VIDYA VIKAS EDUCATION SOCIETY
VIKAS COLLEGE OF ARTS, SCIENCE AND COMMERCE ,VIKHROLI EAST
Kannamwar Nagar – 2, Vikhroli (East), Mumbai – 400083.

COMPUTER SCIENCE

Submitted To :

Mr. MILIND PARADKAR SIR

Submitted By :

Name: Aditya Subhash Nikam

Class/Sec: B.Sc.CS

Roll No.: 222716

SUBJECT: COMPUTER NETWORK'S

Vikas College of Arts, Science & Commerce

CERTIFICATE

This is to certify that ……Aditya Subhash Nikam……

of class/sec B.Sc.CS has successfully completed theproject entitled COMPUTER NETWORK'S PRACTICALS to my satisfaction and submitted the same during the academic year 2022-2023

The project is the result of his/her efforts & endeavors.

…… **Date** : ……

(Signature of the teacher)

Mr. MILIND M PARADKAR SIR

(Name of the teacher)

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, pathping, 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).

   iv) netstat -r
      Another option relevant to performance is the display of the discovered Path Maximum Transmission Unit (PMTU).

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.
   ii) arp -g: Same as the arp -a command.

iii) arp -d: This command is used to delete an entry from the ARP table for a particular interface. To delete an entry, write arp -d command along with the IP address in a command prompt to be deleted.

iv) arp -s: This command is used to add the static entry in the ARP table, which resolves the InetAddr (IP address) to the EtherAddr (physical address). To add a static entry in an ARP table, we write arp -s command along with the IP address and MAC address of the device in a command prompt.

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) Pathping: This command sends multiple echo Request messages to each router between a source and destination, over a period of time, and then computes results based on the packets returned from each router. It can be used to find the routers or links having network problems.

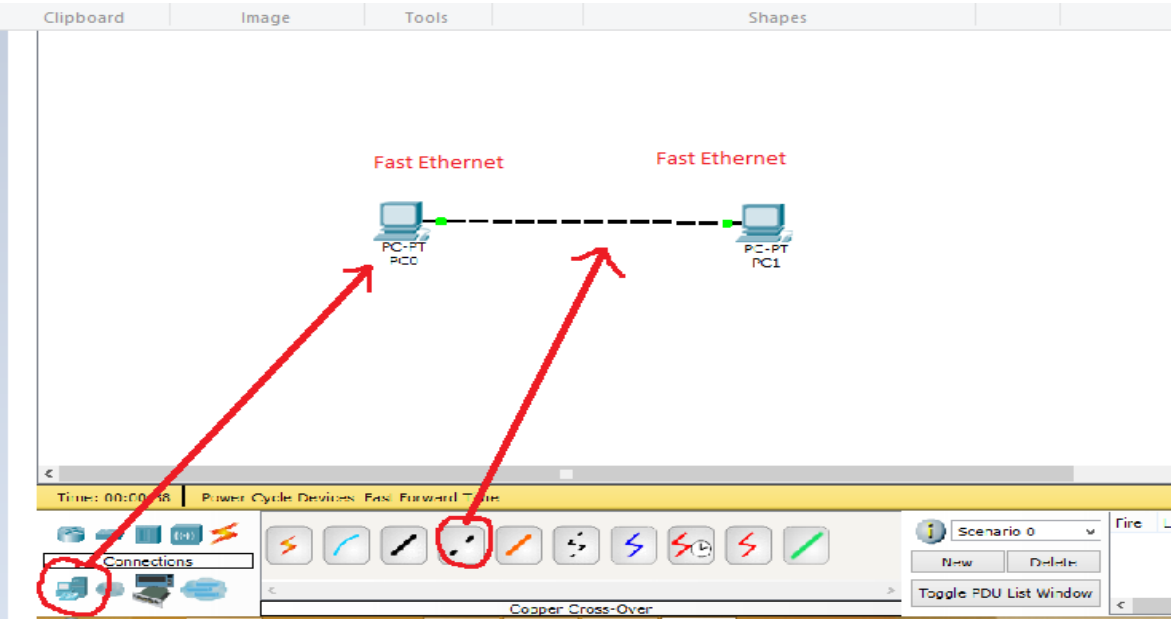
10) SystemInfo: This command is use ot display detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties

Practical No 2

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

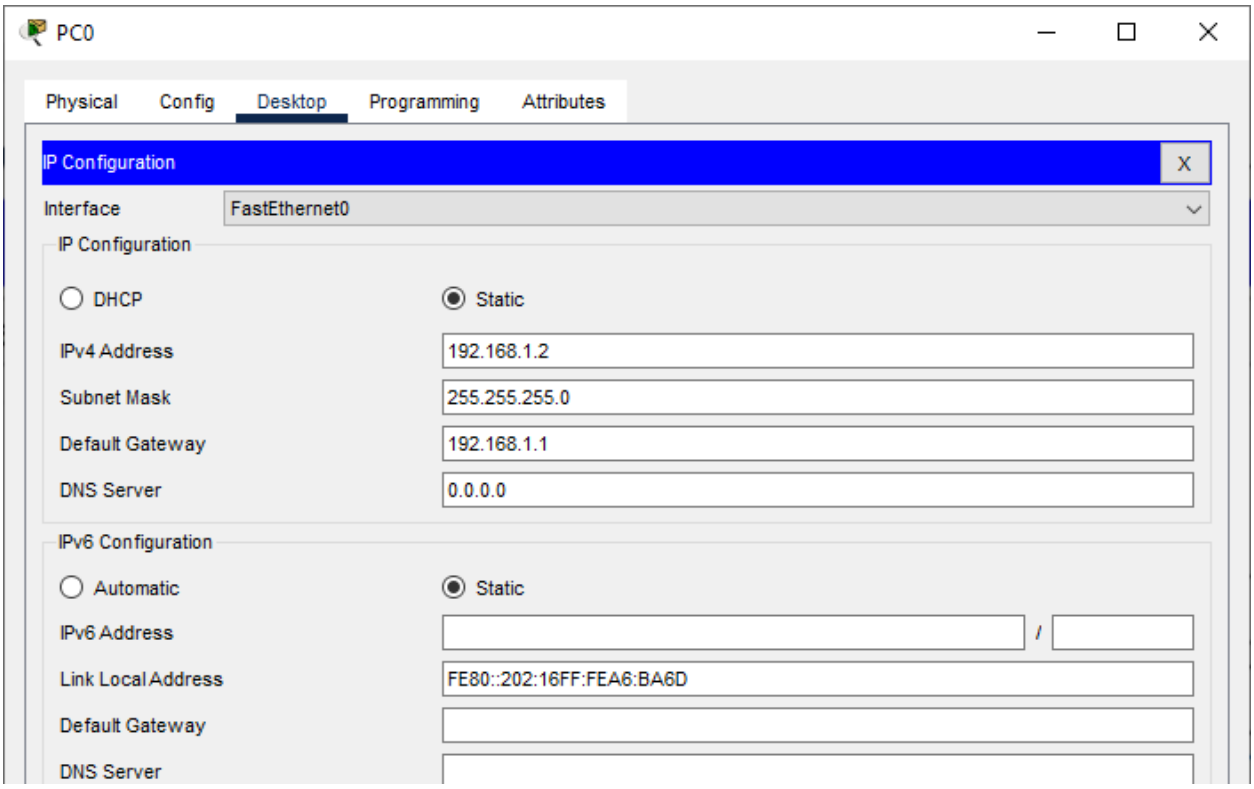
Theory:

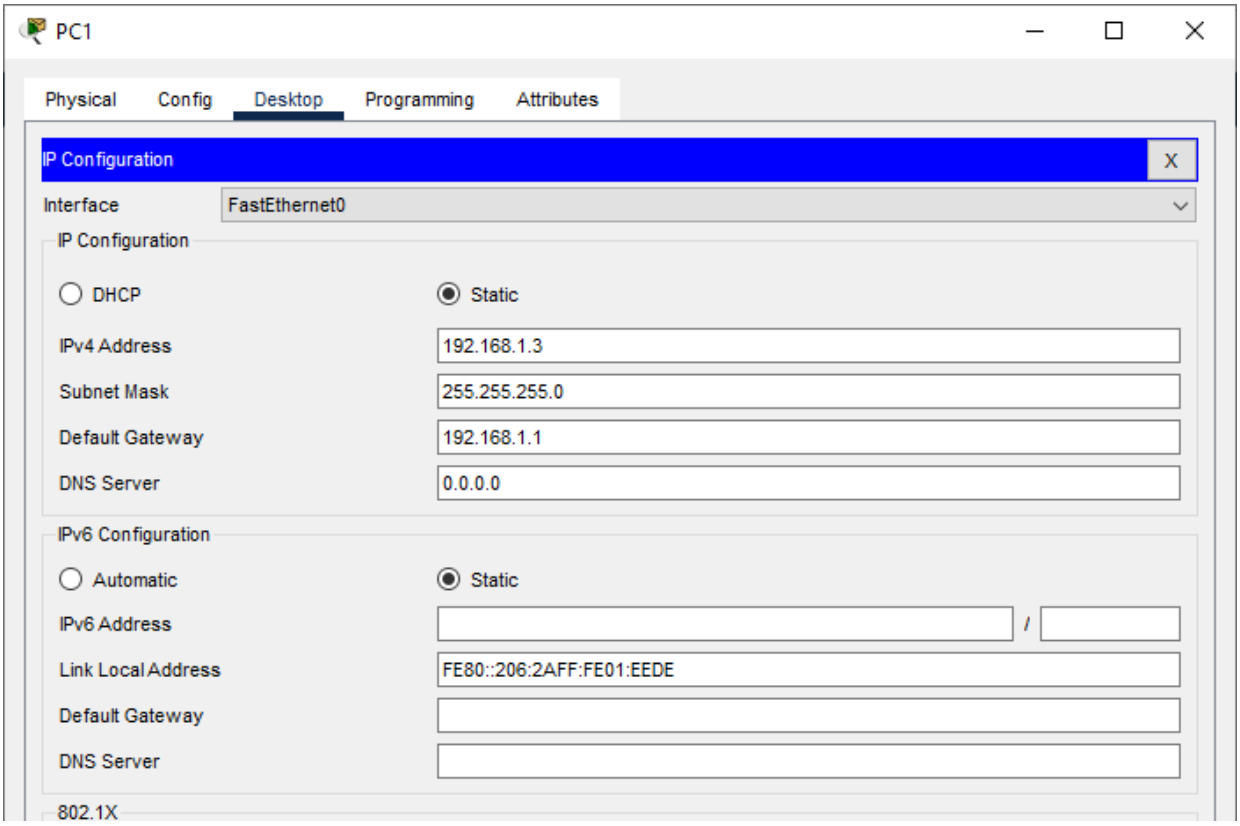
We use the following network to verify the connectivity using Cisco packet tracer



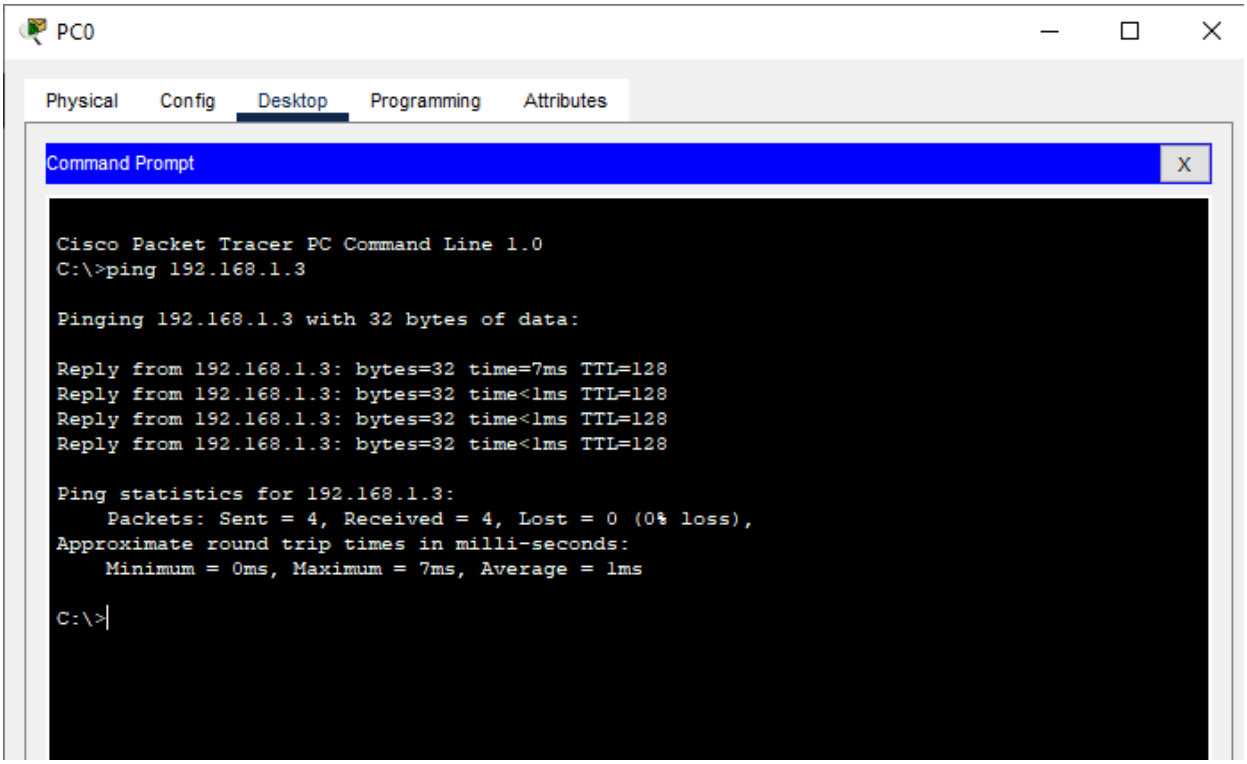
Now we set the ip address of the devices as follows

Host name	ip Address	Default Gateway
PC0	192.168.1.2	192.168.1.1
PC1	192.168.1.3	192.168.1.1


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
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::202:16FF:FEA6:BA6D
Default Gateway
DNS Server


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
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::206:2AFF:FE01:EEDE
Default Gateway
DNS Server
802.1X

In order to check the connectivity we send a ping command from PC0 to PC1 as follows



Result:

Hence the Connectivity between the PCs has been verified.

Practical No 3

Aim: Using Packet Tracer, create a basic network of one server and two computersusing 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 otherrelated configuration information such as the subnet mask and default gateway.

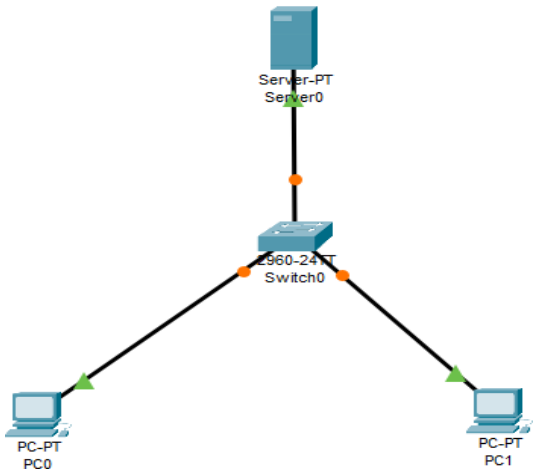
The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it starts up on the network. Because the IP addressesare dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.

DHCP provides the following benefits.

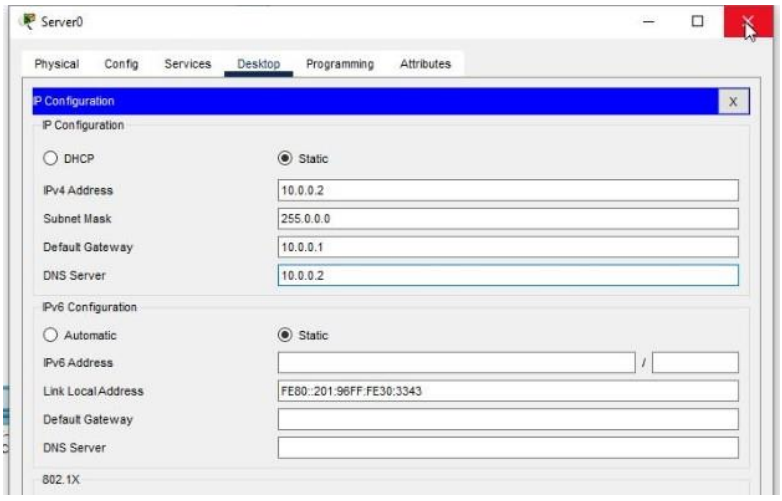
1) Reliable IP address configuration. DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.
2) Reduced network administration. DHCP includes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

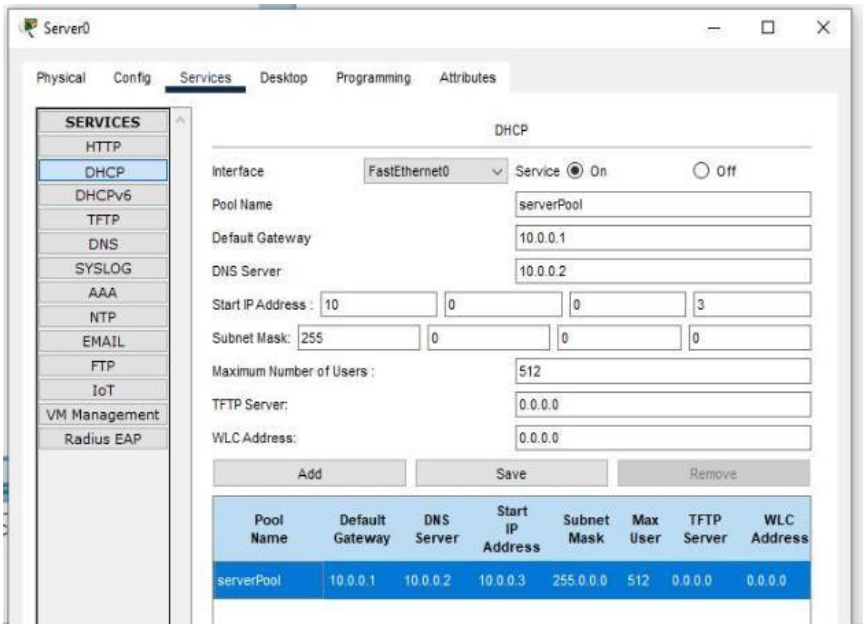
We use the following topology for the present case



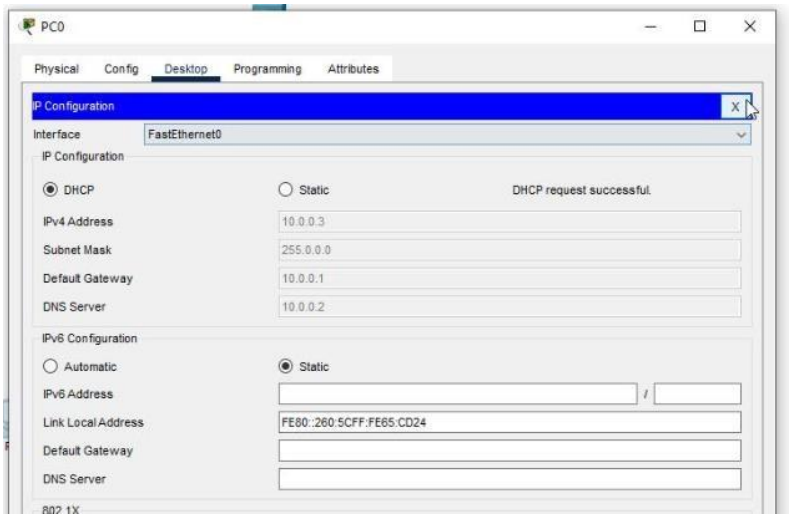
Configuring the Server:

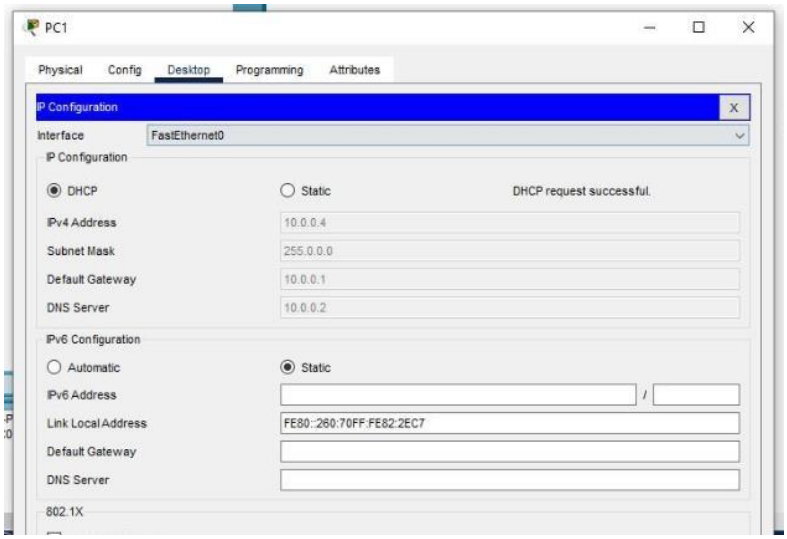


Enabling and setting the DHCP Service on the Server:

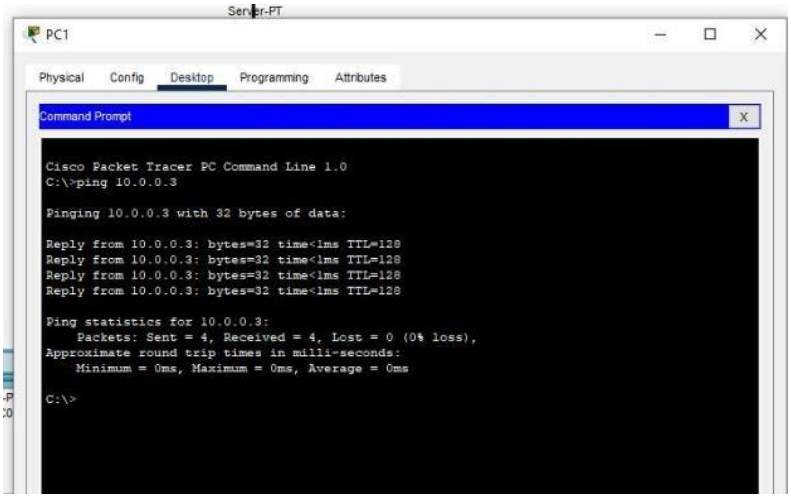


Verifying the Dynamic Addressing on both the PCs:





Checking the connectivity:



Result:

Hence the Connectivity between the PCs has been verified.

Practical No 4

Aim: Using Packet Tracer, create a basic network of one server and two computersand 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 toconnect 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 andyour small business.

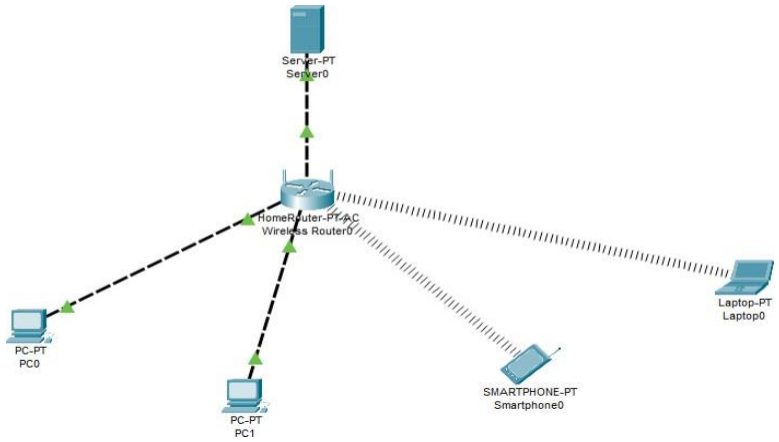
1) It is easier to set up compared to setting up a wired network.
2) It is more convenient to access.
3) It is less complicated to add new users in the network.
4) It gives users more flexibility to stay online even when moving from one area in the office to another.
5) Guest users can have Internet 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.

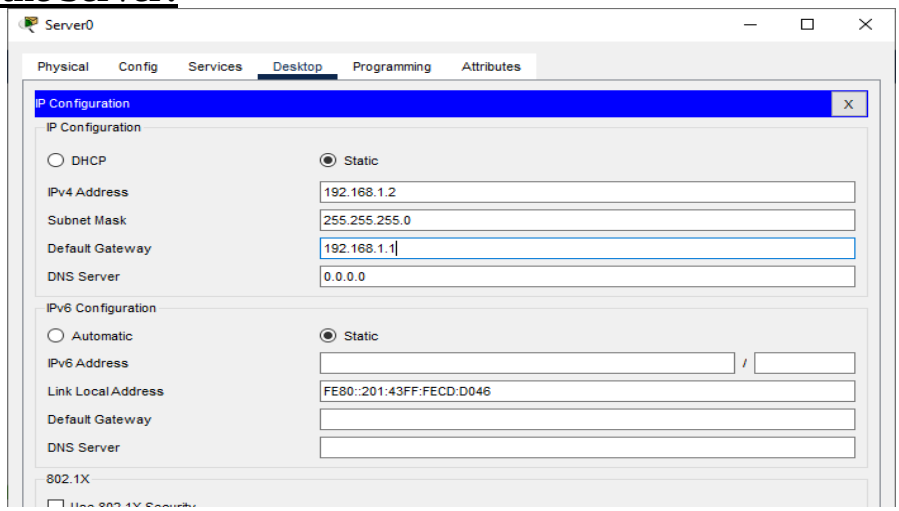
With a WAP, the following can be done:

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.

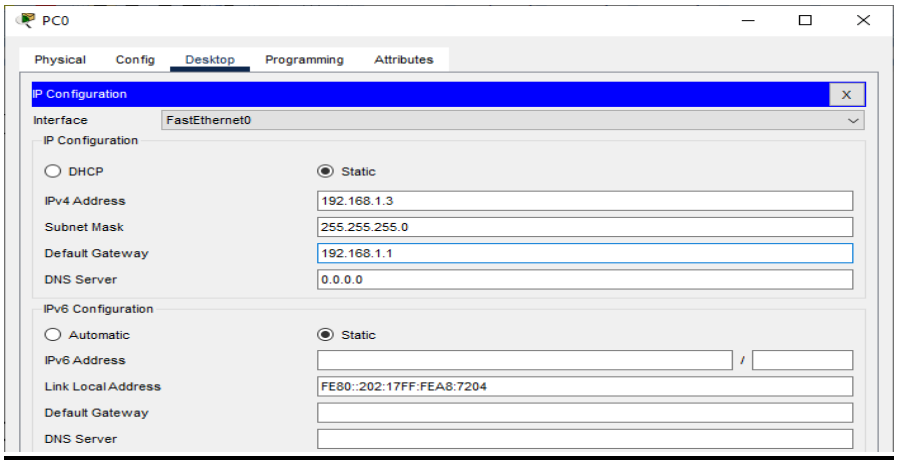
For the present case we use the following topology



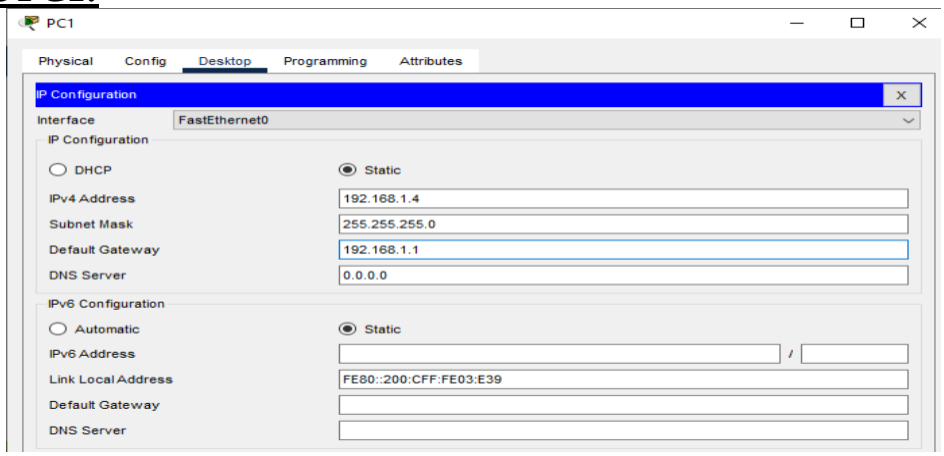
Configure the Server:



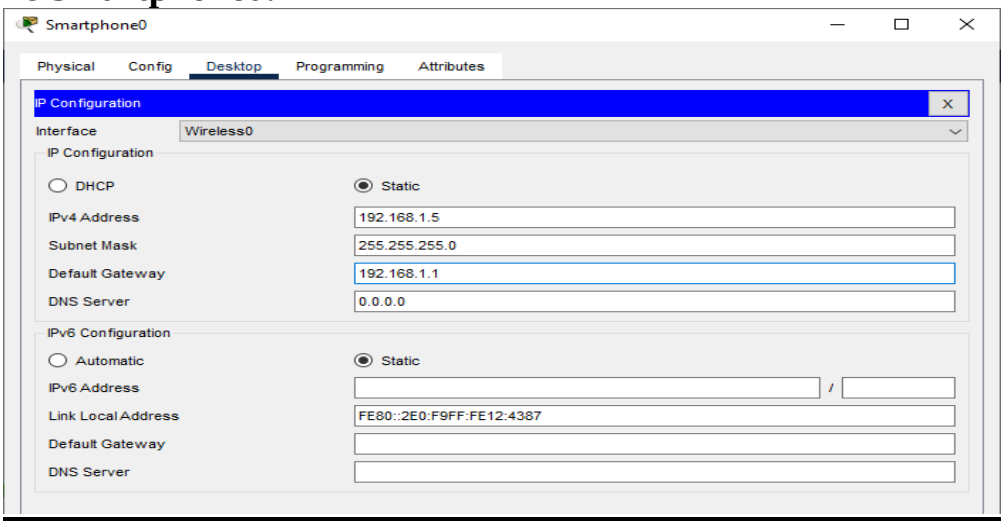
Configure PC0:



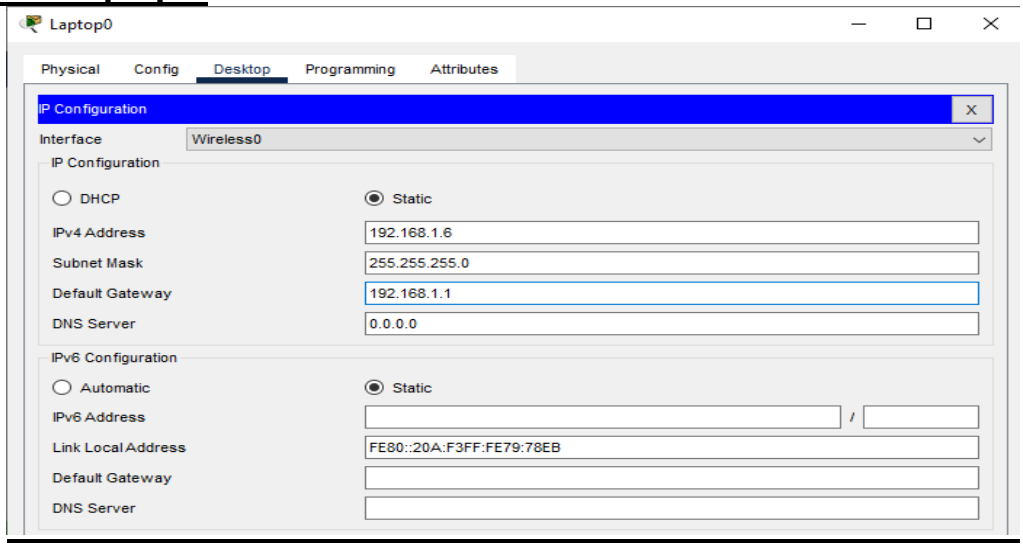
Configure PC1:



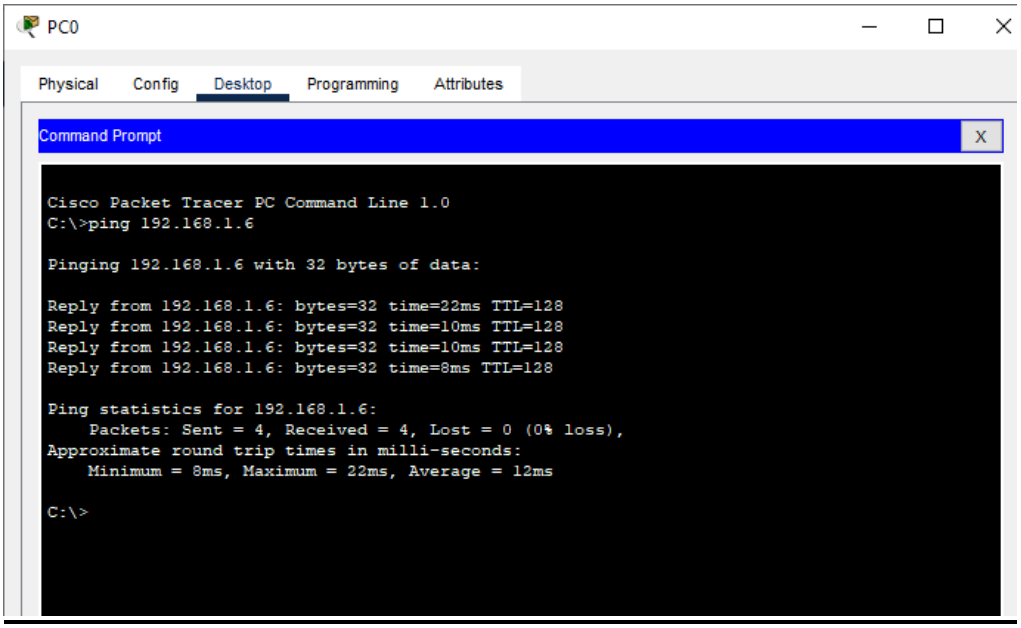
Configure Smartphone0:



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.

Practical No 5

Aim: Using Packet Tracer to create a network with three routers with RIPv1 and each router associated network will have minimum three PC and show the connectivity

Theory:

RIP is one of the dynamic routing protocols and the first distance-vector routing protocol that uses the hop count as a routing metric. A lower hop count is preferred.

Each router between the source and destination network is counted as one hop. RIP prevents routing loops by imposing a maximum number of hops on the path between source and destination.

In RIP, Every 30 seconds, each router broadcasts its entire routing table to its nearest neighbors.

Pros and Cons of RIP Protocol

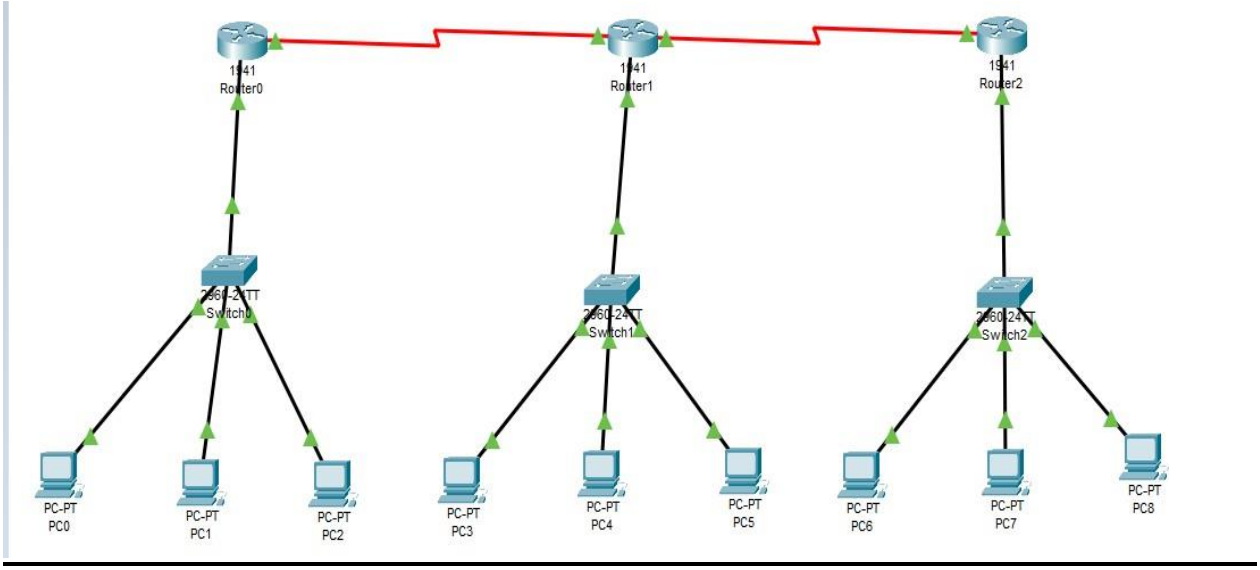
Pros:

1. The RIP protocol is ideal for small networks since it is simple to learn and configure.
2. RIP routing is guaranteed to work with nearly all routers.
3. When the network topology changes, RIP does not require an update.

Cons:

1. RIP does not support variable length subnet masks
2. RIP transmits updates every 30 seconds, which cause traffic and consumes bandwidth.
3. RIP hop counts are restricted to 15, hence any router beyond that distance is deemed infinity and becomes unreachable.
4. The rate of convergence is slow in RIP compared to other routing protocols. When a link fails, finding alternate network paths takes a long time.
5. RIP does not support multiple paths on the same route, which may result in extra routing loops.

We use the following topology for the present case

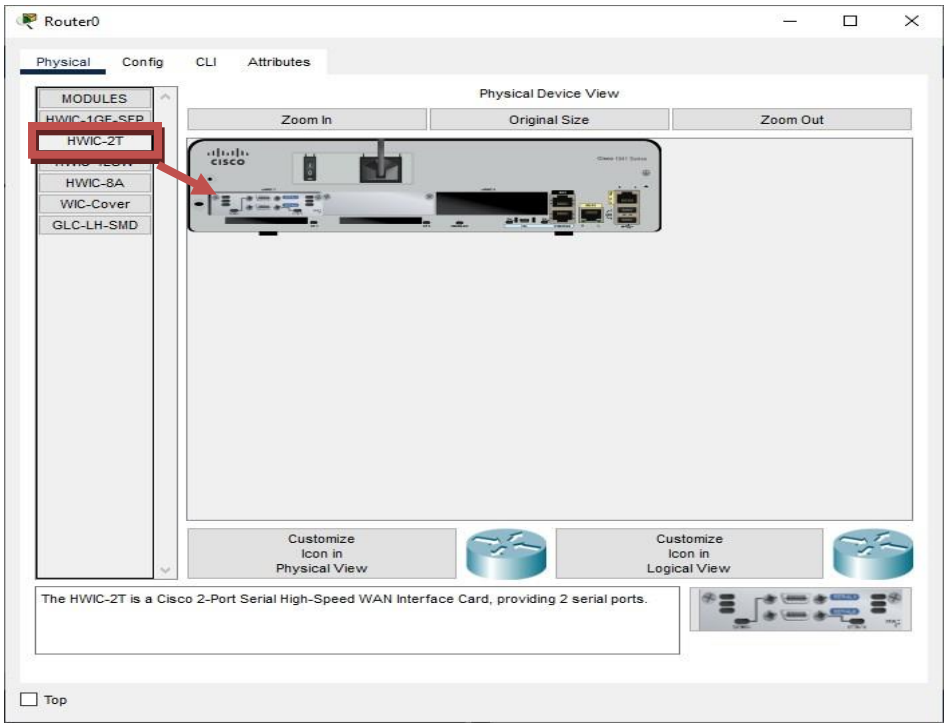


We configure the above network using the following IP addresses

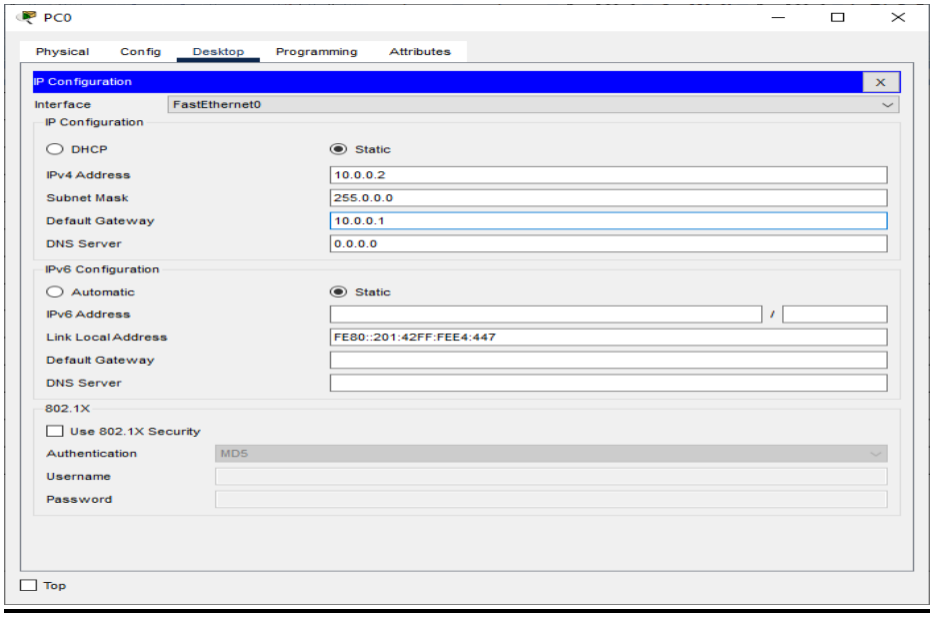
Host	Interface	IP address	Network Address	Default Gateway
Router 0	G0/0	10.0.0.1	10.0.0.0	
	S0/1/0	192.168.0.1	192.168.0.0	
Router 1	G0/0	20.0.0.1	20.0.0.0	
	S0/1/0	192.168.0.2	192.168.0.0	
	S0/1/1	192.168.1.1	192.168.1.0	
Router 2	G0/0	30.0.0.1	30.0.0.0	
	S0/1/1	192.168.1.2	192.168.1.0	
PC0	FastEthernet 0	10.0.0.2	10.0.0.0	10.0.0.1
PC1	FastEthernet 0	10.0.0.3	10.0.0.0	10.0.0.1
PC2	FastEthernet 0	10.0.0.4	10.0.0.0	10.0.0.1
PC3	FastEthernet 0	20.0.0.2	20.0.0.0	20.0.0.1
PC4	FastEthernet 0	20.0.0.3	20.0.0.0	20.0.0.1
PC5	FastEthernet 0	20.0.0.4	20.0.0.0	20.0.0.1

PC6	FastEthernet 0	30.0.0.2	30.0.0.0	30.0.0.1
PC7	FastEthernet 0	30.0.0.3	30.0.0.0	30.0.0.1
PC8	FastEthernet 0	30.0.0.4	30.0.0.0	30.0.0.1

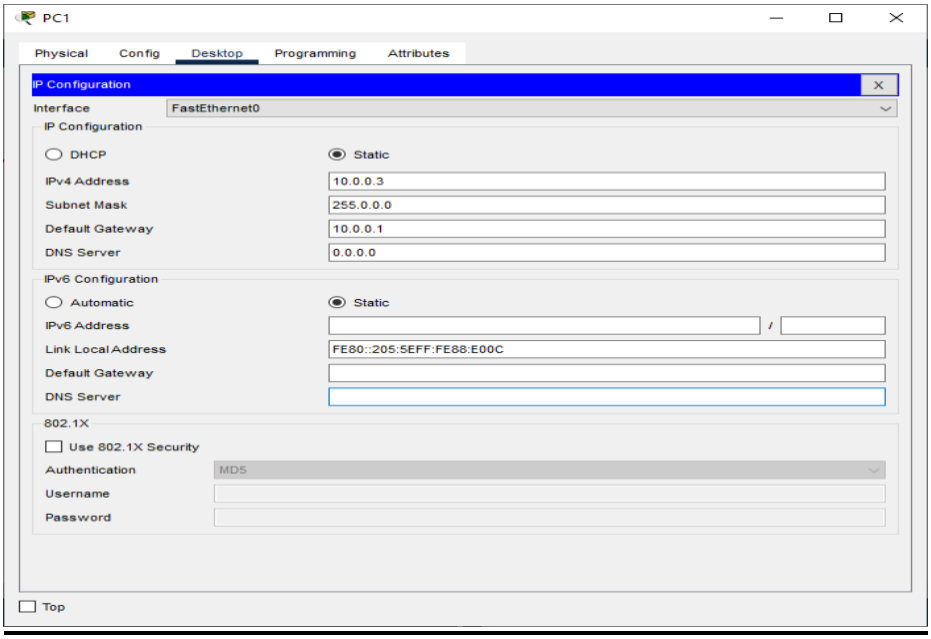
Adding Serial Interface in each Router



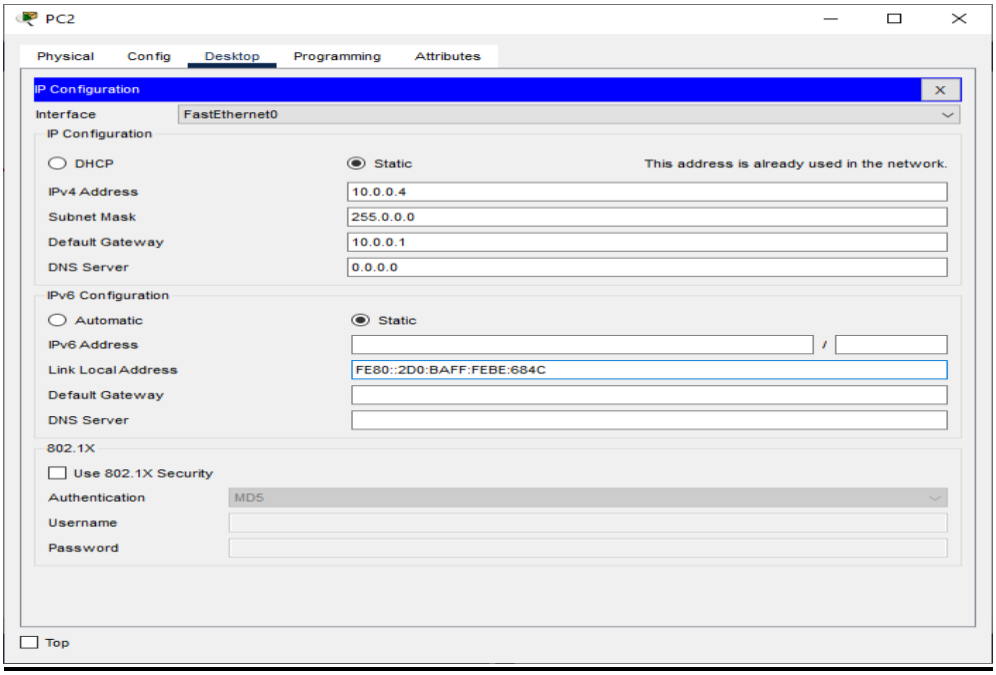
Configuring PC0:

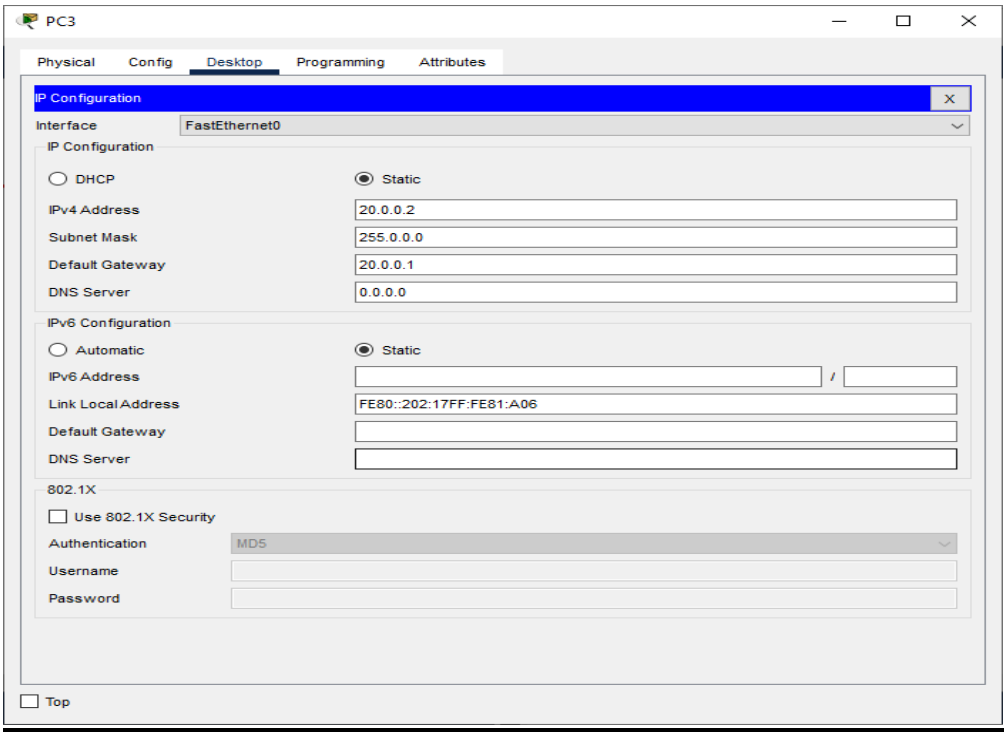


Configuring PC1:

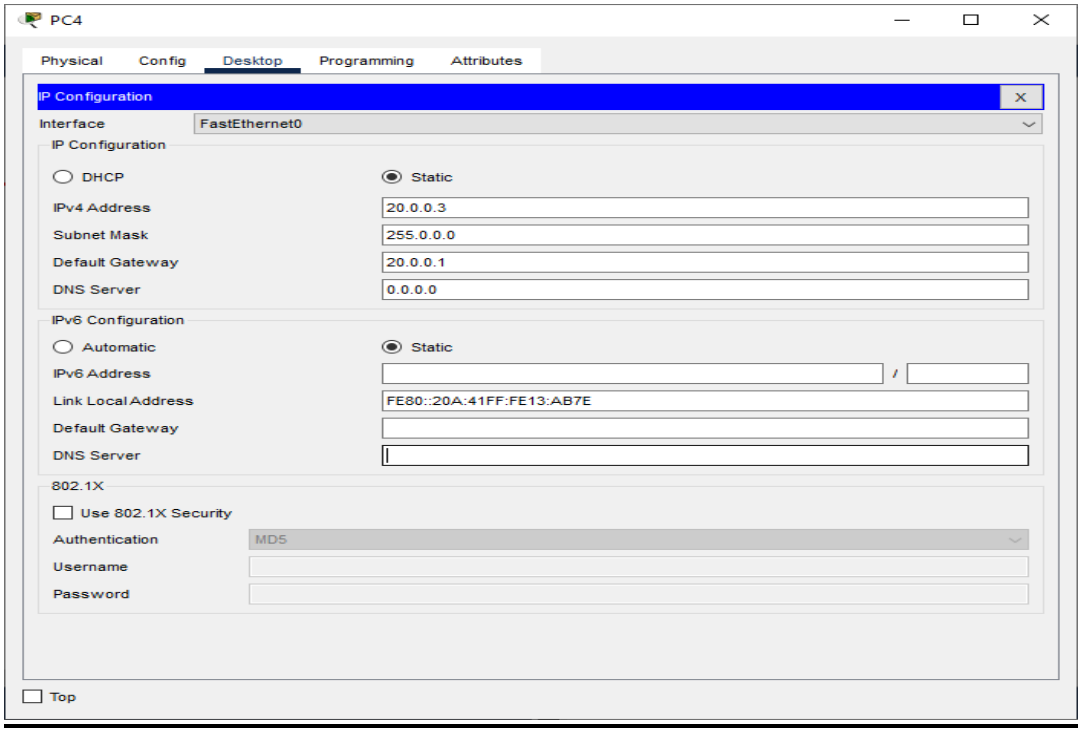


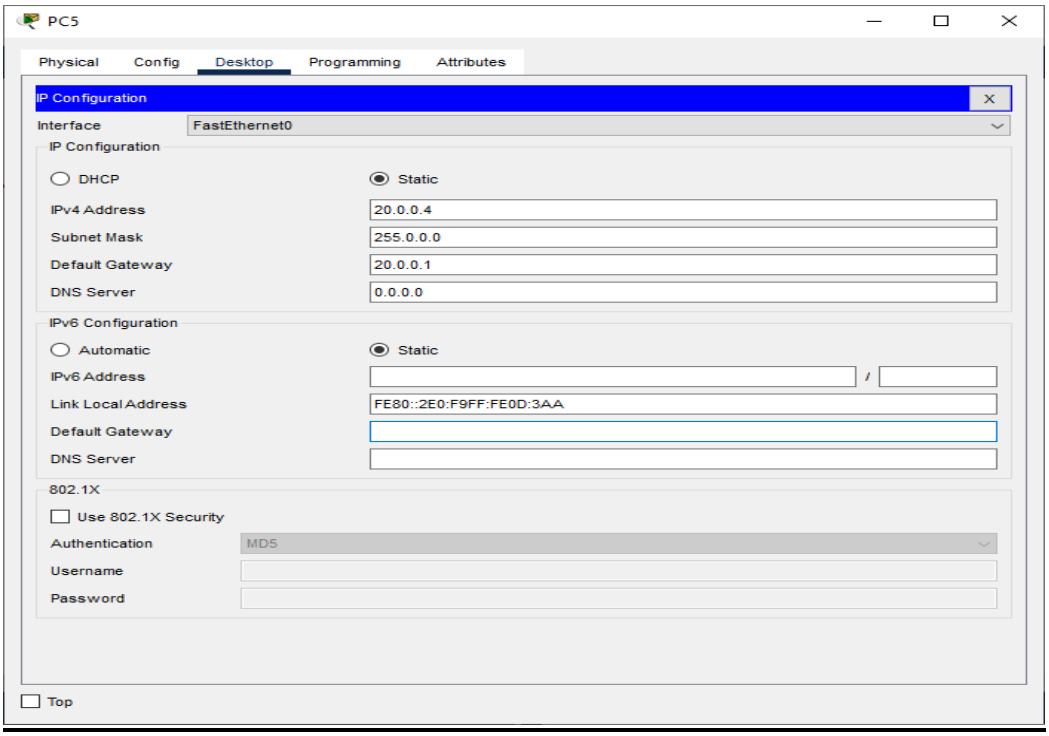
Configuring PC2:



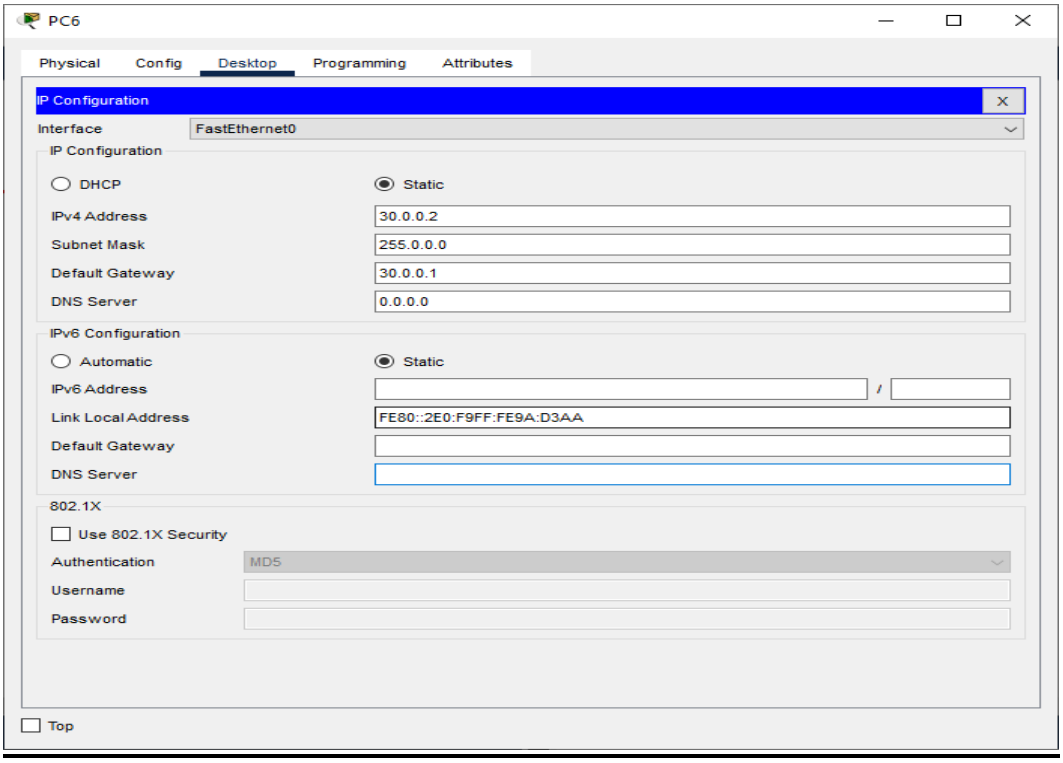


Configuring PC4:

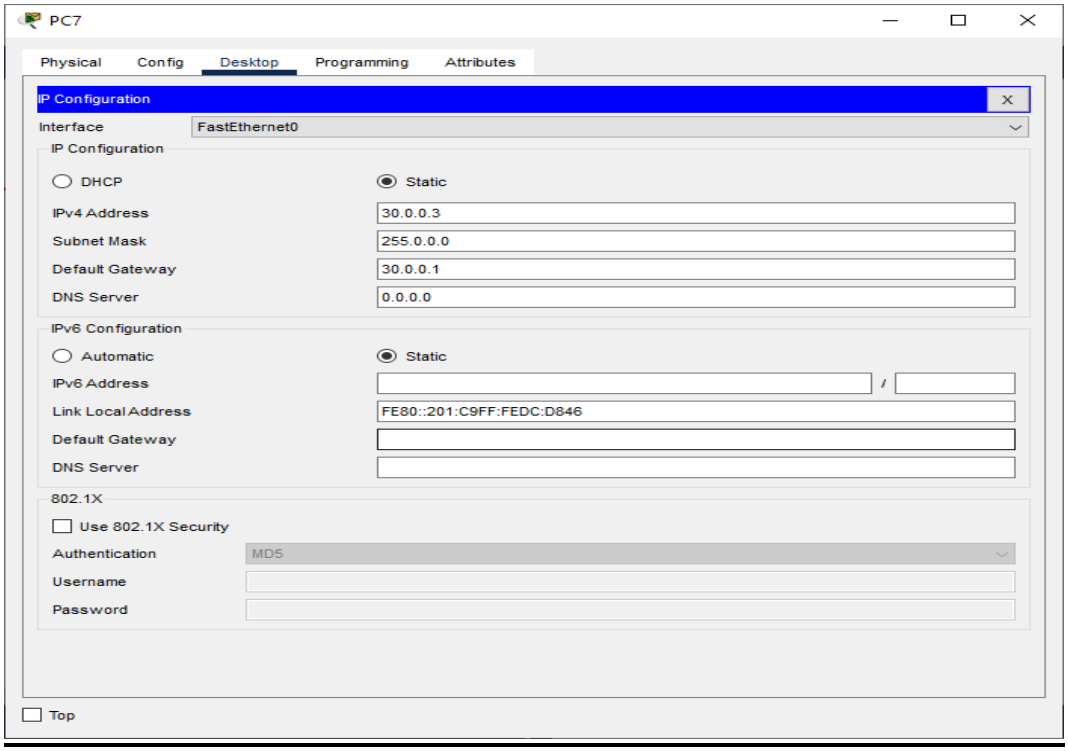




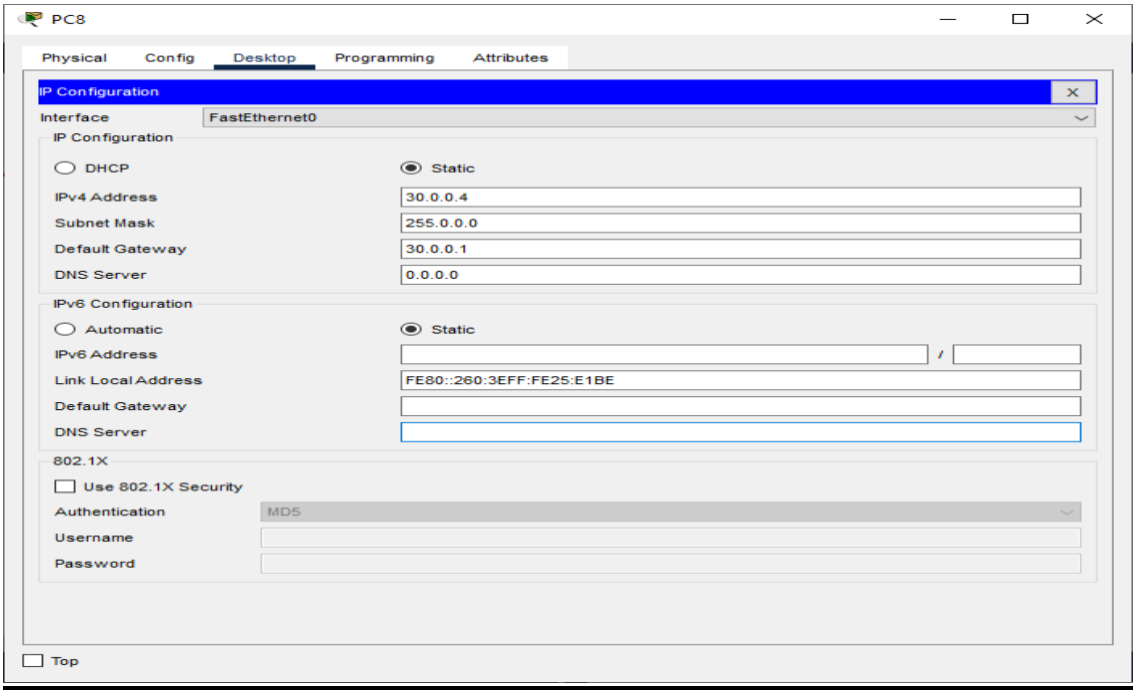
Configuring PC6:



Configuring PC7:



Configuring PC8:



Configuring Router 0 (using the CLI mode)

```
Router>en
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/1/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
Router#
```

Configuring Router 1 (using the CLI mode)

```
Router>enable
Router#configure terminal
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 20.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#interface serial 0/1/0
Router(config-if)#ip address 192.168.0.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#interface serial 0/1/1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
```

Configuring Router 2 (using the CLI mode)

```
Router>enable
Router#configure terminal
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 30.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#interface serial 0/1/1
Router(config-if)#ip address 192.168.1.2 255.255.255.0
Router(config-if)#no shutdown
```

Setting the RIPv1 on Router 0

```
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#network 10.0.0.0
Router(config-router)#network 192.168.0.0
Router(config-router)#exit
```

Setting the RIPv1 on Router 1

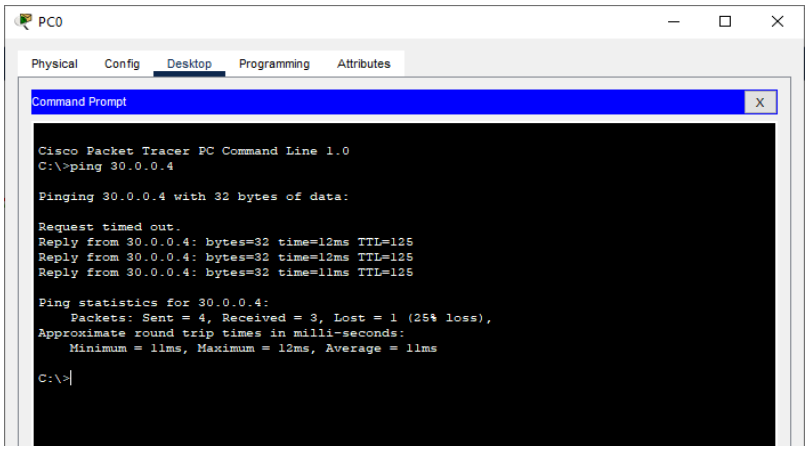
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 192.168.0.0
Router(config-router)#network 20.0.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#
Router#
```

Setting the RIPv1 on Router 2

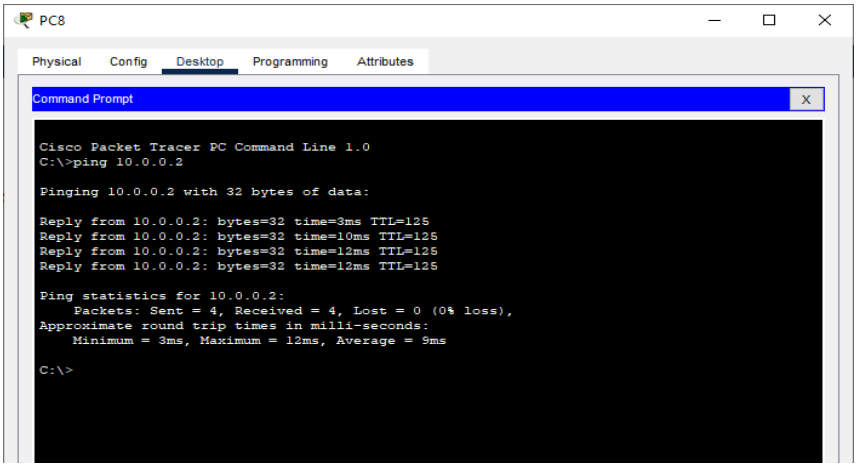
```
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#network 192.168.1.0
Router(config-router)#network 30.0.0.0
Router(config-router)#exit
Router(config)#
```

Checking the connectivity by using the ping command

Pinging PC8 (ip address 30.0.0.4) from PC0



Pinging PC0 (ip address 10.0.0.2) from PC8



Result:

Hence the RIPv1 has been studied and verified through the given network

Practical No 6

Aim: Using Packet Tracer to create a network with three routers with RIPv2 andeach router associated network will have minimum three PC and show the connectivity

Theory:

RIPv2 is an enhancement to the original RIP protocol developed in 1994. RIPv2 isalso a distance vector routing protocol but has a few enhancements to make it moreefficient than RIPv1.
RIPv2 is more efficient than RIPv1, but is not suitable for larger, more complexnetworks. It simply provides more flexibility on smaller networks.
RIPv2 uses the same routing metric as RIPv1, the hop count. Updates with RIPv2are sent via multicasts and not broadcasts. RIPv2 can also be configured to do classless routing. When configured for classless routing, RIPv2 will transmit submit masks when it sends routing updates. This allows for the use of subnettingand discontiguous networks.
RIPv2 allows for authentication to be required for updates. When authentication isenabled, each router is configured with the RIP update password. The password sent with the RIP update must match the password configured on the destination router. If the passwords do not match, then the receiving router will not process theupdate.

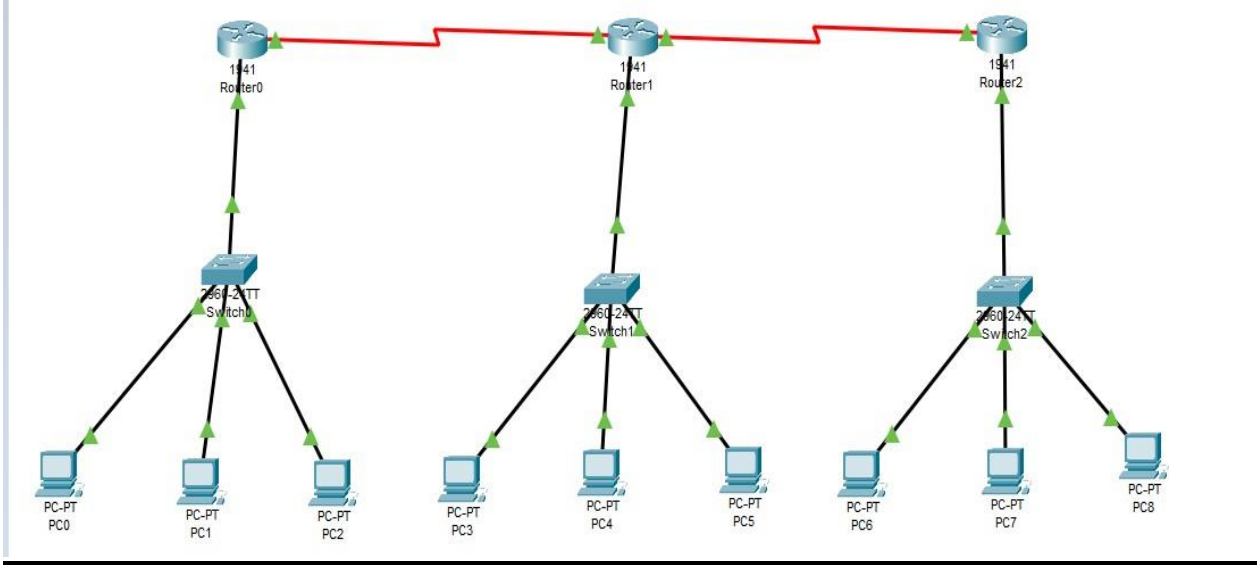
Advantages of RIPv2

1) It's a standardized protocol.
2) It's VLSM compliant.
3) Provides fast convergence.
4) It sends triggered updates when the network changes.
5) Works with snapshot routing – making it ideal for dial networks.

Disadvantage of RIPv2

1) Max hop count of 15, due to the 'count-to-infinity' vulnerability.
2) No concept of neighbors.
3) Exchanges entire table with all neighbors every 30 seconds (except in the case of a triggered update).

We use the following topology for the present case

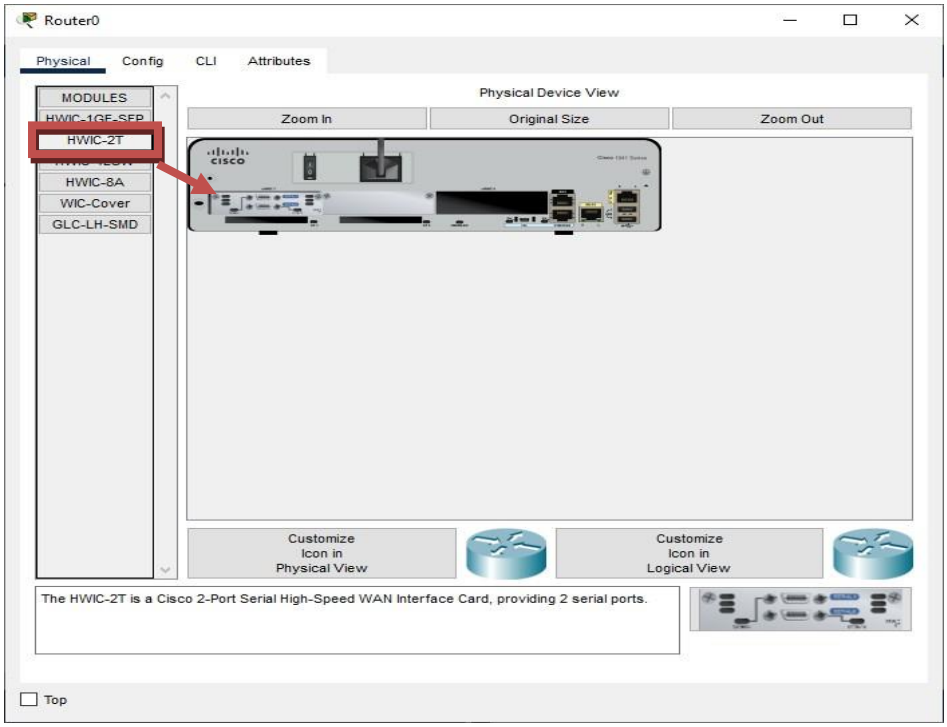


We configure the above network using the following IP addresses

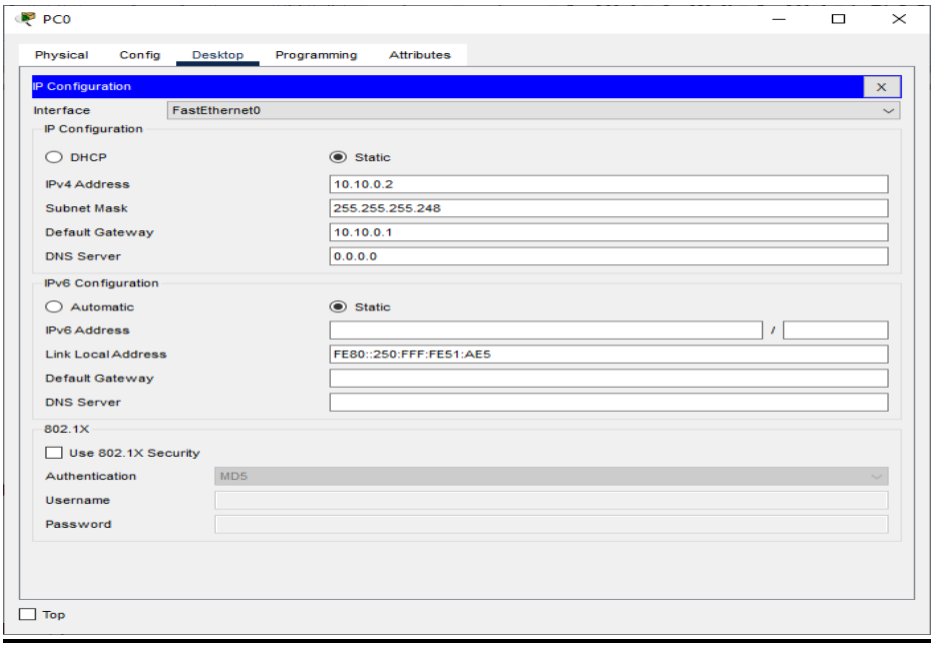
Host	Interface	IP address	Subnet Mask	Network Address	Default Gateway
Router 0	G0/0	10.10.0.1	255.255.255.248	10.10.0.0	
	S0/1/0	192.168.0.1	255.255.255.252	192.168.0.0	
Router 1	G0/0	10.20.0.1	255.255.255.248	10.20.0.0	
	S0/1/0	192.168.0.2	255.255.255.252	192.168.0.0	
	S0/1/1	192.168.1.1	255.255.255.252	192.168.1.0	
Router 2	G0/0	10.30.0.1	255.255.255.248	10.30.0.0	
	S0/1/1	192.168.1.2	255.255.255.252	192.168.1.0	
PC0	FastEthernet 0	10.10.0.2	255.255.255.248	10.10.0.0	10.10.0.1
PC1	FastEthernet 0	10.10.0.3	255.255.255.248	10.10.0.0	10.10.0.1
PC2	FastEthernet 0	10.10.0.4	255.255.255.248	10.10.0.0	10.10.0.1
PC3	FastEthernet 0	10.20.0.2	255.255.255.248	10.20.0.0	10.20.0.1
PC4	FastEthernet 0	10.20.0.3	255.255.255.248	10.20.0.0	10.20.0.1
PC5	FastEthernet	10.20.0.4	255.255.255.248	10.20.0.0	10.20.0.1

	0				
PC6	FastEthernet 0	10.30.0.2	255.255.255.248	10.30.0.0	10.30.0.1
PC7	FastEthernet 0	10.30.0.3	255.255.255.248	10.30.0.0	10.30.0.1
PC8	FastEthernet 0	10.30.0.4	255.255.255.248	10.30.0.0	10.30.0.1

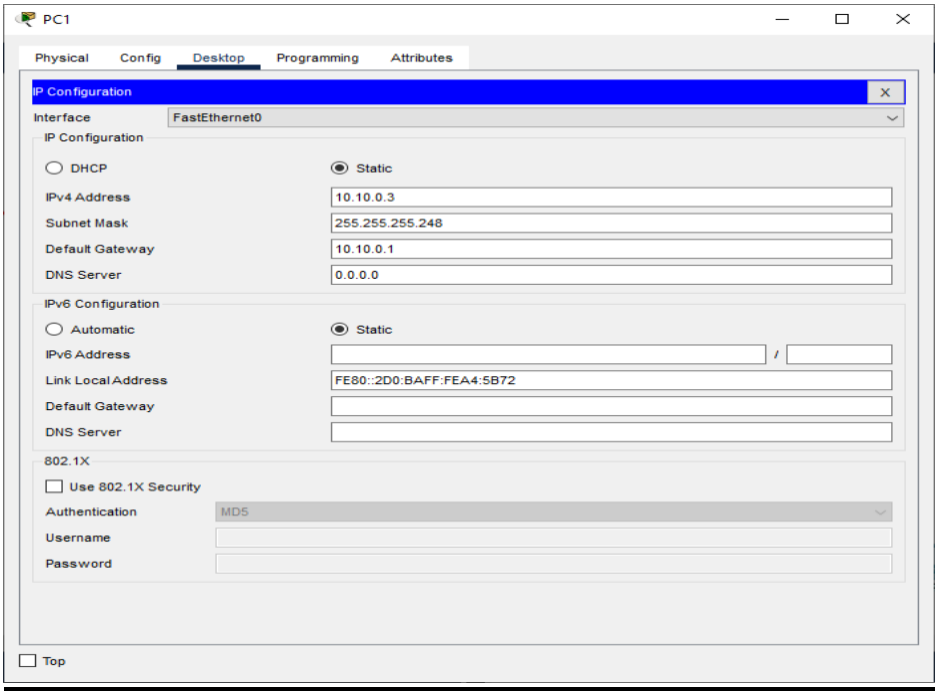
Adding Serial Interface in each Router



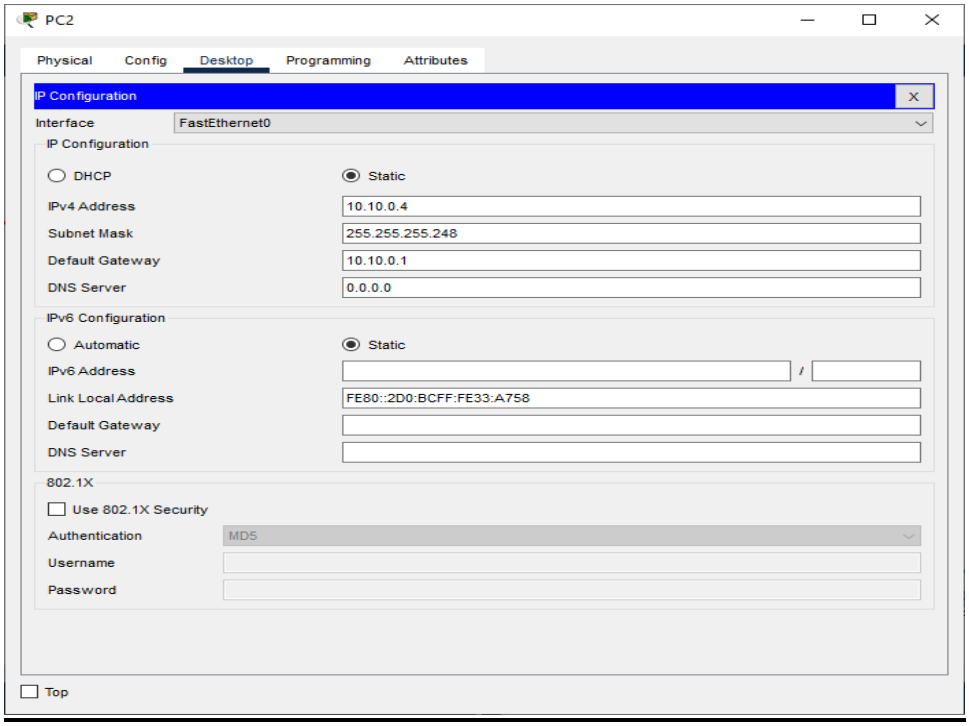
Configuring PC0:



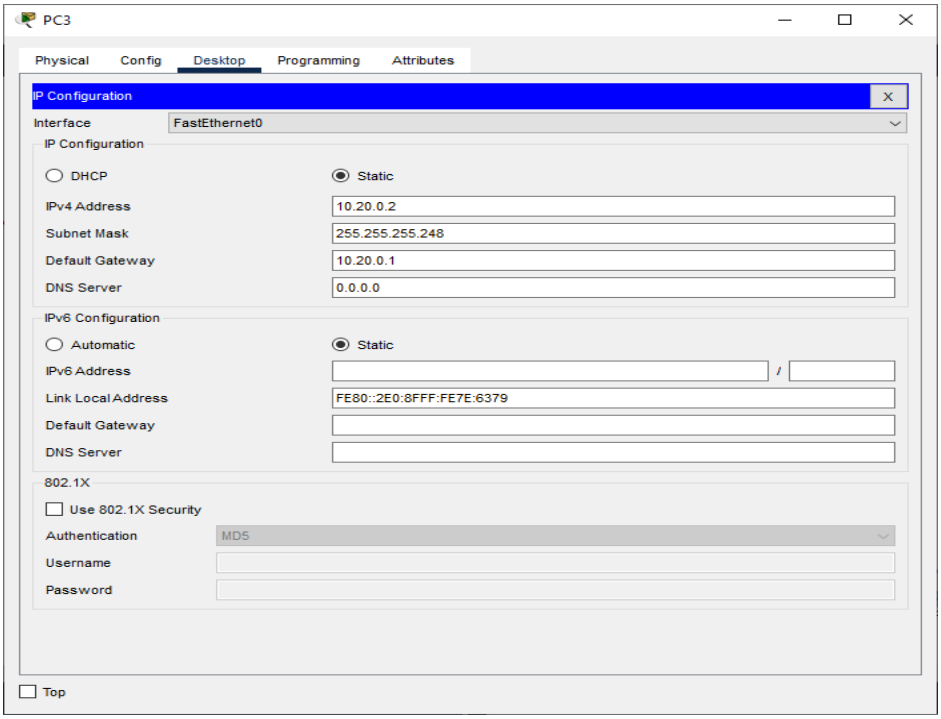
Configuring PC1:



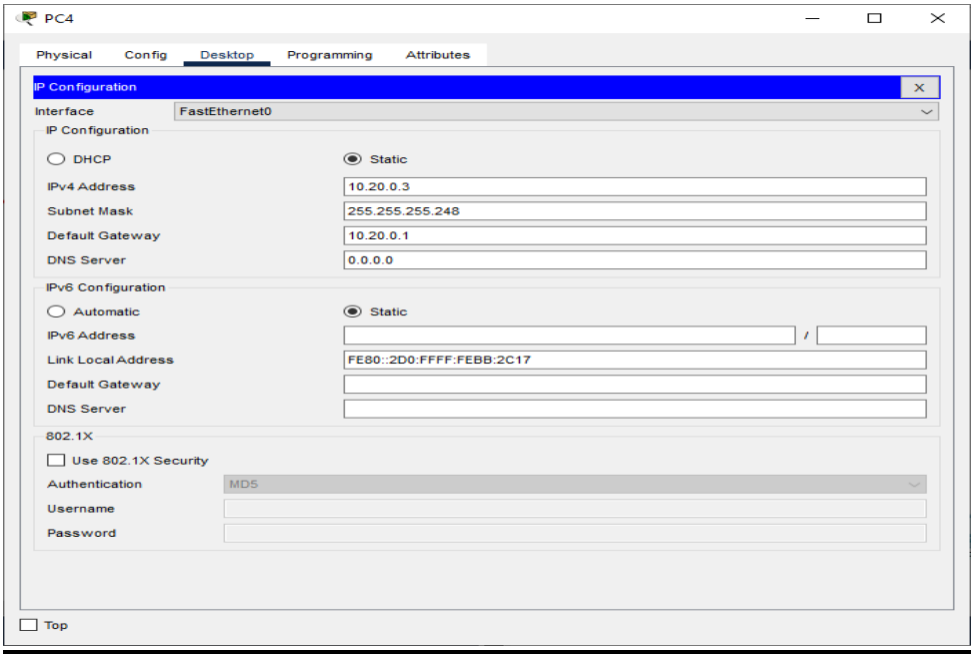
Configuring PC2:

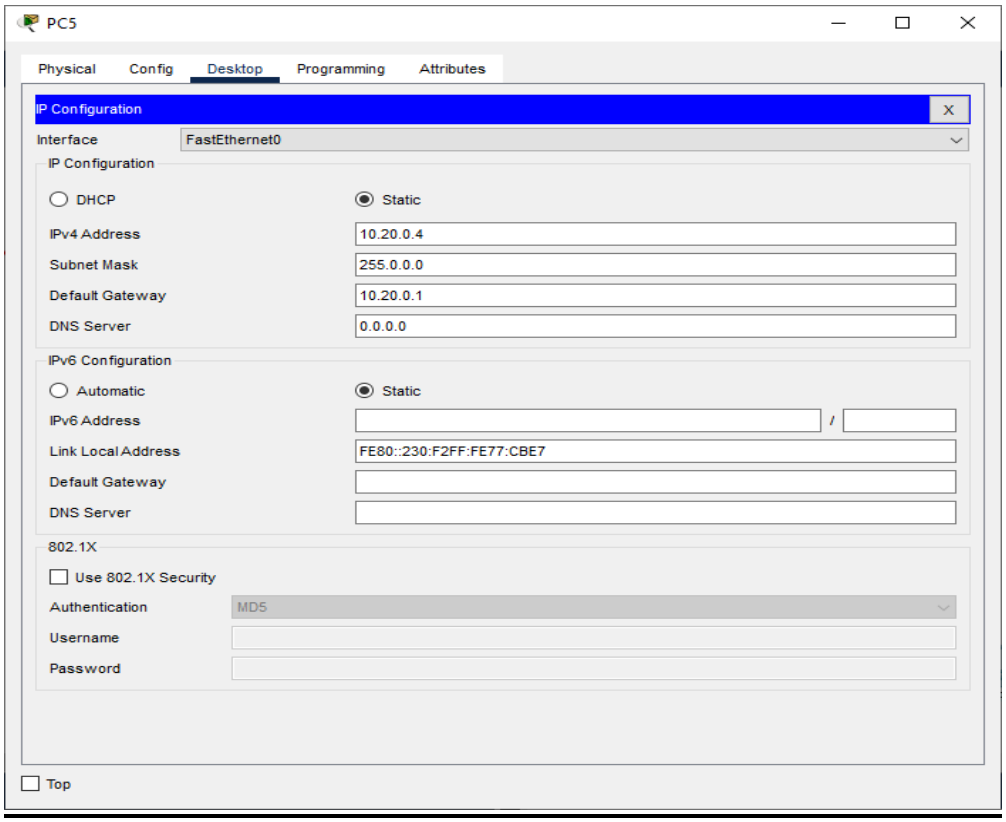


Configuring PC3:

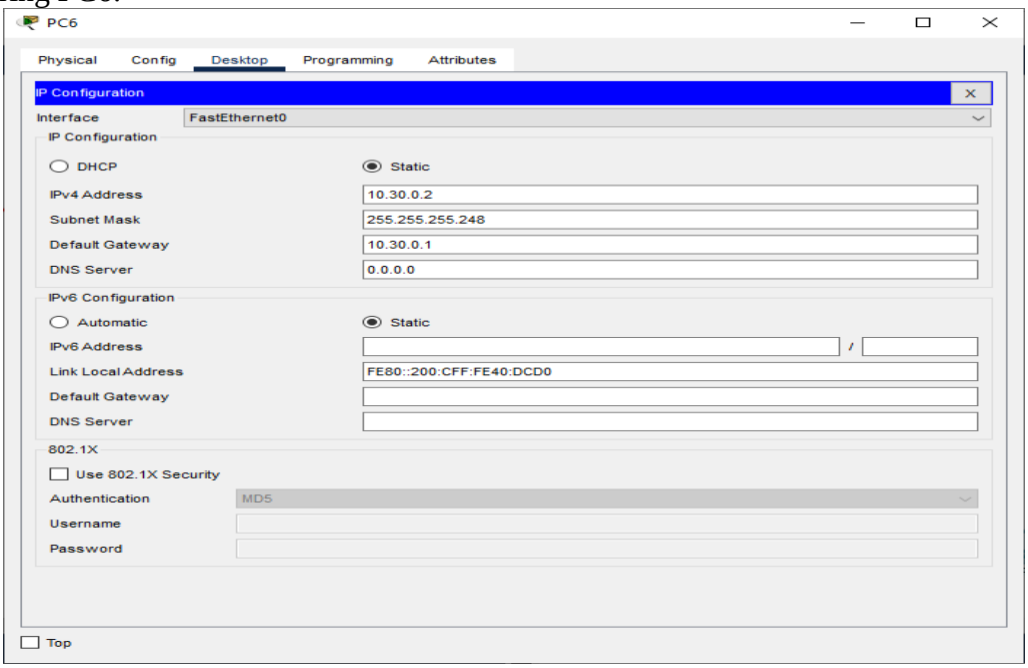


Configuring PC4:

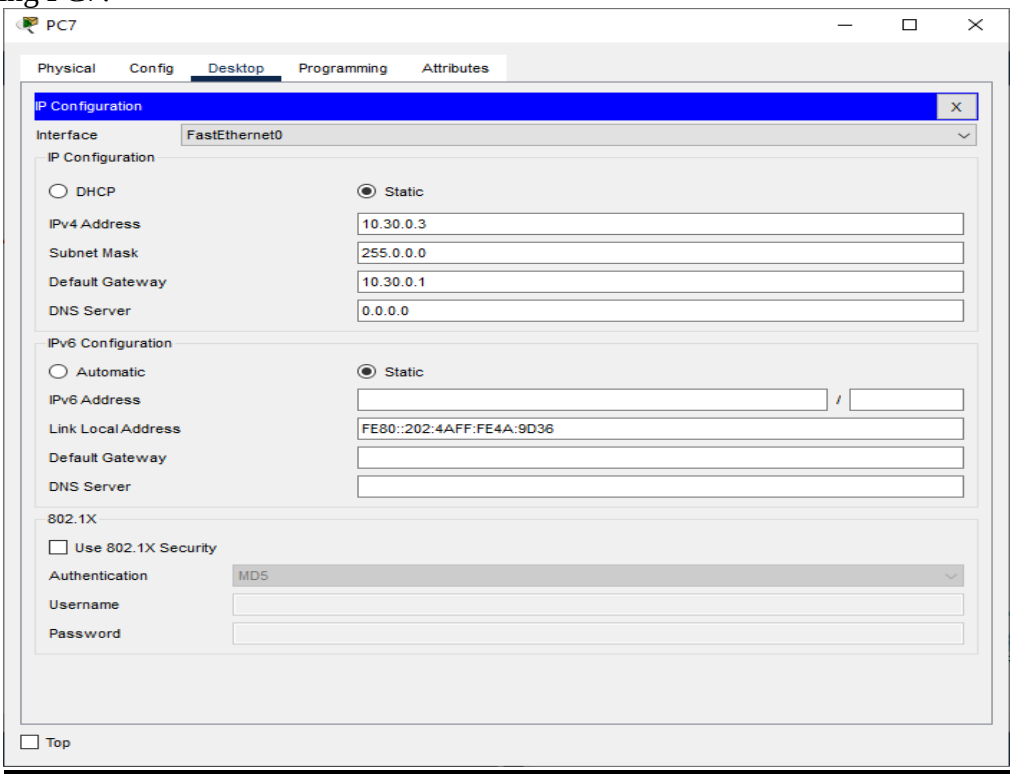




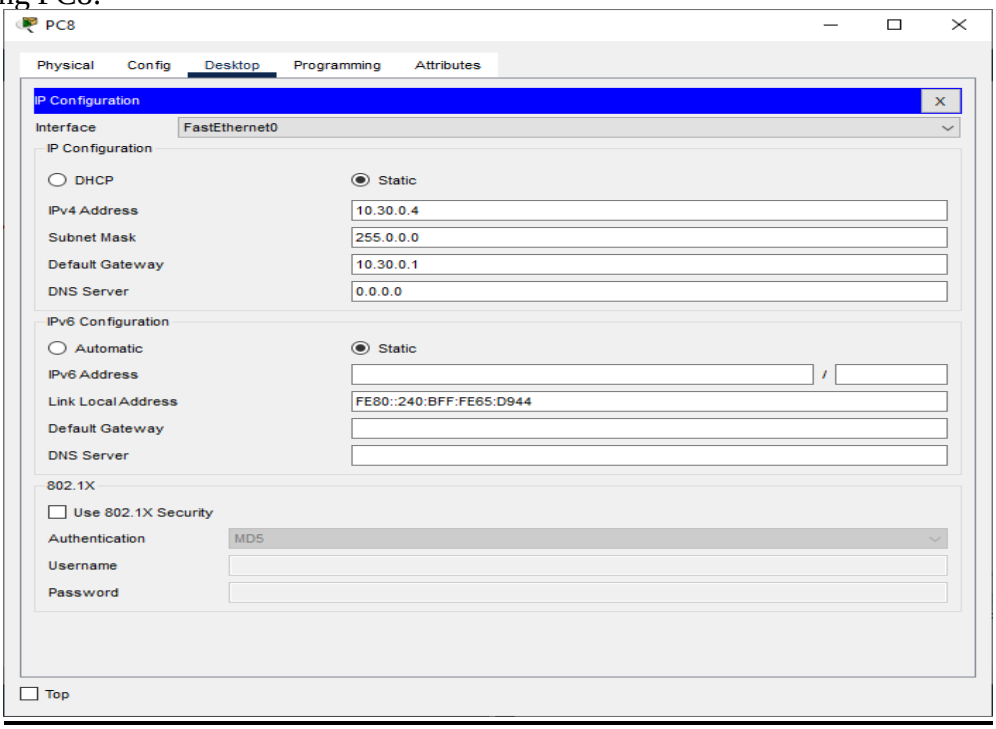
Configuring PC6:



Configuring PC7:

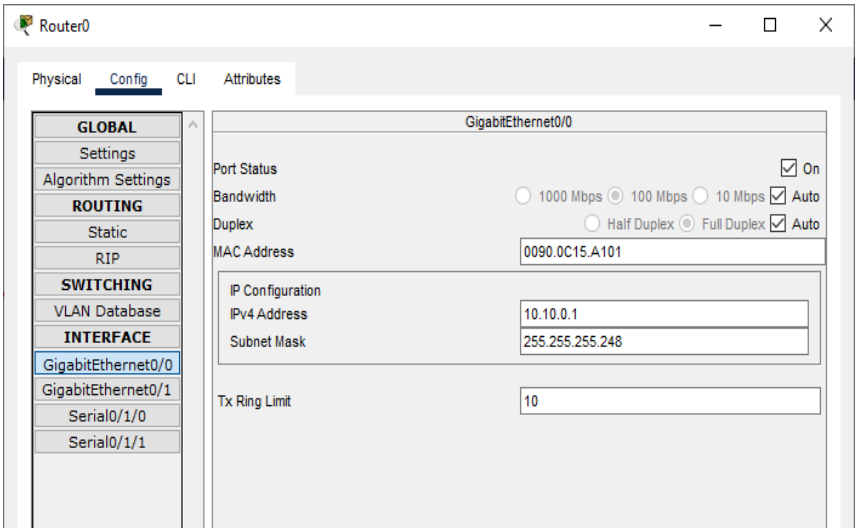


Configuring PC8:

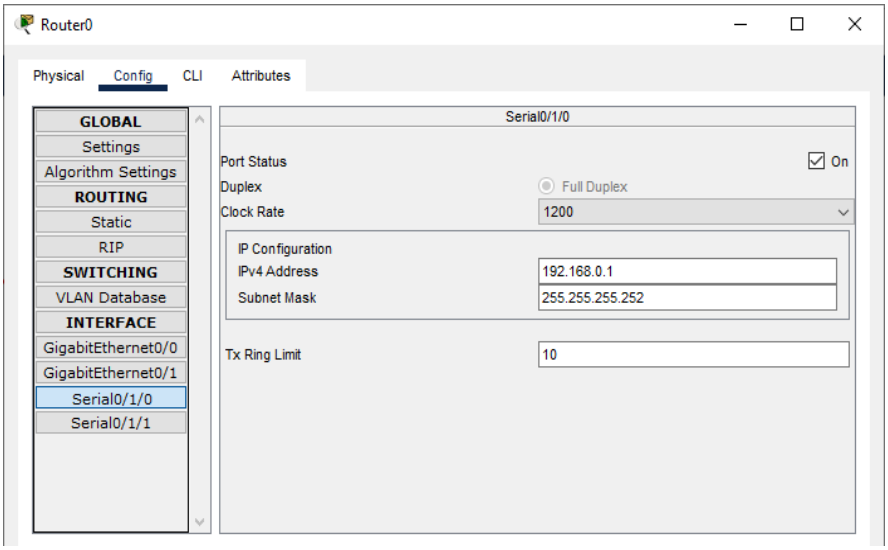


Configuring IP addresses on Router 0

i) Interface G0/0

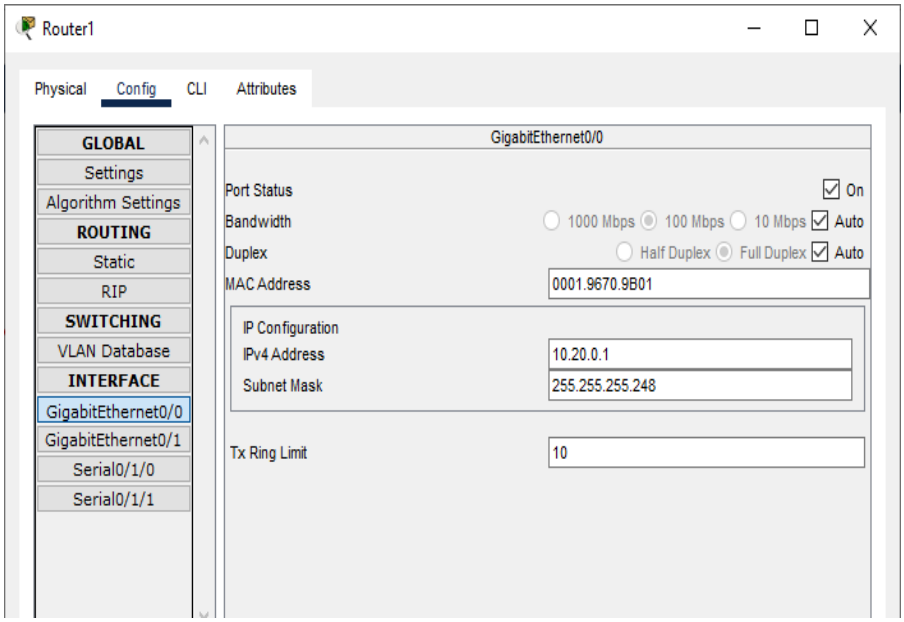


ii) Interface S0/1/0

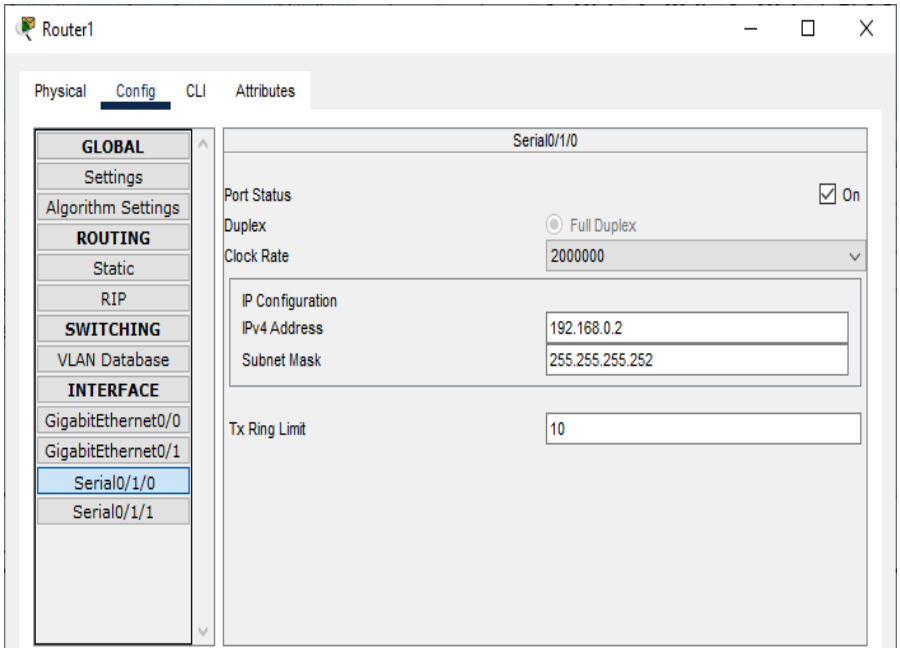


Configuring IP addresses on Router 1

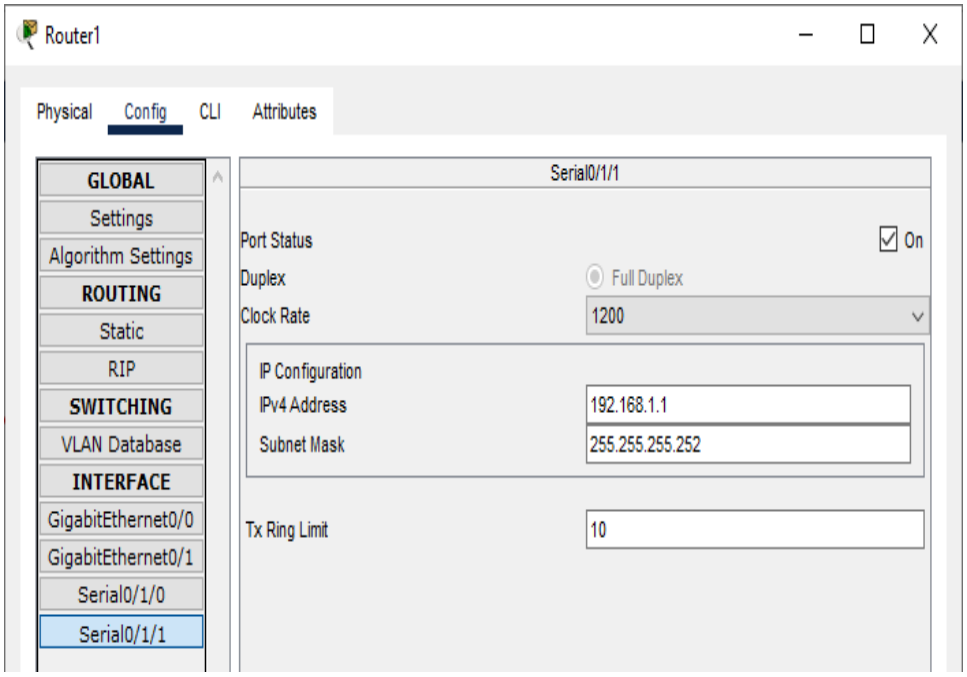
i) Interface G0/0



ii) Interface S0/1/0

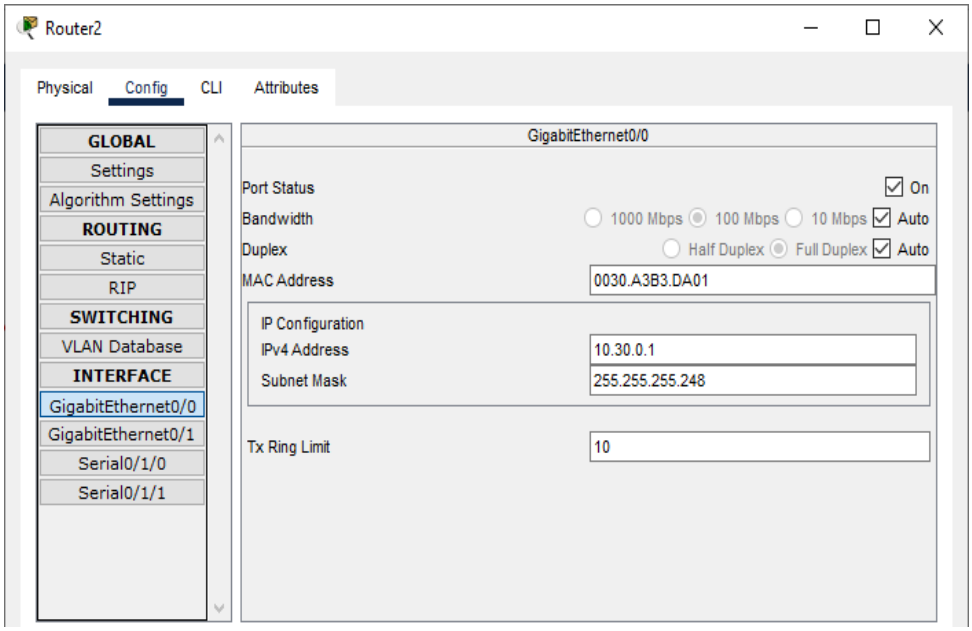


iii) Interface S0/1/1

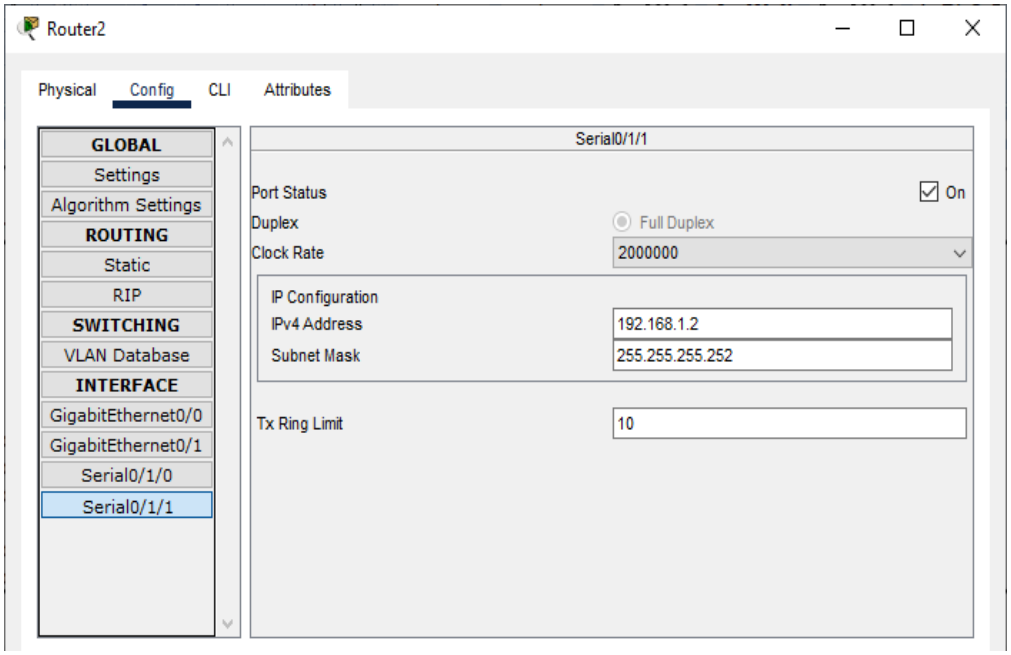


Configuring IP addresses on Router 2

i) Interface G0/0



ii) Interface S0/1/1



Configuring Router 0 for RIPv2 (using the CLI mode)

```
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.10.0.0
Router(config-router)#network 192.168.0.0
Router(config-router)#exit
Router(config)#
```

Configuring Router 1 for RIPv2 (using the CLI mode)

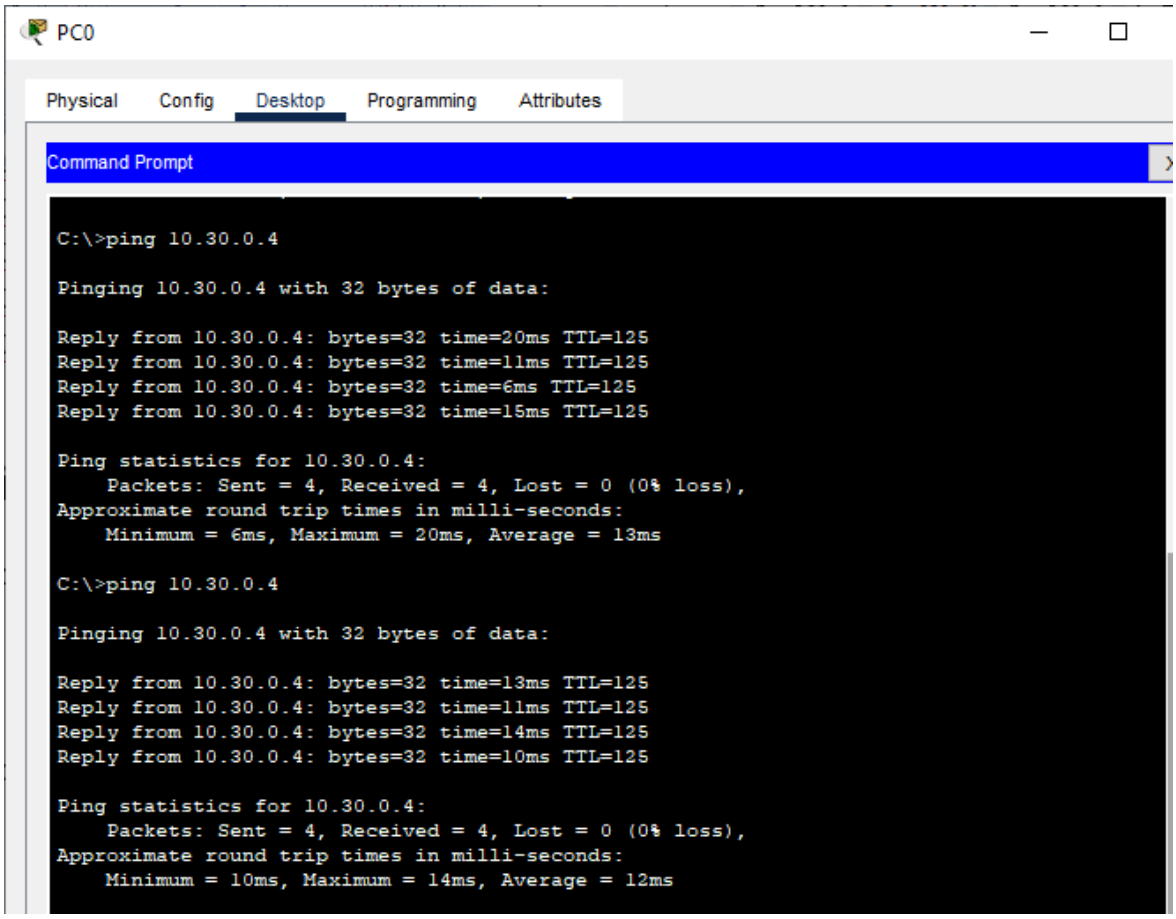
```
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.20.0.0
Router(config-router)#network 192.168.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#
```

Configuring Router 2 for RIPv2 (using the CLI mode)

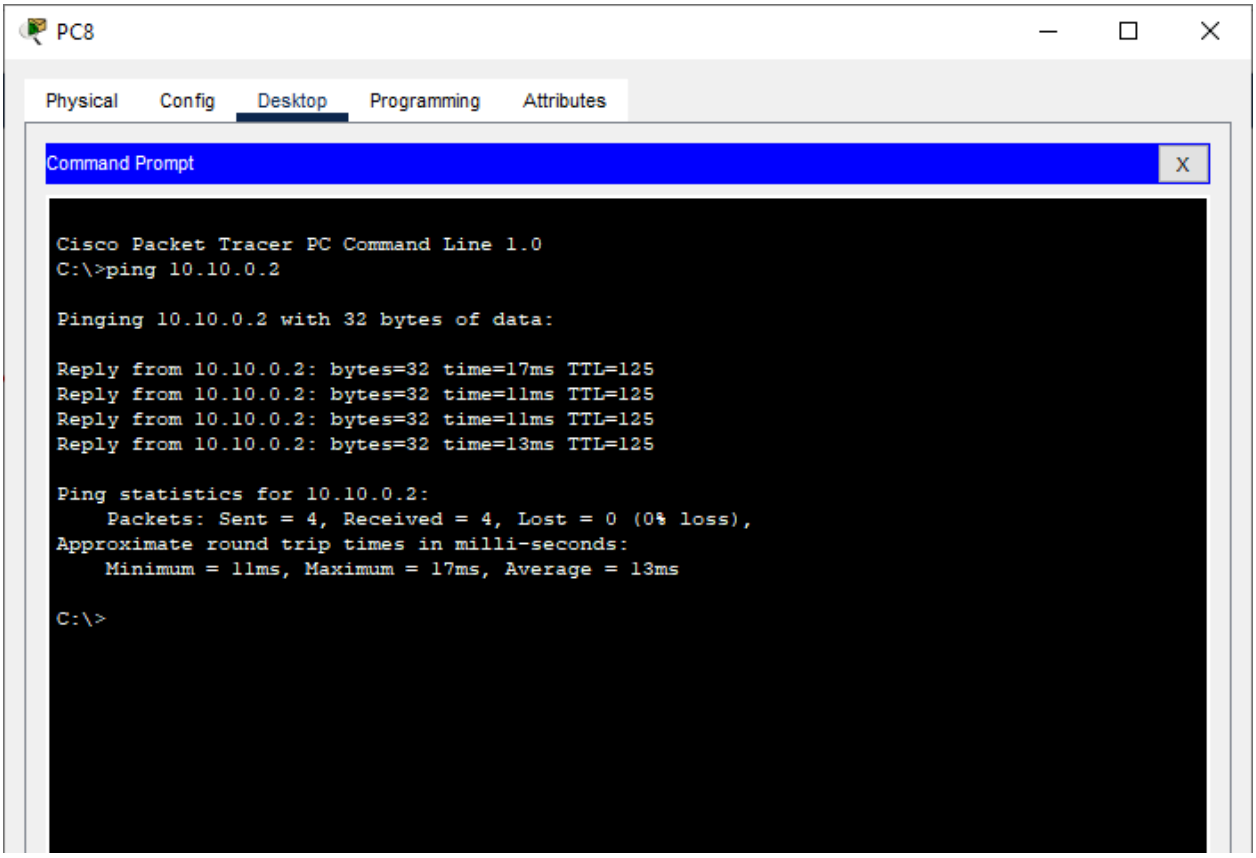
```
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.30.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#
```

Checking the connectivity by using the ping command

i) Pinging PC8 (ip address 10.30.0.4) from PC0



ii) Pinging PC0 (ip address 10.10.0.2) from PC8



Result:

Hence the RIPv2 has been studied and verified through the given network

Practical No 7

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

Theory:

Open shortest path first (OSPF) is a link-state routing protocol that is used to findthe best path between the source and the destination router using its own shortest path first (SPF) algorithm. A link-state routing protocol is a protocol that uses theconcept of triggered updates, i.e., if there is a change observed in the learned routing table then the updates are triggered only, not like the distance-vector routing protocol where the routing table is exchanged at a period of time.

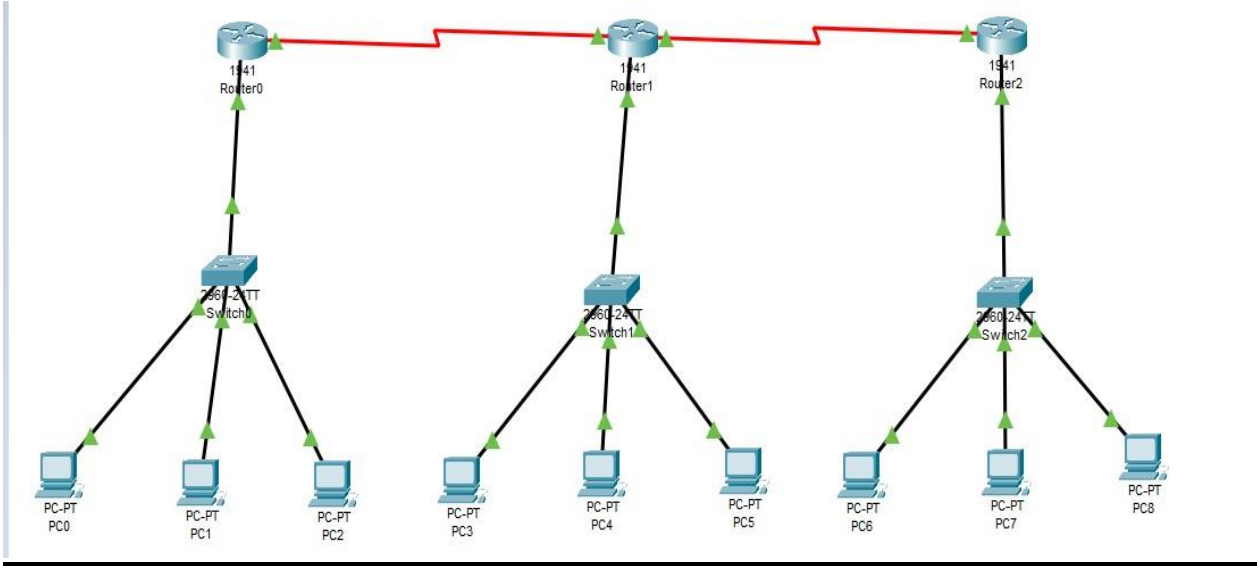
Open shortest path first (OSPF) is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e., the protocol which aimsat moving the packet within a large autonomous system or routing domain.

OSPF advantages –

1. Both IPv4 and IPv6 routed protocols
2. Load balancing with equal-cost routes for the same destination
3. Unlimited hop counts
4. Trigger updates for fast convergence
5. A loop-free topology using SPF algorithm
6. Run-on most routers
7. Classless protocol

There are some disadvantages of OSPF like, it requires an extra CPU process torun the SPF algorithm, requiring more RAM to store adjacency topology, and being more complex to set up and hard to troubleshoot.

We use the following topology for the present case

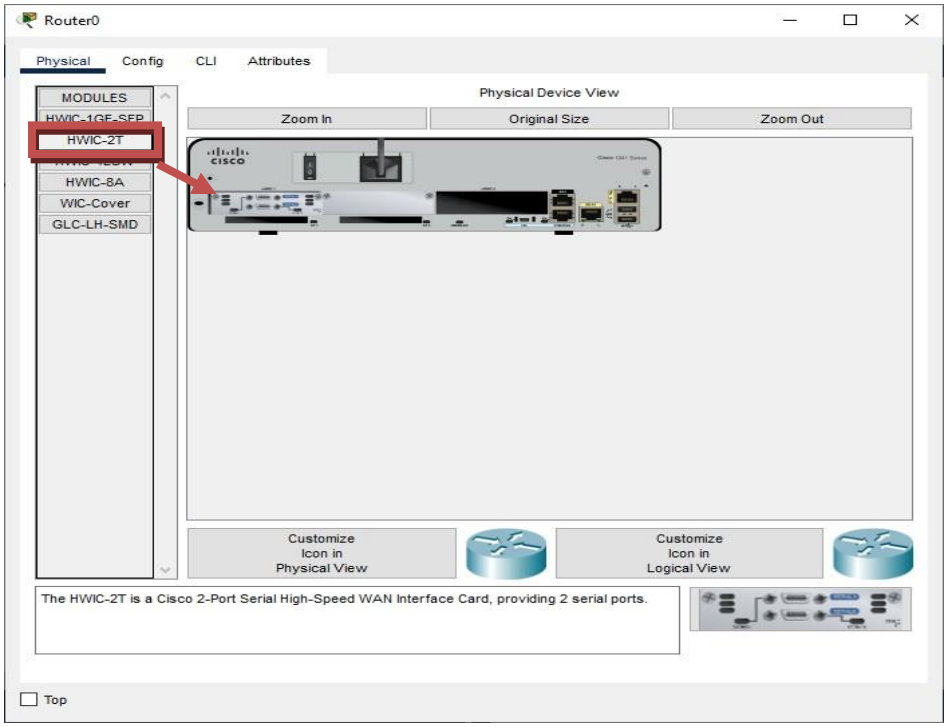


We configure the above network using the following IP addresses

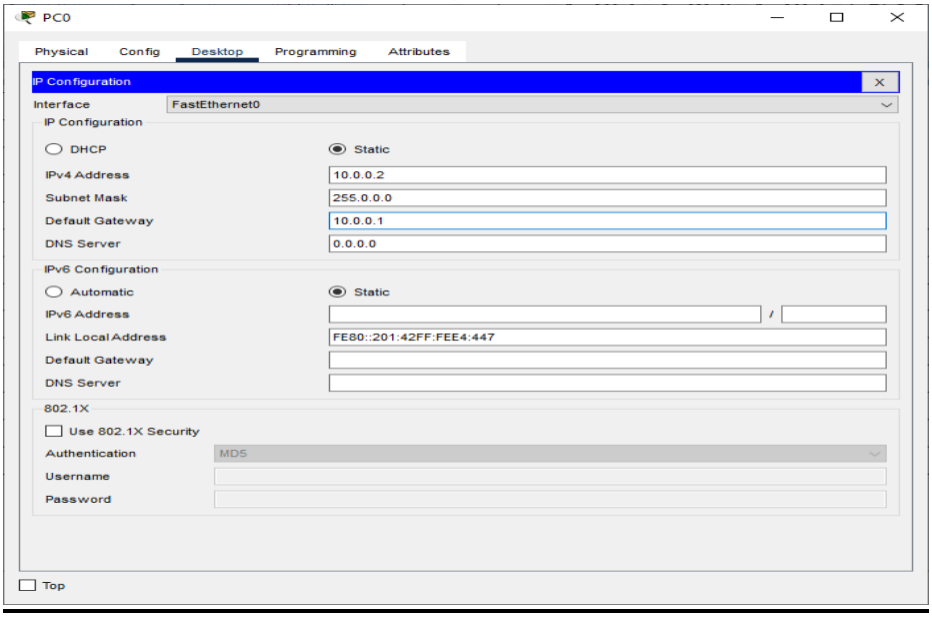
Host	Interface	IP address	Default Gateway	Subnet Mask	Wildcard Mask
Router 0	G0/0	10.0.0.1		255.0.0.0	0.255.255.255
	S0/1/0	40.0.0.1			
Router 1	G0/0	20.0.0.1			
	S0/1/0	40.0.0.2			
	S0/1/1	50.0.0.1			
Router 2	G0/0	30.0.0.1			
	S0/1/1	50.0.0.2			
PC0	FastEthernet 0	10.0.0.2	10.0.0.1		
PC1	FastEthernet 0	10.0.0.3			
PC2	FastEthernet 0	10.0.0.4			
PC3	FastEthernet 0	20.0.0.2	20.0.0.1		
PC4	FastEthernet 0	20.0.0.3			
PC5	FastEthernet 0	20.0.0.4			
PC6	FastEthernet	30.0.0.2			

	0		30.0.0.1		
PC7	FastEthernet 0	30.0.0.3			
PC8	FastEthernet 0	30.0.0.4			

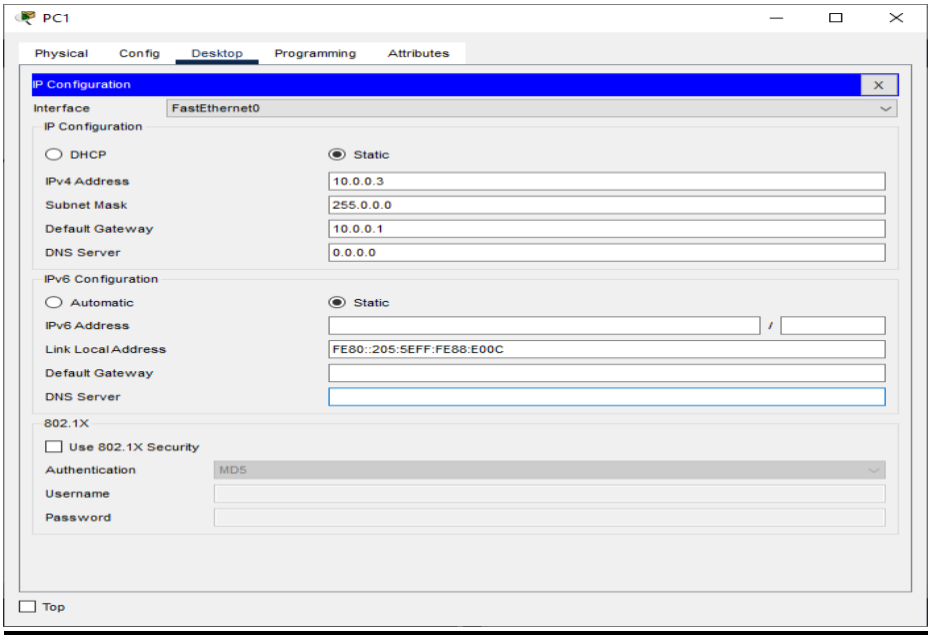
Adding Serial Interface in each Router



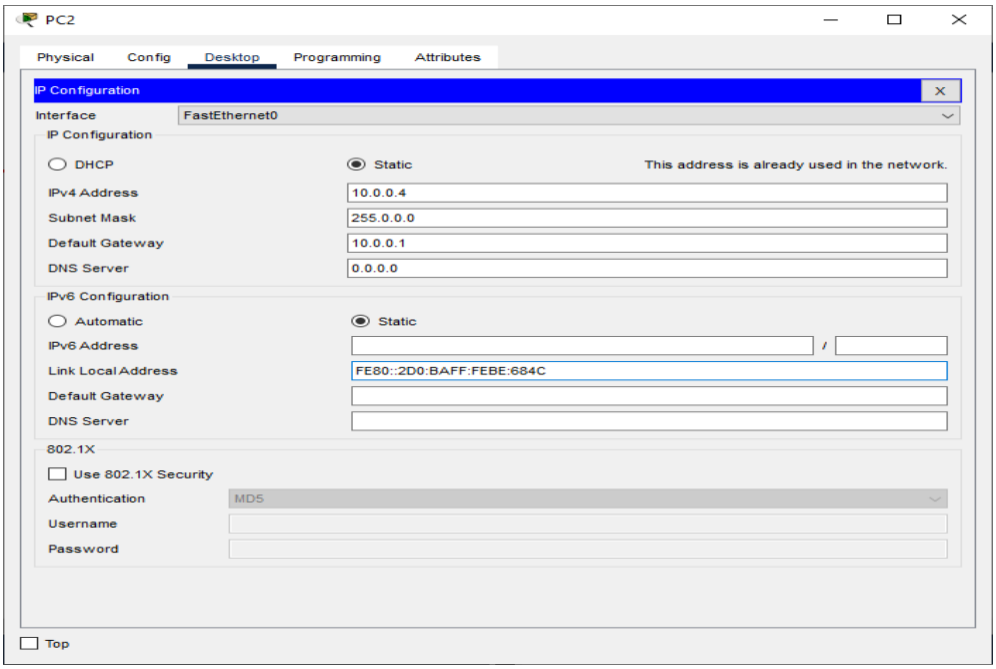
Configuring PC0:

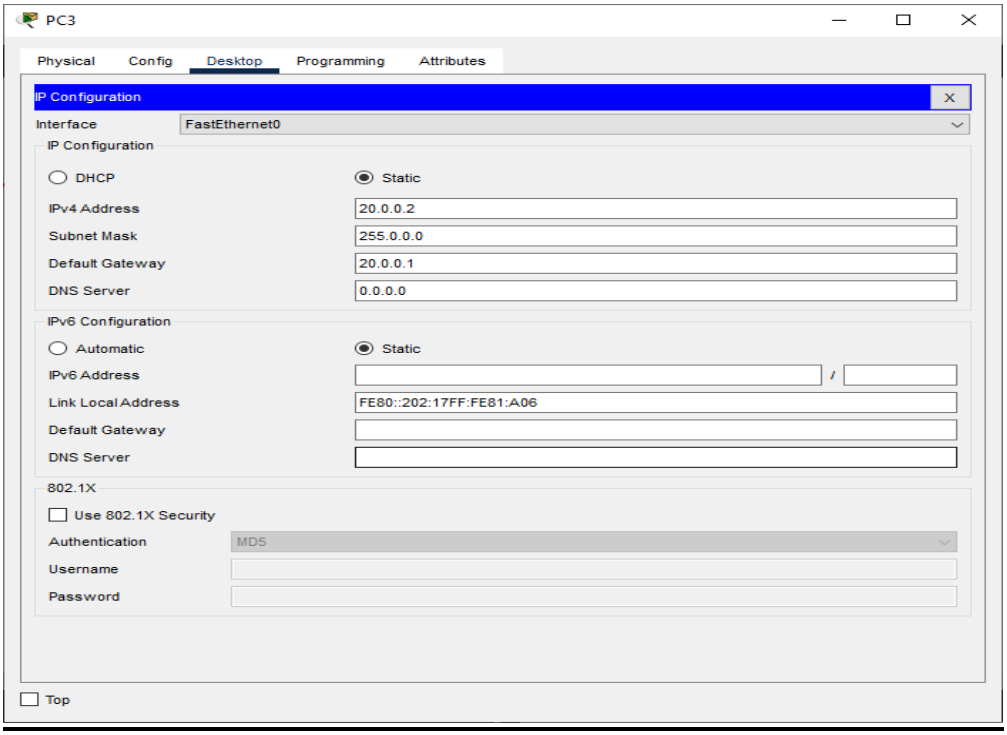


Configuring PC1:

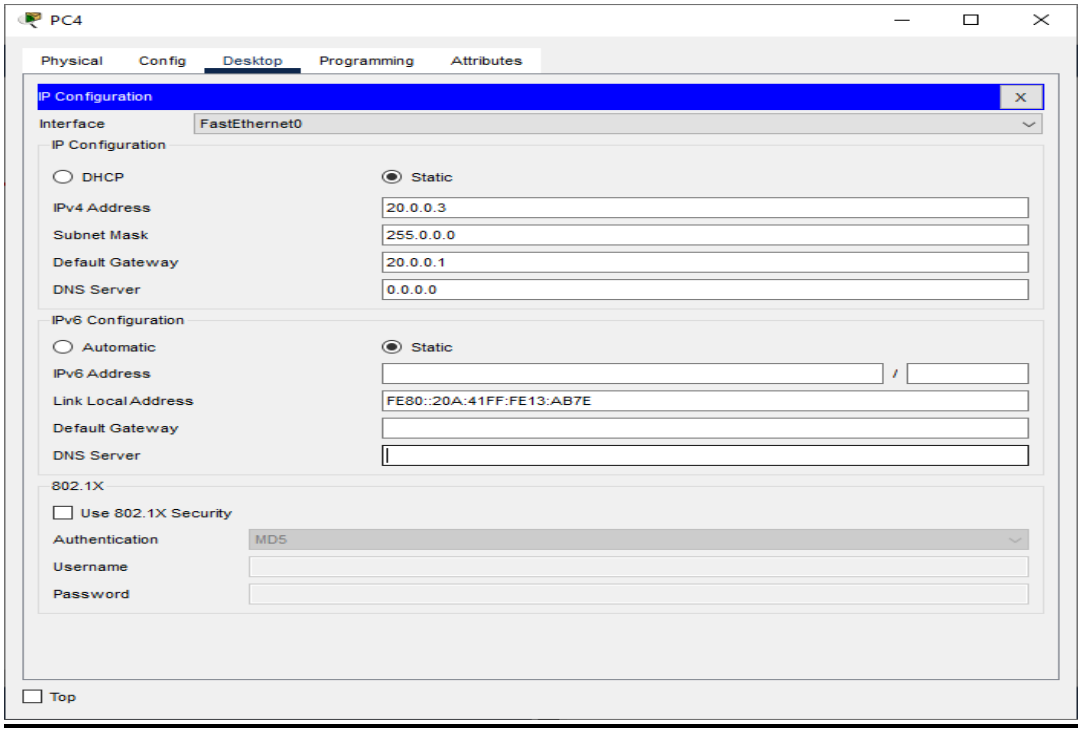


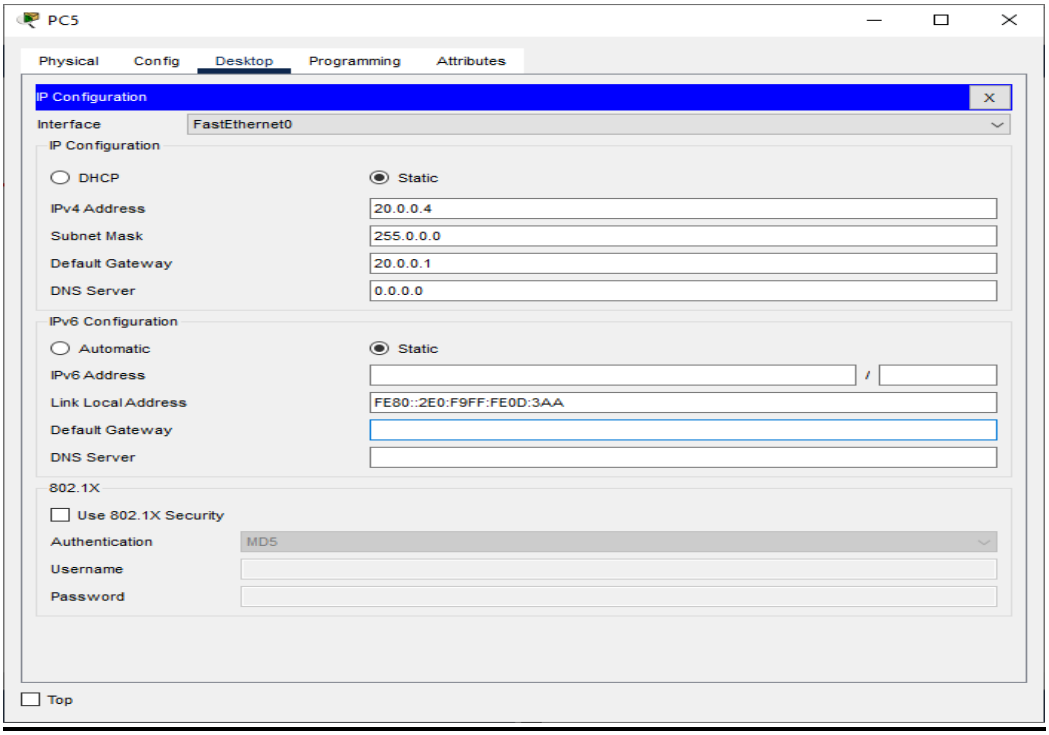
Configuring PC2:



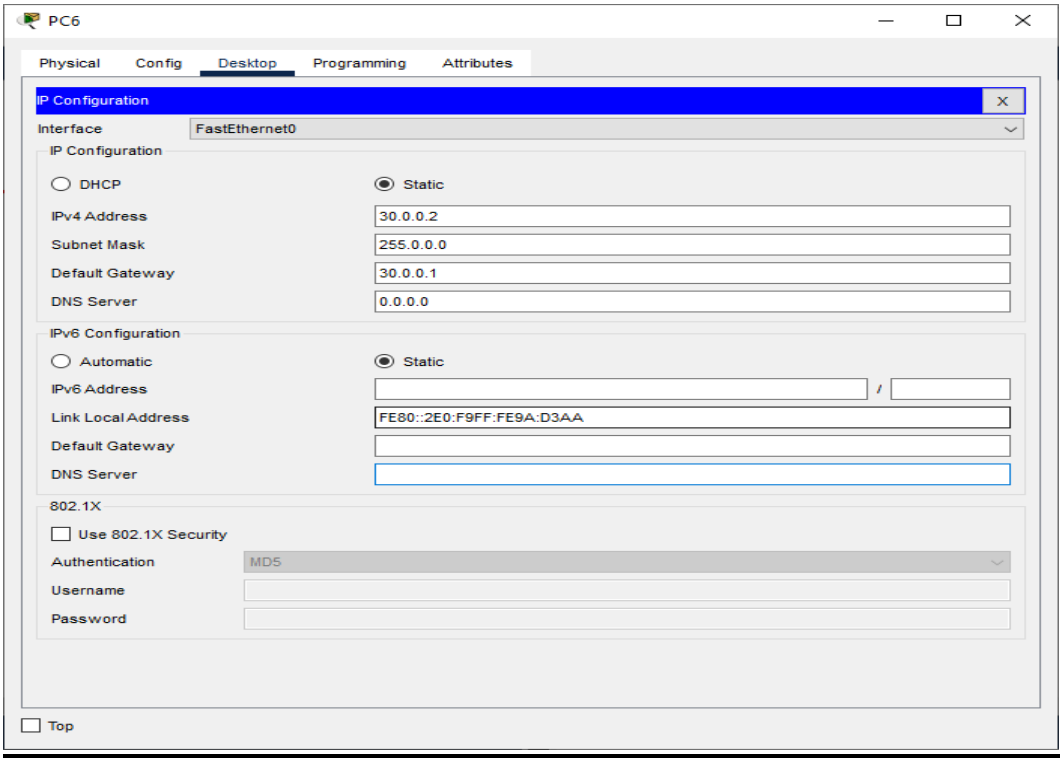


Configuring PC4:

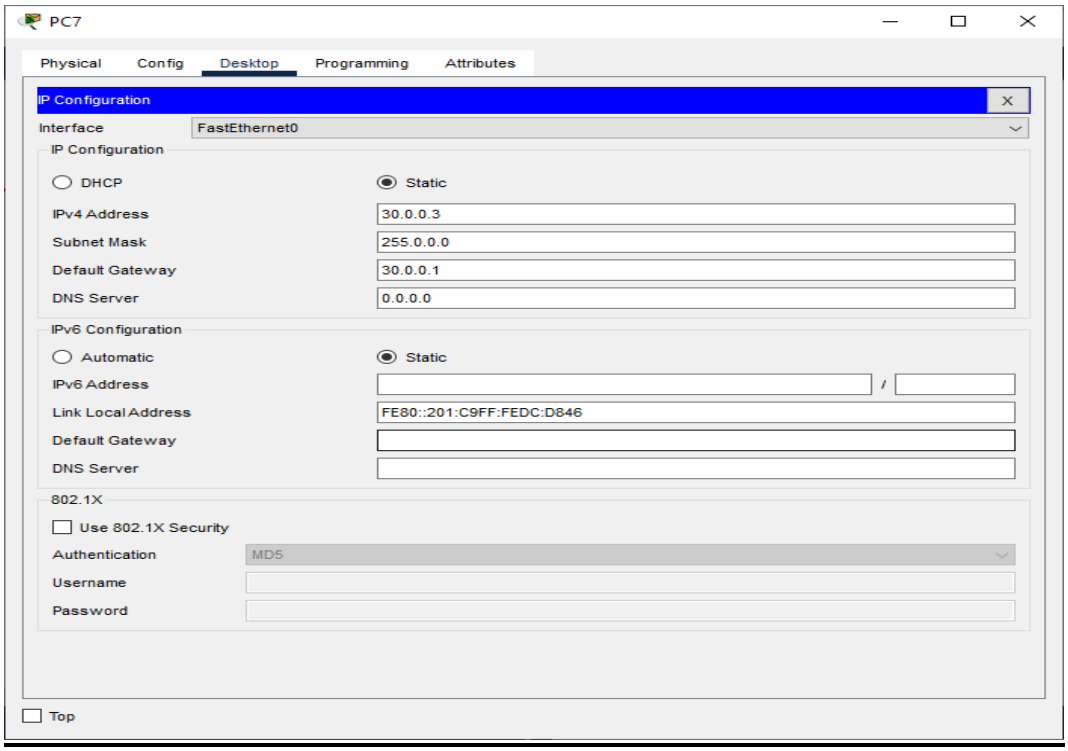




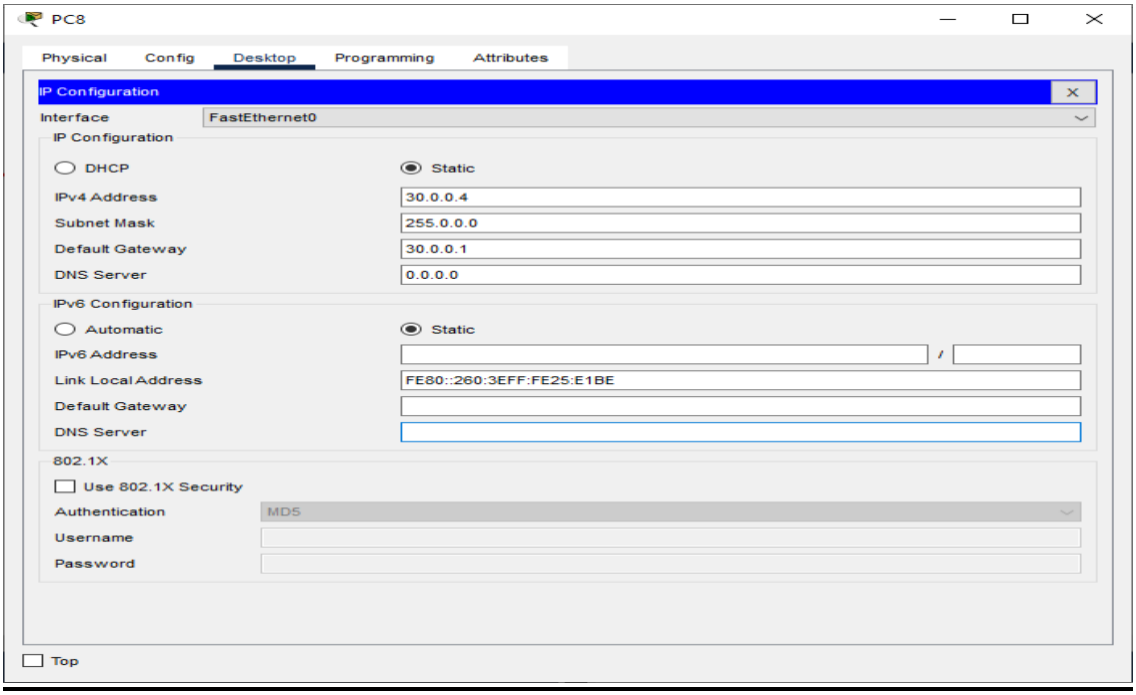
Configuring PC6:



Configuring PC7:

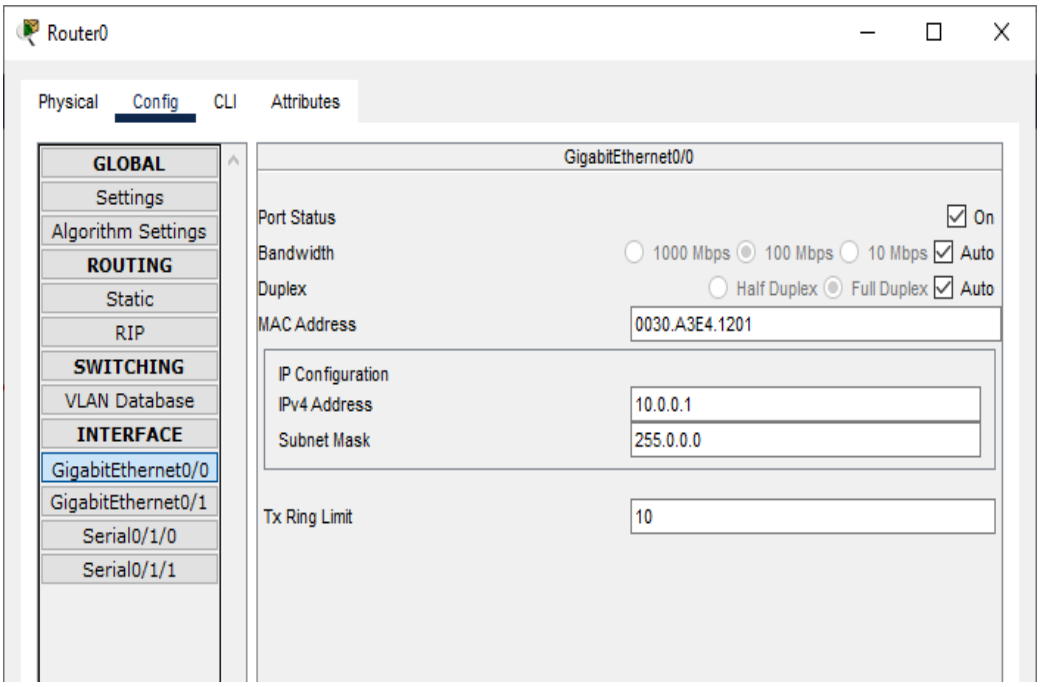


Configuring PC8:

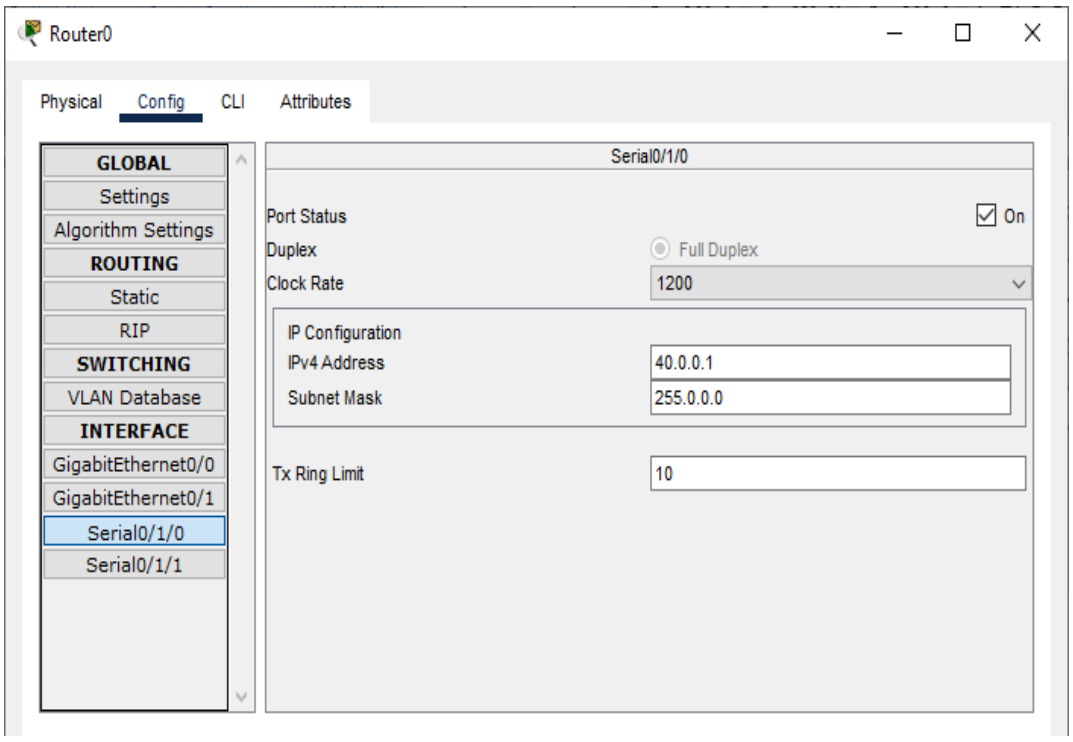


Configuring IP addresses on Router 0

i) Interface G0/0

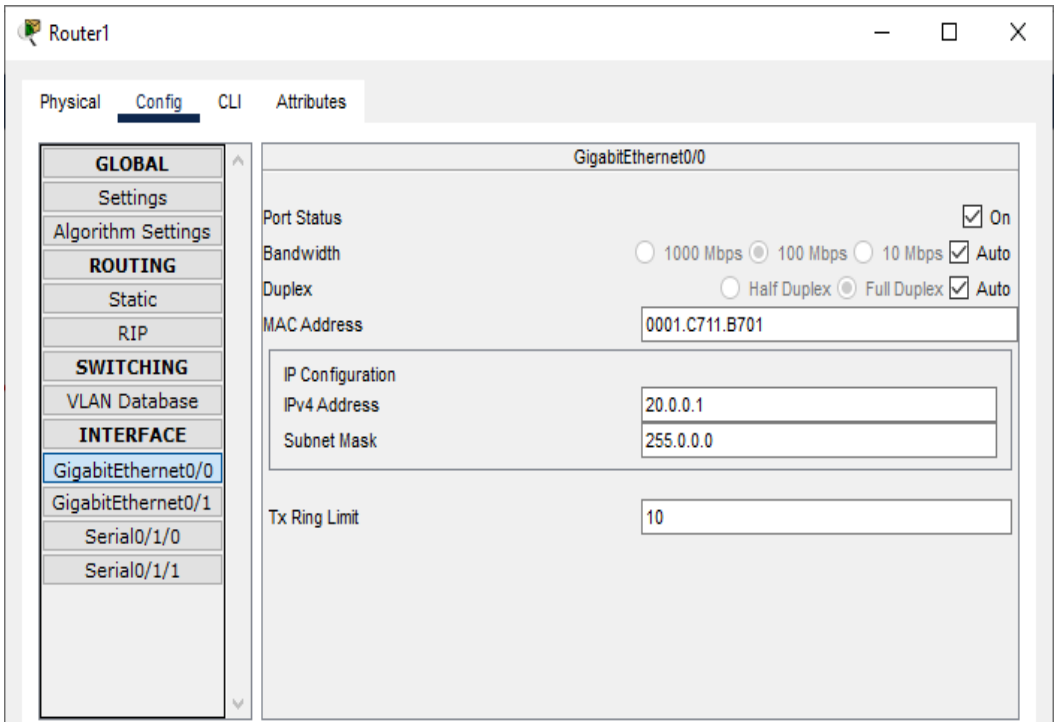


ii) Interface S0/1/0

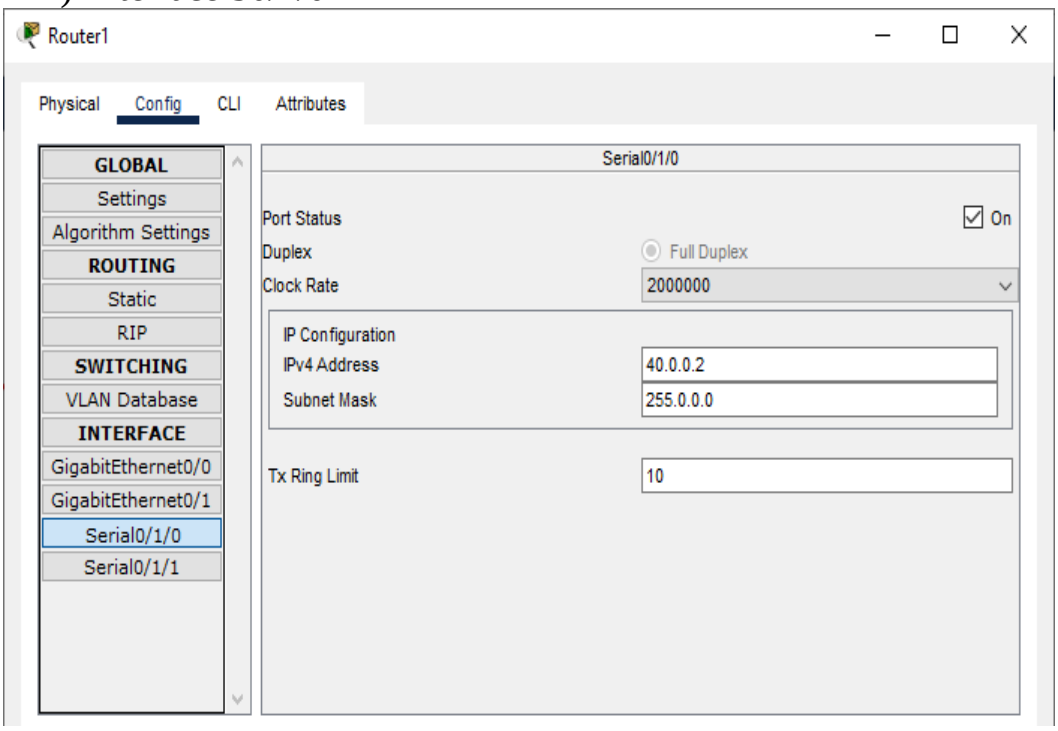


Configuring IP addresses on Router 1

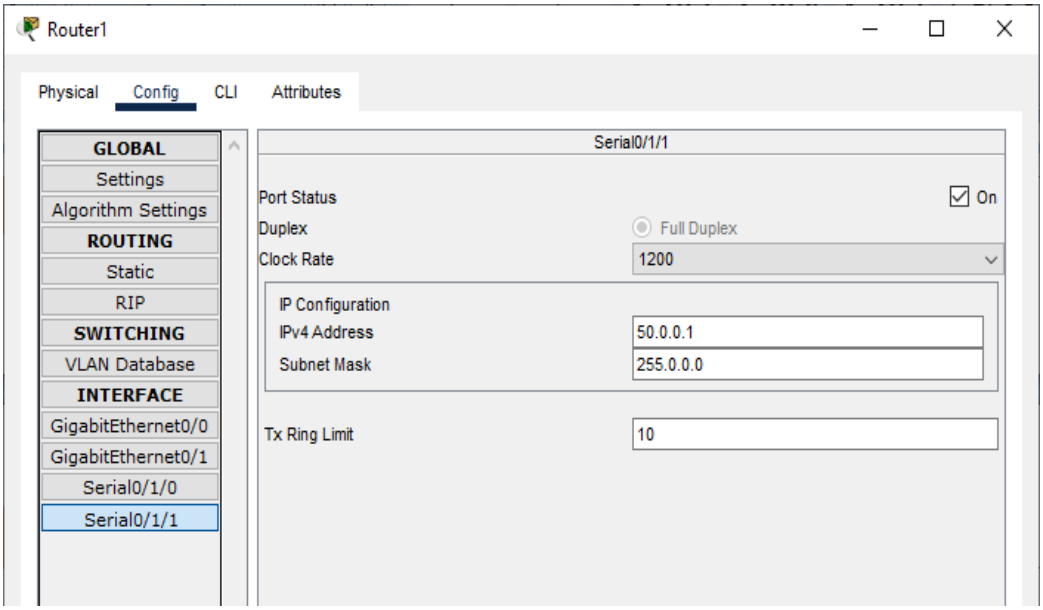
i) Interface G0/0



ii) Interface S0/1/0

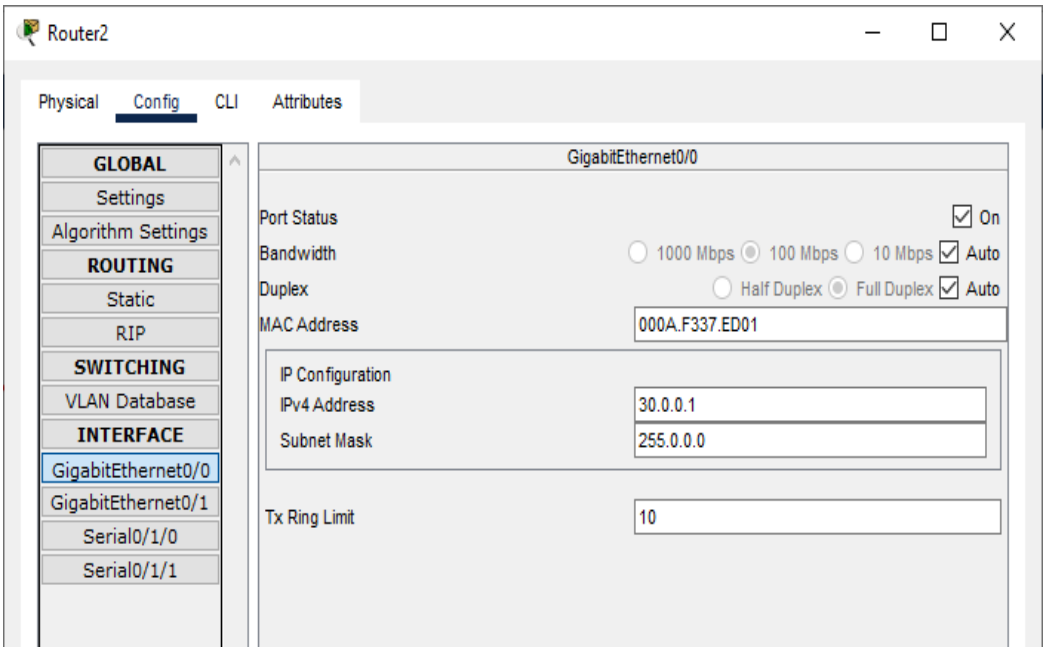


iii) Interface S0/1/1

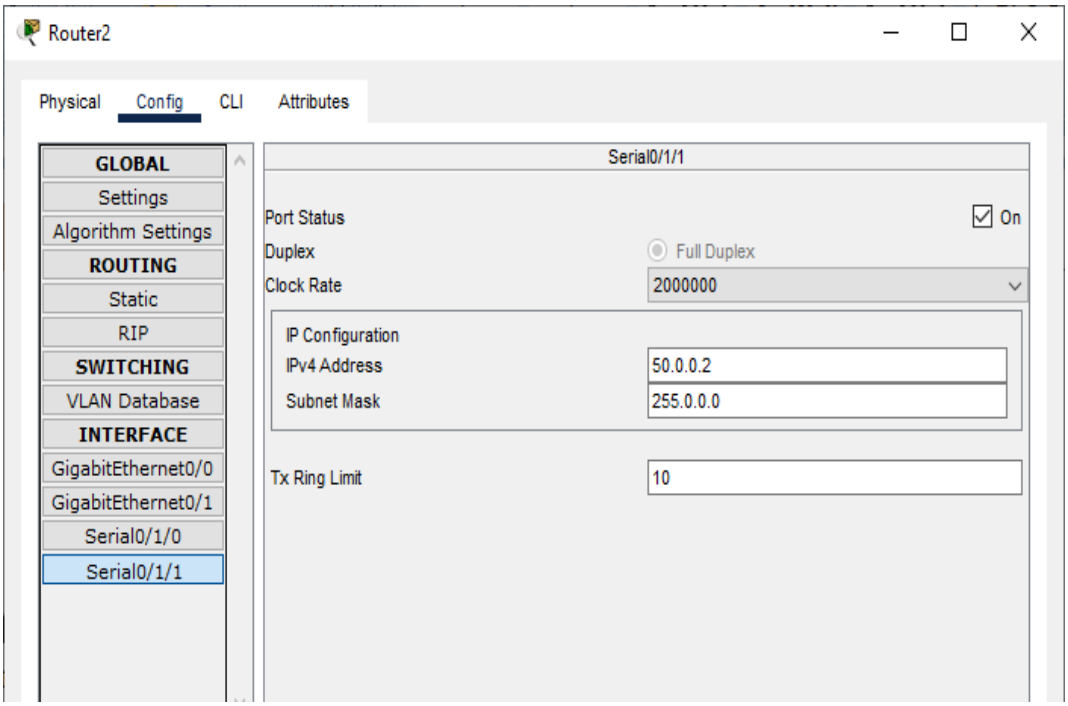


Configuring IP addresses on Router 2

i) Interface G0/0



ii) Interface S0/1/1



Configuring Router 0 for OSPF (using the CLI mode)

```
Router(config)#
Router(config)#router ospf 1
Router(config-router)#network 10.0.0.0 0.0.0.255 area 1
Router(config-router)#network 40.0.0.0 0.0.0.255 area 1
Router(config-router)#exit
Router(config)#
```

Configuring Router 1 for OSPF (using the CLI mode)

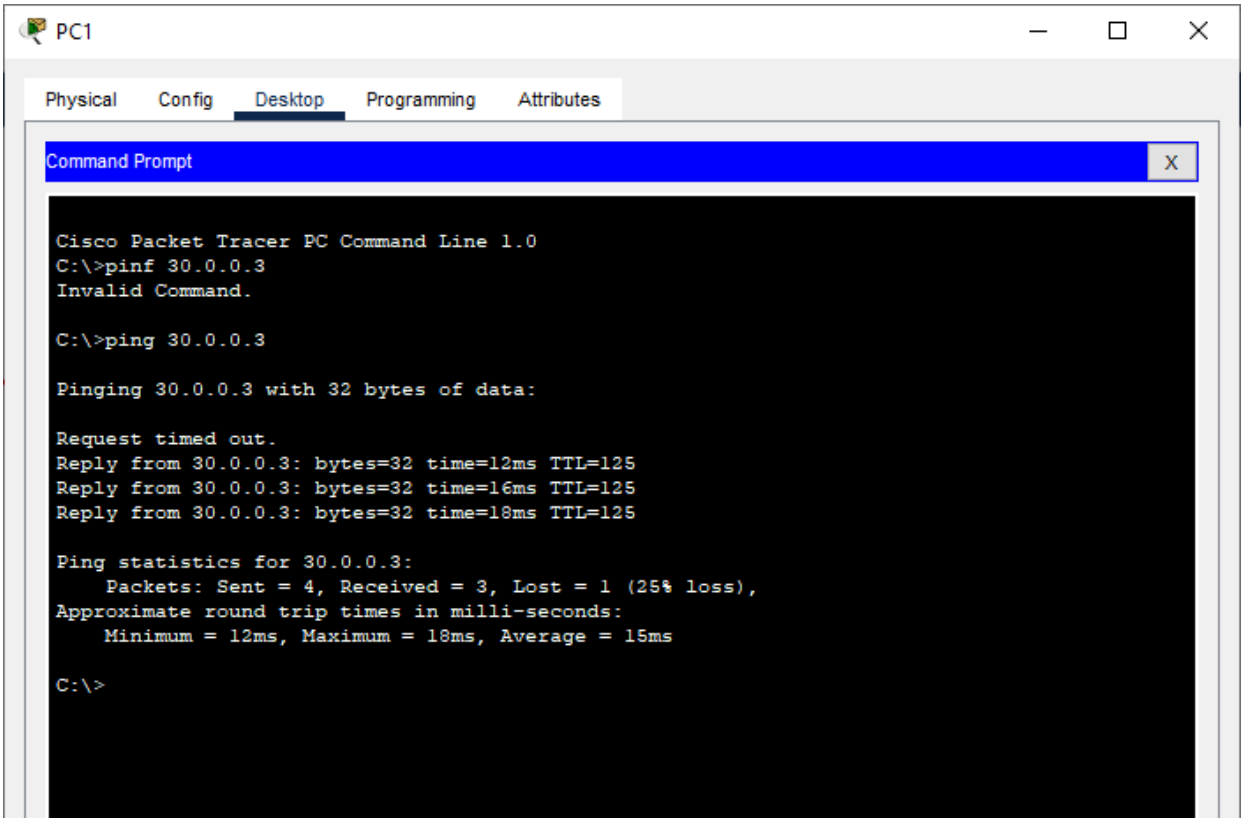
```
Router(config)#
Router(config)#router ospf 1
Router(config-router)#
Router(config-router)#network 20.0.0.0 0.0.0.255 area 1
Router(config-router)#network 40.0.0.0 0.0.0.255 area 1
Router(config-router)#network 50.0.0.0 0.0.0.255 area 1
Router(config-router)#exit
Router(config)#
```

Configuring Router 2 for OSPF (using the CLI mode)

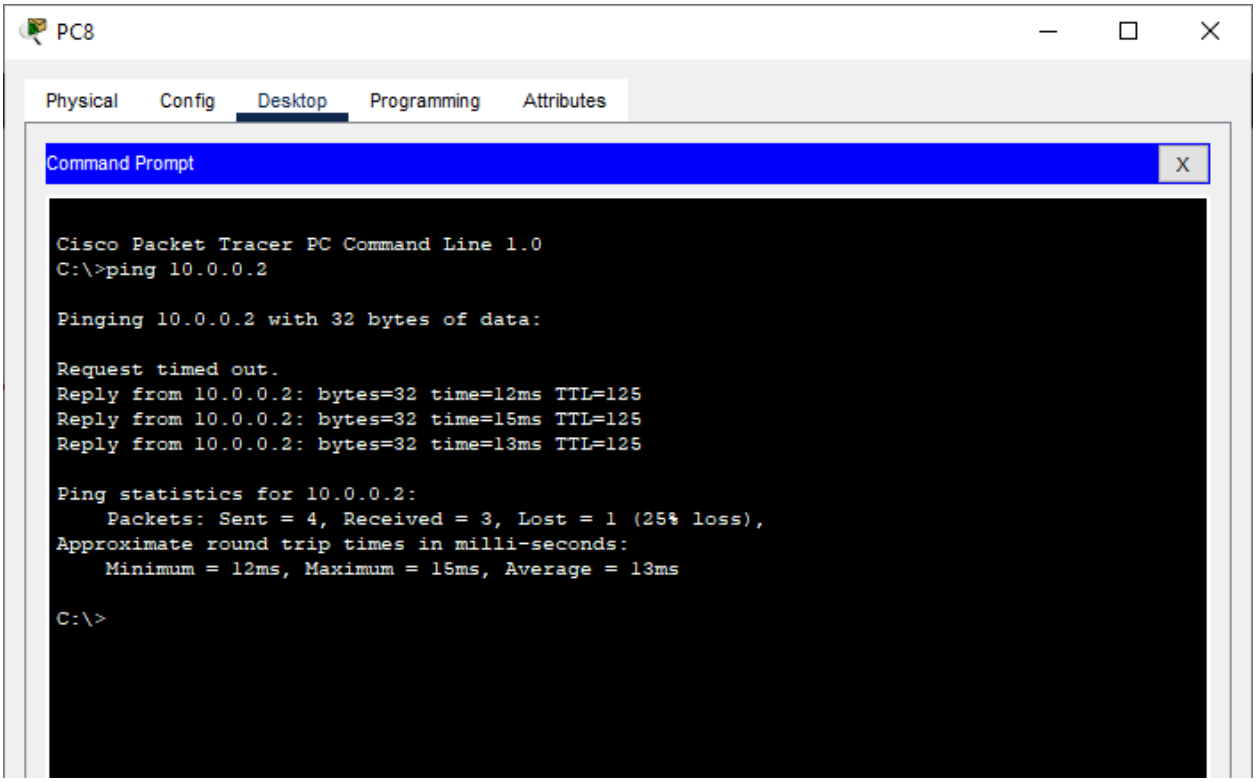
```
Router(config)#
Router(config)#router ospf 1
Router(config-router)#
Router(config-router)#network 30.0.0.0 0.0.0.255 area 1
Router(config-router)#network 50.0.0.0 0.0.0.255 area 1
Router(config-router)# exit
Router(config)#
```

Checking the connectivity by using the ping command

i) Pinging PC8 (ip address 10.30.0.4) from PC1



ii) Pinging PC0 (ip address 10.10.0.2) from PC8



Result:

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

Practical No 8

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

Theory:

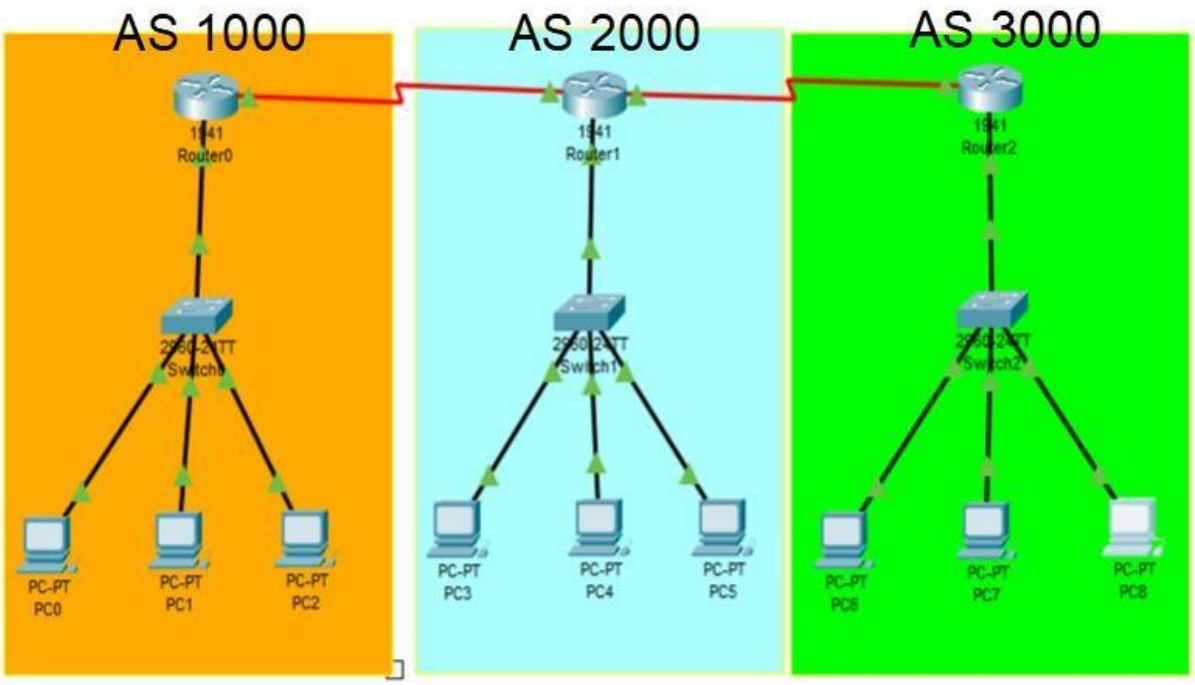
Border Gateway Protocol (BGP) is used to Exchange routing information for theinternet and is the protocol used between ISP which are different Autonoumous Systems (AS).

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 routerthat 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 otherBGP 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

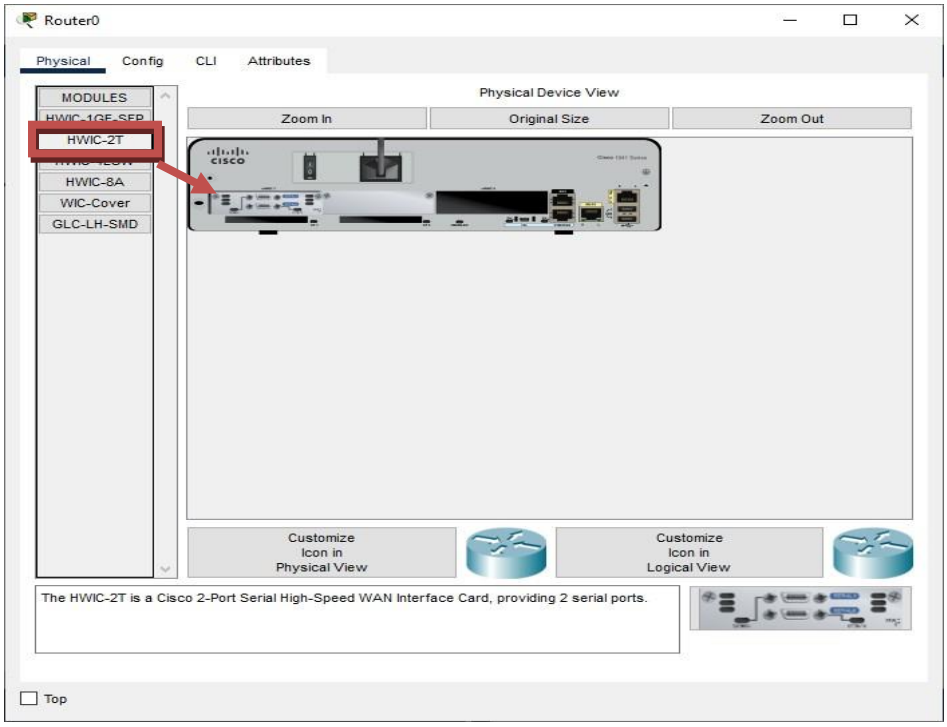


We configure the above network using the following IP addresses

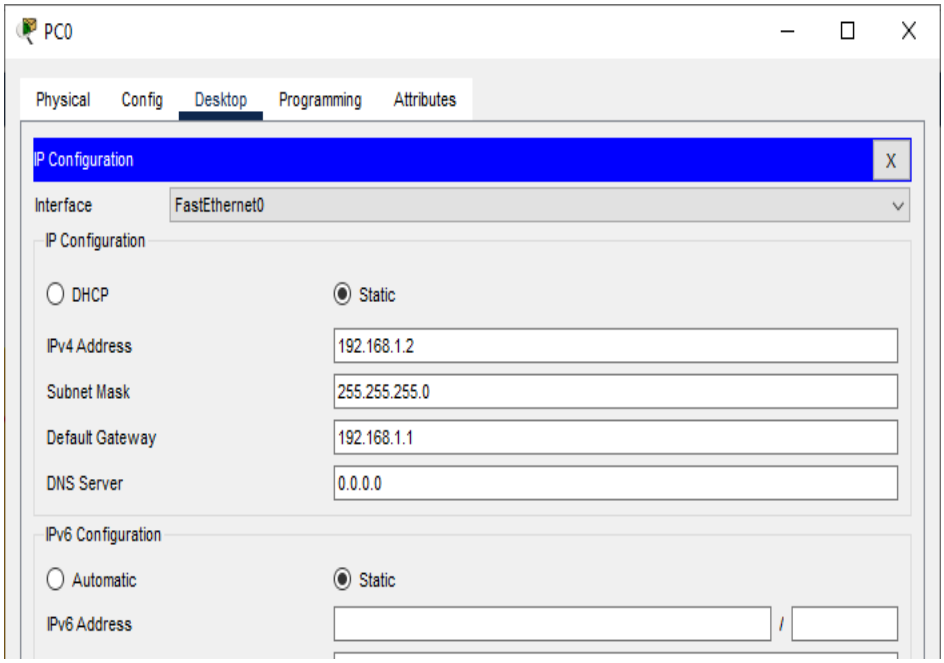
Host	Interface	IP address	Network Address	Default Gateway
Router 0 AS 1000	G0/0	192.168.1.1	192.168.1.0	
	S0/1/0	10.0.0.1	10.0.0.0	
Router 1 AS 2000	G0/0	192.168.2.1	192.168.2.0	
	S0/1/0	10.0.0.2	10.0.0.0	
	S0/1/1	20.0.0.1	20.0.0.0	
Router 2 AS 3000	G0/0	192.168.3.1	192.168.3.0	
	S0/1/1	20.0.0.2	20.0.0.0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

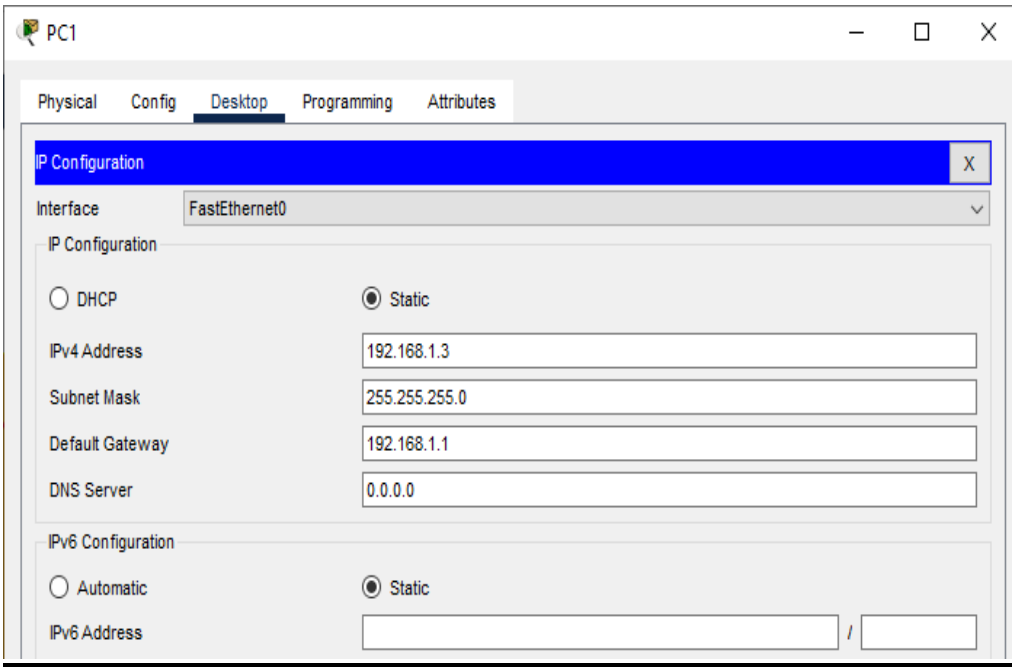
PC5	FastEthernet 0	192.168.2.4		
PC6	FastEthernet 0	192.168.3.2	192.168.3.0	192.168.3.1
PC7	FastEthernet 0	192.168.3.3		
PC8	FastEthernet 0	192.168.3.4		

Adding Serial Interface in each Router

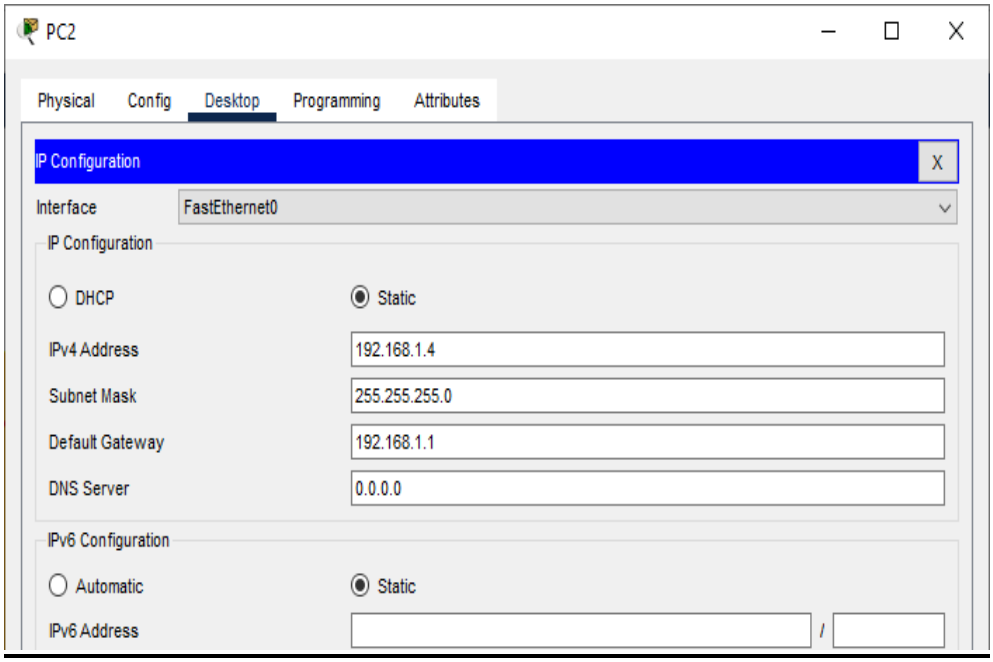


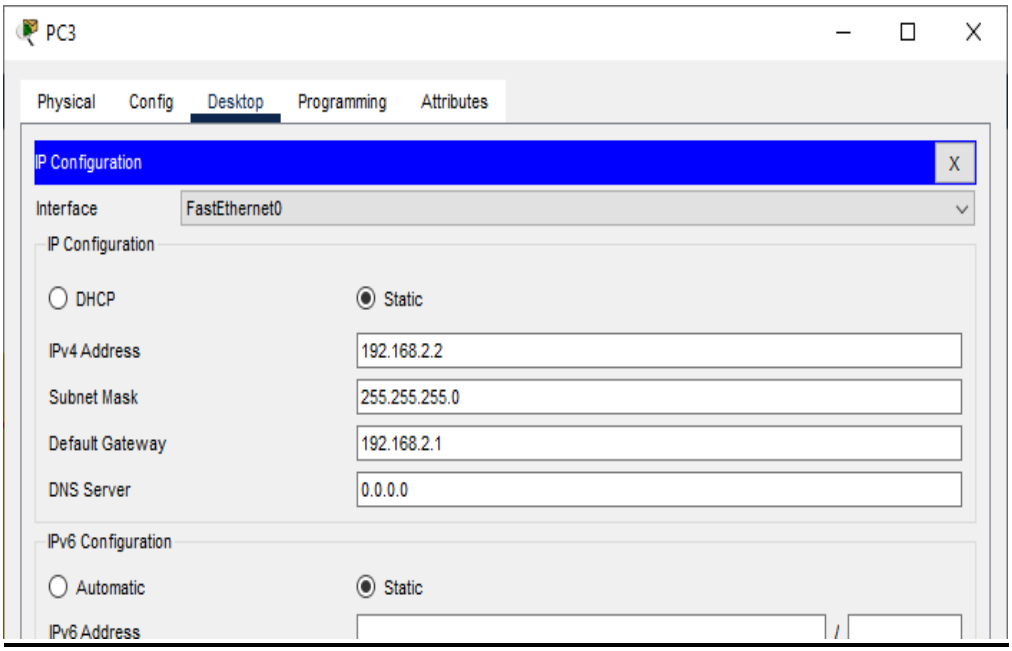
Configuring PC0:



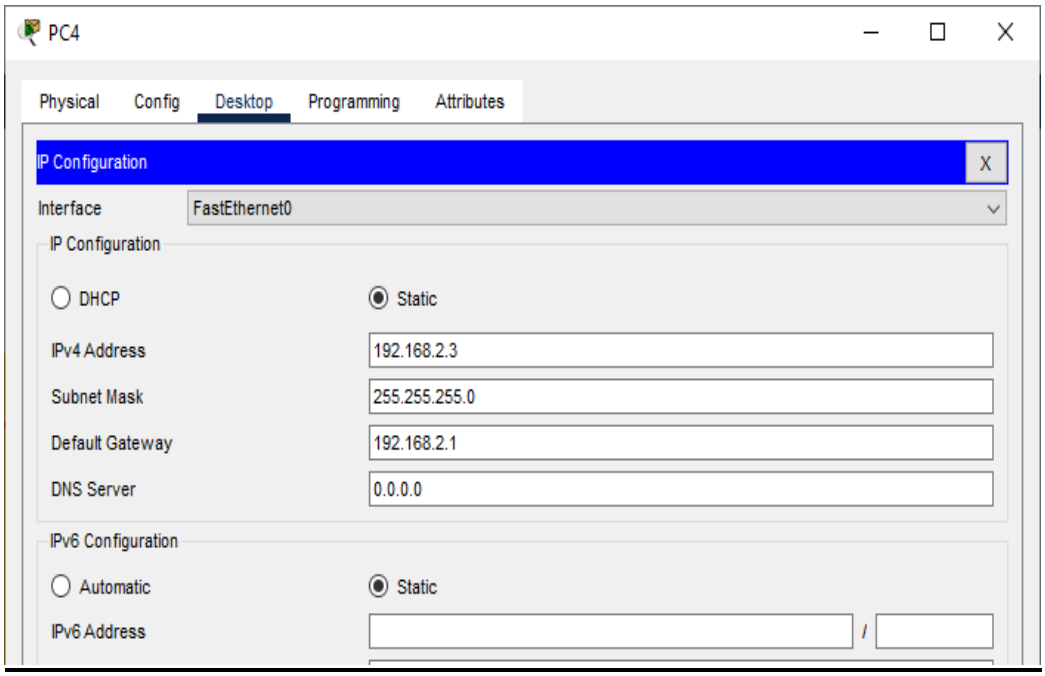


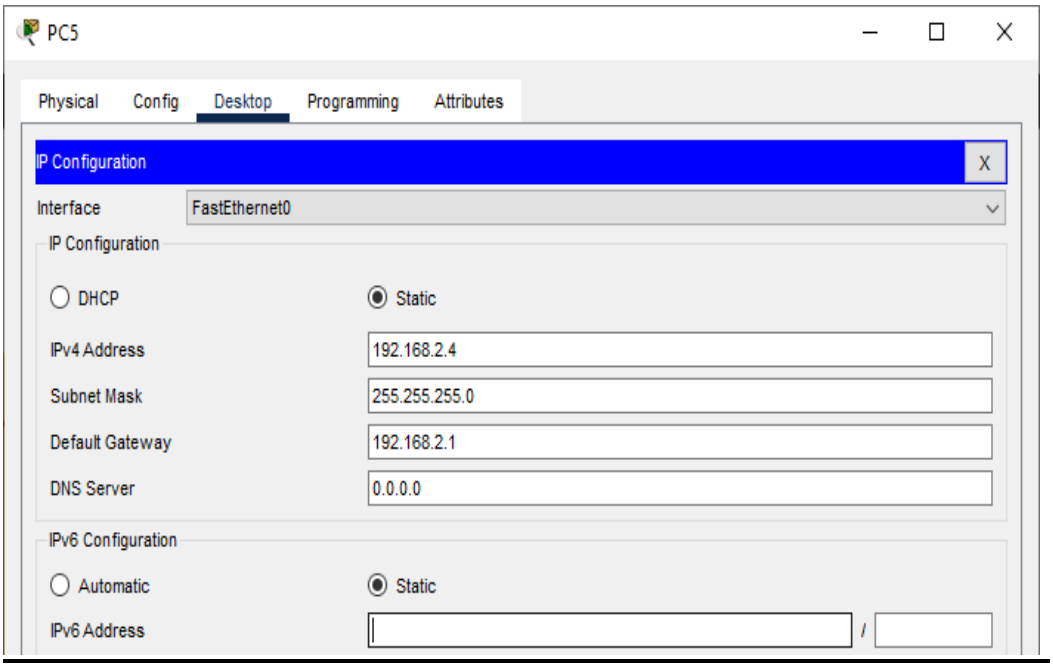
Configuring PC2:



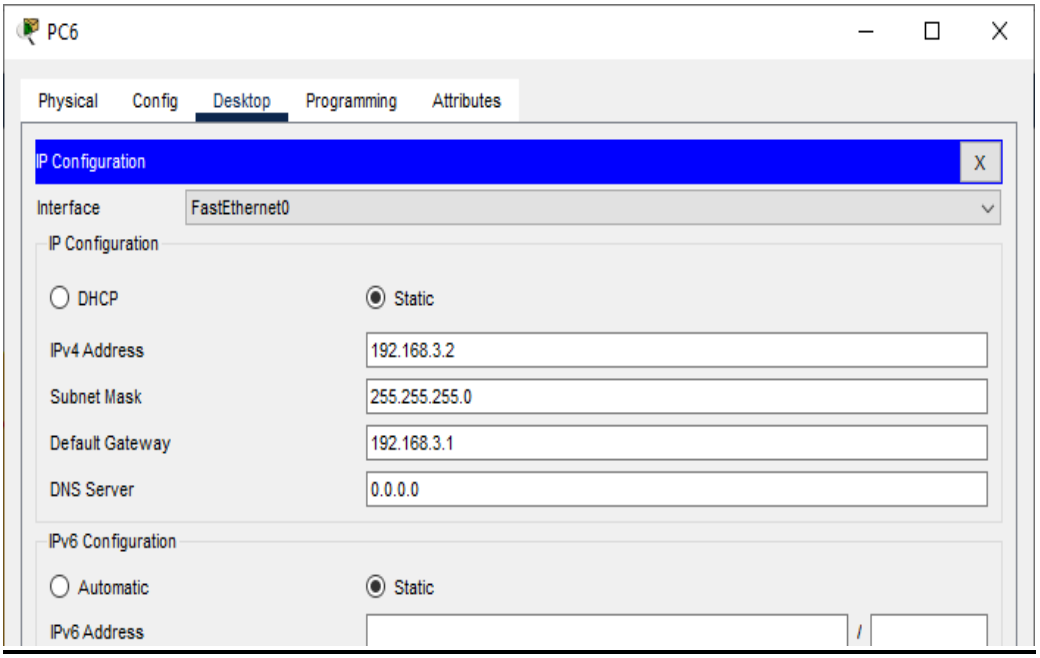


Configuring PC4:

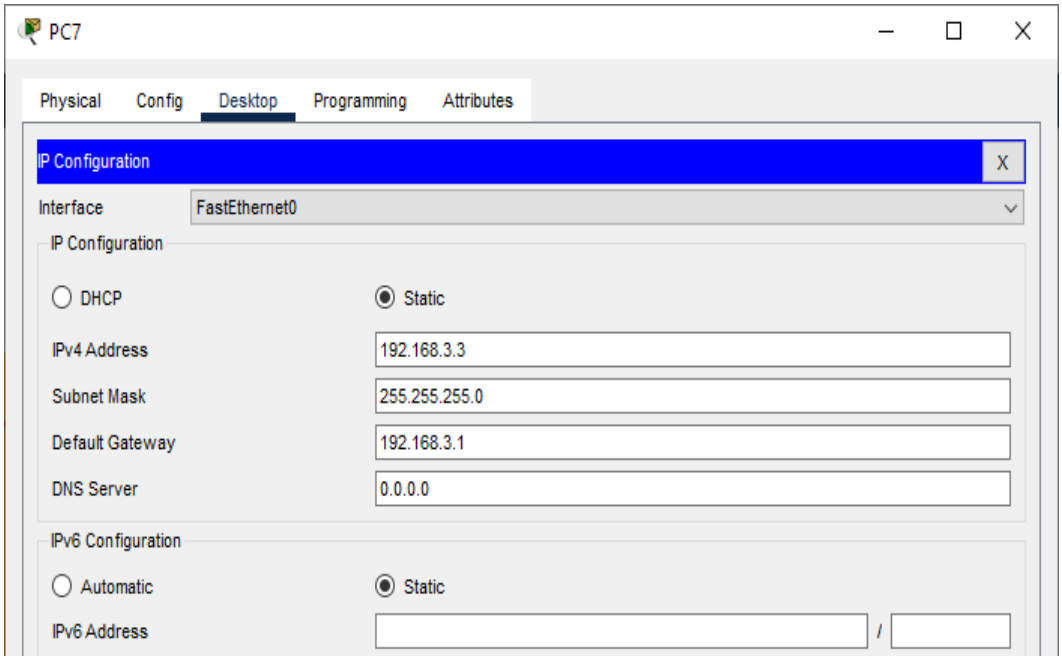




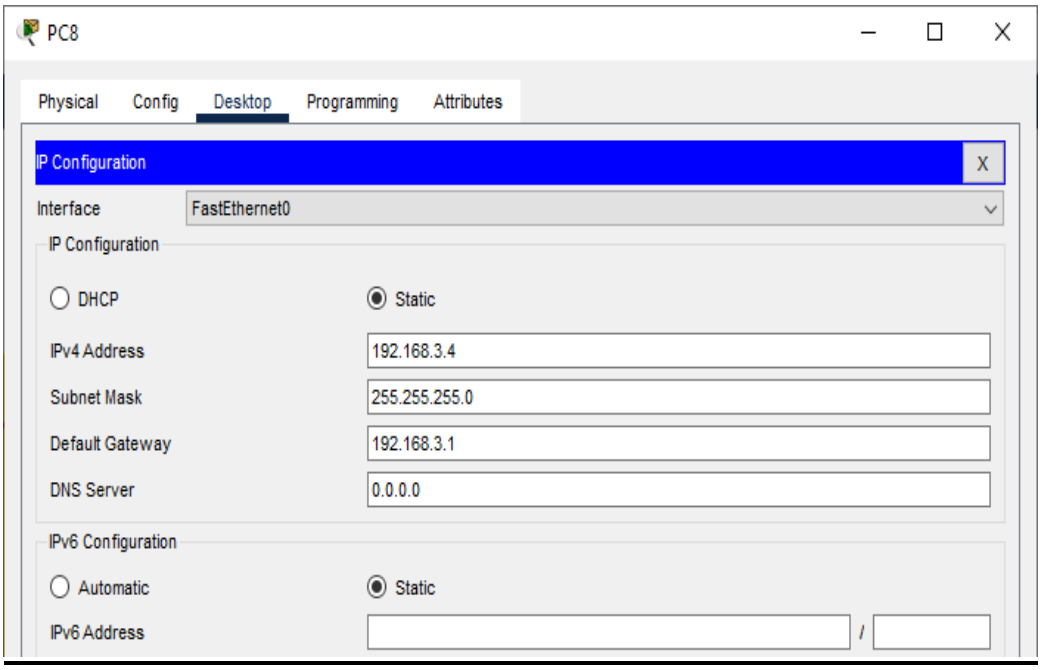
Configuring PC6:



Configuring PC7:

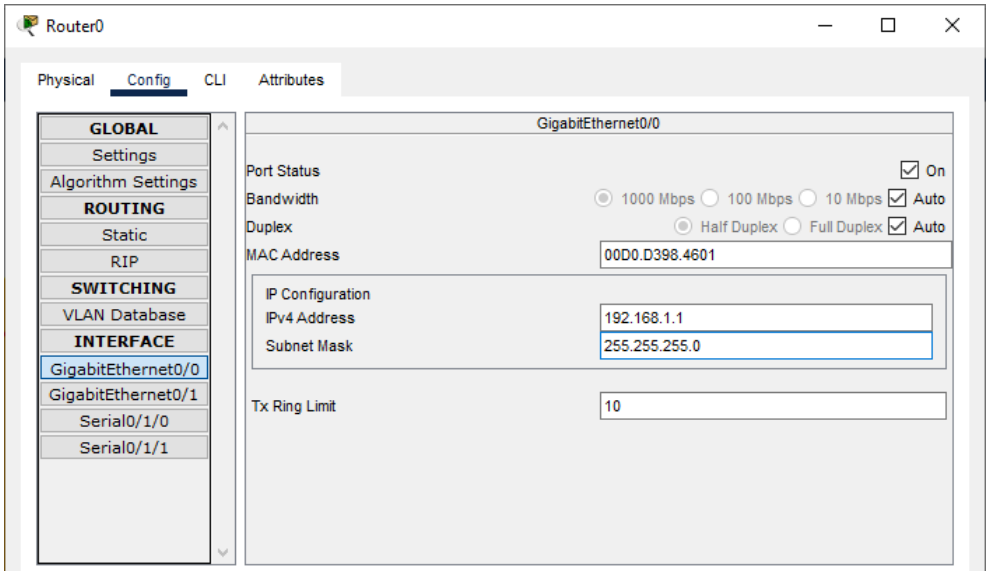


Configuring PC8:

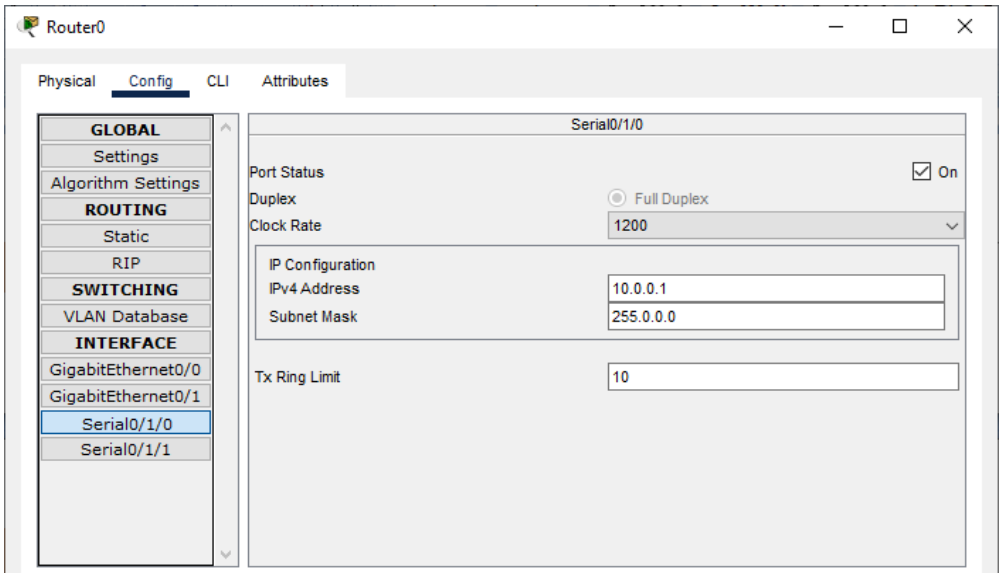


Configuring IP addresses on Router 0

i) Interface G0/0

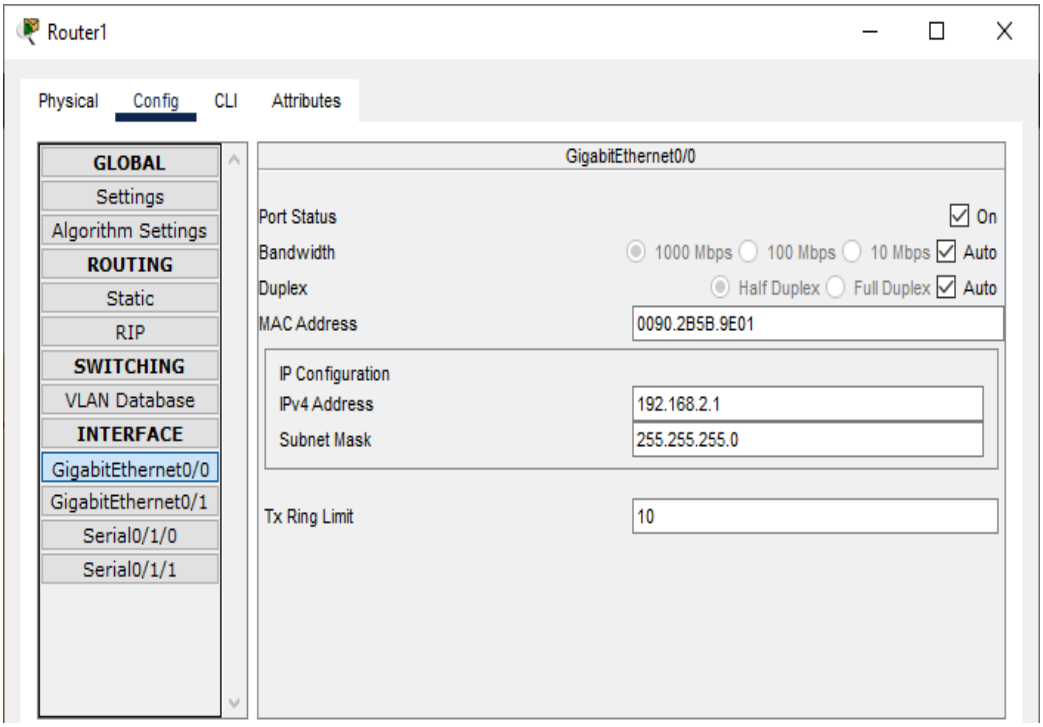


ii) Interface S0/1/0

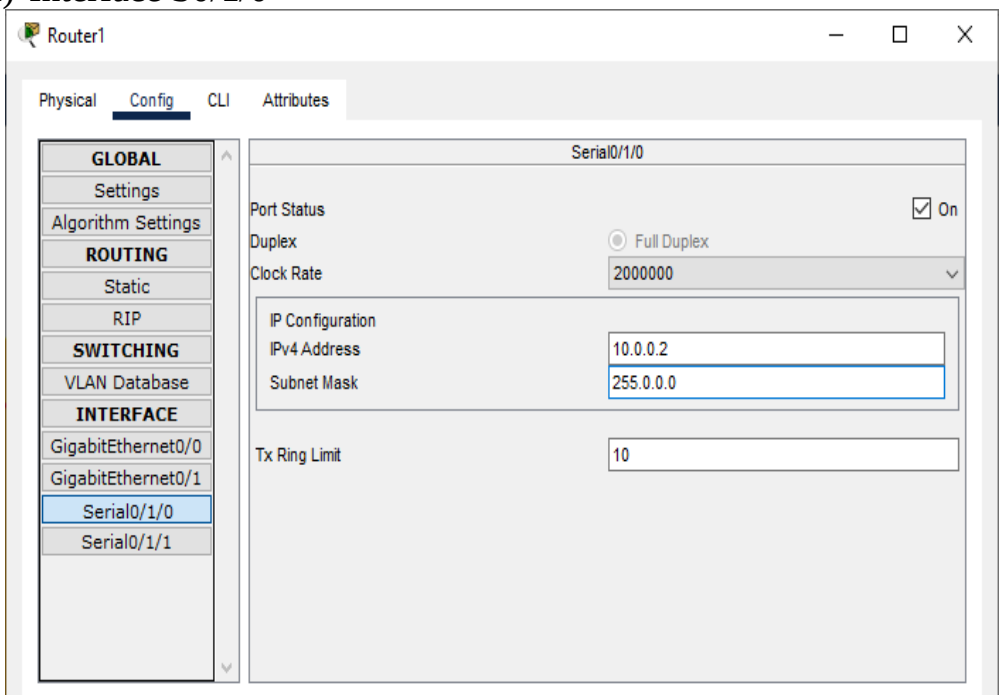


Configuring IP addresses on Router 1

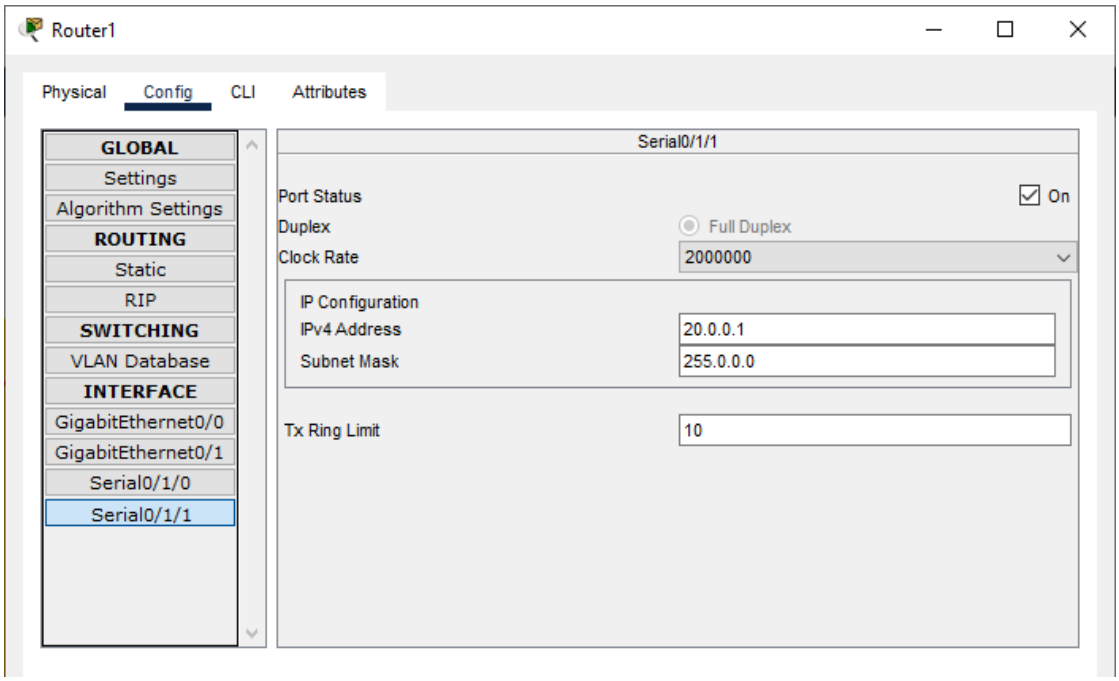
i) Interface G0/0



ii) Interface S0/1/0

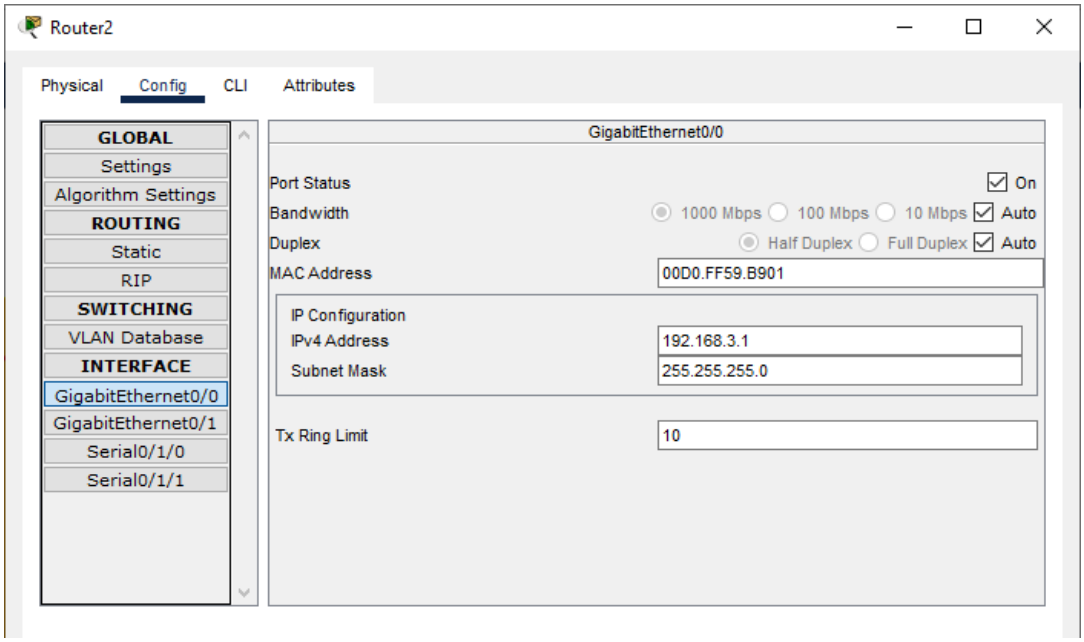


iii) Interface S0/1/1

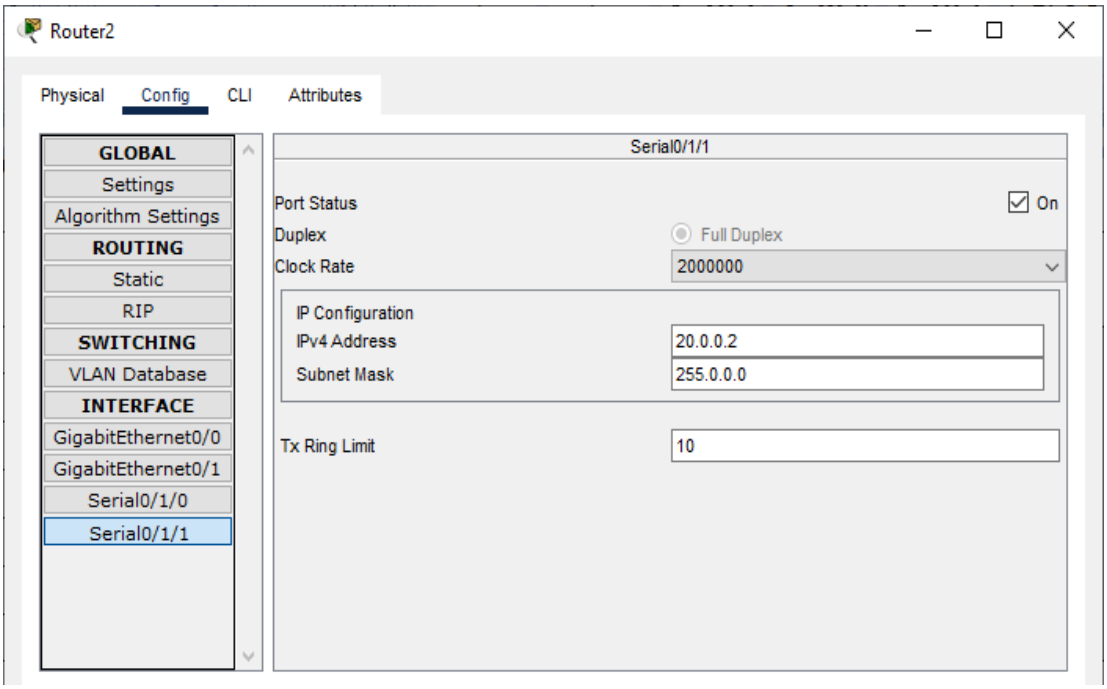


Configuring IP addresses on Router 2

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)

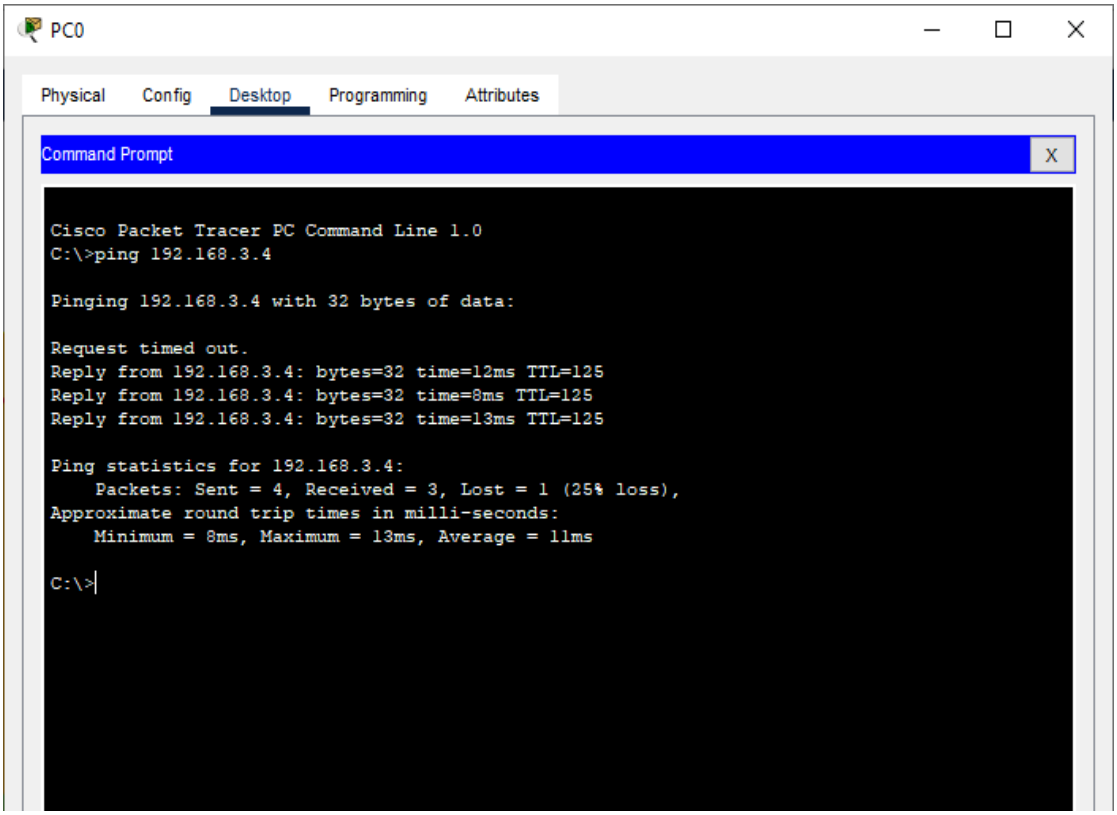
```
Router>enable
Router#configure terminal
Router(config)#
Router(config)#router bgp 2000
Router(config-router)#network 10.0.0.0
Router(config-router)#network 20.0.0.0
Router(config-router)#network 192.168.2.0
Router(config-router)#neighbor 10.0.0.1 remote-as 1000
Router(config-router)#neighbor 20.0.0.2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

Configuring Router 2 for BGP (using the CLI mode)

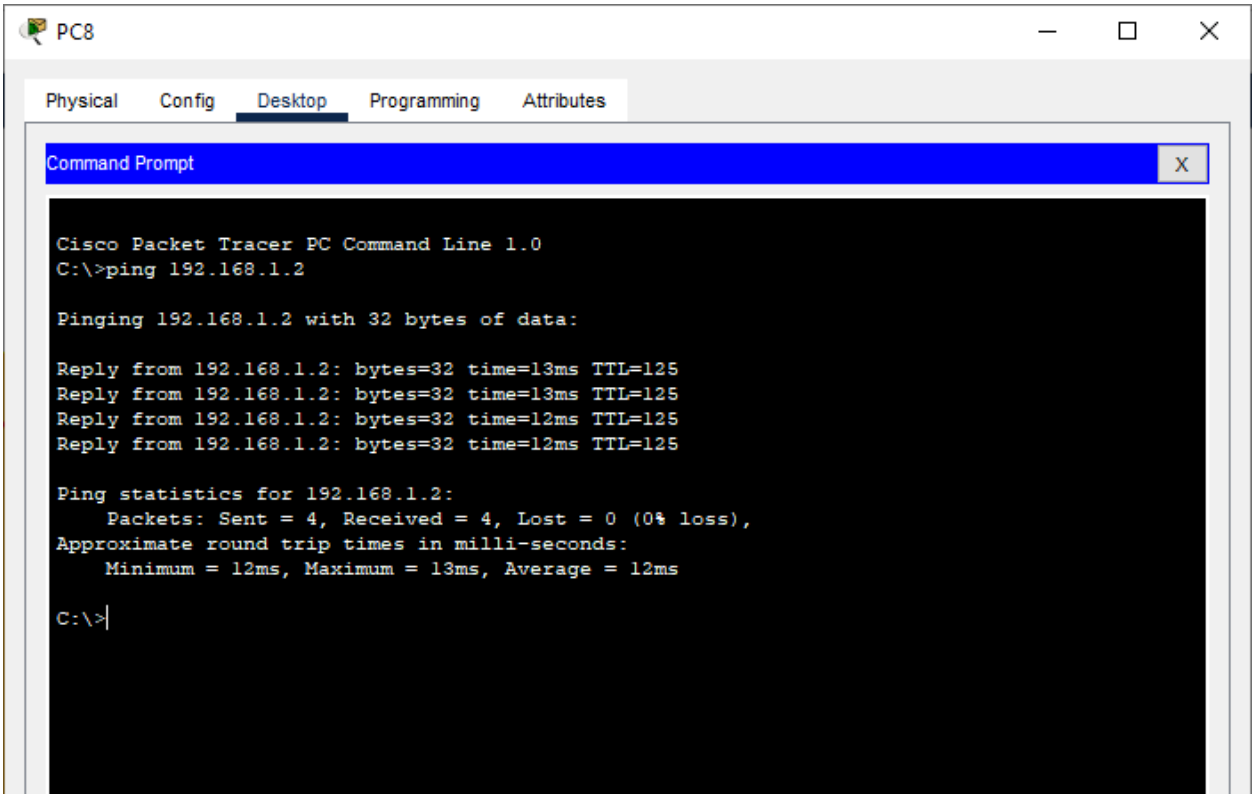
```
Router>enable
Router#configure terminal
Router(config)#
Router(config)#router bgp 3000
Router(config-router)#
Router(config-router)#network 20.0.0.0
Router(config-router)#network 192.168.3.0
Router(config-router)#neighbor 20.0.0.1 remote-as 2000
```

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

Practical No 9

Aim: Using Packet Tracer, create a wireless network of multiple PCs using appropriate access point

Theory:

A Wireless Access Point (WAP) is a networking device that allows connecting the devices with the wired network. A Wireless Access Point (WAP) is used to create the WLAN (Wireless Local Area Network), it is commonly used in large offices and buildings which have expanded businesses.

A wireless AP connects the wired networks to the wireless client. It eases access to the network for mobile users which increases productivity and reduces the infrastructure cost.

Advantages of Wireless Access Point (WAP):

1) More User Access
2) Broader Transmission Range
3) Flexible Networking

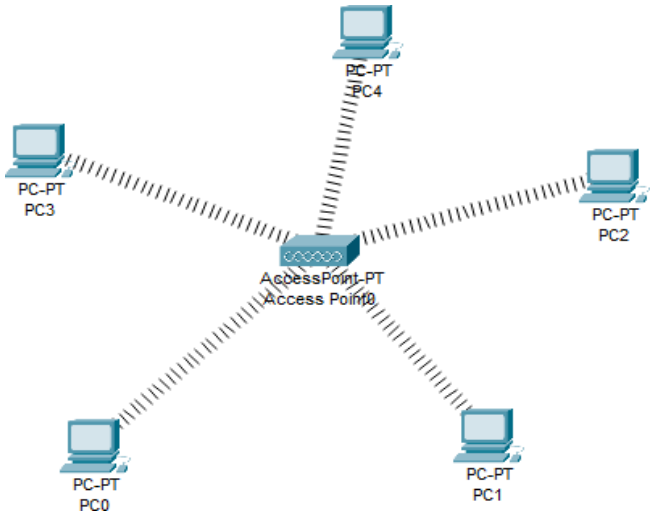
Disadvantages of Wireless Access Point (WAP):

1) High cost
2) Poor stability
3) Less Secure

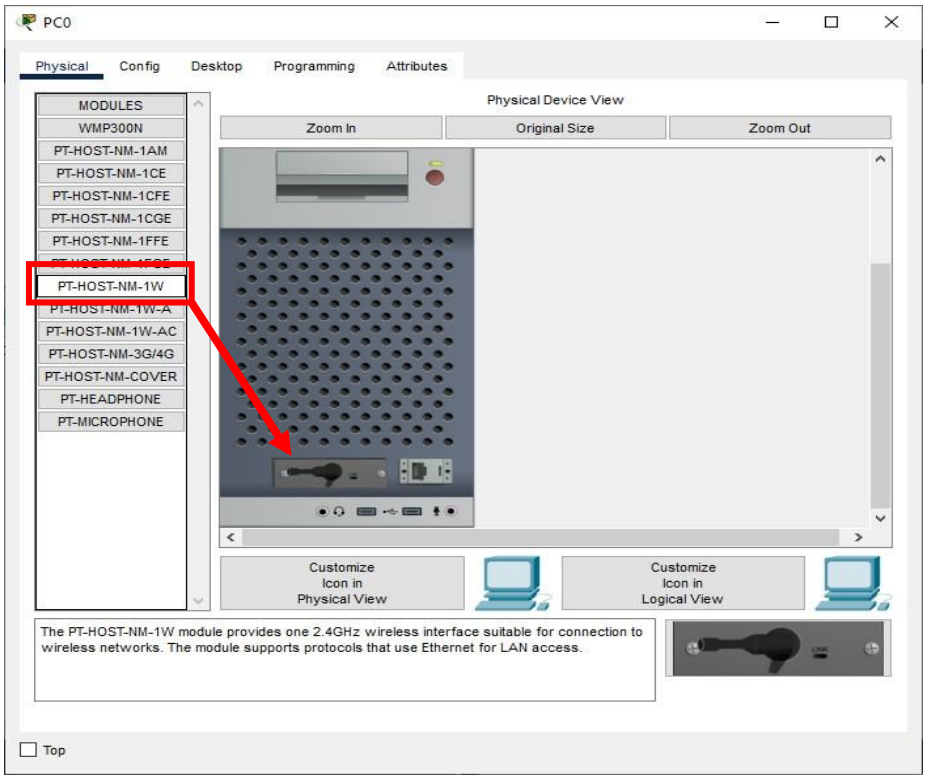
Application of Wireless Access Point:

1) It is a device that creates a WLAN (Wireless Local Area Network) in large enterprises.
2) It is used to extend the coverage area of the network so that it can't disconnect which allows more users to connect to the network easily.
3) An access point connects a switch, Ethernet cable, wired router, and Wi-fi to designate the particular area.
4) It is used to provide connectivity to the users in large offices or enterprises which allows users to roam easily anywhere in the office and be connected to a network.
5) LANs can also be provided in public places such as coffee shops, restaurants, airports, etc.

We use the following topology for the present case (5PCs and an Access Point)

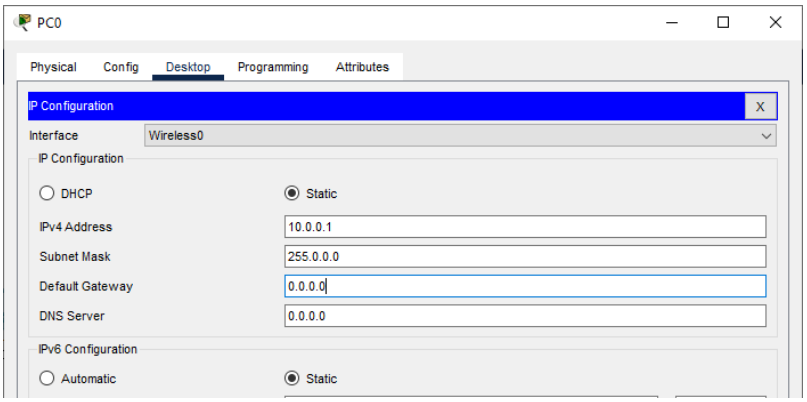


Add a Wireless interface to each PC as follows

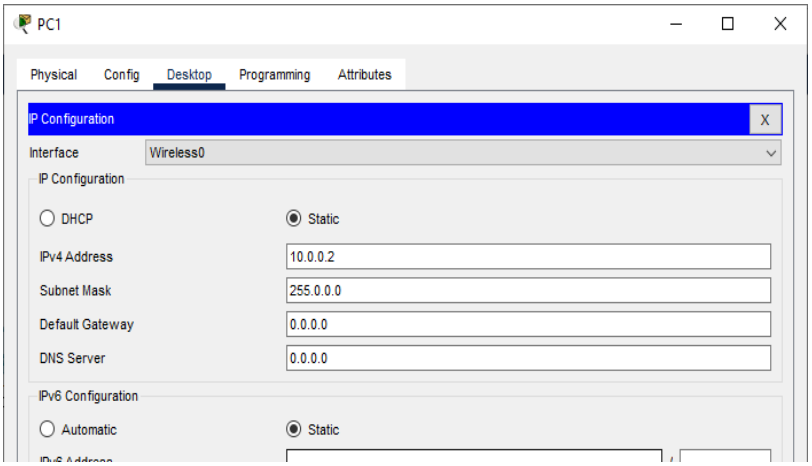


Assigning IP Address to each PC (select Static)

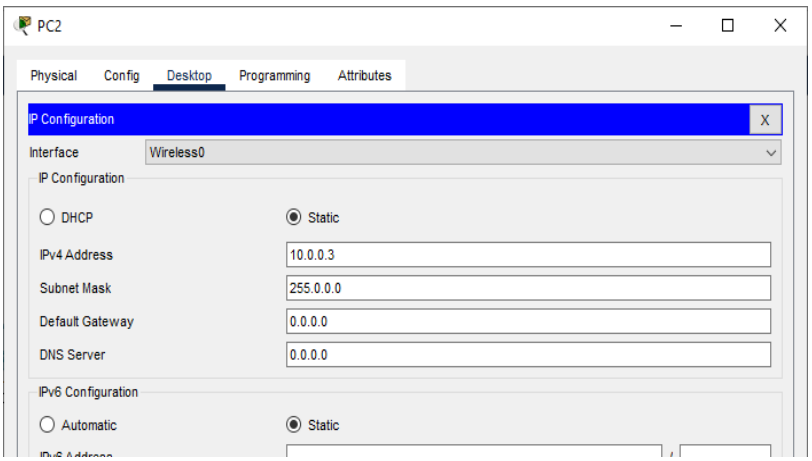
1) PC0 :



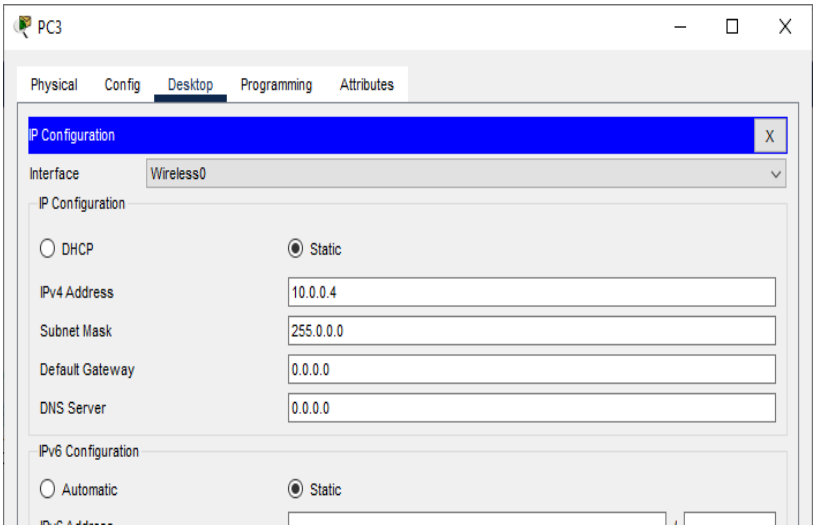
2) PC1 :



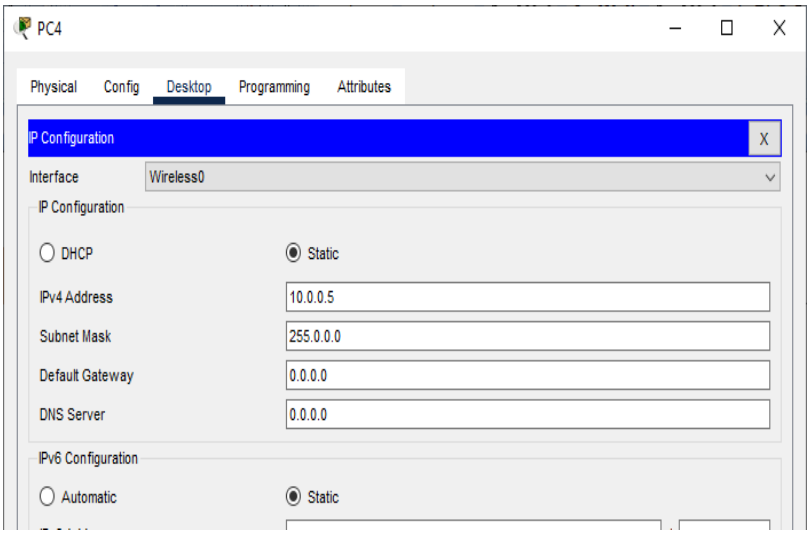
3) PC2 :



4) PC3 :



5) PC4 :

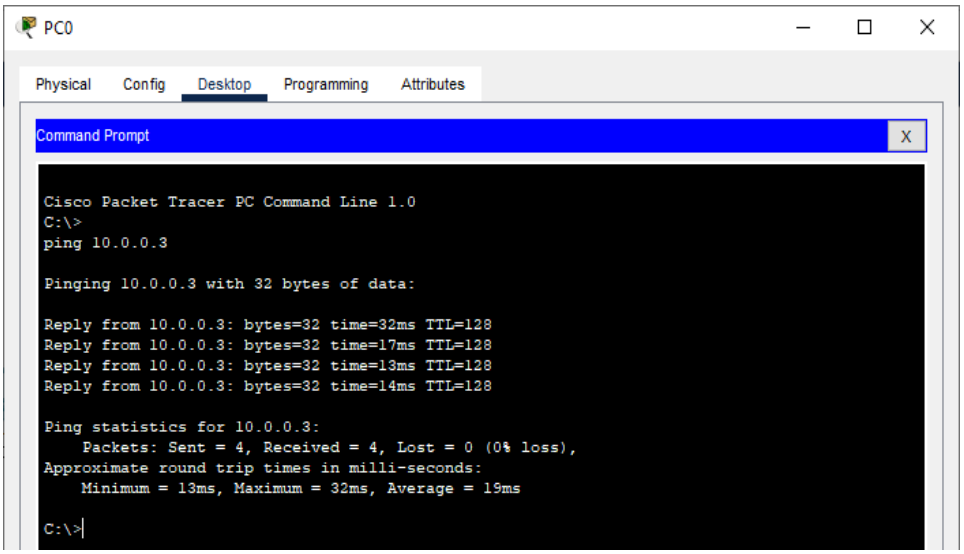


The IP addresses assigned are

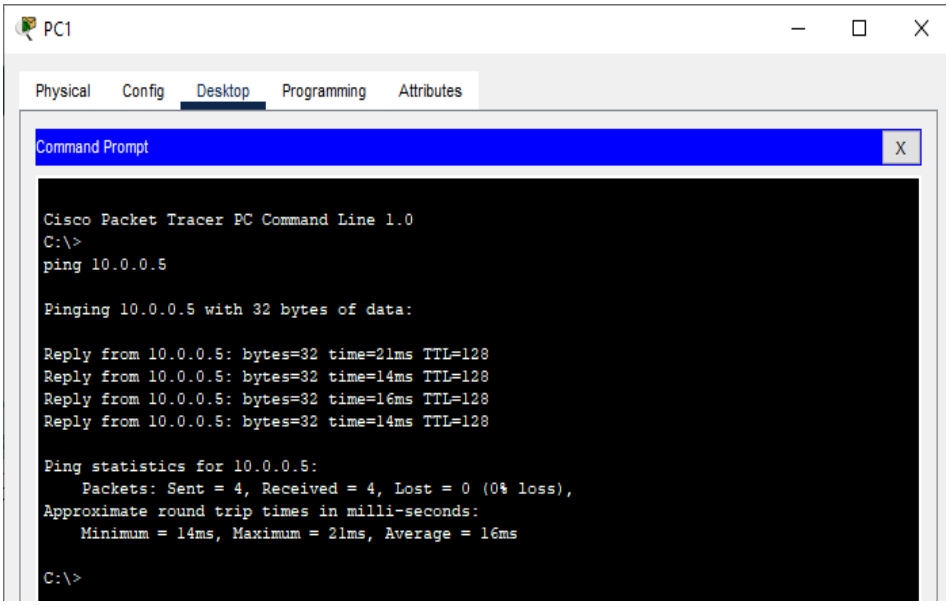
Host	IP address
PC0	10.0.0.1
PC1	10.0.0.2
PC2	10.0.0.3
PC3	10.0.0.4
PC4	10.0.0.5

We verify the connectivity by sending ping message from any PC to any other PC

Pinging PC2 (10.0.0.3) from PC0 (10.0.0.1)



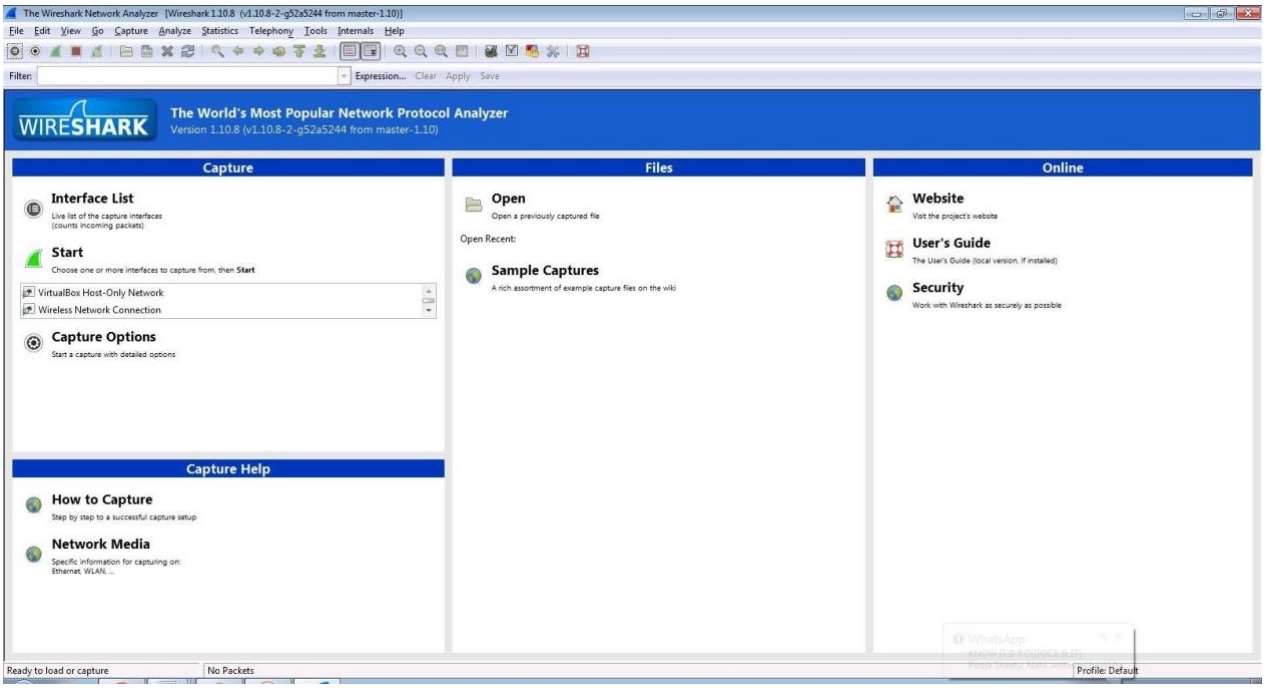
Pinging PC4 (10.0.0.5) from PC1 (10.0.0.2)



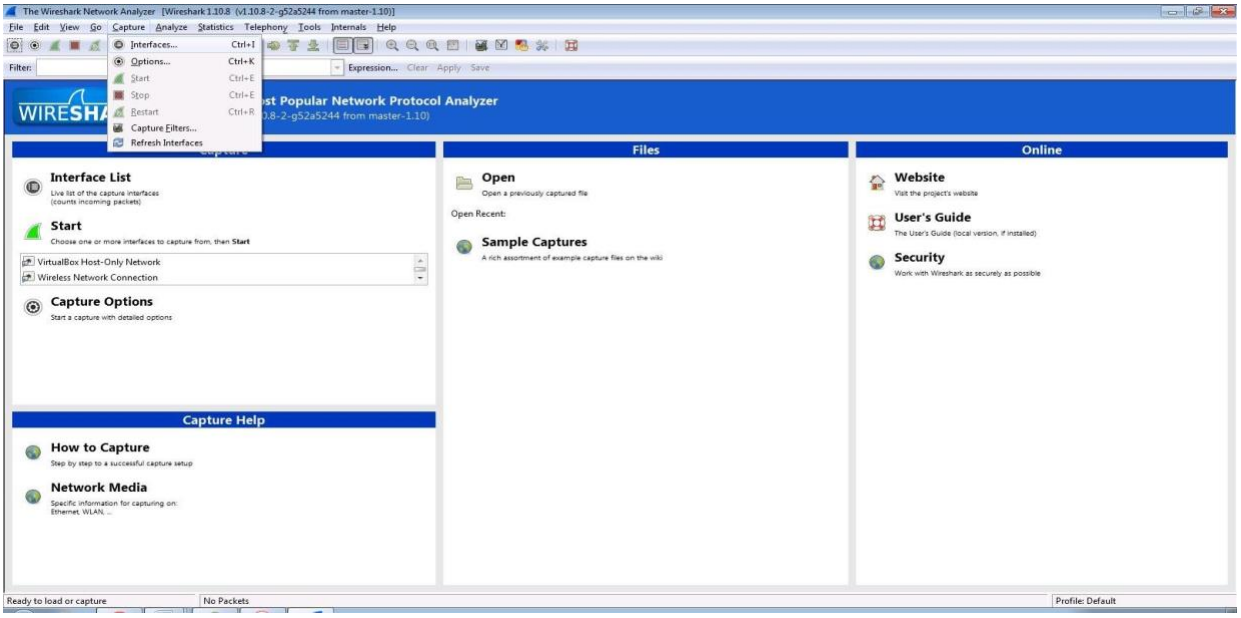
PRACTICAL NO 10

Using Wireshark, network analyzer, set the filter for ICMP, TCP, HTTP, UDP, FTP and perform respective protocol transactions to show/prove that the network analyzer is working

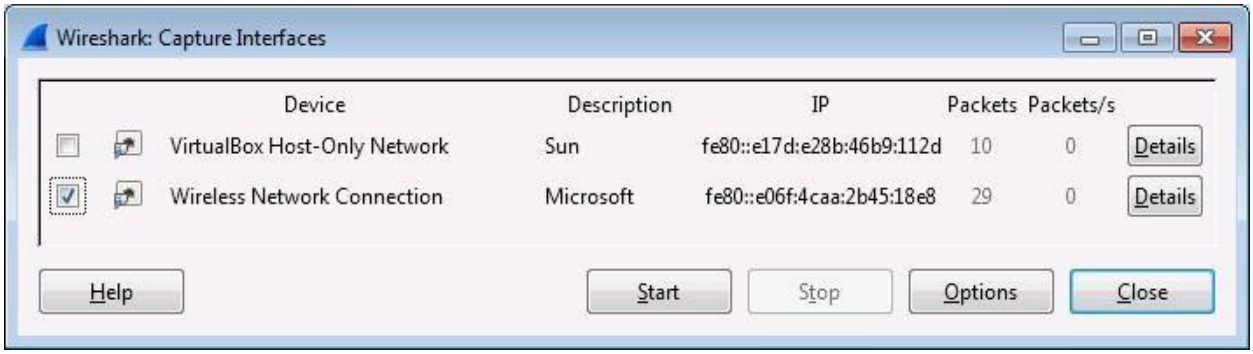
Step 1: Install and open WireShark .



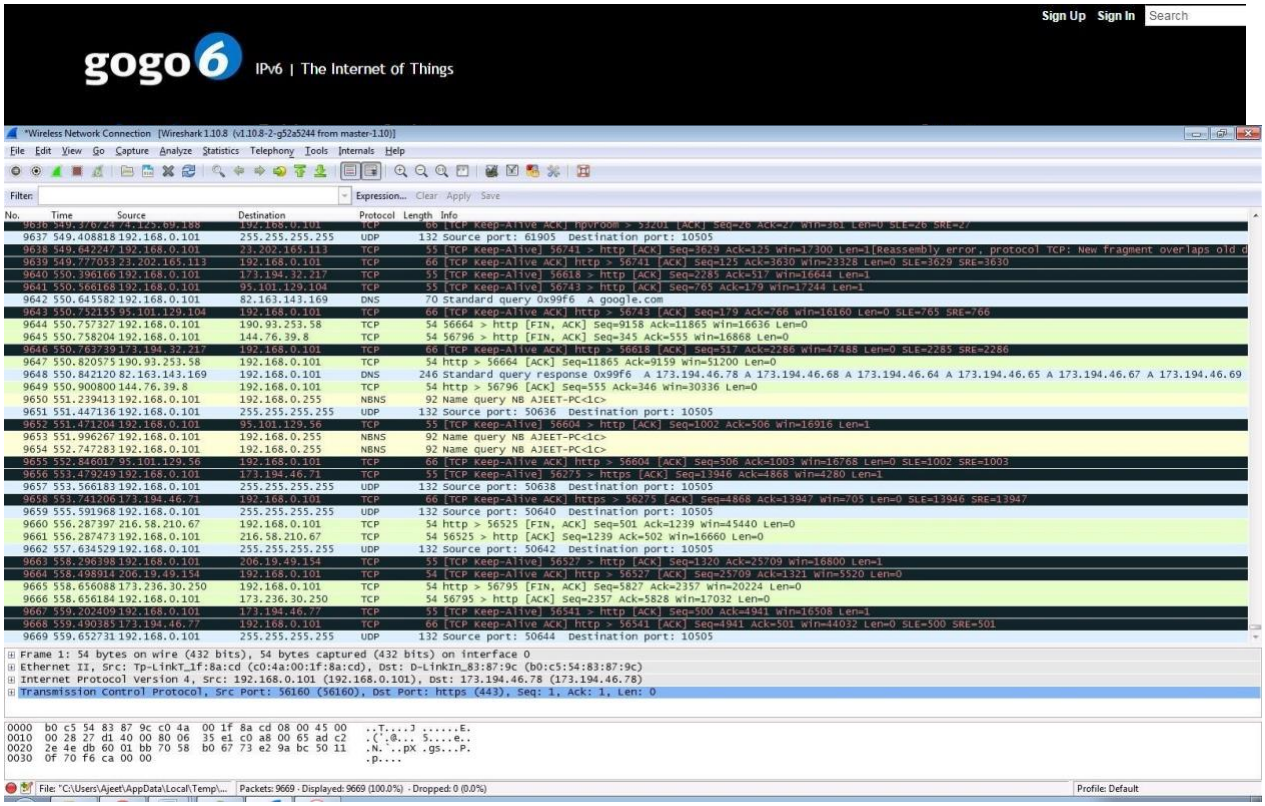
Step 2: Go to Capture tab and select Interface option.



Step 3: In Capture interface, Select Local Area Connection and click on start.

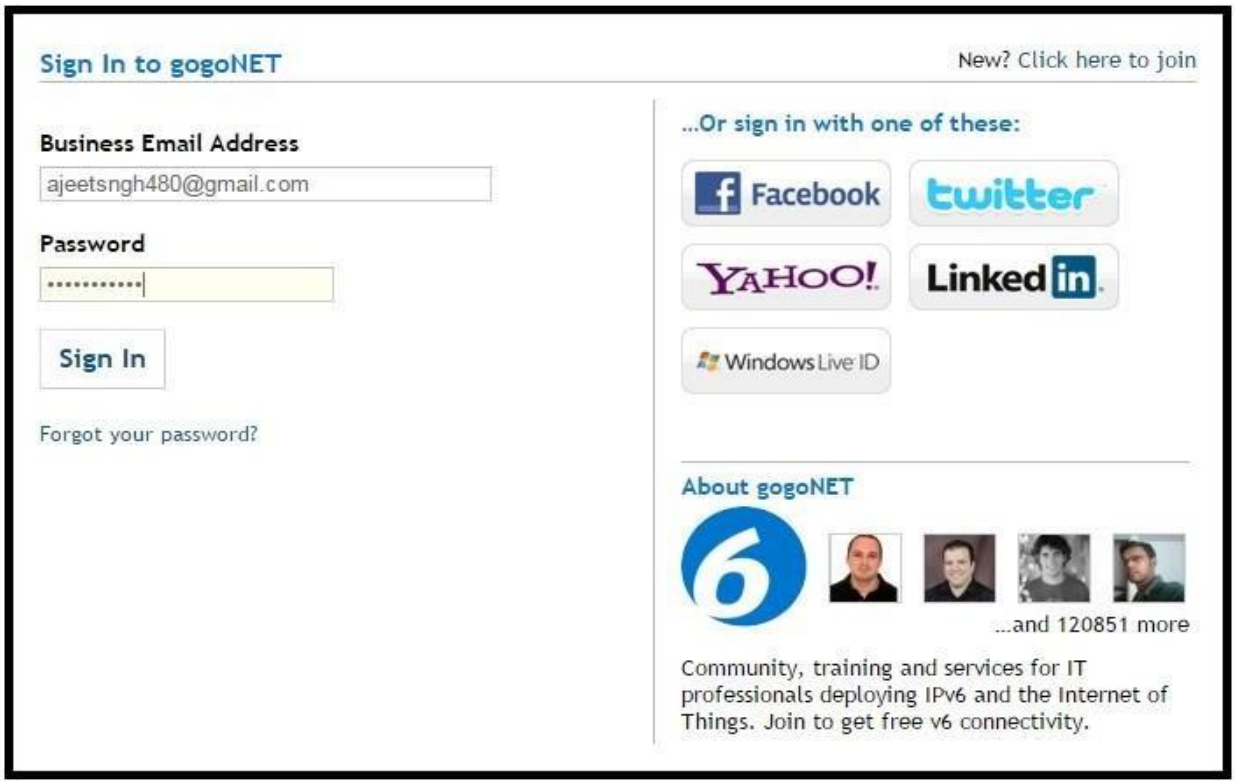


Step 4: The source, Destination and protocols of the packets in the LAN network are displayed.



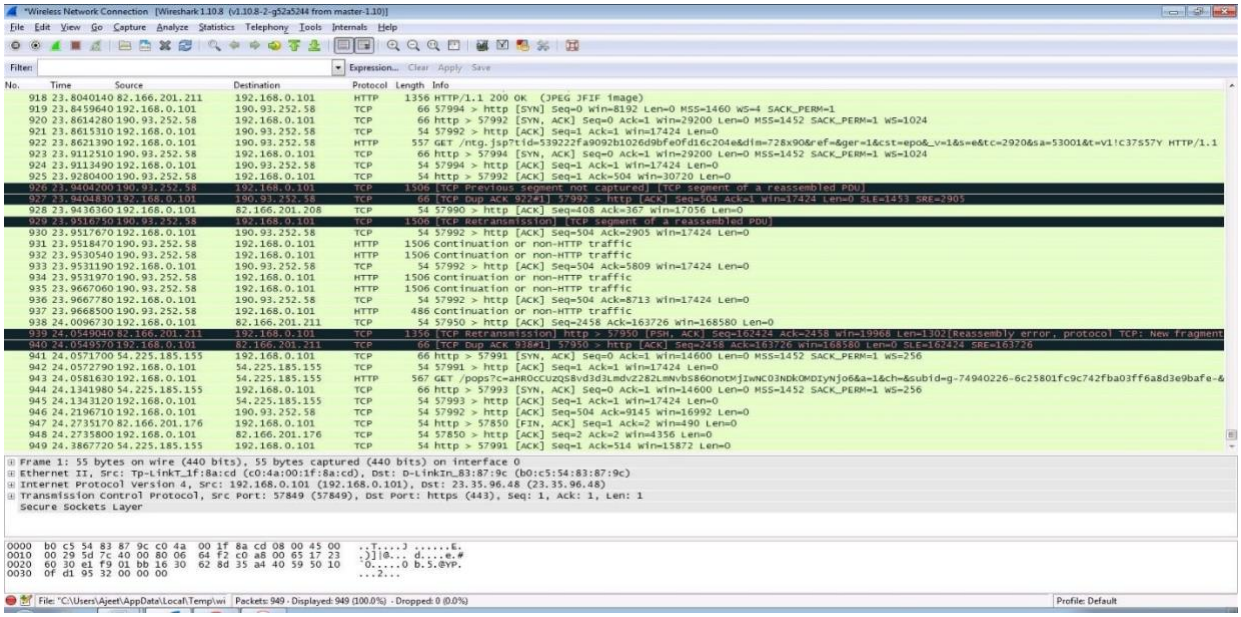
Step 5: Open a website in a new window and enter the user id and password. Register if needed.

Step 6: Enter the credentials and then sign in.

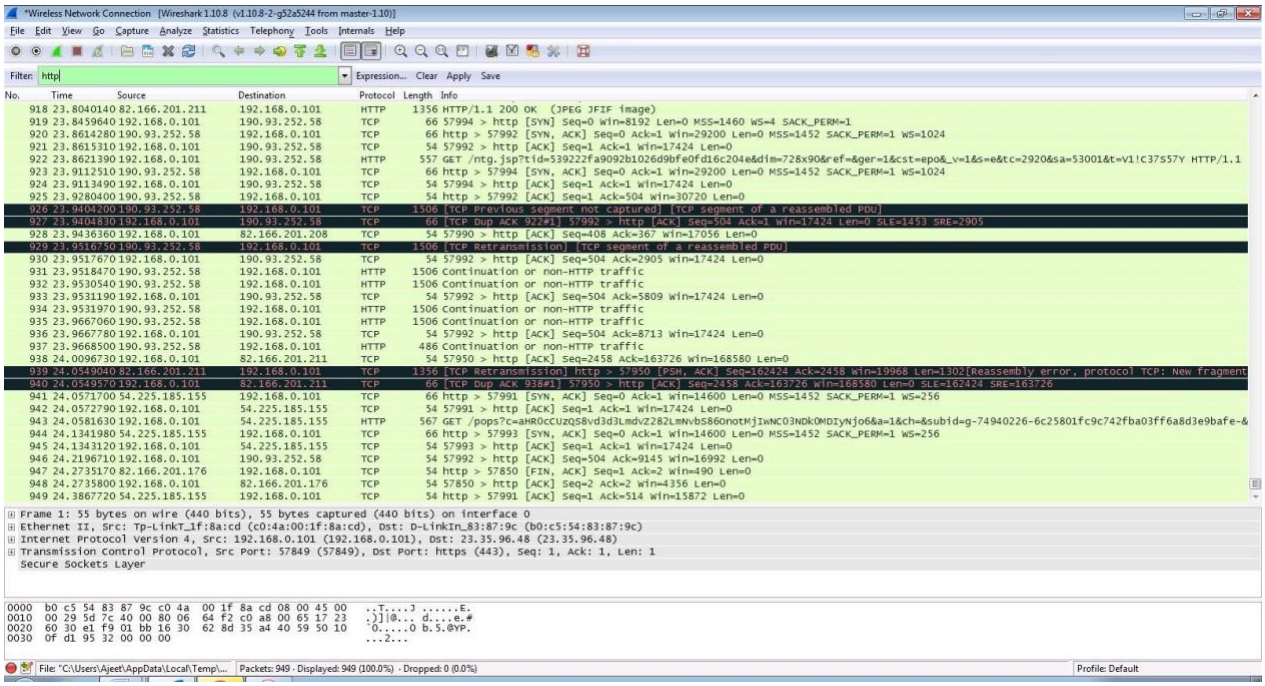


Step 7: The wireshark tool will keep recording the packets

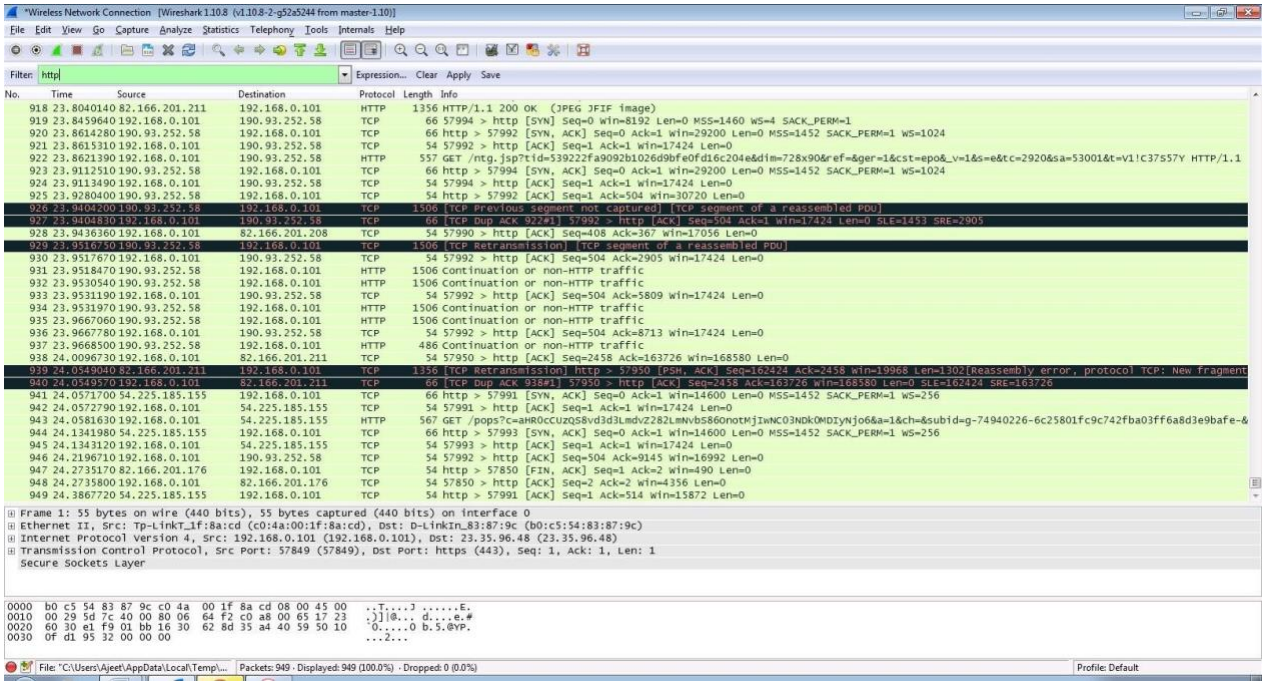
.



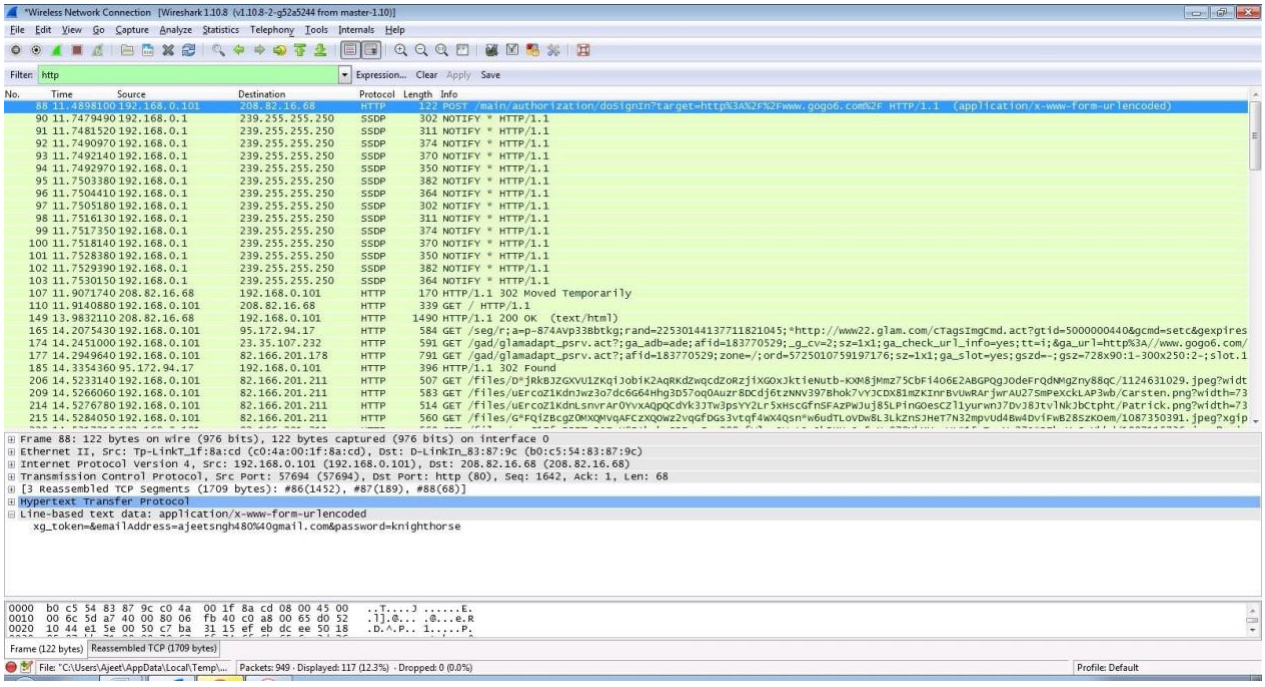
Step 8: Select filter as http to make the search easier and click on apply.



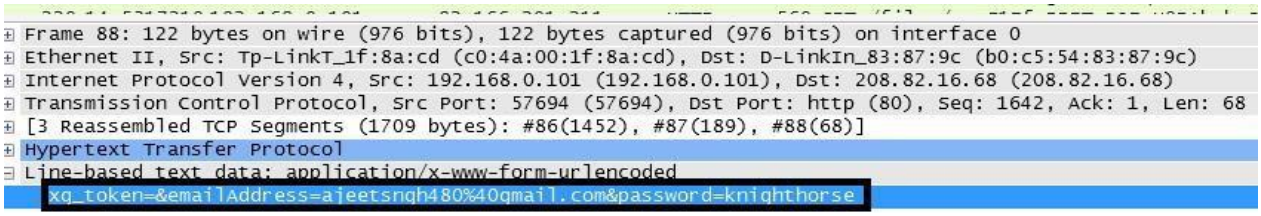
Step 9: Now stop the tool to stop recording.



Step 10: Find the post methods for username and passwords.



Step 11: U will see the email- id and password that you used to log in.


Frame 88: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0
Ethernet II, Src: Tp-LinkT_1f:8a:cd (c0:4a:00:1f:8a:cd), Dst: D-LinkIn_83:87:9c (b0:c5:54:83:87:9c)
Internet Protocol Version 4, Src: 192.168.0.101 (192.168.0.101), Dst: 208.82.16.68 (208.82.16.68)
Transmission Control Protocol, Src Port: 57694 (57694), Dst Port: http (80), Seq: 1642, Ack: 1, Len: 68
[3 Reassembled TCP Segments (1709 bytes): #86(1452), #87(189), #88(68)]
Hypertext Transfer Protocol
Line-based text data: application/x-www-form-urlencoded
xq_token=&emailAddress=ajeetsngh480%40gmail.com&password=knighthorse