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

Link for the video demonstration of the practical:

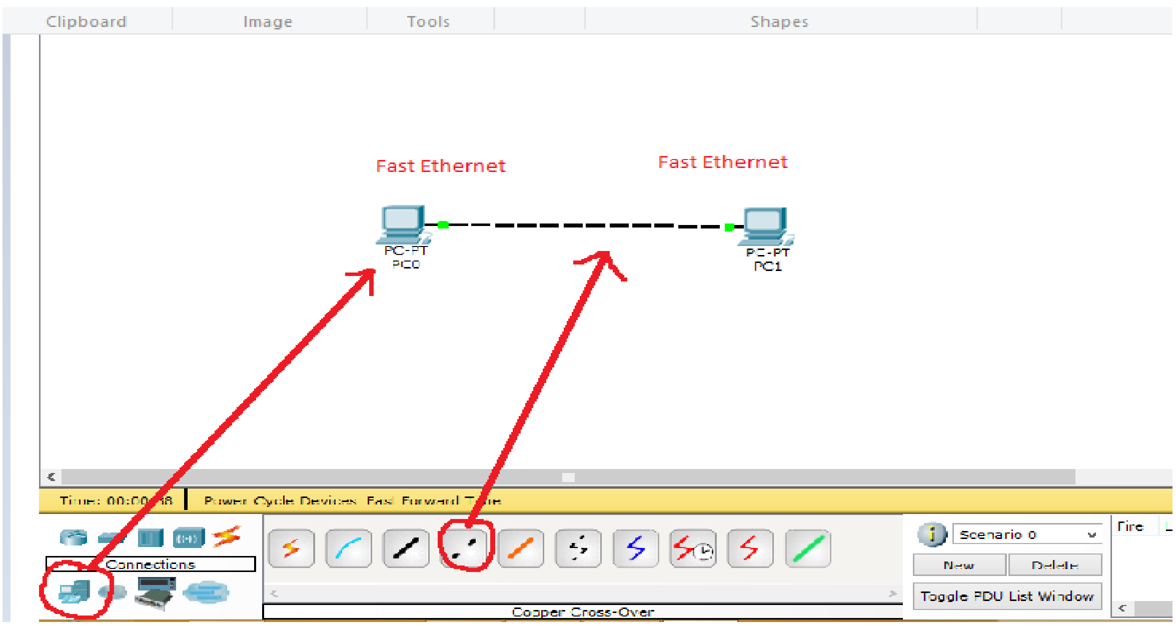
https://youtu.be/CeMNBxW5LsM

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

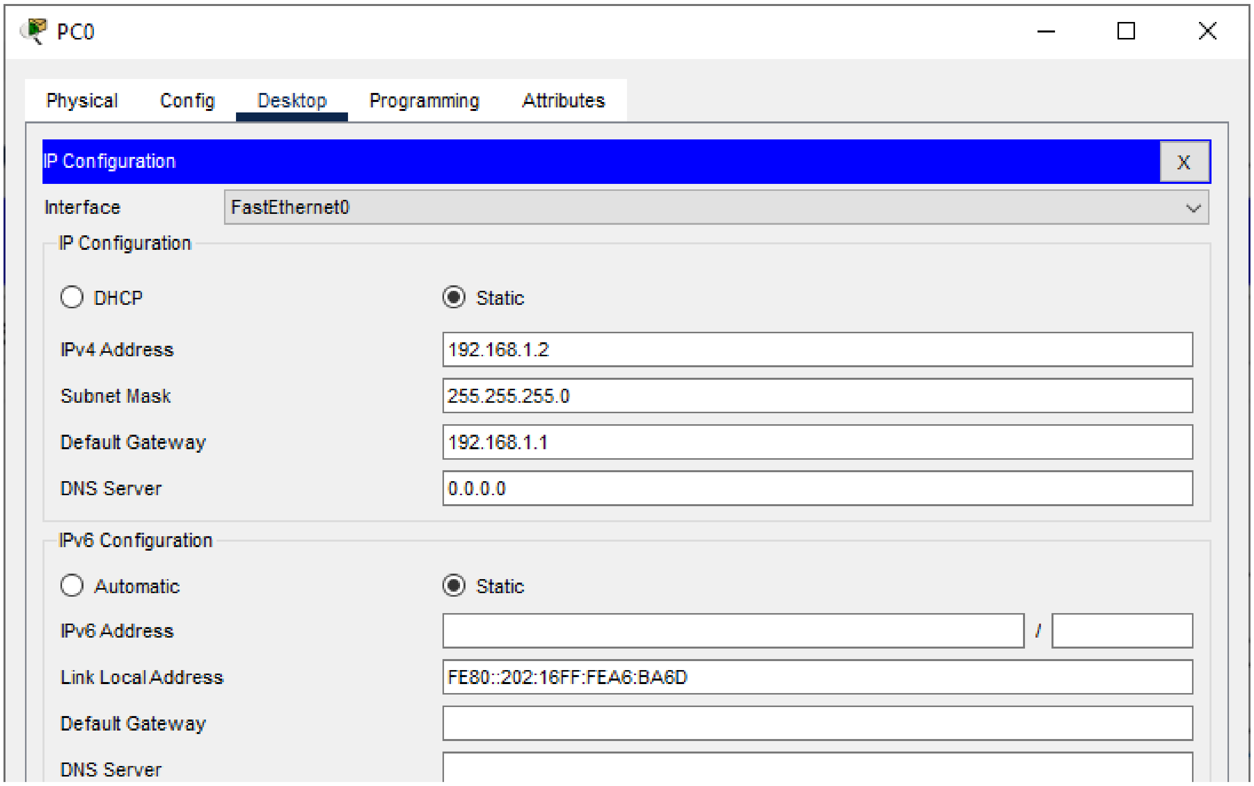
Theory:

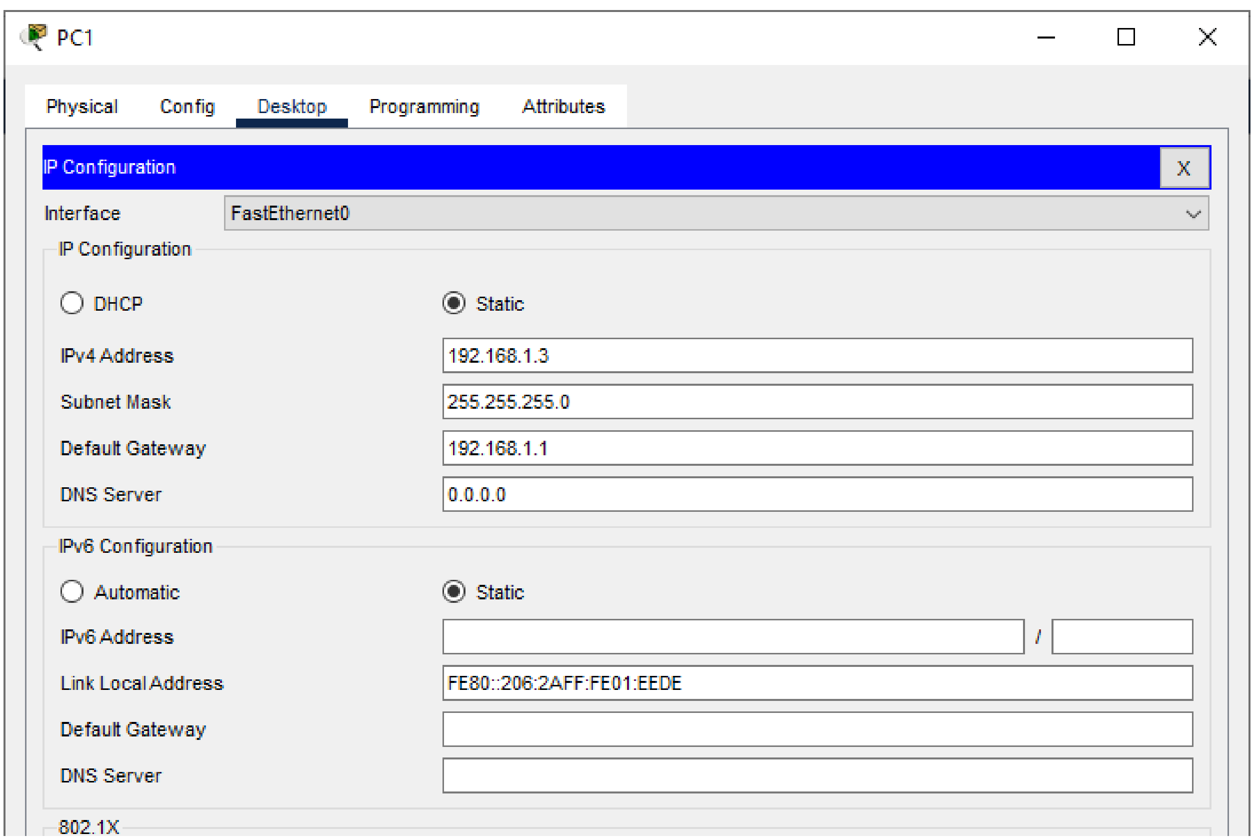
We use the following network to verify the connectivity using Cisco packet tracer



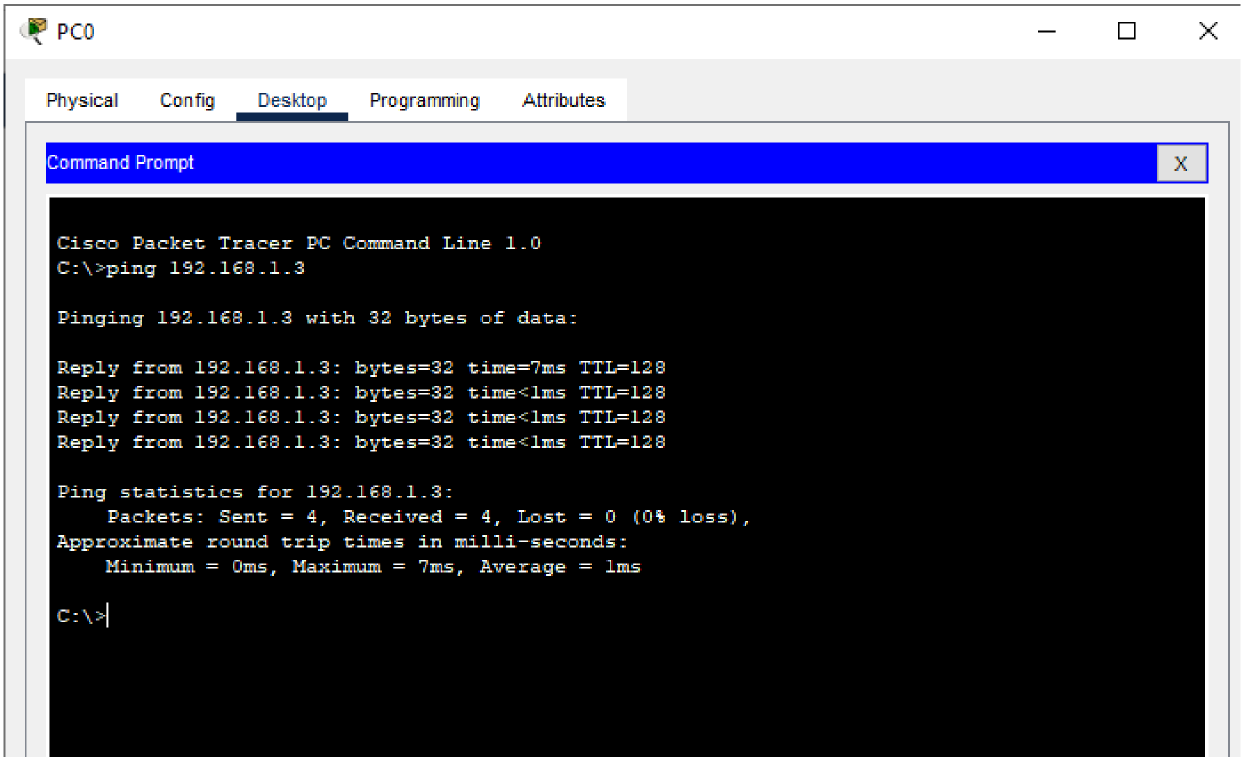
Now we set the ip address of the devices as follows

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.

Link for the video demonstration of the practical:

https://youtu.be/yYYqDgM1XqQ

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.

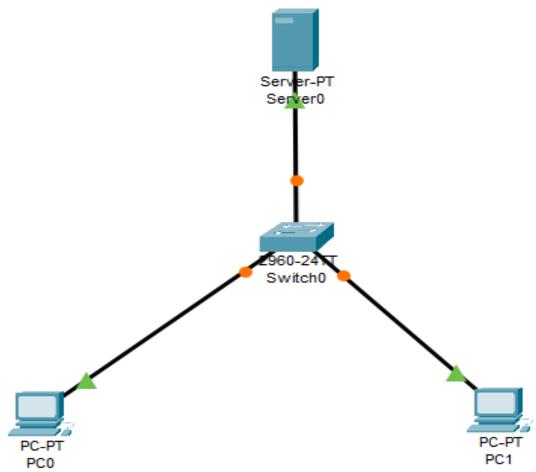
DHCP provides the following benefits.

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.

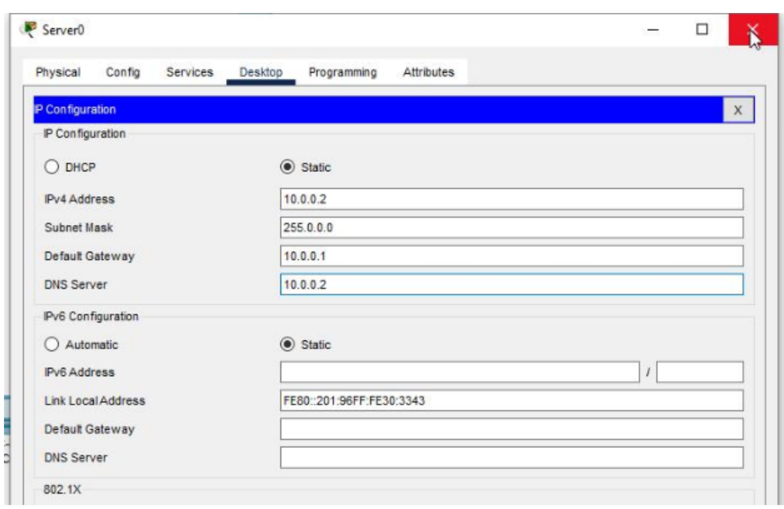
2) Reduced network administration. DHCP includes the following features to reduce network administration

   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.

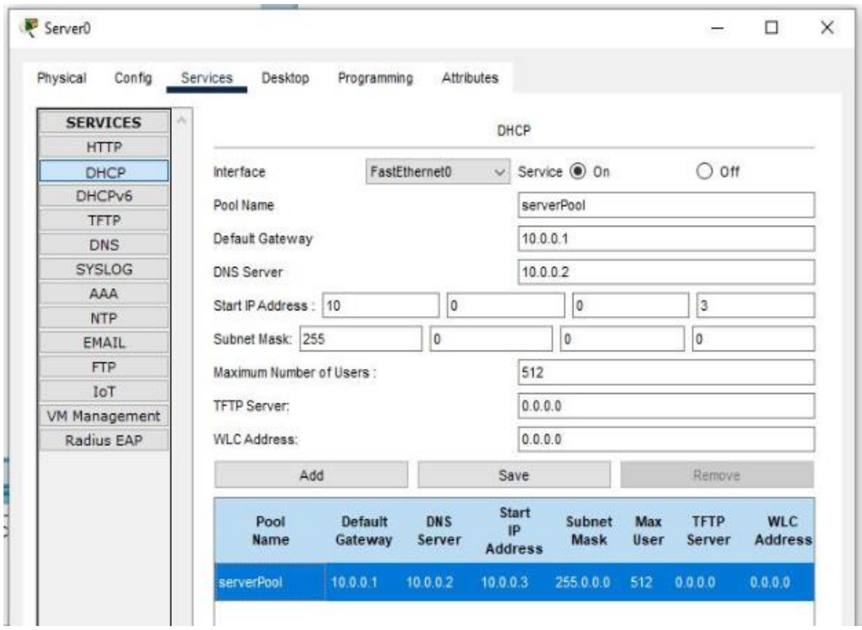
We use the following topology for the present case



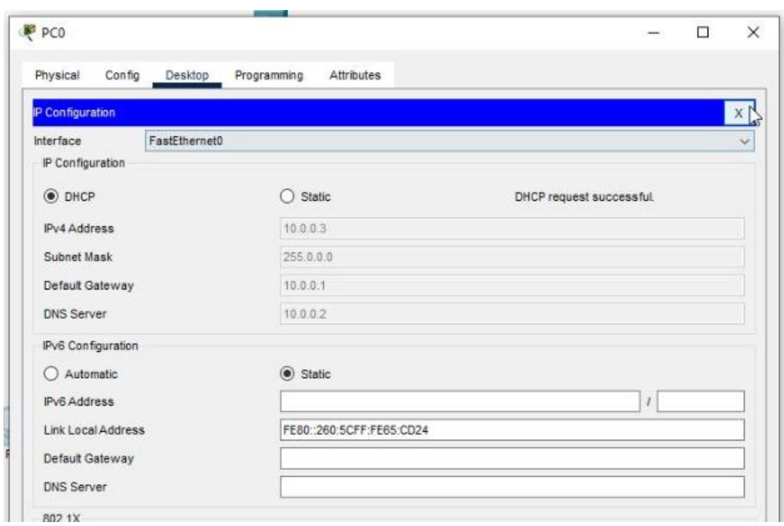
Configuring the Server:

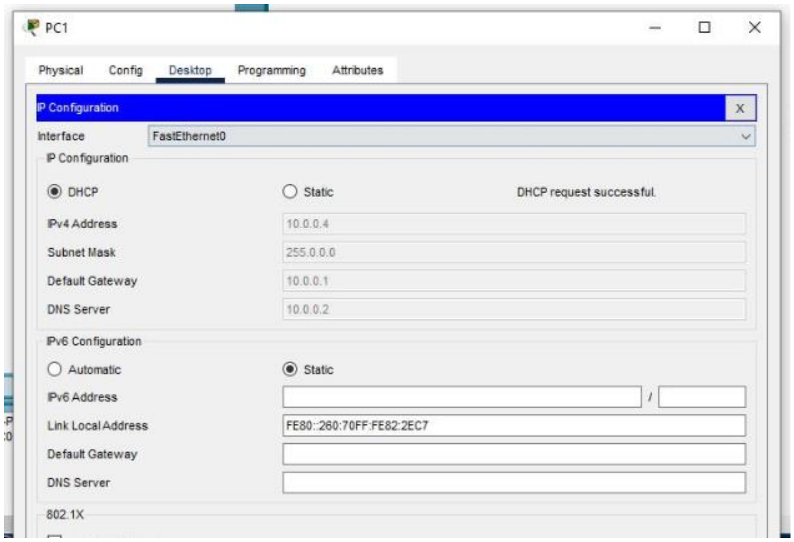


Enabling and setting the DHCP Service on the Server:

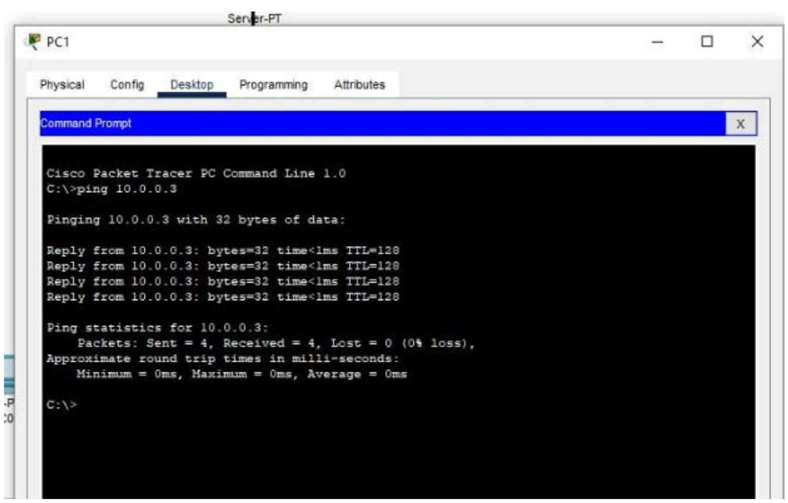


Verifying the Dynamic Addressing on both the PCs:





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.

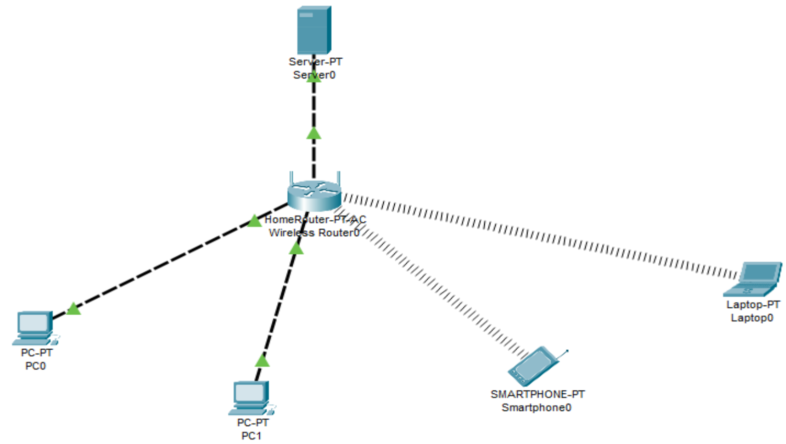
1) It is easier to set up compared to setting up a wired network.
2) It is more convenient to access.
3) It is less complicated to add new users in the network.
4) It gives users more flexibility to stay online even when moving from one area in the office to another.
5) Guest users can have Internet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

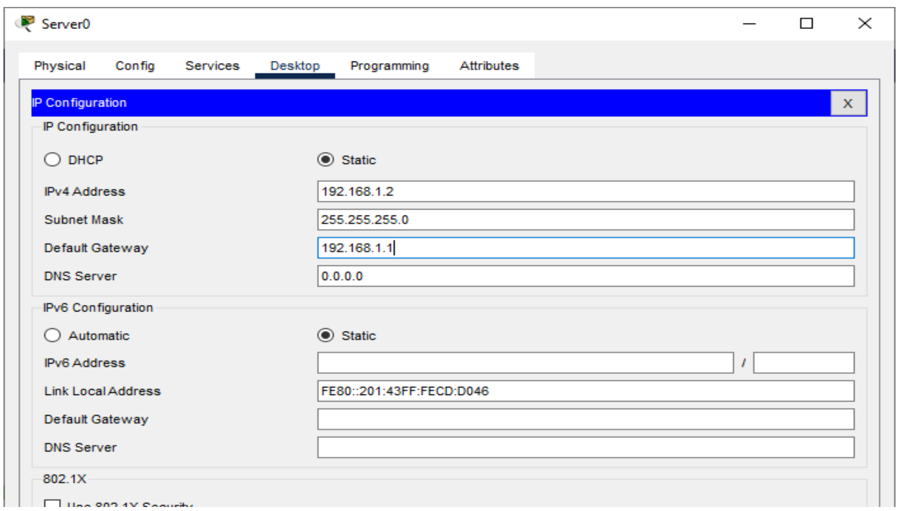
With a WAP, the following can be done:

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.

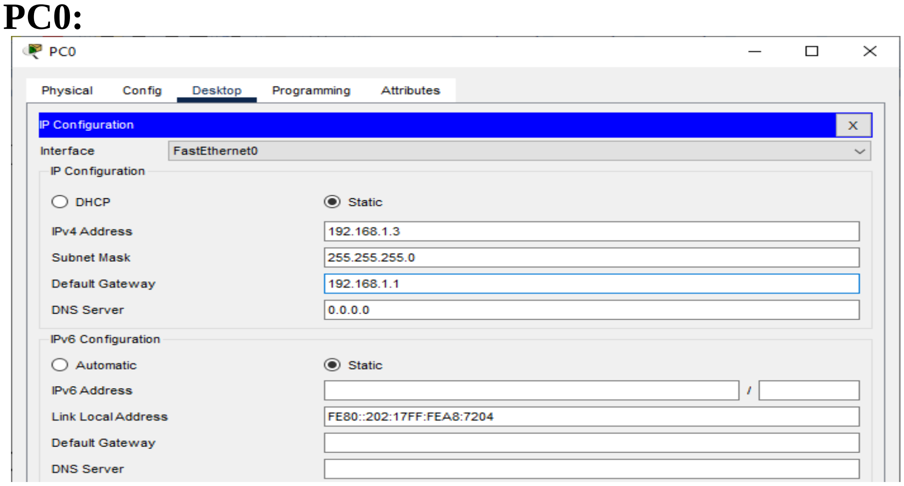
For the present case we use the following topology



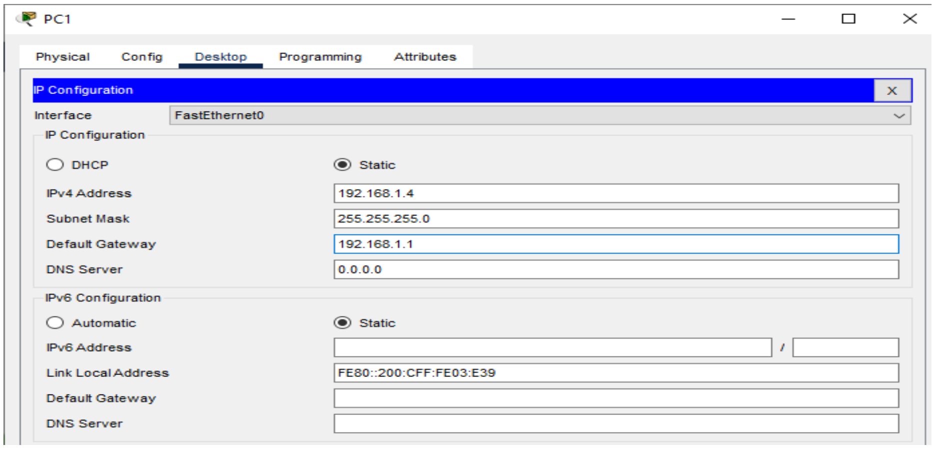
Configure the Server:



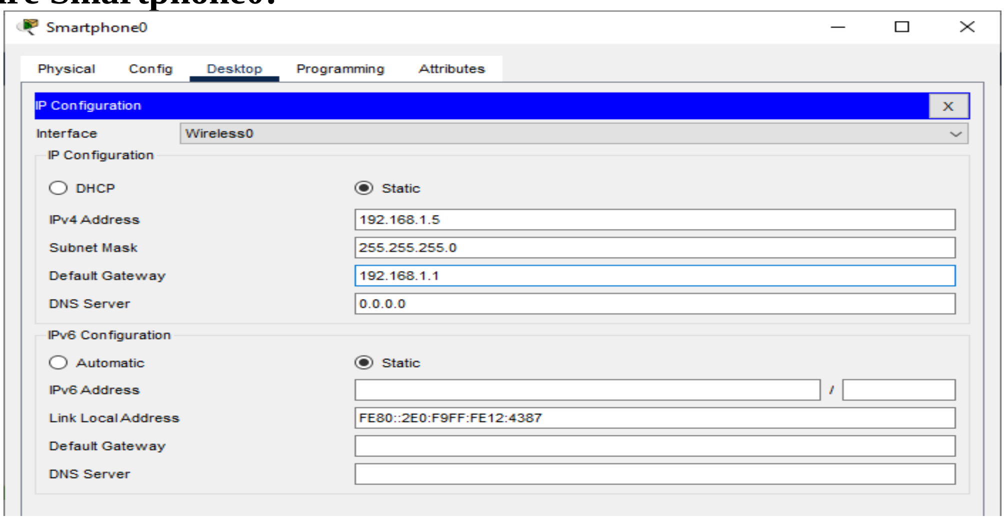
Configure PC0:



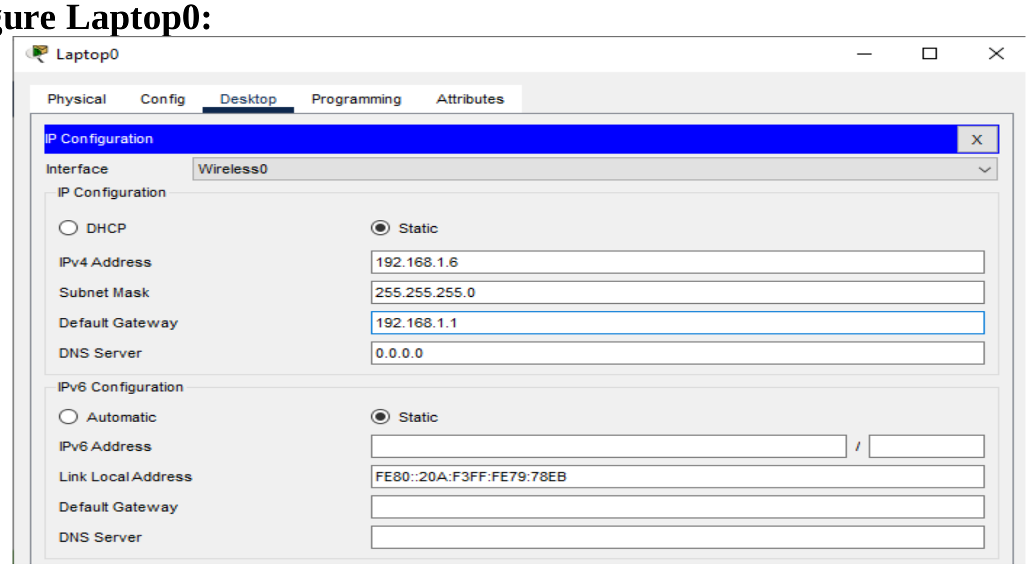
Configure PC1:



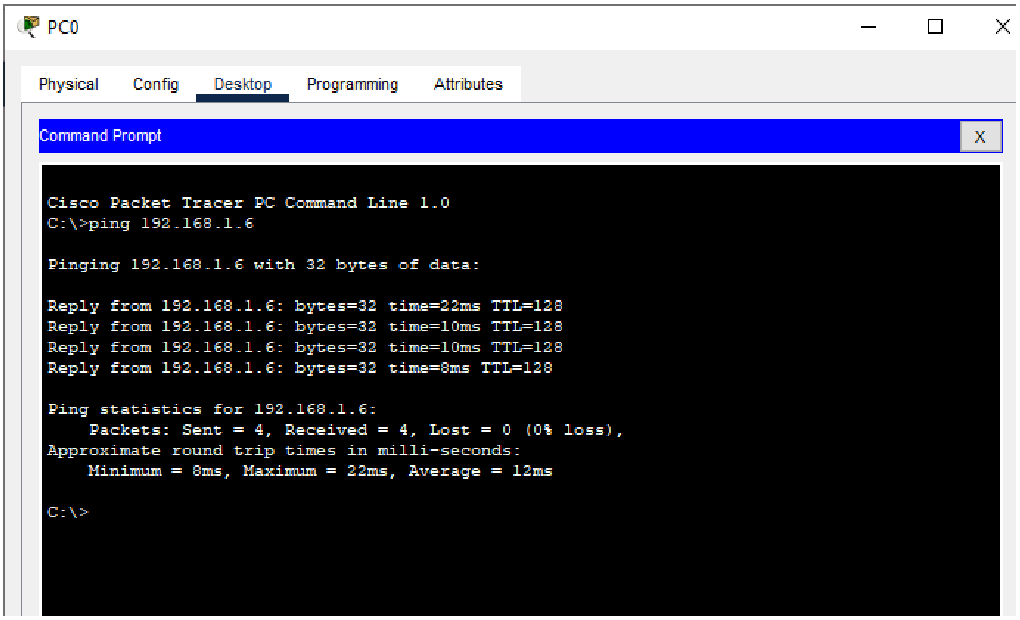
Configure Smartphone0:



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 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

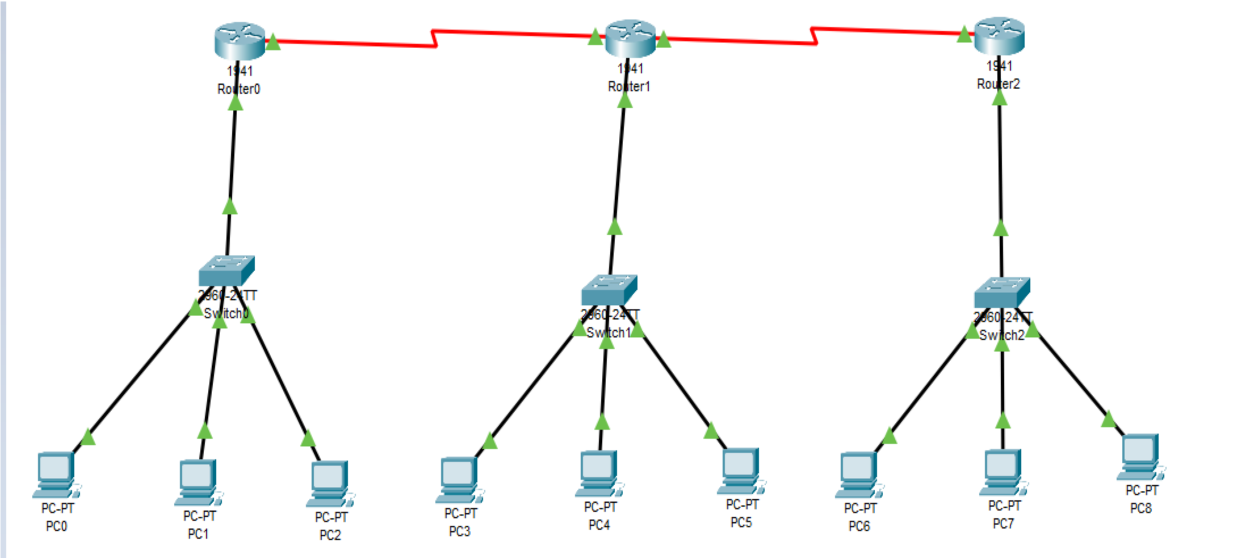
Pros:

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.

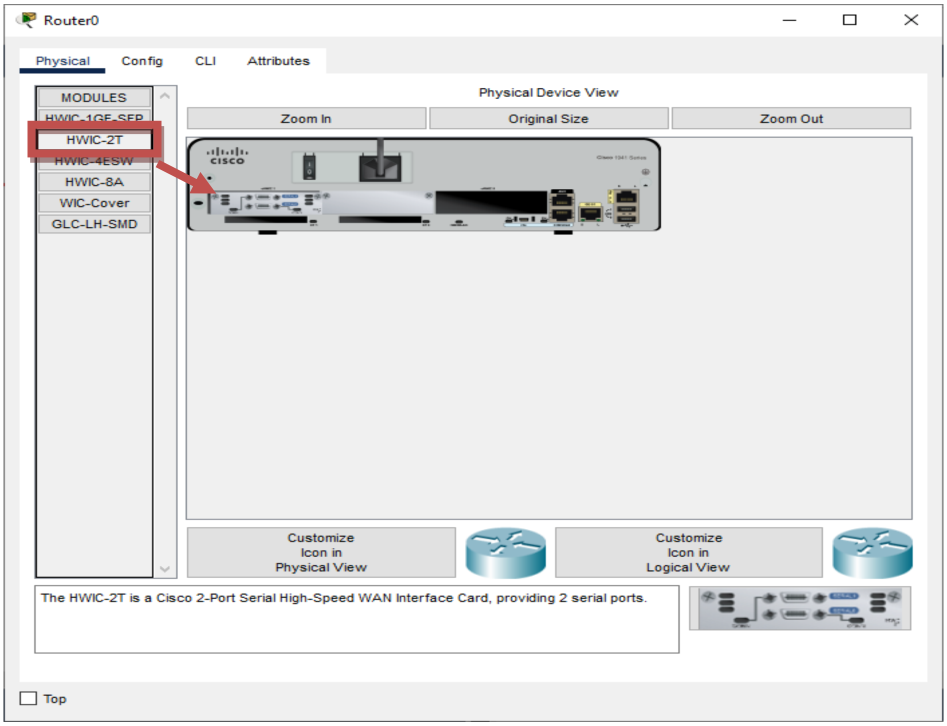
We use the following topology for the present case



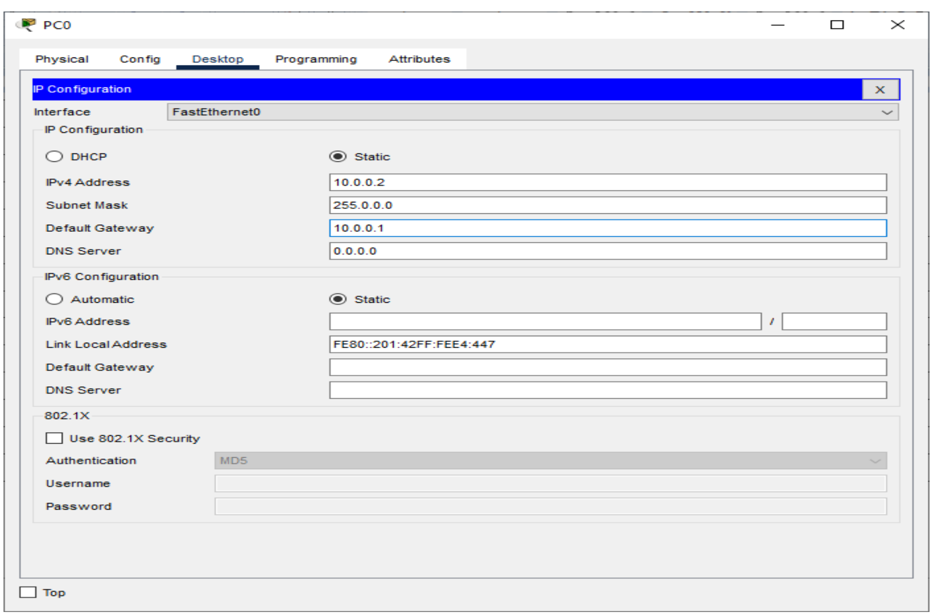
We configure the above network using the following IP addresses

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	FastEthernet0	10.0.0.2	10.0.0.0	10.0.0.1
PC1	FastEthernet0	10.0.0.3	10.0.0.0	10.0.0.1
PC2	FastEthernet0	10.0.0.4	10.0.0.0	10.0.0.1
PC3	FastEthernet0	20.0.0.2	20.0.0.0	20.0.0.1
PC4	FastEthernet0	20.0.0.3	20.0.0.0	20.0.0.1
PC5	FastEthernet0	20.0.0.4	20.0.0.0	20.0.0.1
PC6	FastEthernet0	30.0.0.2	30.0.0.0	30.0.0.1
PC7	FastEthernet0	30.0.0.3	30.0.0.0	30.0.0.1
PC8	FastEthernet0	30.0.0.4	30.0.0.0	30.0.0.1

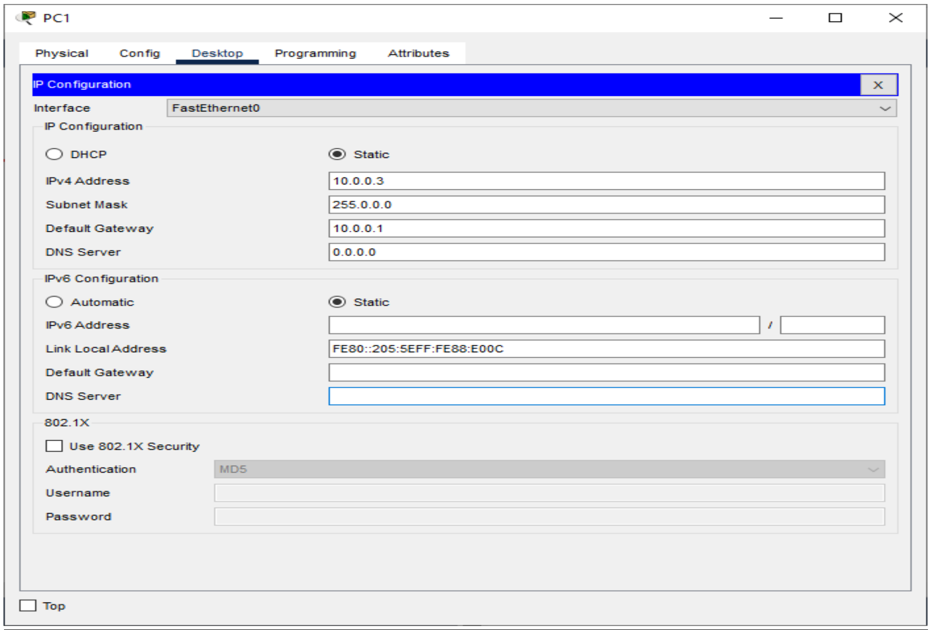
Adding Serial Interface in each Router



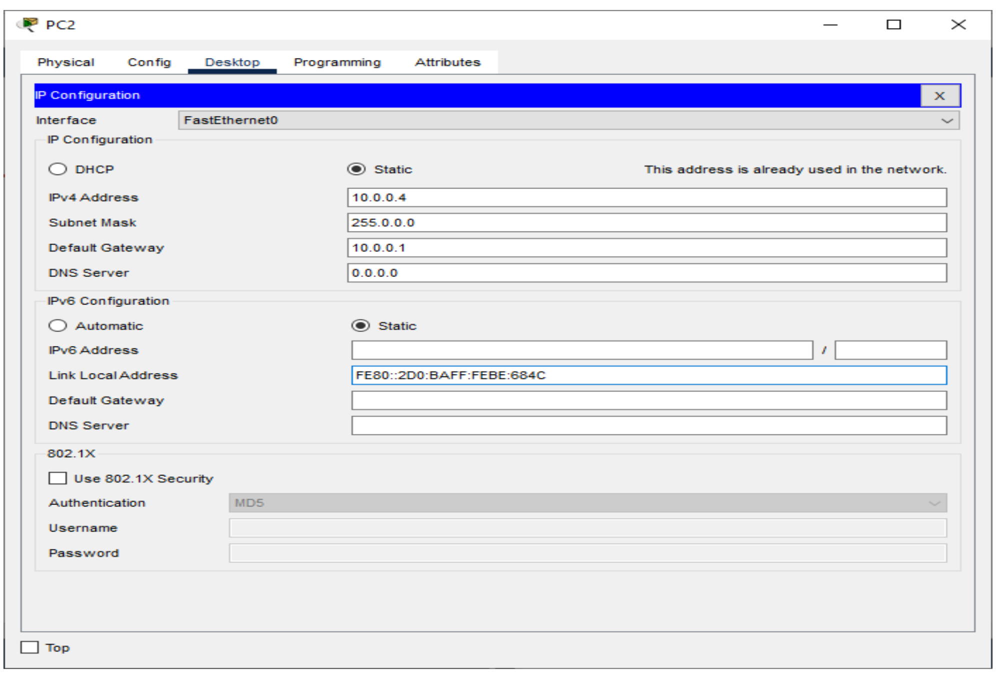
Configuring PC0:



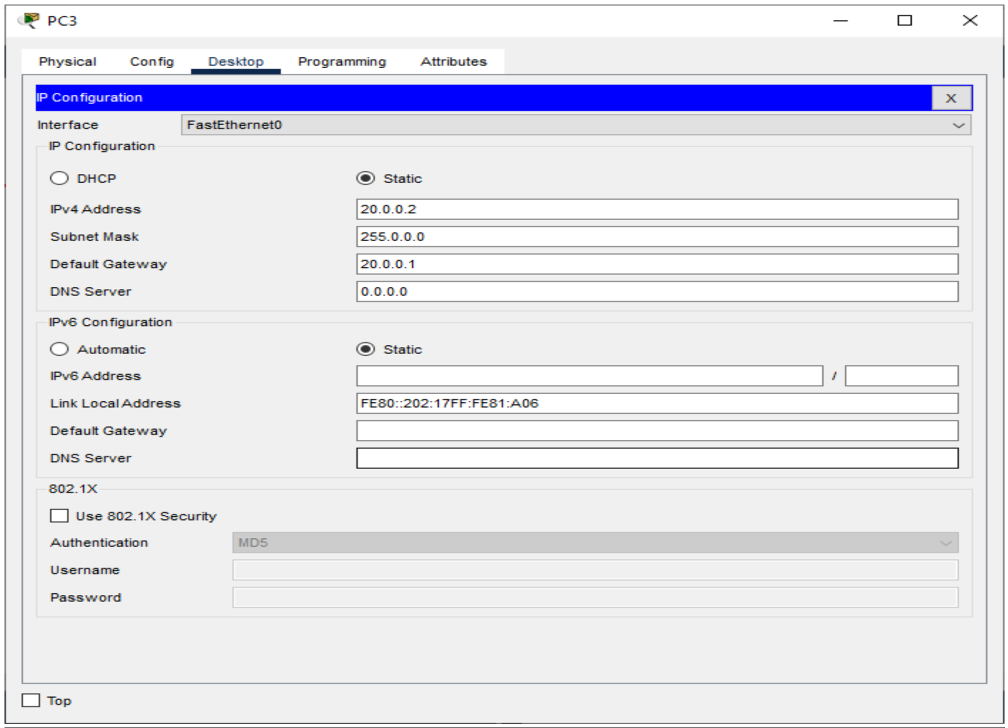
Configuring PC1:



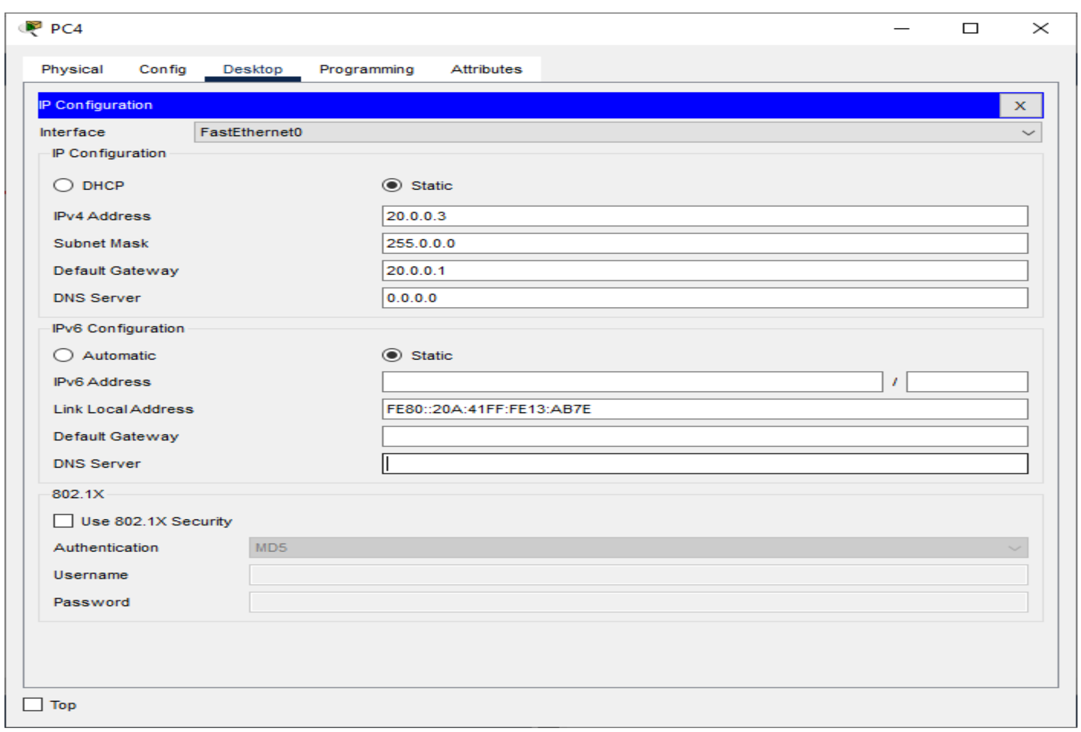
Configuring PC2:



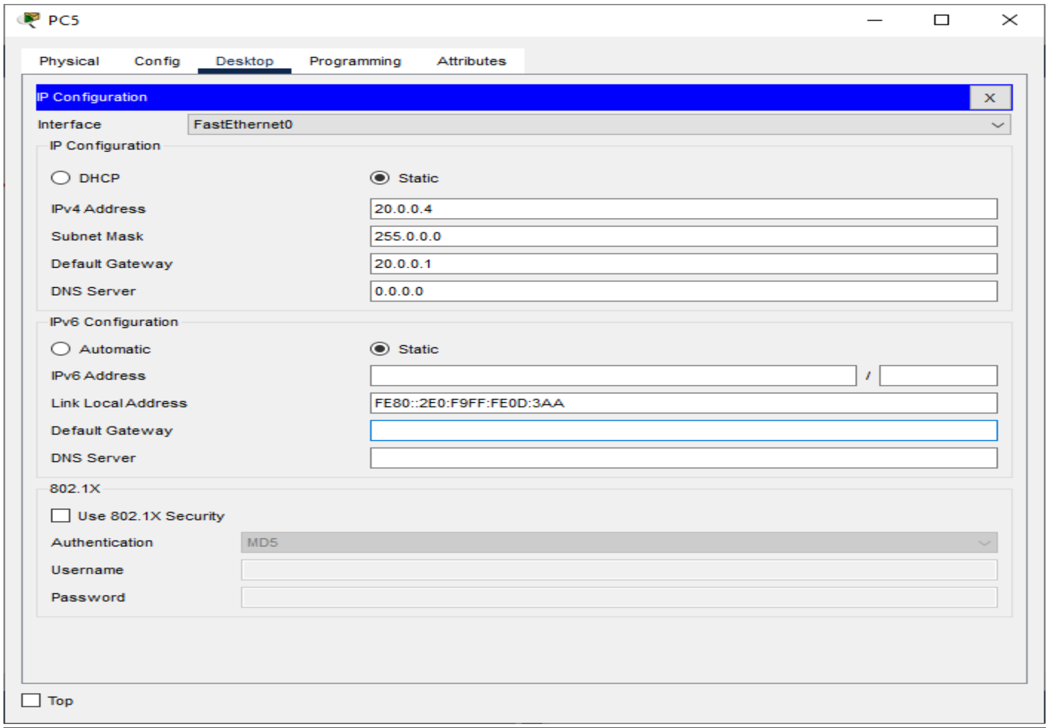
Configuring PC3:



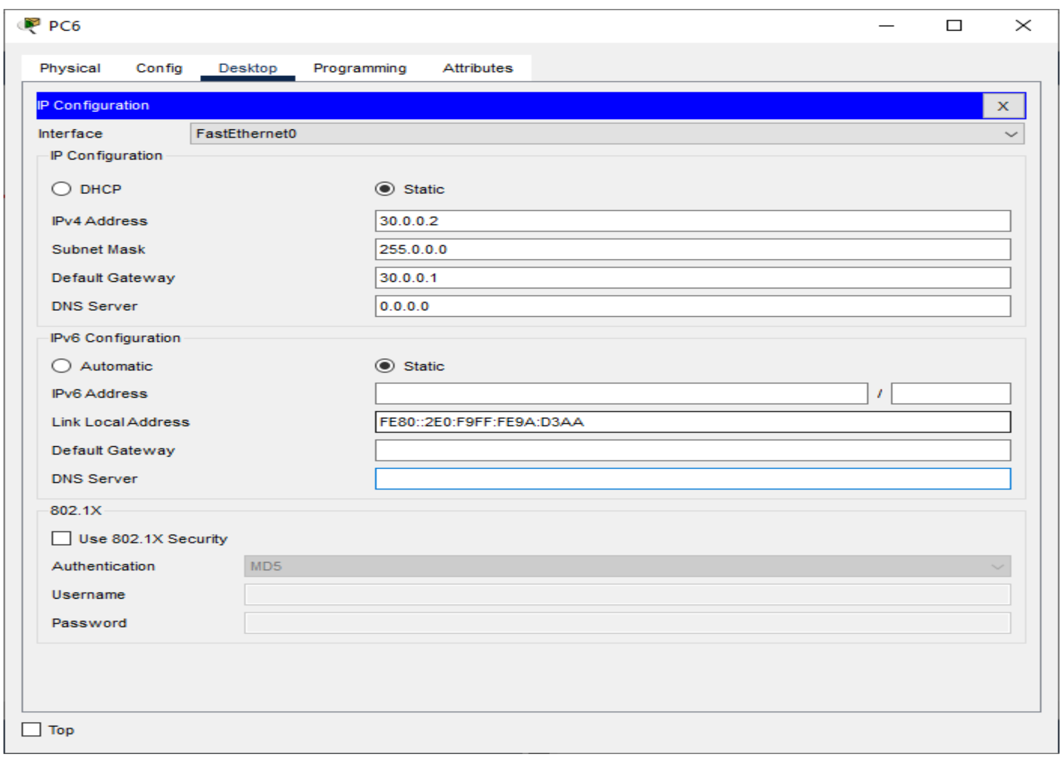
Configuring PC4:



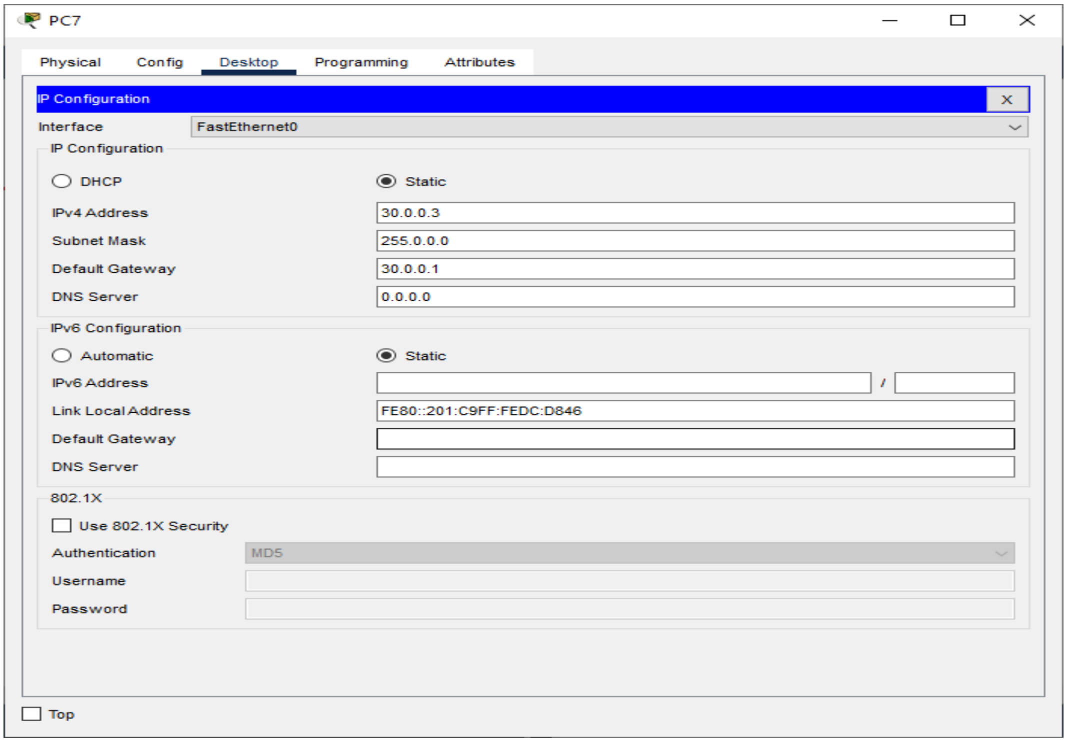
Configuring PC5:



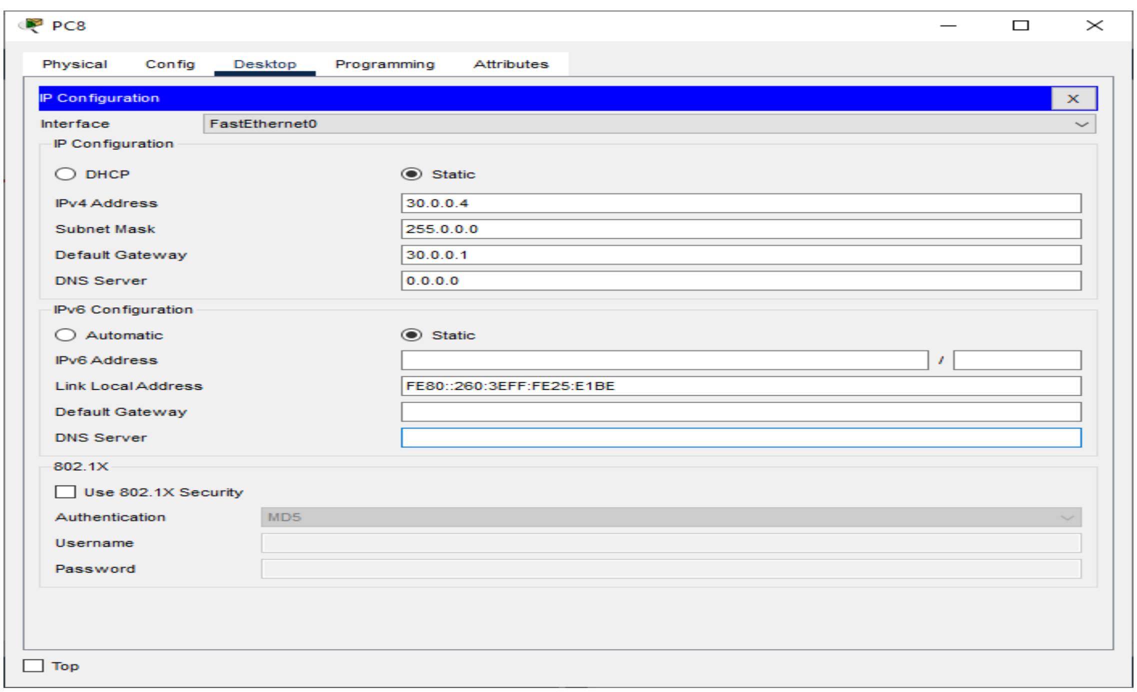
Configuring PC6:



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

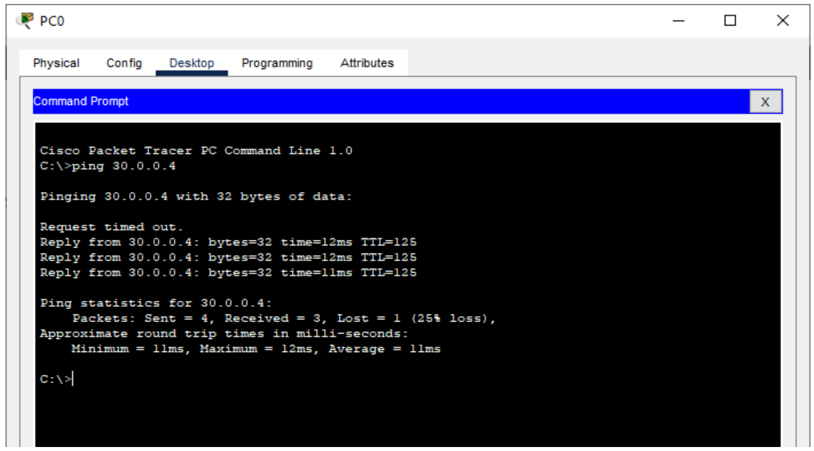
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 192.168.0.0
Router(config-router)#network 20.0.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#
Router#

Setting the RIPv1 on Router 2

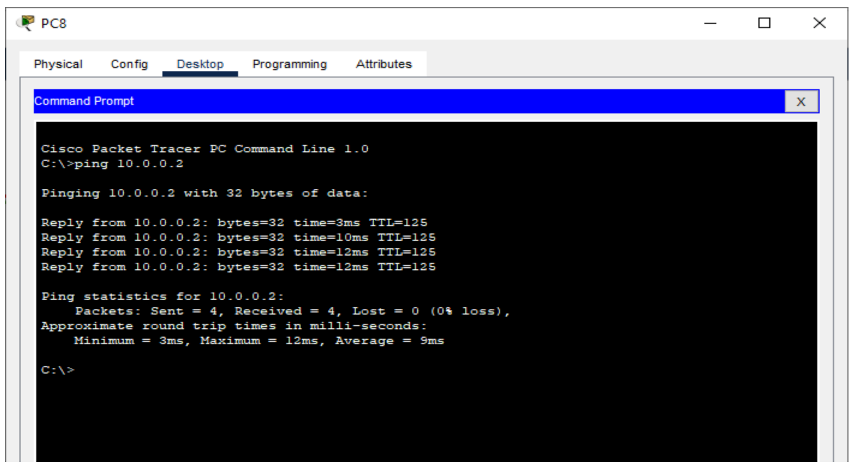
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#network 192.168.1.0
Router(config-router)#network 30.0.0.0
Router(config-router)#exit
Router(config)#

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

Link for the video demonstration of the practical:

https://youtu.be/DLMpobkrDGw

Practical No 6

Aim: Using Packet Tracer to create a network with three routers with RIPv2 and each 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 is also a distance vector routing protocol but has a few enhancements to make it more efficient than RIPv1.
RIPv2 is more efficient than RIPv1, but is not suitable for larger, more complex networks. It simply provides more flexibility on smaller networks.
RIPv2 uses the same routing metric as RIPv1, the hop count. Updates with RIPv2 are 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 subnetting and discontiguous networks.
RIPv2 allows for authentication to be required for updates. When authentication is enabled, 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 the update.

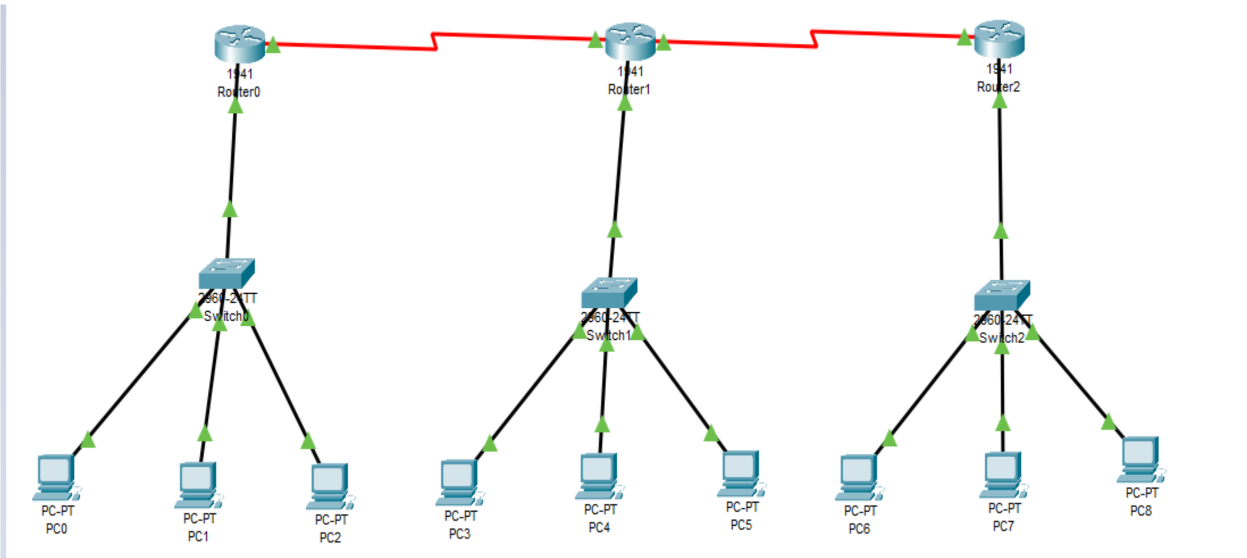
Advantages of RIPv2

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).

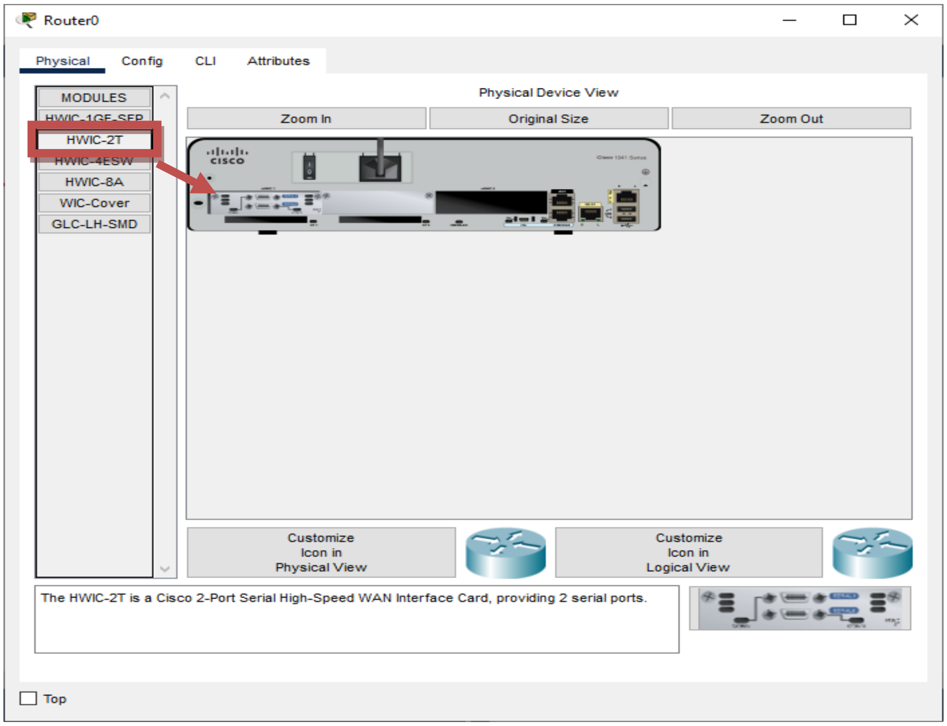
We use the following topology for the present case



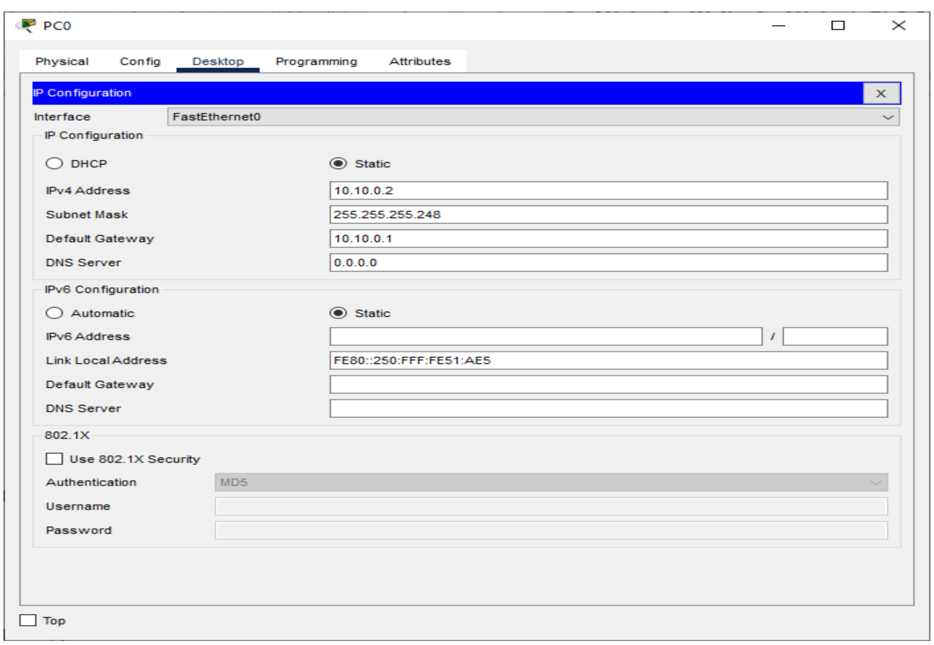
We configure the above network using the following IP addresses

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	FastEthernet0	10.10.0.2	255.255.255.248	10.10.0.0	10.10.0.1
PC1	FastEthernet0	10.10.0.3	255.255.255.248	10.10.0.0	10.10.0.1
PC2	FastEthernet0	10.10.0.4	255.255.255.248	10.10.0.0	10.10.0.1
PC3	FastEthernet0	10.20.0.2	255.255.255.248	10.20.0.0	10.20.0.1
PC4	FastEthernet0	10.20.0.3	255.255.255.248	10.20.0.0	10.20.0.1
PC5	FastEthernet0	10.20.0.4	255.255.255.248	10.20.0.0	10.20.0.1
PC6	FastEthernet0	10.30.0.2	255.255.255.248	10.30.0.0	10.30.0.1
PC7	FastEthernet0	10.30.0.3	255.255.255.248	10.30.0.0	10.30.0.1
PC8	FastEthernet0	10.30.0.4	255.255.255.248	10.30.0.0	10.30.0.1

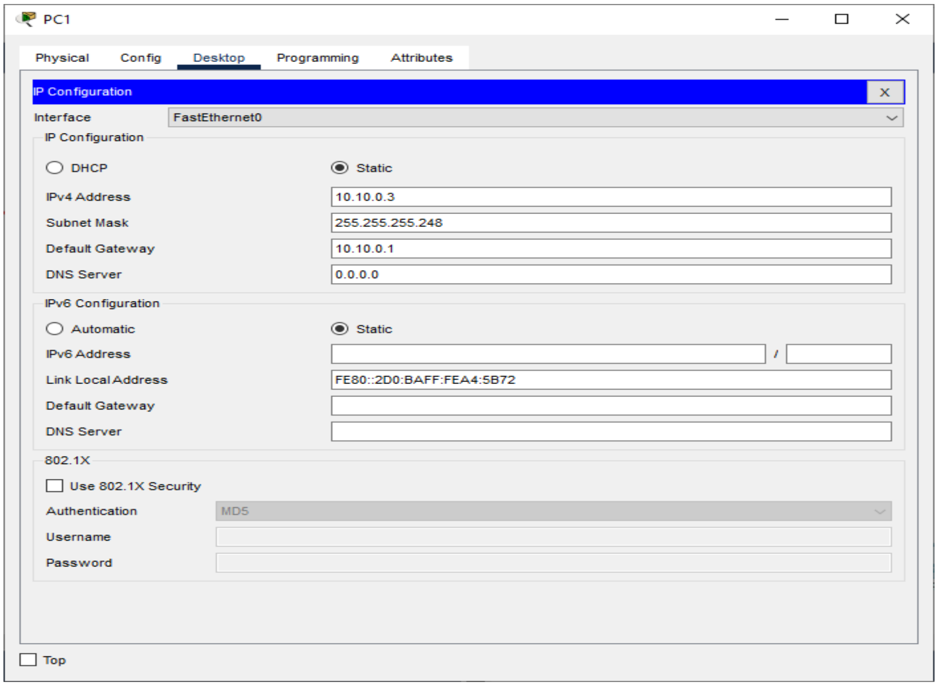
Adding Serial Interface in each Router



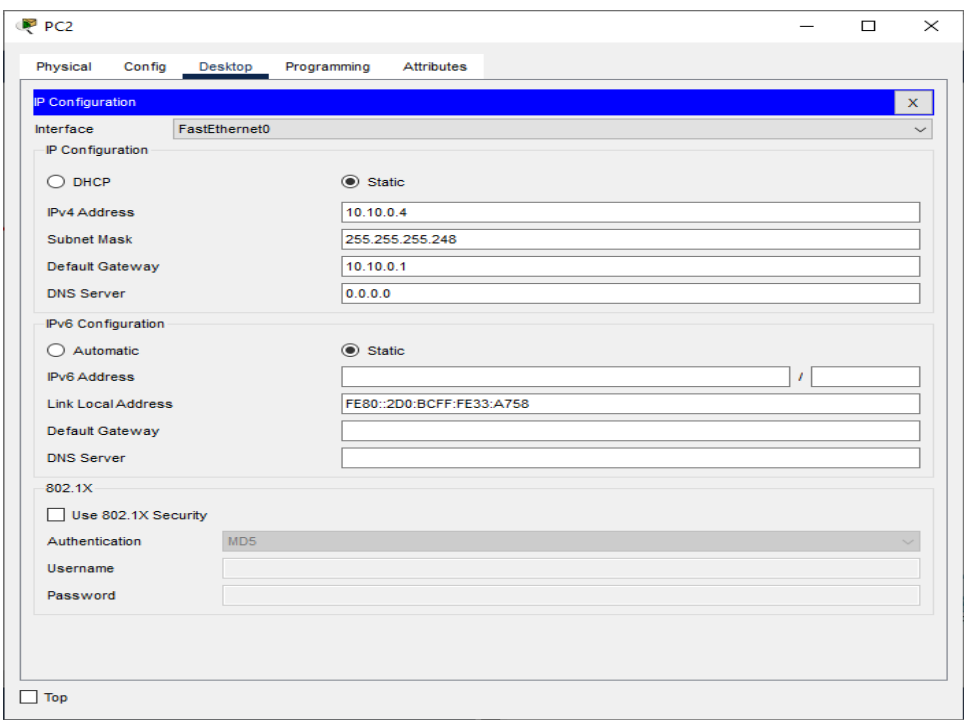
Configuring PC0:



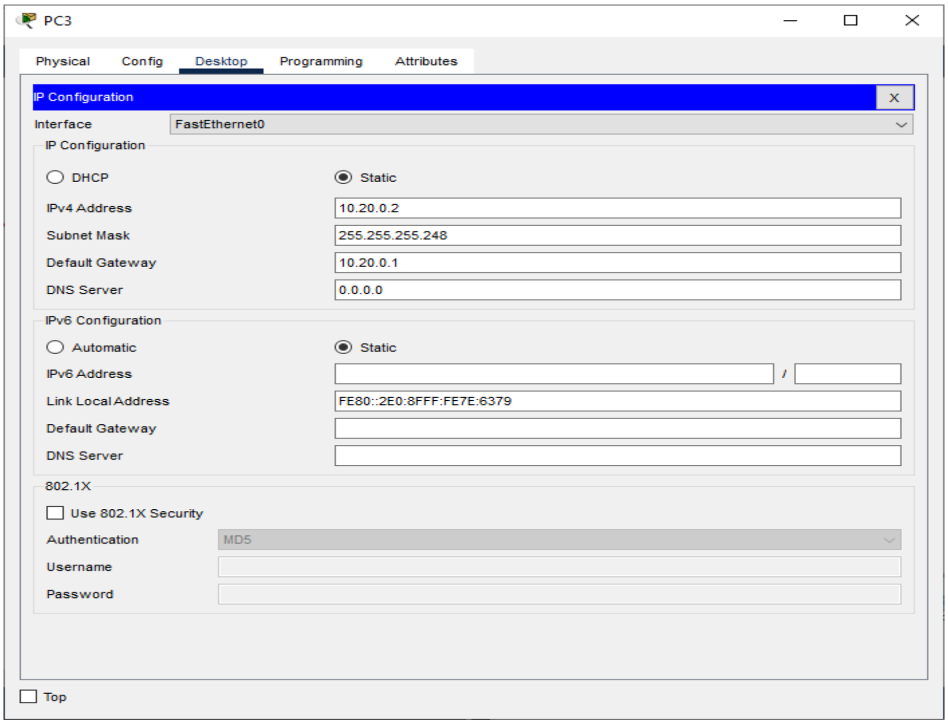
Configuring PC1:



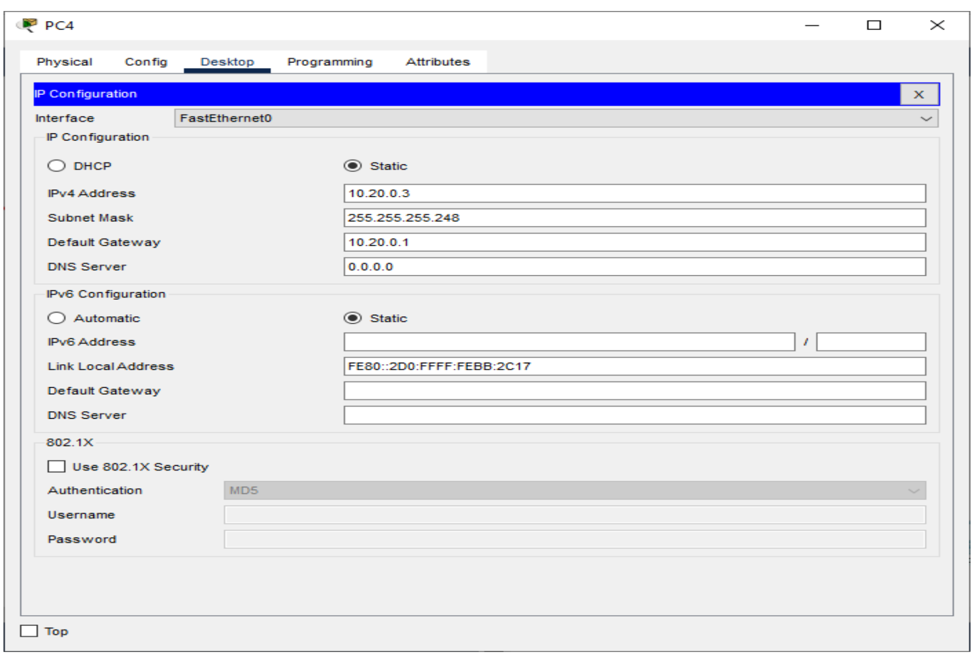
Configuring PC2:



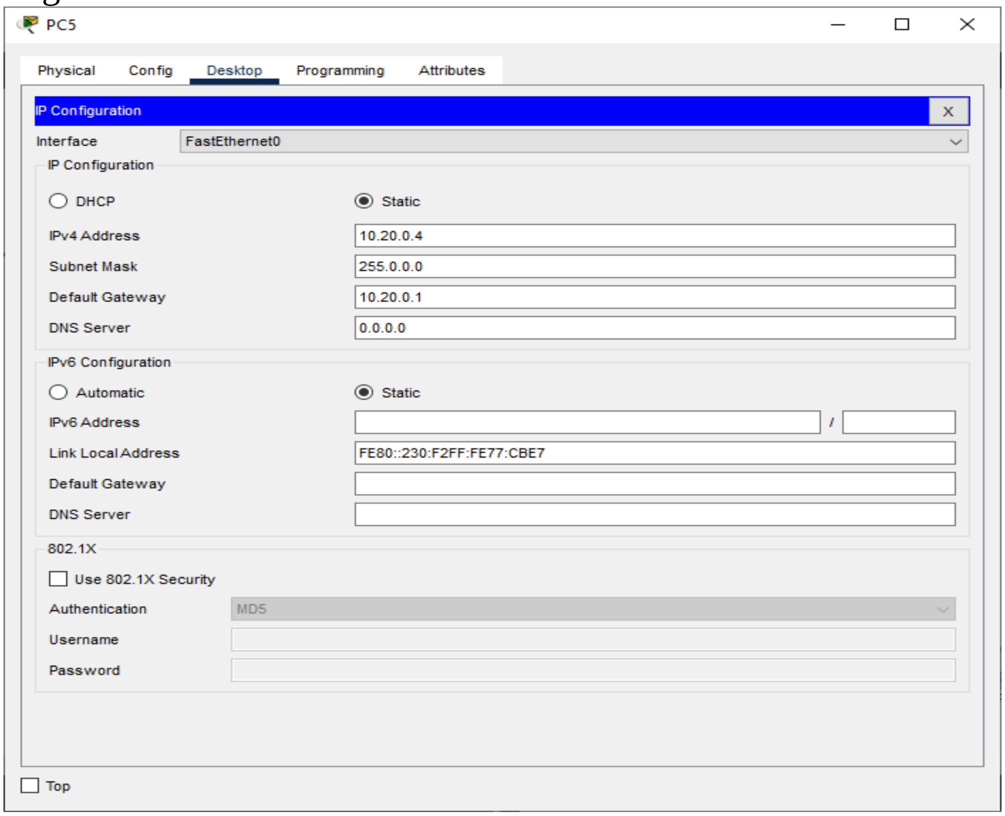
Configuring PC3:



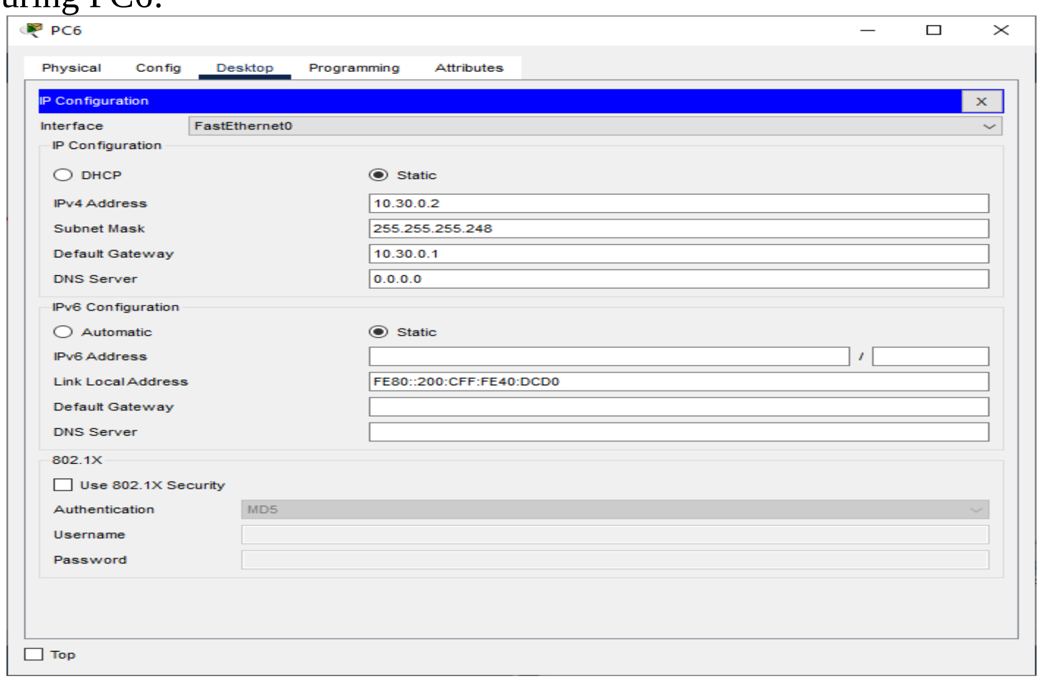
Configuring PC4:



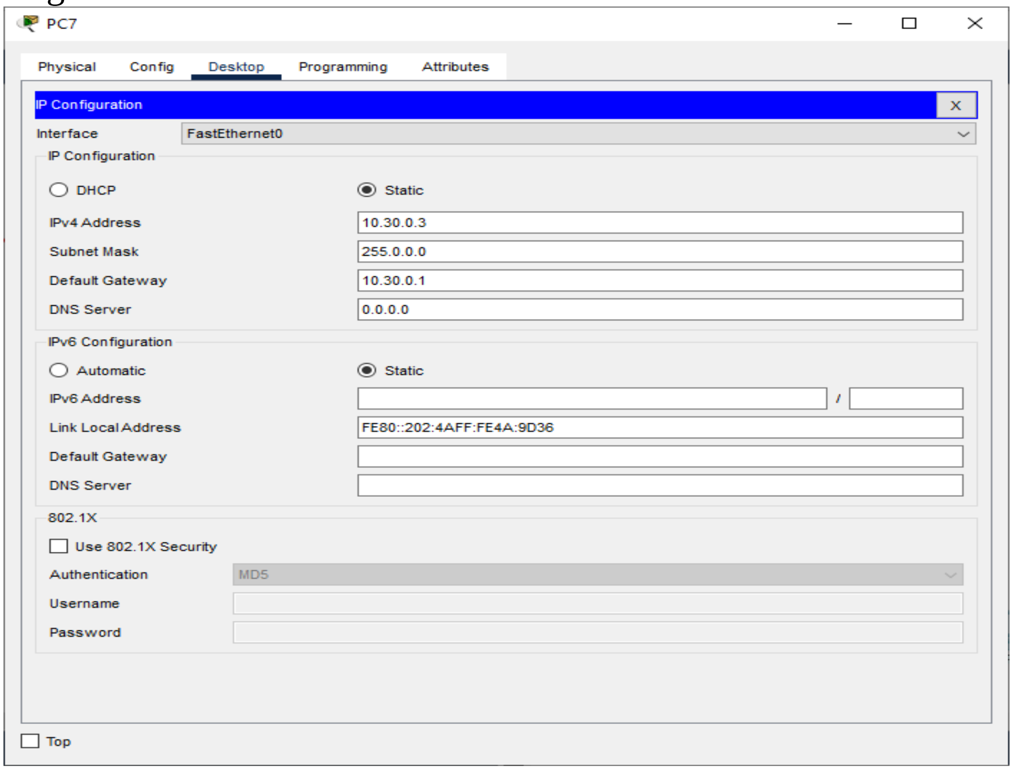
Configuring PC5:



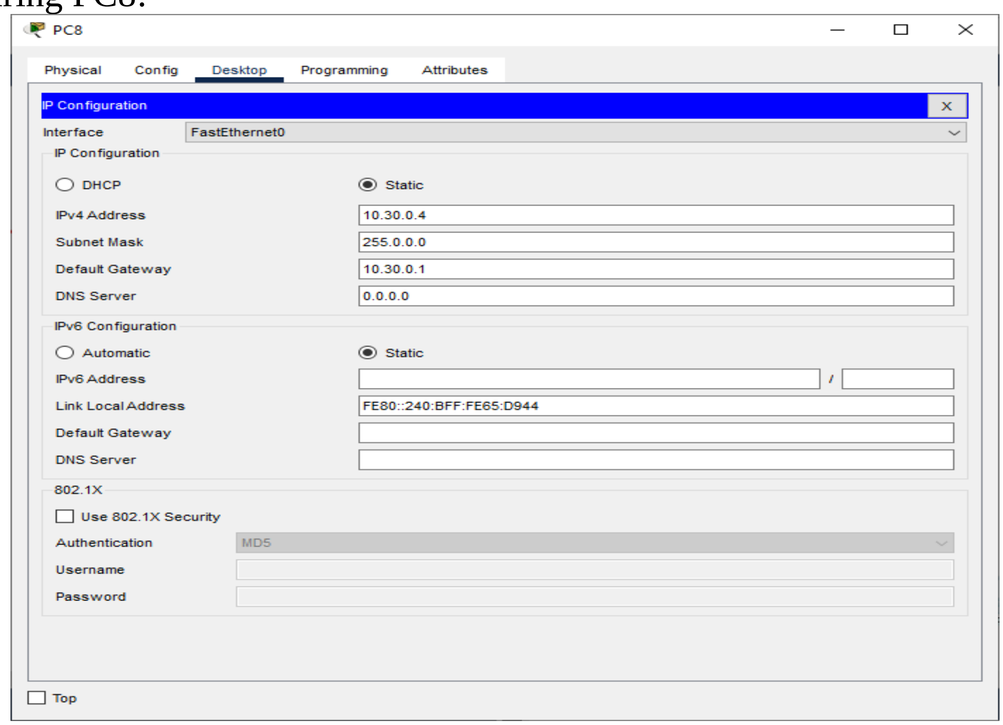
Configuring PC6:



Configuring PC7:

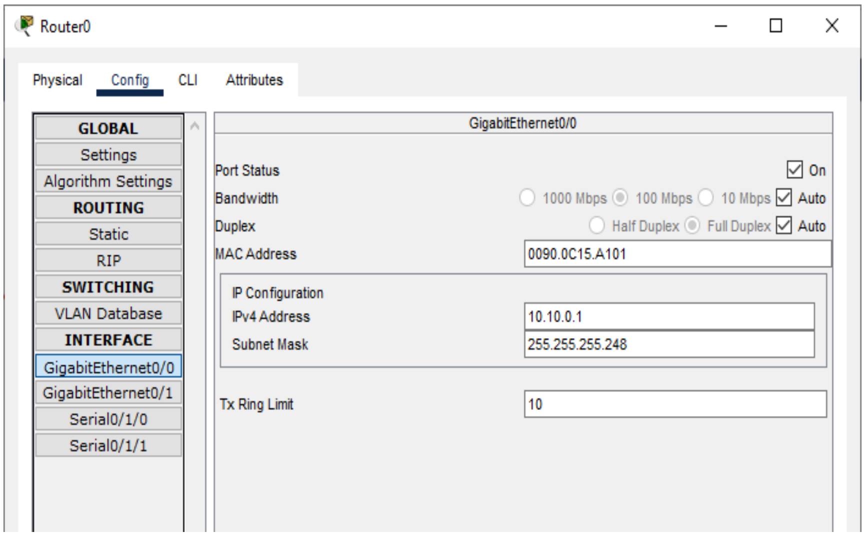


Configuring PC8:

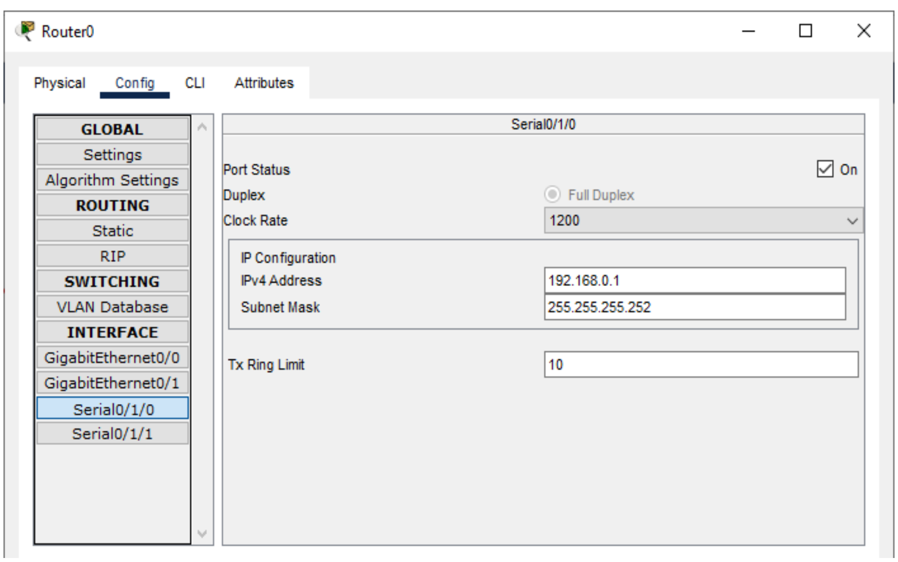


Configuring IP addresses on Router 0

i) Interface G0/0

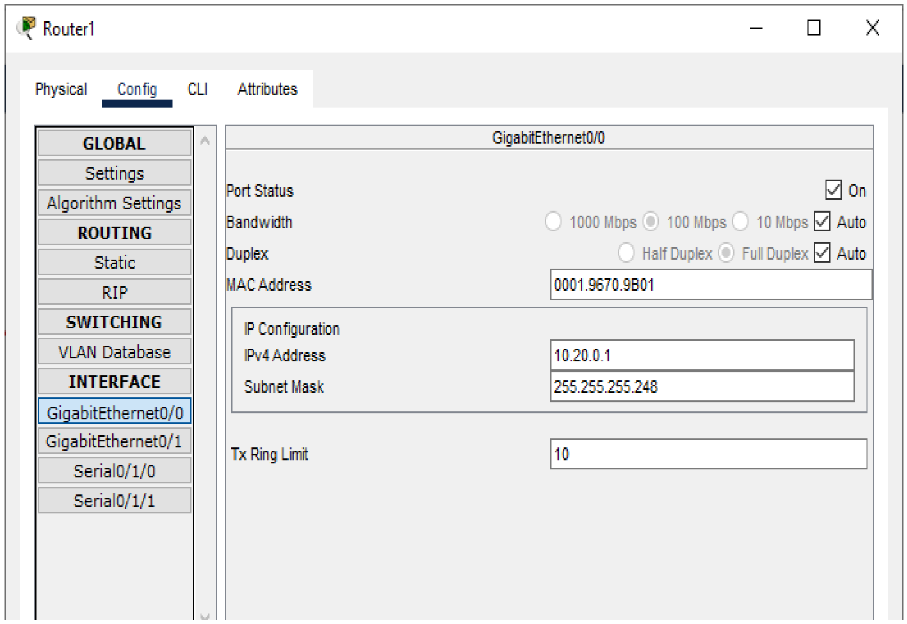


ii) Interface S0/1/0

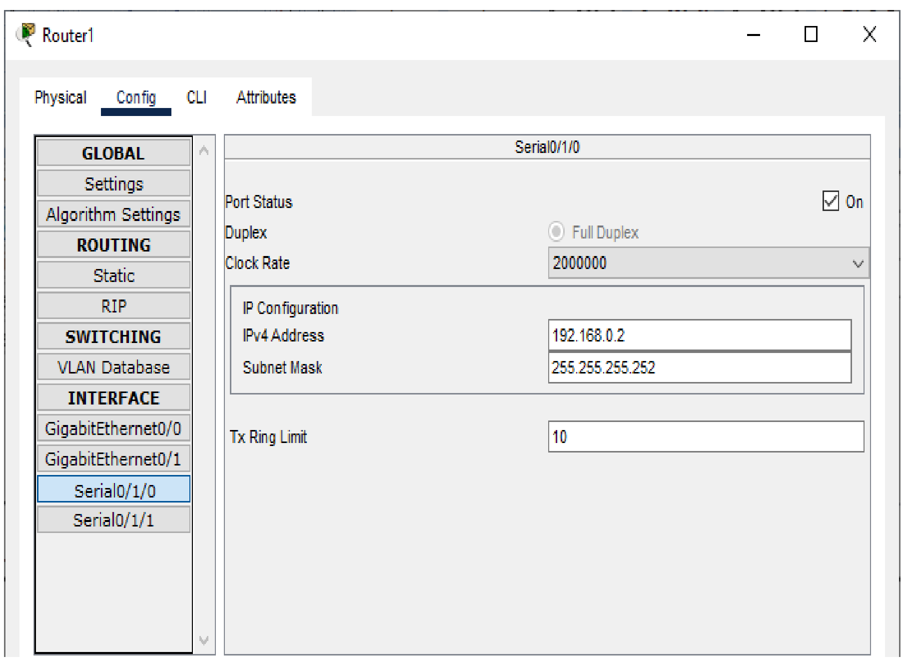


Configuring IP addresses on Router 1

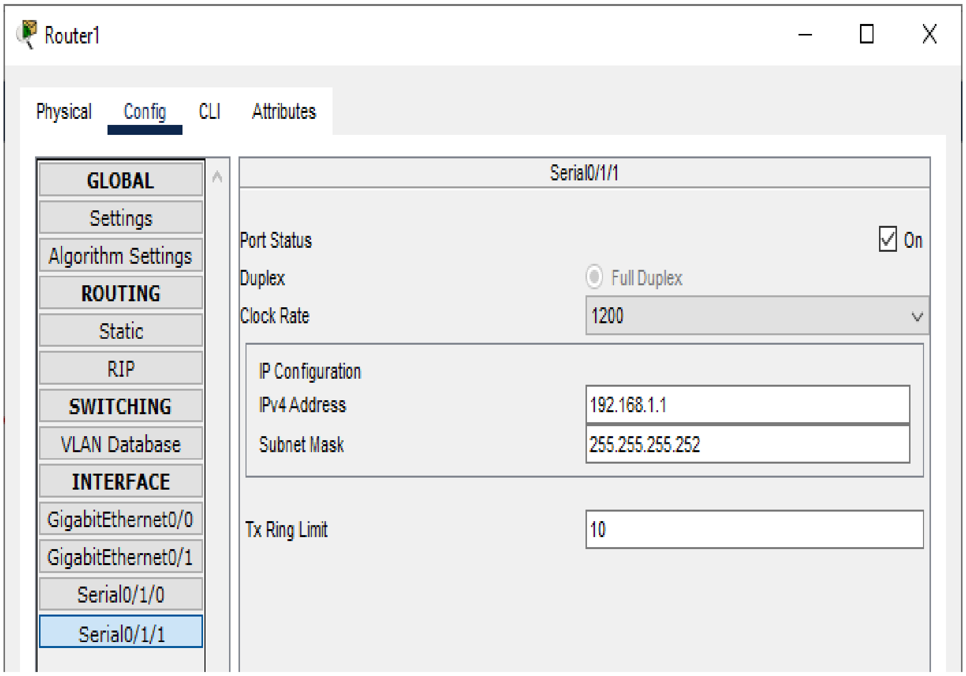
i) Interface G0/0



ii) Interface S0/1/0

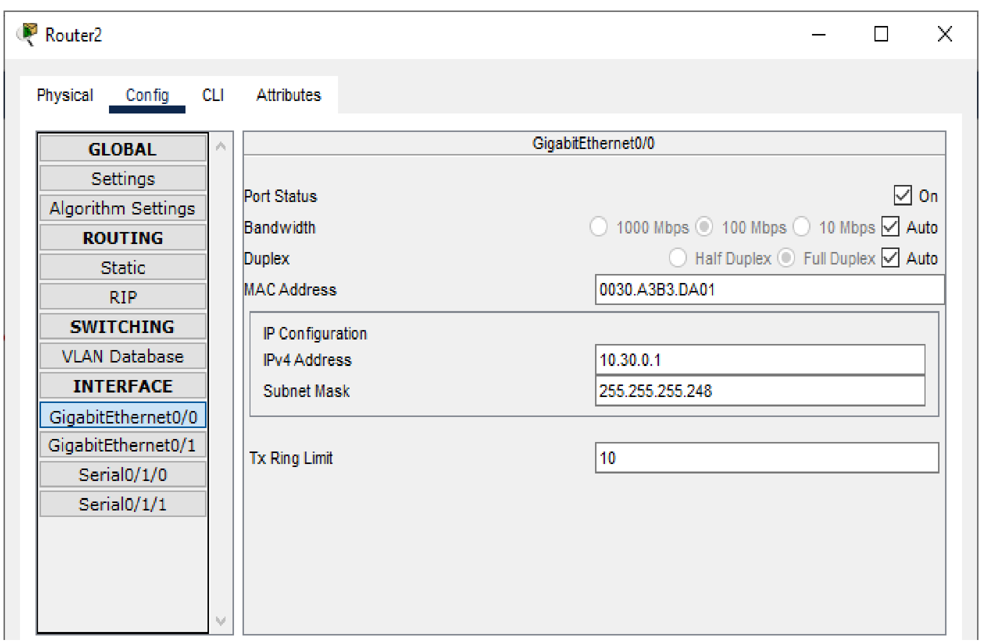


iii) Interface S0/1/1

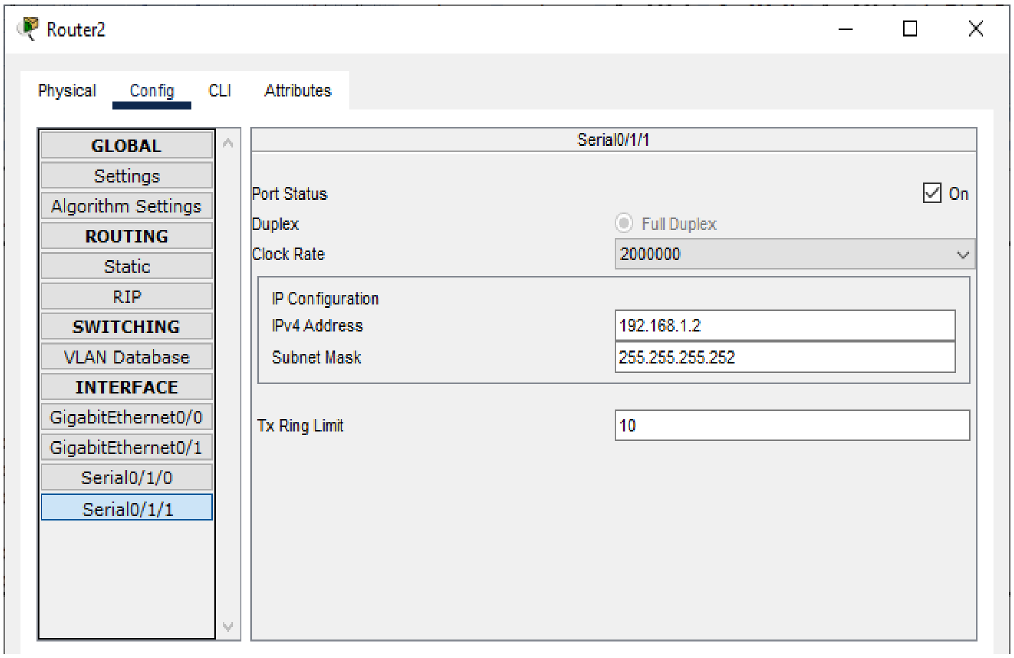


Configuring IP addresses on Router 2

i) Interface G0/0



ii) Interface S0/1/1



Configuring Router 0 for 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)

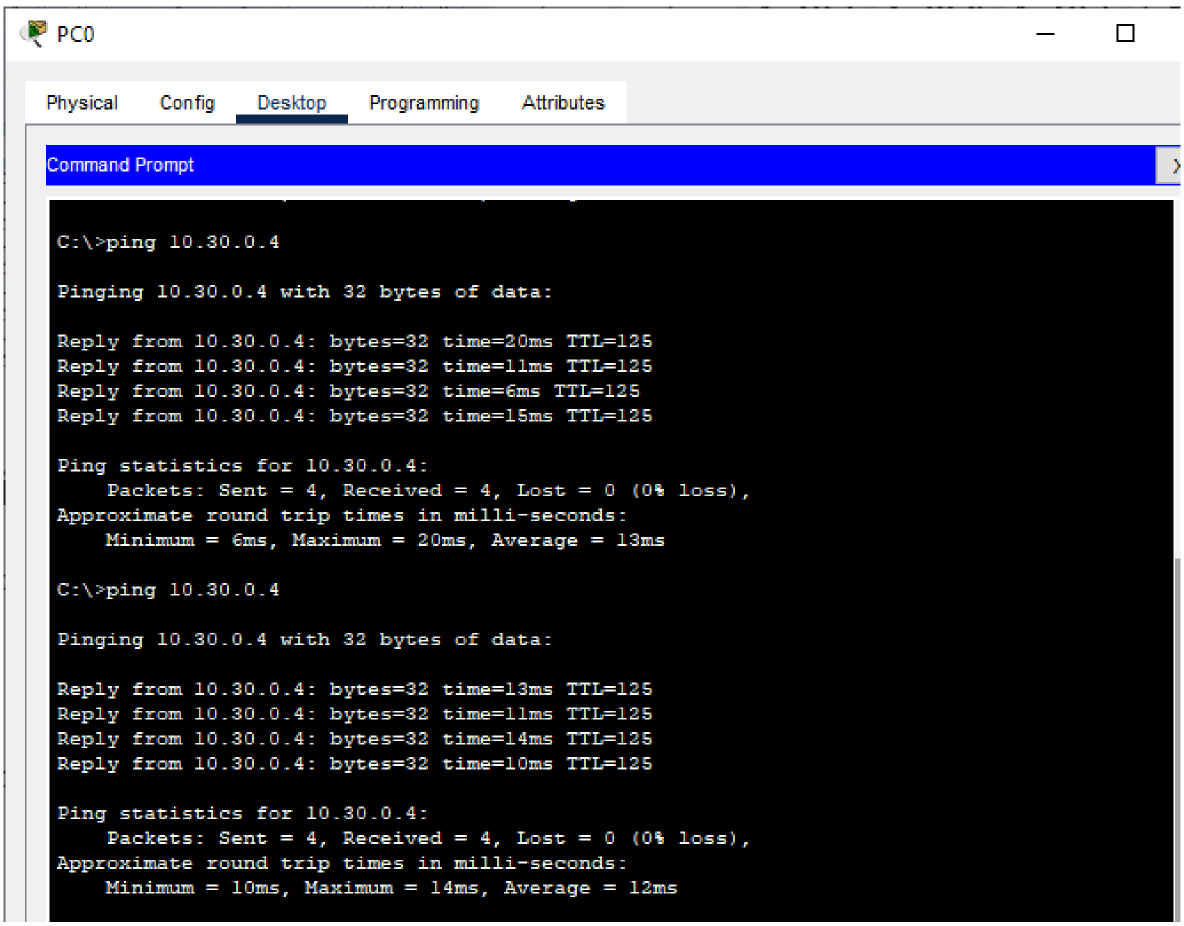
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.20.0.0
Router(config-router)#network 192.168.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#

Configuring Router 2 for RIPv2 (using the CLI mode)

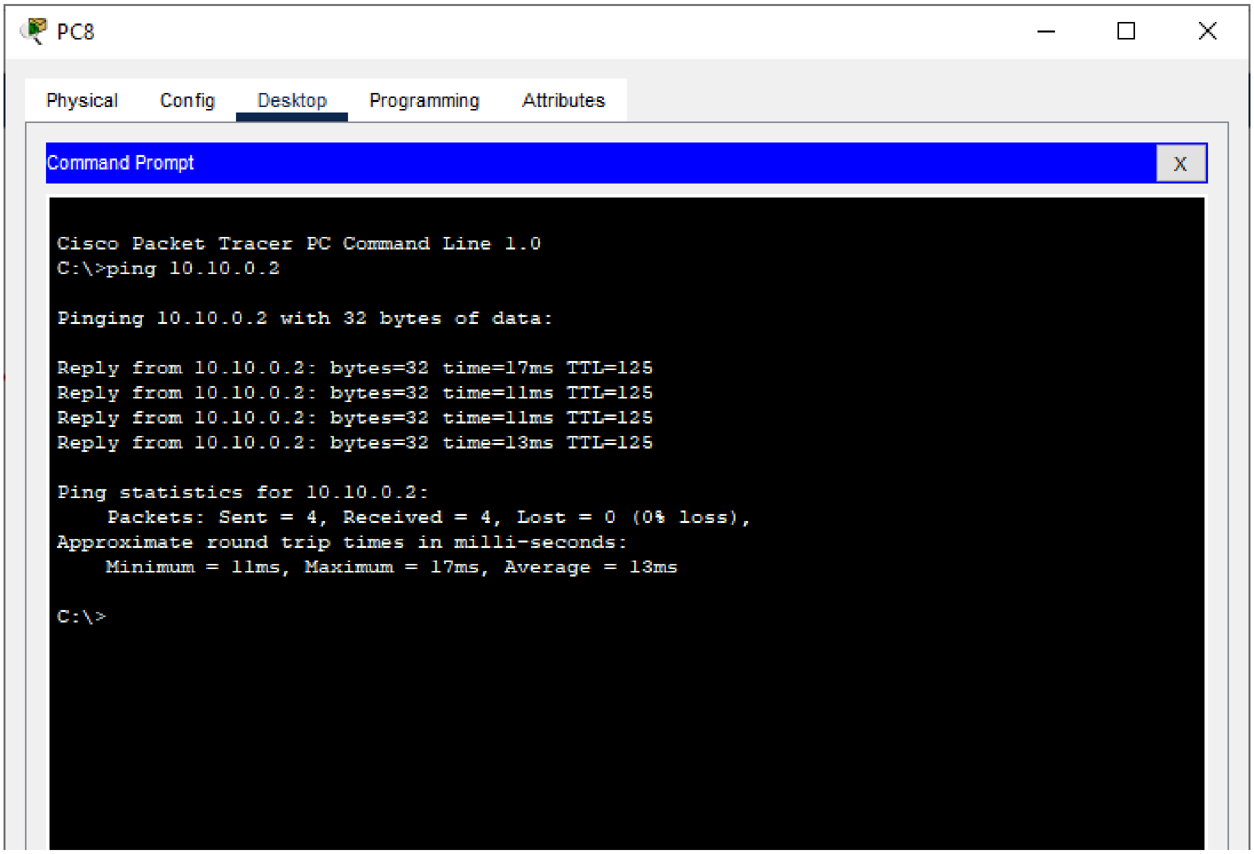
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.30.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#

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

Link for the video demonstration of the practical:

https://youtu.be/qrBpjxSkZY8

Practical No 7

Aim: Using Packet Tracer, create a network with three routers with OSPF and each 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 find the 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 the concept 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.

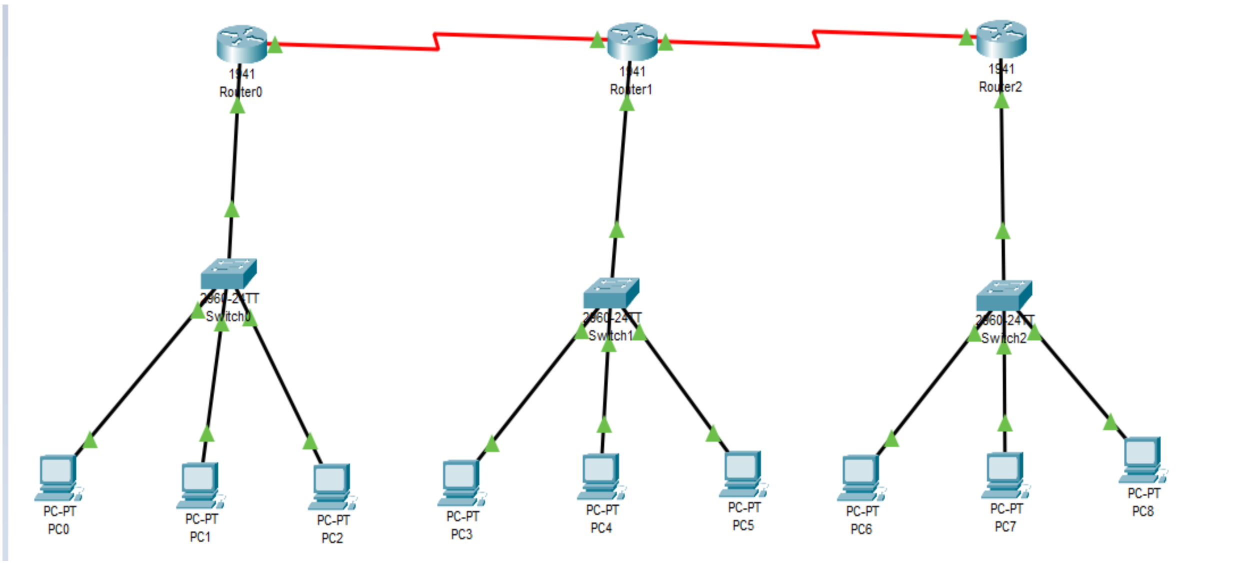
Open shortest path first (OSPF) is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e., the protocol which aims at moving the packet within a large autonomous system or routing domain.

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 to run the SPF algorithm, requiring more RAM to store adjacency topology, and being more complex to set up and hard to troubleshoot.

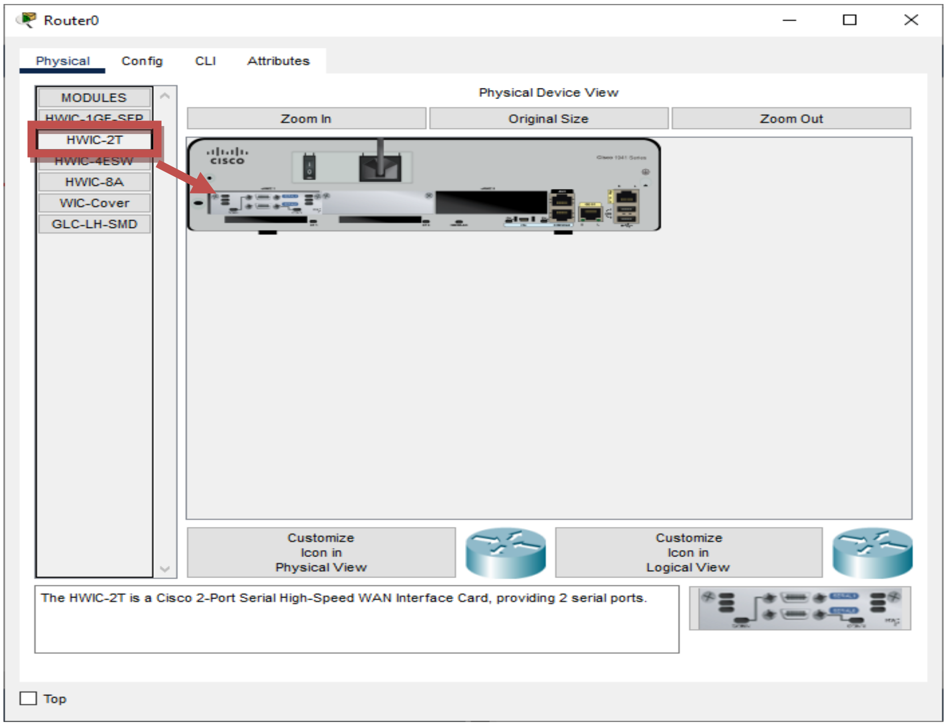
We use the following topology for the present case



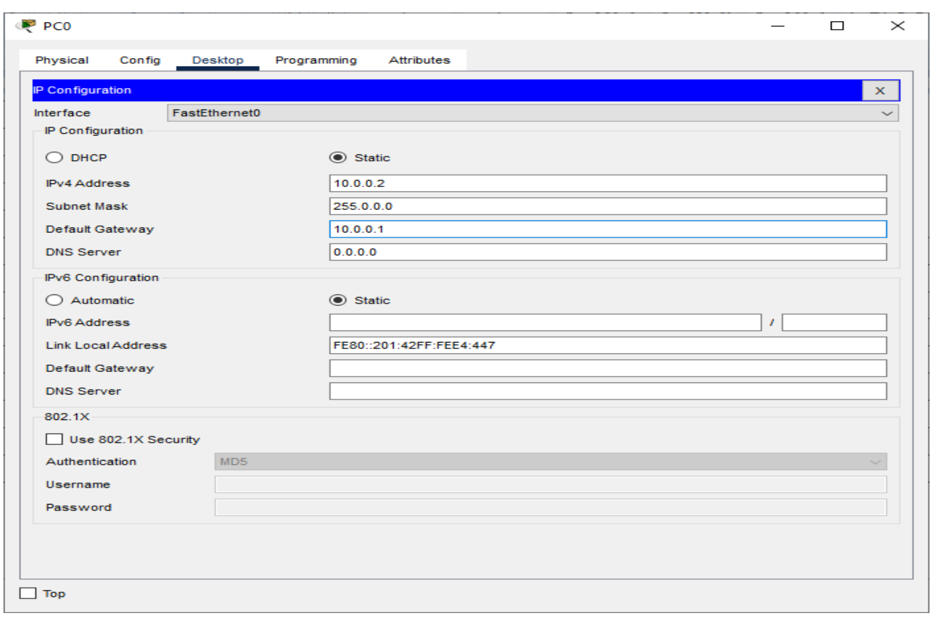
We configure the above network using the following IP addresses

<table>
<tr><th>Host</th><th>Interface</th><th>IP address</th><th>Default Gateway</th><th>Subnet Mask</th><th>Wildcard Mask</th></tr>
<tr><td>Router 0</td><td>G0/0</td><td>10.0.0.1</td><td rowspan="7"></td><td rowspan="16">255.0.0.0</td><td rowspan="16">0.255.255.255</td></tr>
<tr><td></td><td>S0/1/0</td><td>40.0.0.1</td></tr>
<tr><td>Router 1</td><td>G0/0</td><td>20.0.0.1</td></tr>
<tr><td></td><td>S0/1/0</td><td>40.0.0.2</td></tr>
<tr><td></td><td>S0/1/1</td><td>50.0.0.1</td></tr>
<tr><td>Router 2</td><td>G0/0</td><td>30.0.0.1</td></tr>
<tr><td></td><td>S0/1/1</td><td>50.0.0.2</td></tr>
<tr><td>PC0</td><td>FastEthernet0</td><td>10.0.0.2</td><td rowspan="3">10.0.0.1</td></tr>
<tr><td>PC1</td><td>FastEthernet0</td><td>10.0.0.3</td></tr>
<tr><td>PC2</td><td>FastEthernet0</td><td>10.0.0.4</td></tr>
<tr><td>PC3</td><td>FastEthernet0</td><td>20.0.0.2</td><td rowspan="3">20.0.0.1</td></tr>
<tr><td>PC4</td><td>FastEthernet0</td><td>20.0.0.3</td></tr>
<tr><td>PC5</td><td>FastEthernet0</td><td>20.0.0.4</td></tr>
<tr><td>PC6</td><td>FastEthernet0</td><td>30.0.0.2</td><td rowspan="3">30.0.0.1</td></tr>
<tr><td>PC7</td><td>FastEthernet0</td><td>30.0.0.3</td></tr>
<tr><td>PC8</td><td>FastEthernet0</td><td>30.0.0.4</td></tr>
</table>

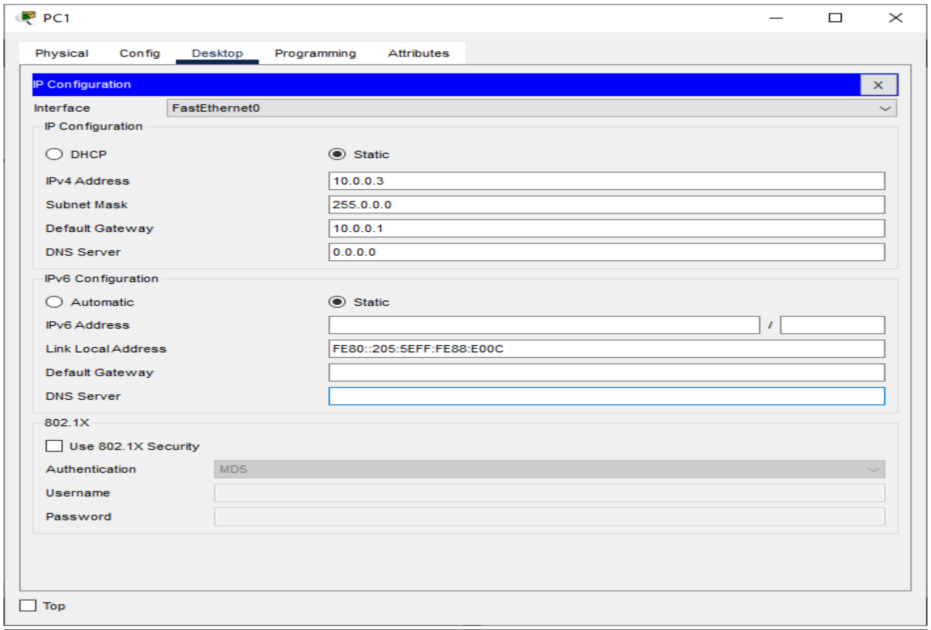
Adding Serial Interface in each Router



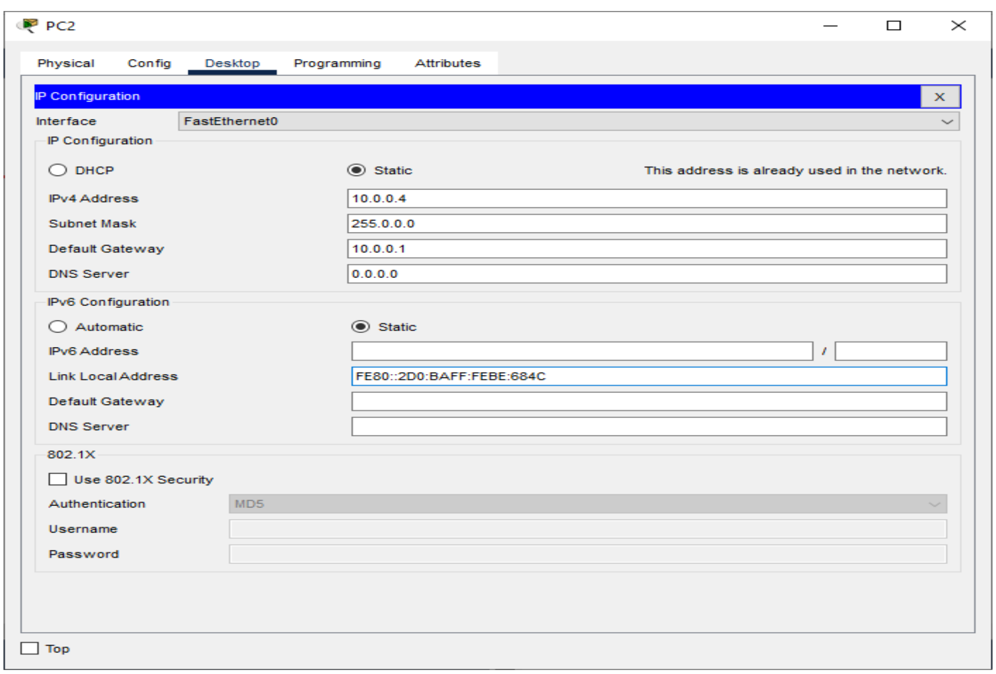
Configuring PC0:



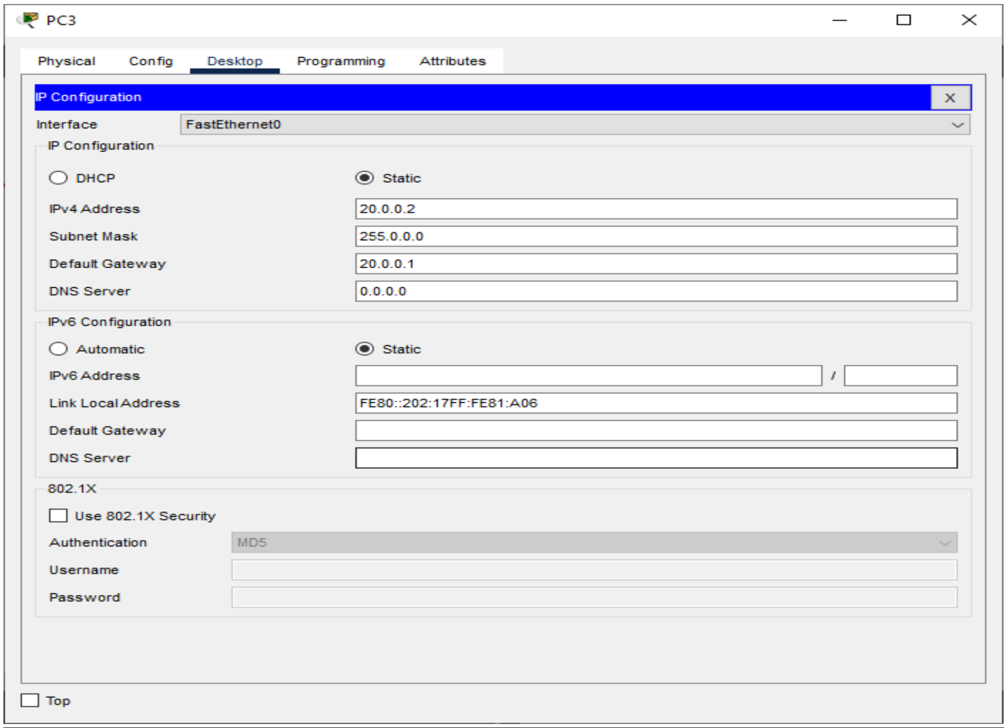
Configuring PC1:



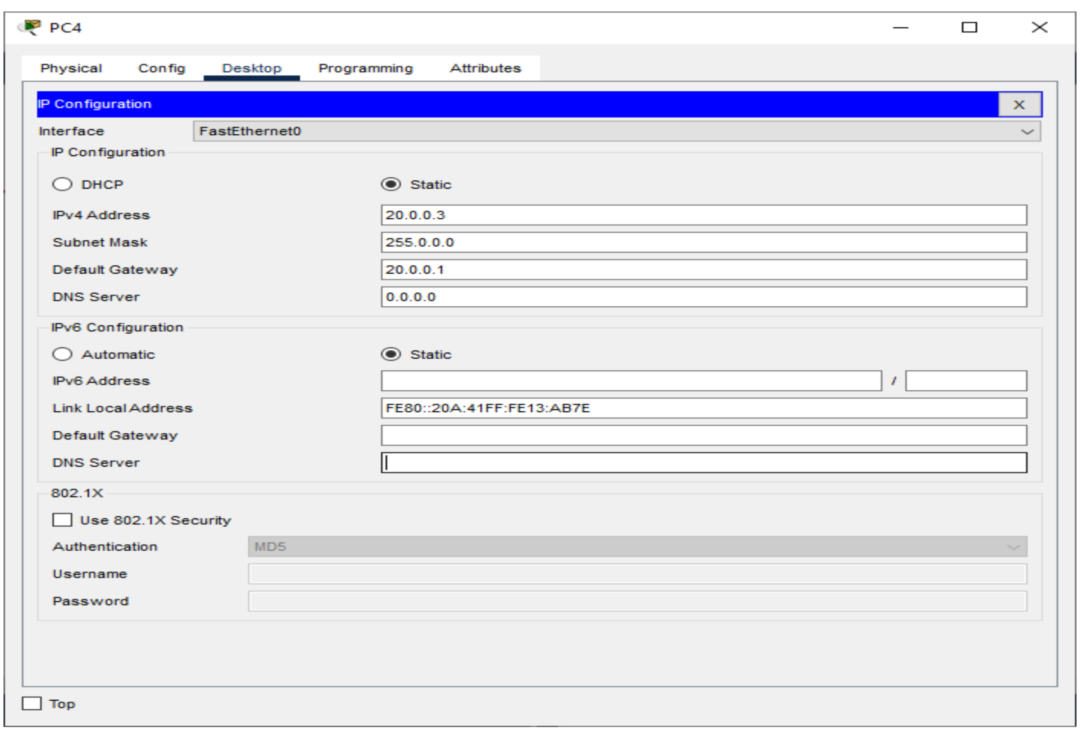
Configuring PC2:



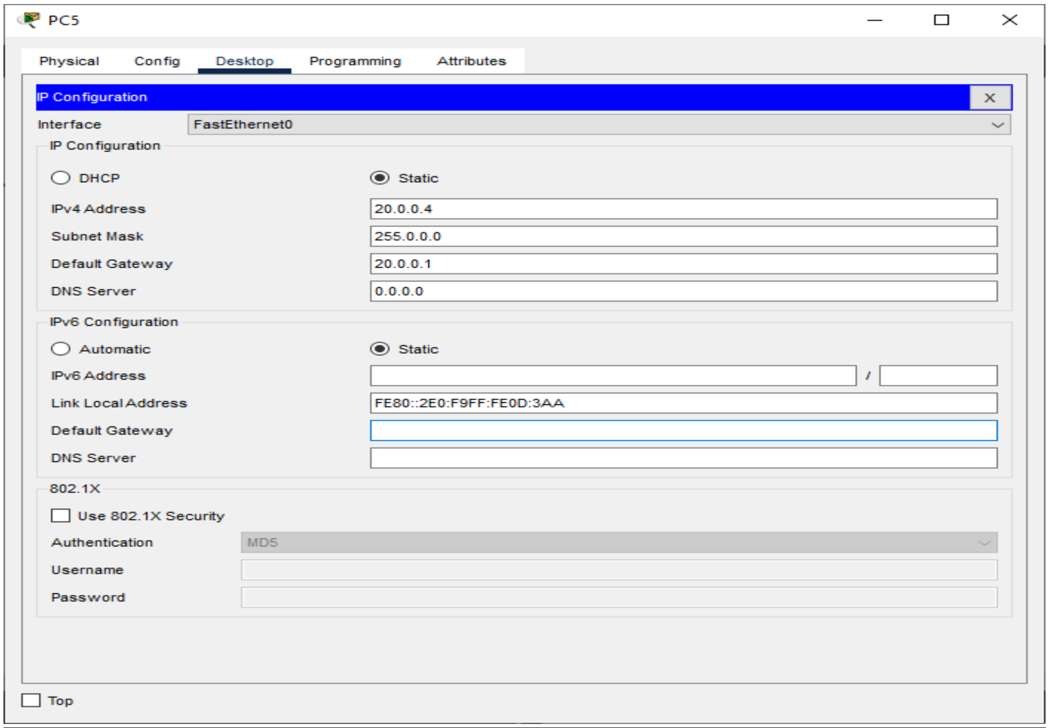
Configuring PC3:



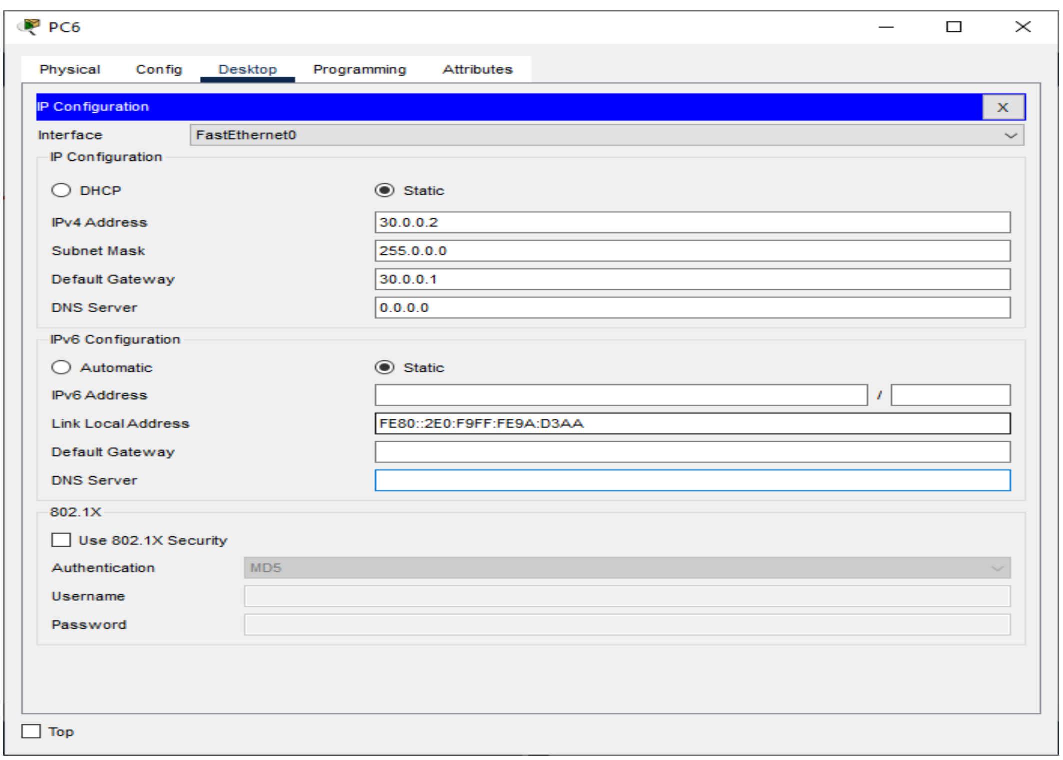
Configuring PC4:



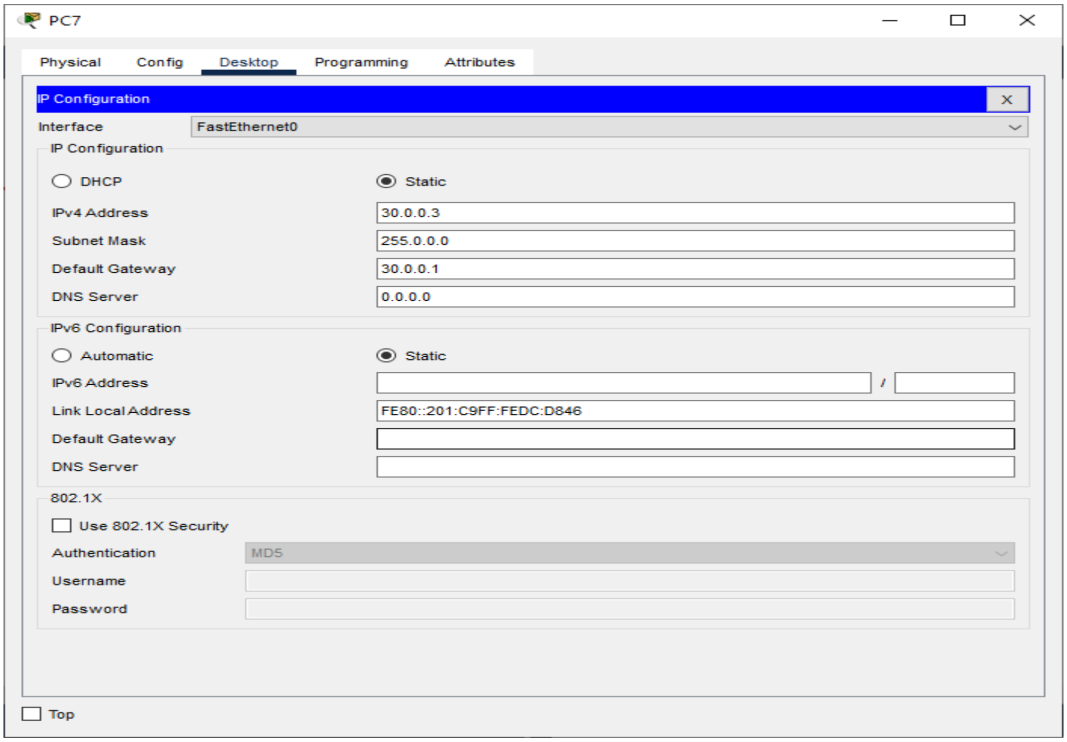
Configuring PC5:



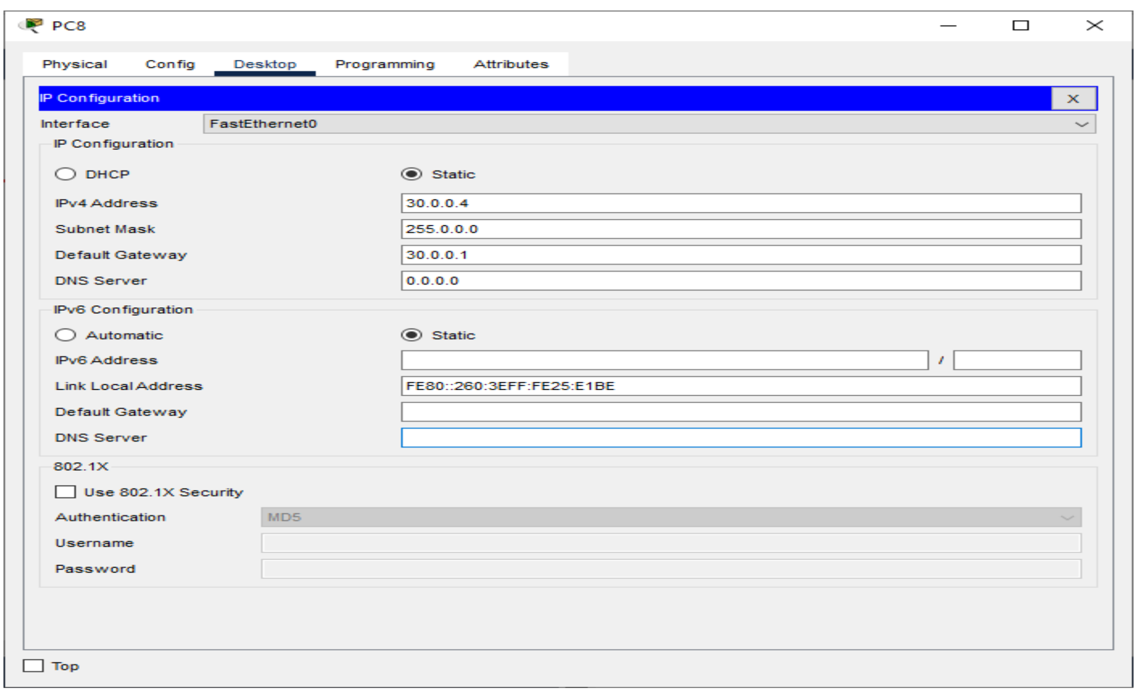
Configuring PC6:



Configuring PC7:

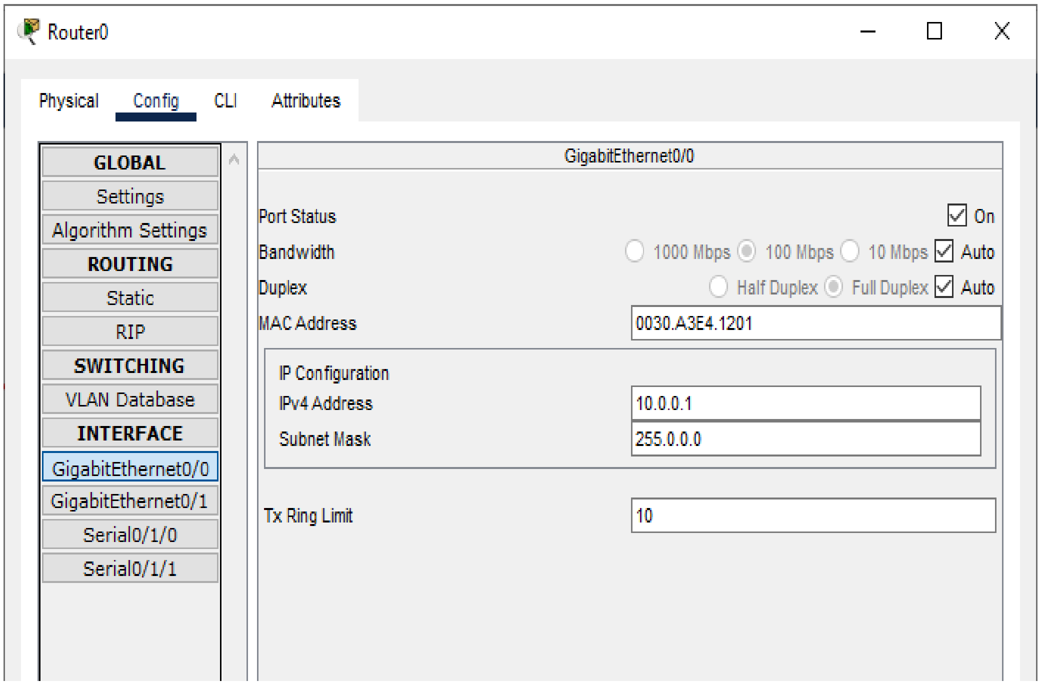


Configuring PC8:

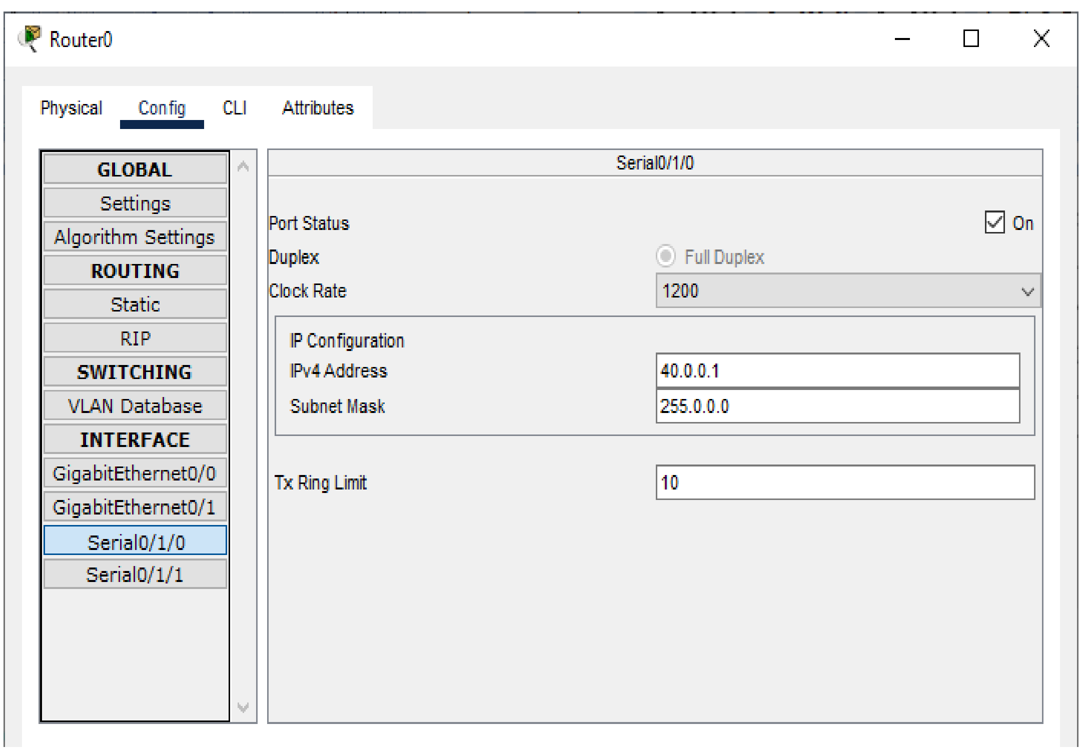


Configuring IP addresses on Router 0

i) Interface G0/0

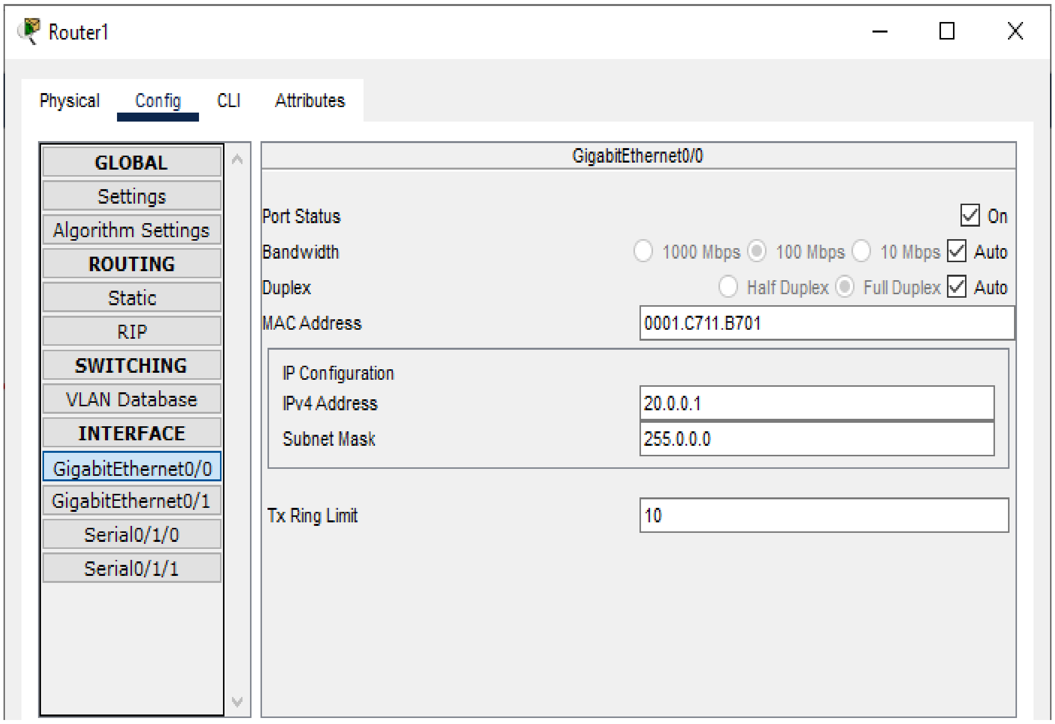


ii) Interface S0/1/0

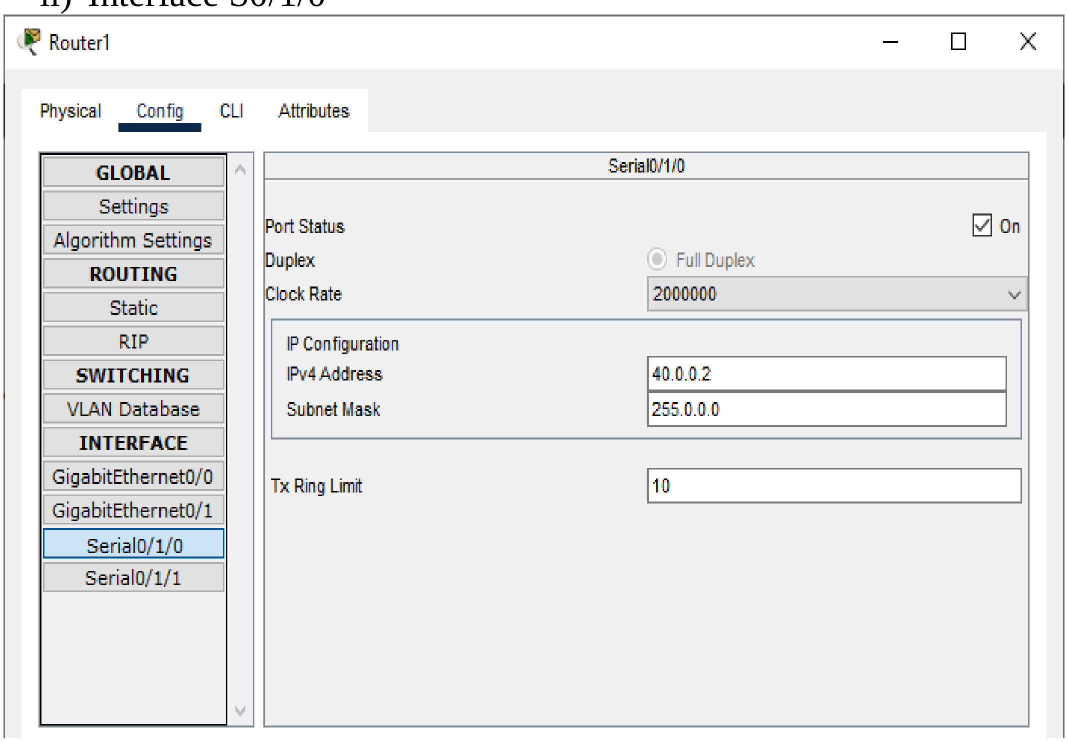


Configuring IP addresses on Router 1

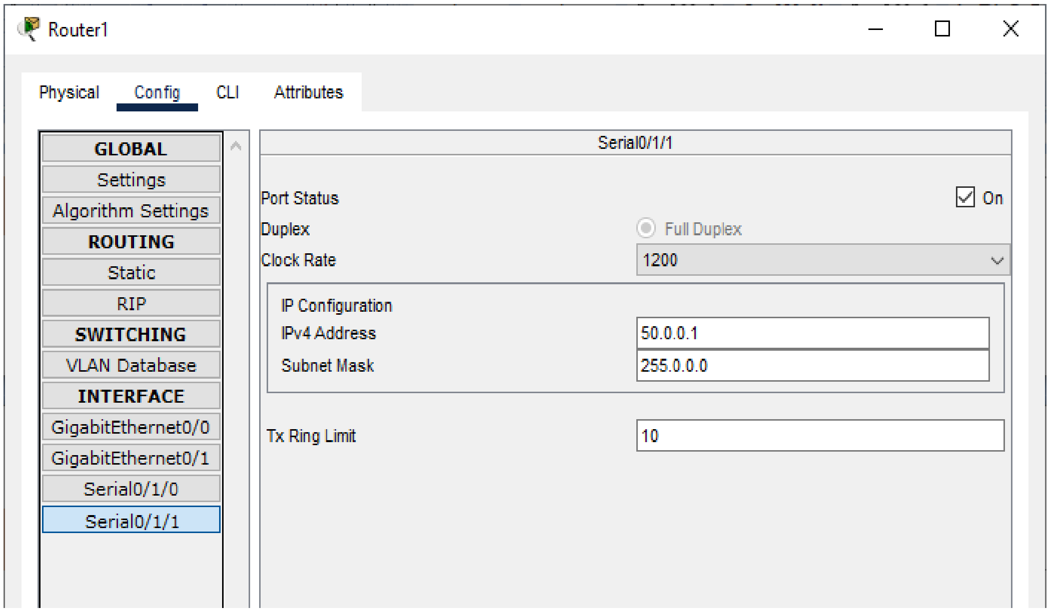
i) Interface G0/0



ii) Interface S0/1/0

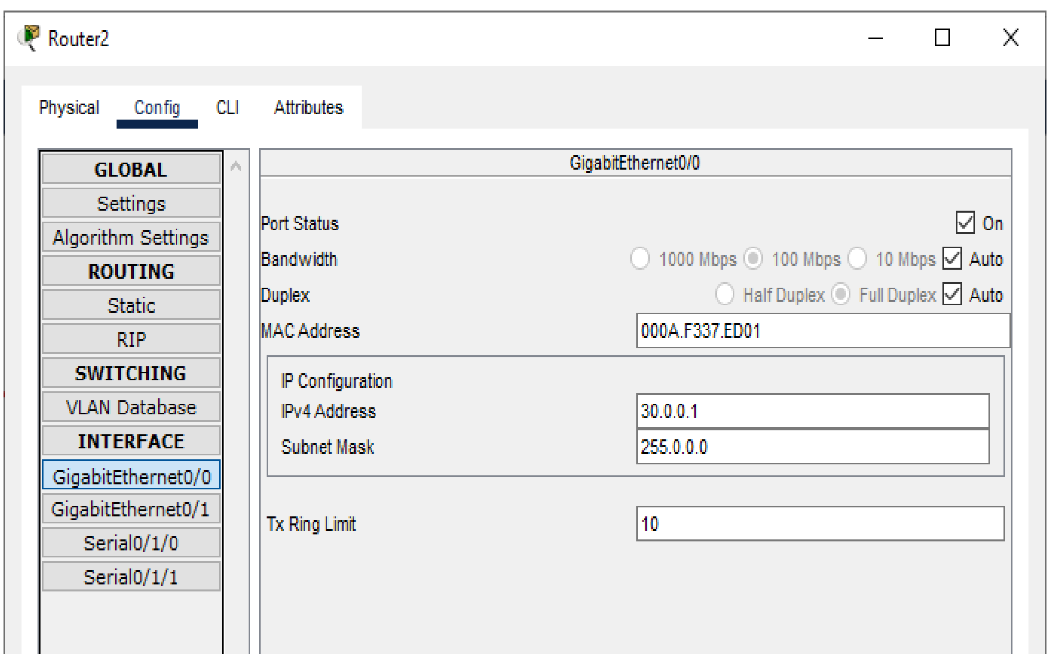


iii) Interface S0/1/1

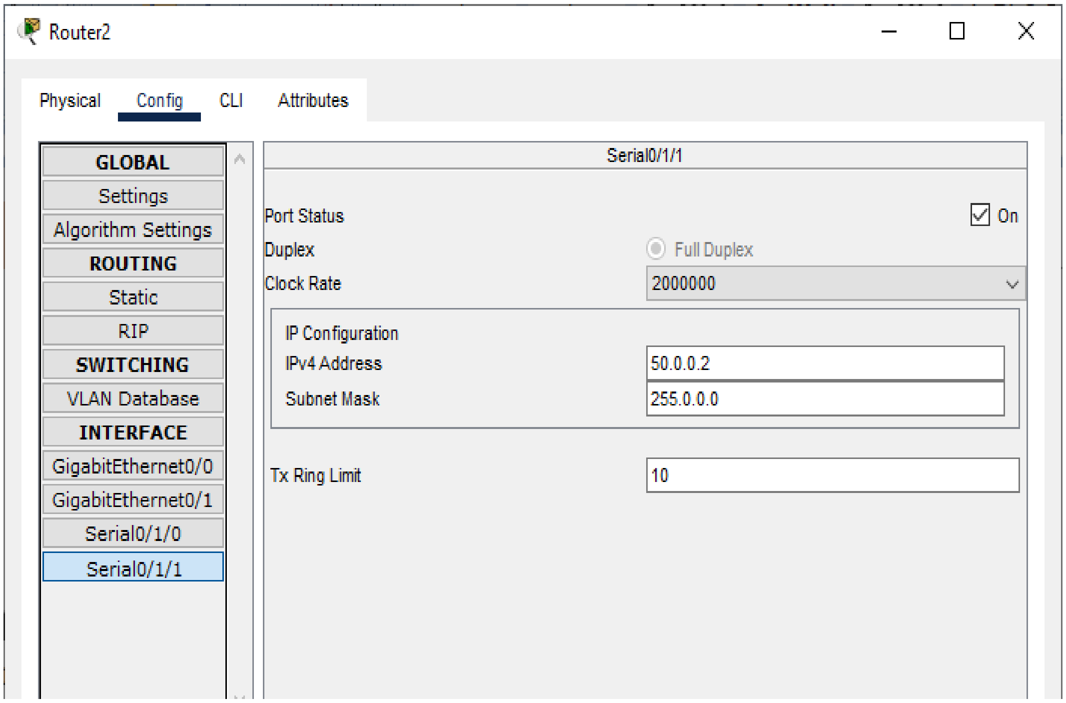


Configuring IP addresses on Router 2

i) Interface G0/0



ii) Interface S0/1/1



Configuring Router 0 for 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)

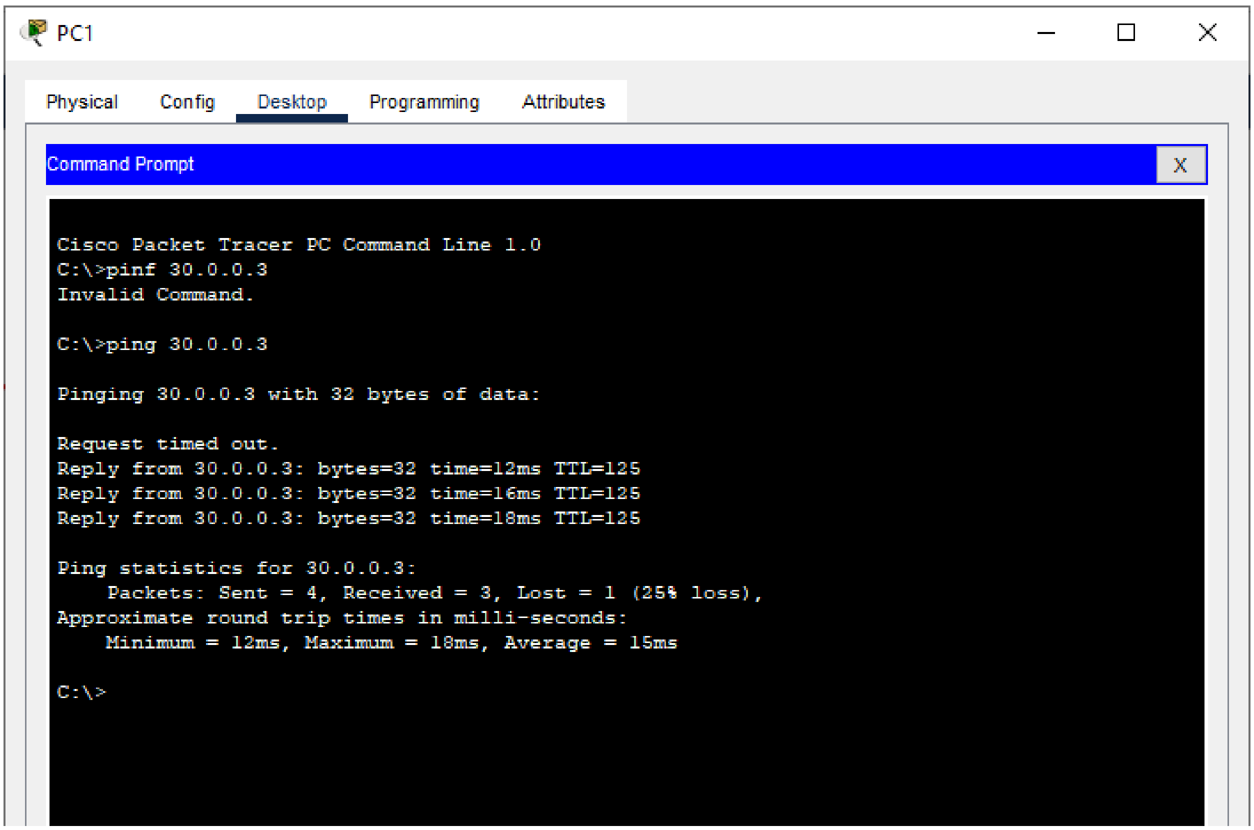
Router(config)#
Router(config)#router ospf 1
Router(config-router)#
Router(config-router)#network 20.0.0.0 0.0.0.255 area 1
Router(config-router)#network 40.0.0.0 0.0.0.255 area 1
Router(config-router)#network 50.0.0.0 0.0.0.255 area 1
Router(config-router)#exit
Router(config)#

Configuring Router 2 for OSPF (using the CLI mode)

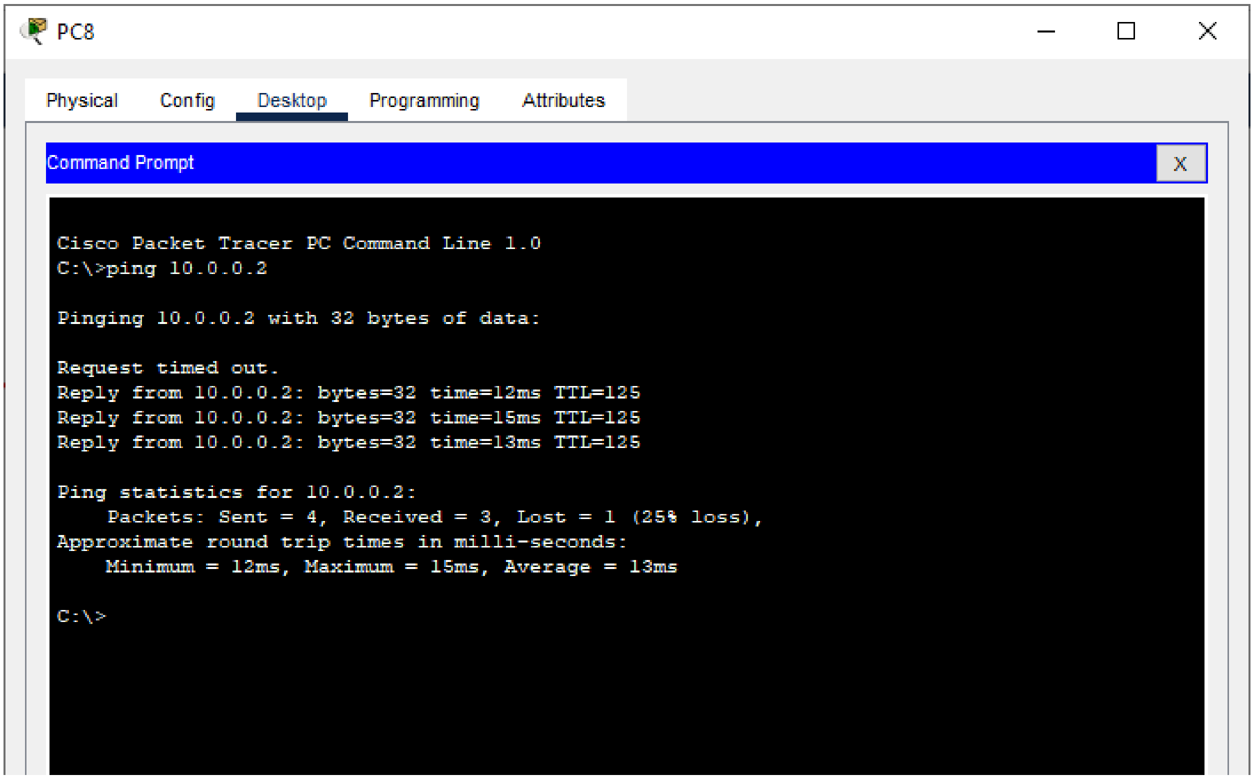
Router(config)#
Router(config)#router ospf 1
Router(config-router)#
Router(config-router)#network 30.0.0.0 0.0.0.255 area 1
Router(config-router)#network 50.0.0.0 0.0.0.255 area 1
Router(config-router)# exit
Router(config)#

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

Link for the video demonstration of the practical:

https://youtu.be/PVaQ3M-Jiq8