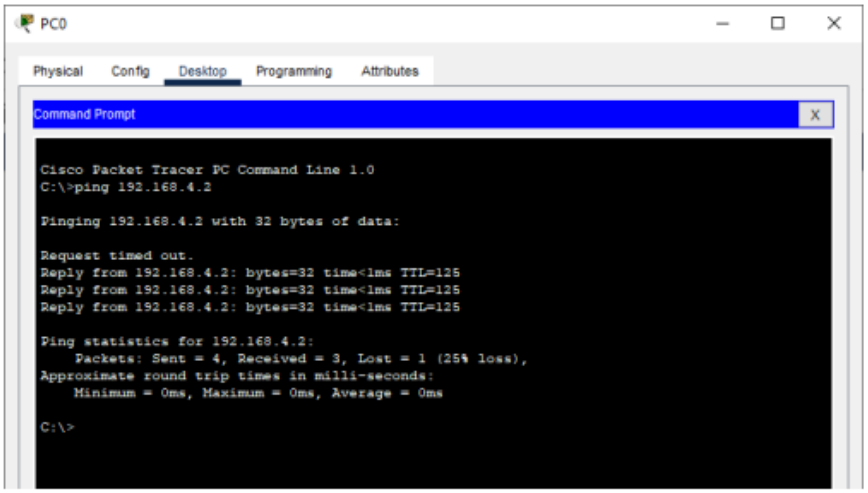
Configuring Router1 for OSPF

```
Router(config)#
Router(config)#router ospf 1
Router(config-router)#
Router(config-router)#network 192.168.2.0 255.255.255.0 area 0
Router(config-router)#network 192.168.3.0 255.255.255.0 area 1
Router(config-router)#exit
```

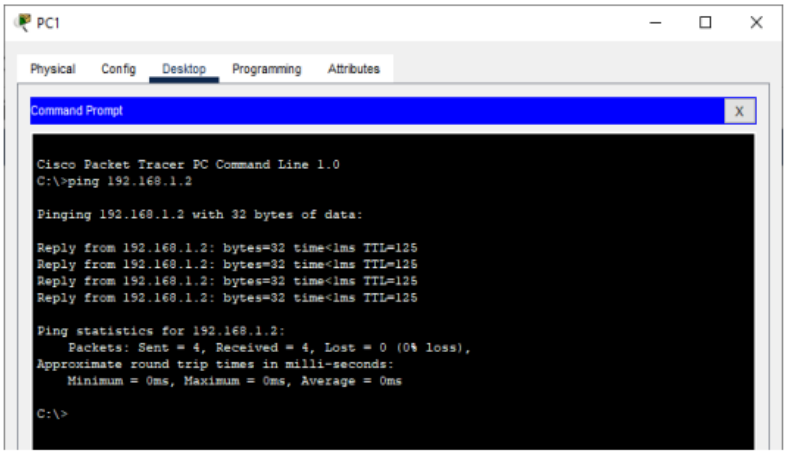
Configuring Router2 for OSPF

```
Router(config)#
Router(config)#router ospf 1
Router(config-router)#
Router(config-router)#network 192.168.3.0 255.255.255.0 area 1
Router(config-router)#network 192.168.4.0 255.255.255.0 area 1
Router(config-router)#exit
```

Verify the connectivity (ping PC1 from PC0)



Verify the connectivity (ping PC0 from PC1)



Hence OSPF with Multiple Areas (area 0 and area 1) was successfully configured and verified

Scan the following QR-code for the video demostaration of the practical OSPF with Multiple Areas

Practical No 8

Aim: Using Packet Tracer, create a network with three routers with BGP and each router associated network will have minimum three PC and show Connectivity

Theory:

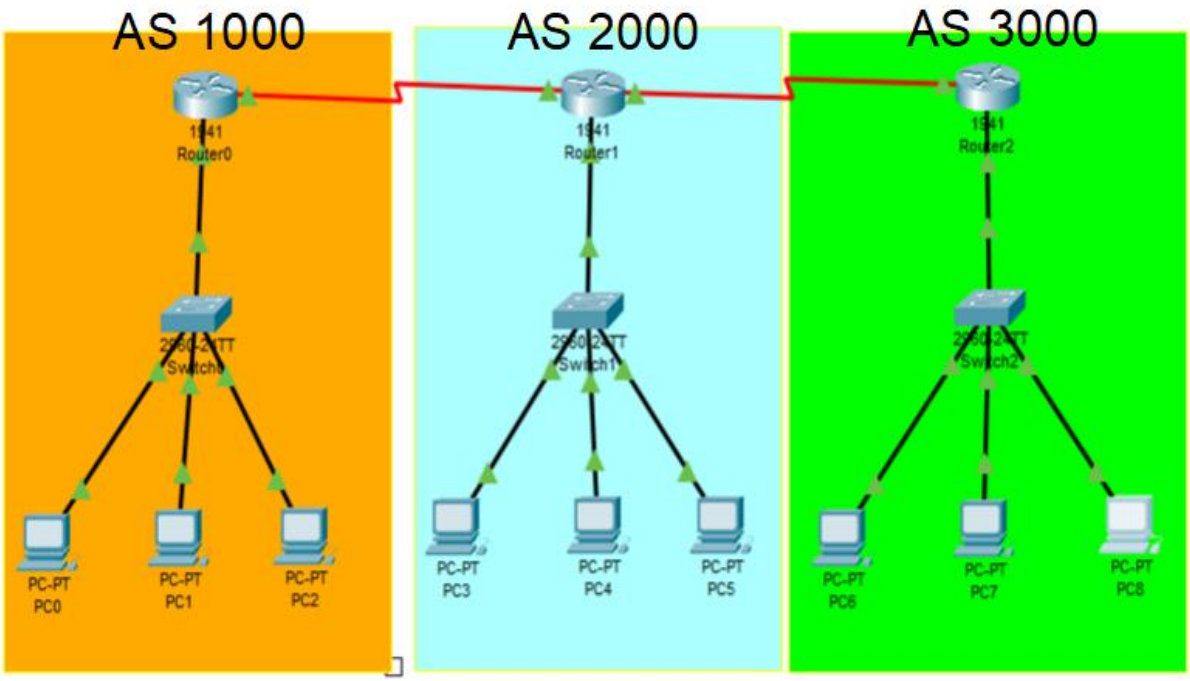
Border Gateway Protocol (BGP) is used to Exchange routing information for the internet and is the protocol used between ISP which are different Autonoumous Systems (AS).

The protocol can connect together any internetwork of autonomous system using an arbitrary topology. The only requirement is that each AS have at least one router that is able to run BGP and that is router connect to at least one other AS's BGP router.
BGP's main function is to exchange network reach-ability information with other BGP systems.

Characteristics of Border Gateway Protocol (BGP):

a) The main role of BGP is to provide communication between two autonomous systems.
b) BGP supports Next-Hop Paradigm.
c) Coordination among multiple BGP speakers within the AS (Autonomous System).
d) BGP advertisement also include path information, along with the reachable destination and next destination pair.
e) BGP can implement policies that can be configured by the administrator.
f) BGP runs Over TCP.
g) BGP conserve network Bandwidth.
h) BGP supports CIDR.
i) BGP also supports Security

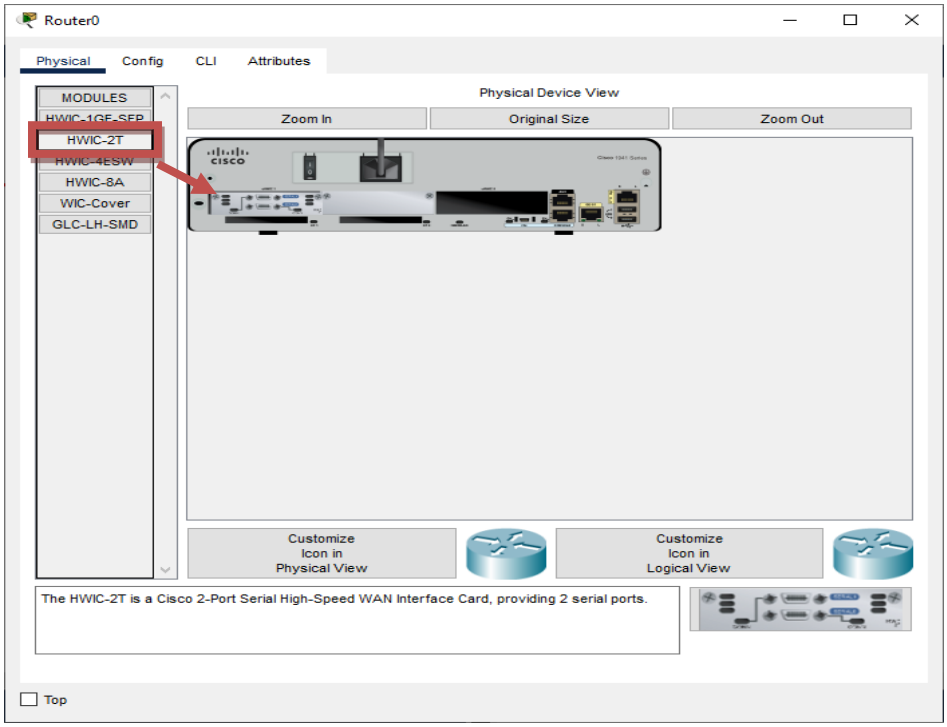
We use the following topology for the present case



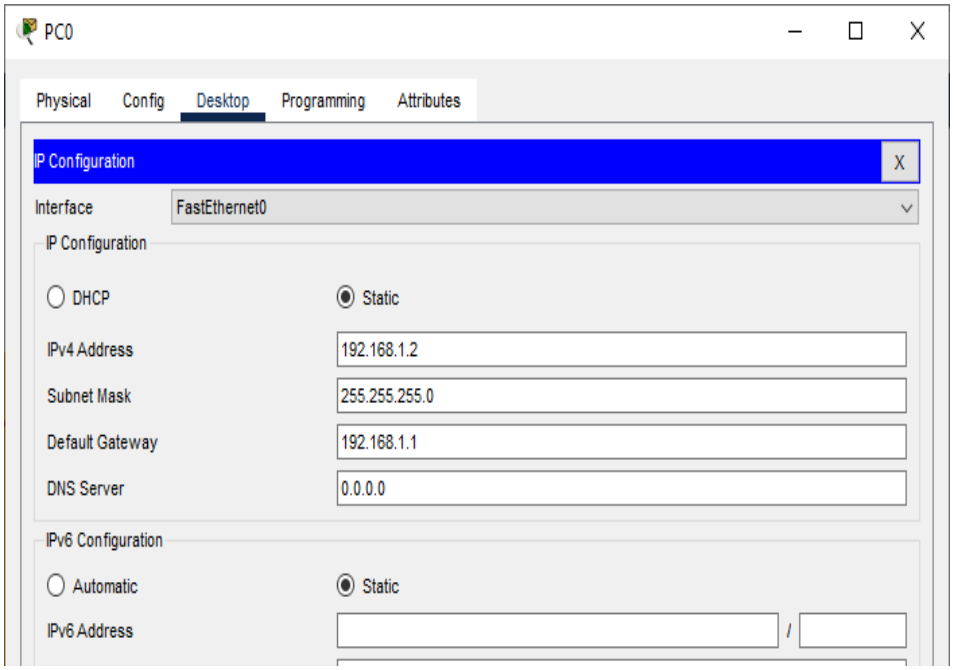
We configure the above network using the following IP addresses

Host	Interface	IP address	Network Address	Default Gateway
Router 0 AS 1000	G0/0	192.168.1.1	192.168.1.0	
	S0/1/0	10.0.0.1	10.0.0.0	
Router 1 AS 2000	G0/0	192.168.2.1	192.168.2.0	
	S0/1/0	10.0.0.2	10.0.0.0	
	S0/1/1	20.0.0.1	20.0.0.0	
Router 2 AS 3000	G0/0	192.168.3.1	192.168.3.0	
	S0/1/1	20.0.0.2	20.0.0.0	
PC0	FastEthernet0	192.168.1.2	192.168.1.0	192.168.1.1
PC1	FastEthernet0	192.168.1.3		
PC2	FastEthernet0	192.168.1.4		
PC3	FastEthernet0	192.168.2.2	192.168.2.0	192.168.2.1
PC4	FastEthernet0	192.168.2.3		
PC5	FastEthernet0	192.168.2.4		
PC6	FastEthernet0	192.168.3.2	192.168.3.0	192.168.3.1
PC7	FastEthernet0	192.168.3.3		
PC8	FastEthernet0	192.168.3.4		

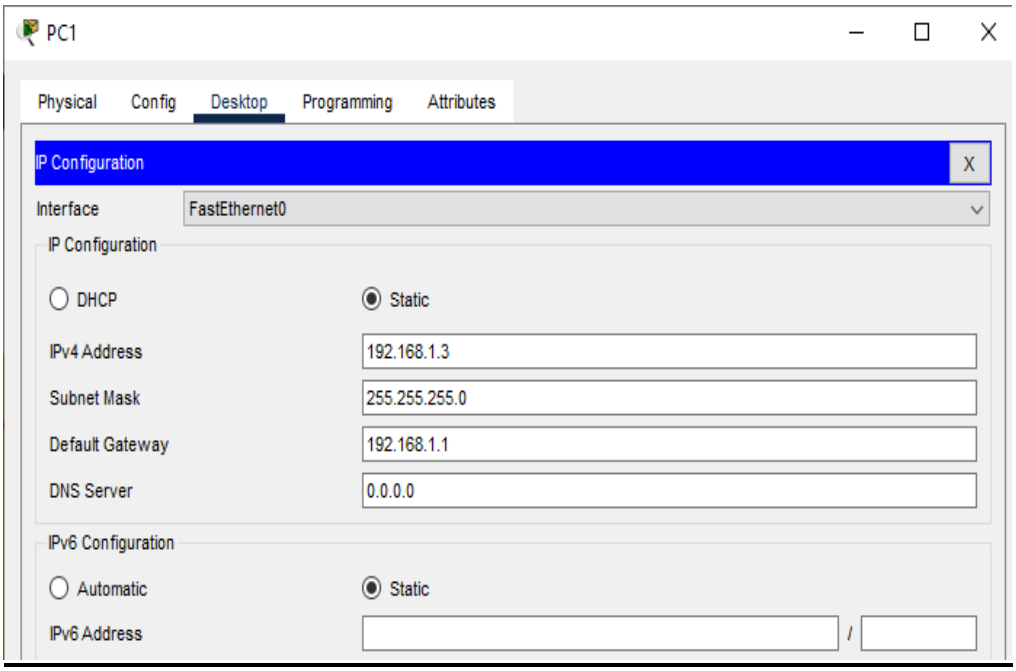
Adding Serial Interface in each Router



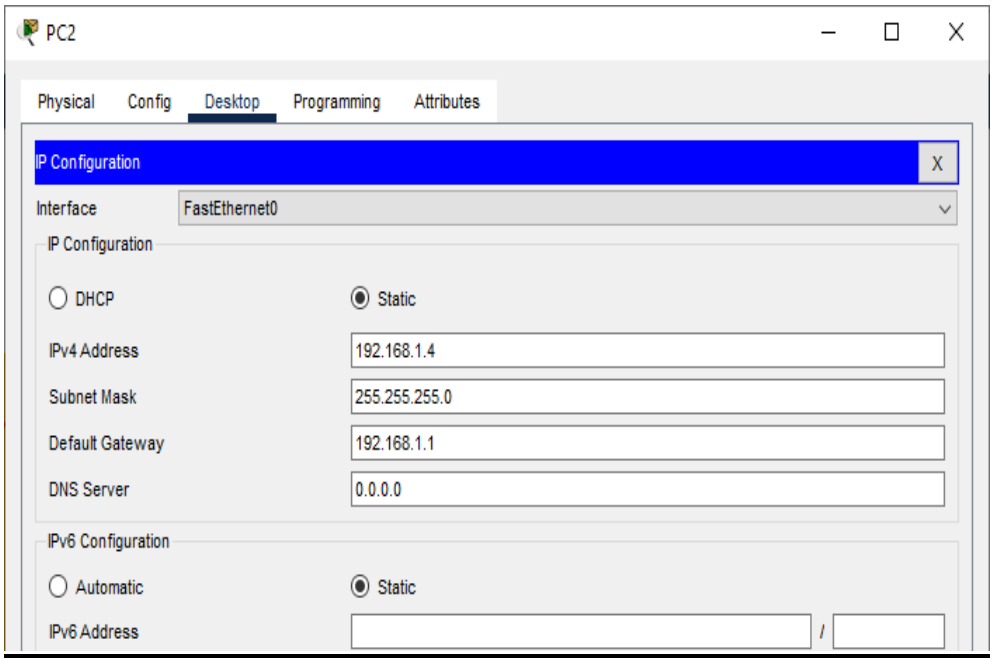
Configuring PC0:



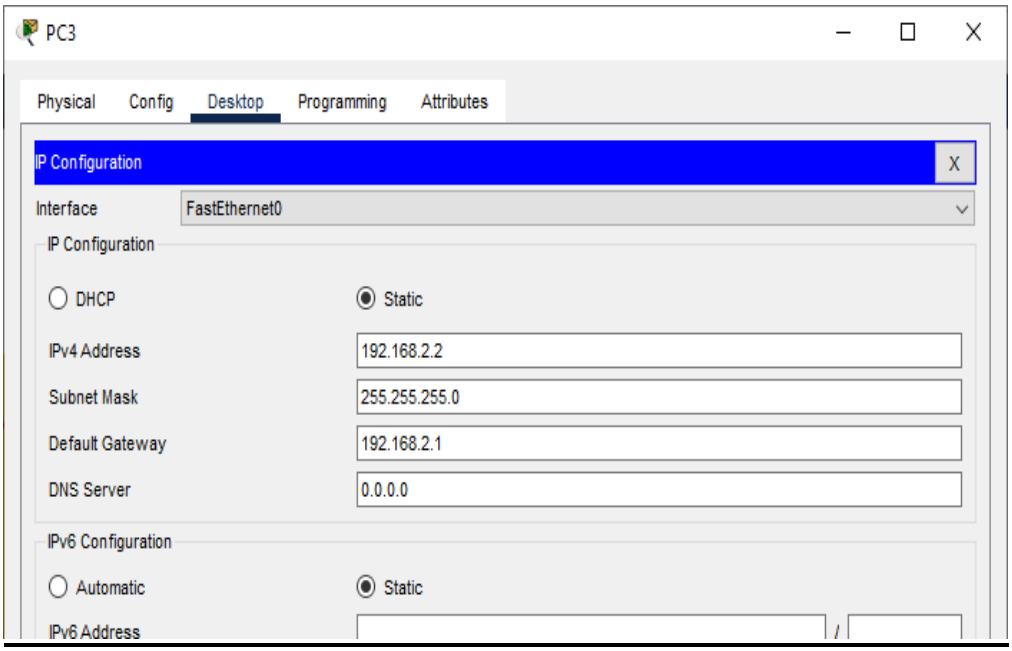
Configuring PC1:



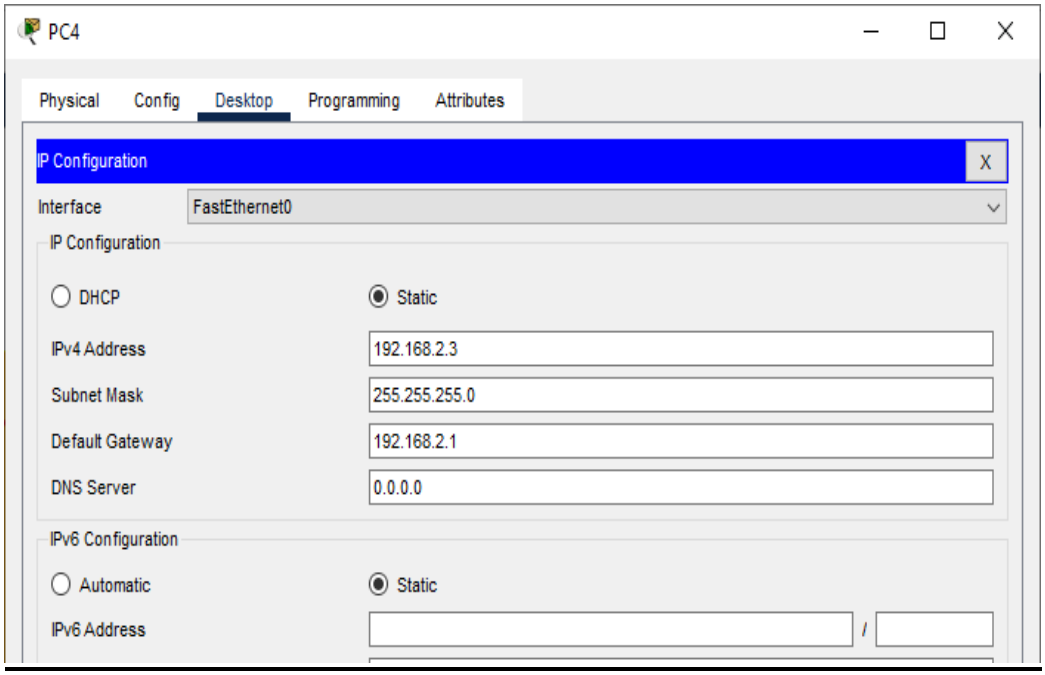
Configuring PC2:



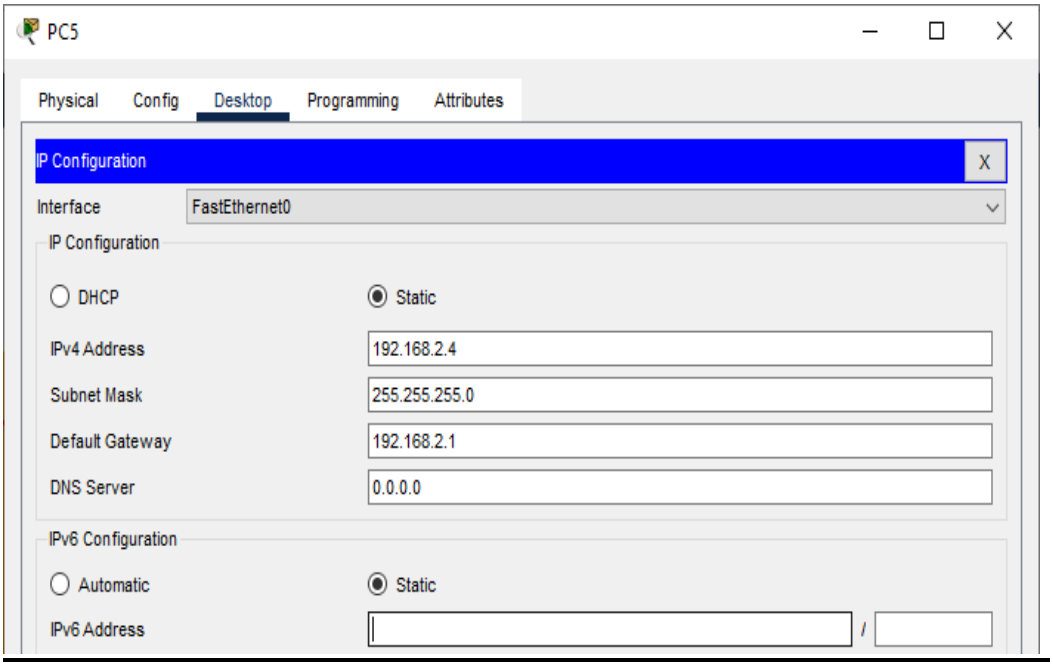
Configuring PC3:



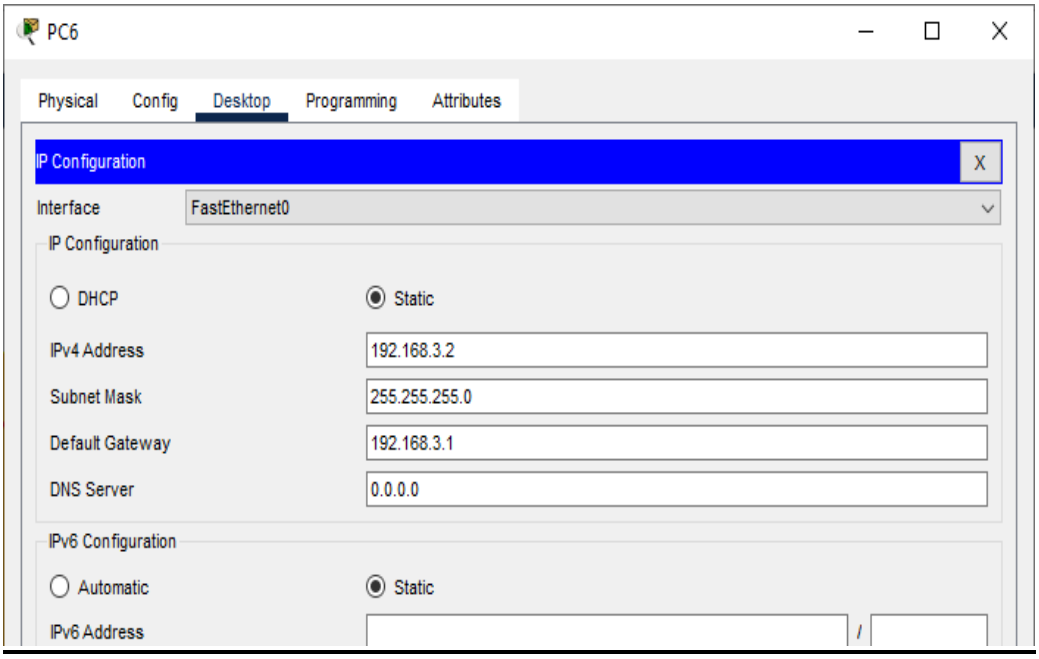
Configuring PC4:



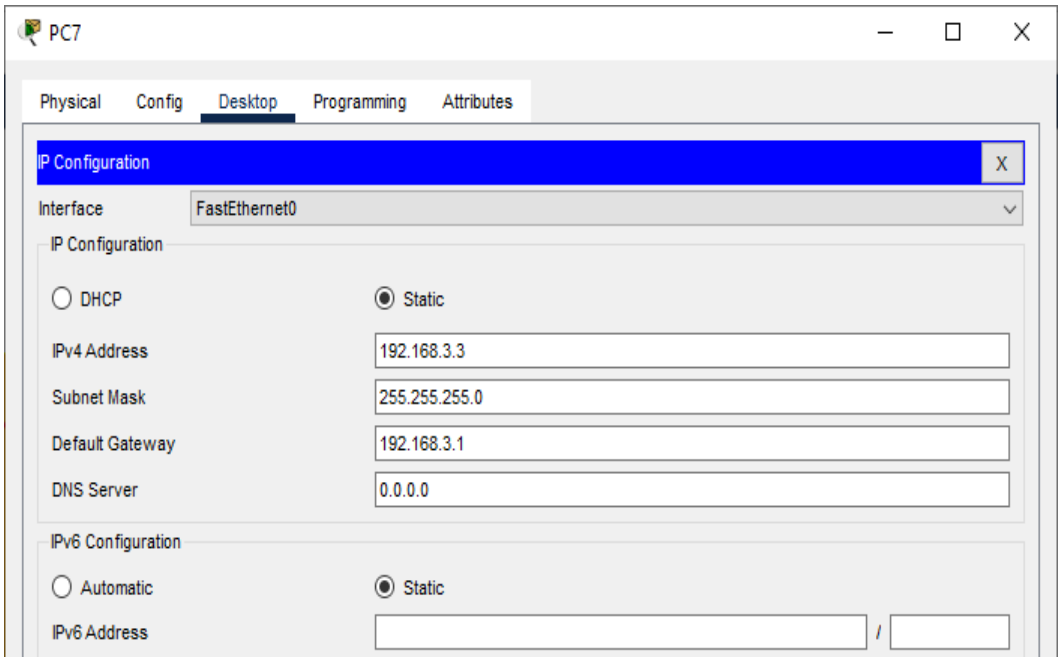
Configuring PC5:



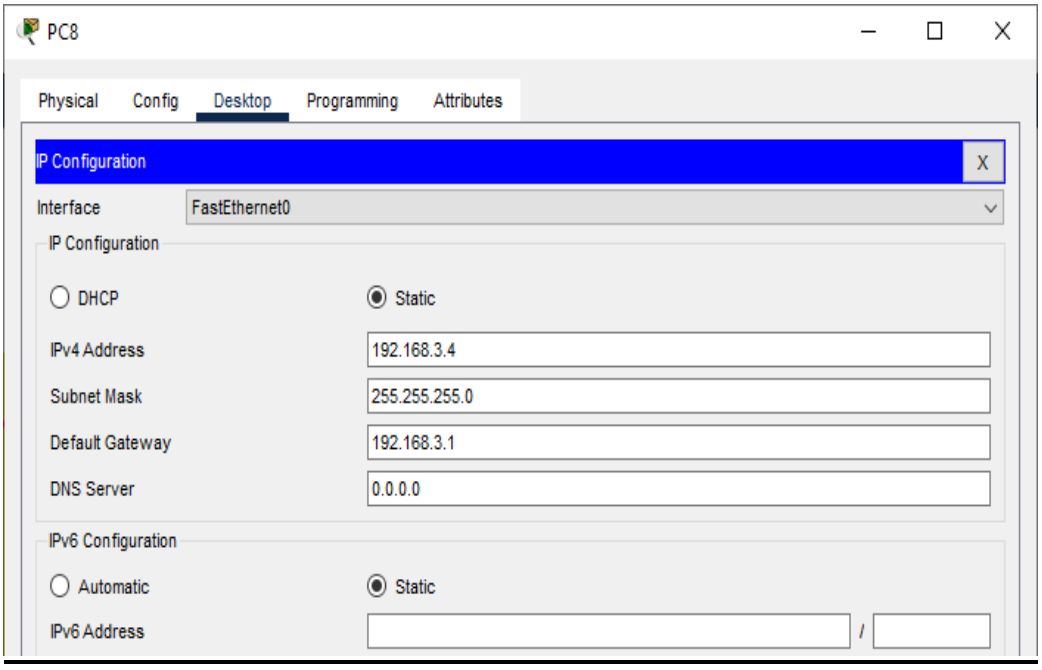
Configuring PC6:



Configuring PC7:

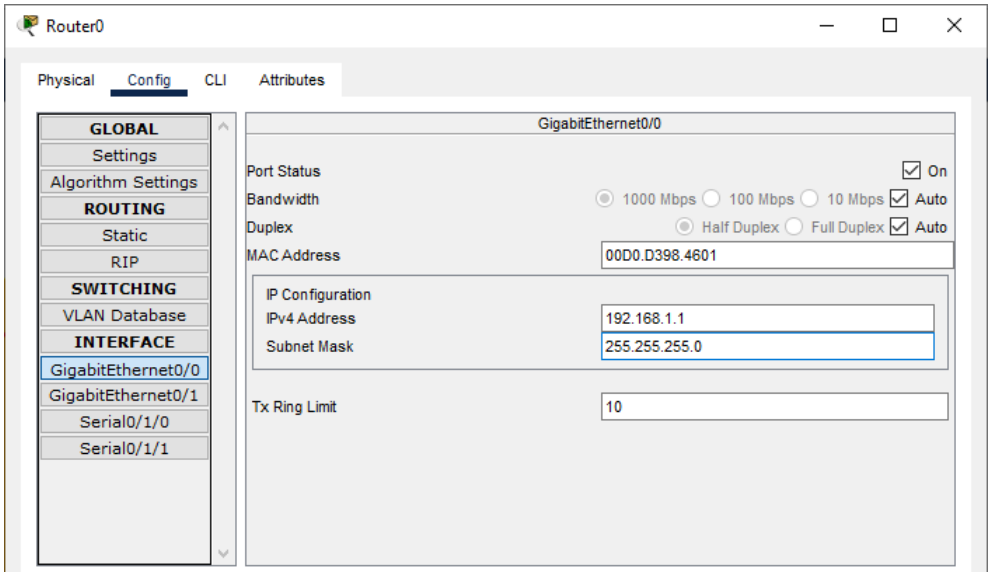


Configuring PC8:

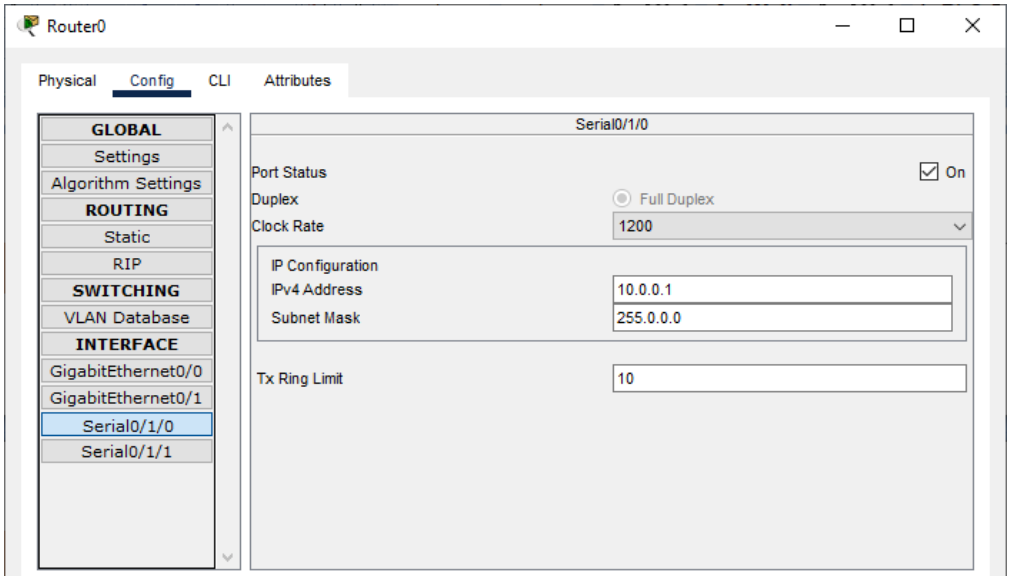


Configuring IP addresses on Router 0

i) Interface G0/0

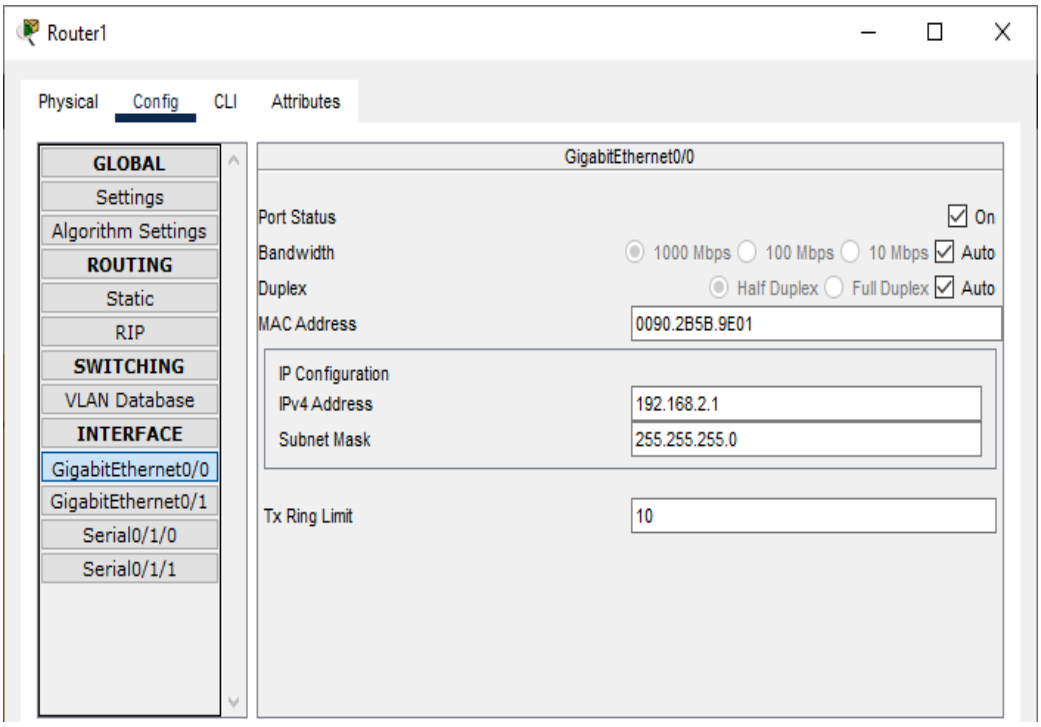


ii) Interface S0/1/0

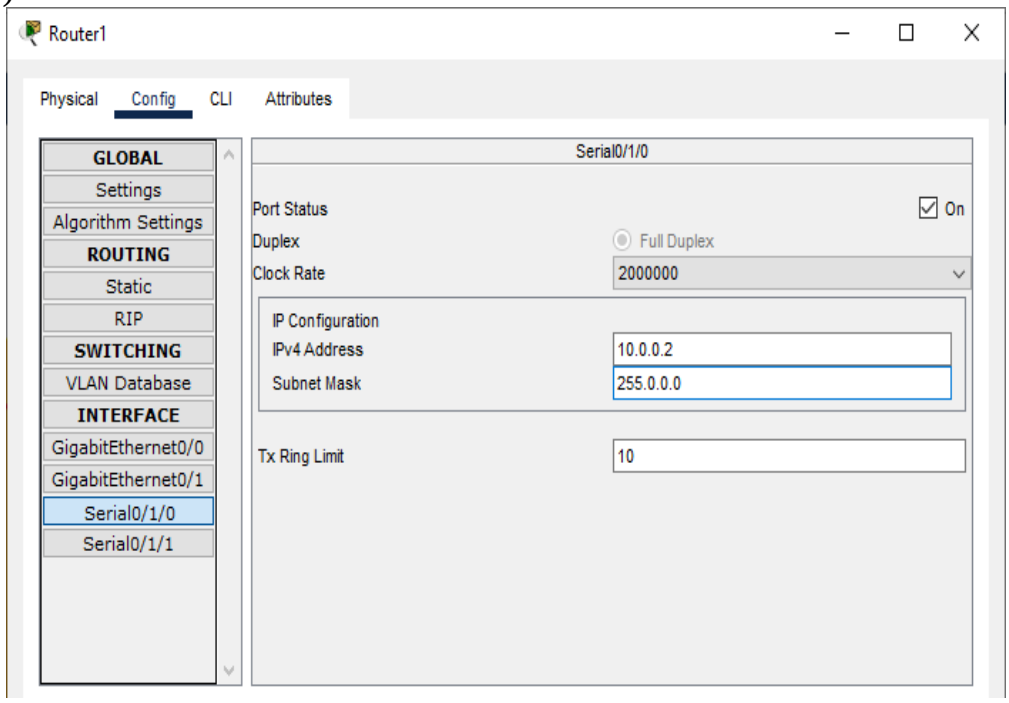


Configuring IP addresses on Router 1

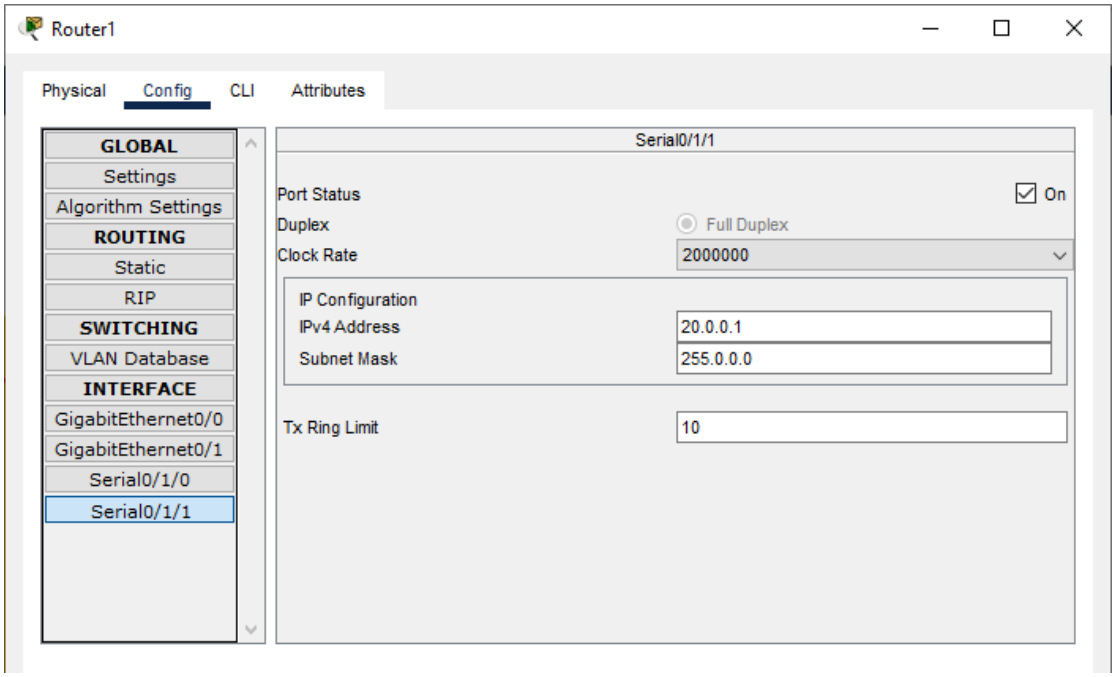
i) Interface G0/0



ii) Interface S0/1/0

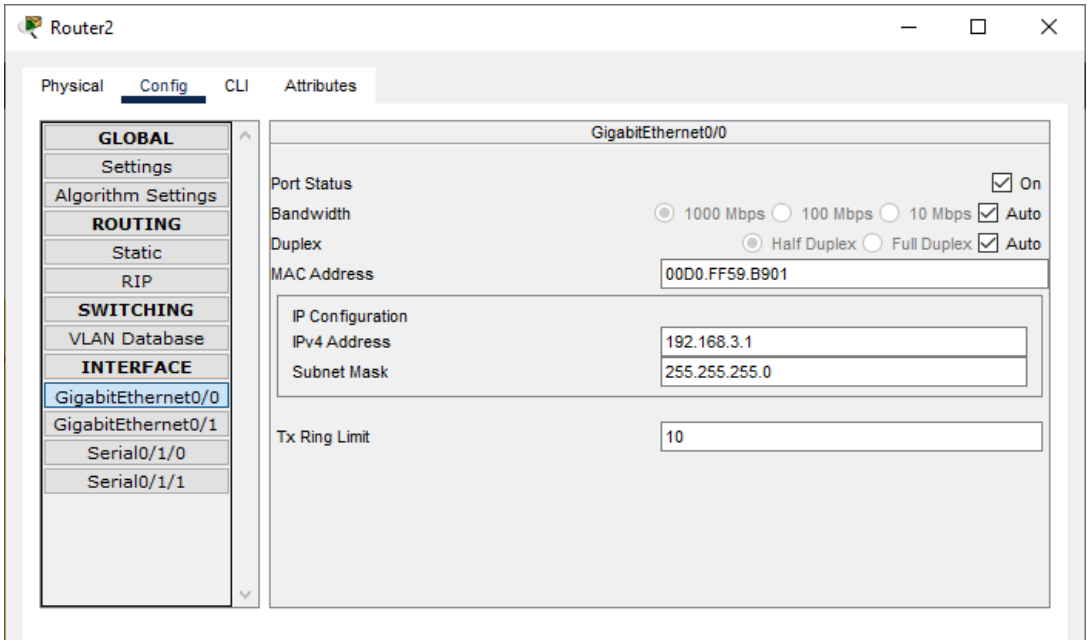


iii) Interface S0/1/1

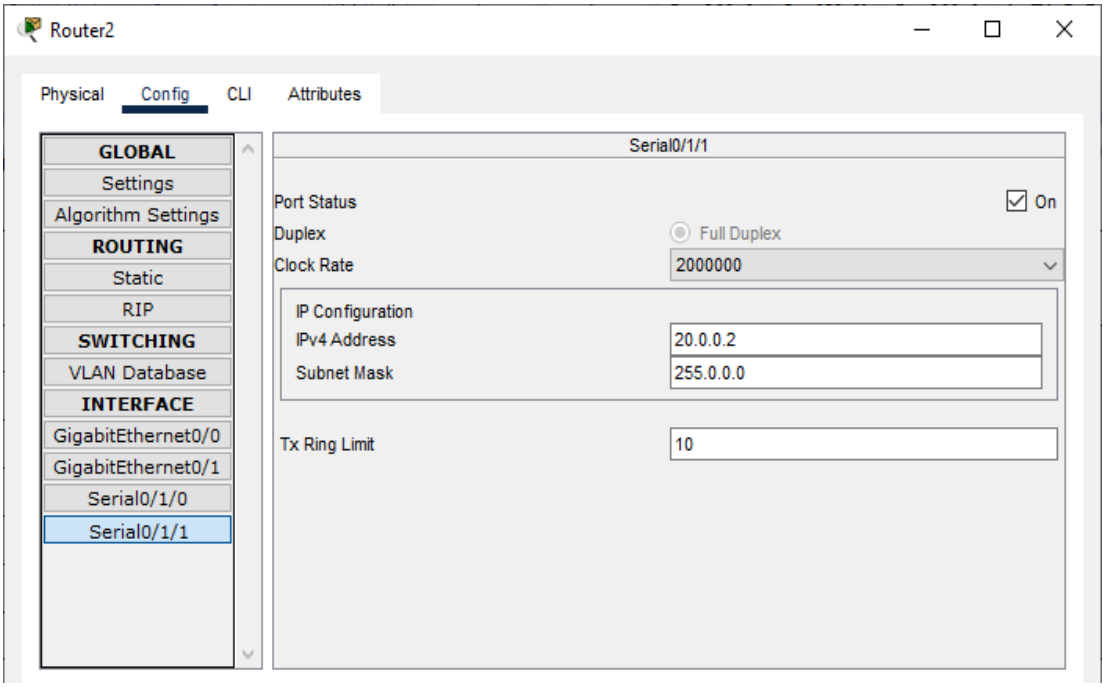


Configuring IP addresses on Router 2

i) Interface G0/0



ii) Interface S0/1/1



Configuring Router 0 for BGP (using the CLI mode)

Router>enable
Router#configure terminal
Router(config)#
Router(config)#router bgp 1000
Router(config-router)#
Router(config-router)#network 10.0.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#neighbor 10.0.0.2 remote-as 2000

Configuring Router 1 for BGP (using the CLI mode)

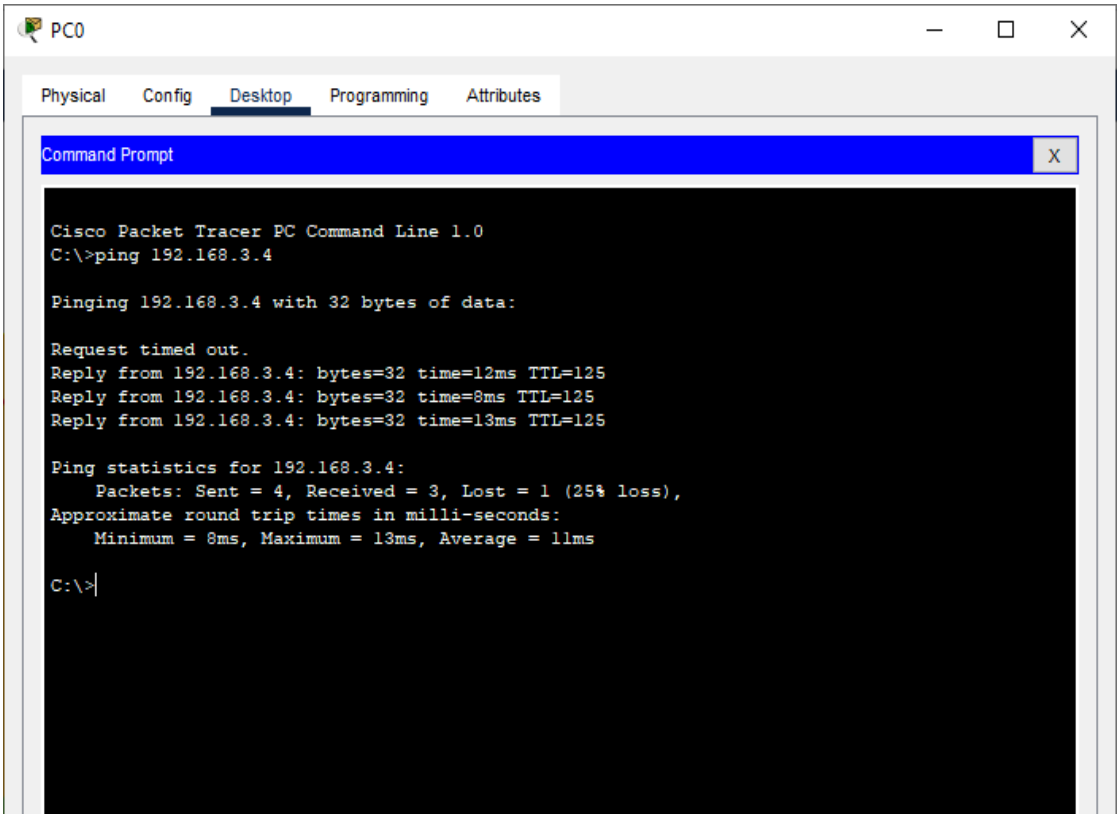
Router>enable
Router#configure terminal
Router(config)#
Router(config)#router bgp 2000
Router(config-router)#network 10.0.0.0
Router(config-router)#network 20.0.0.0
Router(config-router)#network 192.168.2.0
Router(config-router)#neighbor 10.0.0.1 remote-as 1000
Router(config-router)#neighbor 20.0.0.2 remote-as 3000

Configuring Router 2 for BGP (using the CLI mode)

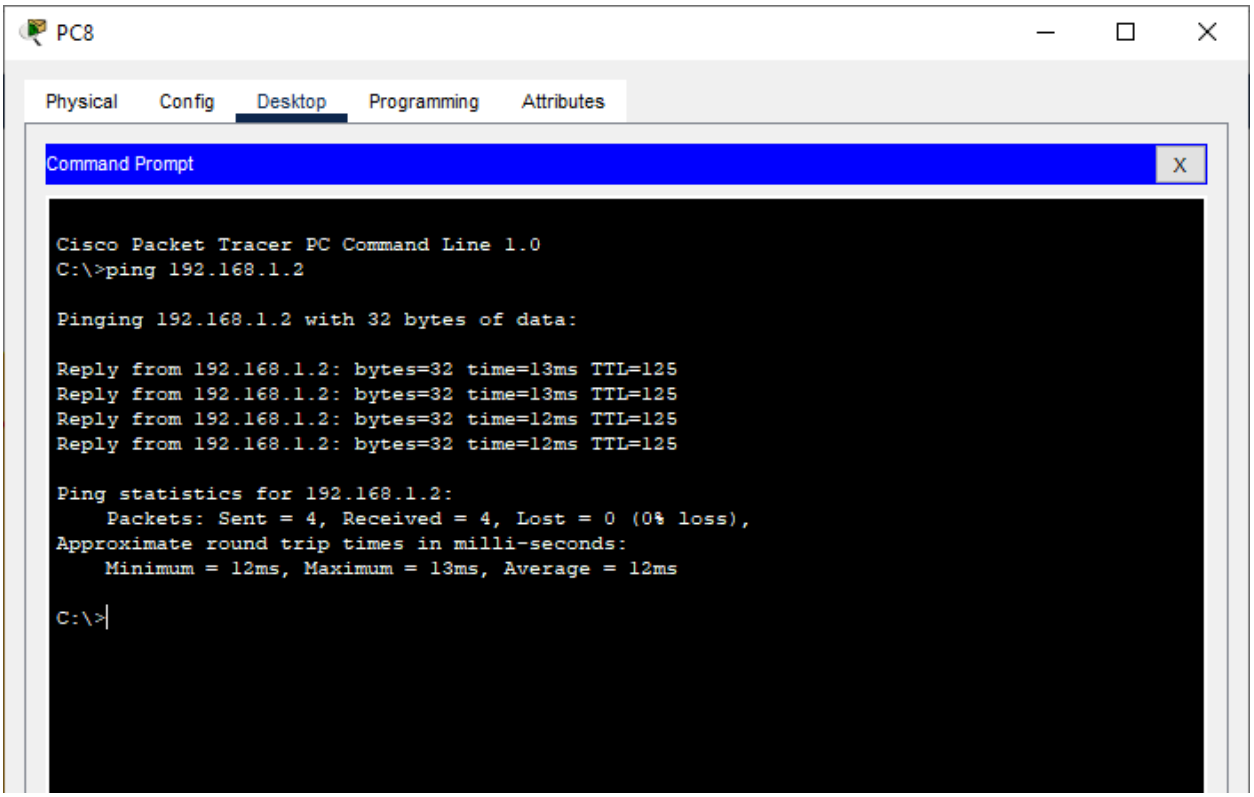
Router>enable
Router#configure terminal
Router(config)#
Router(config)#router bgp 3000
Router(config-router)#
Router(config-router)#network 20.0.0.0
Router(config-router)#network 192.168.3.0
Router(config-router)#neighbor 20.0.0.1 remote-as 2000

Checking the connectivity by using the ping command

i) Pinging PC8 (ip address 192.168.3.4) from PC1



ii) Pinging PC0 (ip address 192.168.1.2) from PC8



Result:

Hence the BGP has been studied and verified through the given network

Link for the video demonstration of the practical:

https://youtu.be/fBEFfW-TWec