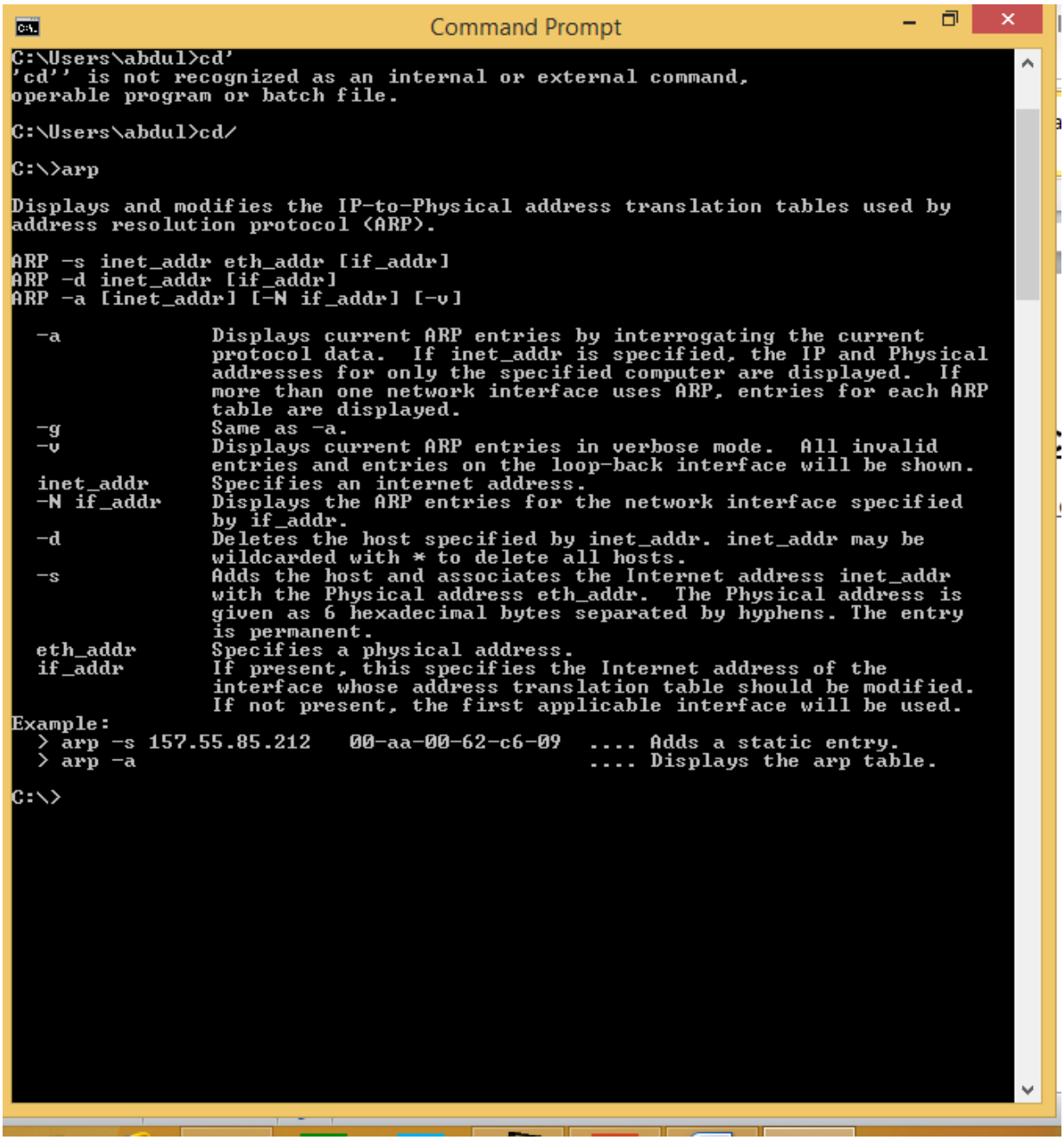
PRACTICAL NO 4

Using the various command utilities

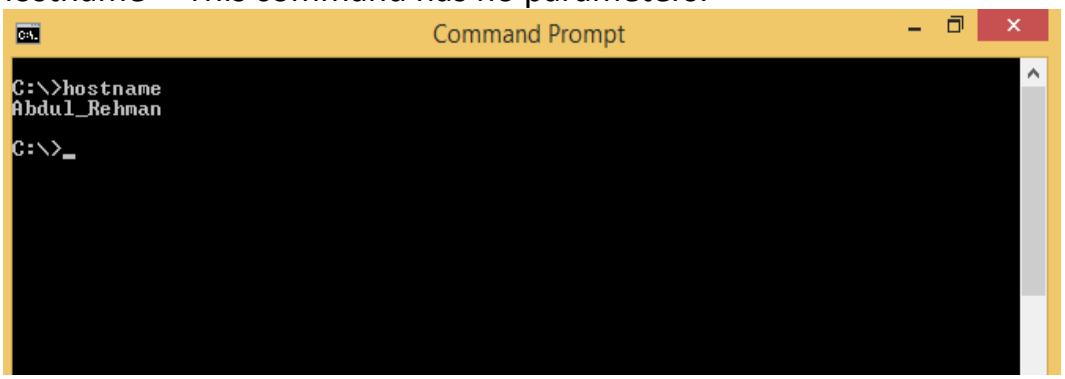
1) arp : This diagnostic command displays and modifies the IP-to-Ethernet or Token Ring physical address translation tables used by the Address Resolution Protocol (ARP).



2) hostname: This diagnostic command prints the name of the host on which the command is used.

Syntax

hostname -- This command has no parameters.

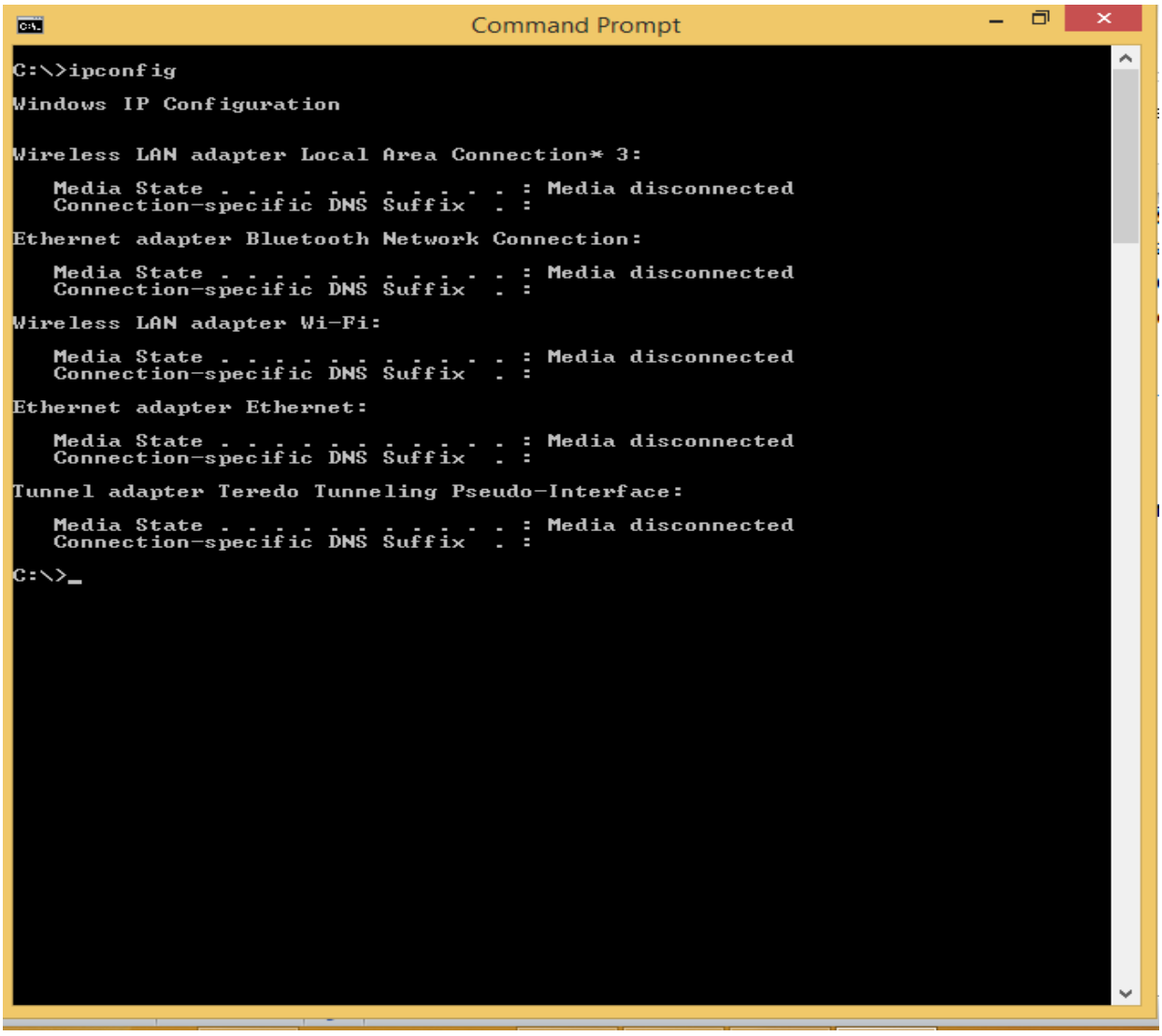


3) ipconfig:

This diagnostic command displays all current TCP/IP network configuration values. This command is useful on computers running DHCP because it enables users to determine which TCP/IP configuration values have been configured by DHCP. If you enter only ipconfig without parameters, the response is a display of all of the current TCP/IP configuration values, including IP address, subnet mask, and default gateway.

Syntax

ipconfig [/all | /renew [adapter] | /release [adapter]



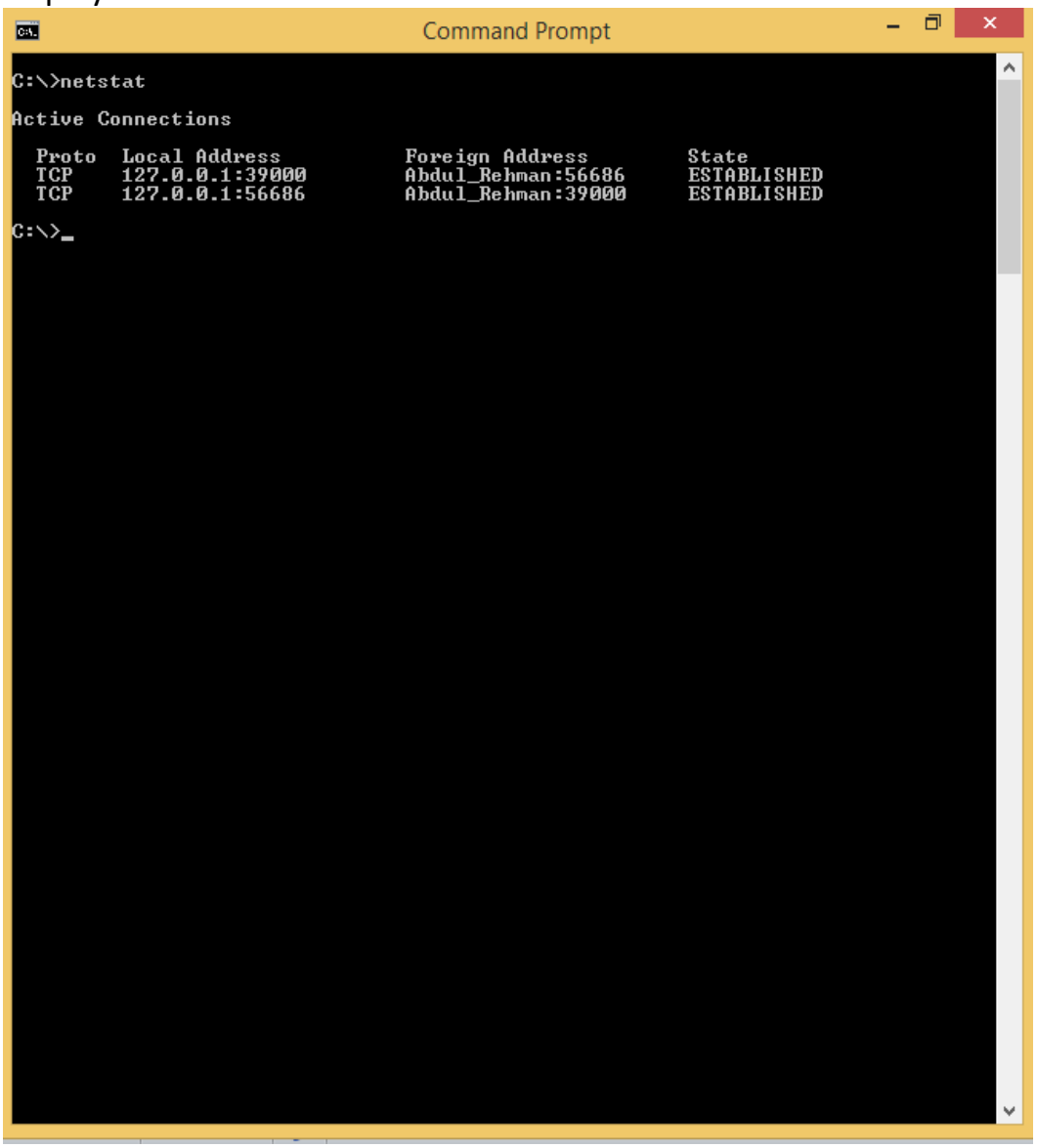
4) netstat:

   This diagnostic command displays protocol statistics and current TCP/IP network connection

   Syntax

   netstat [-a] [-e][-n][-s] [-p protocol] [-r] [interval]

Parameters
-a Displays all connections and listening ports; server connections are usually not shown. -e Displays Ethernet statistics. This can be combined with the -s option. -n Displays addresses and port numbers in numerical form (rather than attempting name lookups). -s Displays per-protocol statistics. By default, statistics are shown for TCP, UDP, ICMP, and IP; the -p option can be used to specify a subset of the default.
-p protocol Shows connections for the protocol specified.
-r Displays the contents of the routing table.
Interval Redisplays selected statistics, pausing interval seconds between each display.



5) ping: This diagnostic command verifies connections to one or more remote computers.

Syntax

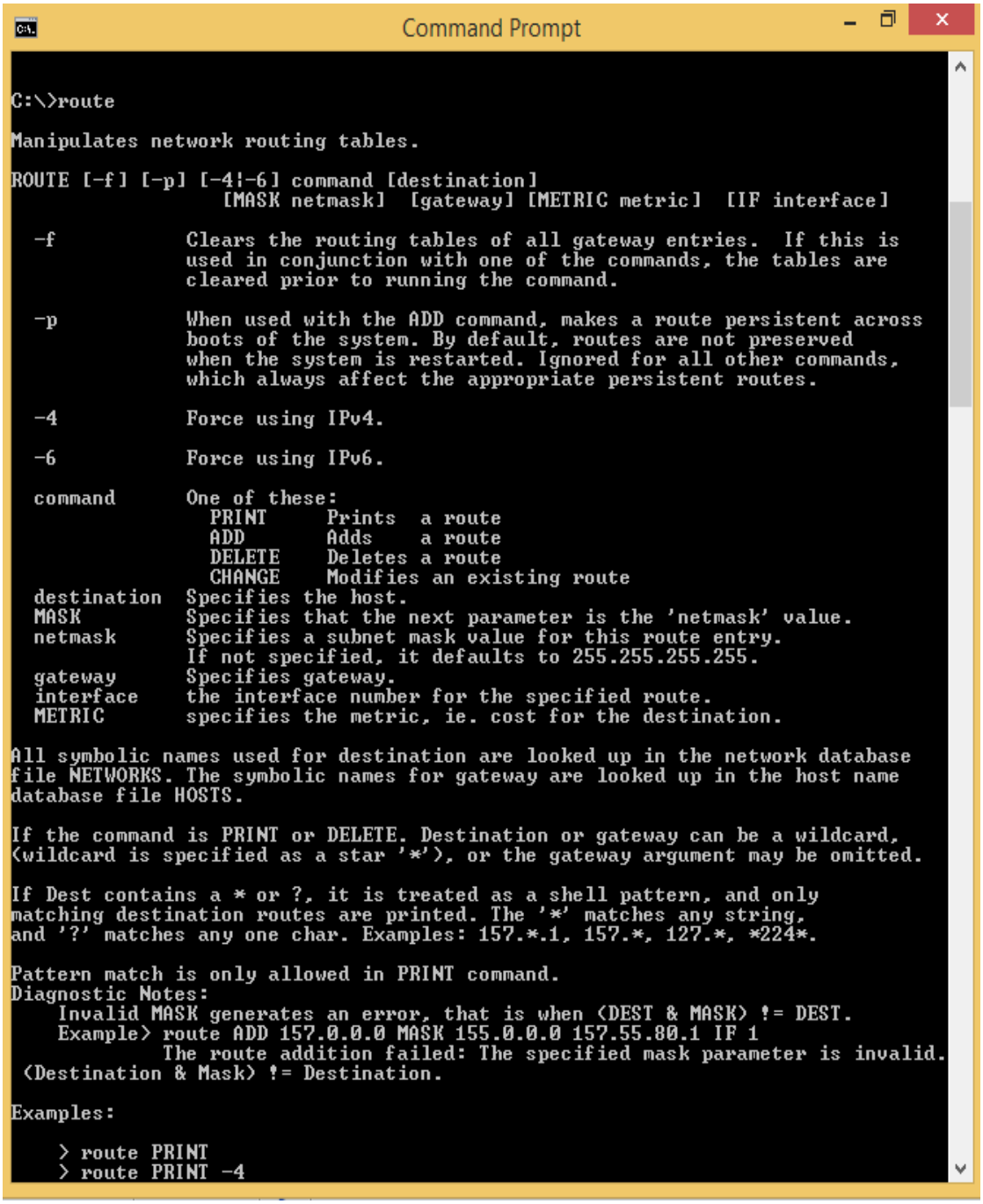
ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j host-list] | [-k host-list]] [-w timeout] destination-list

6) route:

This diagnostic command manipulates network routing tables.

Syntax

route [-f] [command [destination] [MASK netmask] [gateway] [METRIC metric]]



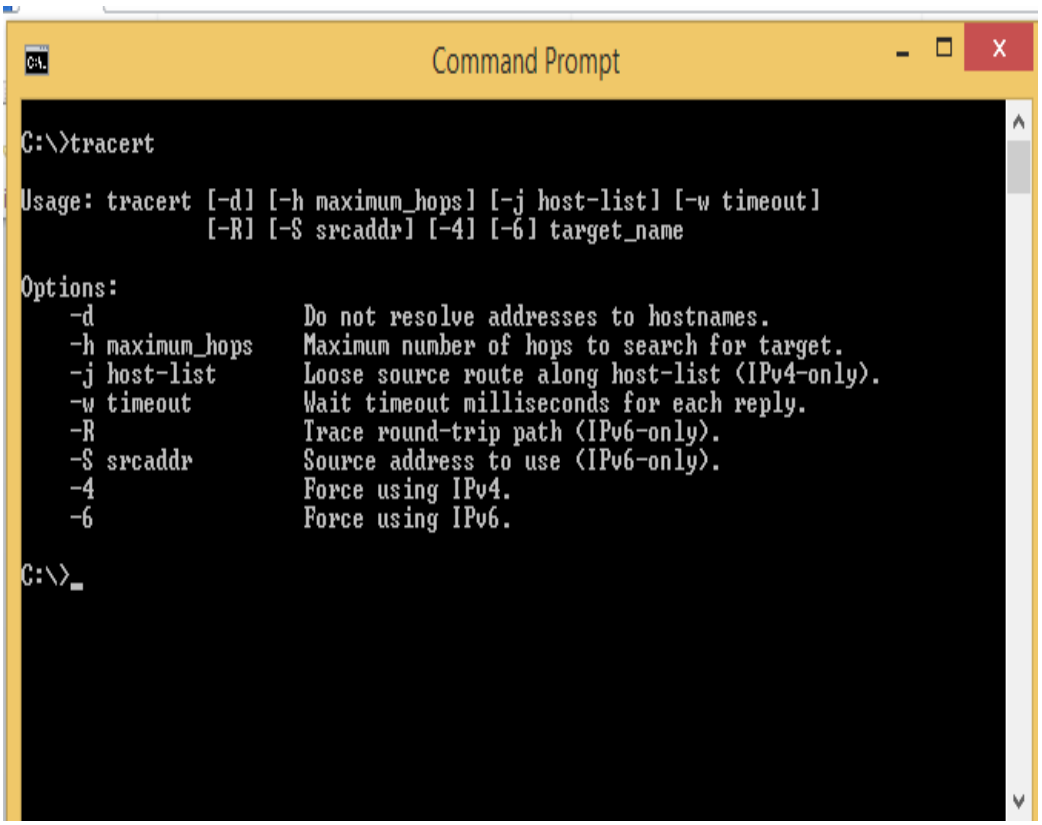
7) tracert:

This diagnostic utility determines the route taken to a destination by sending Internet Control Message Protocol (ICMP) echo packets with varying time-to-live (TTL) values to the destination. Each router along the path is required to decrement the TTL on a packet by at least 1 before forwarding it, so the TTL is effectively a hop count. When the TTL on a packet reaches 0, the router is supposed to send back an ICMP Time Exceeded message to the source computer.

tracert determines the route by sending the first echo packet with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum TTL is reached. The route is determined by examining the ICMP Time Exceeded messages sent back by intermediate routers. Notice that some routers silently drop packets with expired TTLs and will be invisible to tracert.

Syntax

tracert[-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name



PRACTICAL NO 2

Static Routing

Static Route

1. Static routing method is most trusted by a router.
2. Static routing is not really a routing protocol.
3. Static routes do not dynamically adapt to network changes, are not particularly scalable, and require manual updating to reflect changes.

Static routing has the following advantages

1. There is no bandwidth usage between routers, which means you could possibly save money on WAN links.
2. There is no overhead on the router CPU, which means you could possibly buy a cheaper router than you would use if you were using dynamic routing.
3. It adds security because the administrator can choose to allow routing access to certain networks only.

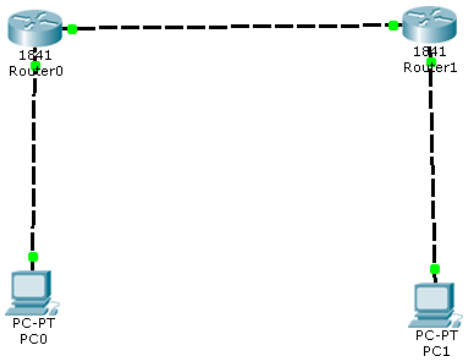
Static routing has the following disadvantages

1. Static routes don't dynamically adapt to network change.
2. If a network is added to the internet work, the administrator has to add a route to it on all routers—by hand.
3. It's not feasible in large networks because maintaining it would be a full-time job in itself.
4. With static routing, as your network grows, it can be difficult just keep adding static routes makes sure everybody can still get everything.
5. The administrator must really understand the internetwork and how each router is connected in order to configure routes correctly.

There are two different styles to configure an "ip route" command:

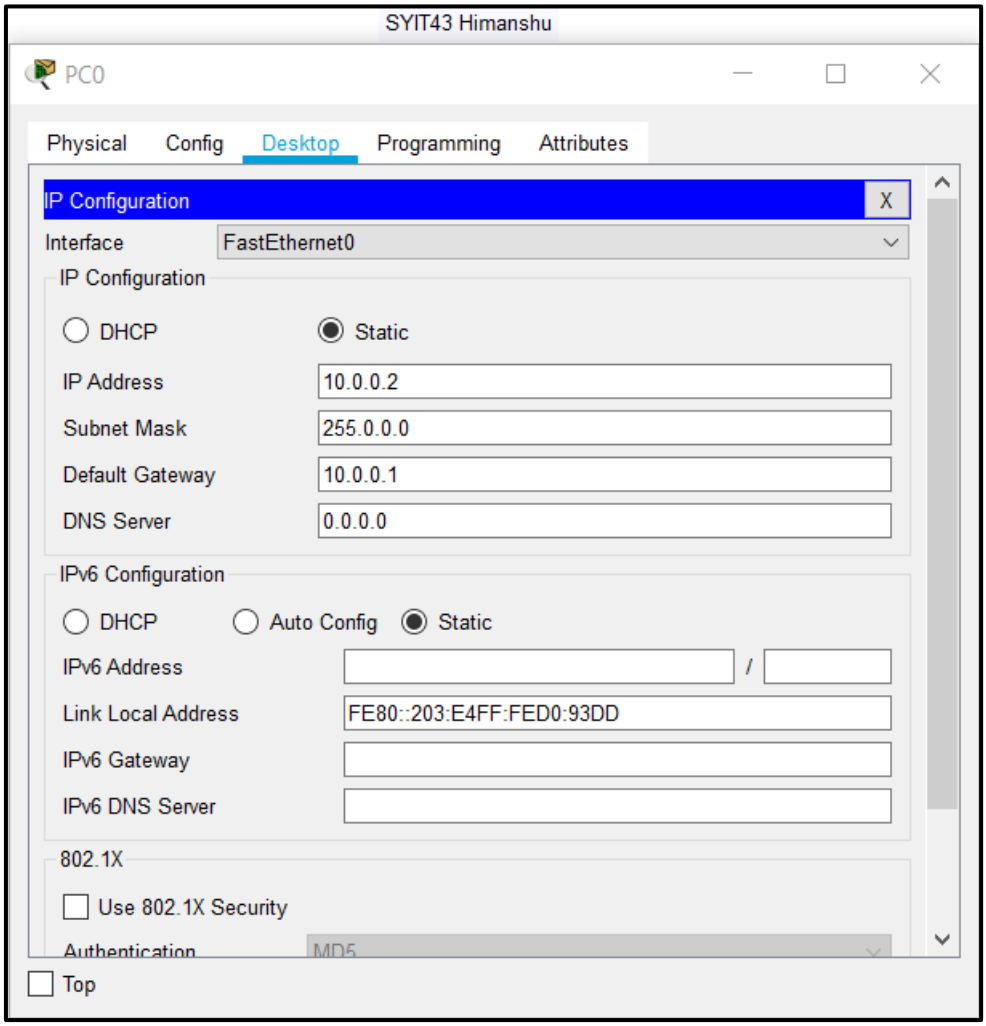
1. Using a next hop IP address
2. Using an outgoing interface

Consider the following network

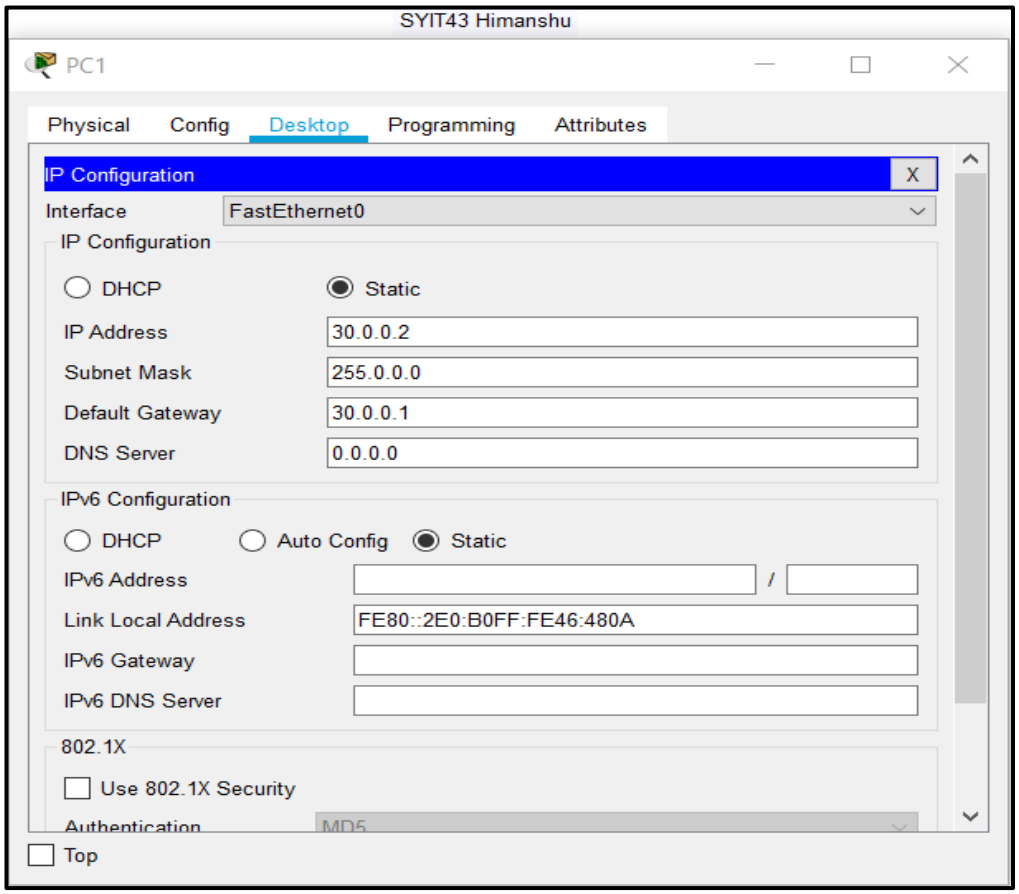


We configure it as follows

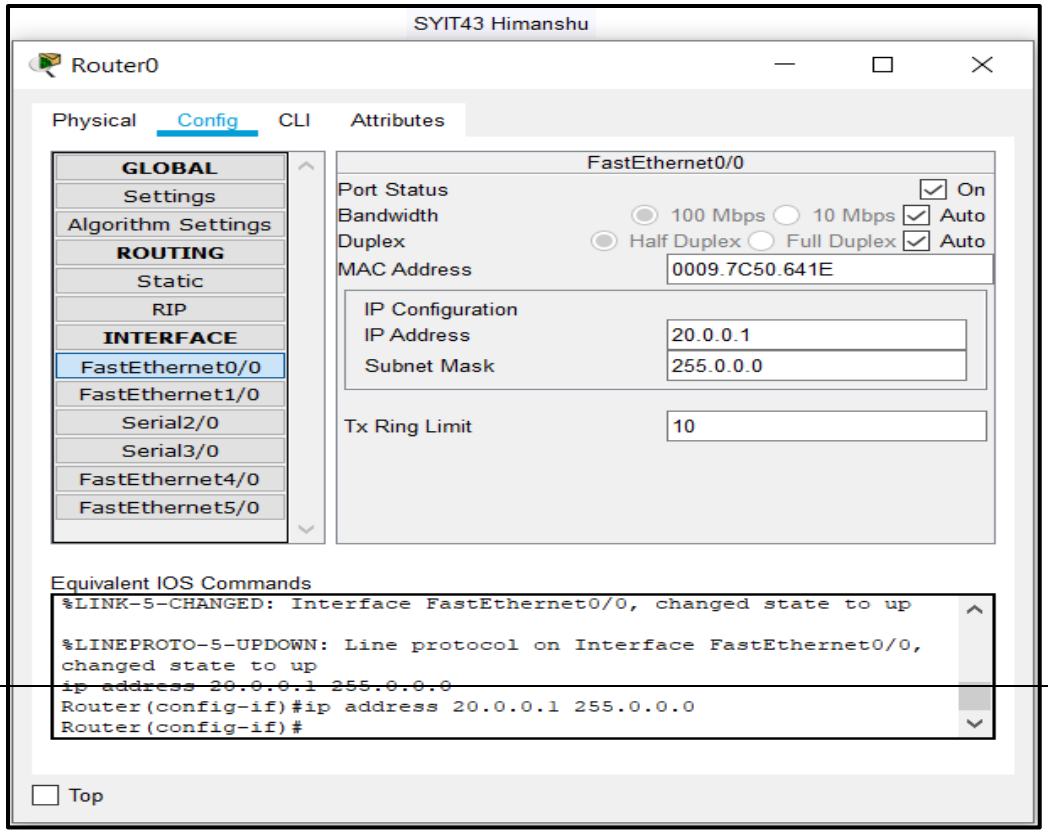
Step 1: (CONFIGURE PC0)

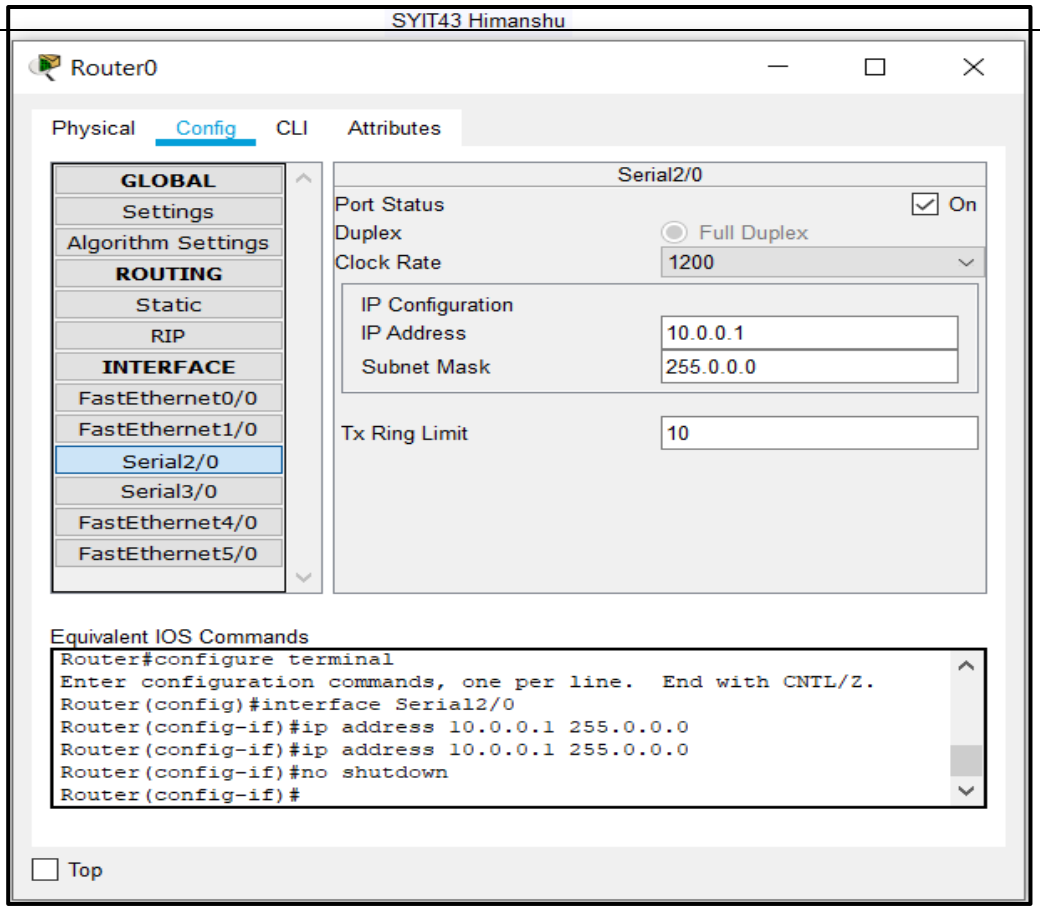


Step 2: (CONFIGURE PC1)

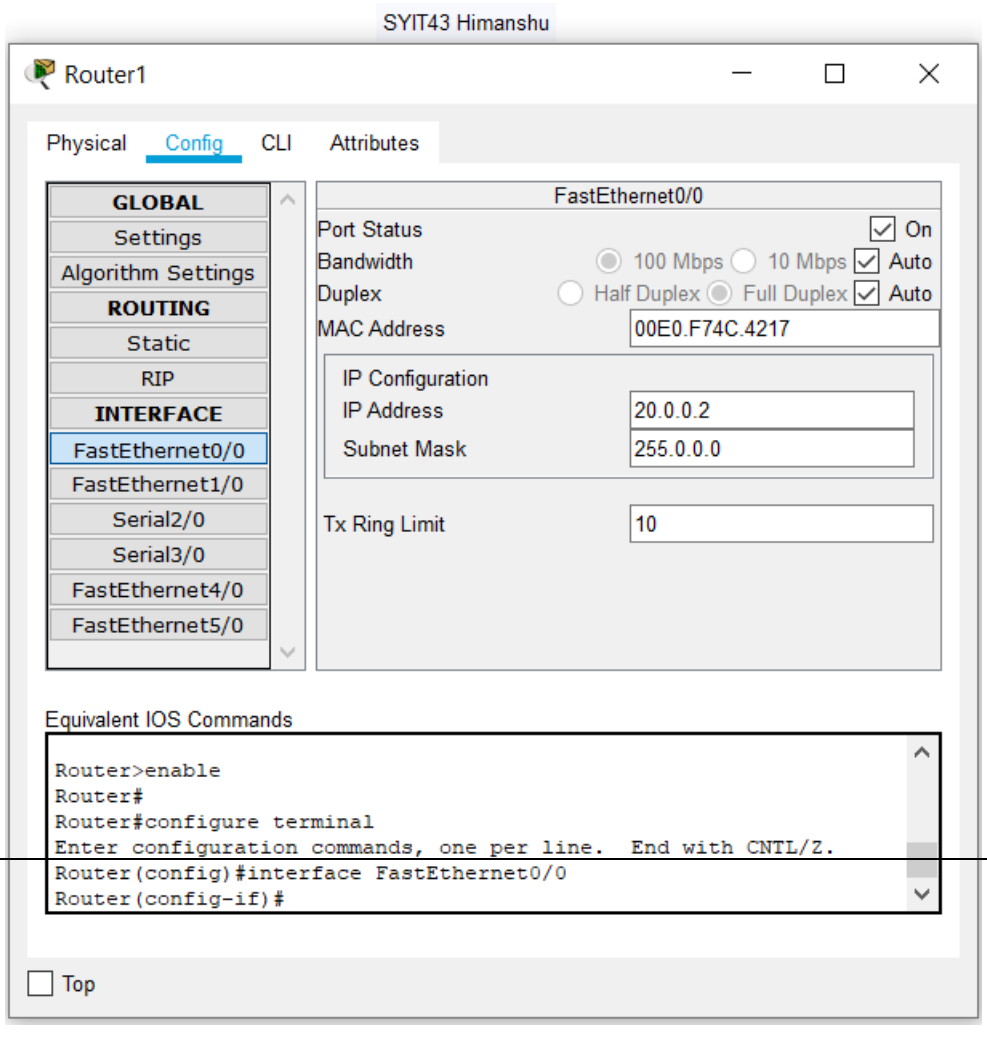


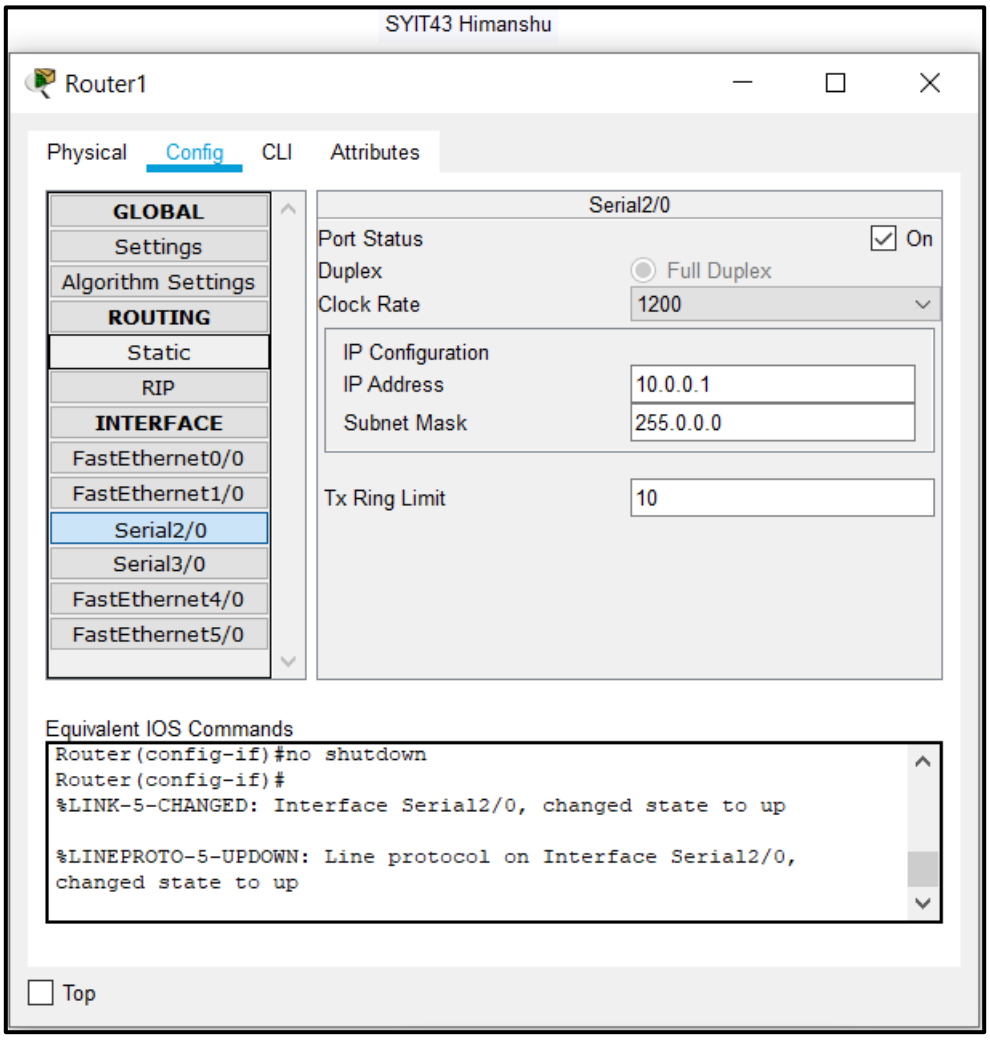
Step 3: (CONFIGURE Router0)





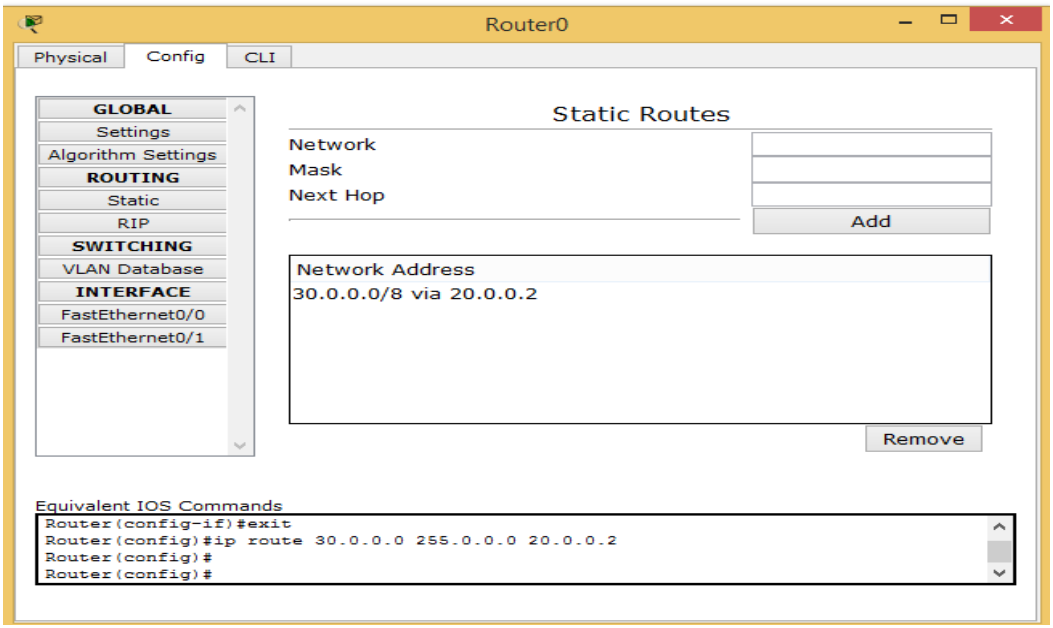
Step 4: (configure Router 1)



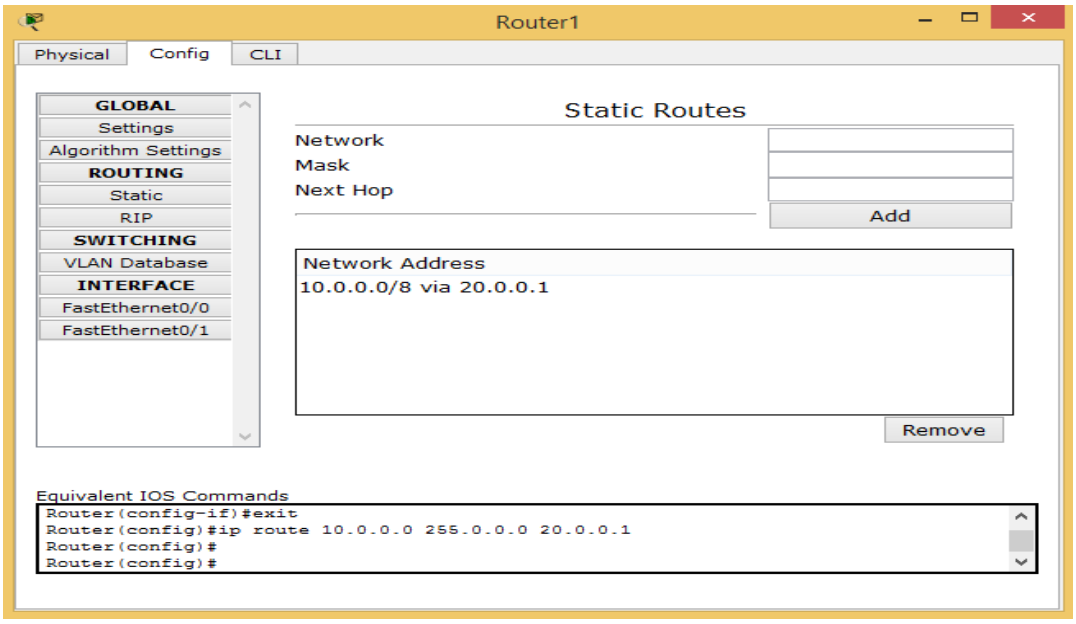


The routing table is configured in the following way

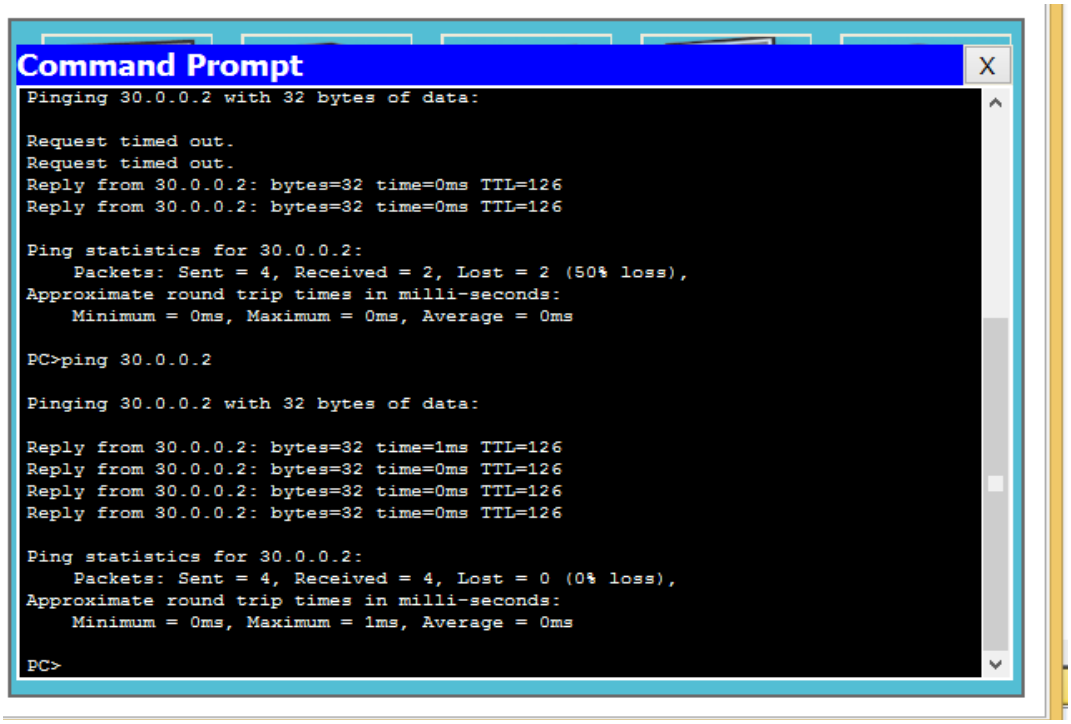
For router 0


Router0
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Static Routes
Network
Mask
Next Hop
Add
Network Address
30.0.0.0/8 via 20.0.0.2
Remove
Equivalent IOS Commands
Router(config-if)#exit
Router(config)#ip route 30.0.0.0 255.0.0.0 20.0.0.2
Router(config)#
Router(config)#

For router 1



Now we can give the ping command as shown to check the connectivity



So static routing has been studied

PRACTICAL NO 5

Configuring DHCP and DNS

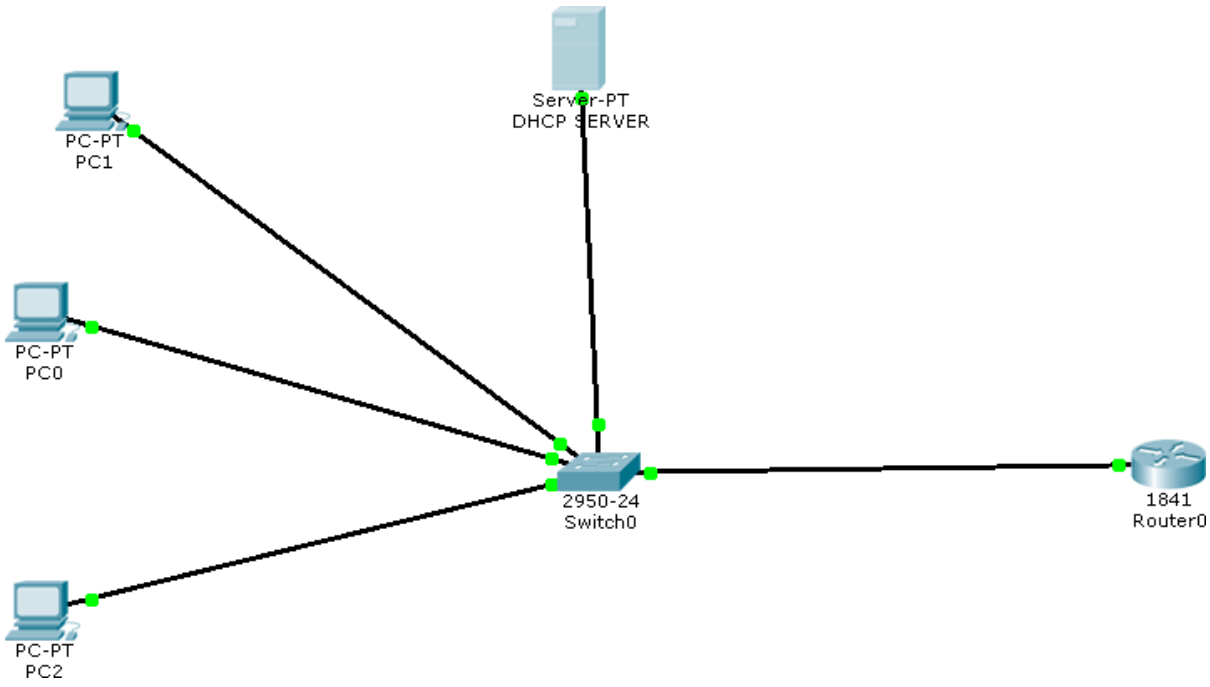
DHCP

The Dynamic Host Configuration Protocol (DHCP) is a client/server protocol designed to provide the four pieces of information for a diskless computer or a computer that is booted for the first time. DHCP is a successor to BOOTP and is backward compatible with it. Although BOOTP is considered deprecated, there may be some systems that may still use BOOTP for host configuration. The part of the discussion in this chapter that does not deal with the dynamic aspect of DHCP can also be applied to BOOTP.

The DHCP client and server can either be on the same network or on different networks. When on same network it works as follows.

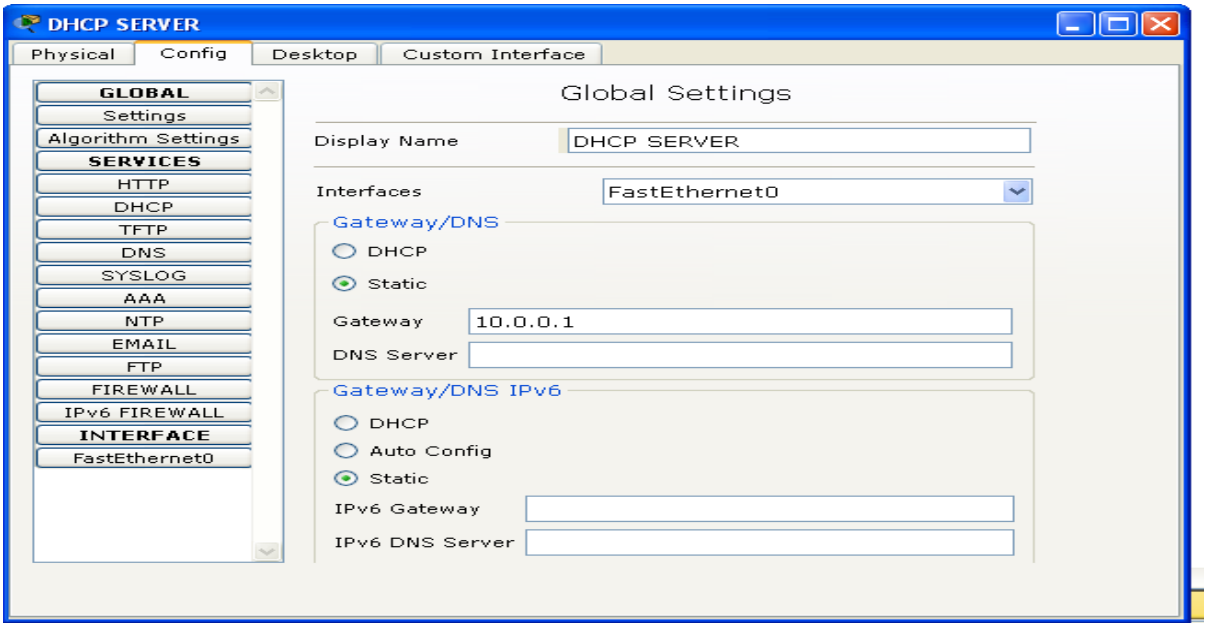
i. The DHCP server issues a passive open command on UDP port number 67 and waits for a client.
ii. A booted client issues an active open command on port number 68. The message is encapsulated in a UDP user datagram, using the destination port number 67 and the source port number 68. The UDP user datagram, in turn, is encapsulated in an IP datagram. The reader may ask how a client can send an IP datagram when it knows neither its own IP address (the source address) nor the server's IP address (the destination address). The client uses all 0s as the source address and all 1s as the destination address.
iii. The server responds with either a broadcast or a unicast message using UDP source port number 67 and destination port number 68. The response can be unicast because the server knows the IP address of the client. It also knows the physical address of the client, which means it does not need the services of ARP for logical to physical address mapping. However, some systems do not allow the bypassing of ARP, resulting in the use of the broadcast address

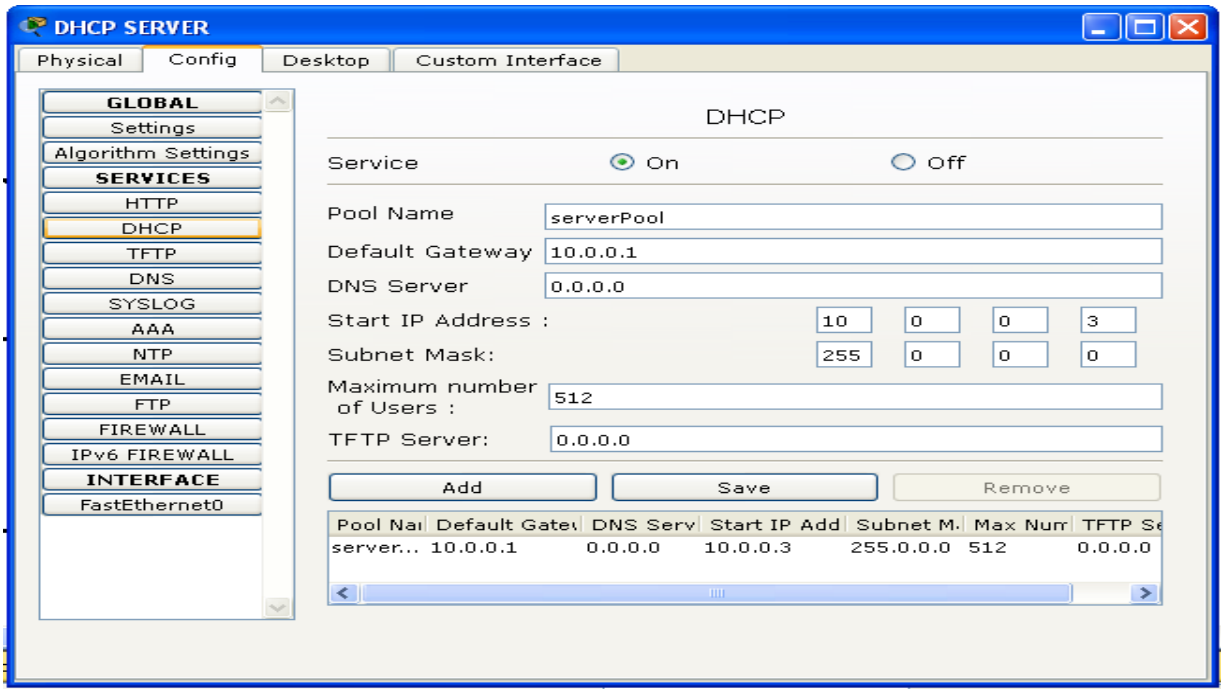
We can study the working of DHCP using the cisco packet tracer using the following example.



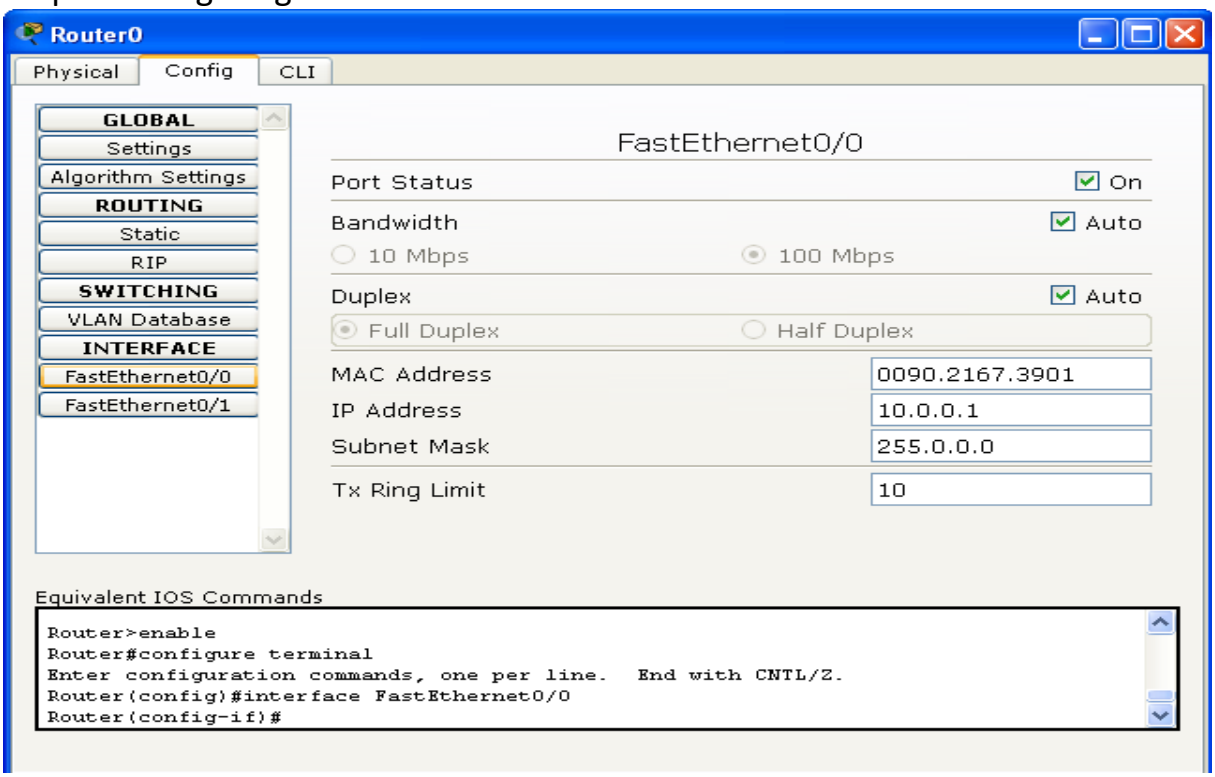
We configure the various components through the following steps

Step 1: Configuring the DHCP server



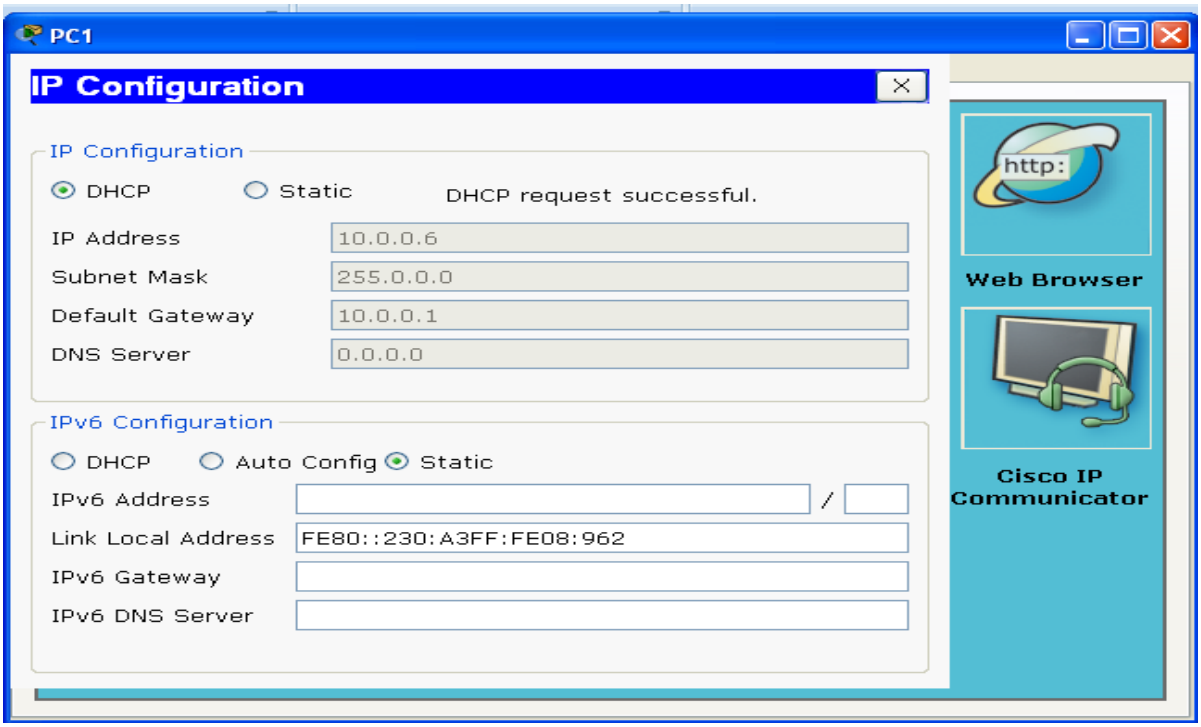


Step 2: Configuring the Router



Now we test the working of the DHCP server by sending a DHCP request from any of the PC as shown

Step 3: Sending DHCP request



Hence we have configured a DHCP server and also verified its operation

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.

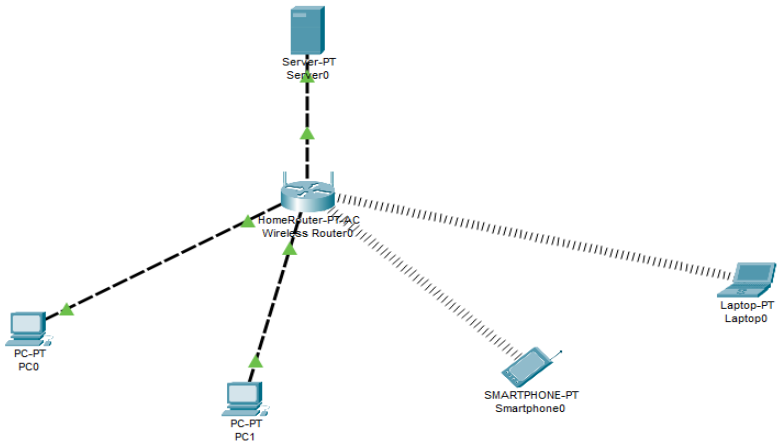
1) It is easier to set up compared to setting up a wired network.
2) It is more convenient to access.
3) It is less complicated to add new users in the network.
4) It gives users more flexibility to stay online even when moving from one area in the office to another.
5) Guest users can have Internet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

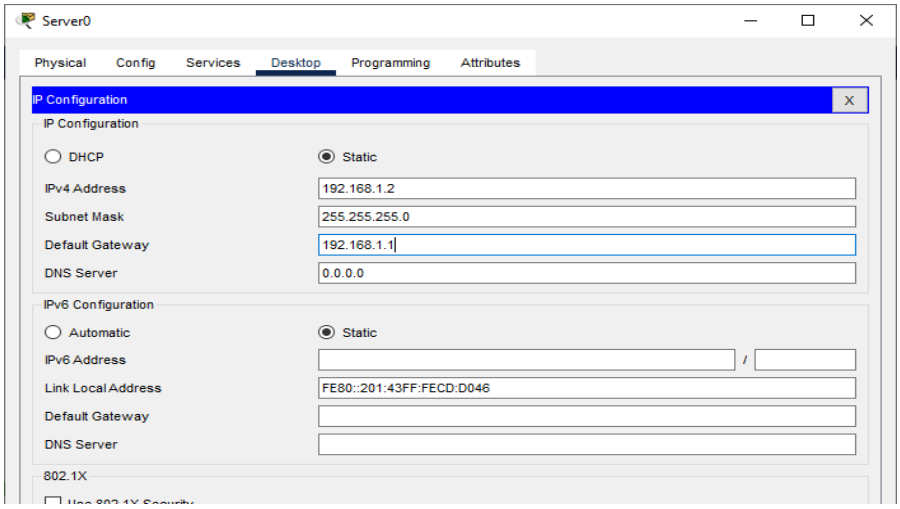
With a WAP, the following can be done:

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.

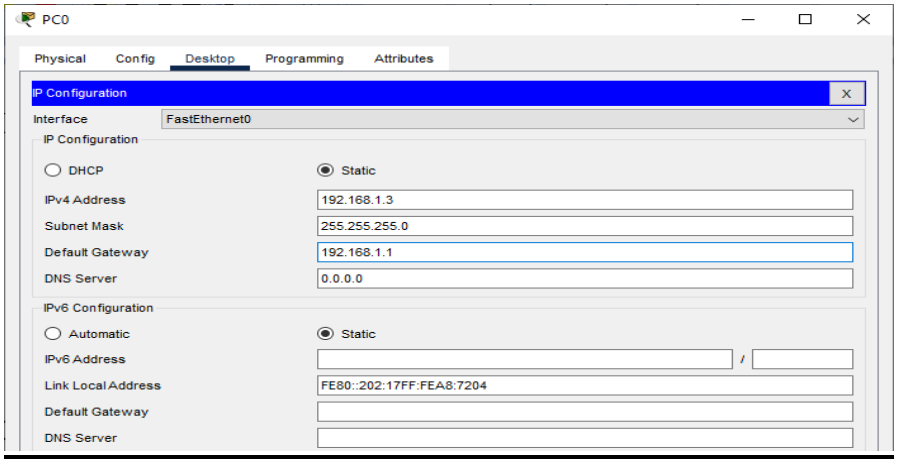
For the present case we use the following topology



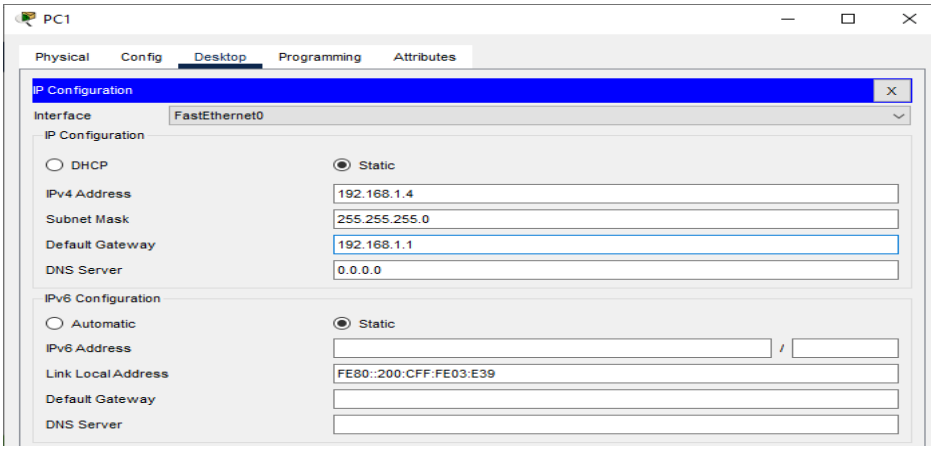
Configure the Server:



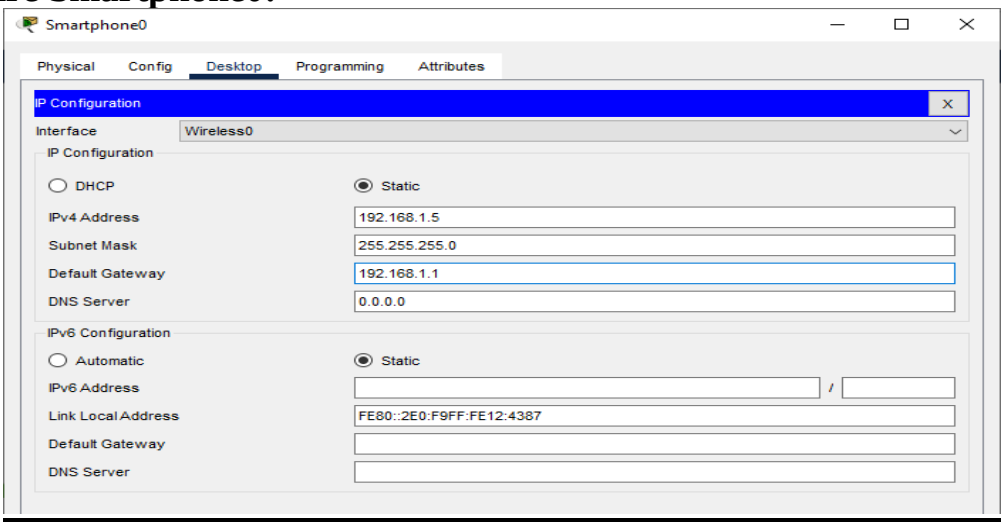
Configure PC0:



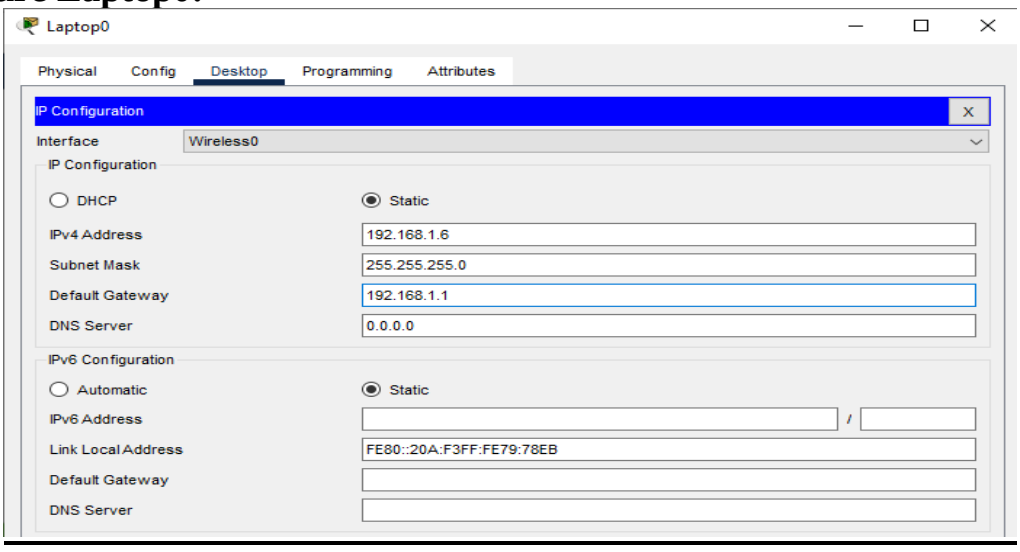
Configure PC1:



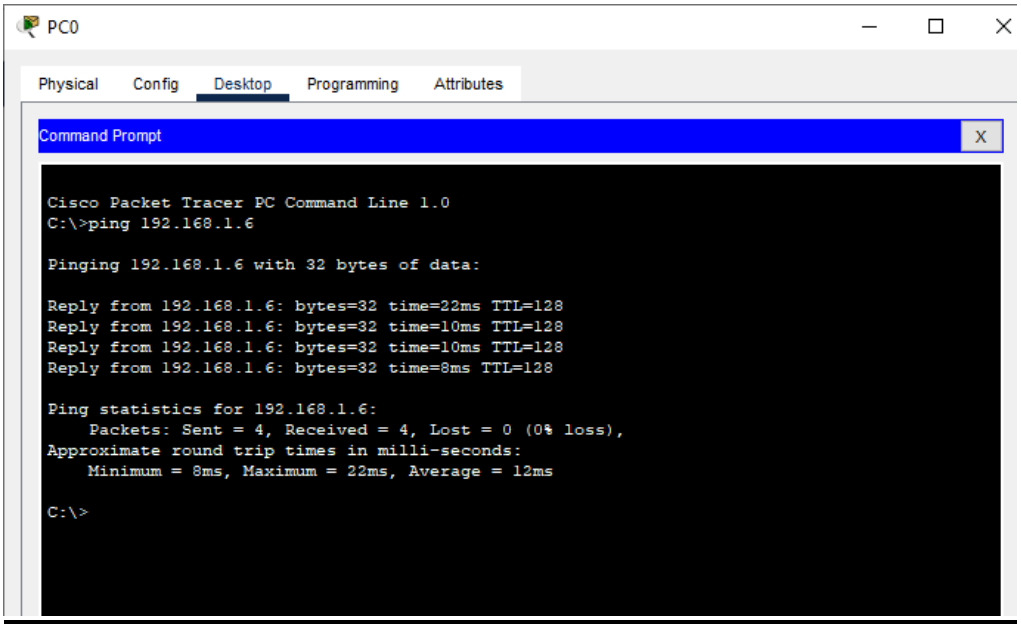
Configure Smartphone0:



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

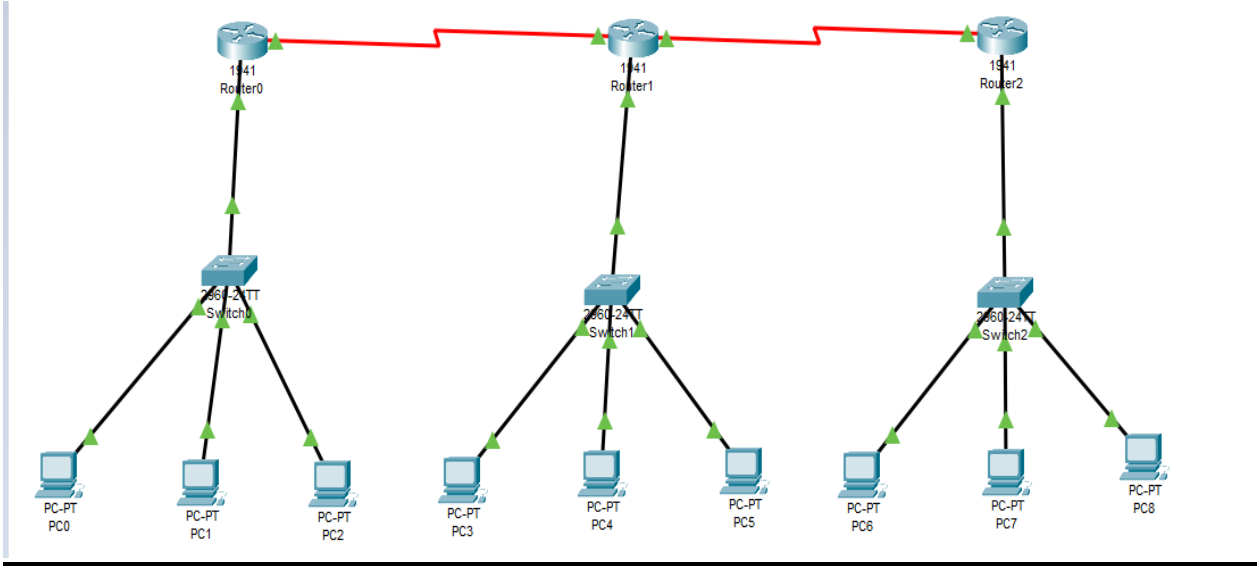
Pros:

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.

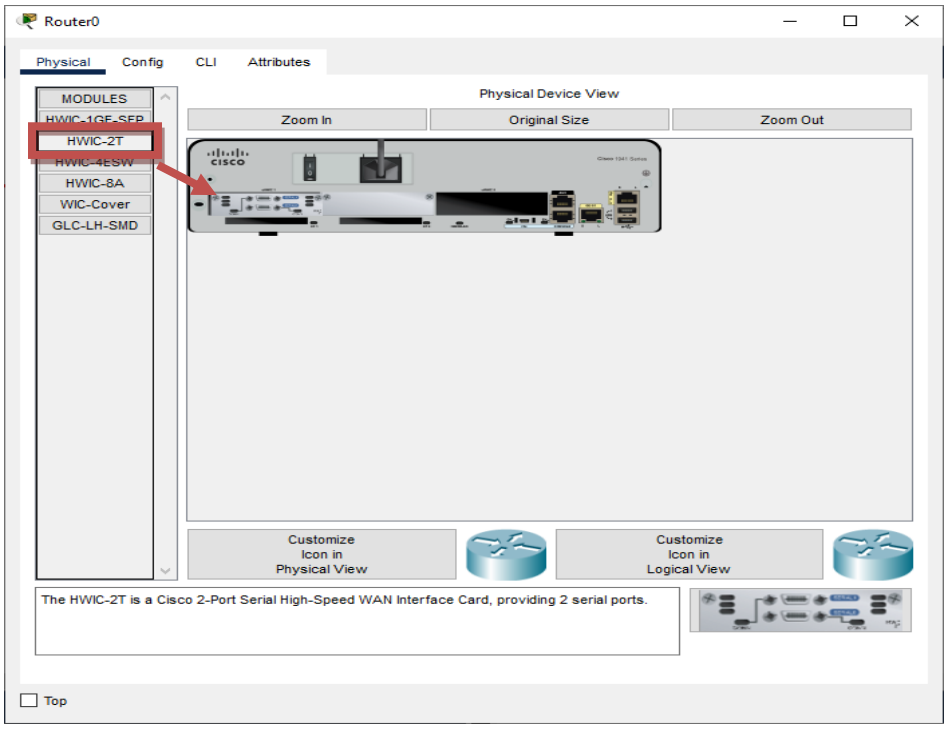
We use the following topology for the present case



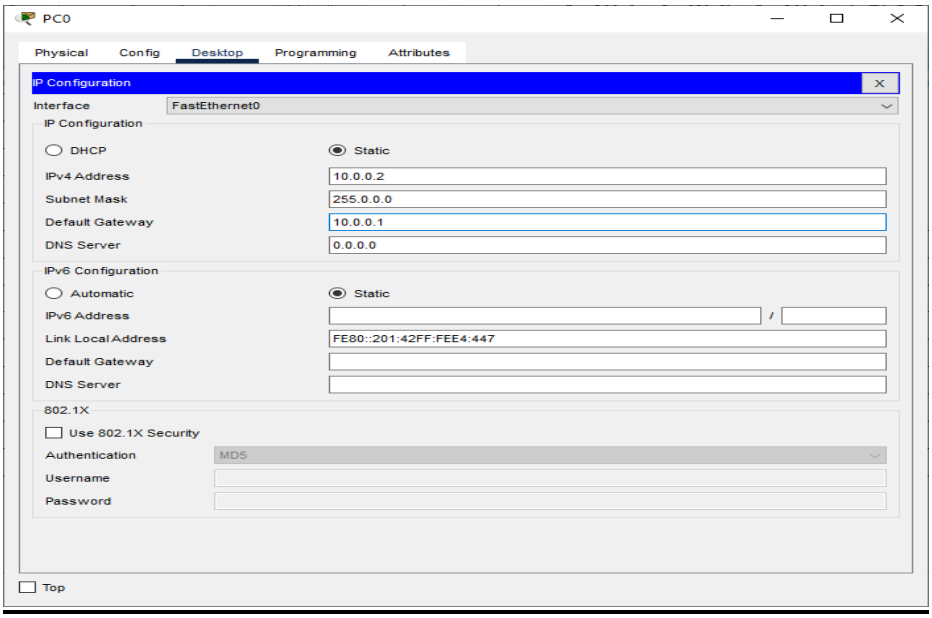
We configure the above network using the following IP addresses

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

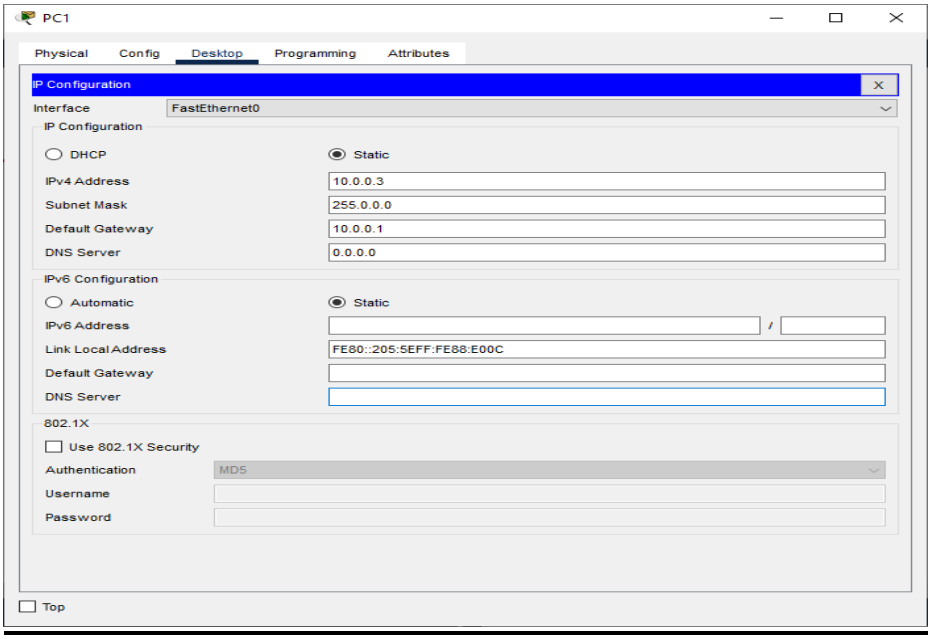
Adding Serial Interface in each Router



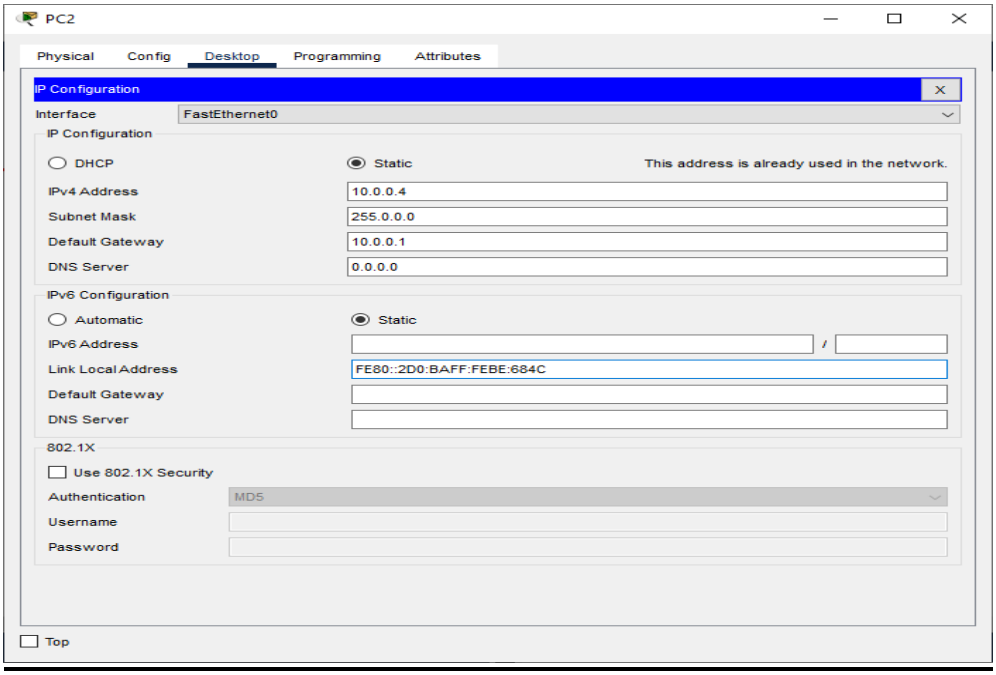
Configuring PC0:



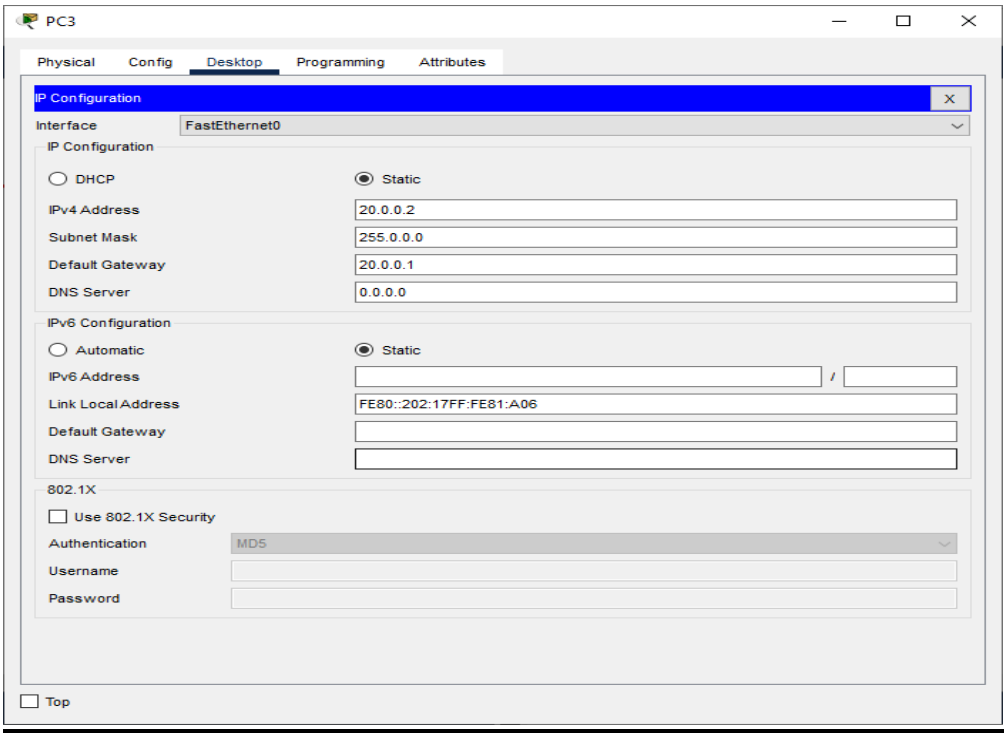
Configuring PC1:



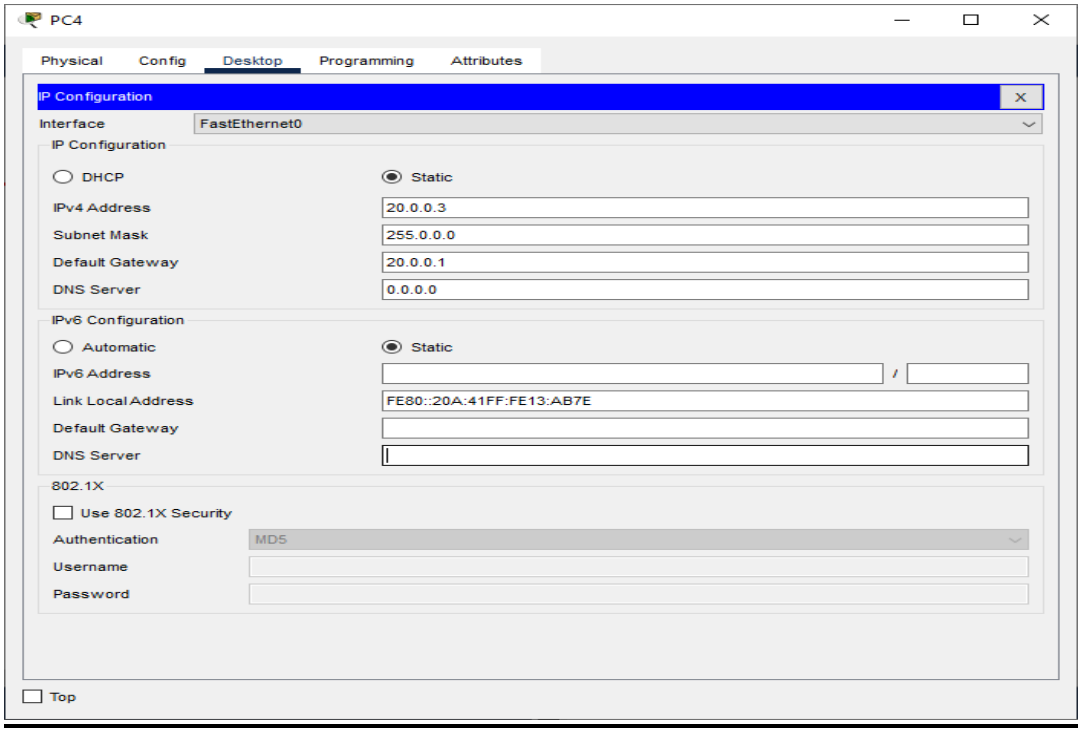
Configuring PC2:



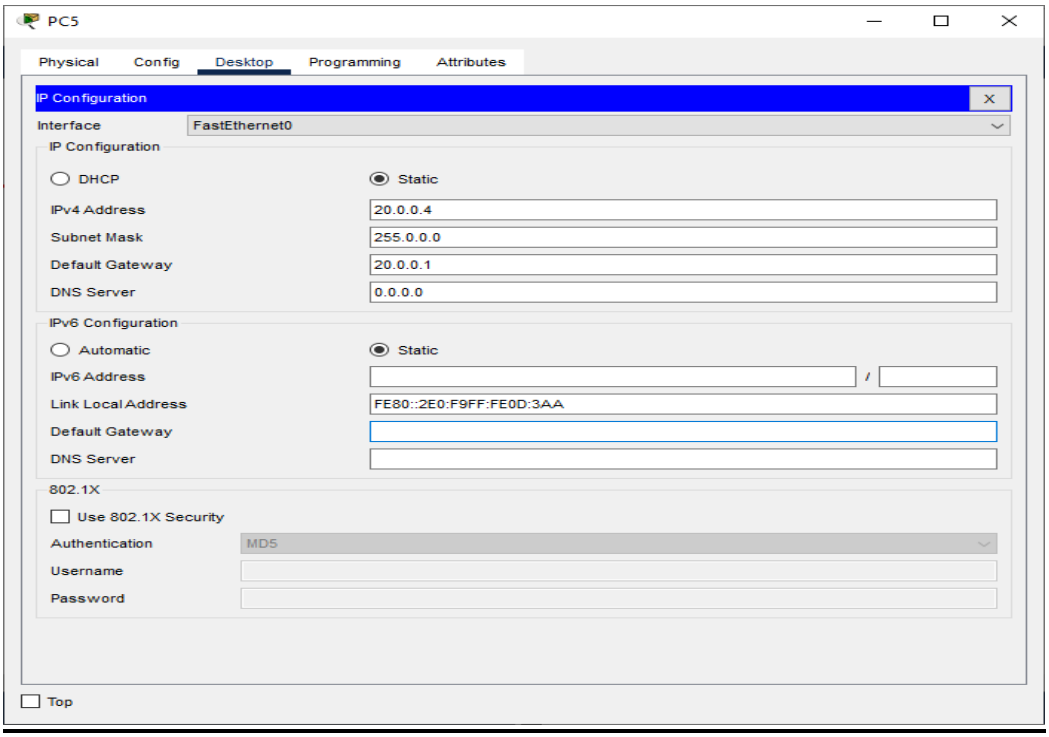
Configuring PC3:



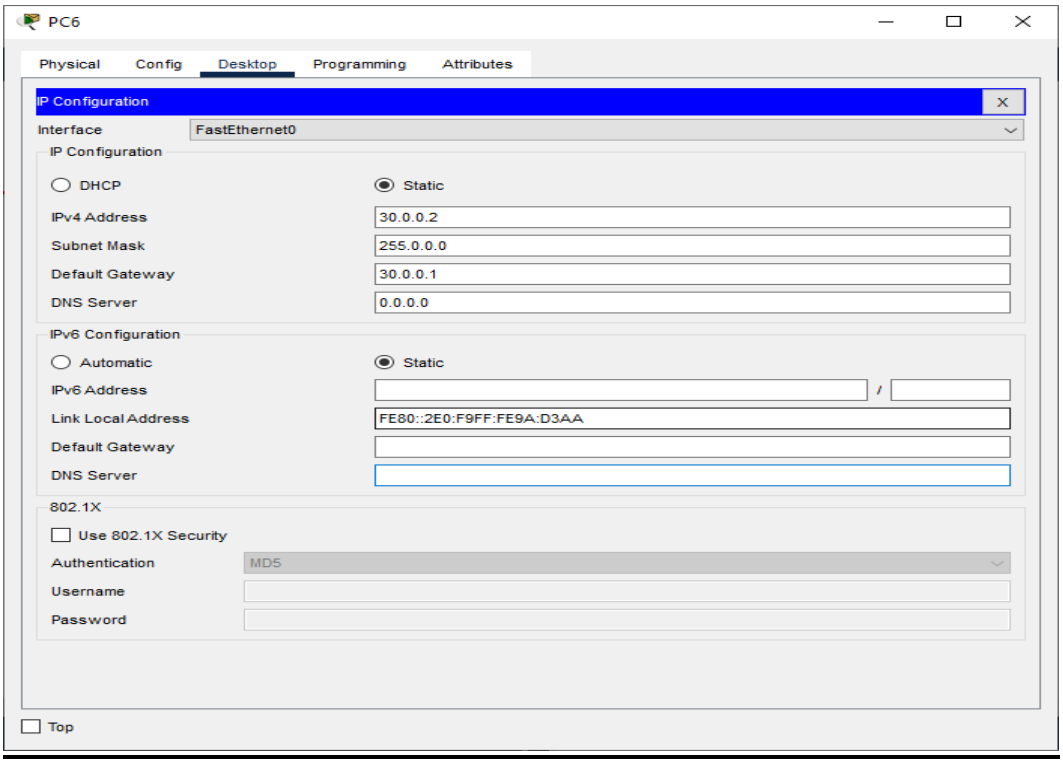
Configuring PC4:



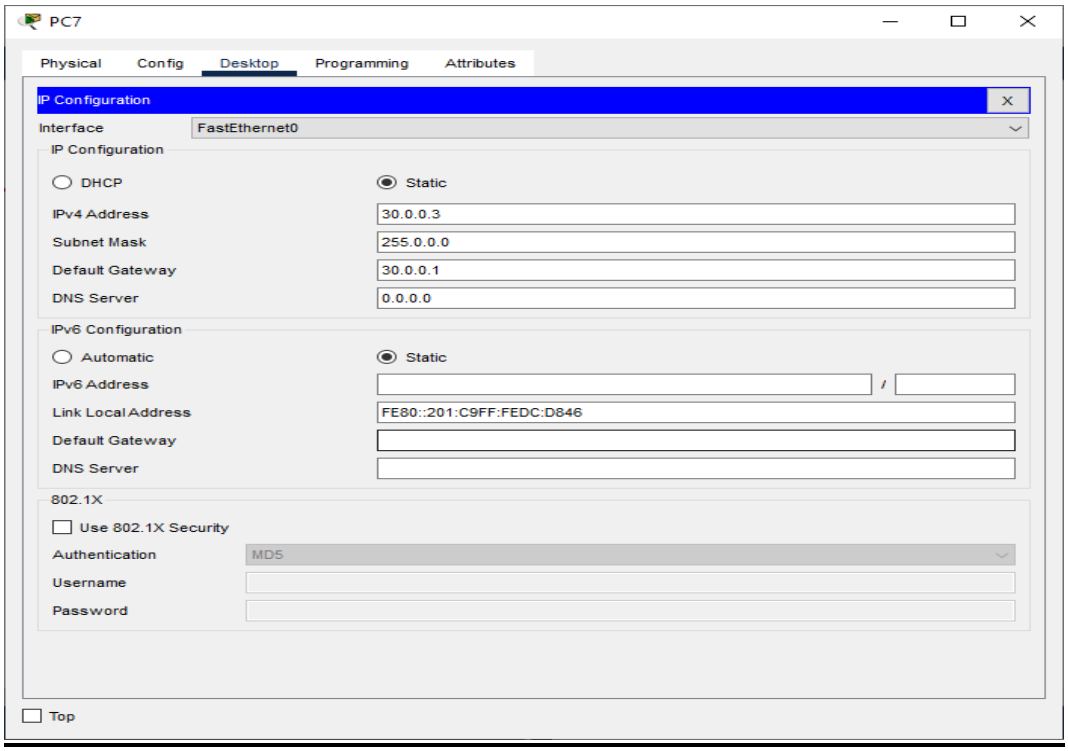
Configuring PC5:



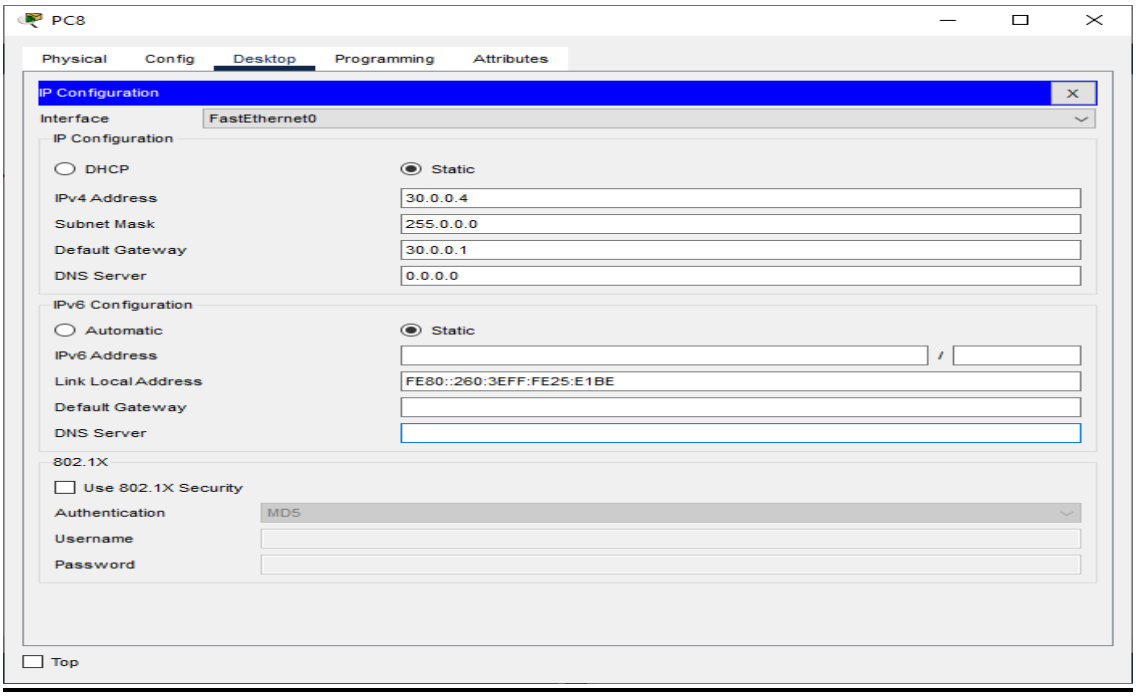
Configuring PC6:



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

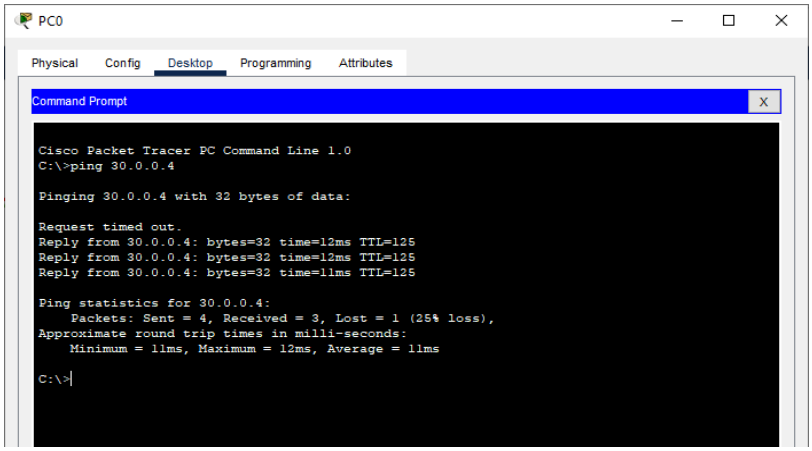
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 192.168.0.0
Router(config-router)#network 20.0.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#
Router#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

Setting the RIPv1 on Router 2

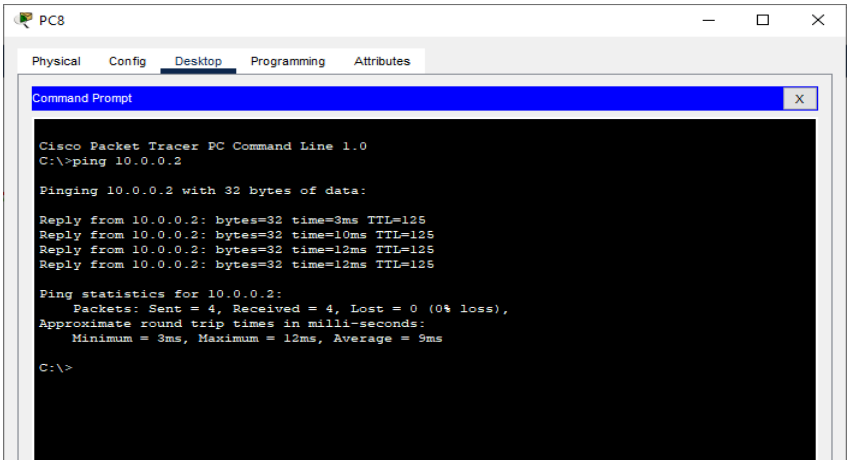
```
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#network 192.168.1.0
Router(config-router)#network 30.0.0.0
Router(config-router)#exit
Router(config)#
```

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.

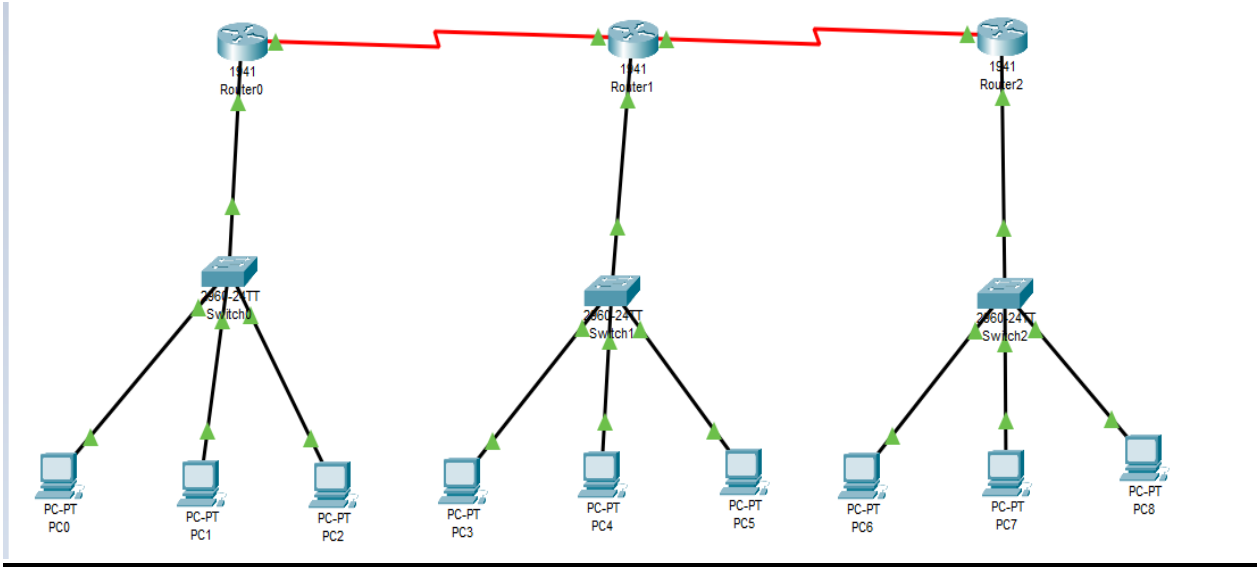
Advantages of RIPv2

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).

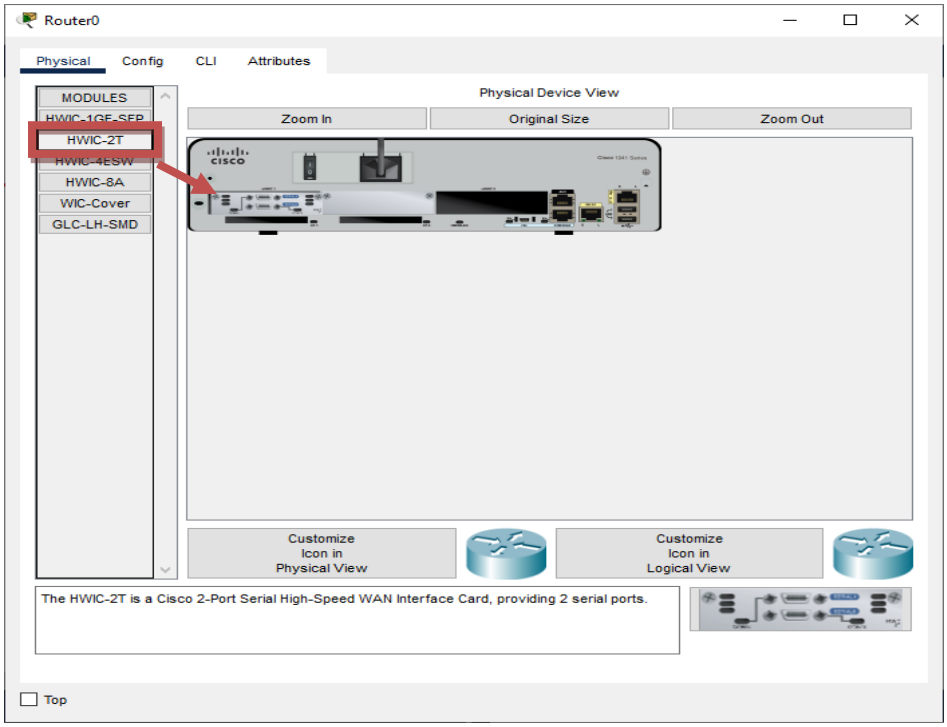
We use the following topology for the present case



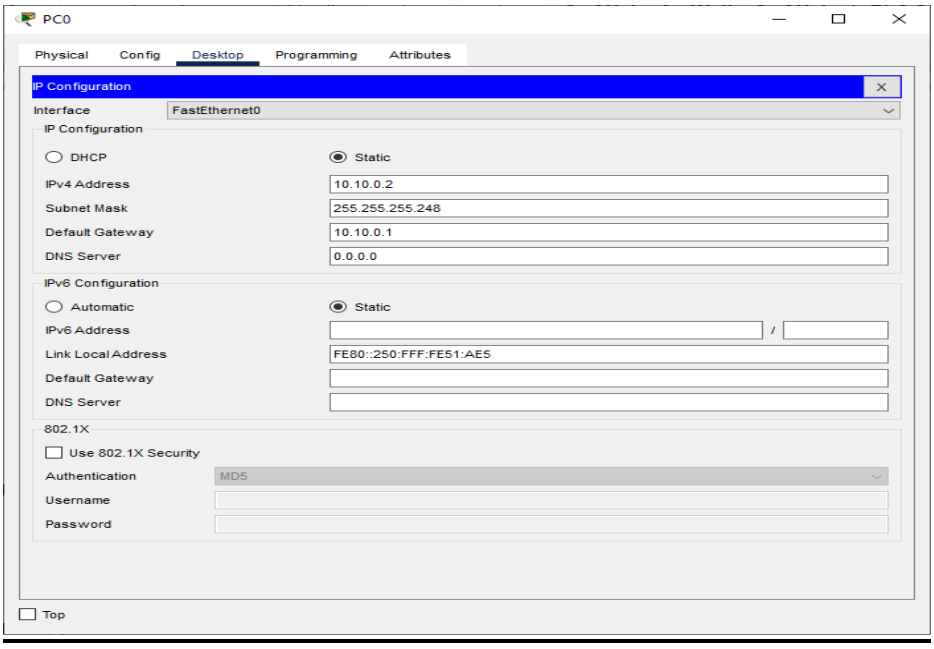
We configure the above network using the following IP addresses

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

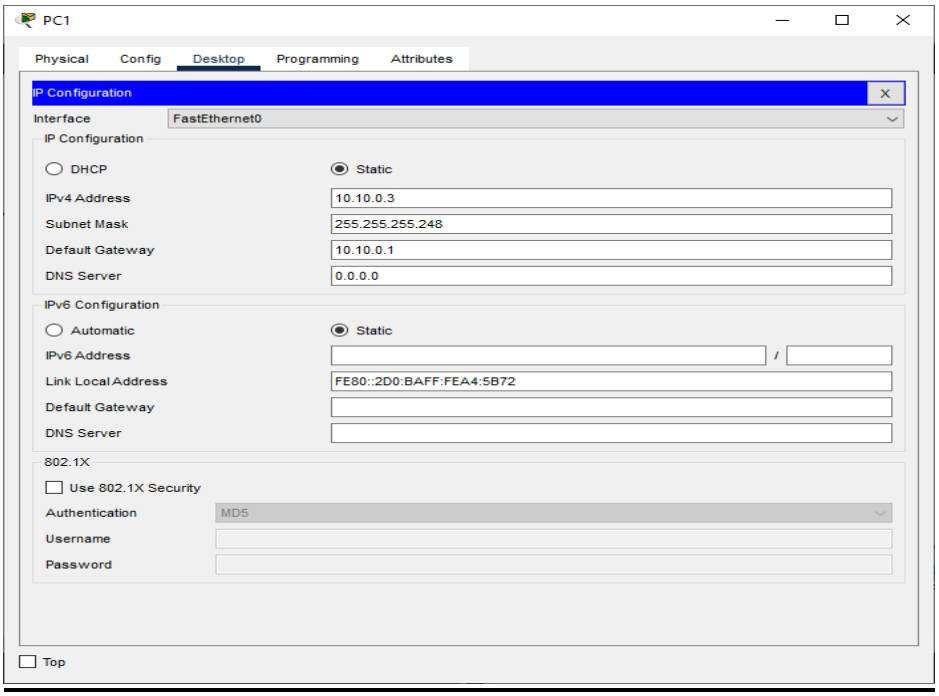
Adding Serial Interface in each Router



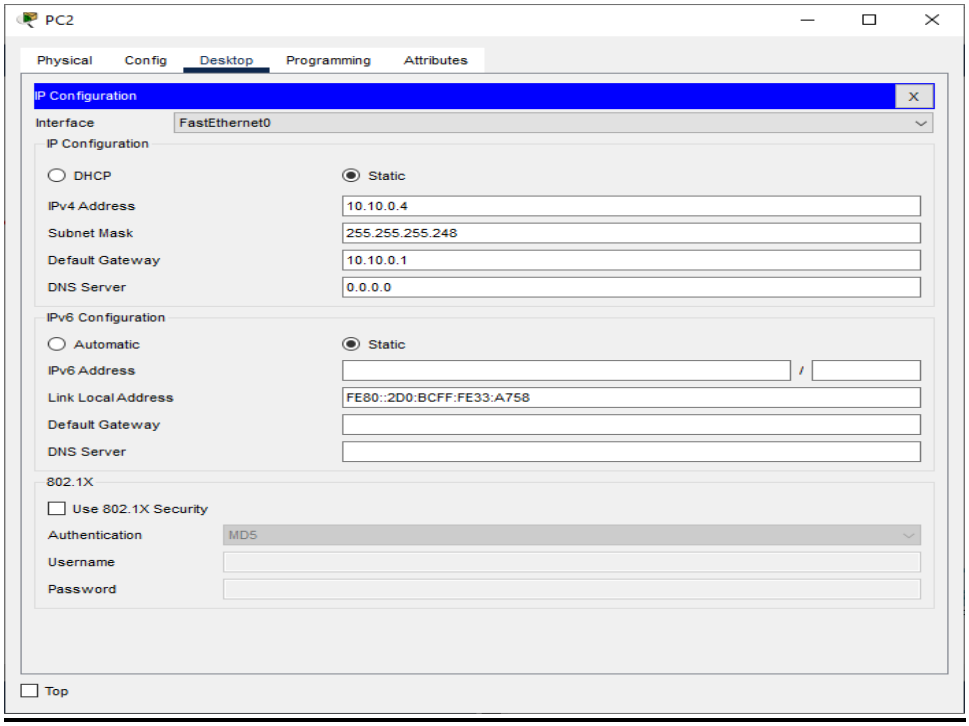
Configuring PC0:



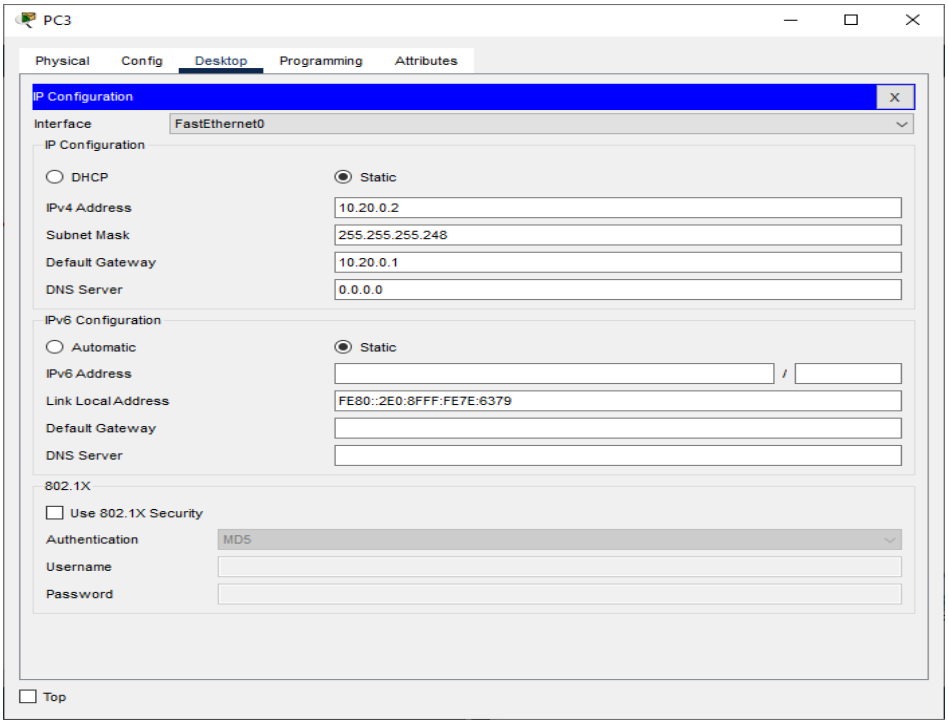
Configuring PC1:



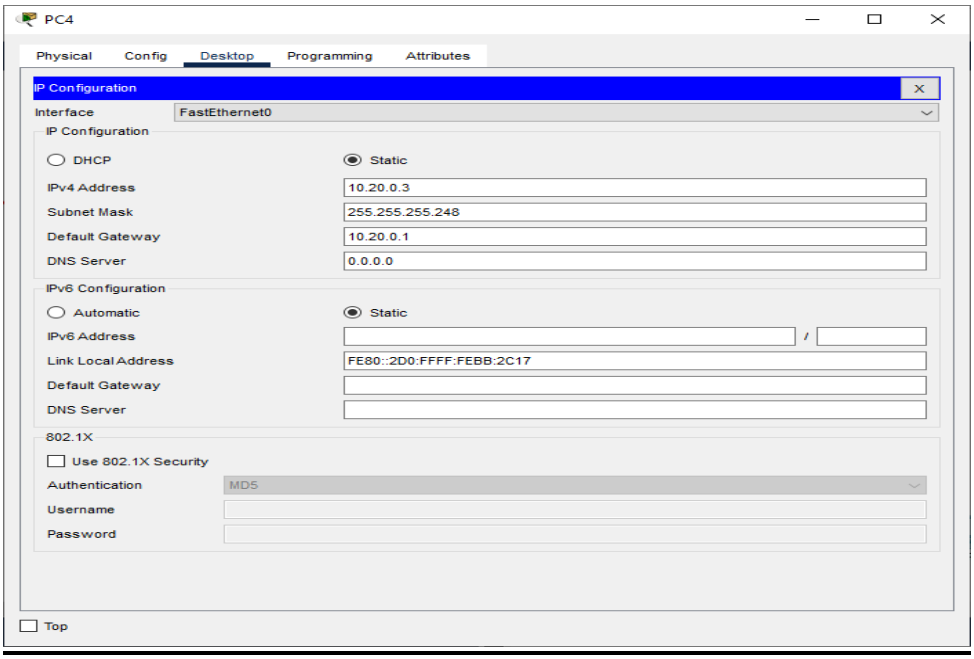
Configuring PC2:



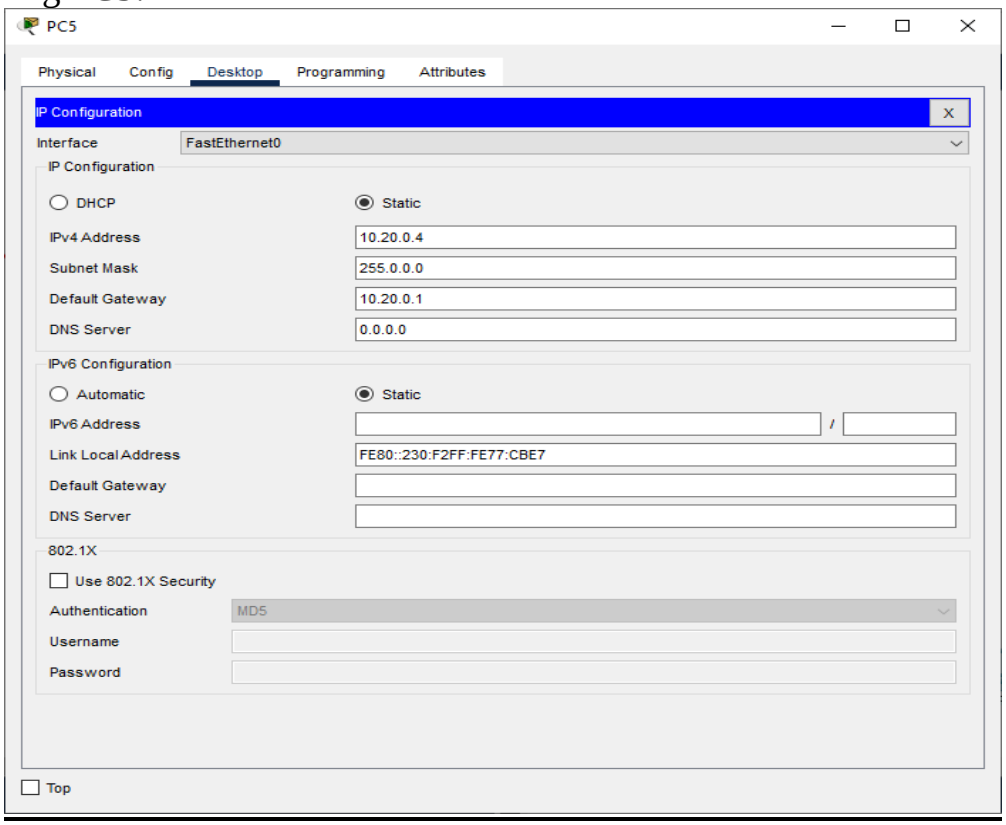
Configuring PC3:



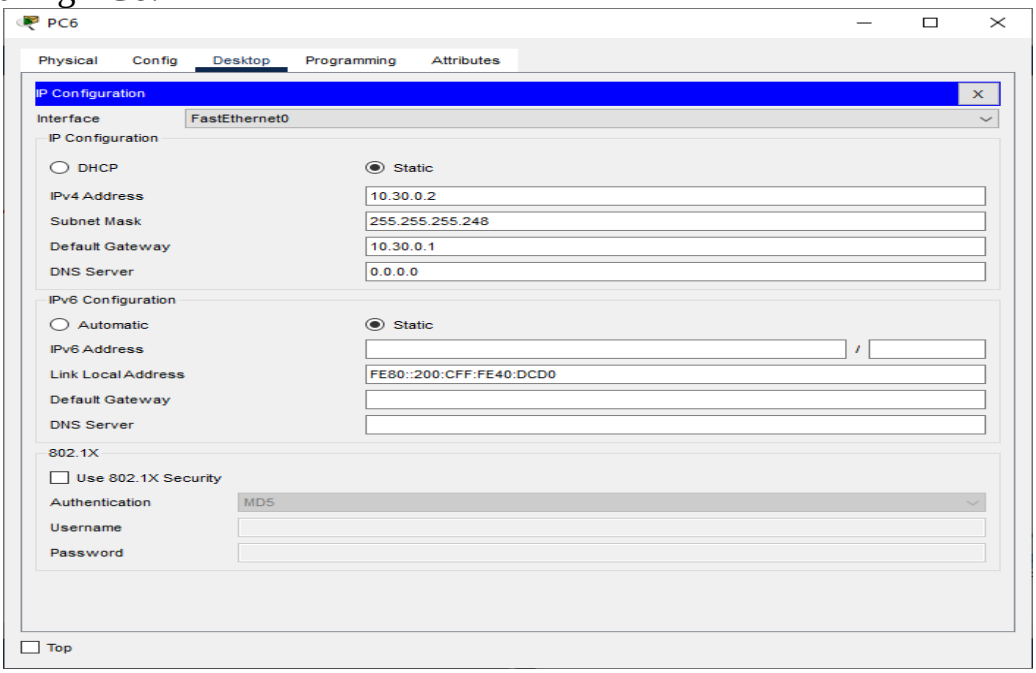
Configuring PC4:



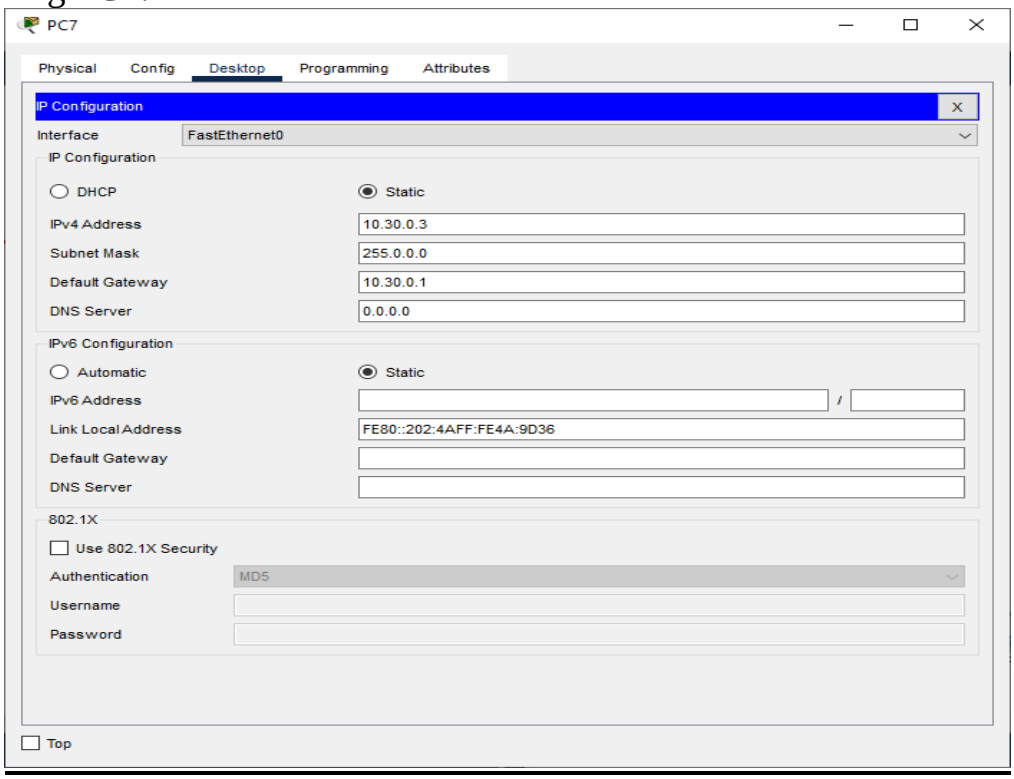
Configuring PC5:



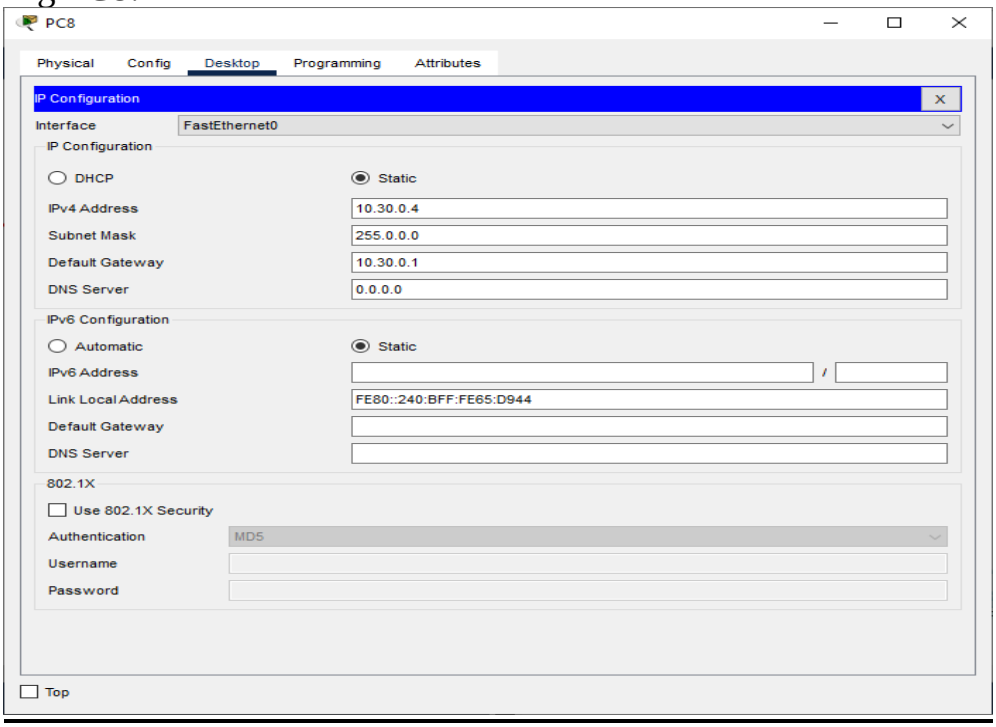
Configuring PC6:



Configuring PC7:

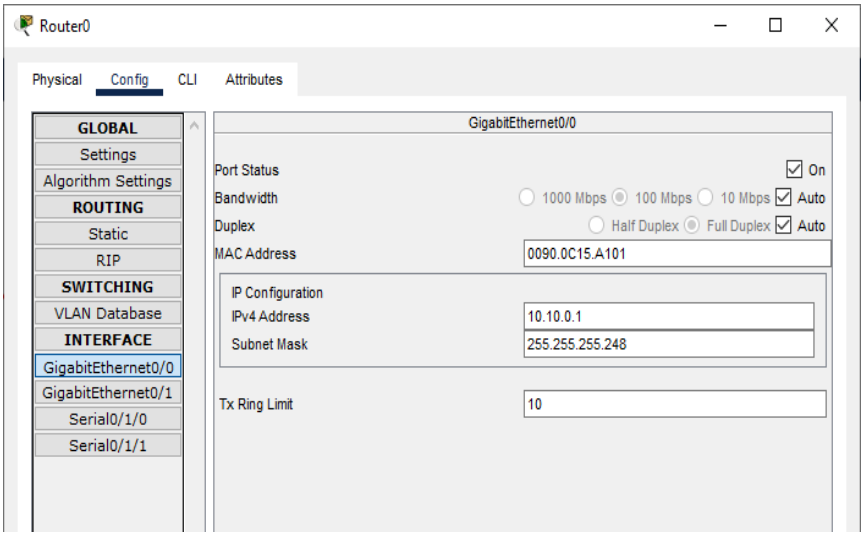


Configuring PC8:

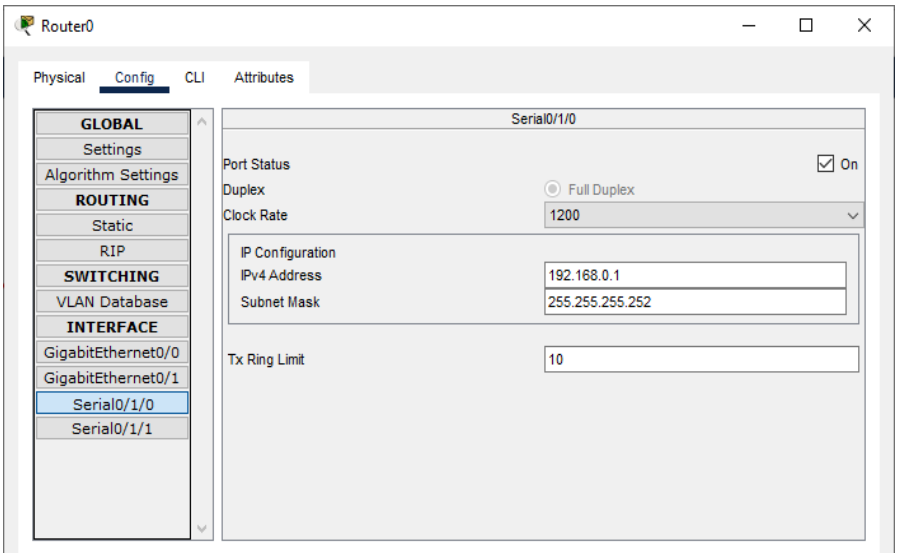


Configuring IP addresses on Router 0

i) Interface G0/0

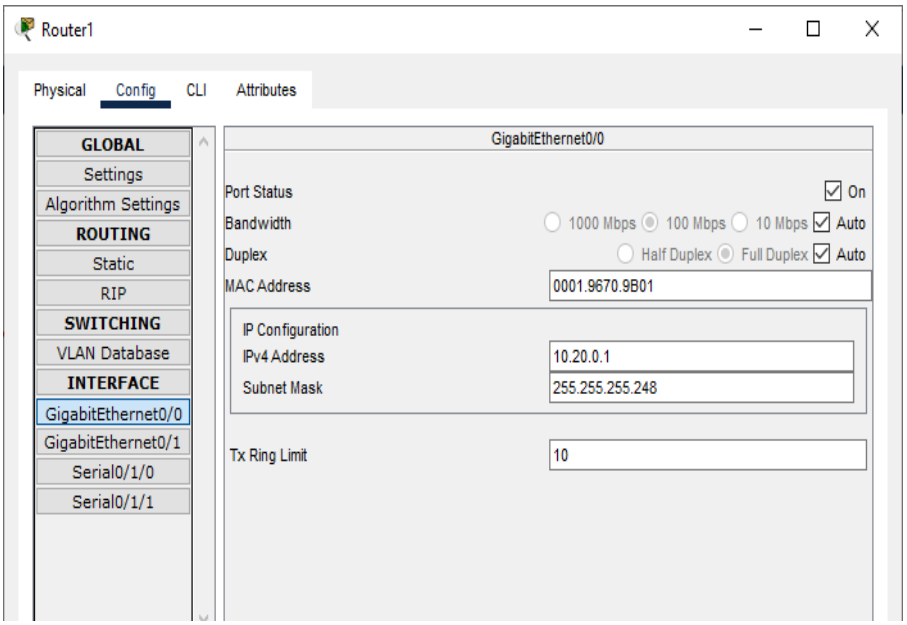


ii) Interface S0/1/0

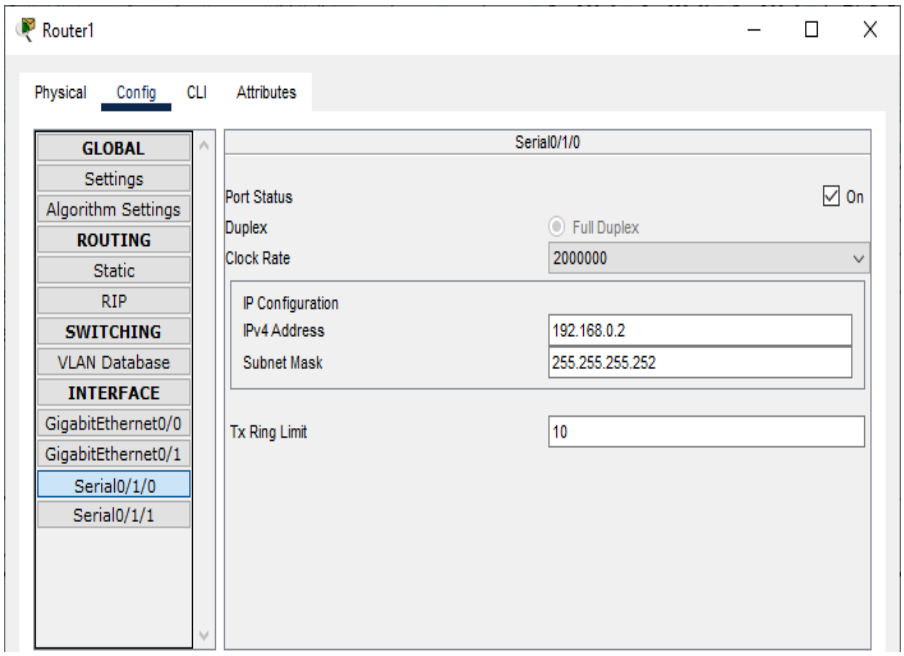


Configuring IP addresses on Router 1

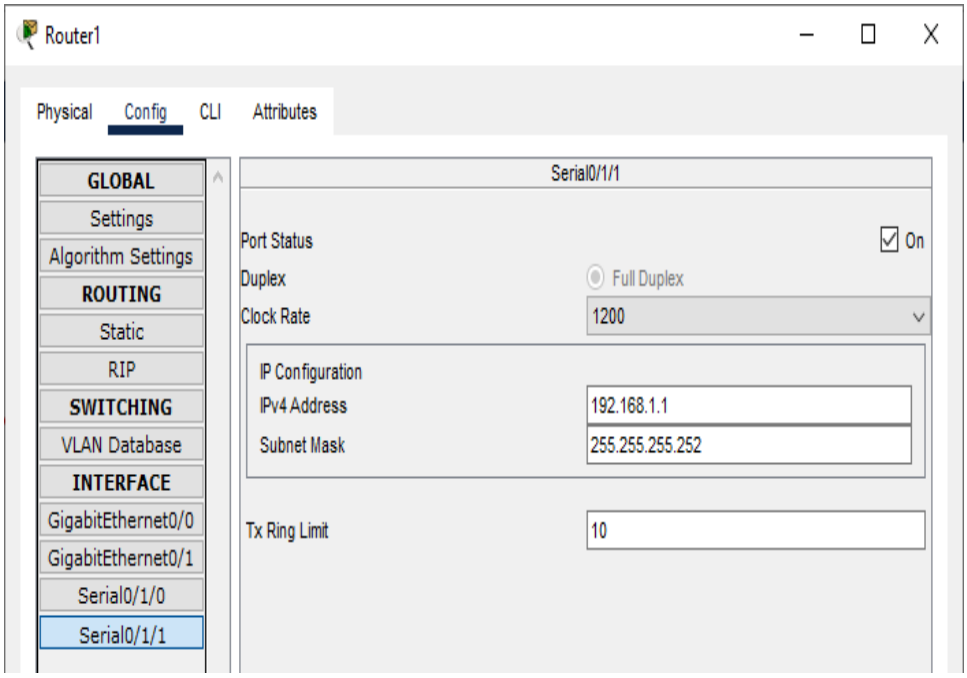
i) Interface G0/0



ii) Interface S0/1/0

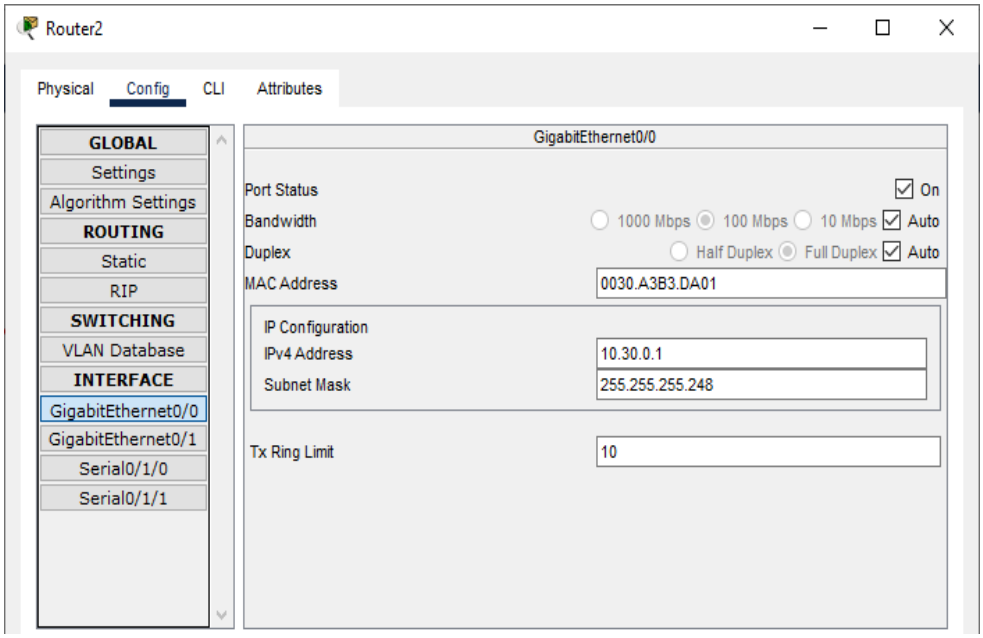


iii) Interface S0/1/1

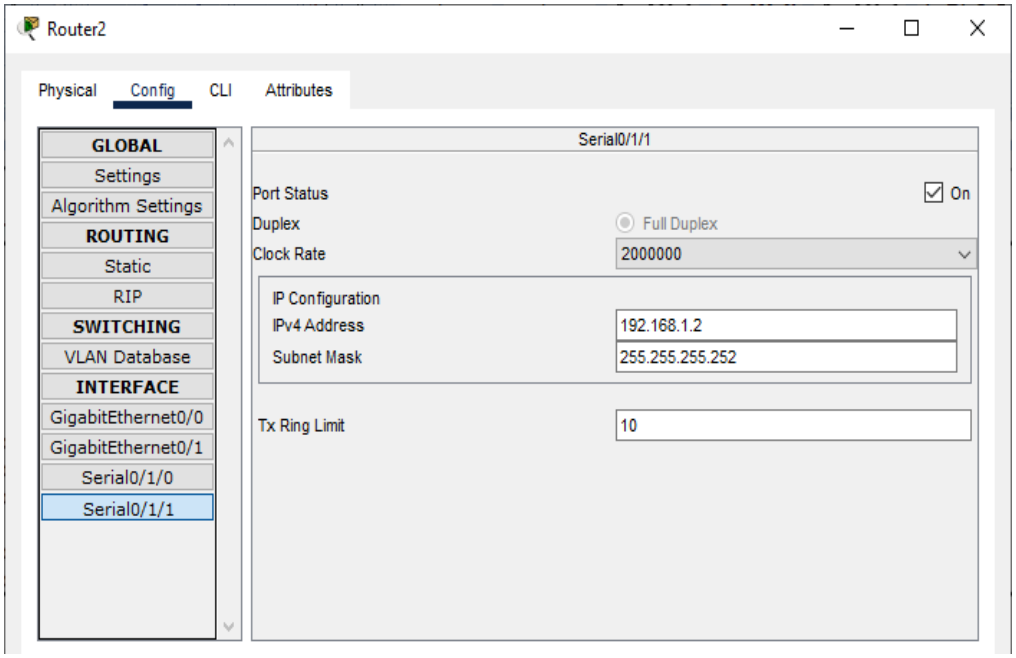


Configuring IP addresses on Router 2

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)

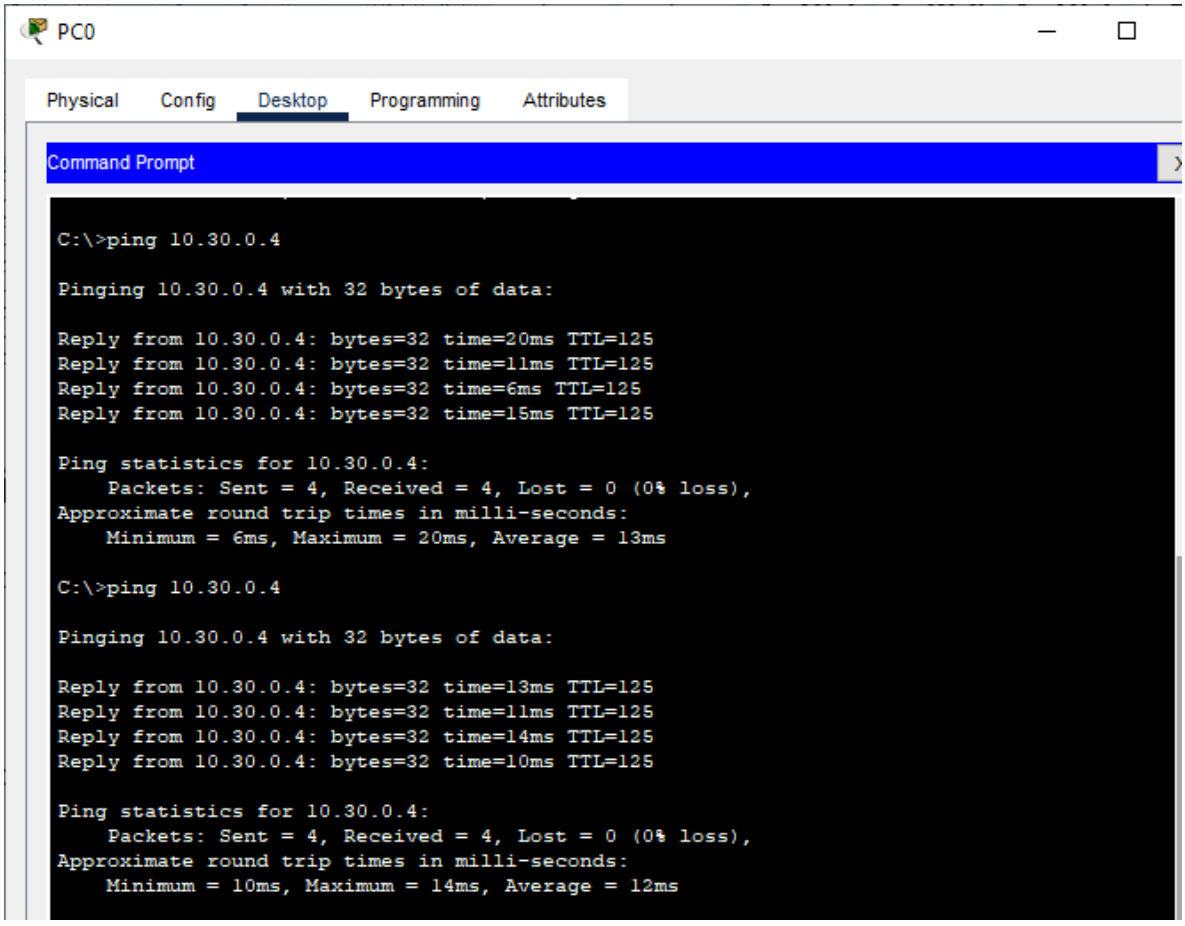
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.20.0.0
Router(config-router)#network 192.168.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#

Configuring Router 2 for RIPv2 (using the CLI mode)

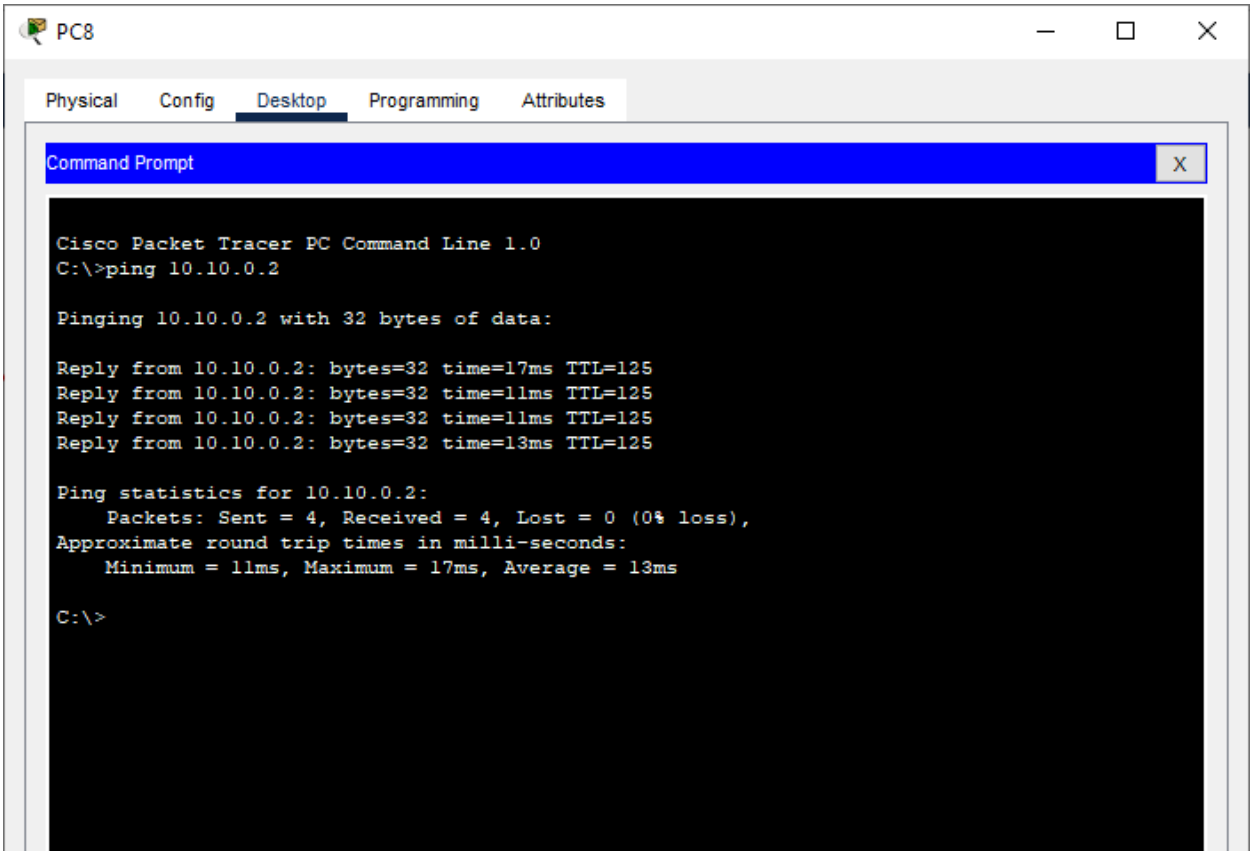
```
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.30.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#
```

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.

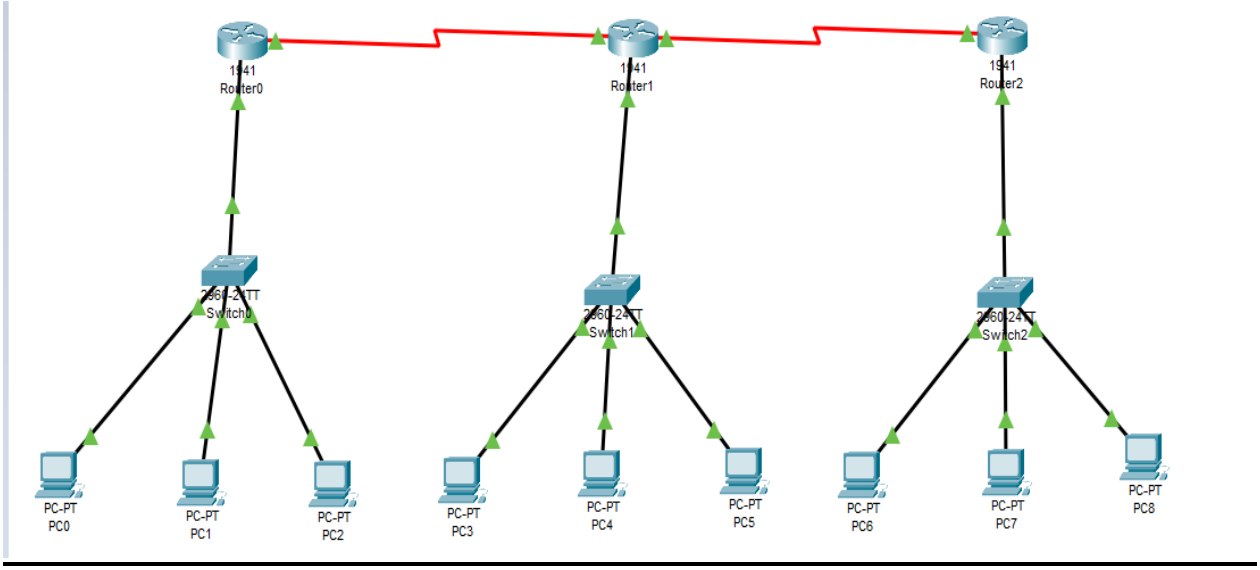
Open shortest path first (OSPF) is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e., the protocol which aims at moving the packet within a large autonomous system or routing domain.

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.

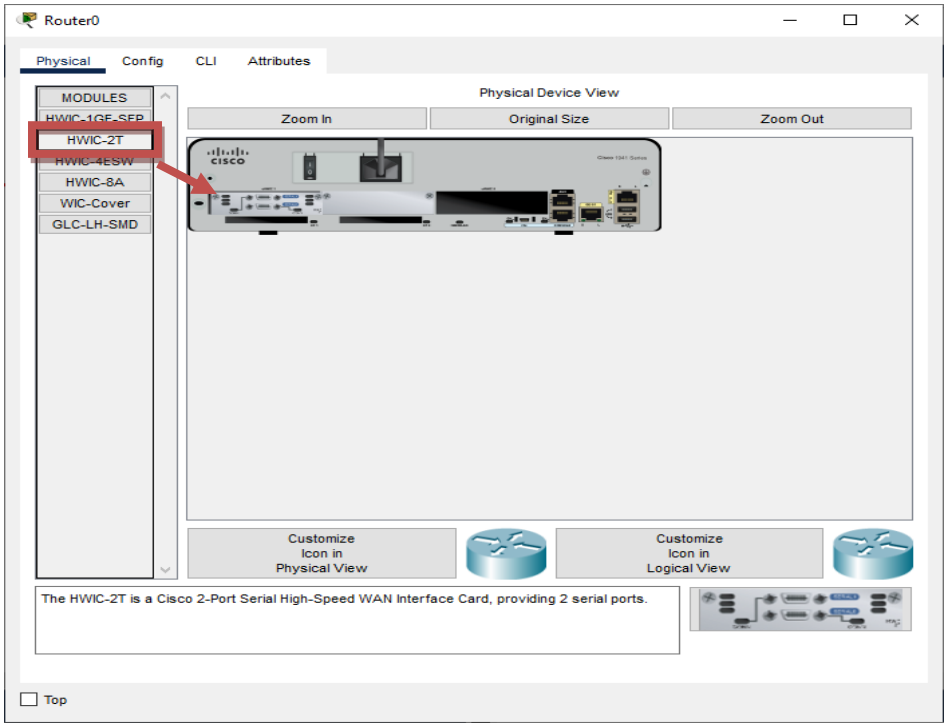
We use the following topology for the present case



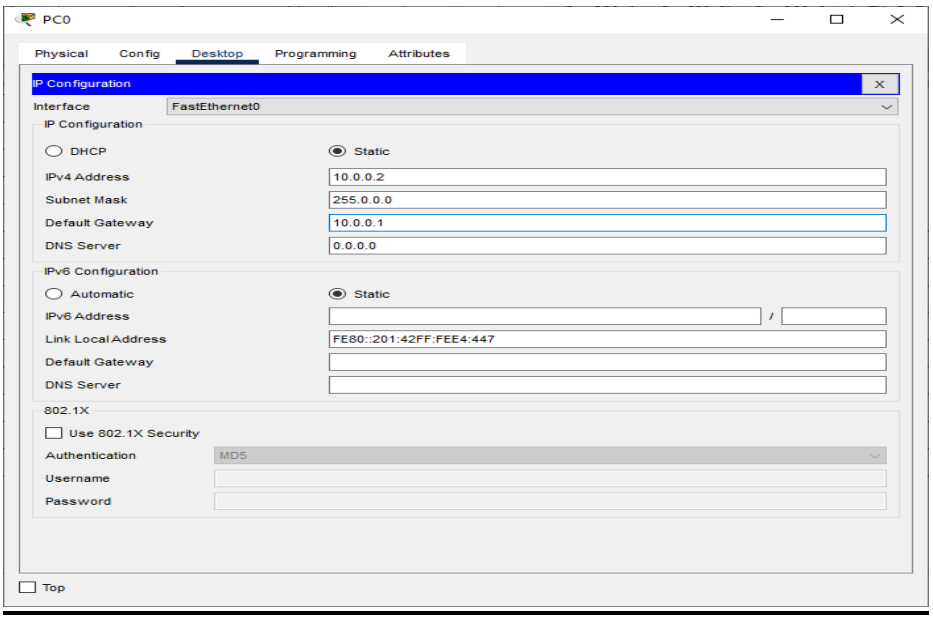
We configure the above network using the following IP addresses

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

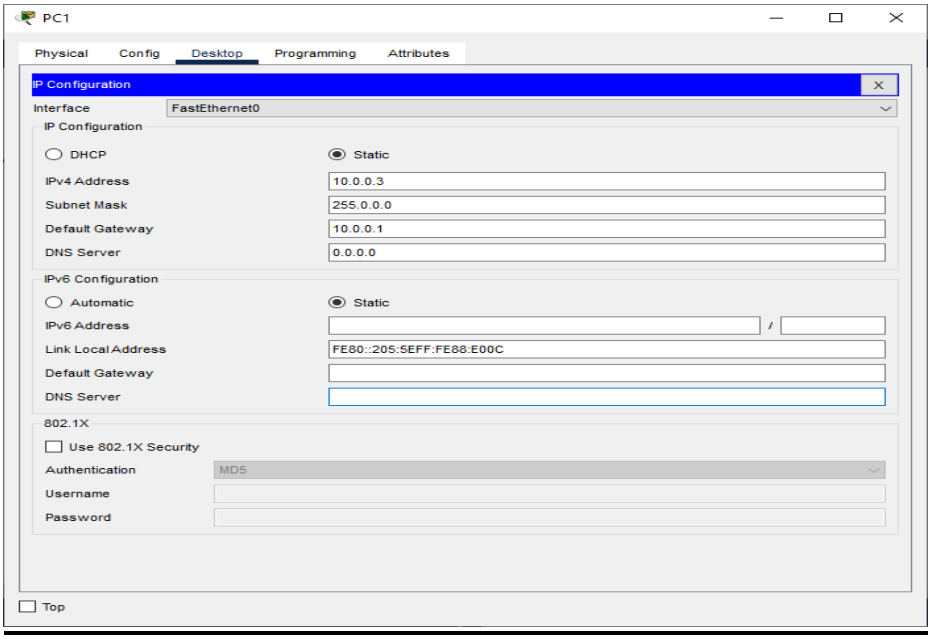
Adding Serial Interface in each Router



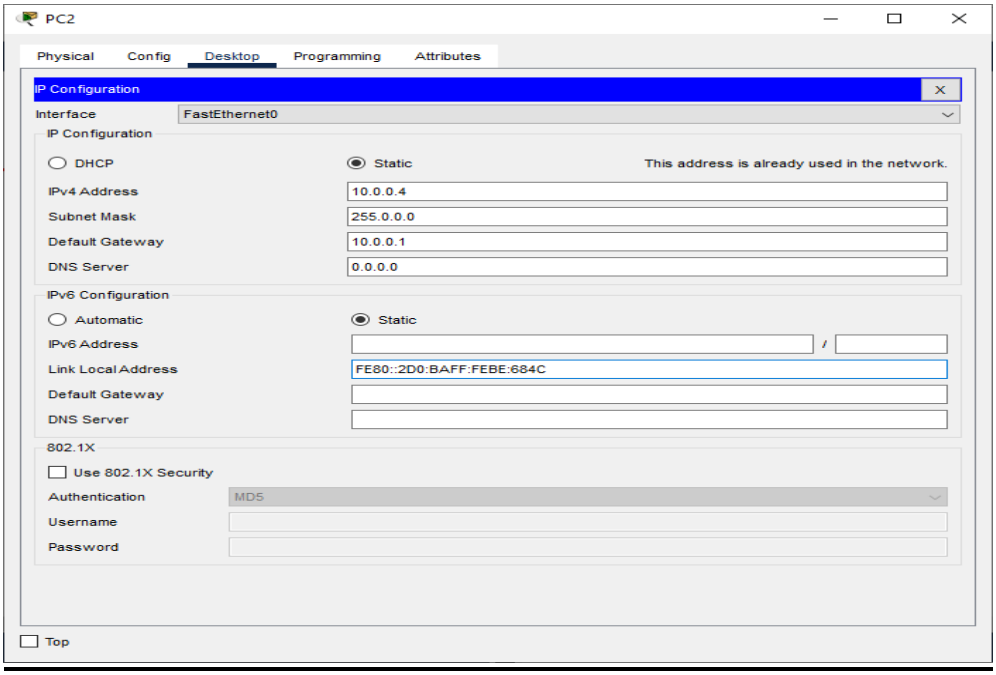
Configuring PC0:



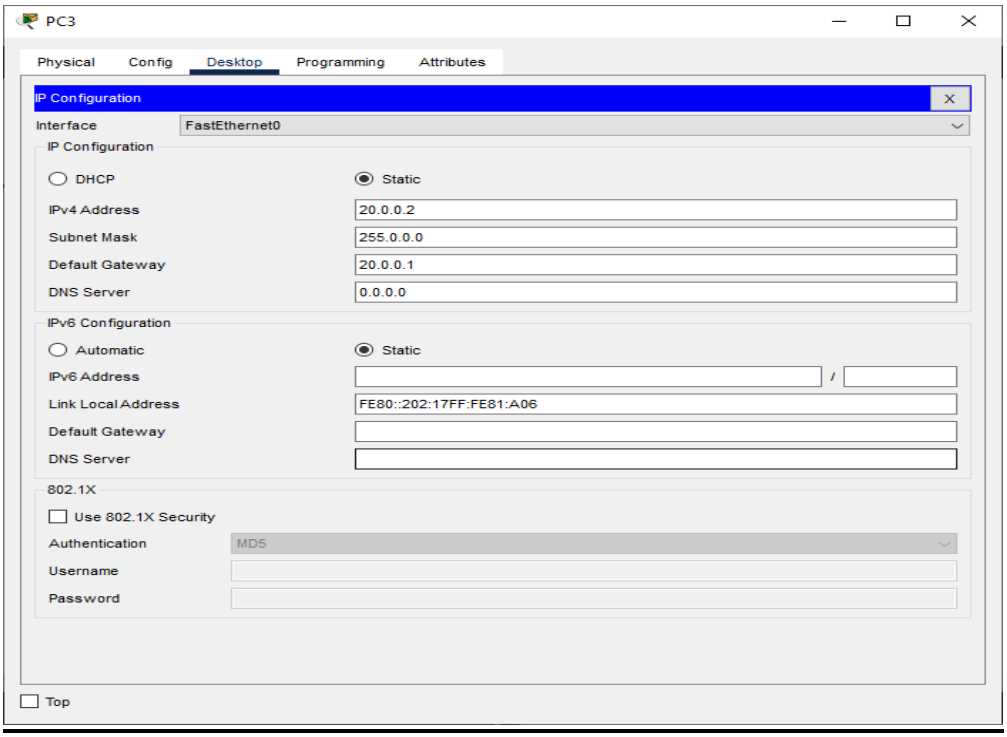
Configuring PC1:



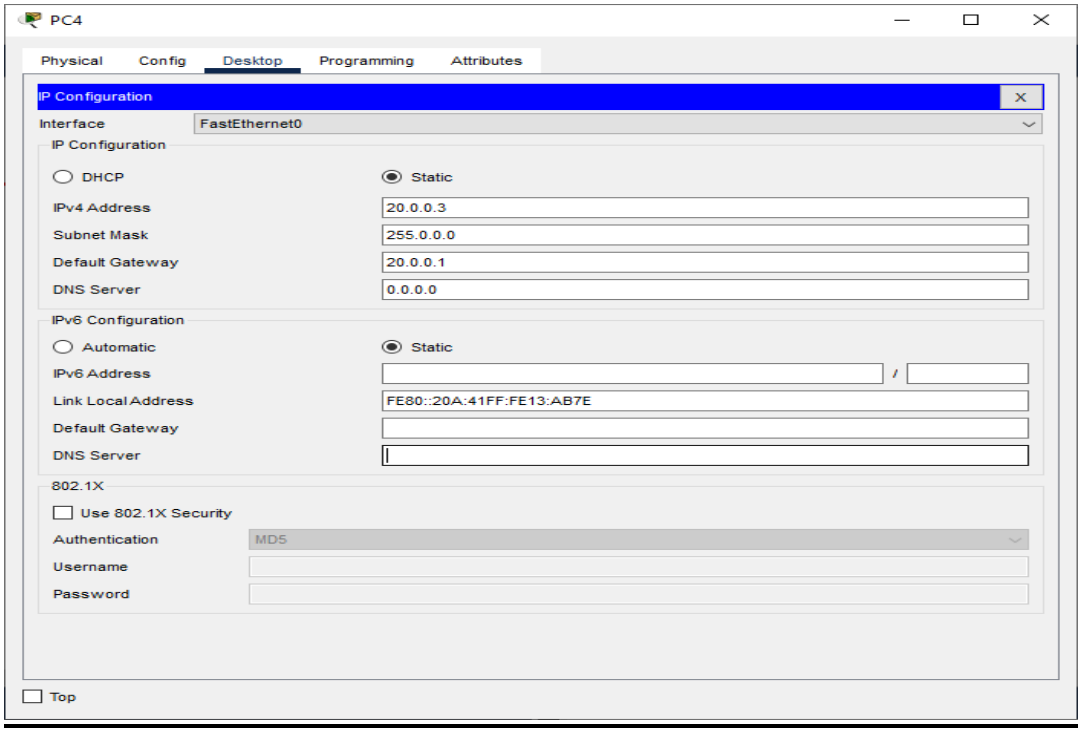
Configuring PC2:



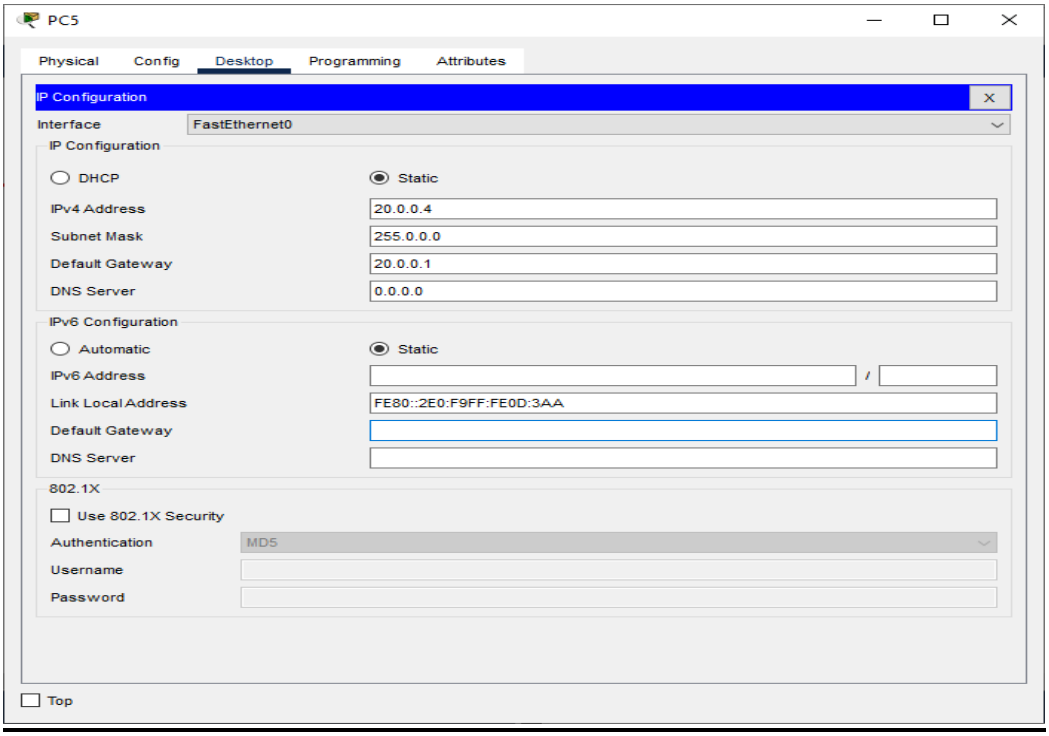
Configuring PC3:



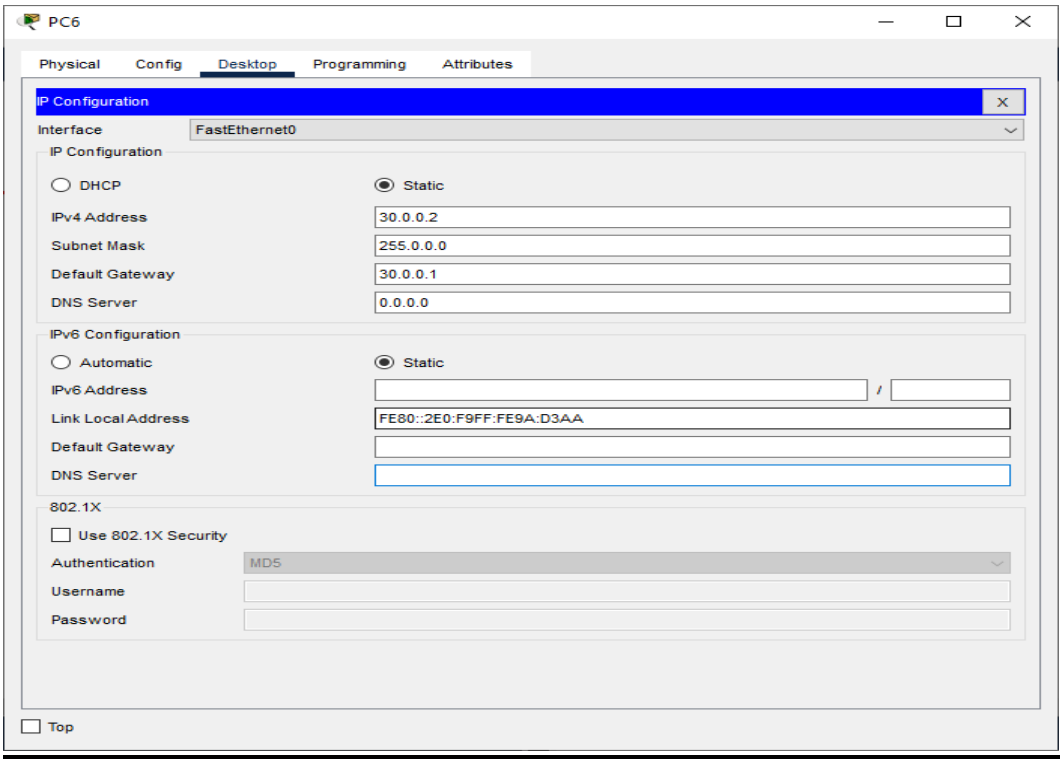
Configuring PC4:



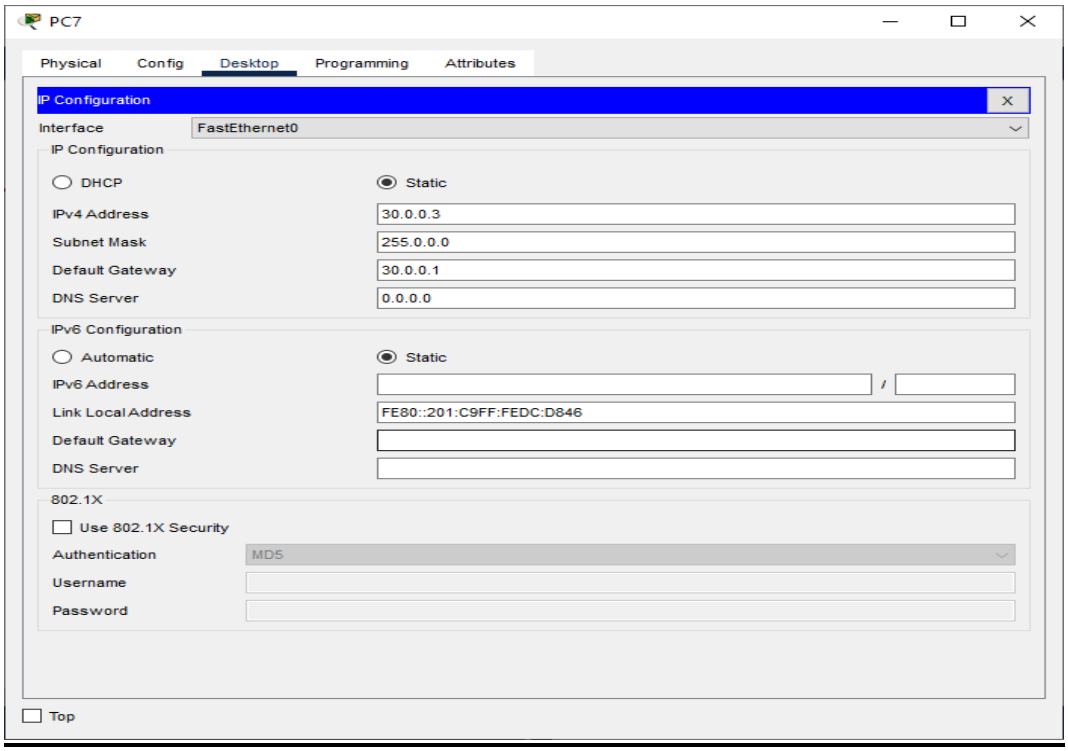
Configuring PC5:



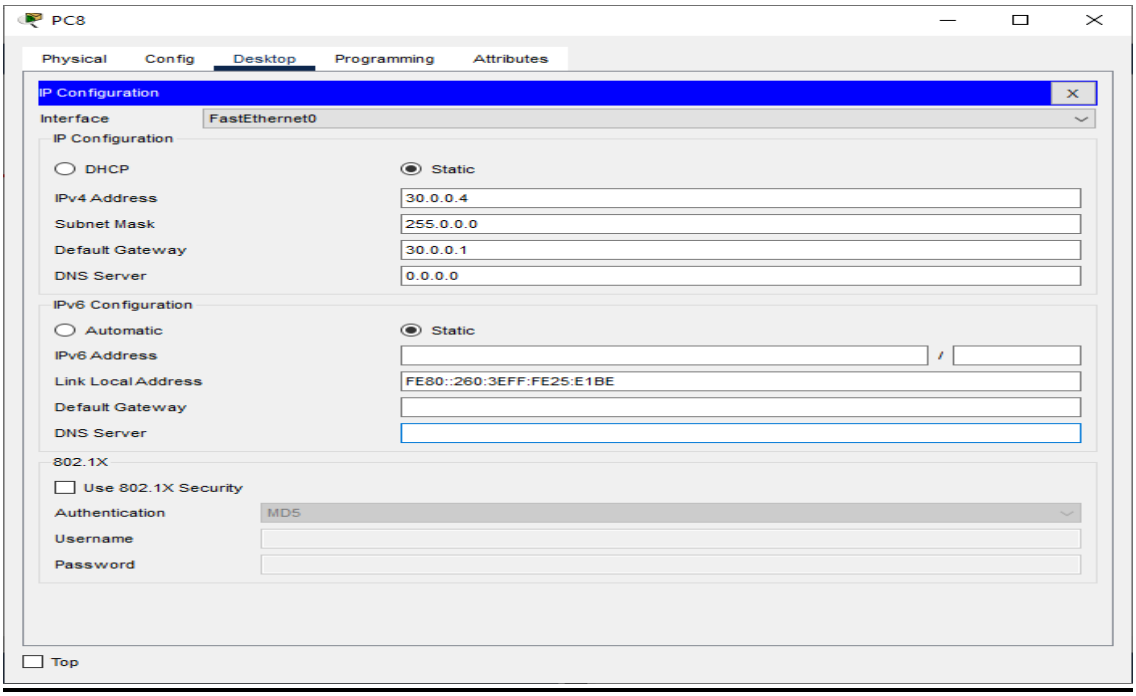
Configuring PC6:



Configuring PC7:

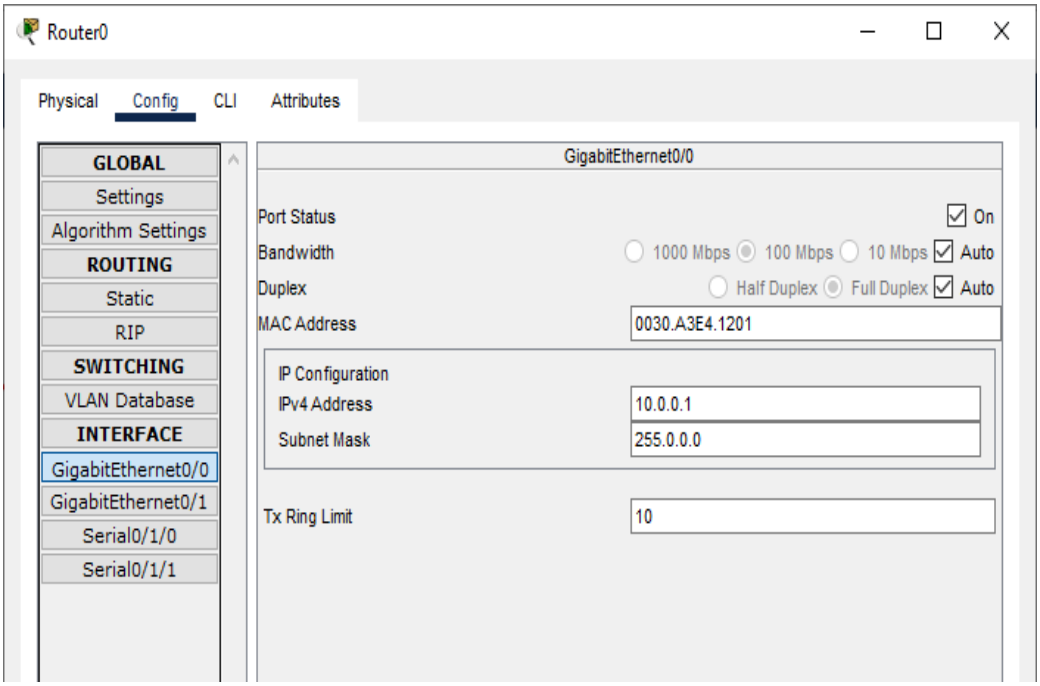


Configuring PC8:

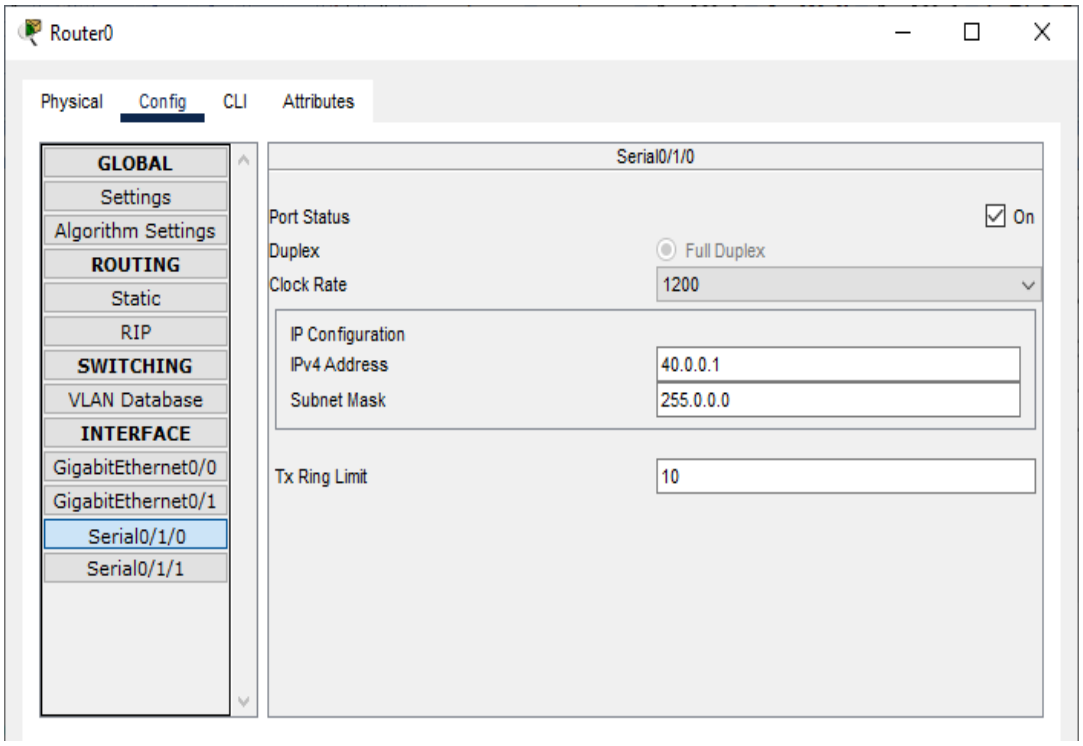


Configuring IP addresses on Router 0

i) Interface G0/0

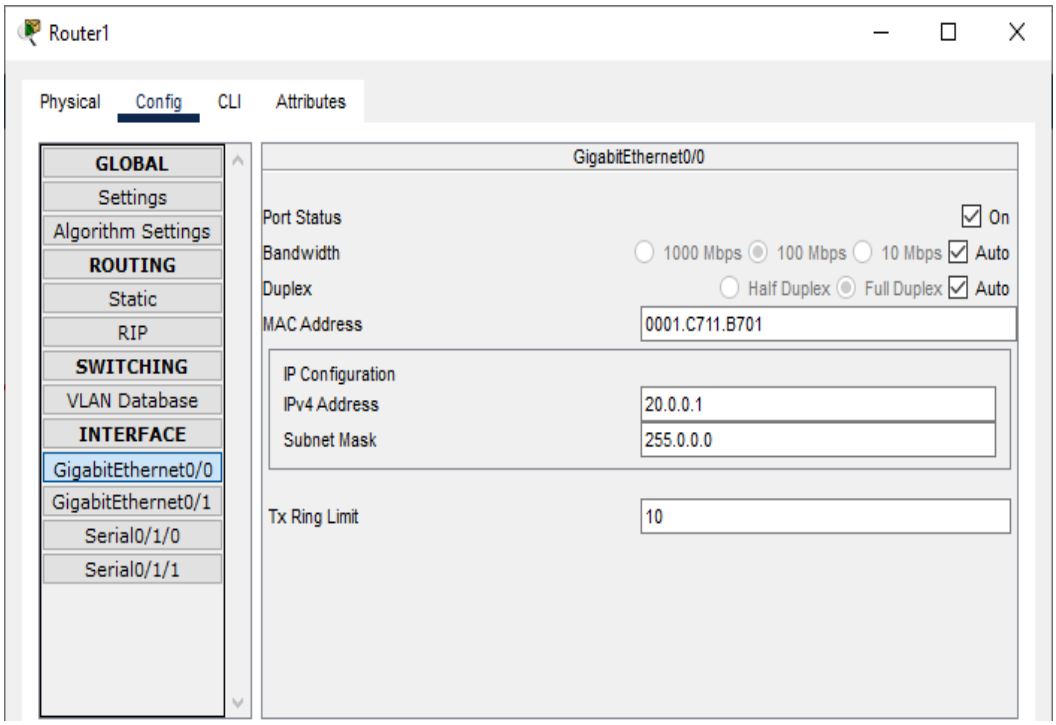


ii) Interface S0/1/0

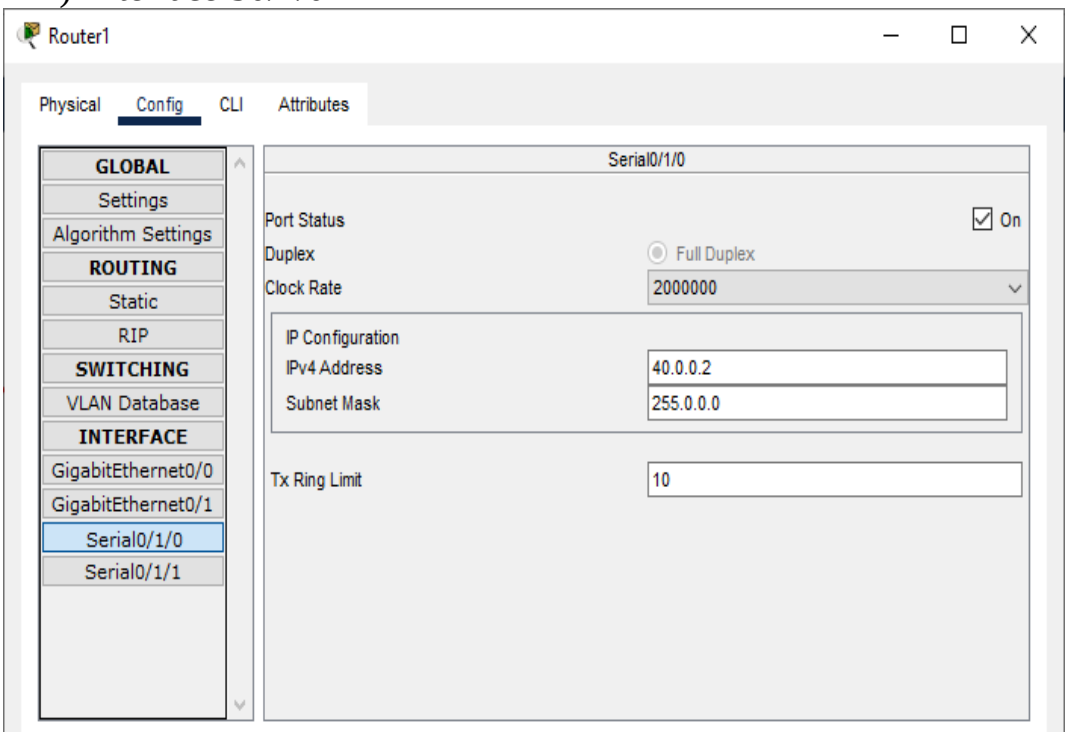


Configuring IP addresses on Router 1

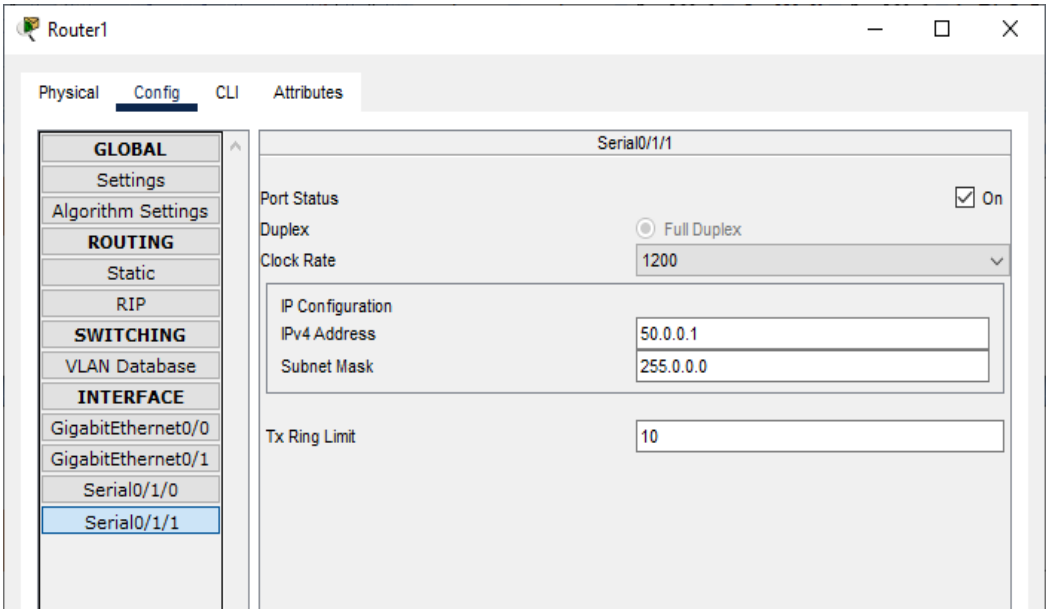
i) Interface G0/0



ii) Interface S0/1/0

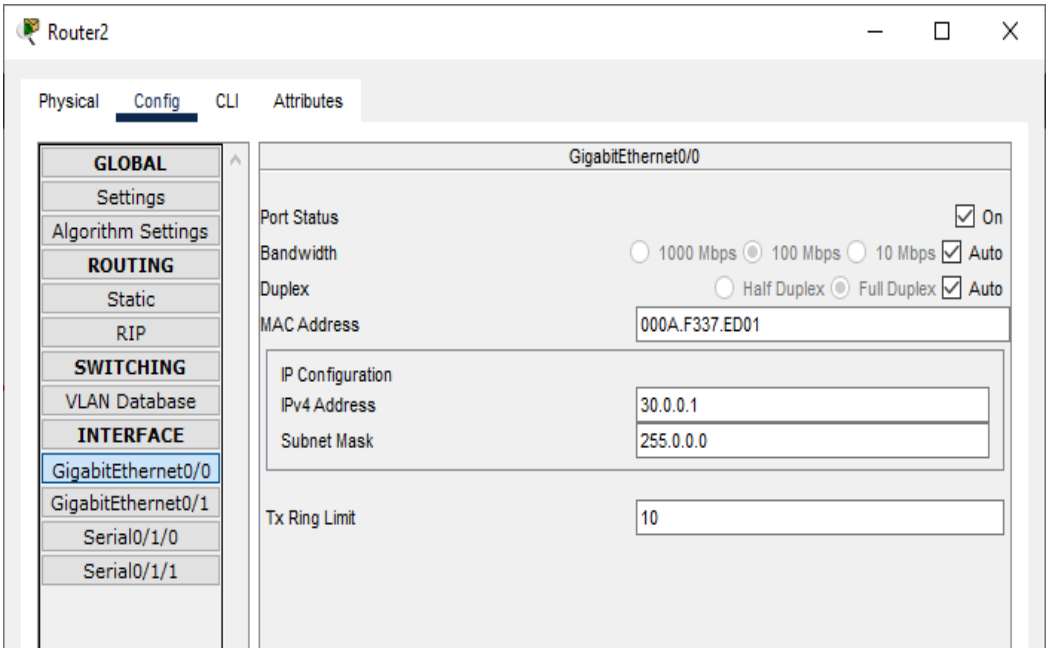


iii) Interface S0/1/1

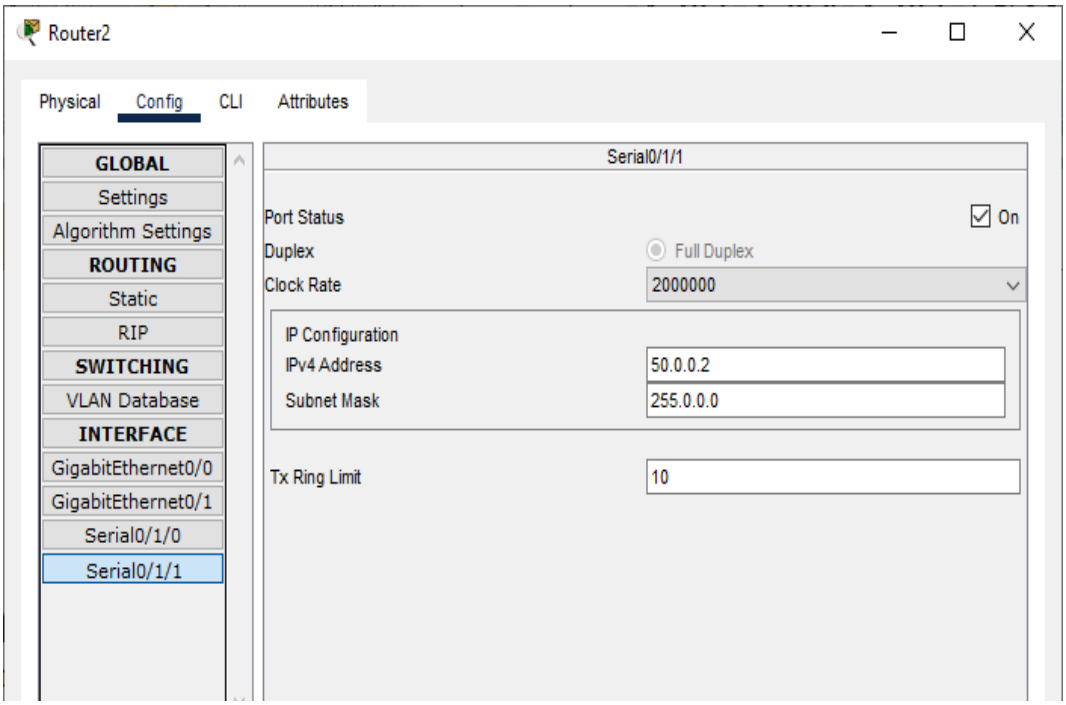


Configuring IP addresses on Router 2

i) Interface G0/0



ii) Interface S0/1/1



Configuring Router 0 for 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)

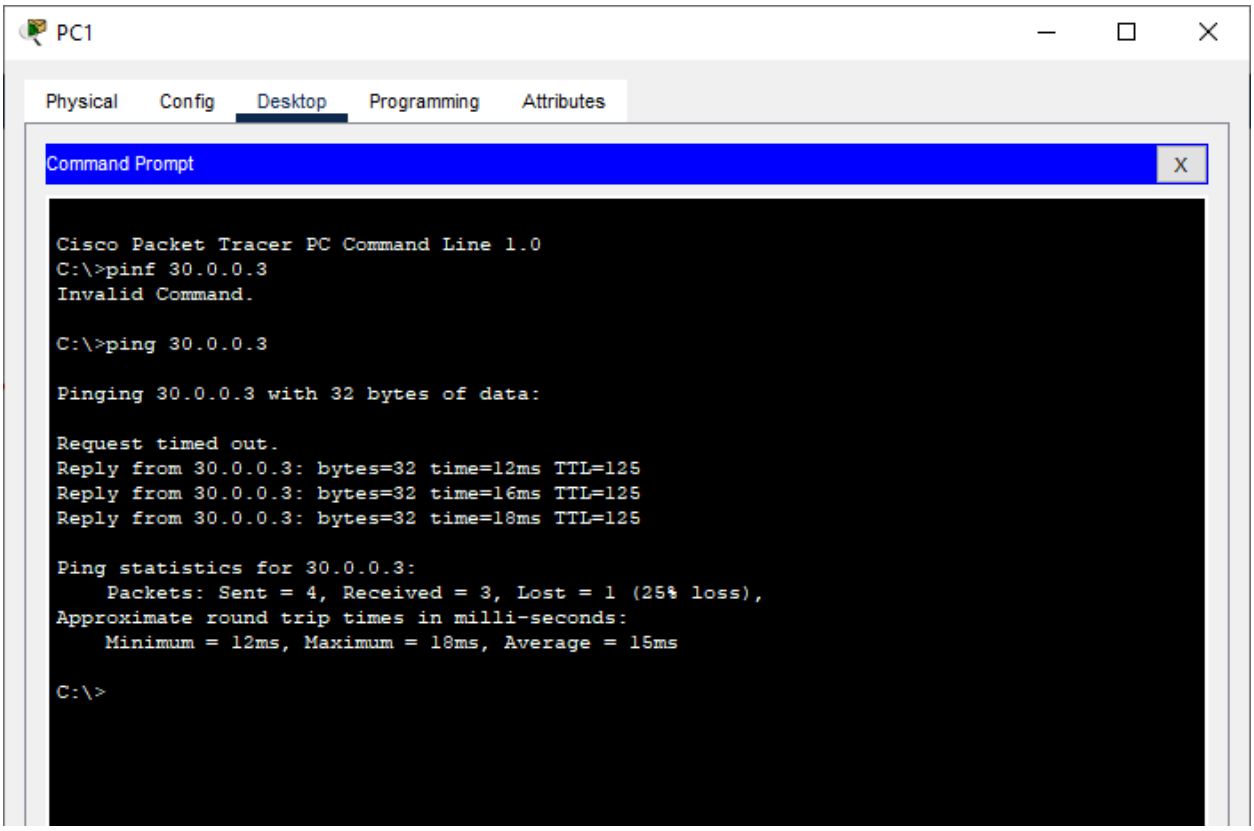
Router(config)#
Router(config)#router ospf 1
Router(config-router)#
Router(config-router)#network 20.0.0.0 0.0.0.255 area 1
Router(config-router)#network 40.0.0.0 0.0.0.255 area 1
Router(config-router)#network 50.0.0.0 0.0.0.255 area 1
Router(config-router)#exit
Router(config)#

Configuring Router 2 for OSPF (using the CLI mode)

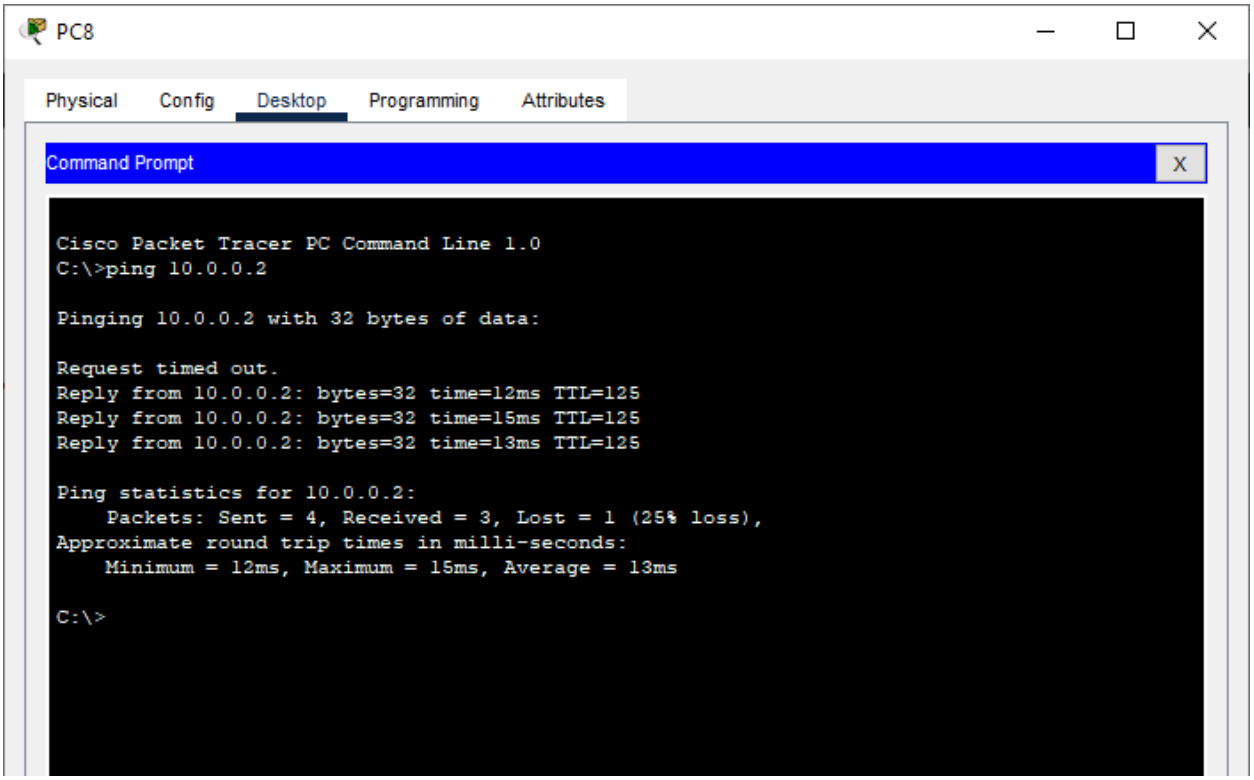
```
Router(config)#
Router(config)#router ospf 1
Router(config-router)#
Router(config-router)#network 30.0.0.0 0.0.0.255 area 1
Router(config-router)#network 50.0.0.0 0.0.0.255 area 1
Router(config-router)# exit
Router(config)#
```

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

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

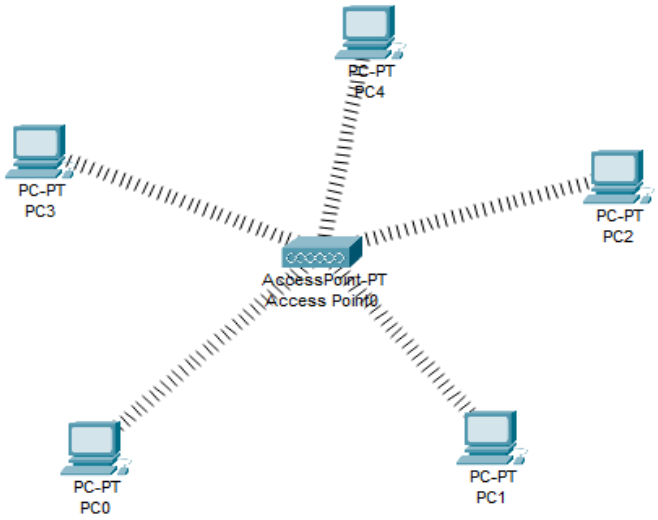
Disadvantages of Wireless Access Point (WAP):

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

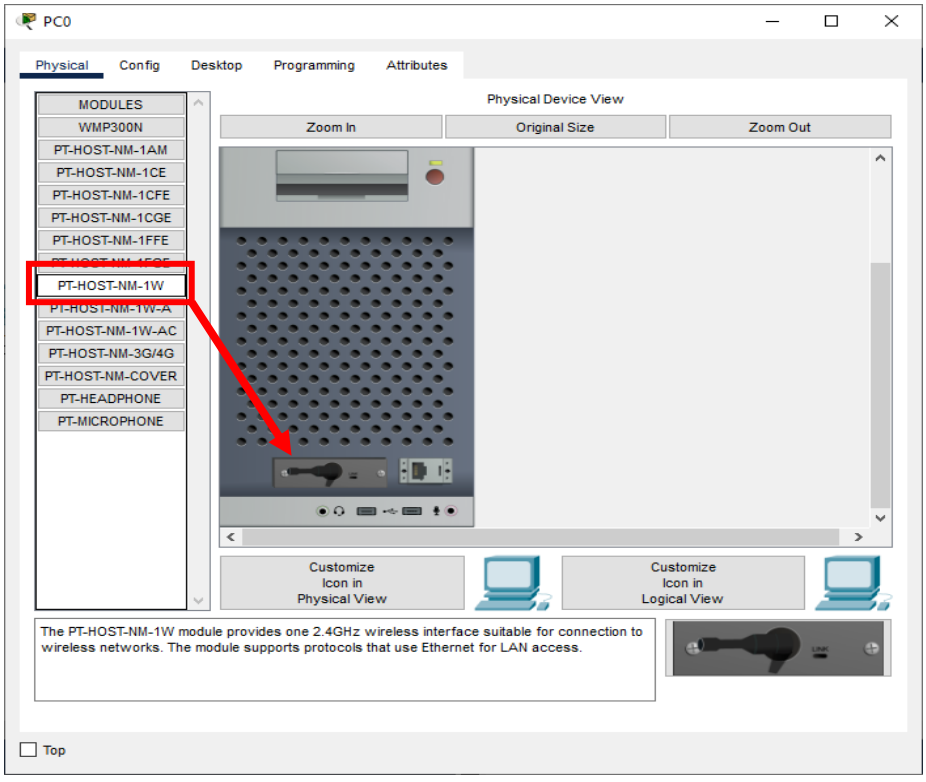
Application of Wireless Access Point:

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)

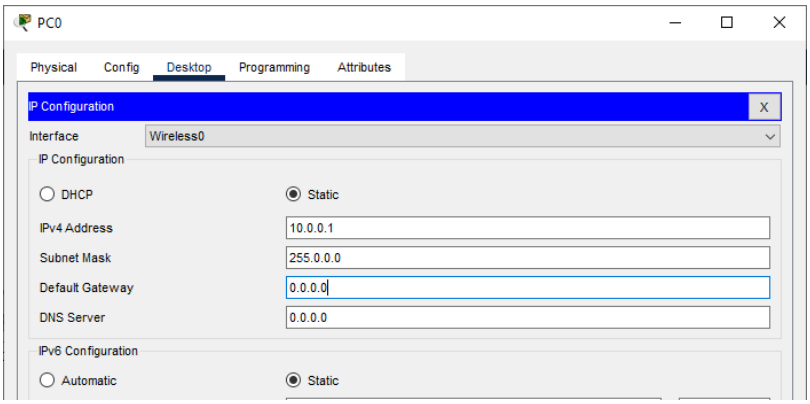


Add a Wireless interface to each PC as follows

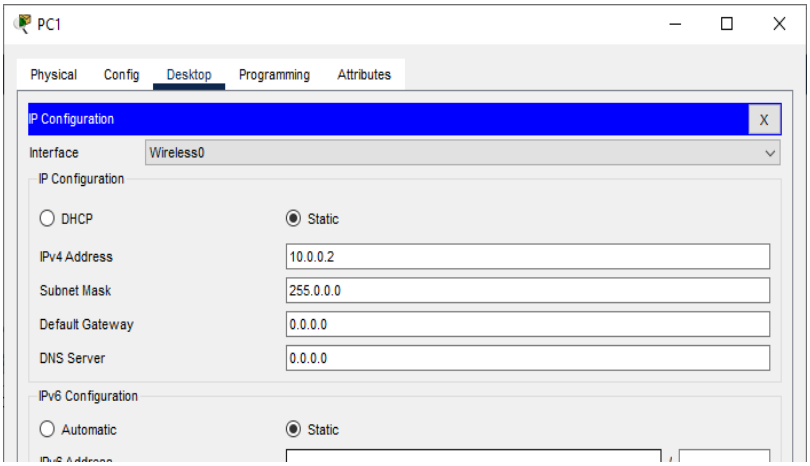


Assigning IP Address to each PC (select Static)

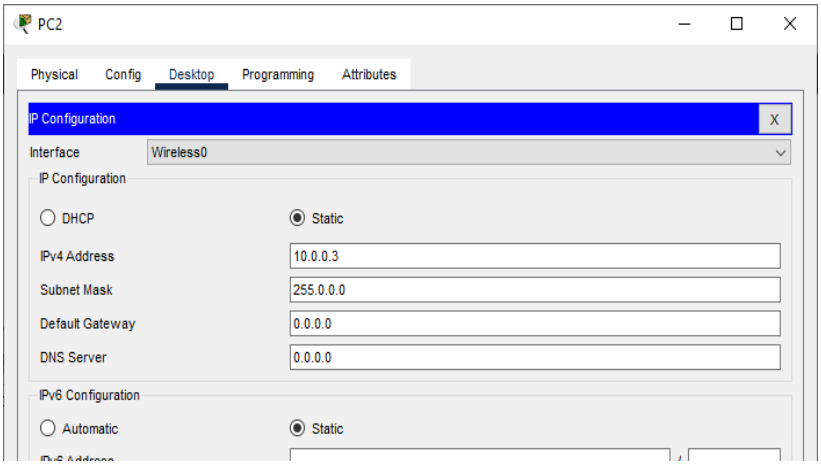
1) PC0 :



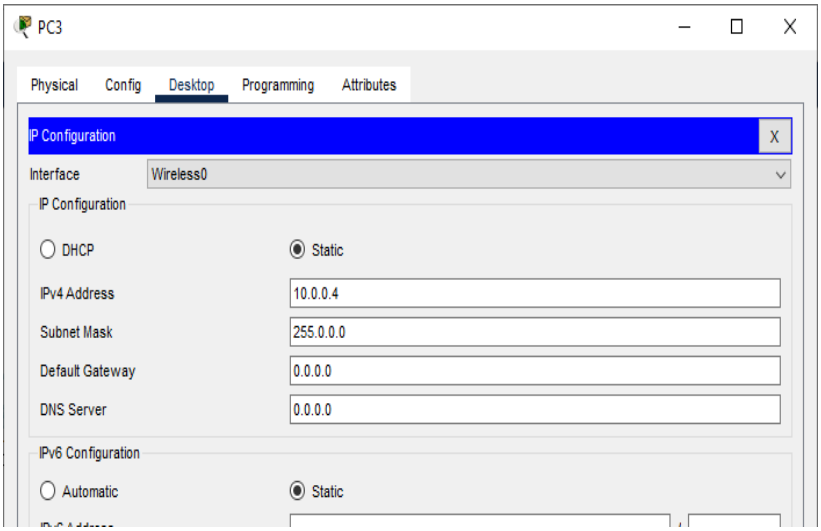
2) PC1 :



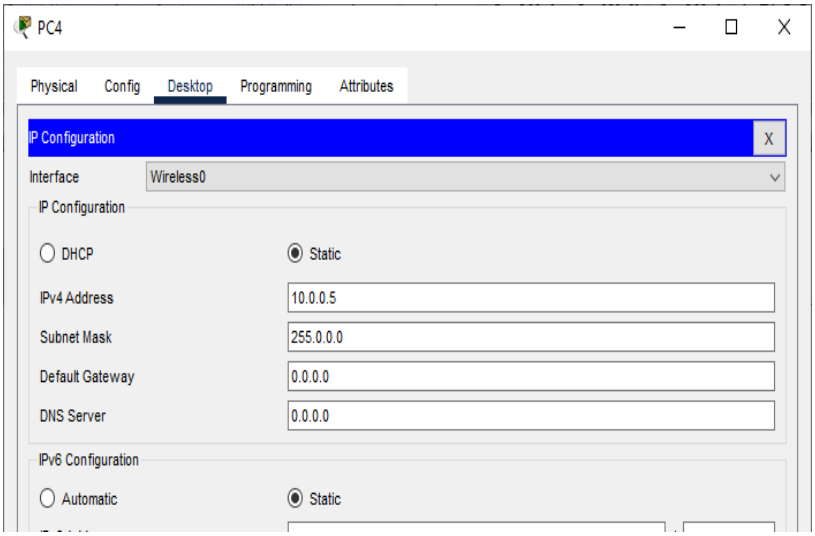
3) PC2 :



4) PC3 :



5) PC4 :

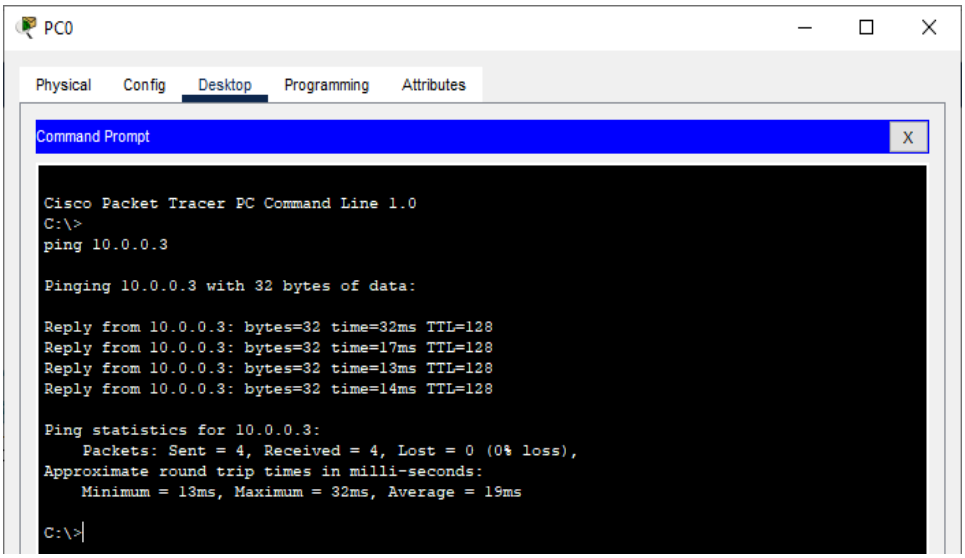


The IP addresses assigned are

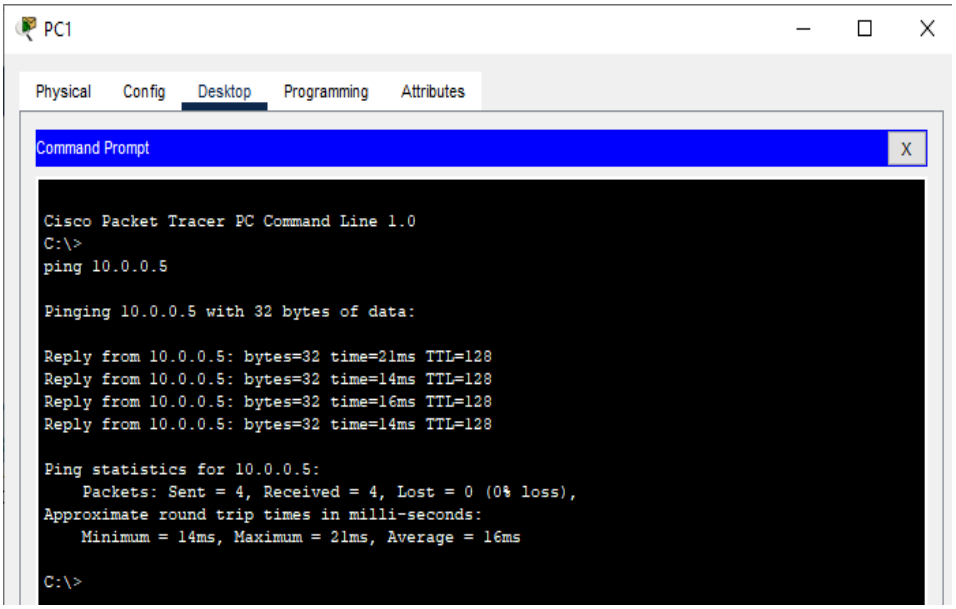
Host	IP address
PC0	10.0.0.1
PC1	10.0.0.2
PC2	10.0.0.3
PC3	10.0.0.4
PC4	10.0.0.5

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)



For the video demonstration of the given practical click on the following link:

https://youtu.be/c91hCh01DCA