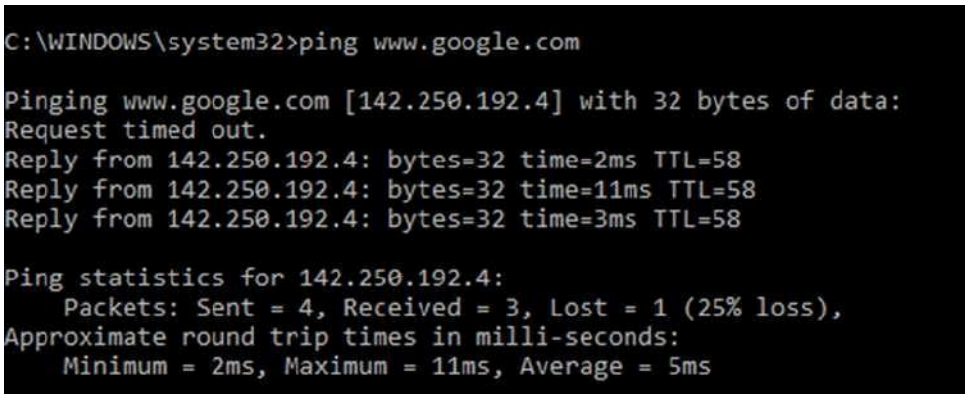
Practical No.1

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.

PROGRAM:

1. **ping:** ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol 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.

```
C:\WINDOWS\system32>traceroute www.toolsvilla.com
'traceroute' is not recognized as an internal or external command,
operable program or batch file.

C:\WINDOWS\system32>tracert www.toolsvilla.com

Tracing route to www.toolsvilla.com [172.66.43.34]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.128.0.2
  2     3 ms     *        5 ms  static-17.218.143.114-tataidc.co.in [114.143.218.17]
  3     2 ms     2 ms    30 ms  10.124.253.101
  4     *        *        *     Request timed out.
  5     2 ms     2 ms     *     115.113.165.21.static-mumbai.vsnl.net.in [115.113.165.21]
  6     3 ms     2 ms     3 ms  172.28.176.217
  7     3 ms     *        3 ms  172.28.177.190
  8     4 ms     4 ms     4 ms  121.240.241.246
  9     6 ms    11 ms    35 ms  172.71.196.4
 10     *        3 ms     5 ms  172.66.43.34

Trace complete.
```

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:

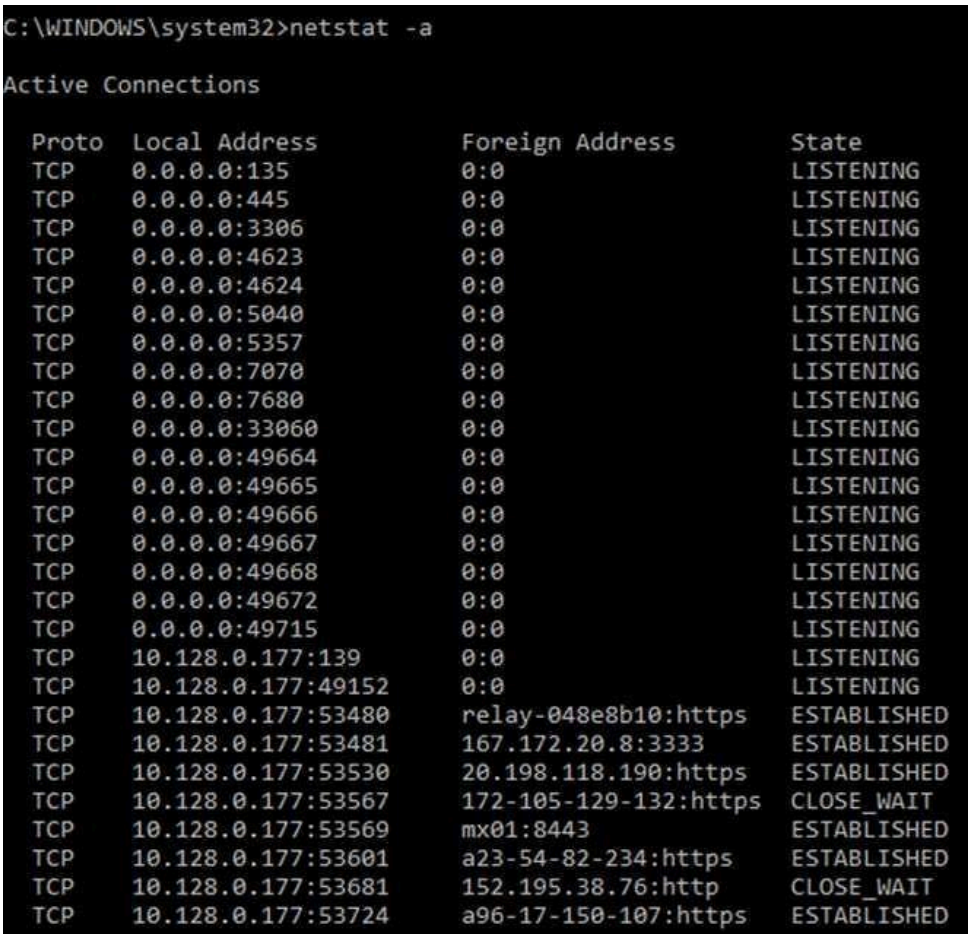
(i) **netstat-in command**

This netstat function shows the state of all configured interfaces.

```
C:\WINDOWS\system32>netstat -in

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

  -a            Displays all connections and listening ports.
  -b            Displays the executable involved in creating each connection or
                listening port. In some cases well-known executables host
                multiple independent components, and in these cases the
                sequence of components involved in creating the connection
                or listening port is displayed. In this case the executable
                name is in [] at the bottom, on top is the component it called,
                and so forth until TCP/IP was reached. Note that this option
                can be time-consuming and will fail unless you have sufficient
                permissions.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -f            Displays Fully Qualified Domain Names (FQDN) for foreign
                addresses.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -q            Displays all connections, listening ports, and bound
                nonlistening TCP ports. Bound nonlistening ports may or may not
                be associated with an active connection.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  -t            Displays the current connection offload state.
  -x            Displays NetworkDirect connections, listeners, and shared
                endpoints.
  -y            Displays the TCP connection template for all connections.
                Cannot be combined with the other options.
```

(ii) **netstat-a command**

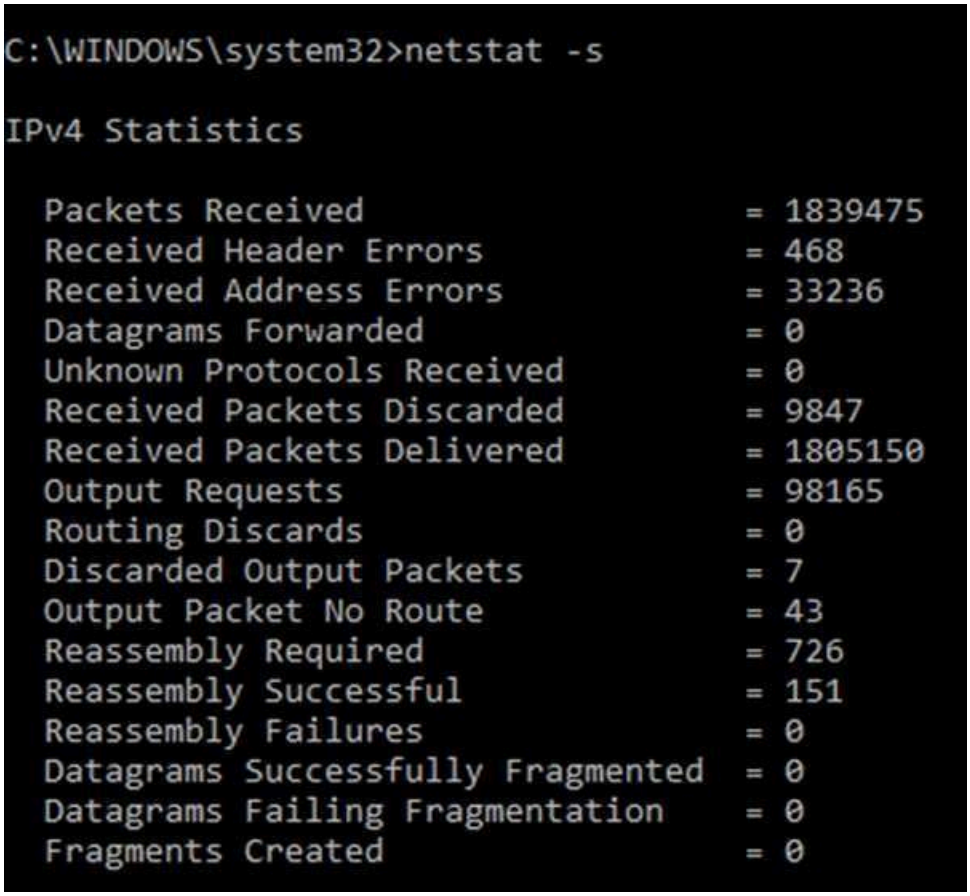
The netstat-a command shows the state of all sockets.



```
C:\WINDOWS\system32>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0:0                    LISTENING
  TCP    0.0.0.0:445            0:0                    LISTENING
  TCP    0.0.0.0:3306           0:0                    LISTENING
  TCP    0.0.0.0:4623           0:0                    LISTENING
  TCP    0.0.0.0:4624           0:0                    LISTENING
  TCP    0.0.0.0:5040           0:0                    LISTENING
  TCP    0.0.0.0:5357           0:0                    LISTENING
  TCP    0.0.0.0:7070           0:0                    LISTENING
  TCP    0.0.0.0:7680           0:0                    LISTENING
  TCP    0.0.0.0:33060          0:0                    LISTENING
  TCP    0.0.0.0:49664          0:0                    LISTENING
  TCP    0.0.0.0:49665          0:0                    LISTENING
  TCP    0.0.0.0:49666          0:0                    LISTENING
  TCP    0.0.0.0:49667          0:0                    LISTENING
  TCP    0.0.0.0:49668          0:0                    LISTENING
  TCP    0.0.0.0:49672          0:0                    LISTENING
  TCP    0.0.0.0:49715          0:0                    LISTENING
  TCP    10.128.0.177:139       0:0                    LISTENING
  TCP    10.128.0.177:49152     0:0                    LISTENING
  TCP    10.128.0.177:53480     relay-048e8b10:https   ESTABLISHED
  TCP    10.128.0.177:53481     167.172.20.8:3333      ESTABLISHED
  TCP    10.128.0.177:53530     20.198.118.190:https   ESTABLISHED
  TCP    10.128.0.177:53567     172-105-129-132:https  CLOSE_WAIT
  TCP    10.128.0.177:53569     mx01:8443              ESTABLISHED
  TCP    10.128.0.177:53601     a23-54-82-234:https    ESTABLISHED
  TCP    10.128.0.177:53681     152.195.38.76:http     CLOSE_WAIT
  TCP    10.128.0.177:53724     a96-17-150-107:https   ESTABLISHED
```

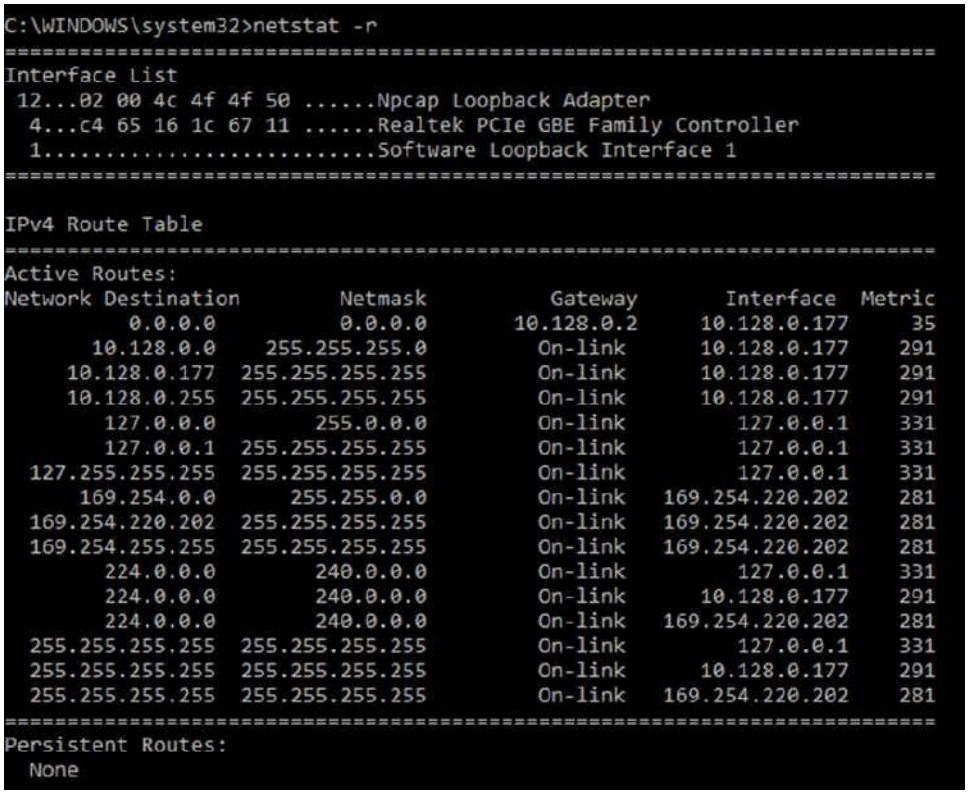
(iii) **netstat-s**

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).

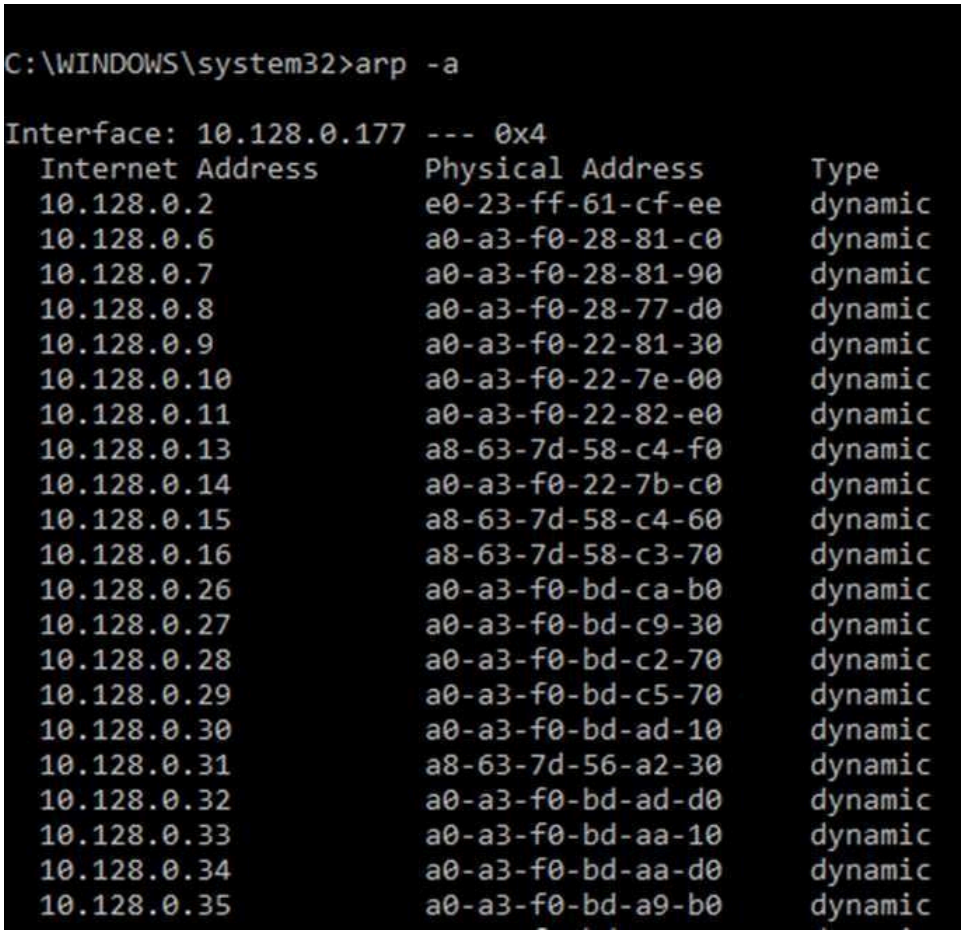


```
C:\WINDOWS\system32>netstat -r
===========================================================================
Interface List
 12...02 00 4c 4f 4f 50 ......Npcap Loopback Adapter
  4...c4 65 16 1c 67 11 ......Realtek PCIe GBE Family Controller
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      10.128.0.2     10.128.0.177     35
       10.128.0.0    255.255.255.0         On-link      10.128.0.177    291
     10.128.0.177  255.255.255.255         On-link      10.128.0.177    291
     10.128.0.255  255.255.255.255         On-link      10.128.0.177    291
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      169.254.0.0      255.255.0.0         On-link   169.254.220.202    281
  169.254.220.202  255.255.255.255         On-link   169.254.220.202    281
  169.254.255.255  255.255.255.255         On-link   169.254.220.202    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      10.128.0.177    291
        224.0.0.0        240.0.0.0         On-link   169.254.220.202    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      10.128.0.177    291
  255.255.255.255  255.255.255.255         On-link   169.254.220.202    281
===========================================================================
Persistent Routes:
  None
```

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

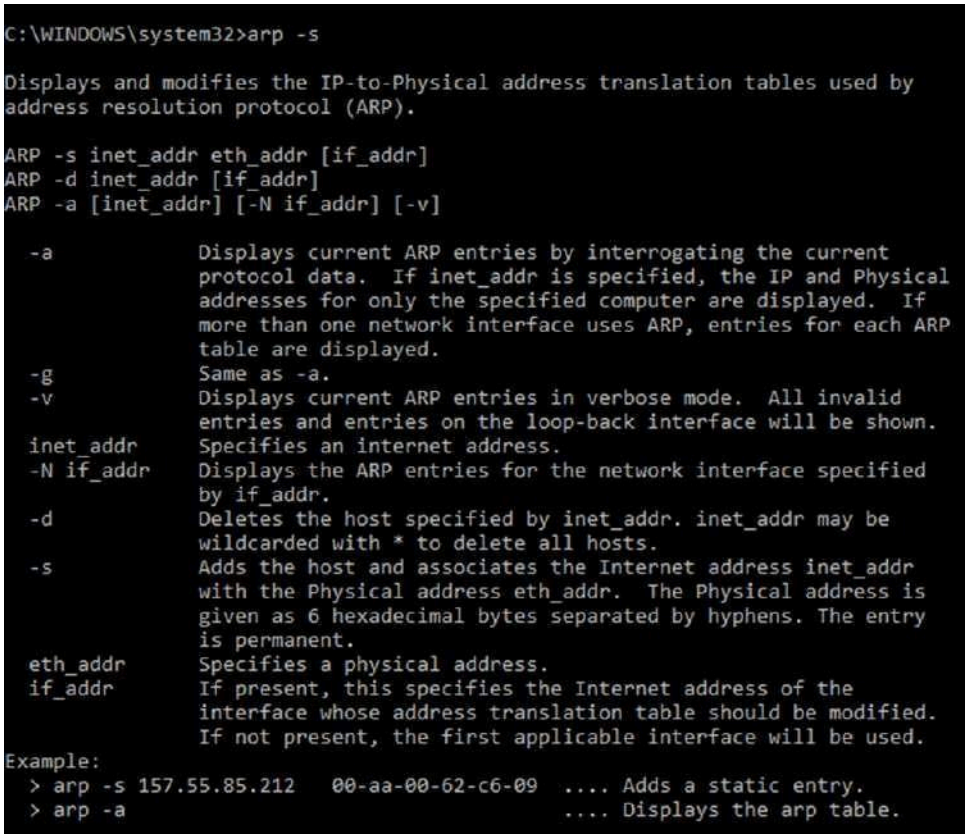
(i) arp-a: This command is used to display the ARP table for a particular It also shows all the entries of the ARP cache or table.



(ii) rap-g: Same as the arp-a

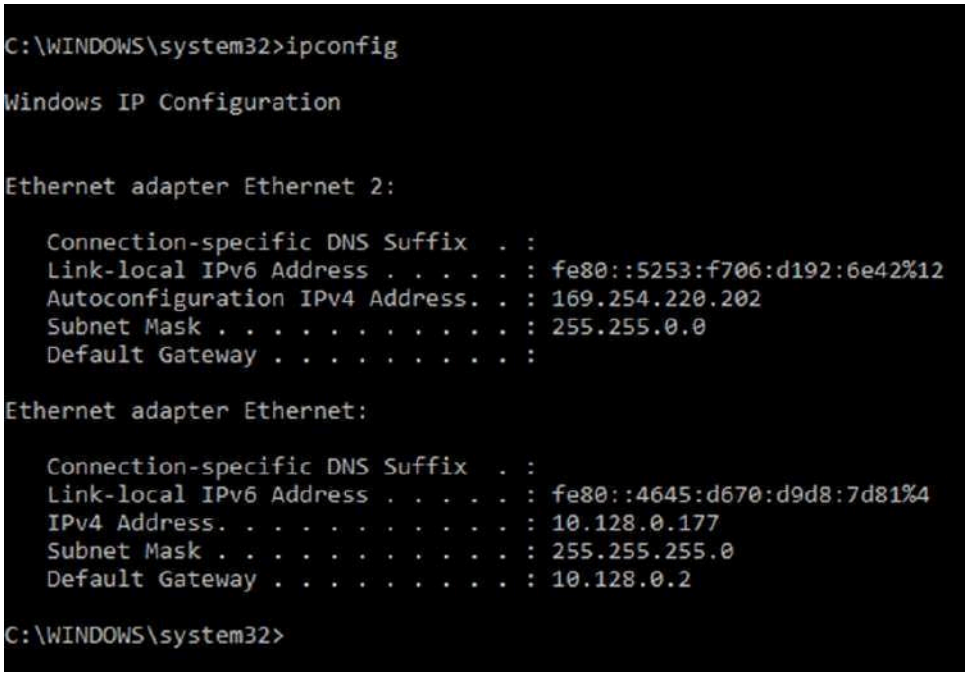
(iii) arp -d: This command is used to delete an entry from the ARP table for a particular interface. To delete an entry, write arp –d command along with the IP address in a command prompt to be

(iv) arp -s: This command is used to add the static entry in the ARP table, which resolves theInetAddr(IPaddress) to the Ether Addr (physicaladdress). To adda 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.



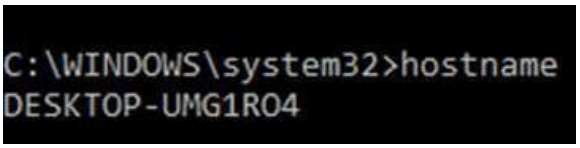
```
C:\WINDOWS\system32>arp -s

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

5. **ipconfig:** ipconfig (Internet Protocol CONFIGuration) is used to display and manage the IP address assigned to the 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.

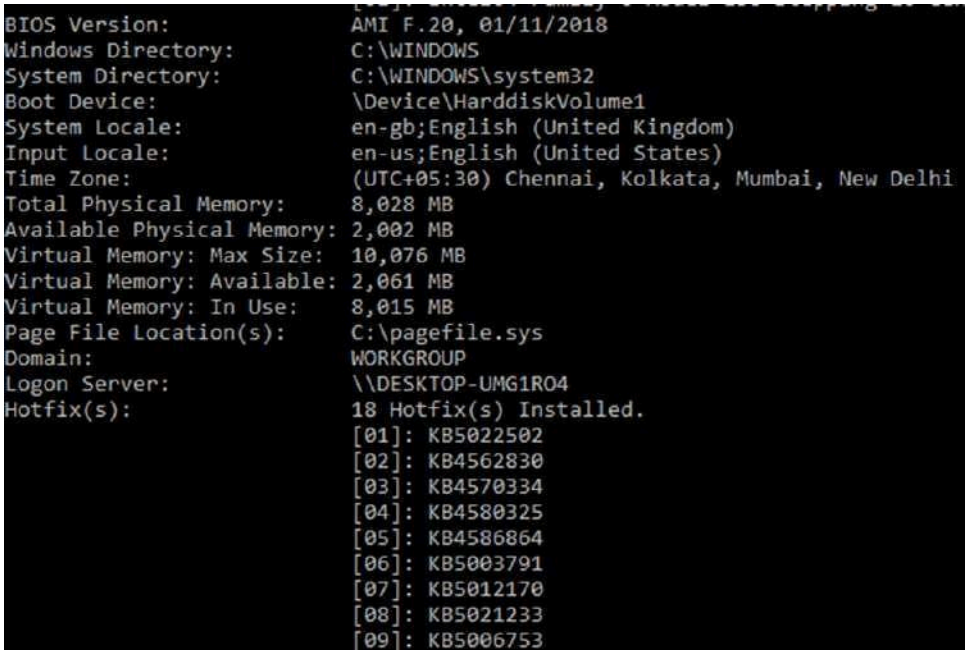
```
C:\WINDOWS\system32>nslookup
Default Server:  ns3.tataidc.co.in
Address:  103.8.45.5
```

1. **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.

```
C:\WINDOWS\system32>pathping

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
                [-p period] [-q num_queries] [-w timeout]
                [-4] [-6] target_name

Options:
    -g host-list     Loose source route along host-list.
    -h maximum_hops  Maximum number of hops to search for target.
    -i address       Use the specified source address.
    -n               Do not resolve addresses to hostnames.
    -p period        Wait period milliseconds between pings.
    -q num_queries   Number of queries per hop.
    -w timeout       Wait timeout milliseconds for each reply.
    -4               Force using IPv4.
    -6               Force using IPv6.

C:\WINDOWS\system32>_
```

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

```
C:\WINDOWS\system32>systeminfo

Host Name:                 DESKTOP-UMG1RO4
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19044 N/A Build 19044
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00331-10000-00001-AA073
Original Install Date:     25/11/2021, 12:40:36
System Boot Time:          15/01/2024, 13:34:01
System Manufacturer:       HP
System Model:              HP RCTO 280 G4 PCI MT PC
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 158 Stepping 10 GenuineIntel ~3000 Mhz
```

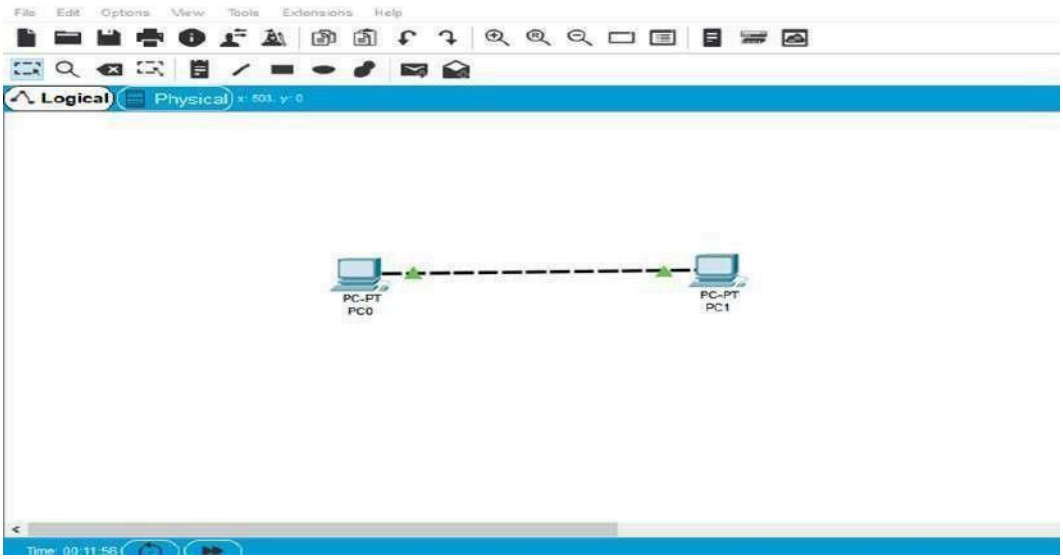


CONCLUSION: Hence we have successfully completed the practical.

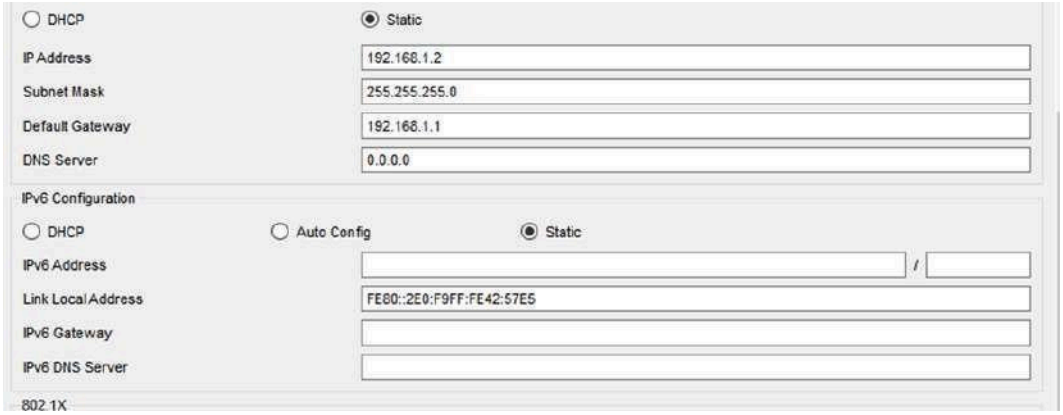
Practical No.2

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

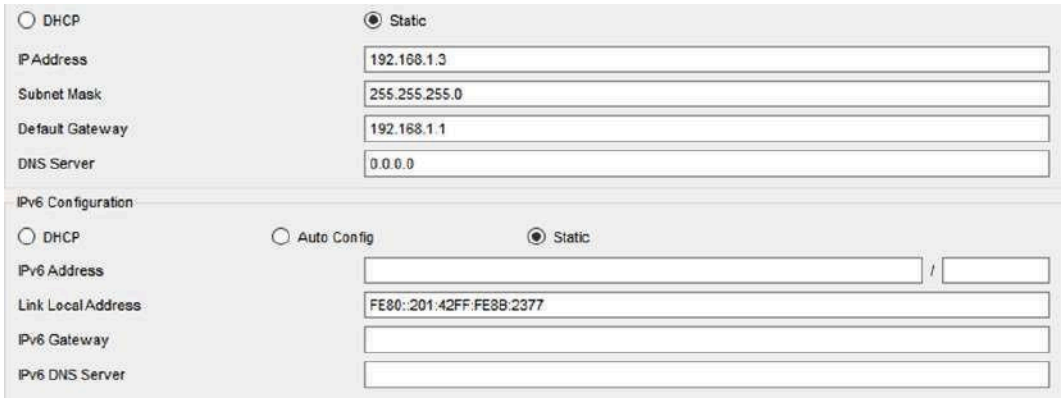
PROGRAM:



PROGRAM (1st PC IP):



PROGRAM (2nd PC IP):



OUTPUT:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=7ms TTL=128
Reply from 192.168.1.2: bytes=32 time=5ms TTL=128
Reply from 192.168.1.2: bytes=32 time=3ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 7ms, Average = 4ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Practical No.3

AIM: 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.

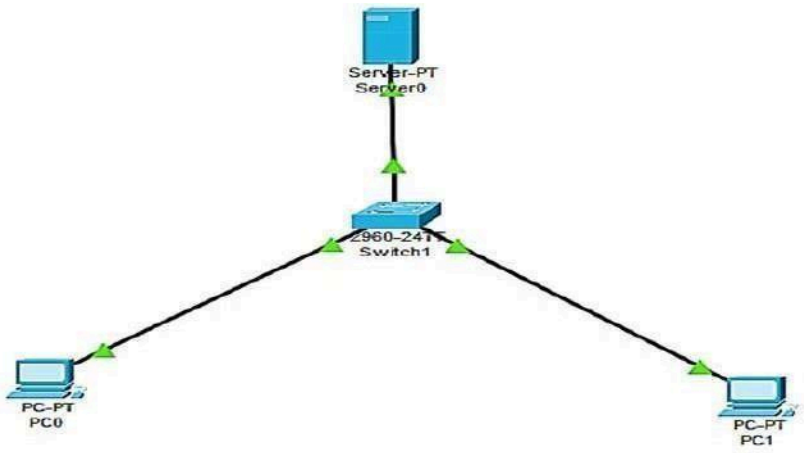
THEORY:

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.

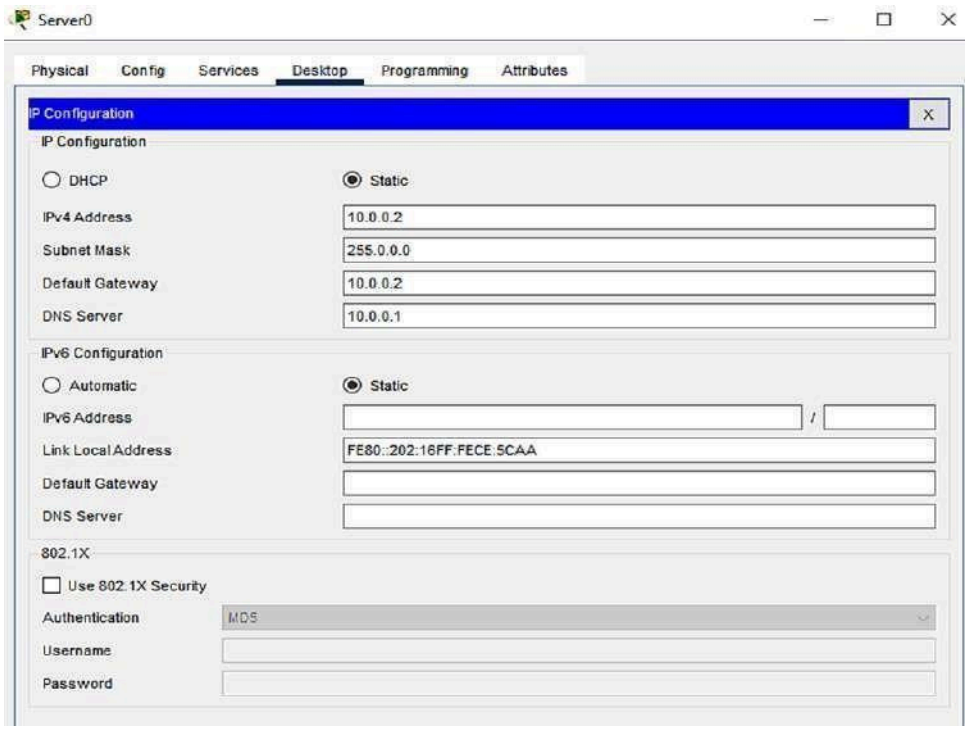
1. Reliable IP address configuration. DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.

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

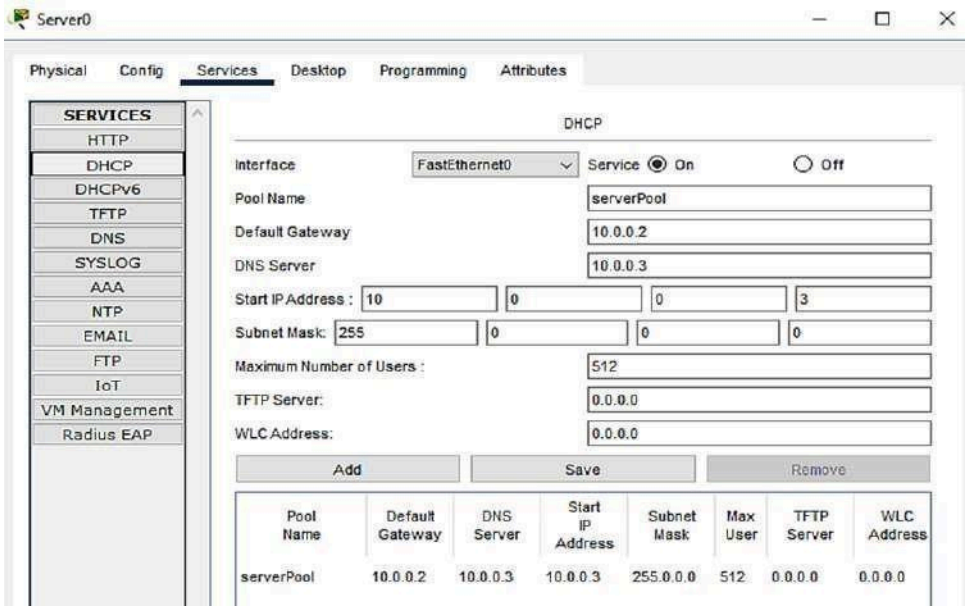
PROGRAM 1: (Make this type of diagram)



PROGRAM 2: (Now configure the Server-Pt Server 0)

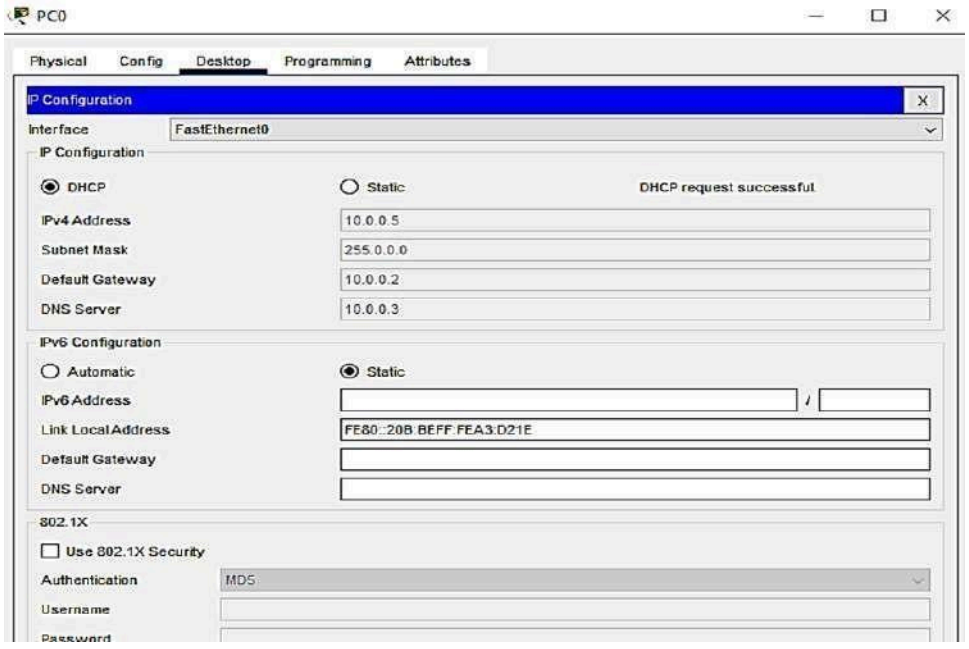


PROGRAM 3: (Now enable and set the DHCP Service on the Server)

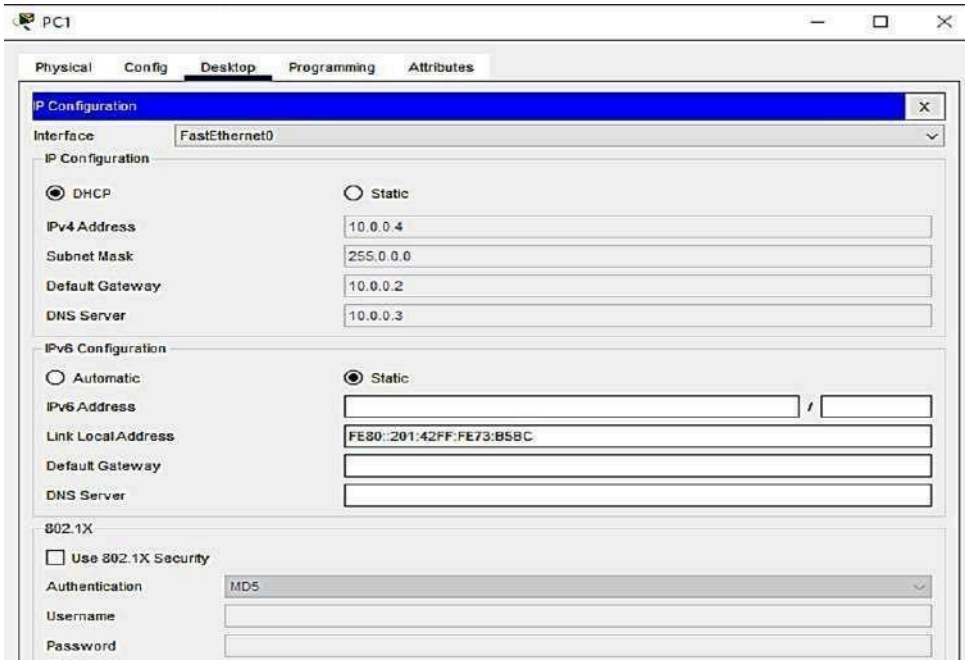


<u>PROGRAM 4:</u> (Change the IP Address on both the PC)

<u>4(A):</u> PC-PT PC 0 :It will be set on Static you have to choose the DHCP option

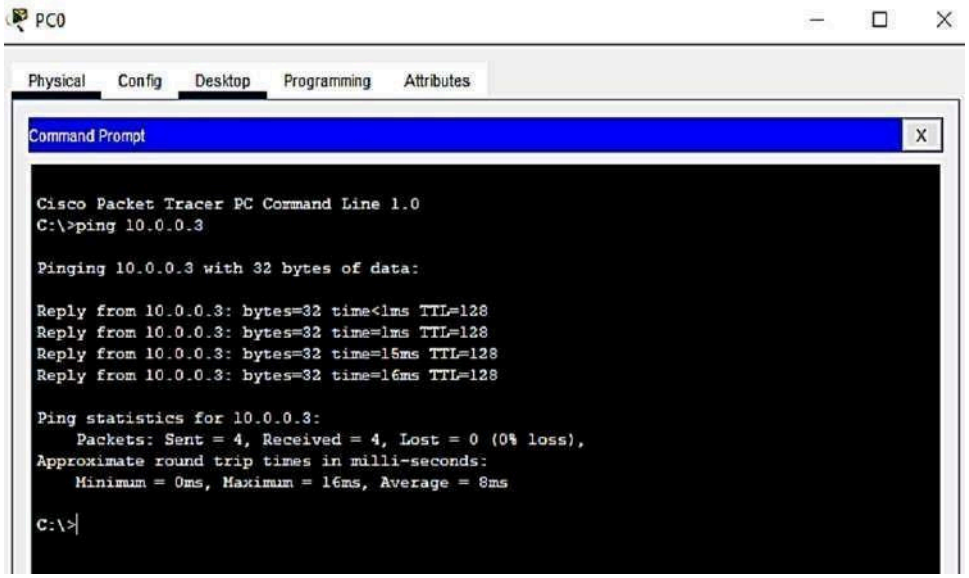


<u>4(B):</u> PC-PT PC 1 :It will be set on Static you have to choose the DHCP option

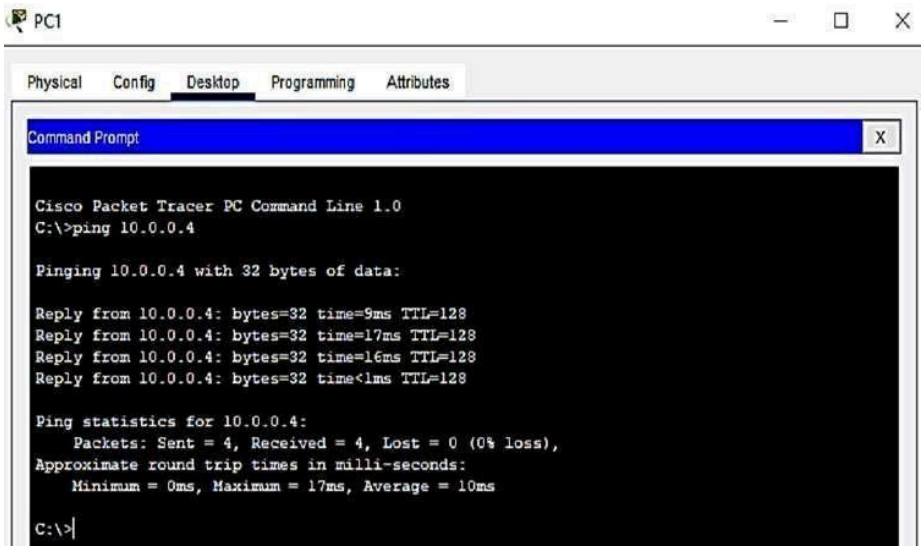


<u>PROGRAM 5:</u> (Check the connectivity)

<u>5(A):</u> PC-PT PC 0› write the command in cmd : <u>ping 10.0.0.</u>



<u>5(B):</u> PC-PT PC 1 : Write the command in cmd : <u>ping 10.0.0.4</u>


PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.4
Pinging 10.0.0.4 with 32 bytes of data:
Reply from 10.0.0.4: bytes=32 time=9ms TTL=128
Reply from 10.0.0.4: bytes=32 time=17ms TTL=128
Reply from 10.0.0.4: bytes=32 time=16ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Ping statistics for 10.0.0.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 17ms, Average = 10ms
C:\>

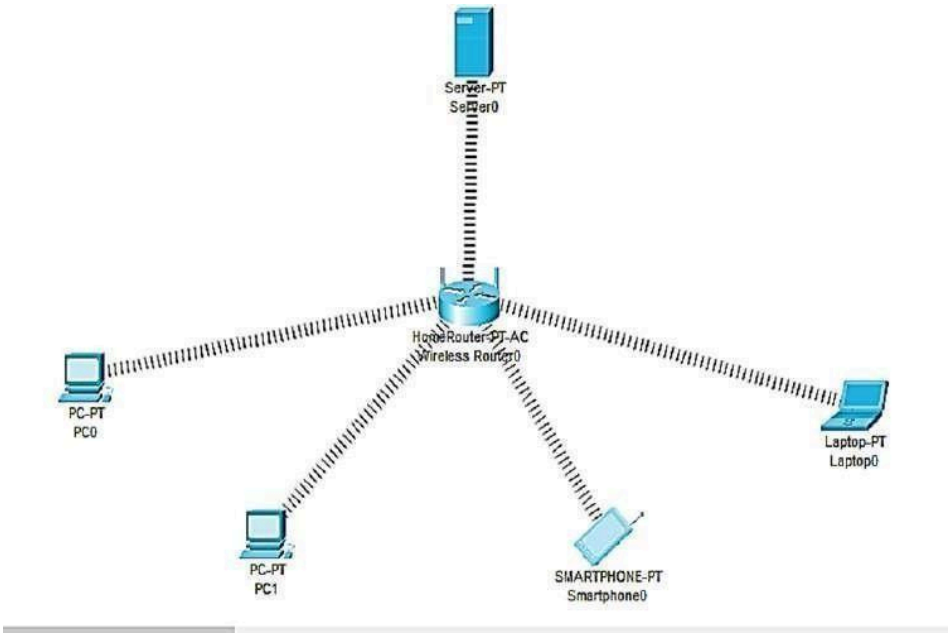
Practical No.4

AIM: Using Packet Tracer, Create a basic network of two computer's using appropriate network wire. Use Static IP Address allocation and show connectivity.

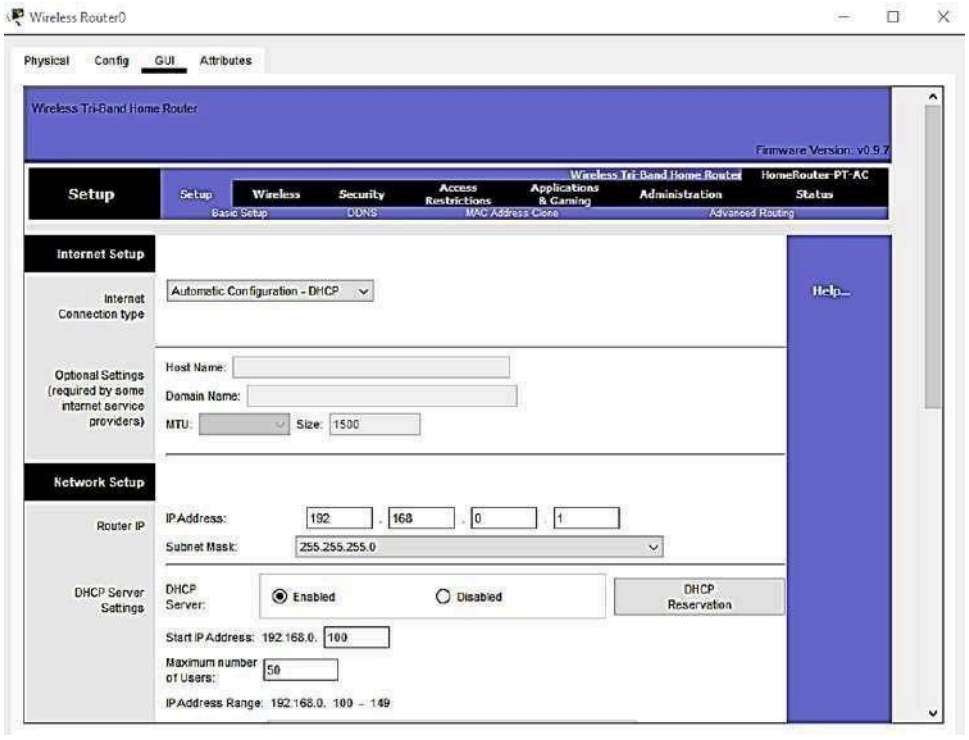
THEORY:

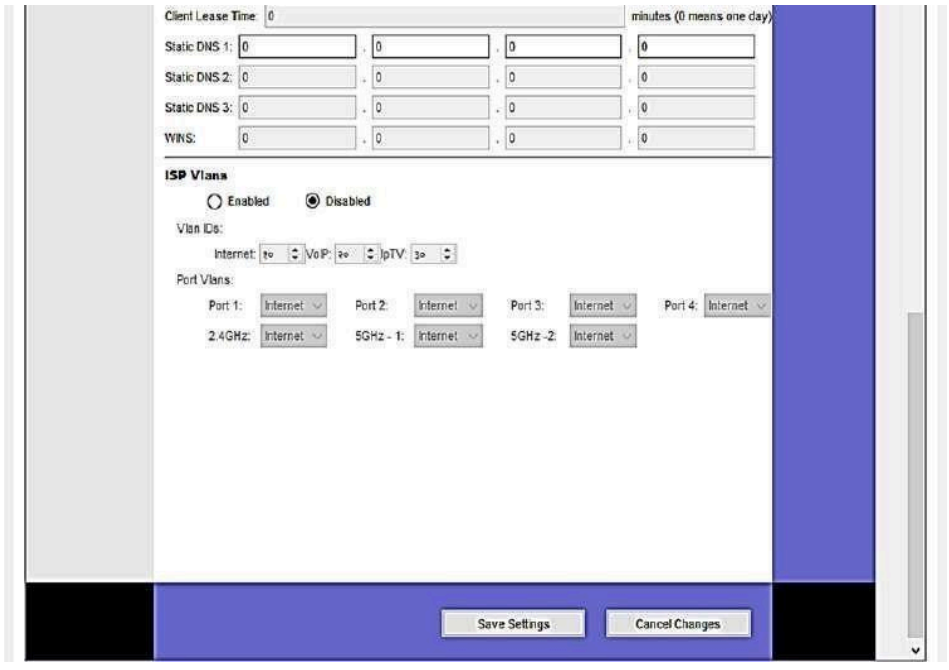
A wireless access point (WAP) is a networking device that enables wireless devices to connect to a wired network. It acts as a central hub for wireless devices, allowing them to communicate with each other and with devices on the wired network.
A wireless access point typically connects to a wired network, such as a local area network (LAN), and broadcasts a wireless signal using radio waves. Wireless devices, such as laptops, smartphones, and tablets, can connect to the WAP and access the network resources that are available on the wired network.
Wireless access points are commonly used in homes, offices, and public places such as airports and cafes to provide wireless connectivity to users. They can be stand alone devices or built into other networking equipment such as routers or switches.

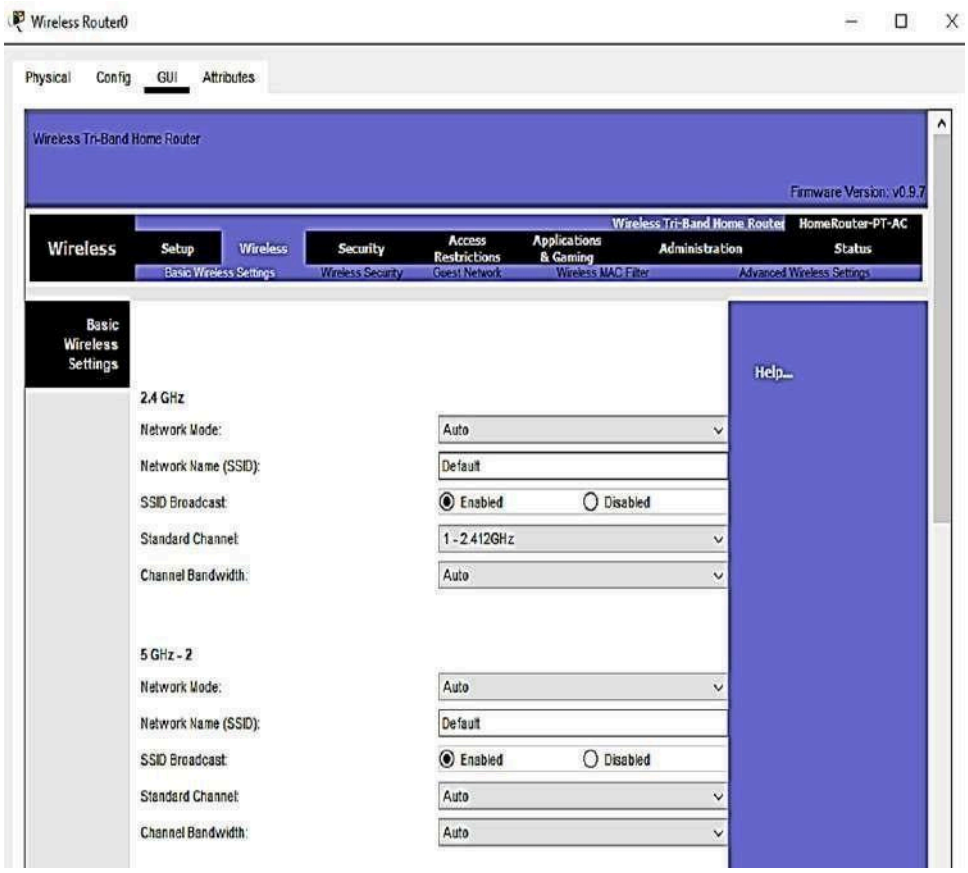
PROGRAM 1: (**This the the following toplolgy**)

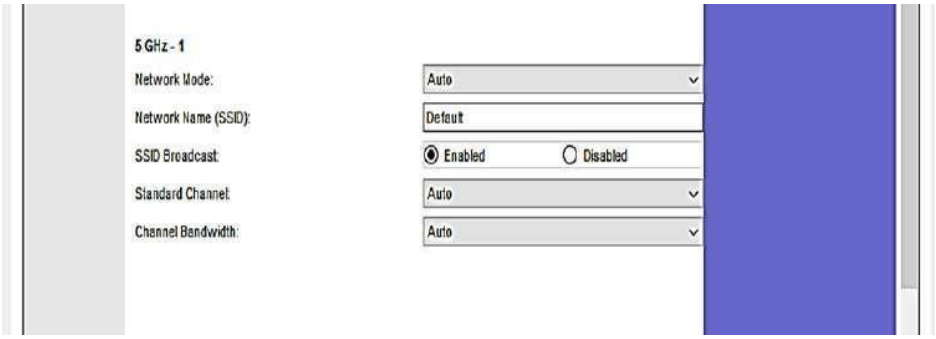


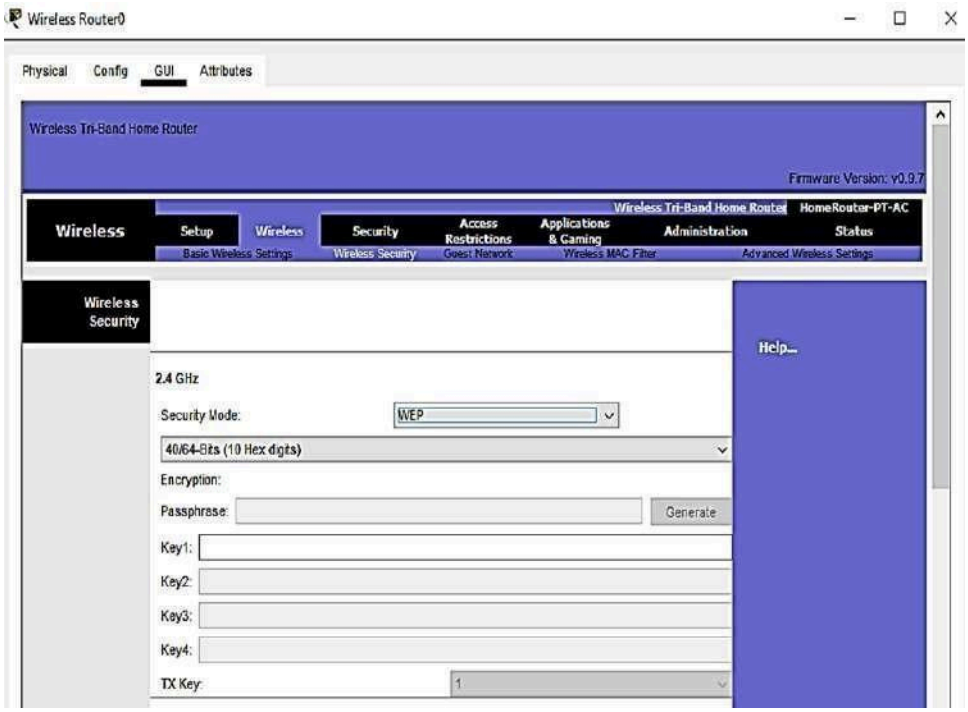
PROGRAM 2: (**HomeRouter PT-AC Wireless Router 0 : follow given**)



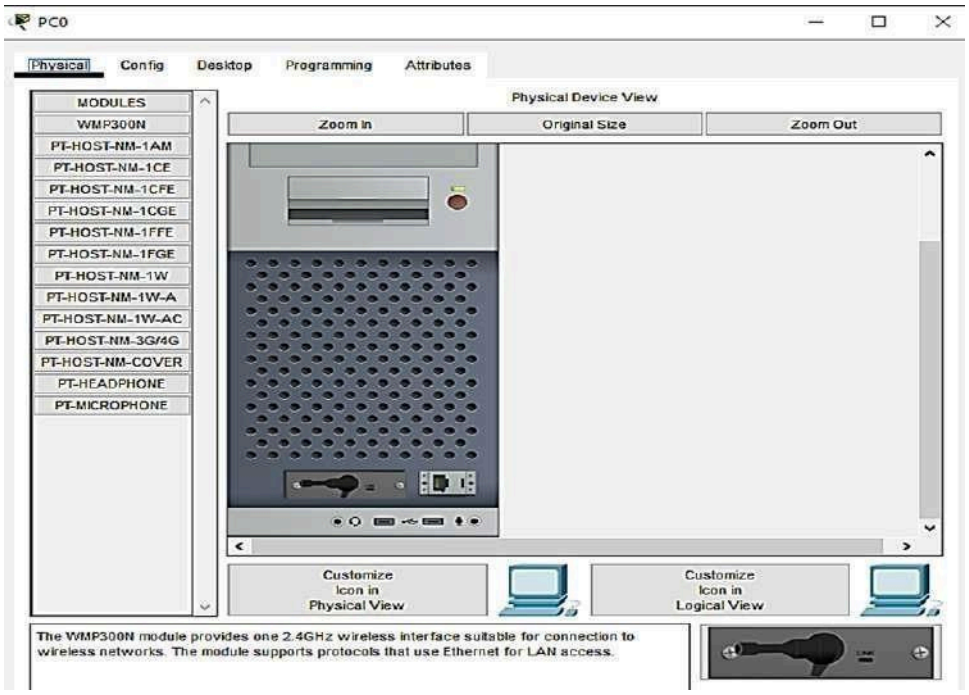



Wireless Router0
Physical
Config
GUI
Attributes
Wireless Tri-Band Home Router
Firmware Version: v0.9.7
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settings
Wireless Security
Guest Network
Wireless MAC Filter
Advanced Wireless Settings
Wireless Tri-Band Home Router
HomeRouter-PT-AC
Basic Wireless Settings
Help...
2.4 GHz
Network Mode:
Auto
Network Name (SSID):
Default
SSID Broadcast:
Enabled
Disabled
Standard Channel:
1 - 2.412GHz
Channel Bandwidth:
Auto
5 GHz - 2
Network Mode:
Auto
Network Name (SSID):
Default
SSID Broadcast:
Enabled
Disabled
Standard Channel:
Auto
Channel Bandwidth:
Auto

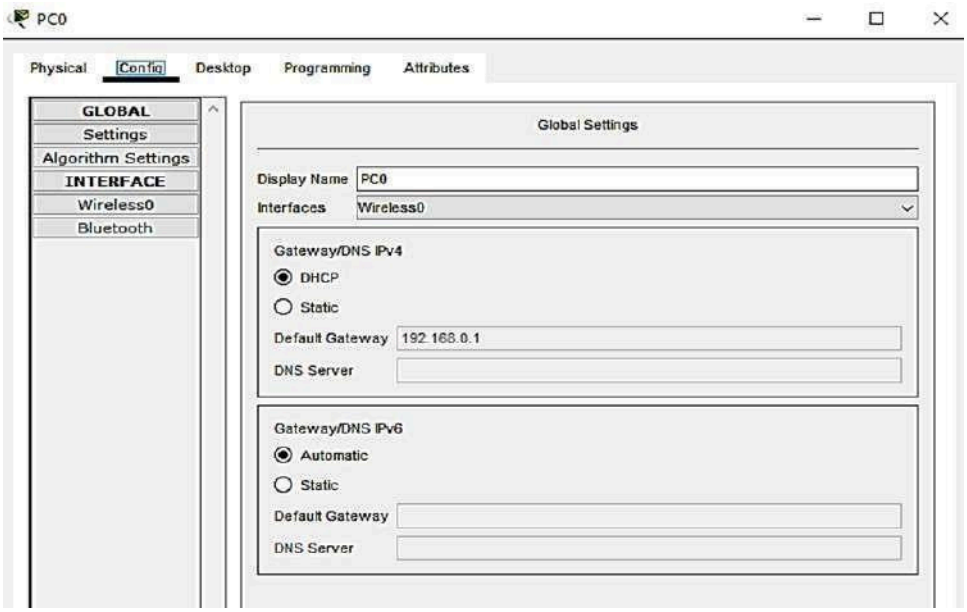

5 GHz - 1
Network Mode:
Auto
Network Name (SSID):
Default
SSID Broadcast:
Enabled
Disabled
Standard Channel:
Auto
Channel Bandwidth:
Auto



<u>PROGRAM 3:</u> (**Change the physical configuration in PC-PT PC 0**) **<u>3(A):</u>** C**hange PT-HOST-NM-1CFE to Linksys-WMP300N**



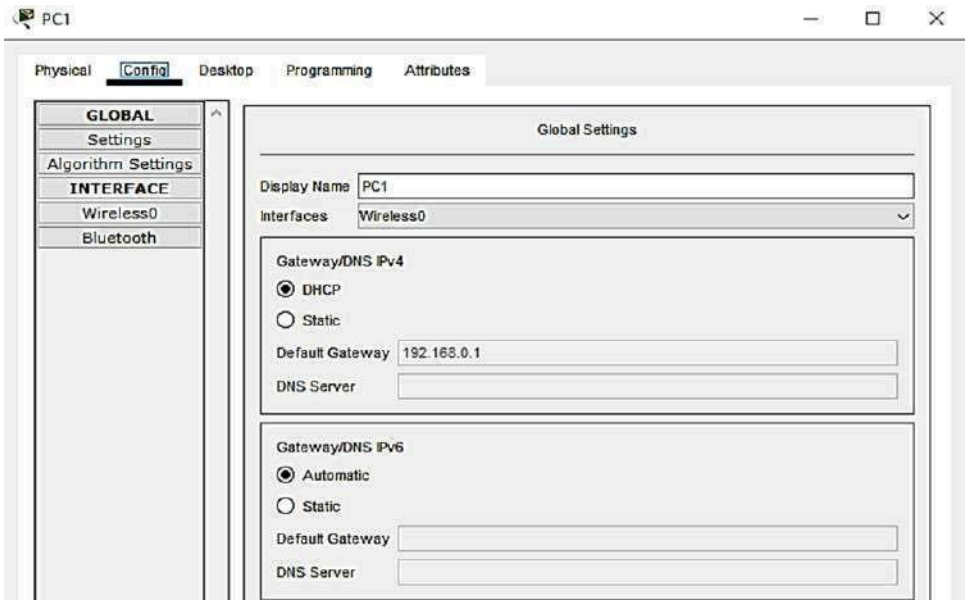
<u>3(B):</u> A**nd now check the default gateway in configure section**



<u>PROGRAM 4:</u> (**Change the physical configuration in PC-PT PC**

1) **<u>4(A):</u>** C**hange PT-HOST-NM-1CFE to Linksys-WMP300N**

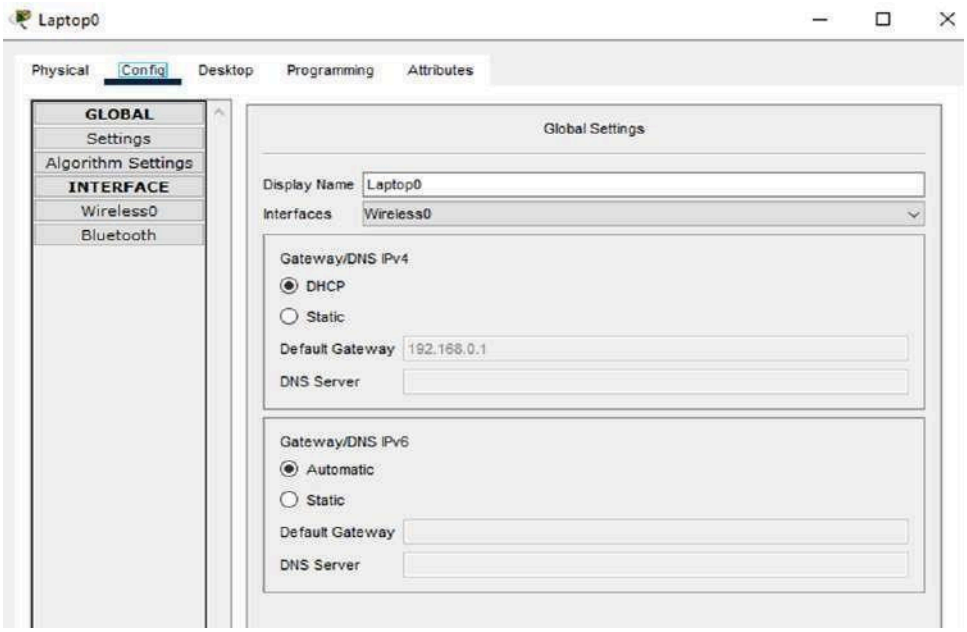
<u>4(B):</u> And now check the default gateway in configure section



PROGRAM 5: (**Change the physical configuration in Laptop-PT Laptop 0**)

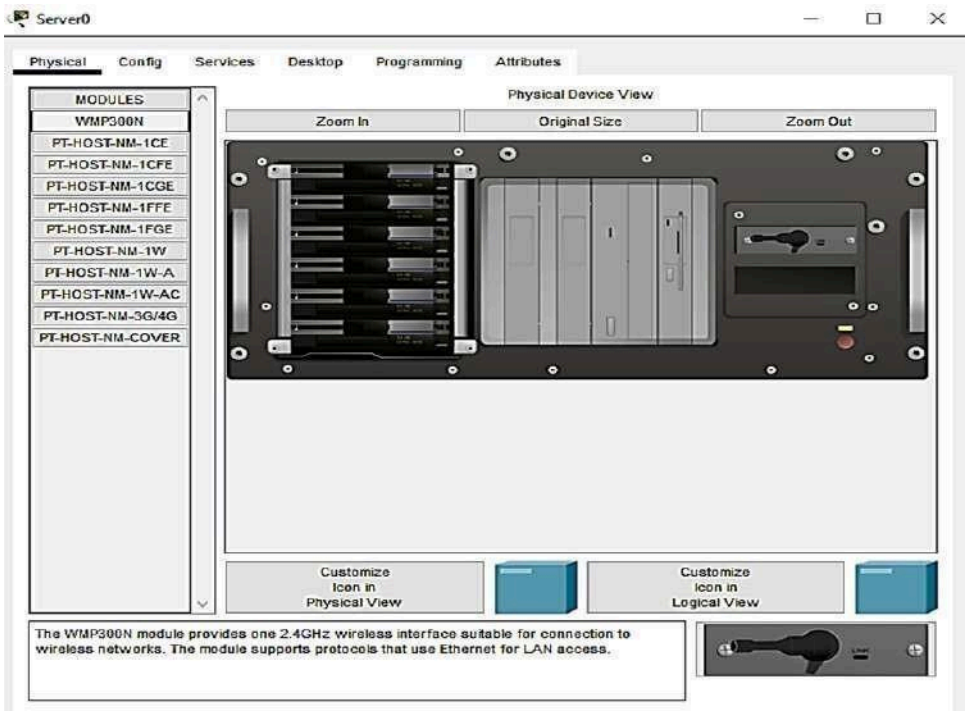
5(A): C**hange PT-LAPTOP-NM-1AM to PT-LAPTOP-NM-1W**

5(B): **And now check the default gateway in configure section**

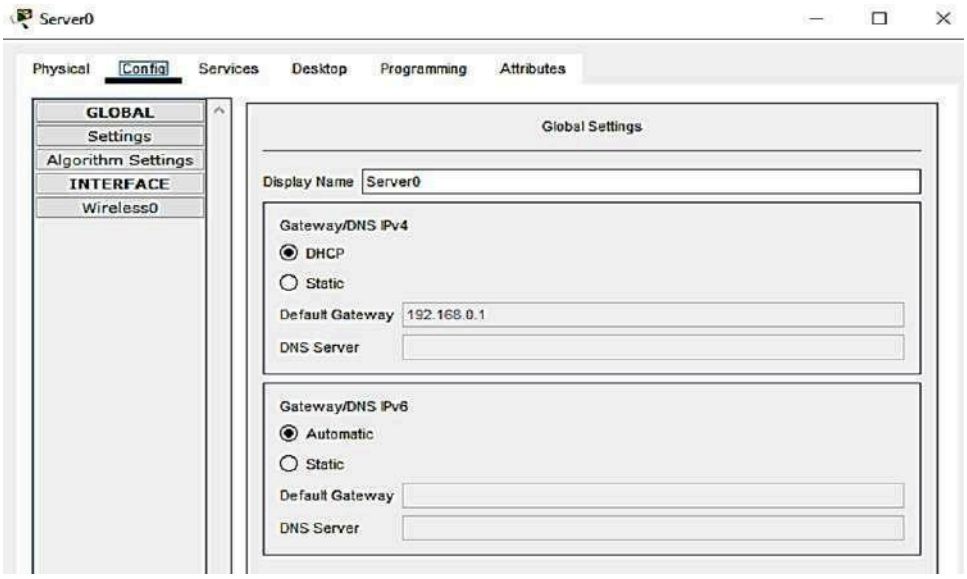


<u>PROGRAM 6:</u> (**Change the physical configuration in Server-PT server 0**)

<u>6(A):</u> C**hange PT-HOST-NM-1CFE to Linksys-WMP300N**



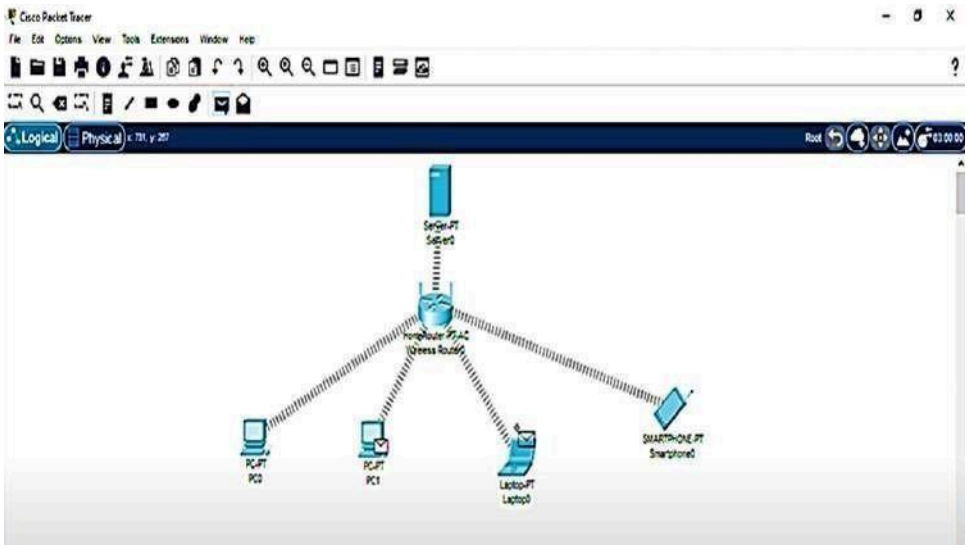
<u>6(B):</u> And now check the default gateway in configure section



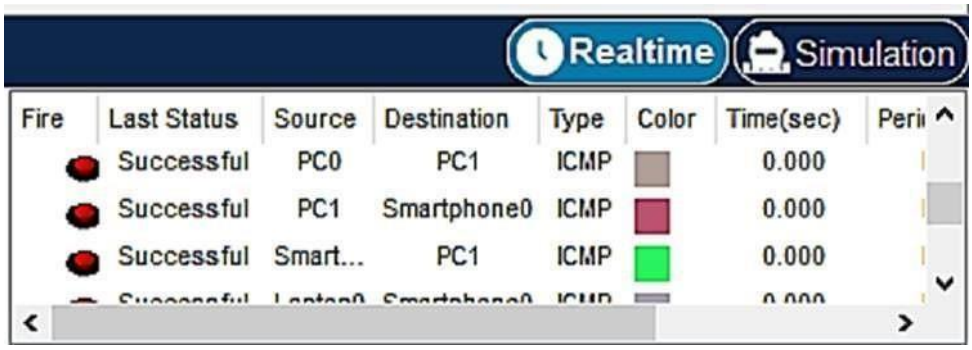
<u>PROGRAM 7:</u> (**Click on: PC-PT PC 0 Desktop>PC Wirelss**)

And Now Click on The Connect Option and in Site Information click on Wireless Mode it will show (infrastructure) :

<u>PROGRAM 8:</u> (**Now you have to add the PDU P ( ) IN PC 0, PC 1, Laptop, Smart Phone and Server**)



<u>PROGRAM 9:</u> (Final Output)


Realtime
Simulation
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Successful PC0 PC1 ICMP 0.000
Successful PC1 Smartphone0 ICMP 0.000
Successful Smart... PC1 ICMP 0.000


Realtime
Simulation
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Successful Laptop0 Smartphone0 ICMP 0.000
Successful Smart... Laptop0 ICMP 0.000
Successful PC0 Server0 ICMP 0.000

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. 1. The RIP protocol is ideal for small networks since it is simple to learn and

configure.

1. 2. RIP routing is guaranteed to work with nearly all routers.
2. 3. When the network topology changes, RIP does not require an

update. Cons:

1. 1. RIP does not support variable length subnet masks
2. 2. RIP transmits updates every 30 seconds, which cause traffic and consumes

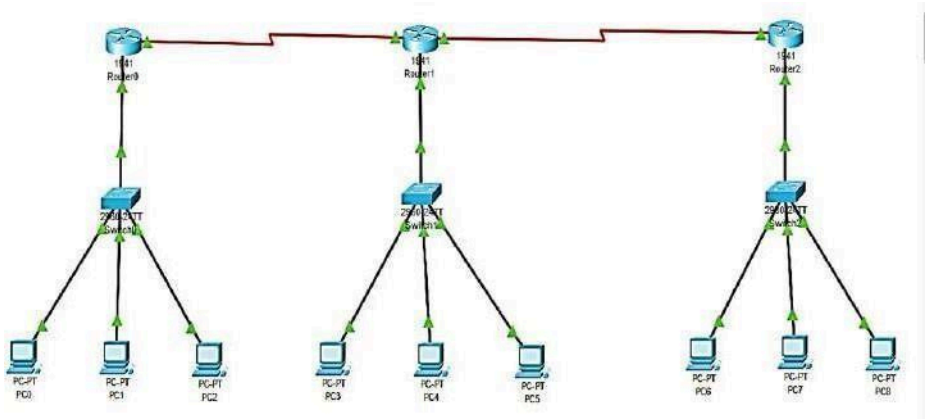
bandwidth.

1. 3. RIP hop counts are restricted to 15, hence any router beyond that distance is deemed infinity and becomes unreachable.
2. 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.

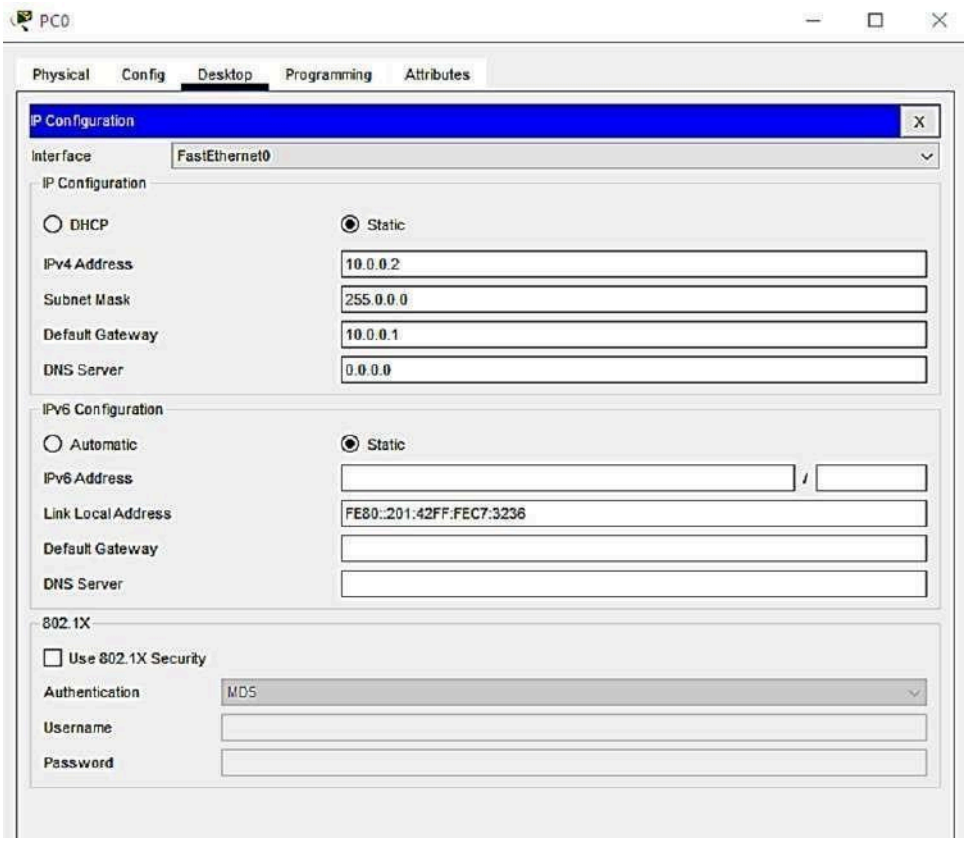
1. 5. RIP does not support multiple paths on the same route, which may result in extra routing loops.

PROGRAM 1: (We got the following topology)

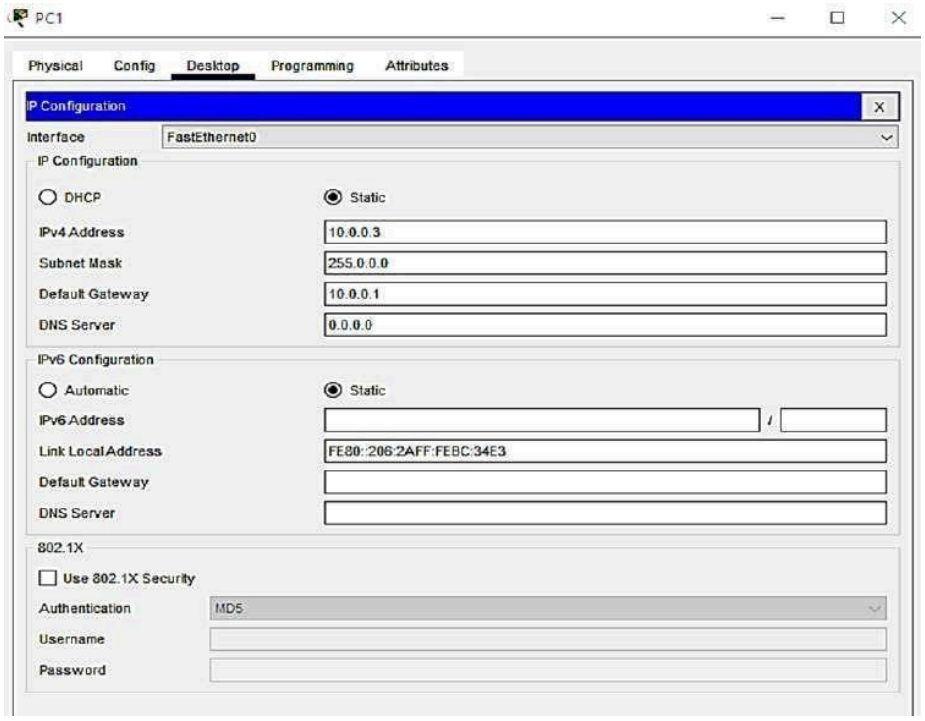


PROGRAM 2:

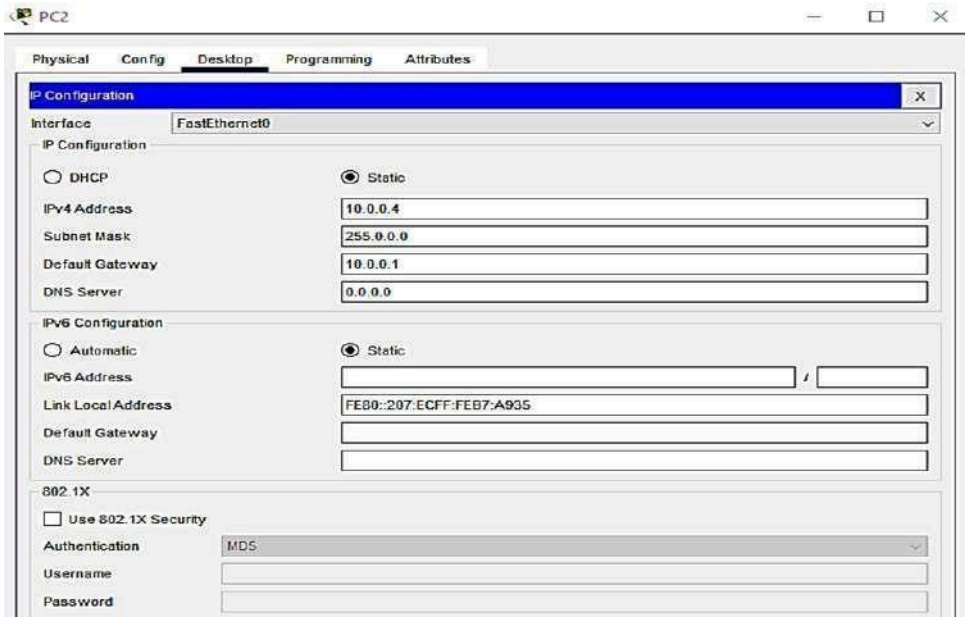
2(A): Now configure the PC 0 IP Address



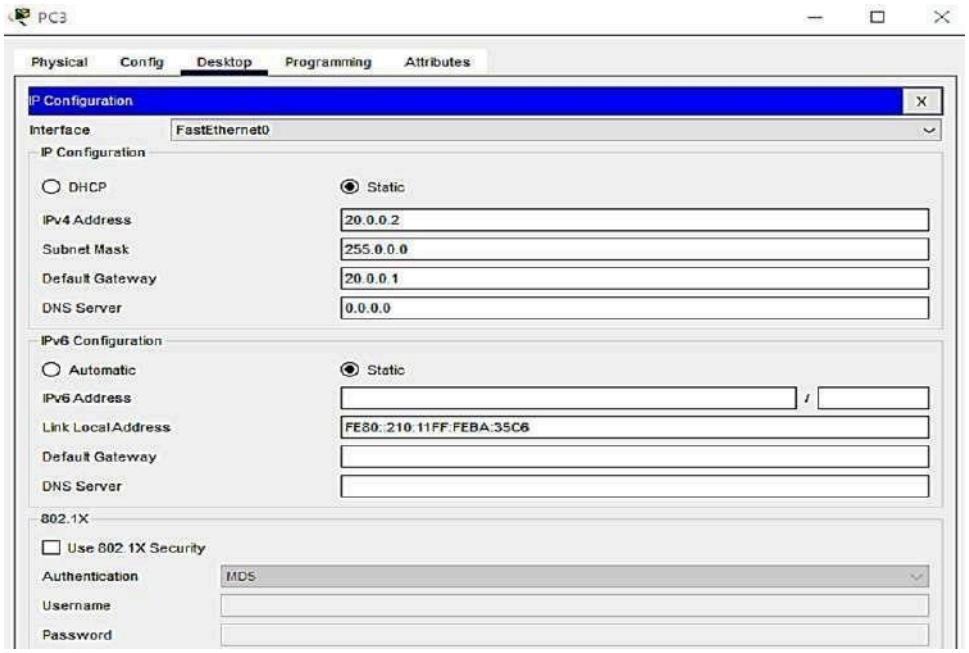
2(B): Now configure the PC 1 IP Address



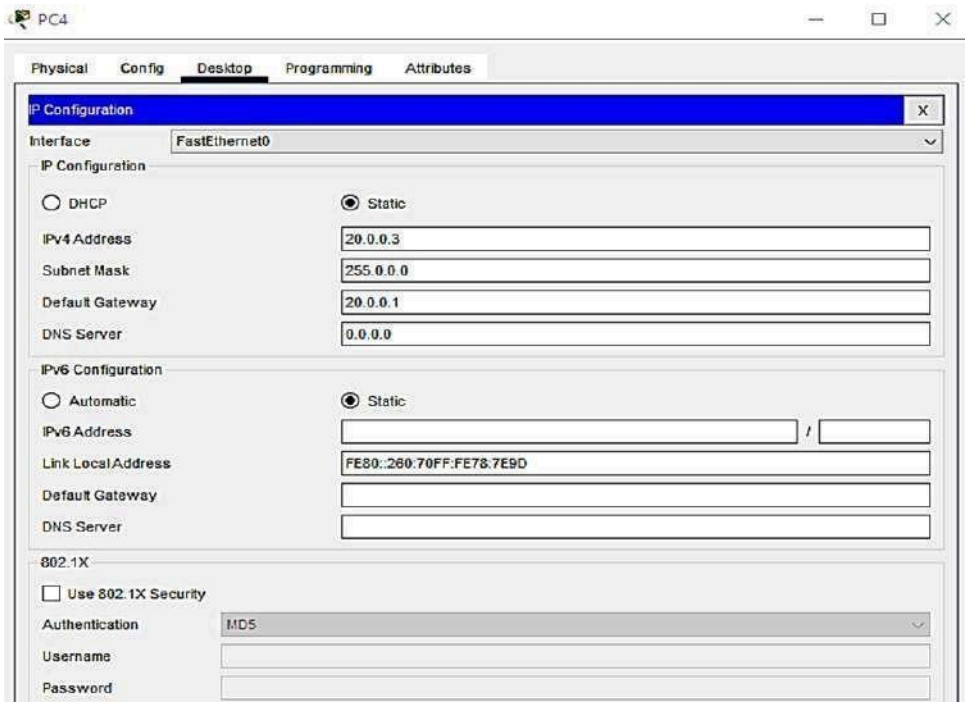
2(C): Now configure the PC 2 IP Address



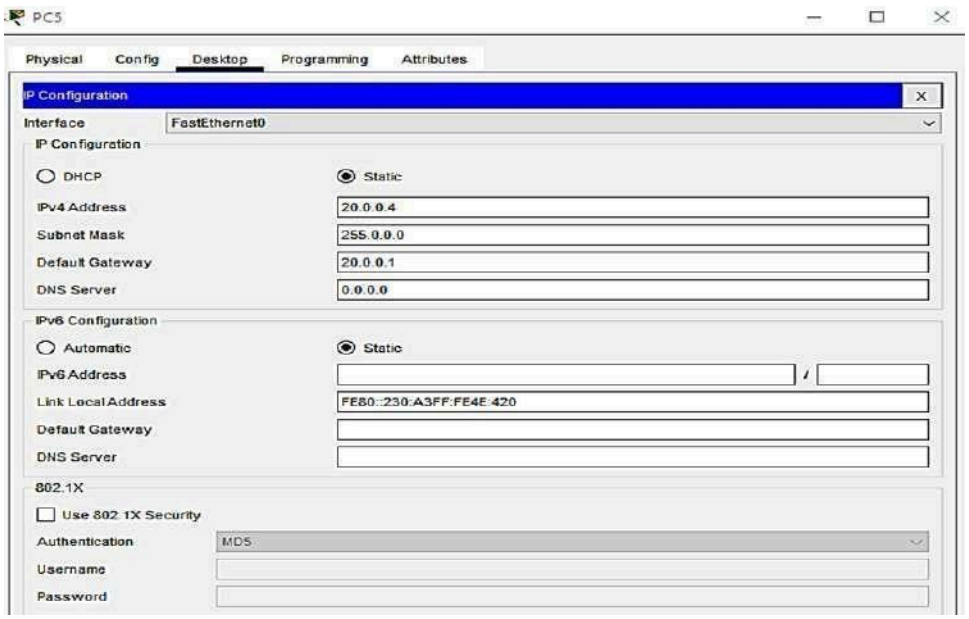
2(D): Now configure the PC 3 IP Address



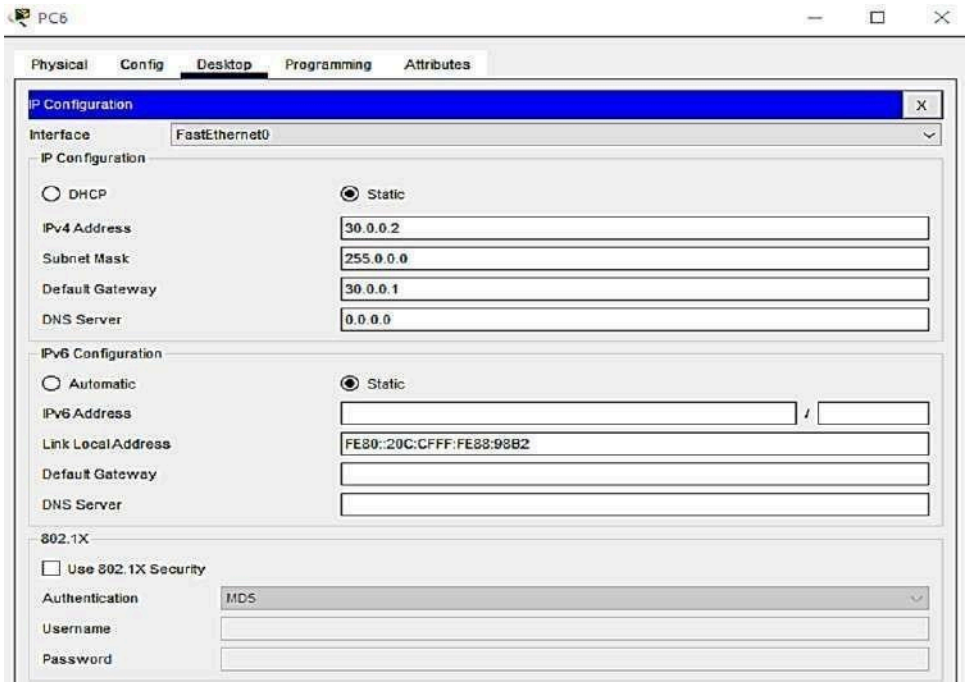
2(E): Now configure the PC 4 IP Address



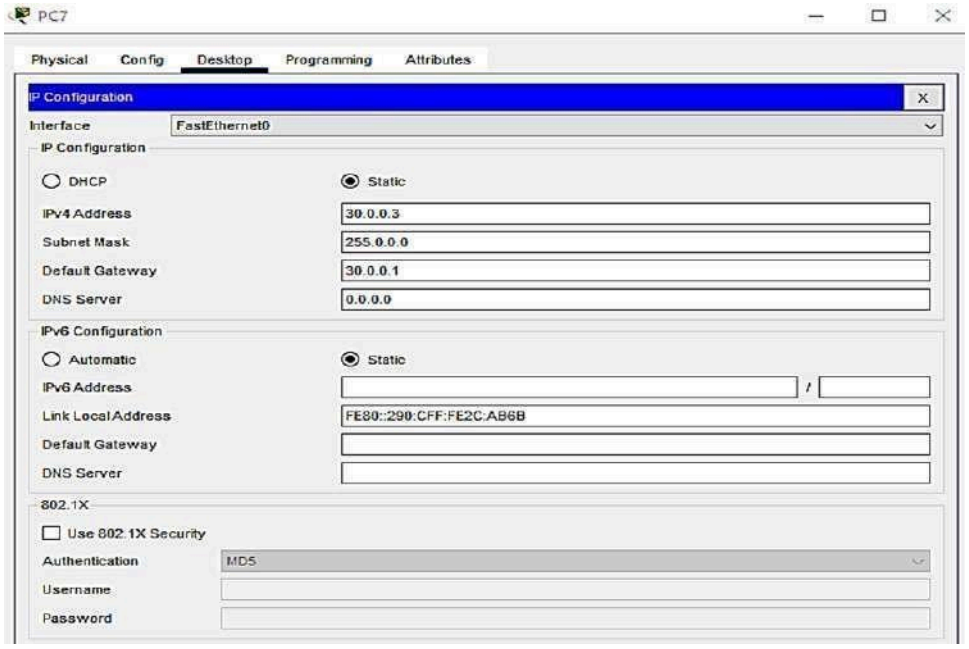
2(F): Now configure the PC 5 IP Address



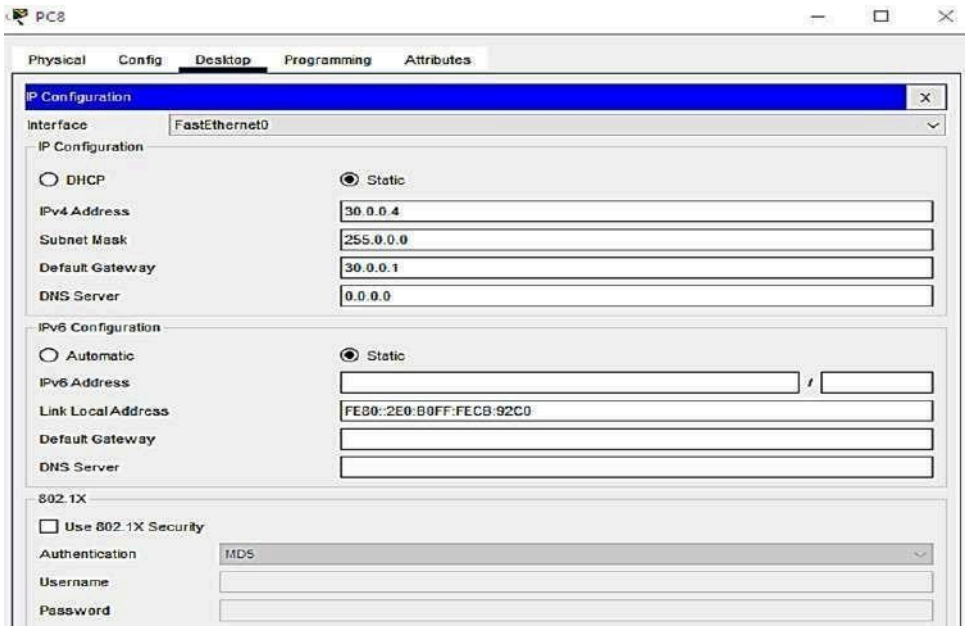
2(G): Now configure the PC 6 IP Address



2(H): Now configure the PC 7 IP Address

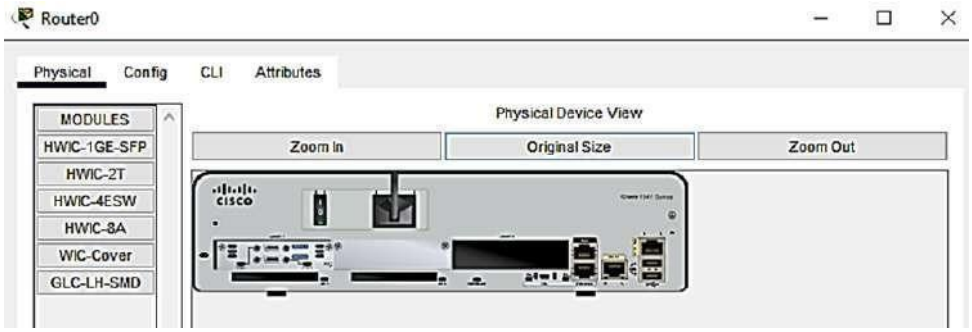


2(I): Now configure the PC 8 IP Address

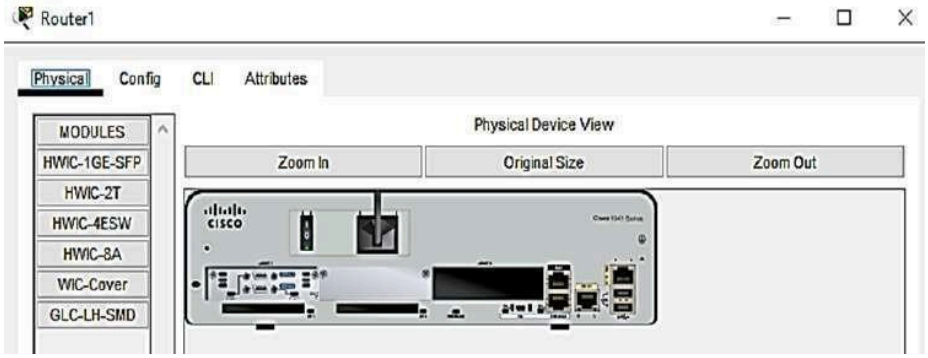


PROGRAM 3:

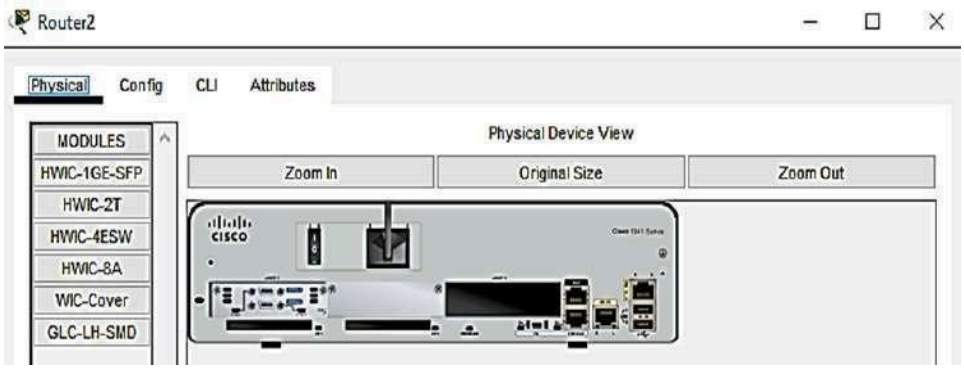
3(A): Router 0



3(B): Router 1



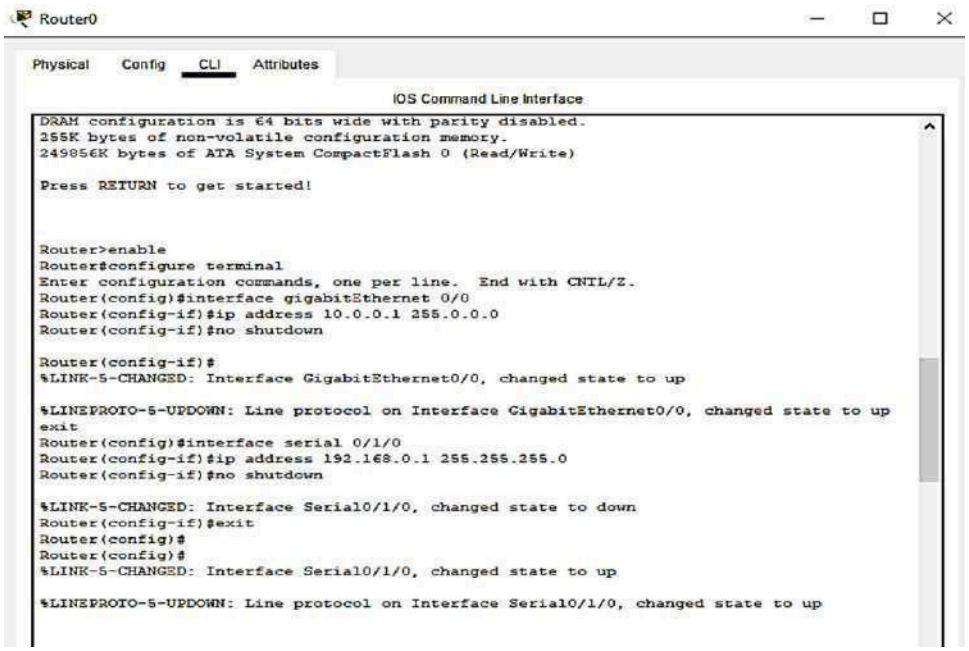
3(C): Router 2



Remember You have to OFF the switch while adding Serial Interface and ON the Switch after adding the interface in all the Routers

PROGRAM 4:

4(A): Router 0



Type the following command in CLI :

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

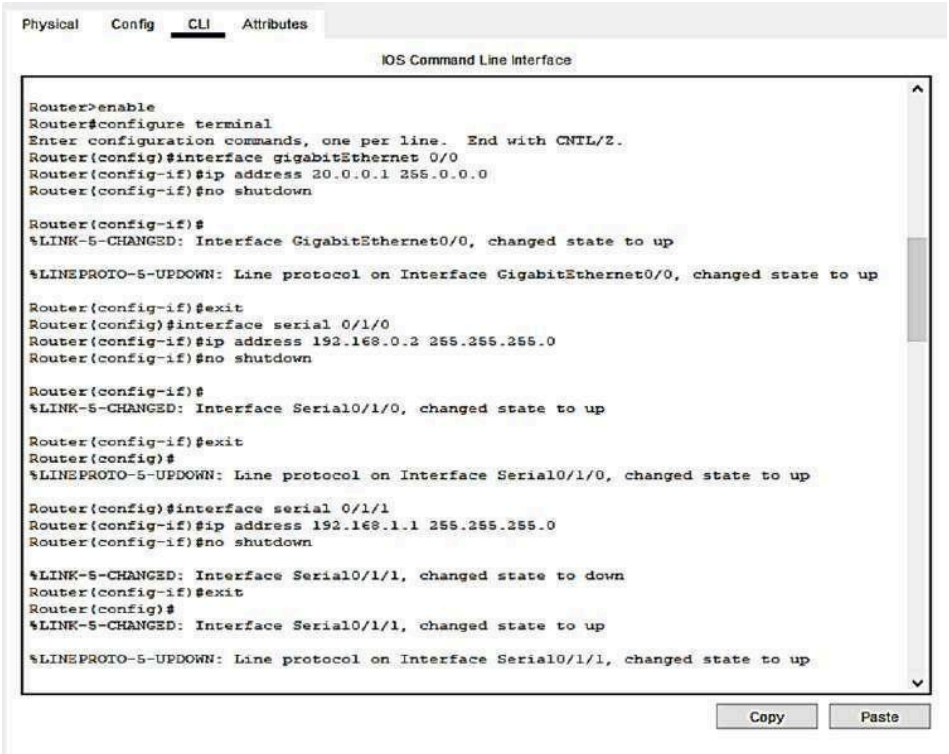
Router(config-if)#exit

Router(config)#interface serial 0/1/1

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#no shutdown

4(B): Router 1



Type the Following Command in CLI :

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

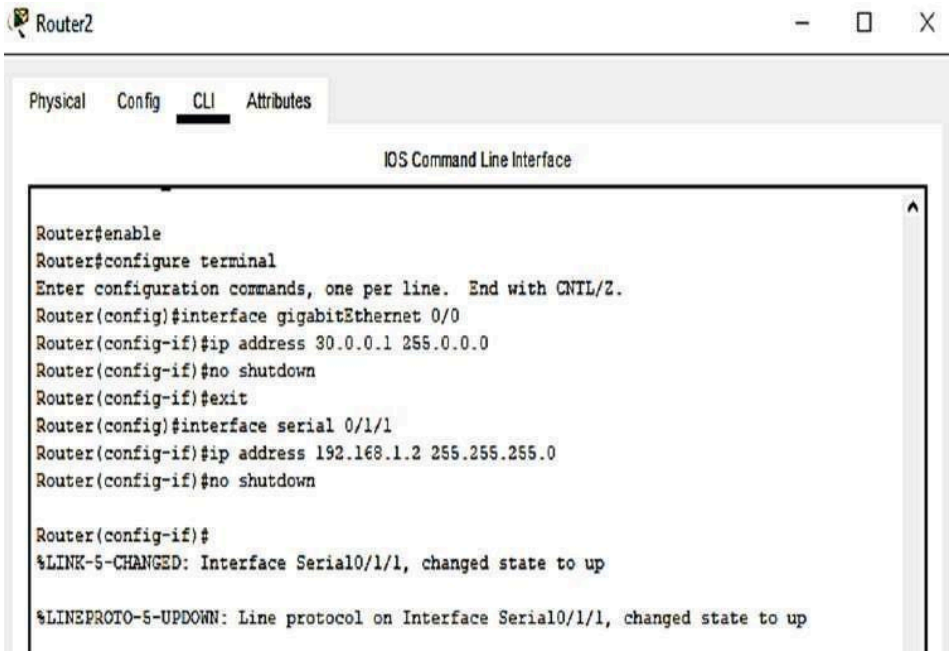
Router(config-if)#exit

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

4(C): Router 2



Type the following Command in CLI :

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

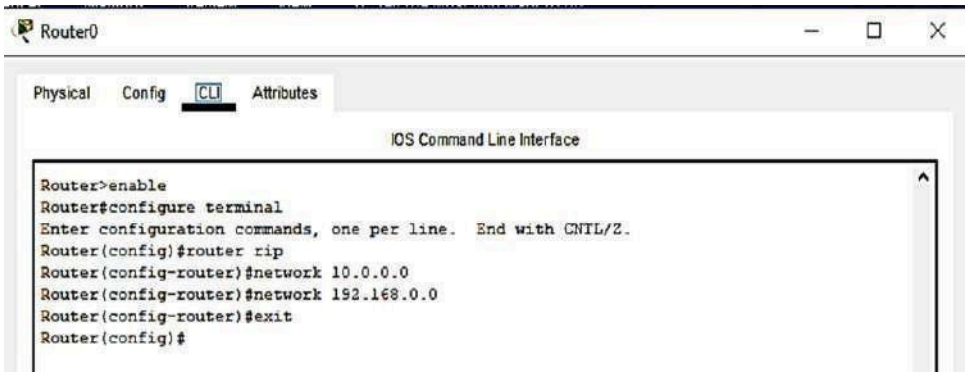
Router(config)#interface serial 0/1/1

Router(config-if)#ip address 192.168.1.2 255.255.255.0

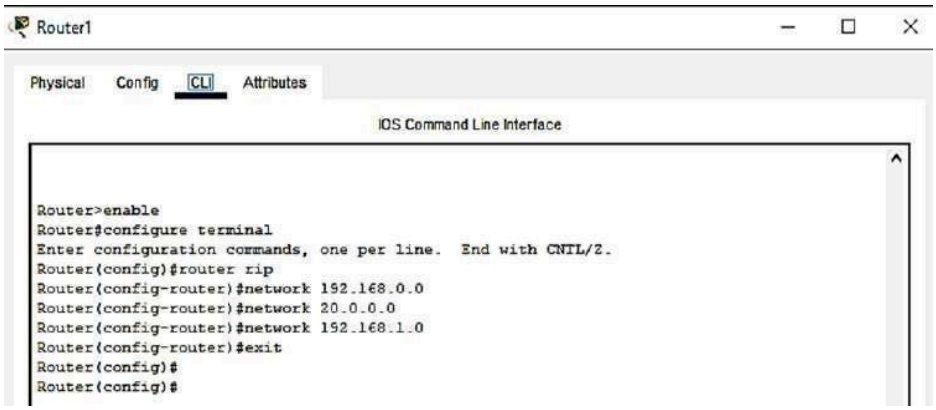
Router(config-if)#no shutdown

PROGRAM 5:

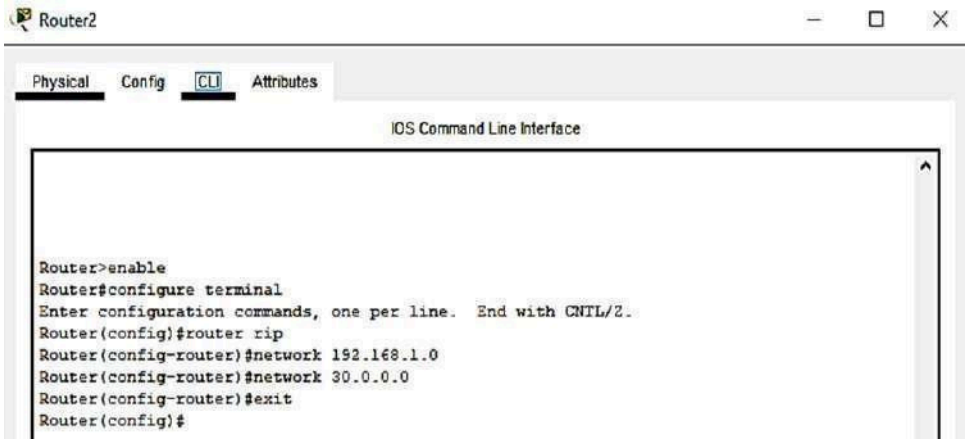
5(A): Router 0



5(B): Router 1

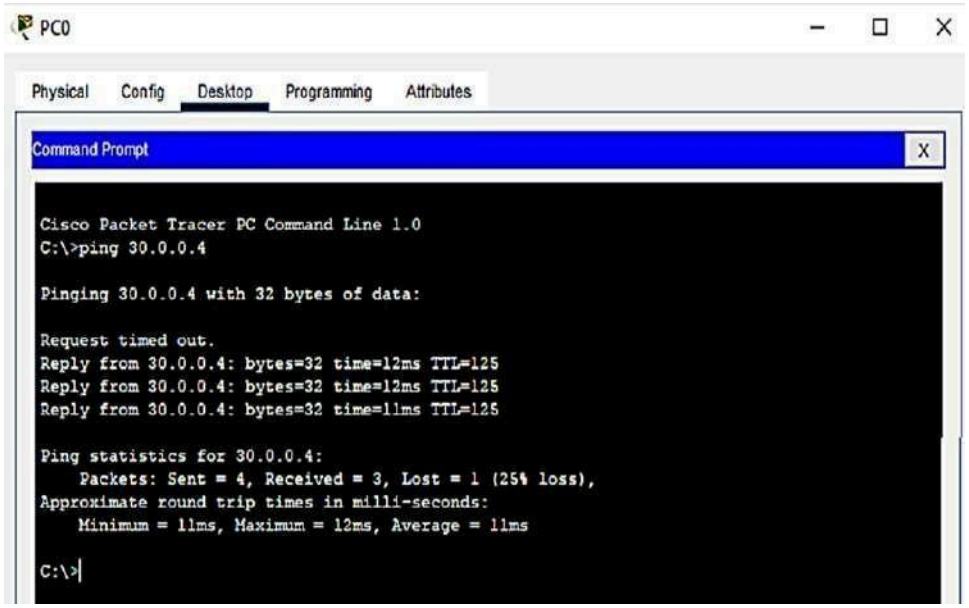


5(C): Router 2

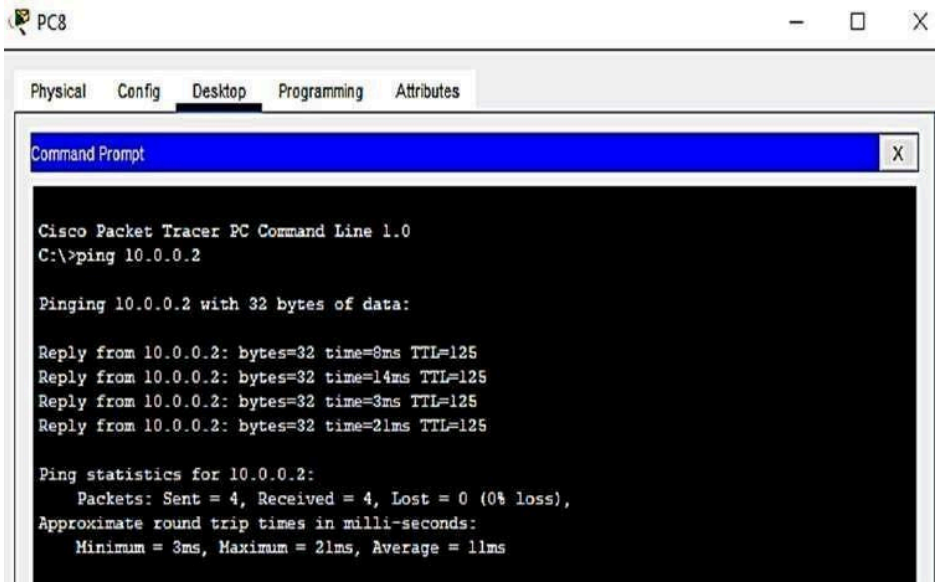


PROGRAM 6:

6(A): PC 0



6(B): PC 8


PC8
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2
Pinging 10.0.0.2 with 32 bytes of data:
Reply from 10.0.0.2: bytes=32 time=8ms TTL=125
Reply from 10.0.0.2: bytes=32 time=14ms TTL=125
Reply from 10.0.0.2: bytes=32 time=3ms TTL=125
Reply from 10.0.0.2: bytes=32 time=21ms TTL=125
Ping statistics for 10.0.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 21ms, Average = 11ms

Practical No.6

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:

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

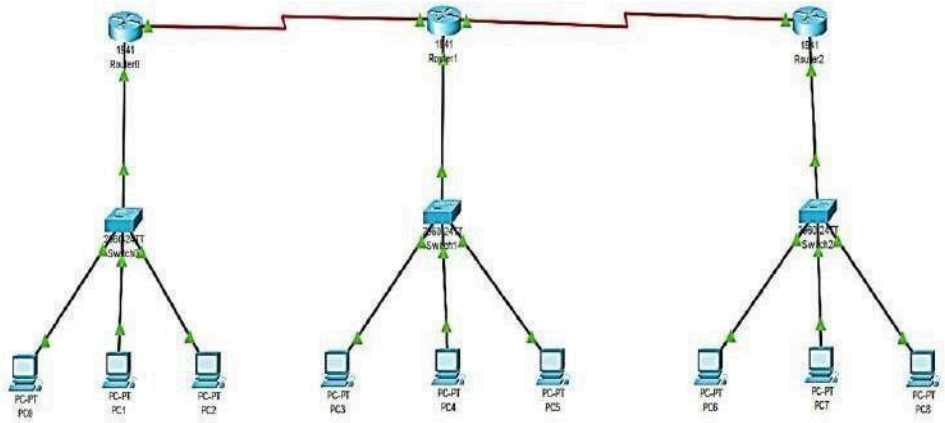
1. It's a standardized protocol.
2. It's VLSM compliant.
3. Provides fast convergence.
4. It sends triggered updates when the network changes.
5. Works with snapshot routing – making it ideal for dial networks.

Disadvantage of RIPv2

6. Max hop count of 15, due to the 'count-to-infinity' vulnerability.
7. No concept of neighbors.

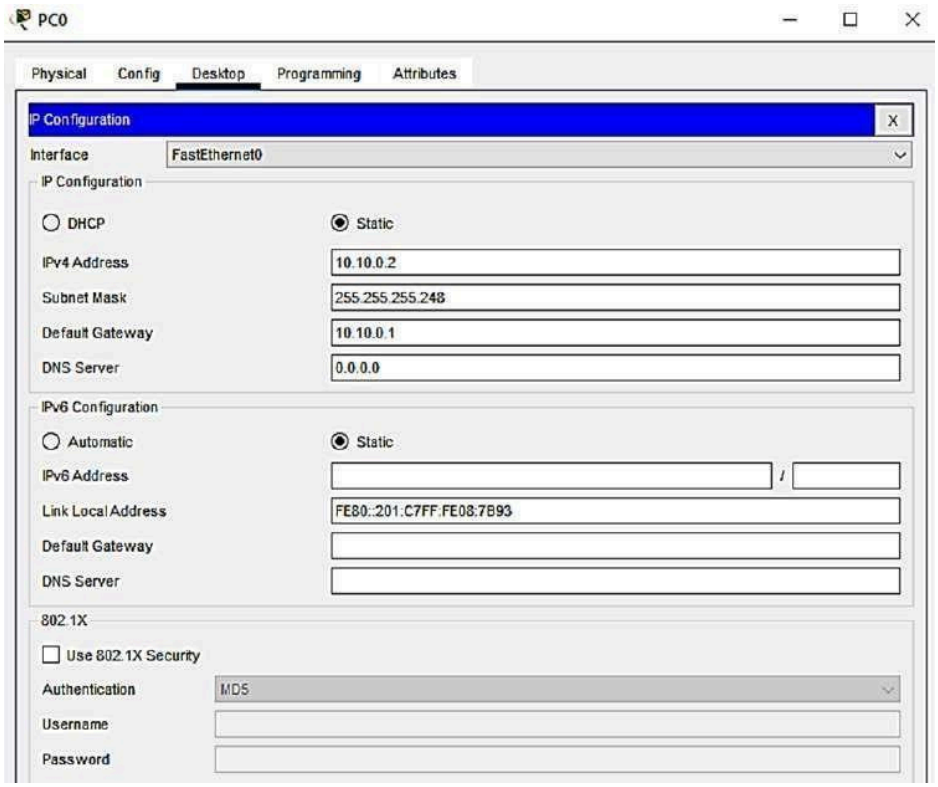
8. Exchanges entire table with all neighbors every 30 seconds (except in the case of a triggered update).

PROGRAM 1: (We got the following topology)

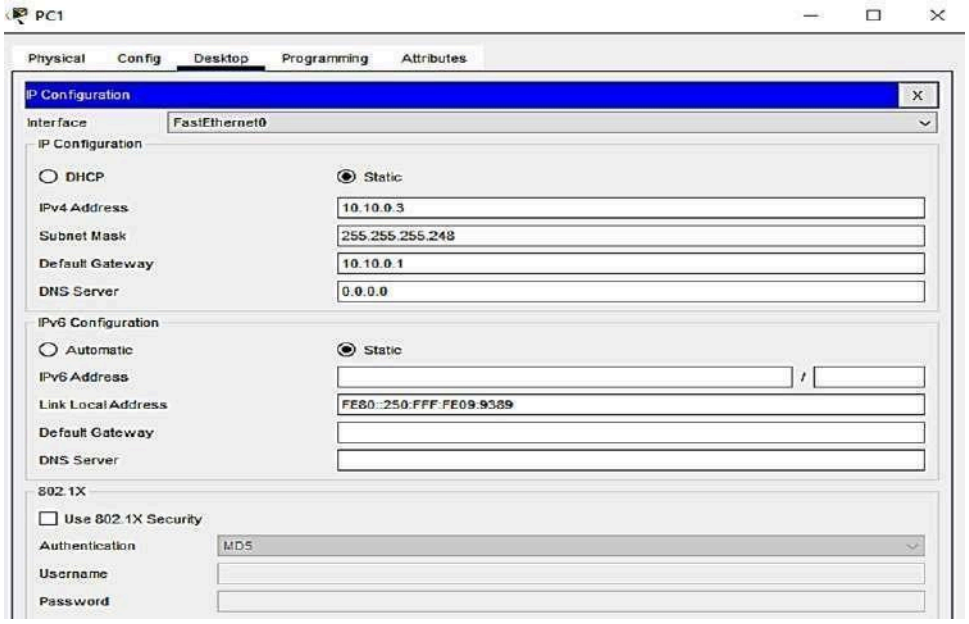


PROGRAM 2:

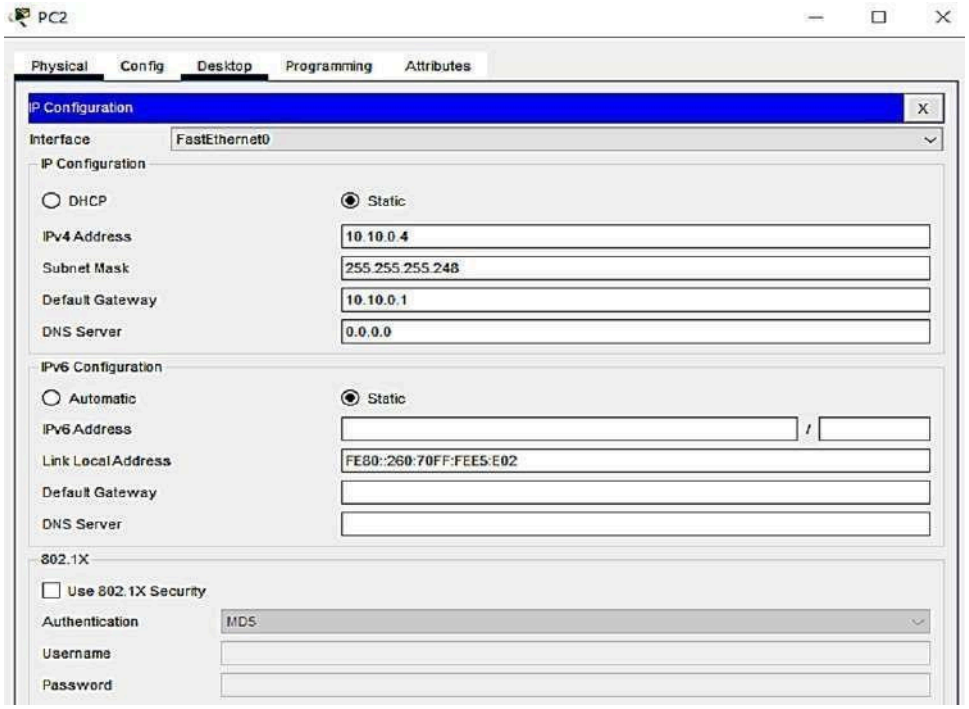
2(A): Now configure the PC 0 IP Address



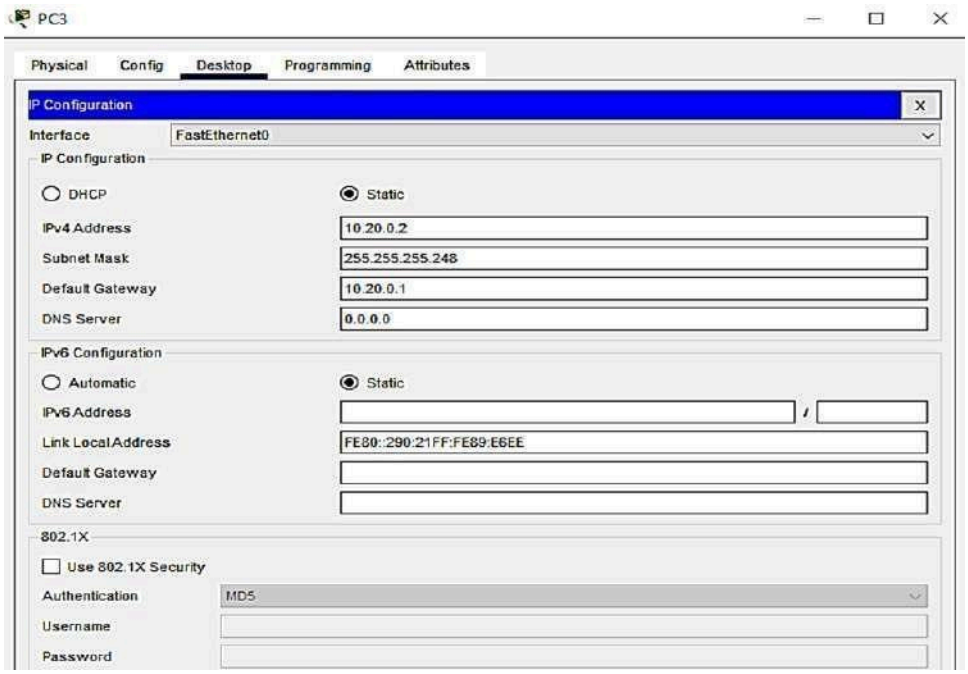
2(B): Now configure the PC 1 IP Address



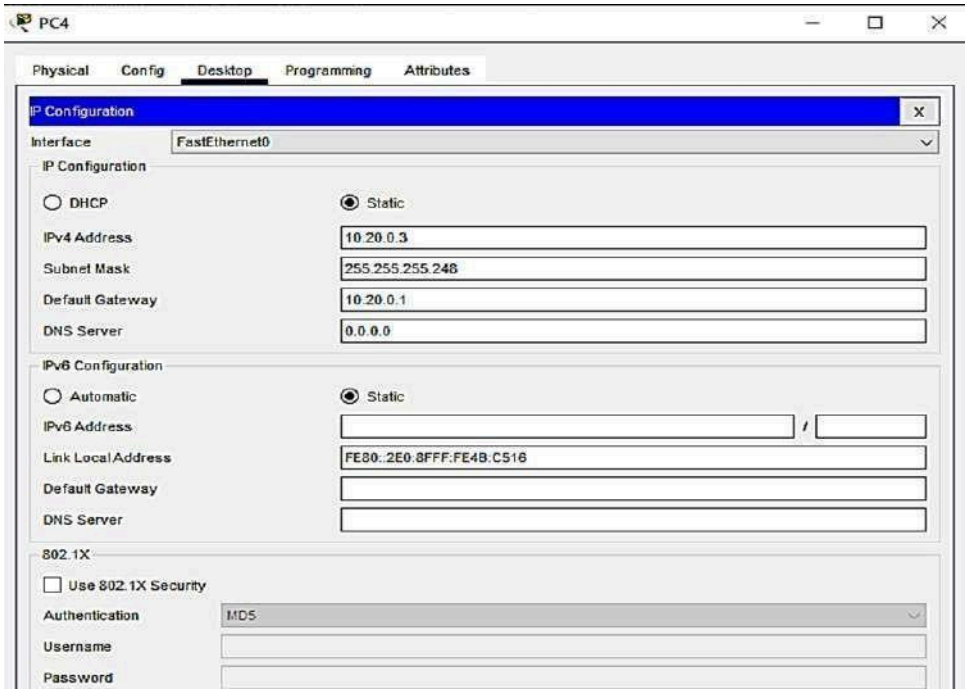
2(C): Now configure the PC 2 IP Address



2(D): Now configure the PC 3 IP Address

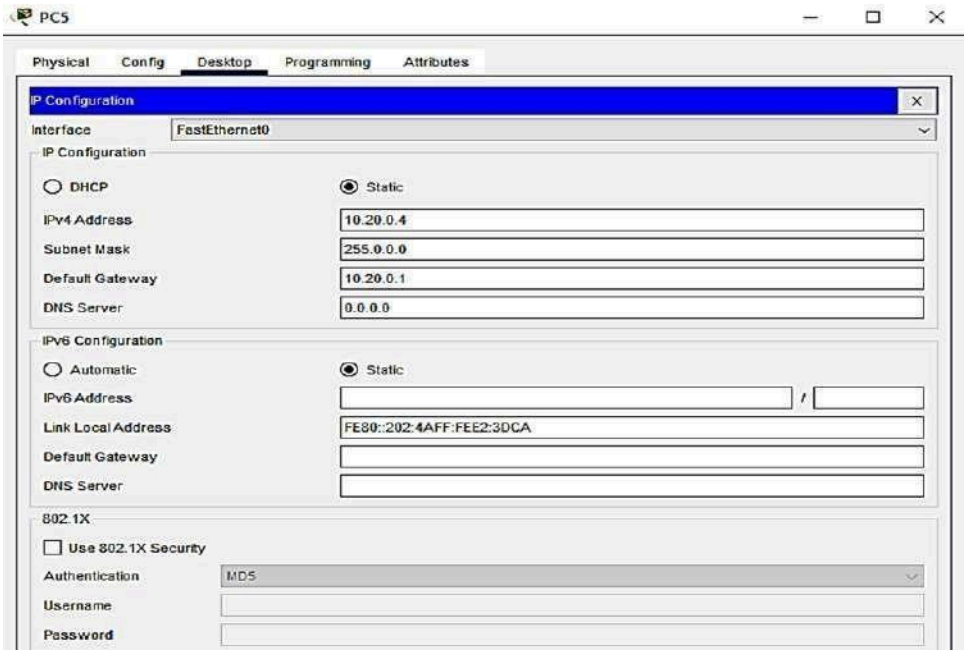


2(E): Now configure the PC 4 IP Address

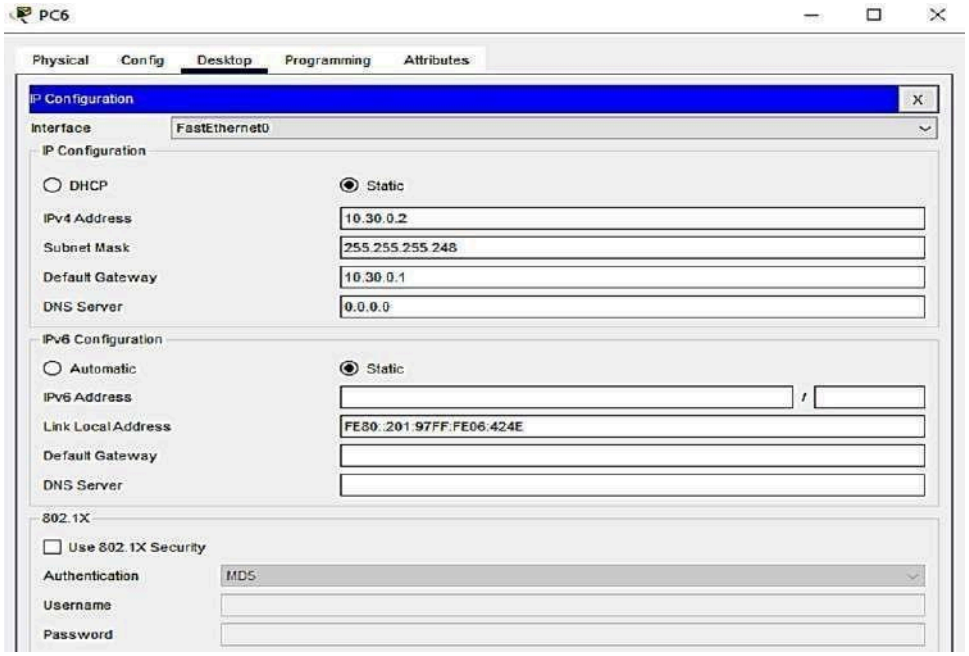


2(F): Now configure the PC 5 IP Address

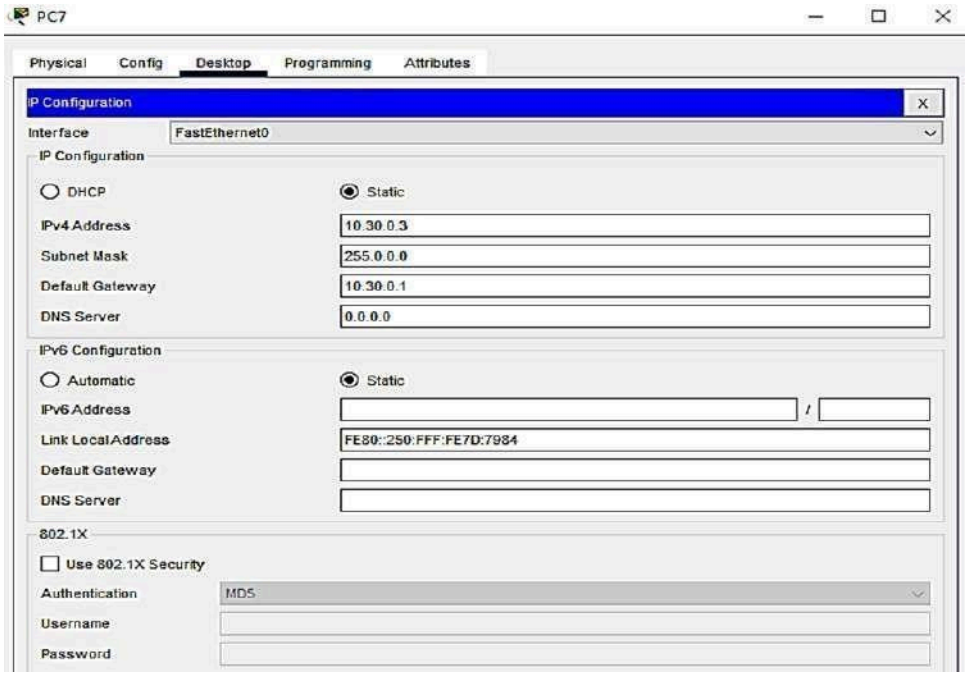
J



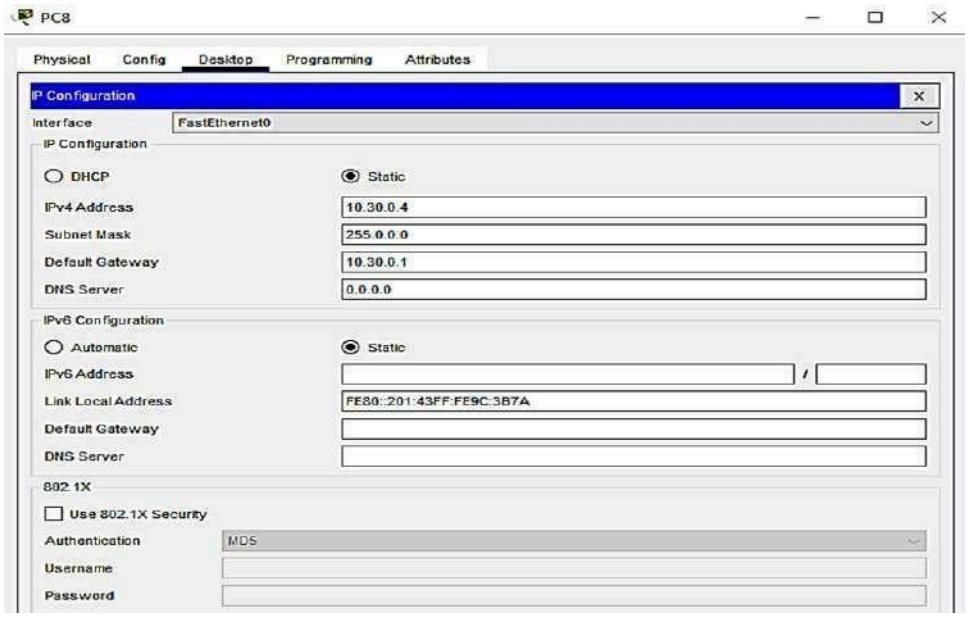
2(G): Now configure the PC 6 IP Address



2(H): Now configure the PC 7 IP Address

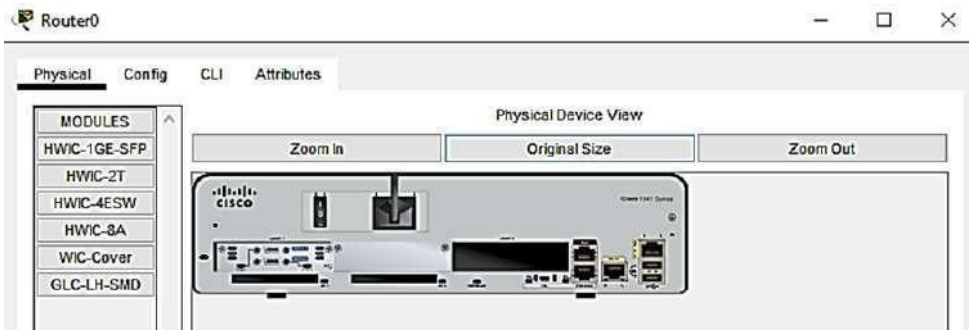


2(I): Now configure the PC 8 IP Address

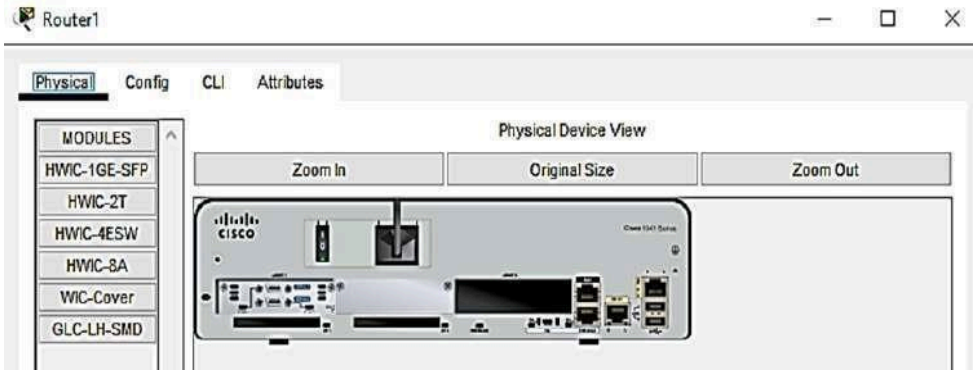


PROGRAM 3: Now in All Router's Physical Section add the Serial Interface of : HWIC-2T

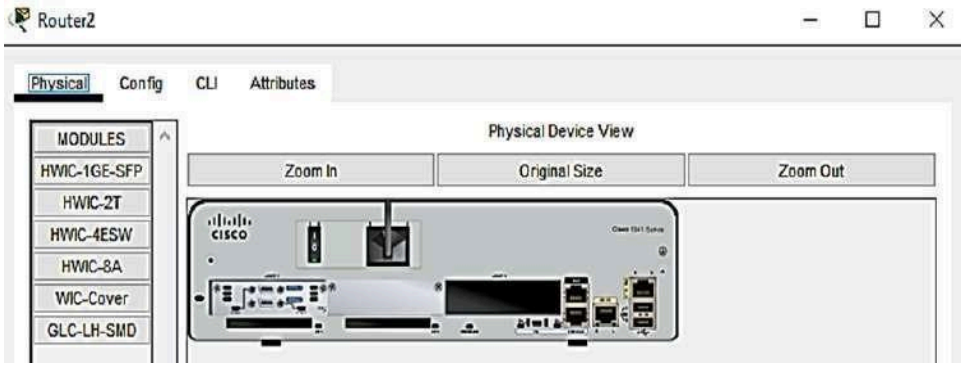
3(A): Router 0



3(B): Router 1



3(C): Router 2

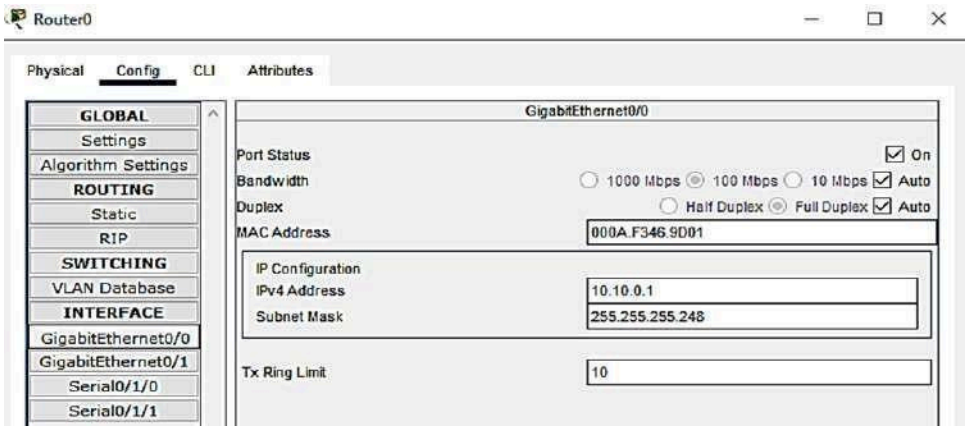


Remember You have to OFF the switch while adding Serial Interface and ON the Switch after adding the interface in all the Routers

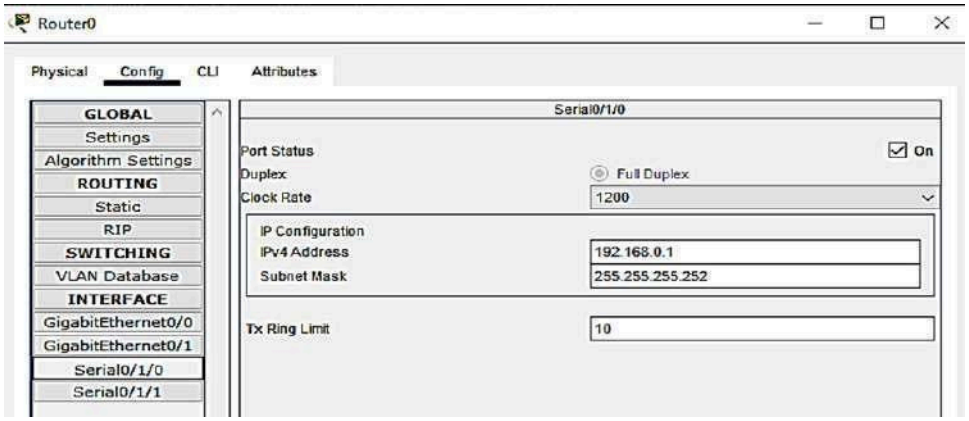
PROGRAM 4:

4(A): Router 0

(i) GigabitEthernet 0/0



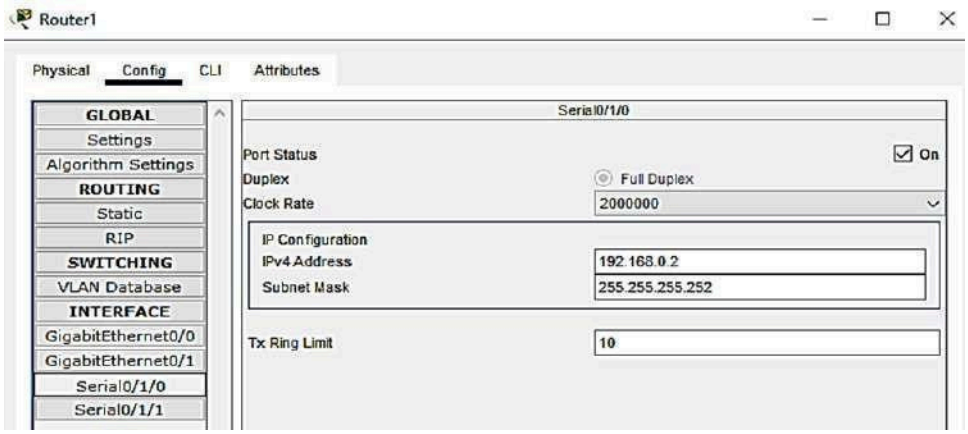
(ii) Serial 0/1/0



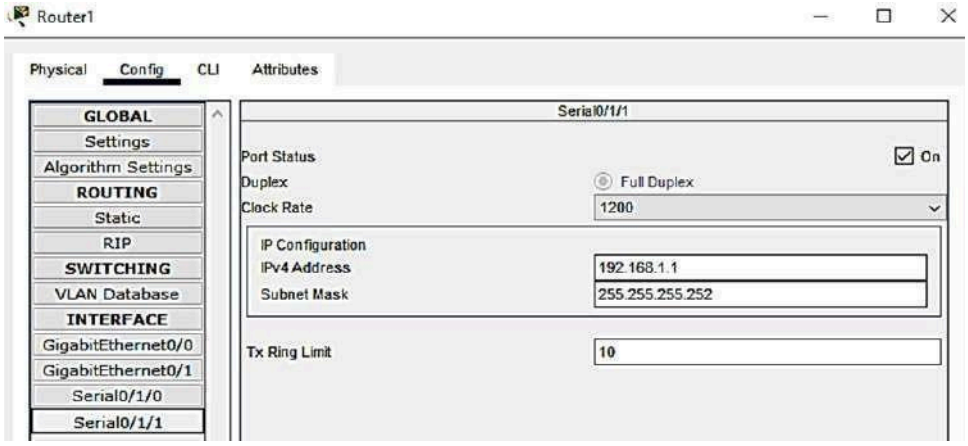
4(B): Router 1

(i) GigabitEthernet 0/0

(ii) Serial 0/1/0

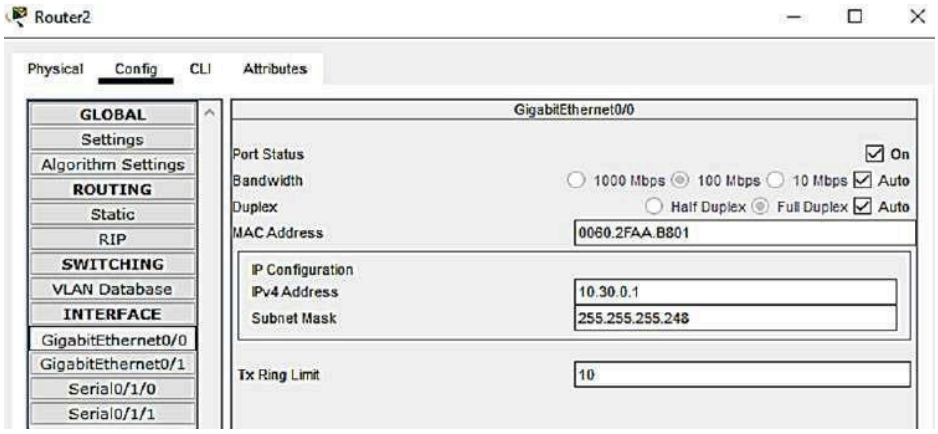


(iii) Serial 0/1/1

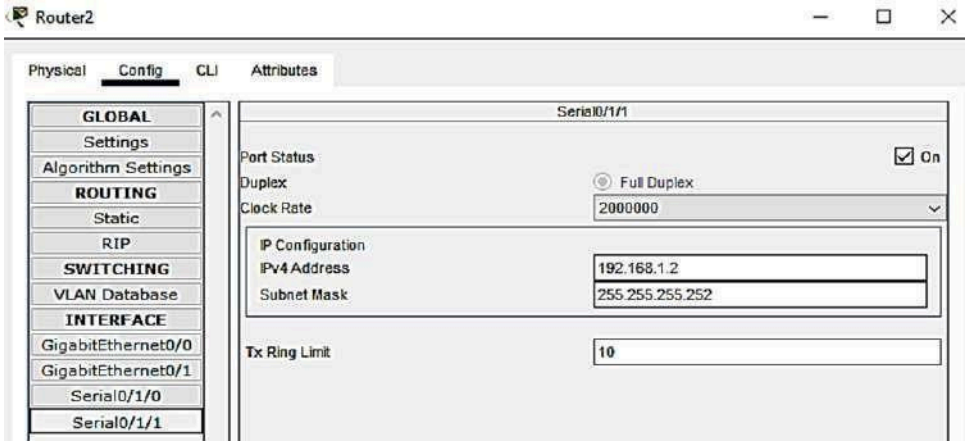


4(C): Router 2

(i) GigabitEthernet 0/0

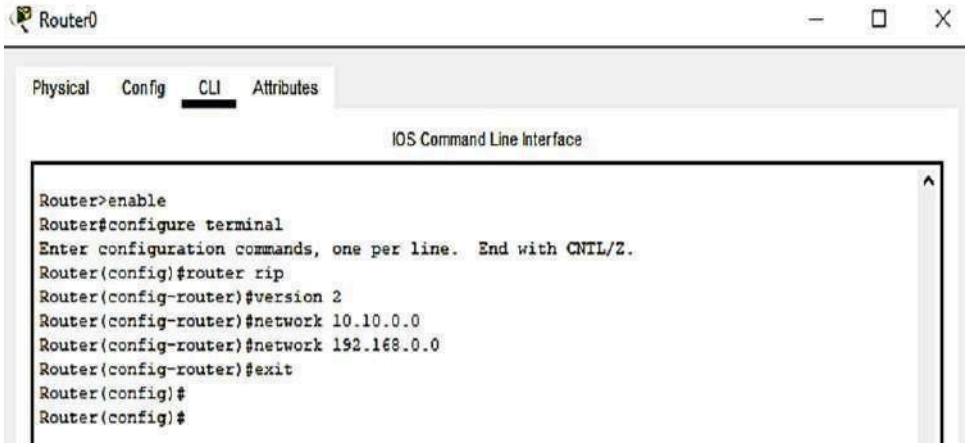


(ii) Serial 0/1/1

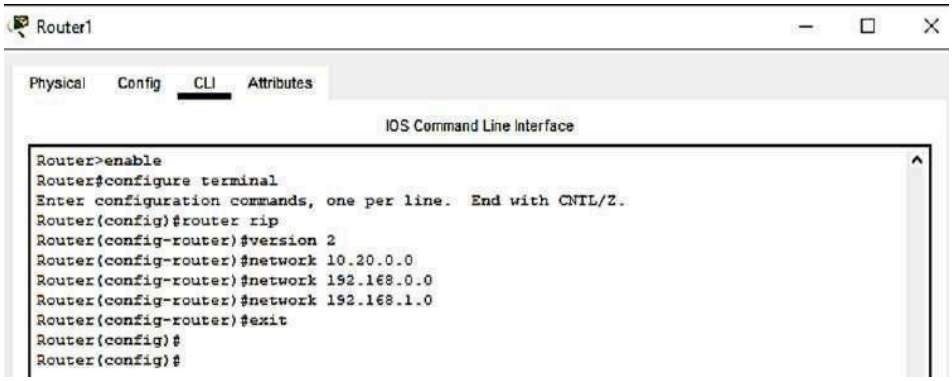


PROGRAM 5:

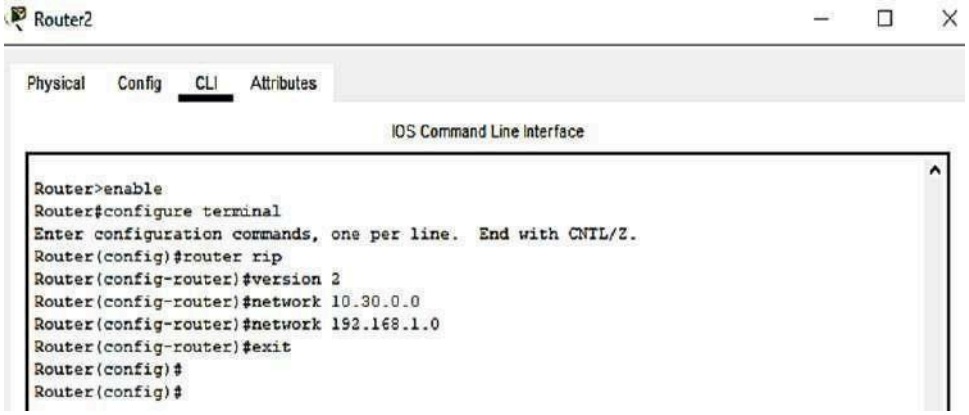
5(A): Router 0



5(B): Router 1

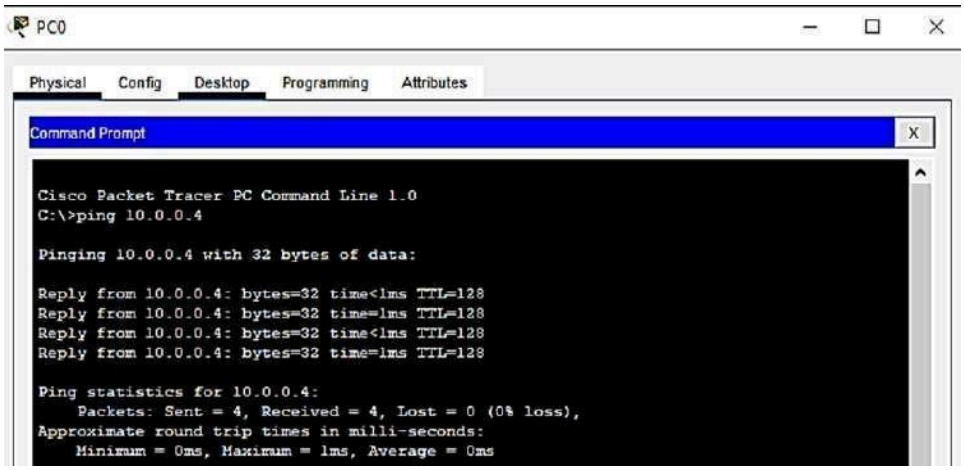


5(C): Router 2

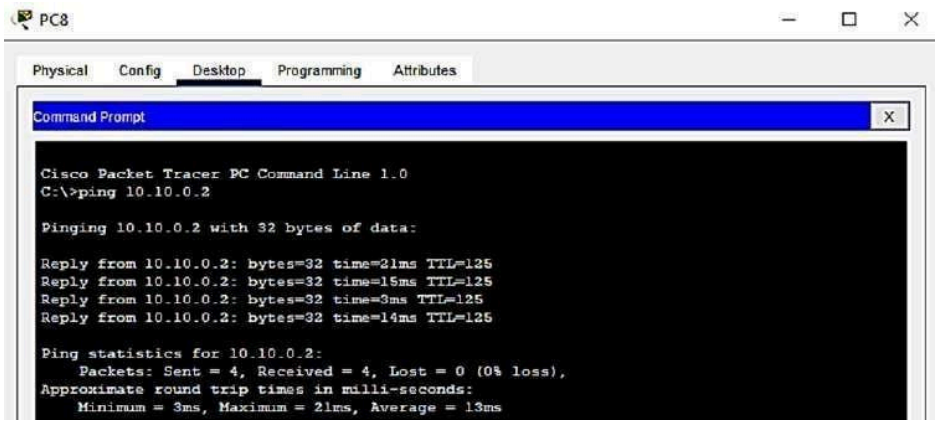


PROGRAM 6: (**Now check the connectivity by using ping command with CMD)**

6(A): PC 0: ping 10.0.0.4



6(B): PC 8: ping 10.0.0.2


PC8
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.0.2
Pinging 10.10.0.2 with 32 bytes of data:
Reply from 10.10.0.2: bytes=32 time=21ms TTL=125
Reply from 10.10.0.2: bytes=32 time=15ms TTL=125
Reply from 10.10.0.2: bytes=32 time=3ms TTL=125
Reply from 10.10.0.2: bytes=32 time=14ms TTL=125
Ping statistics for 10.10.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 21ms, Average = 13ms

Practical No.7

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:

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,

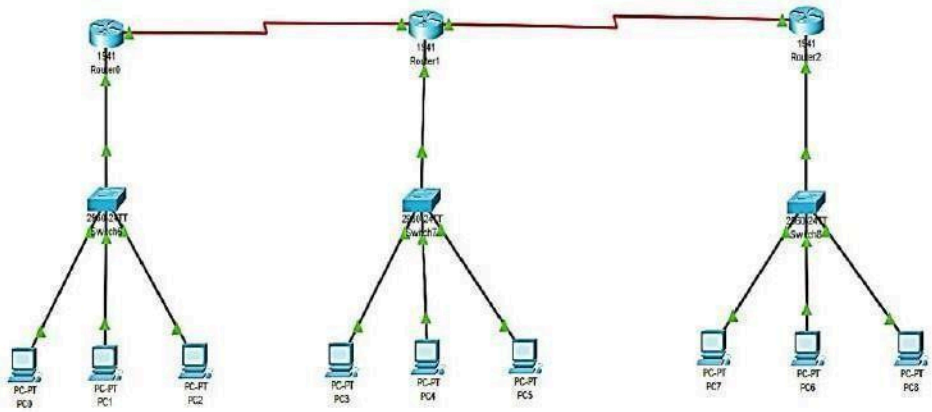
Open shortest path first (OSPF) is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e., the protocol which aims at moving the packet within a large autonomous system or routing domain.

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

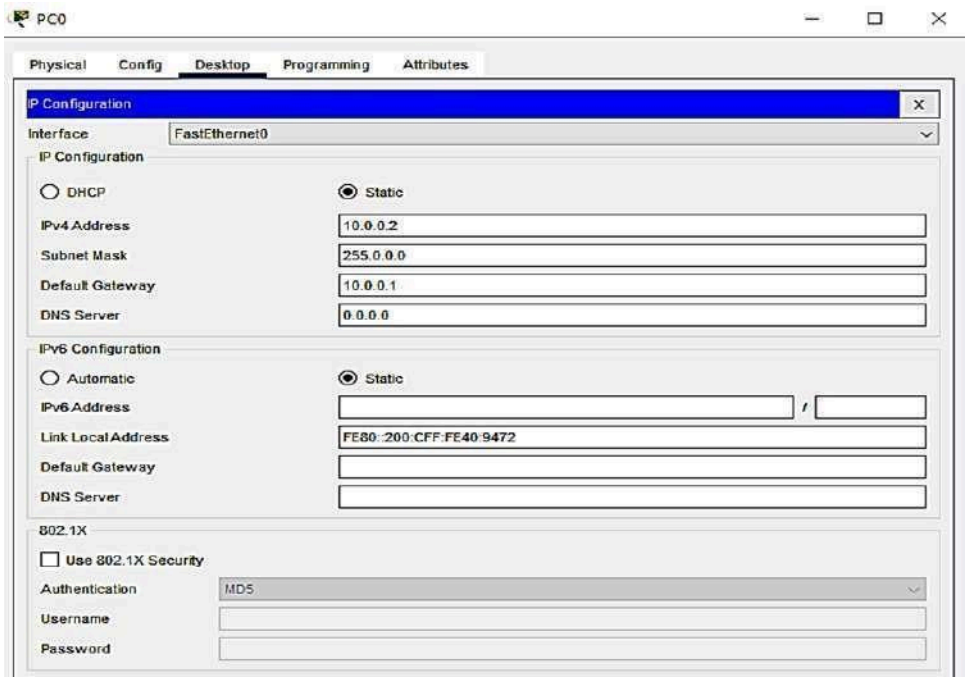
There are some disadvantages of OSPF like, it requires an extra CPU process to run the SPF algorithm, requiring more RAM to store adjacency topology, and being more complex to set up and hard to troubleshoot.

PROGRAM 1: (We get the following topology)

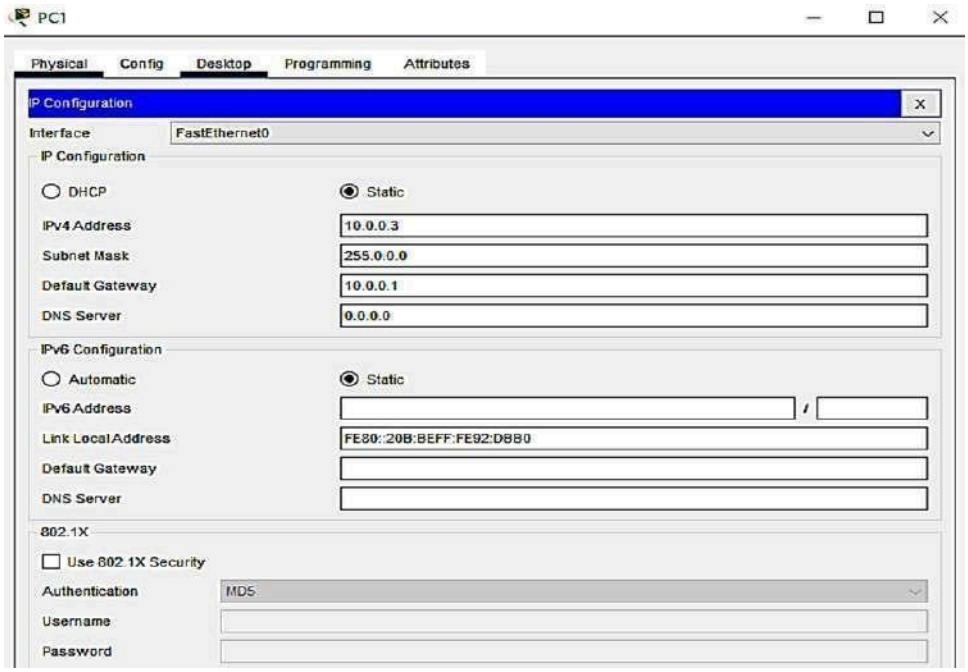


PROGRAM 2:

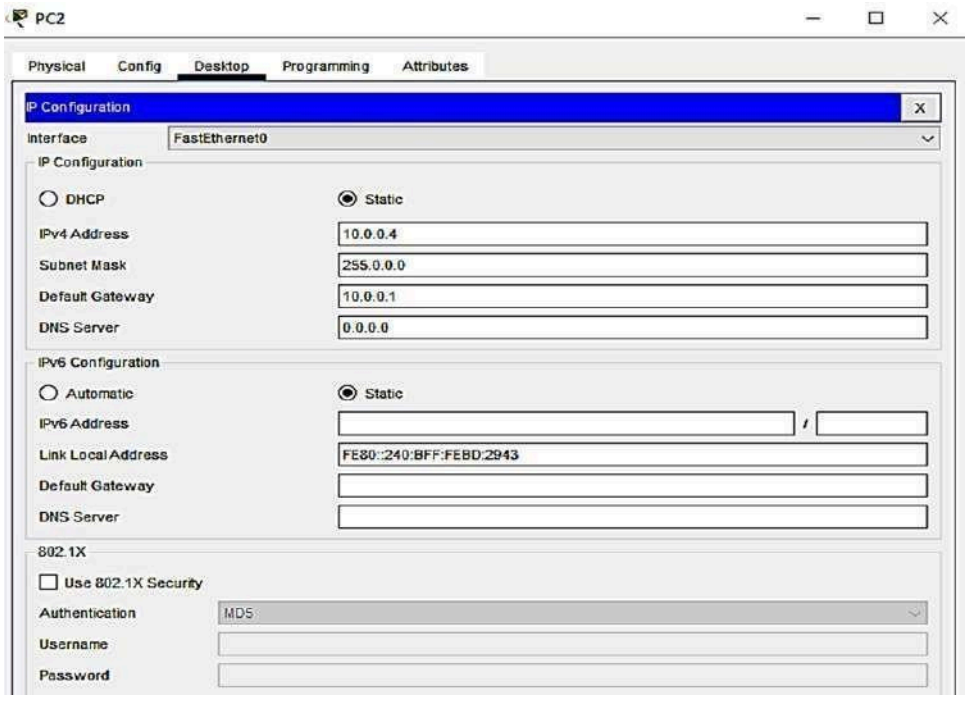
2(A): Now configure the PC 0 IP Address



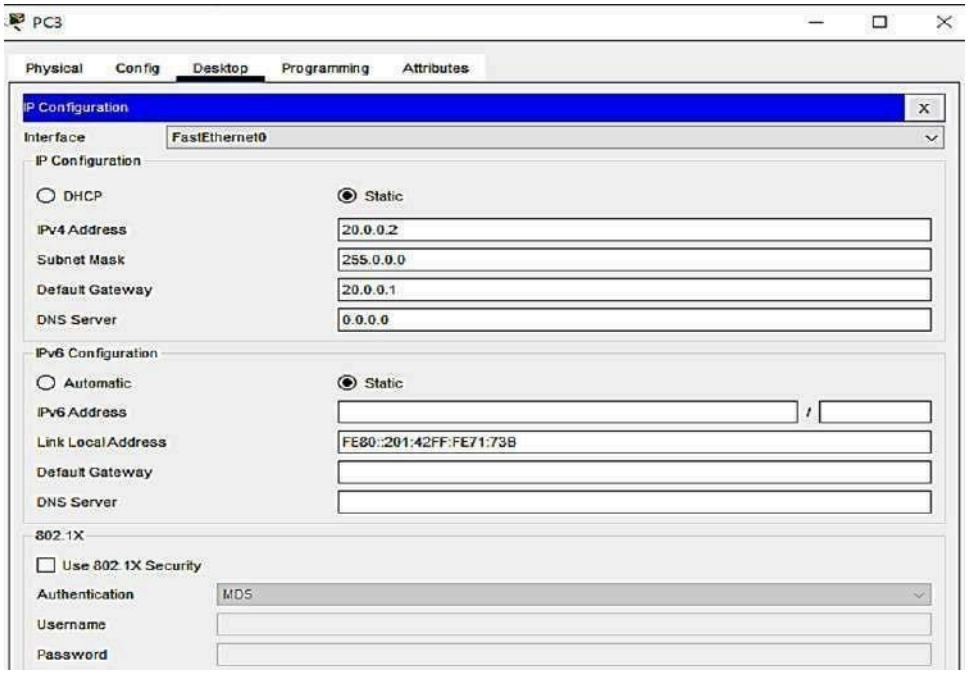
2(B): Now configure the PC 0 IP Address



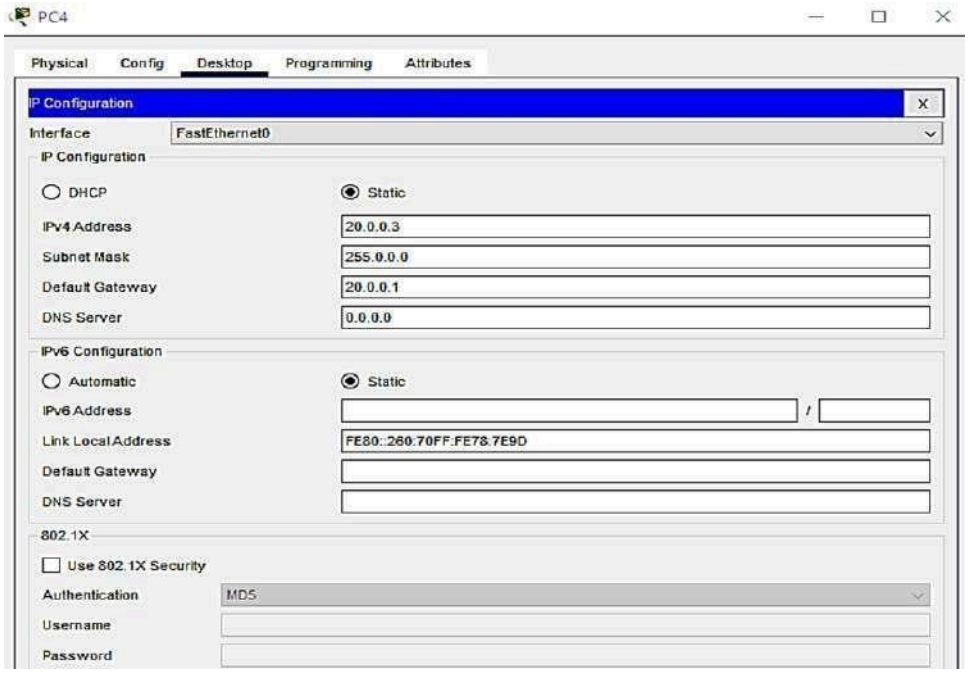
2(C): Now configure the PC 0 IP Address



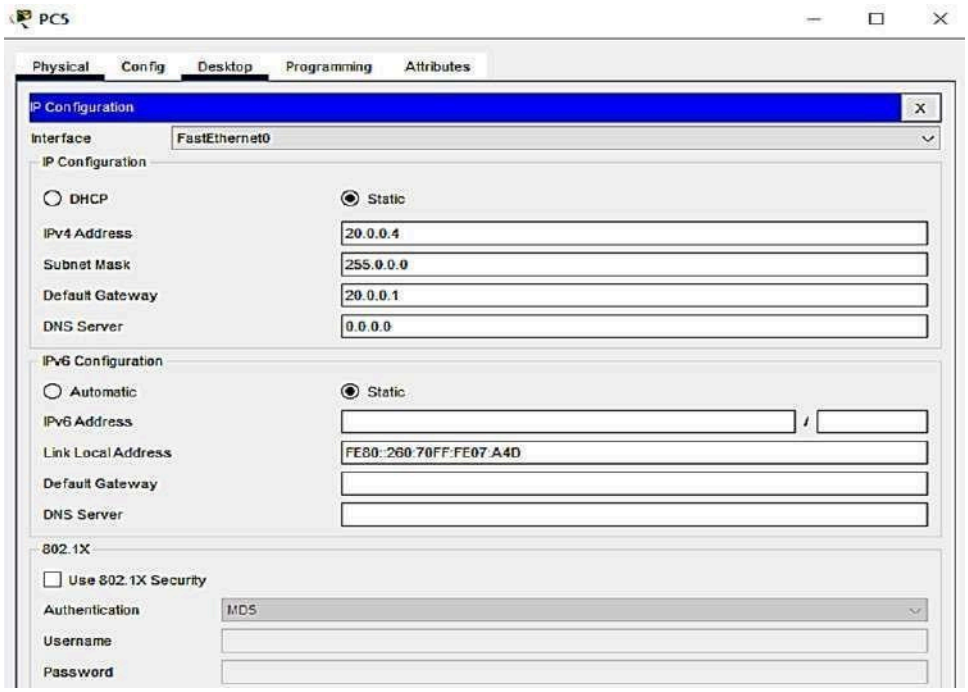
2(D): Now configure the PC 0 IP Address



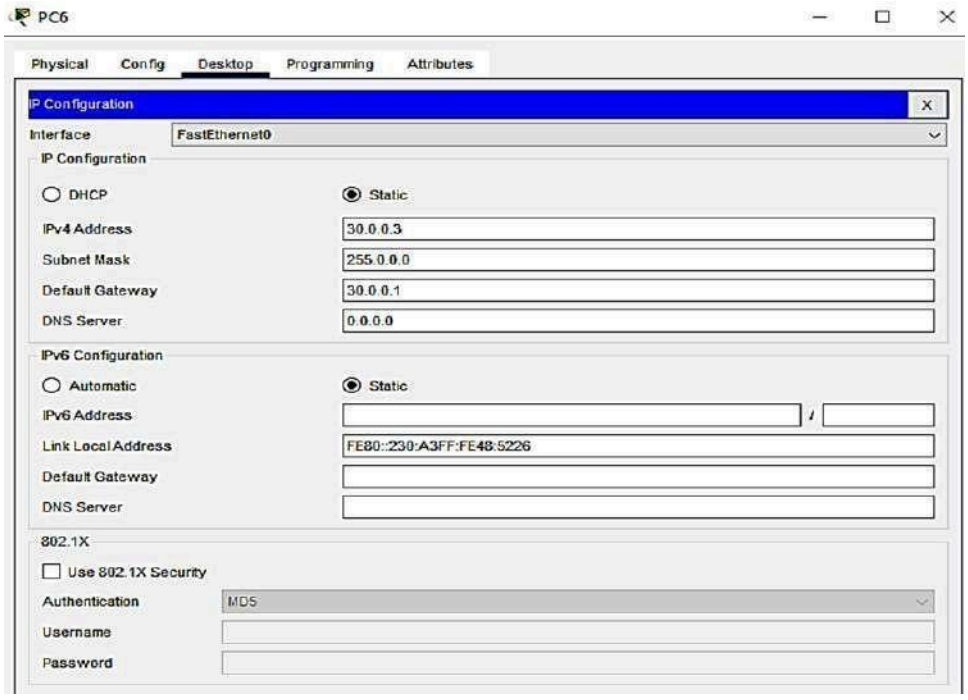
2(E): Now configure the PC 0 IP Address



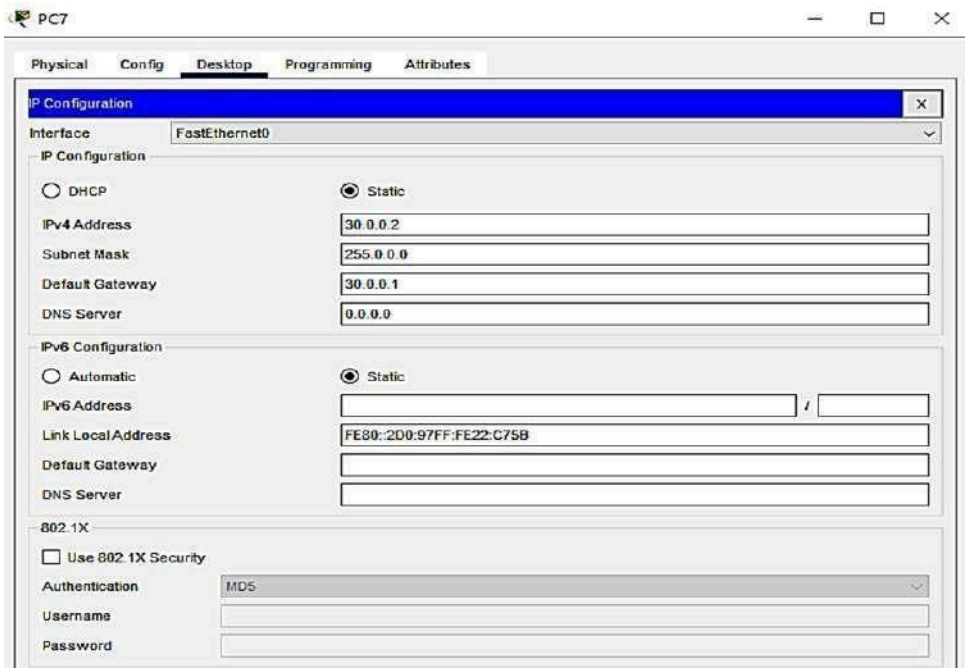
2(F): Now configure the PC 0 IP Address



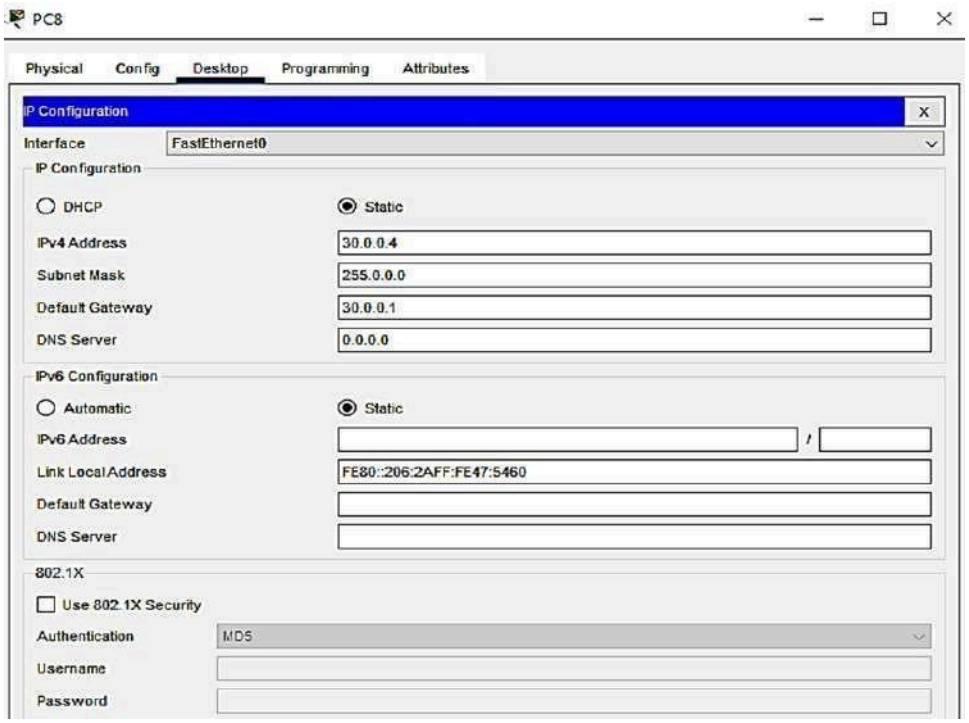
2(G): Now configure the PC 0 IP Address



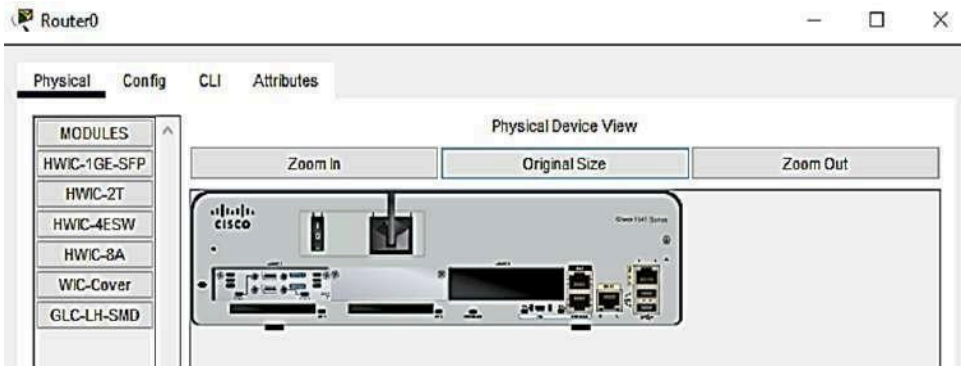
2(H): Now configure the PC 0 IP Address



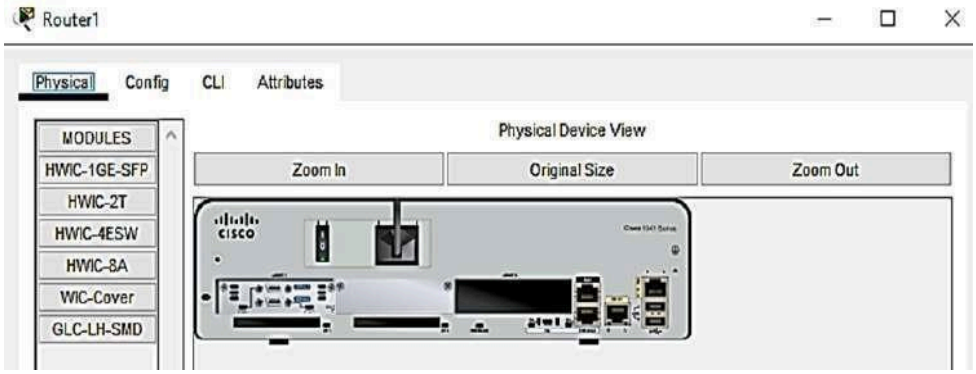
2(I): Now configure the PC 0 IP Address



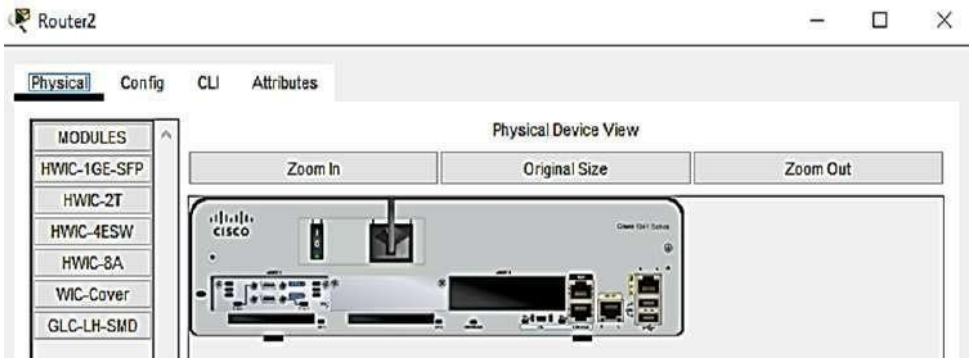
PROGRAM 3: Now in All Router's Physical Section add the Serial Interface of : HWIC-2T



3(B): Router 1



3(C): Router 2

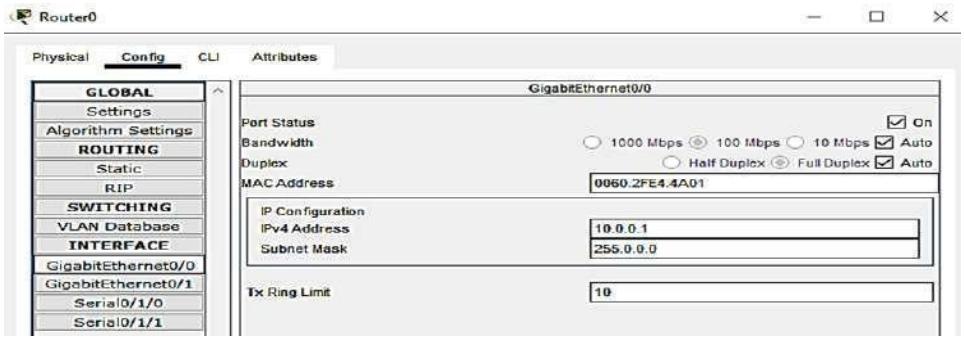


Remember You have to OFF the switch while adding Serial Interface and ON the Switch after adding the interface in all the Routers

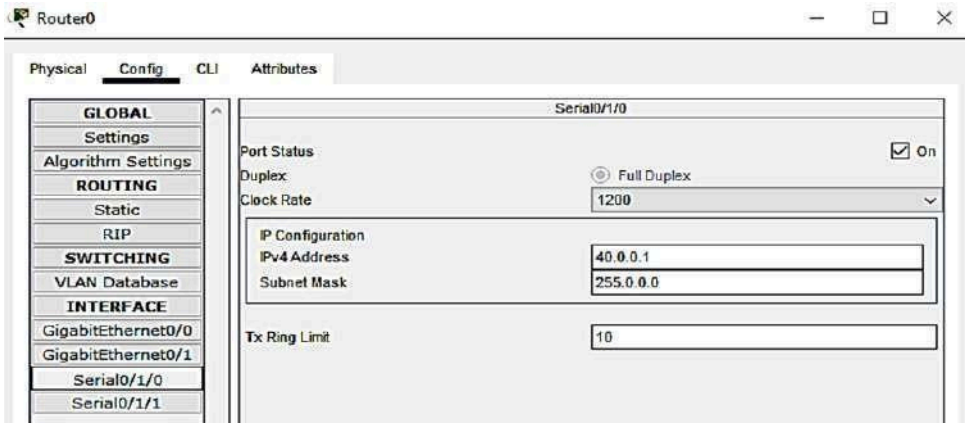
PROGRAM 4: (**Now Configure IP Address on all the router)**

4(A): Router 0

(i) GigabitEthernet 0/0

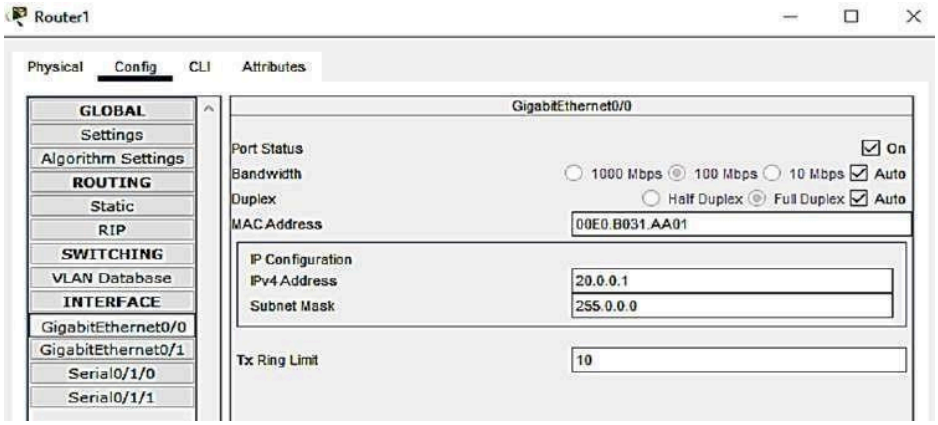


(ii) Serial 0/1/0

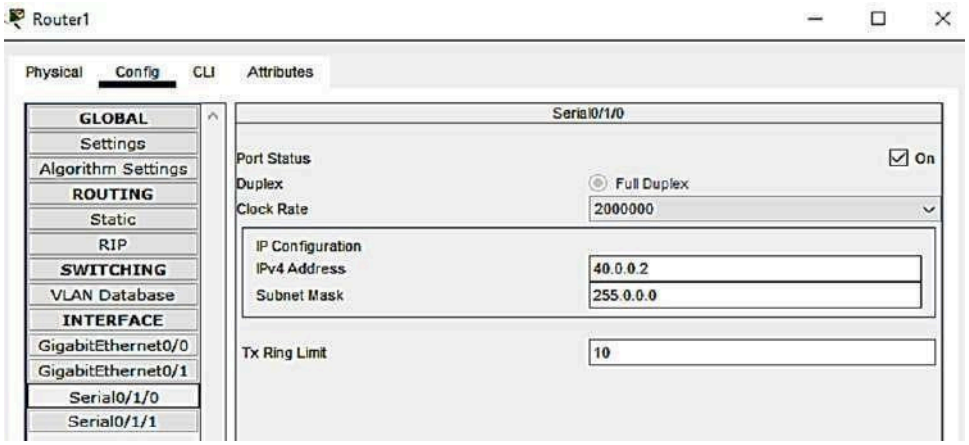


4(B): Router 1

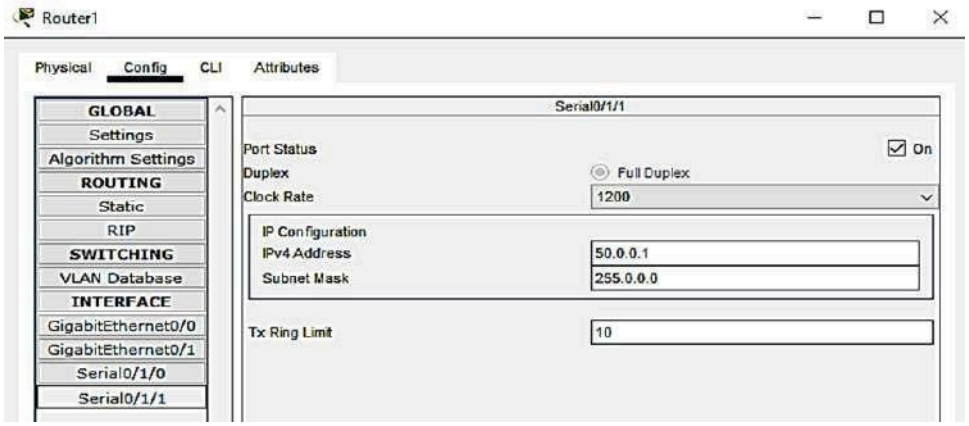
(i) GigabitEthernet 0/0



(ii) Serial 0/1/0

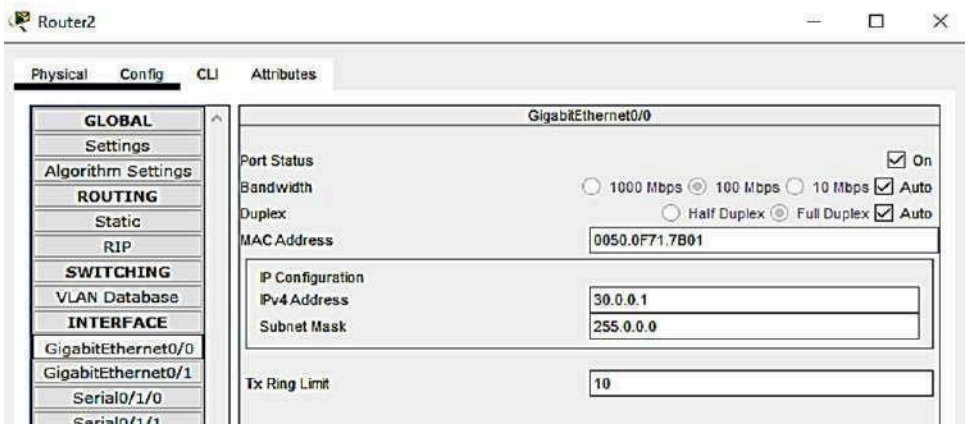


(iii) Serial 0/1/1

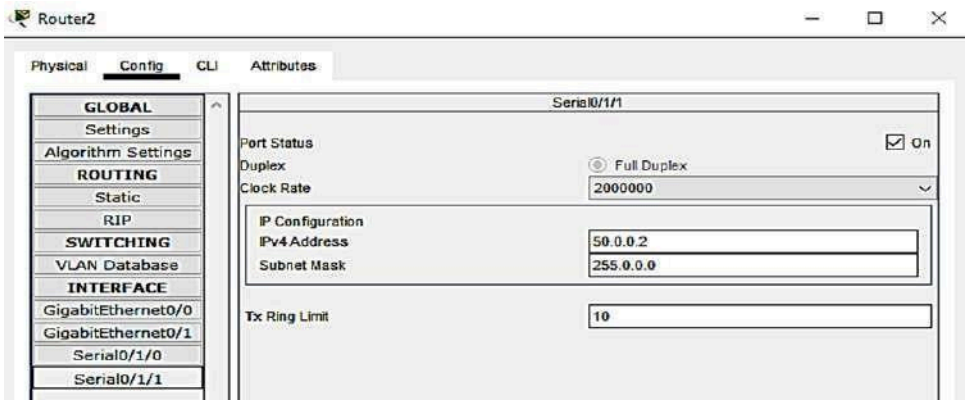


4(C): Router 2

(i) GigaabitEthernet 0/0

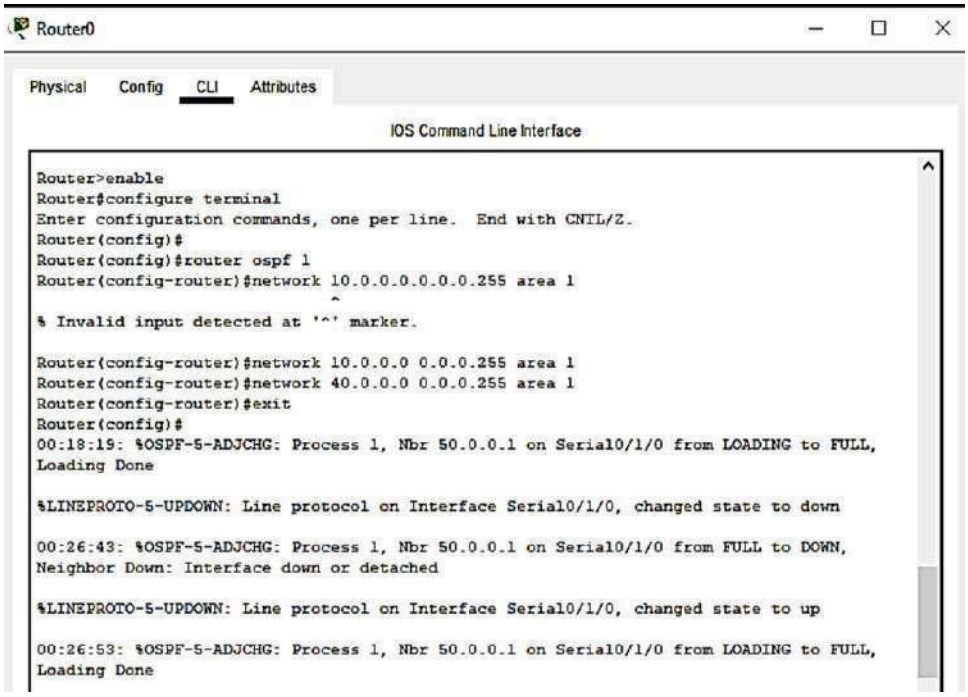


(ii) Serial 0/1/1

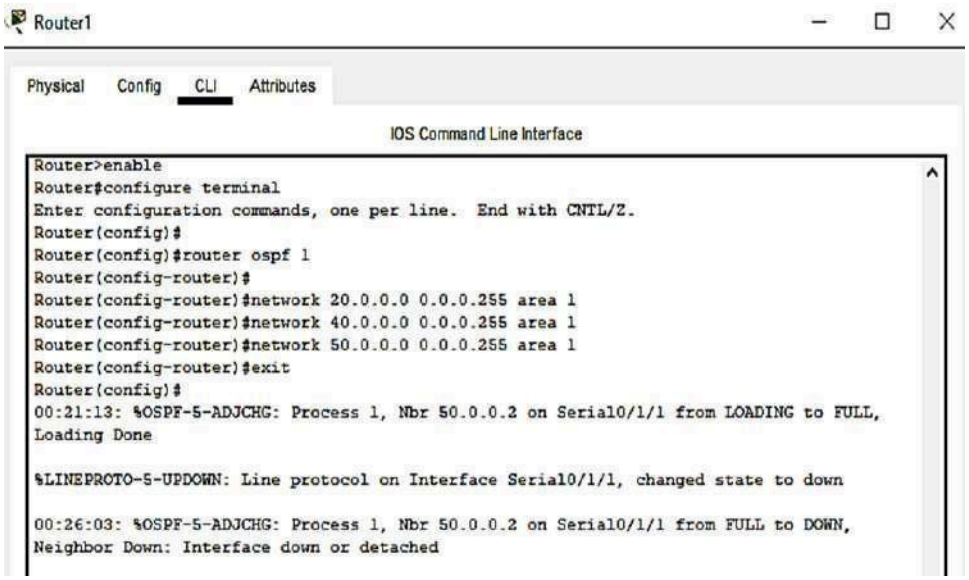


<u>PROGRAM 5:</u> Now Configure All the Router with (CLI Mode)

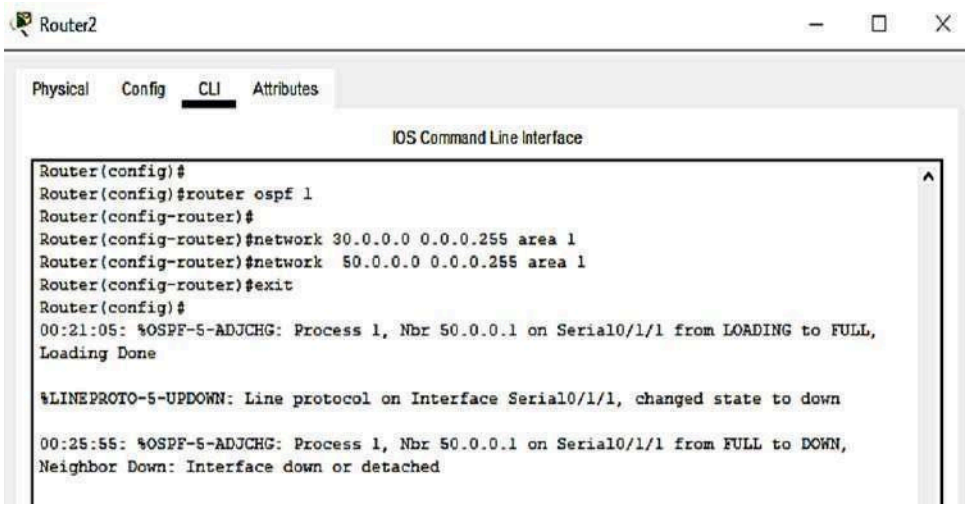
<u>5(A):</u> Router 0



5(B): Router 1

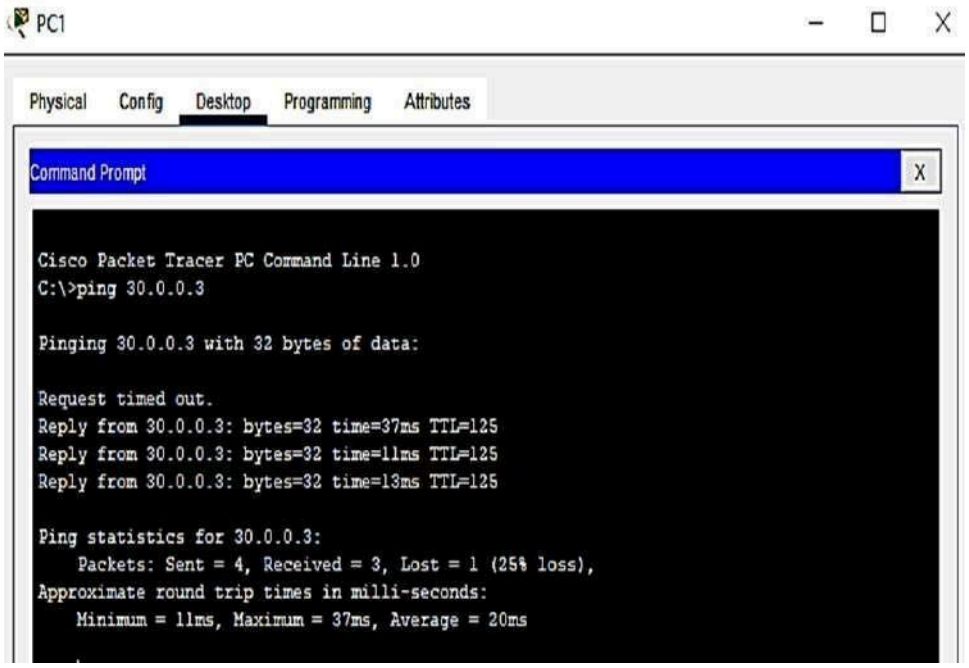


5(C): Router 2

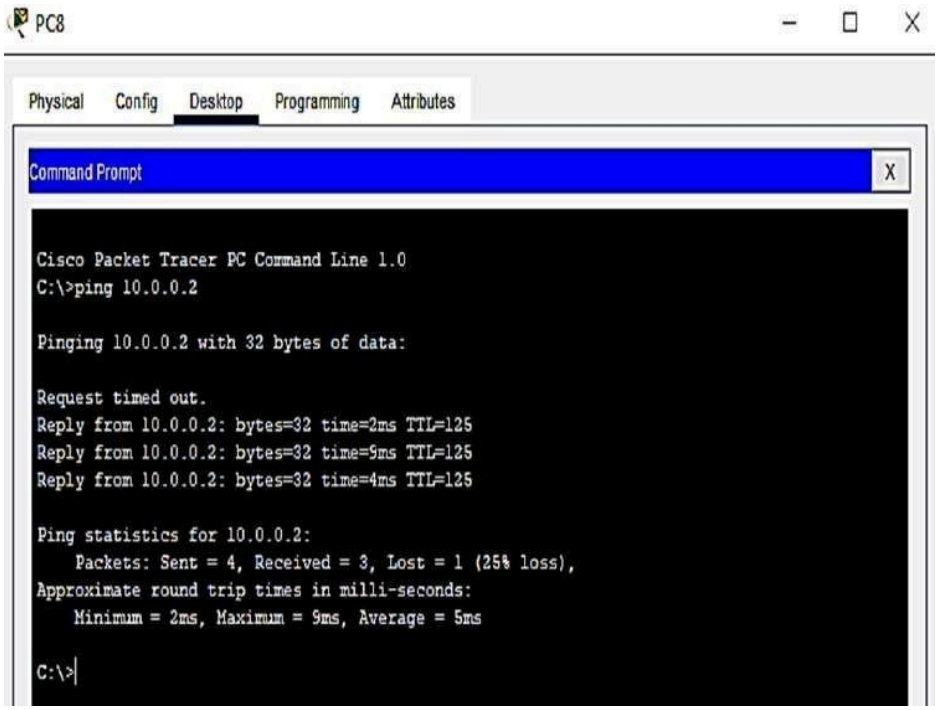


<u>PROGRAM 6:</u> (**Now check the connectivity by using ping command with CMD)**

<u>6(A):</u> PC 0 : ping 30.0.0.3



<u>6(B):</u> PC 8 : ping 10.0.0.2


PC8
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2
Pinging 10.0.0.2 with 32 bytes of data:
Request timed out.
Reply from 10.0.0.2: bytes=32 time=2ms TTL=125
Reply from 10.0.0.2: bytes=32 time=9ms TTL=125
Reply from 10.0.0.2: bytes=32 time=4ms TTL=125
Ping statistics for 10.0.0.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 9ms, Average = 5ms
C:\>

Practical No.8

AIM: **Using Packet Tracer, create a network with three routers with BGP and each router associated network will have minimum three PC. Show Connectivity.**

THEORY:

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

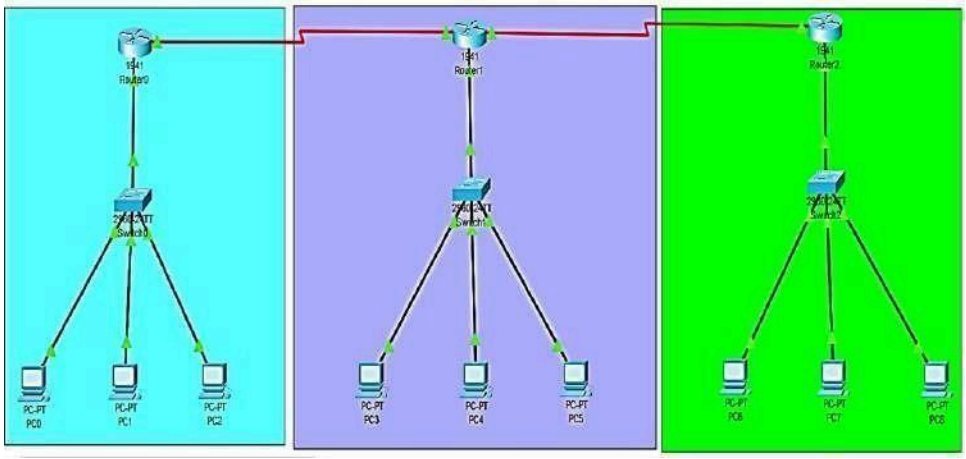
The protocol can connect together any internetwork of autonomous system using an arbitrary topology. The only requirement is that each AS have at least one router that is able to run BGP and that is router connect to at least one other AS's BGP router.

BGP's main function is to exchange network reach-ability information with other BGP systems.

Characteristics of Border Gateway Protocol (BGP):

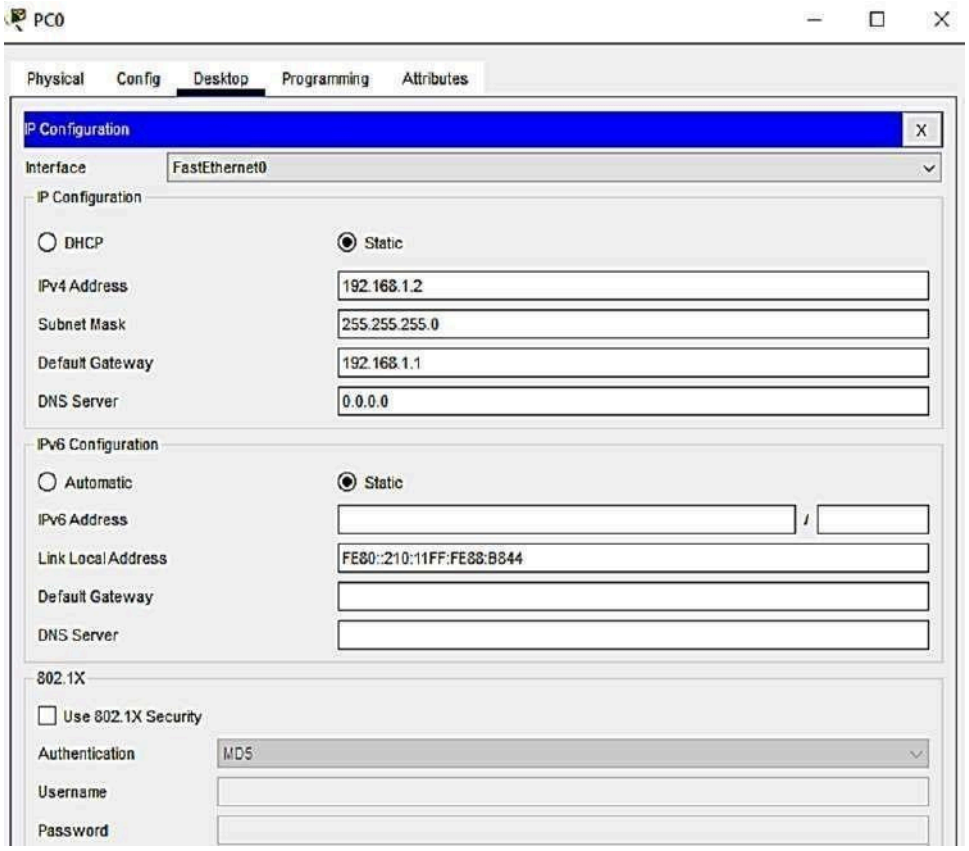
1. a) The main role of BGP is to provide communication between two autonomous systems.
2. b) BGP supports Next-Hop Paradigm.
3. c) Coordination among multiple BGP speakers within the AS (Autonomous System).
4. d) BGP advertisement also include path information, along with the reachable destination and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

PROGRAM 1: (We got the following topology)

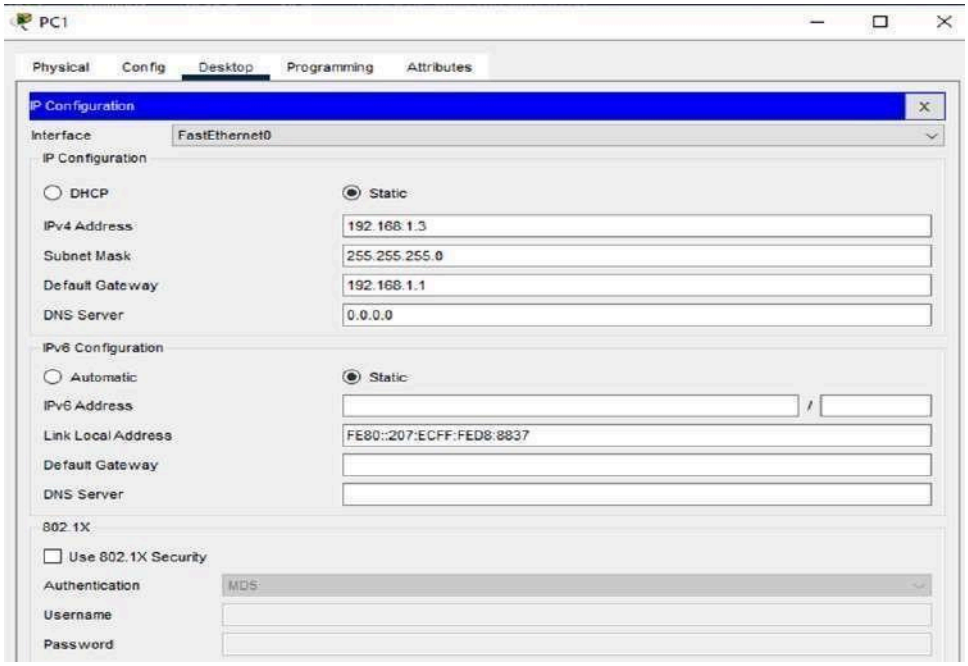


PROGRAM 2:

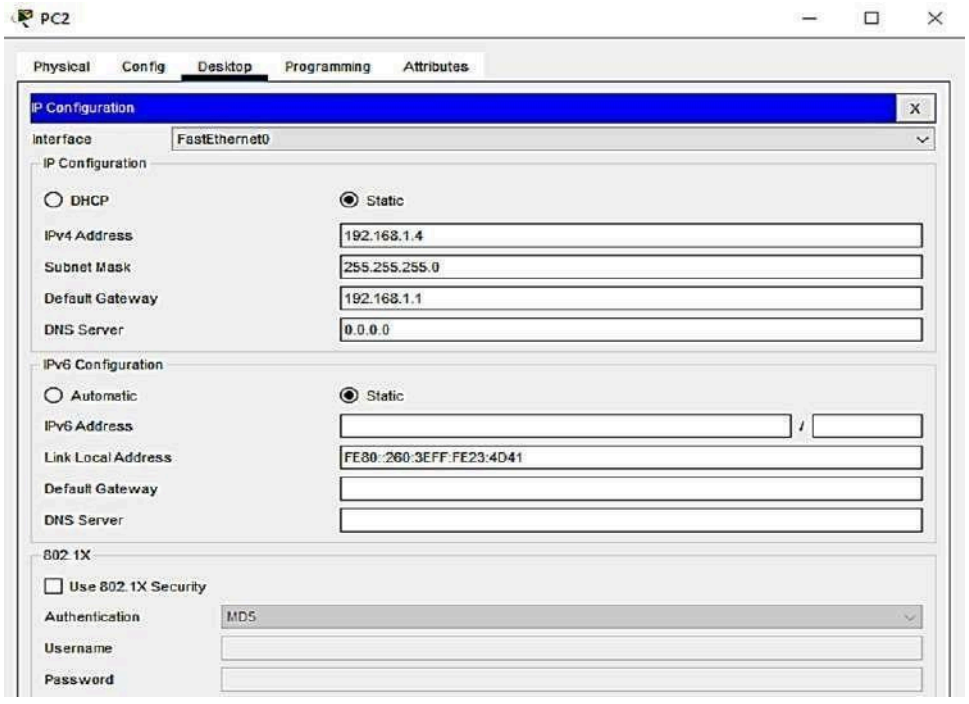
2(A): Now configure the PC 0 IP Address



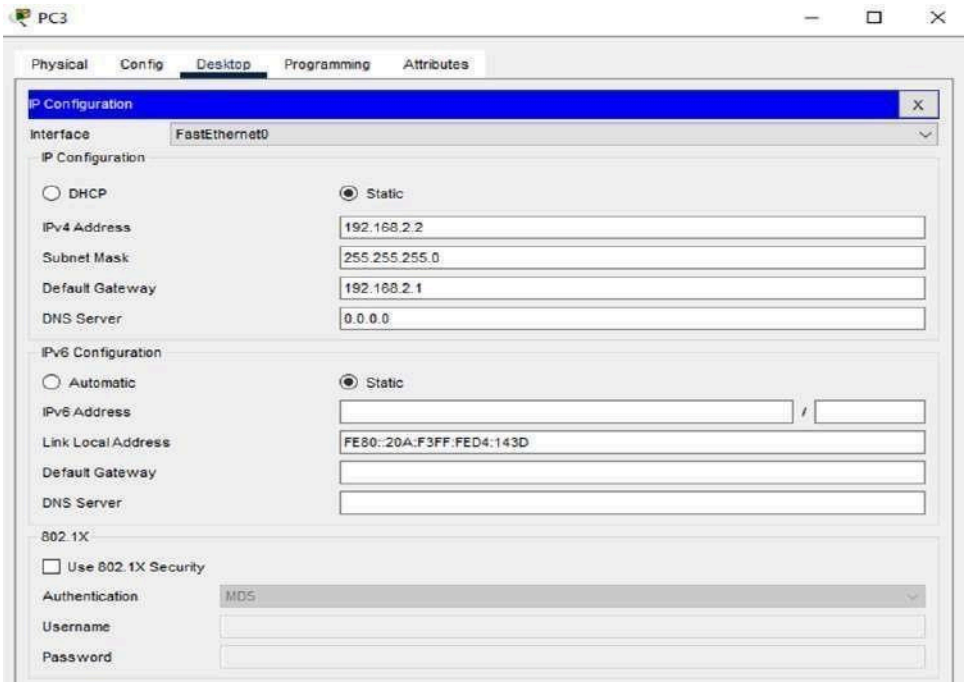
2(B): Now configure the PC 1 IP Address



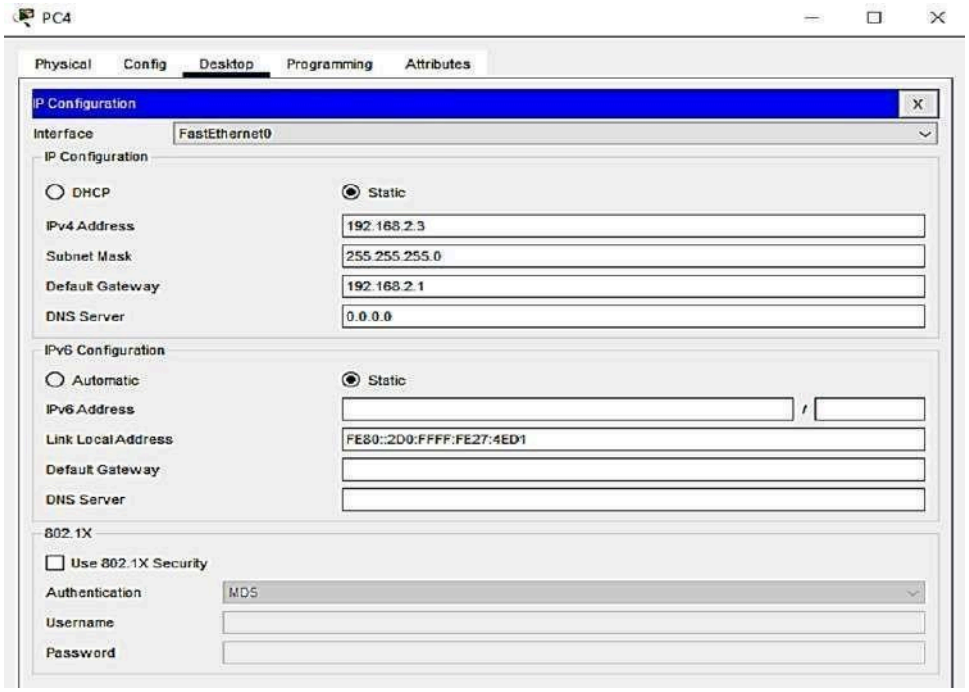
2(C): Now configure the PC 2 IP Address



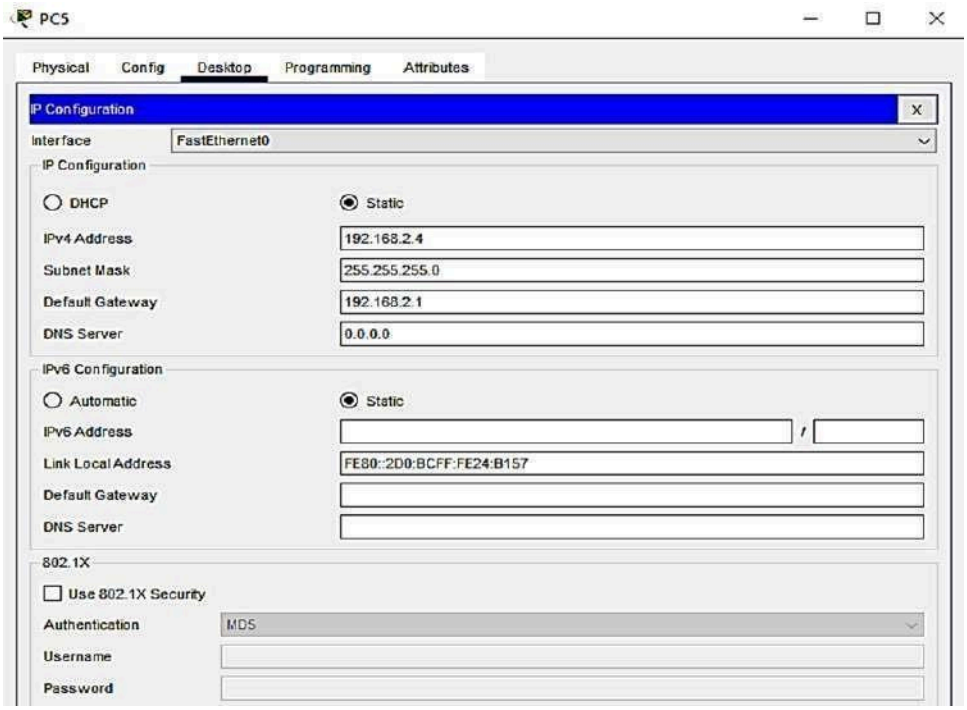
2(D): Now configure the PC 3 IP Address



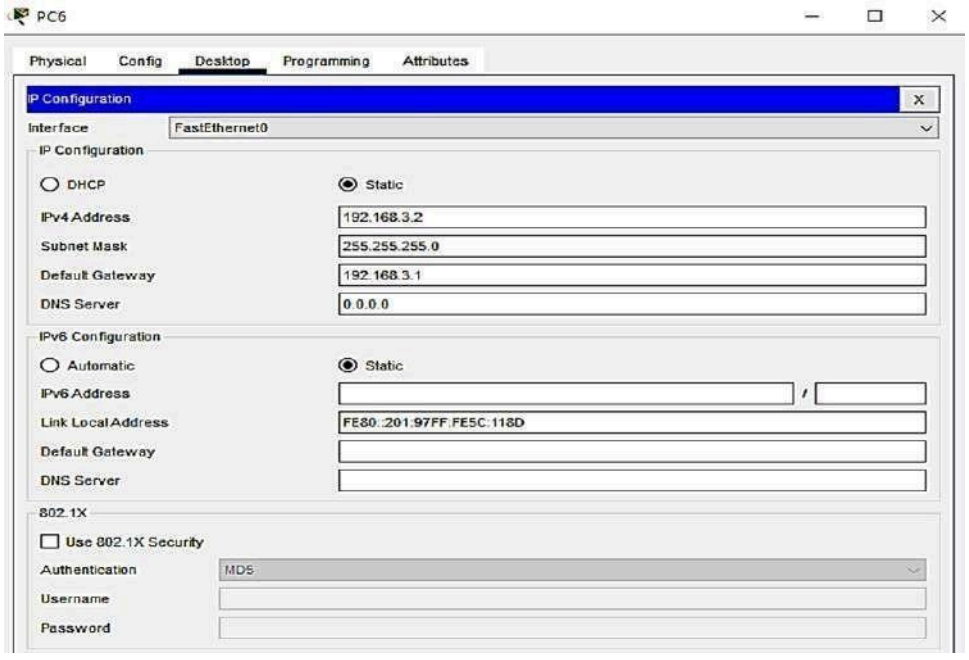
2(E): Now configure the PC 4 IP Address



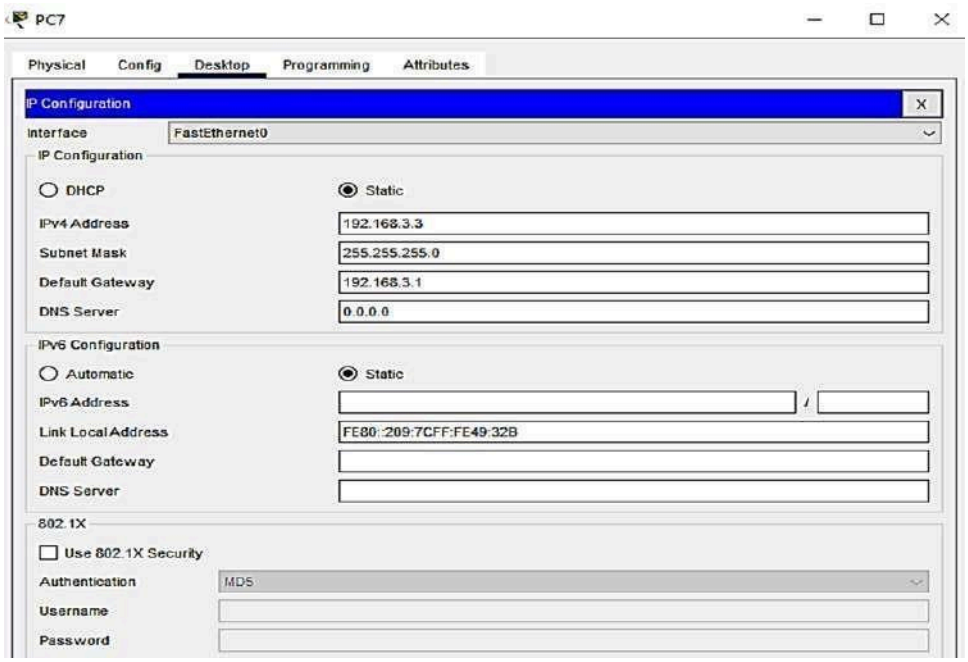
2(F): Now configure the PC 5 IP Address



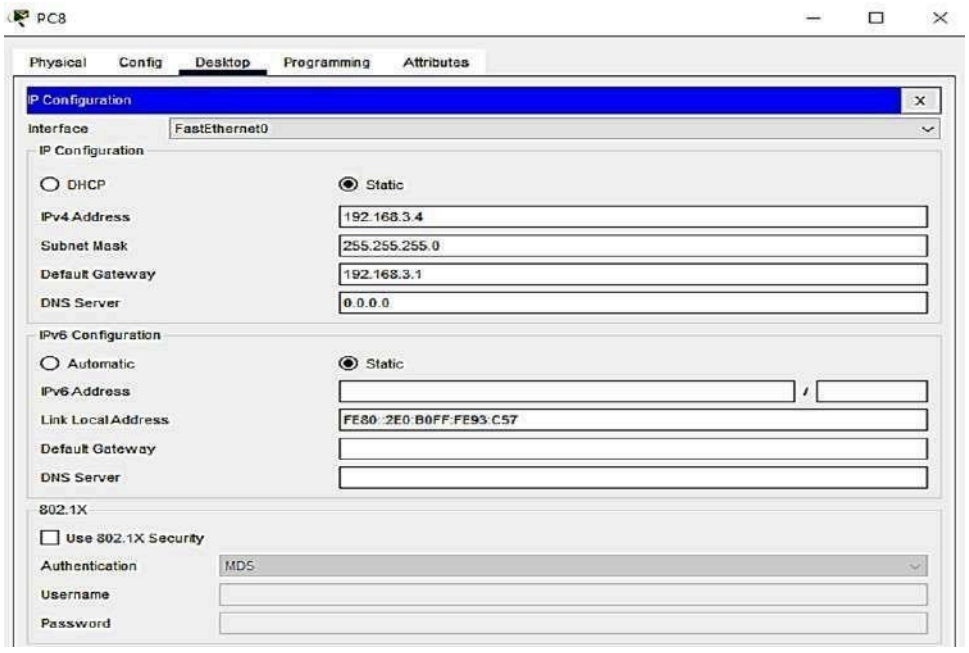
2(G): Now configure the PC 6 IP Address



2(H): Now configure the PC 7 IP Address

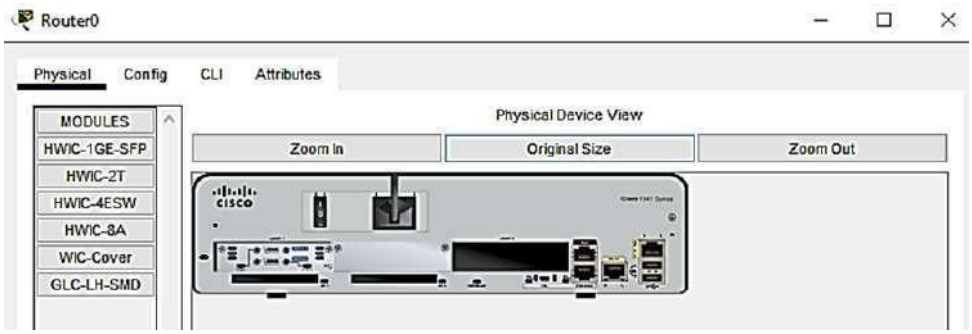


2(I): Now configure the PC 8 IP Address

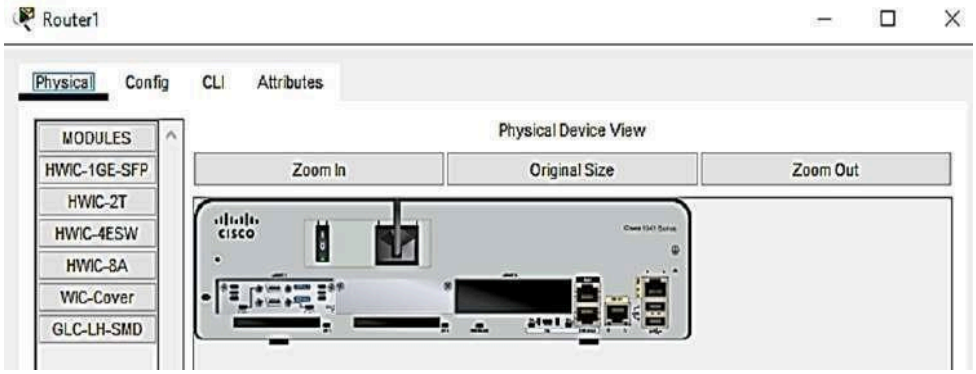


PROGRAM 3: (**Now in All Router's Physical Section add the Serial Interface of : HWIC-2T)**

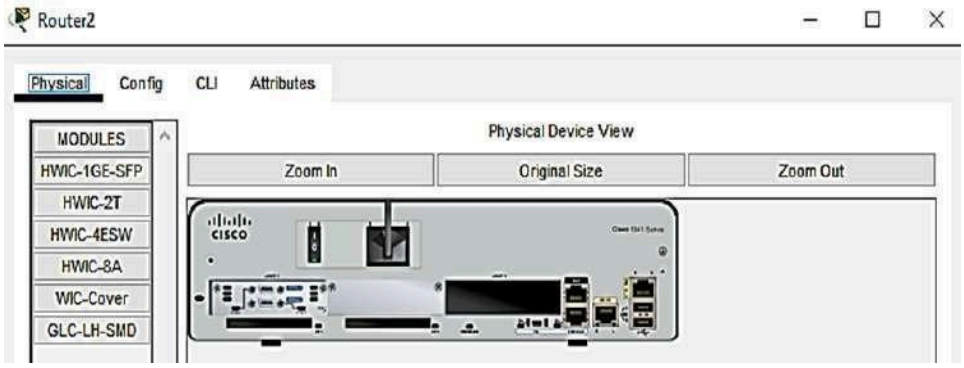
3(A): Router 0



3(B): Router 1



3(C): Router 2



Remember You have to OFF the switch while adding Serial Interface and ON the Switch after adding the interface in all the Routers

PROGRAM 4: (Now configure All the Router with (CLI Mode)

4(A): Router 0

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

4(B): Router 1

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

4(C): Router 2 Router>enable

Router#configure terminal

Router(config)#

Router(config)#router bgp

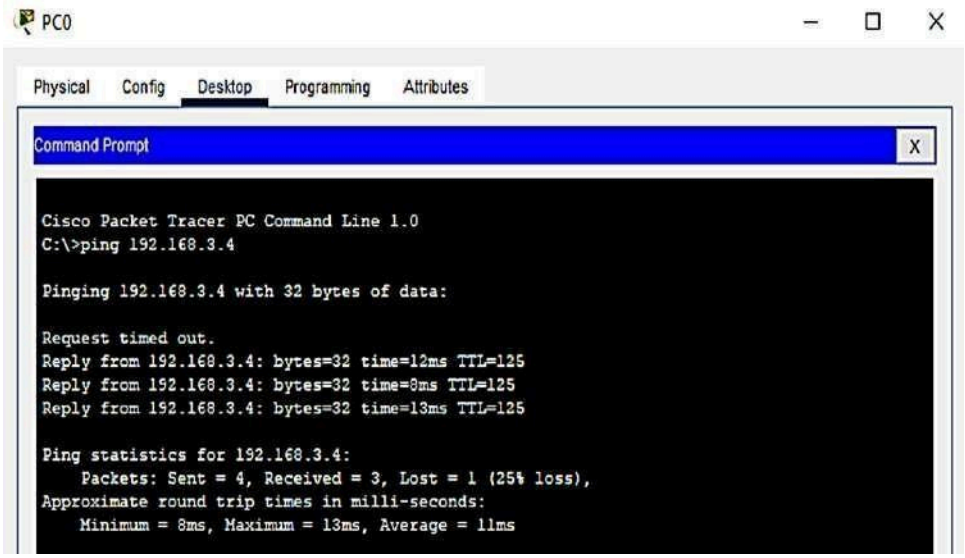
3000 Router(config-router)#

Router(config-router)#network 20.0.0.0

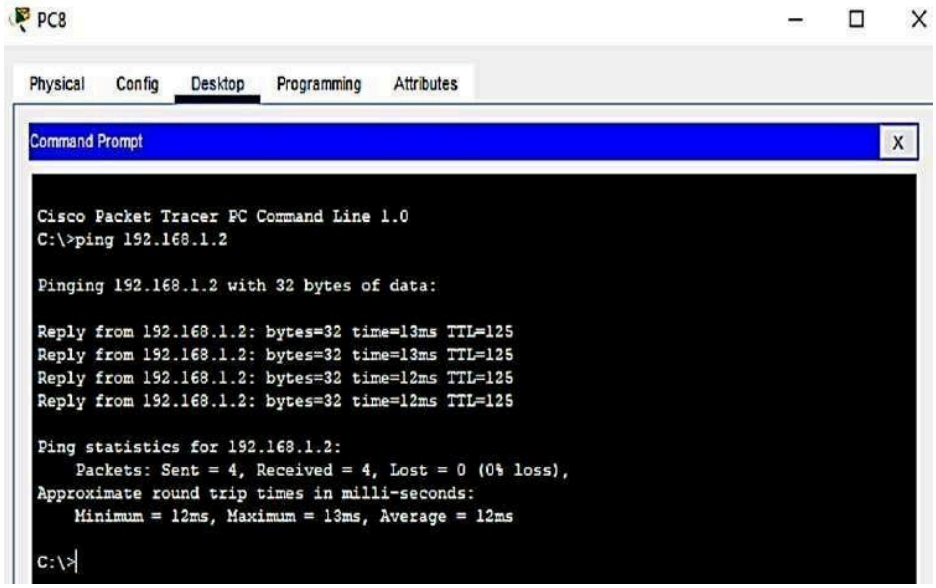
Router(config-router)#network 192.168.3.0

Router(config-router)#neighbor 20.0.0.1 remote-as 2000

Program 6: (**Now check the connectivity by using ping command with CMD) 6(A): PC 0 : ping 192.168.3.4**



6(B): PC 8 : ping 192.168.1.2



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):
4. High cost
5. Poor stability
6. Less Secure
   Application of Wireless Access Point:

   7. It is a device that creates a WLAN (Wireless Local Area Network) in large enterprises.

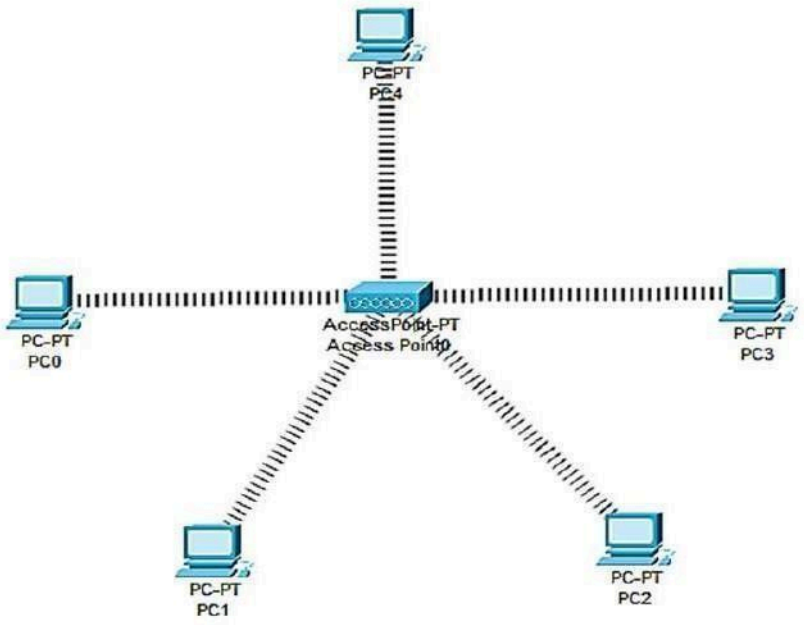
   8. It is used to extend the coverage area of the network so that it can't disconnect which
   allows more users to connect to the network easily.

9. An access point connects a switch, Ethernet cable, wired router, and Wi-fi to designate
the particular area.

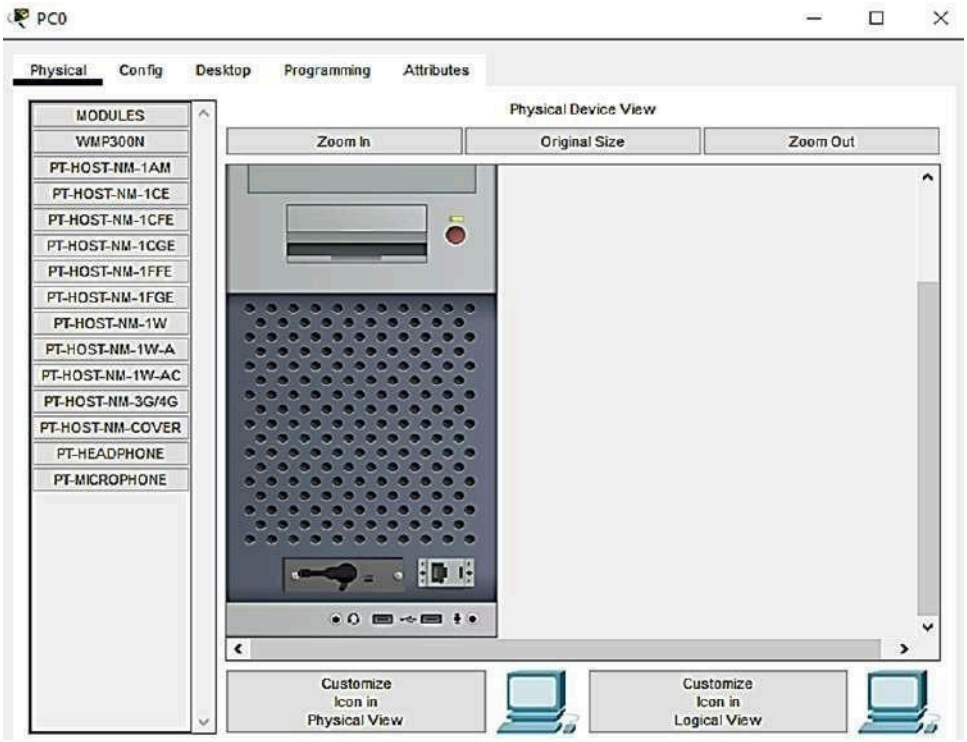
10. It is used to provide connectivity to the users in large offices or enterprises which allows
users to roam easily anywhere in the office and be connected to a network.

11. LANs can also be provided in public places such as coffee shops, restaurants, airports,etc

PROGRAM 1: (We got the following topology)

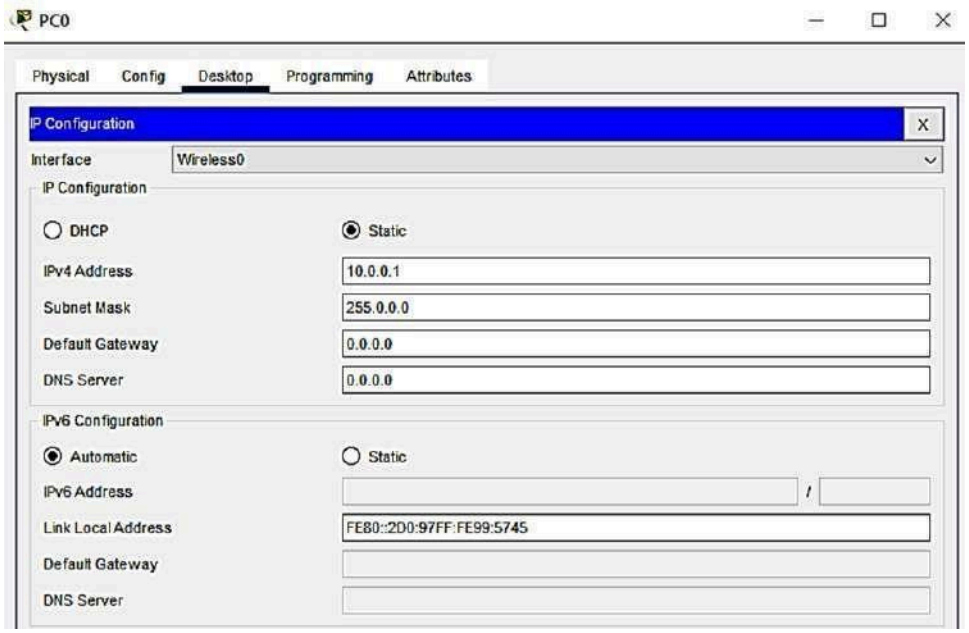


PROGRAM 2: (**Now Change all 5 PC'S Serial Interface from PT-HOST-NM-1CFE to PT-HOST-NM-1W)**

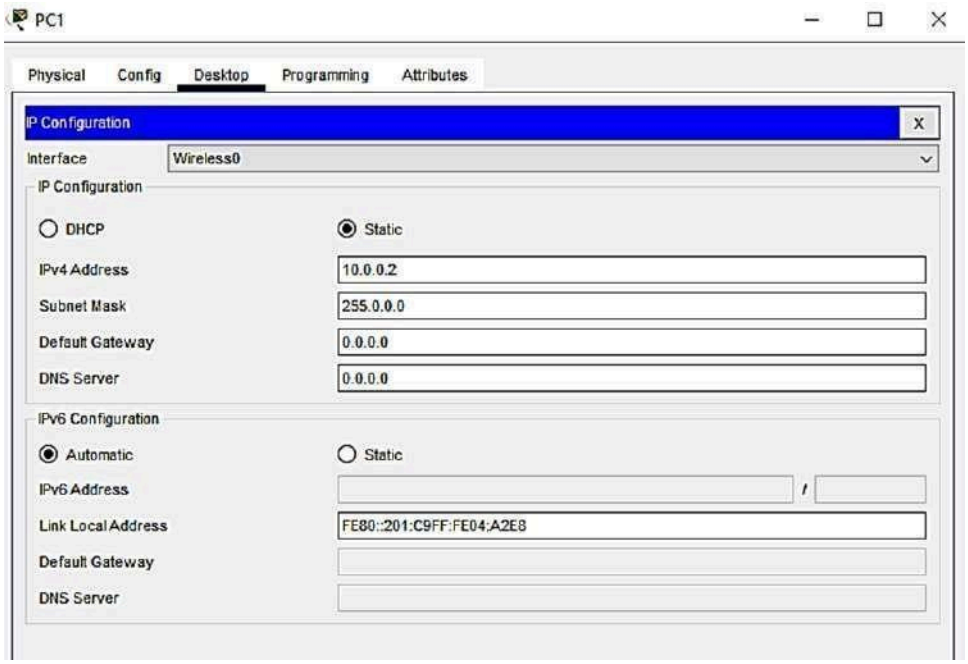


PROGRAM 3:

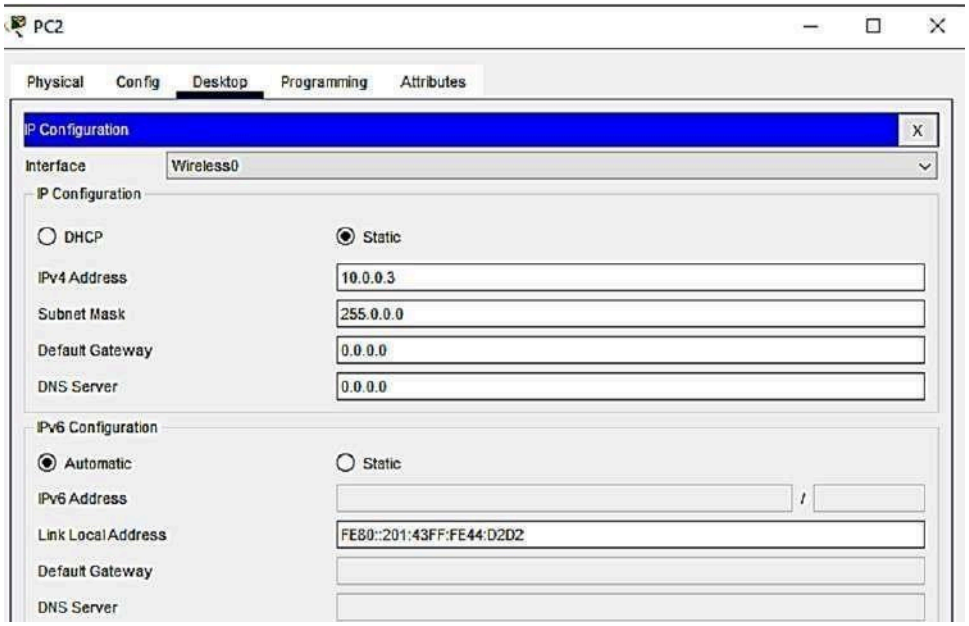
3(A): Now configure the PC 0 IP Address



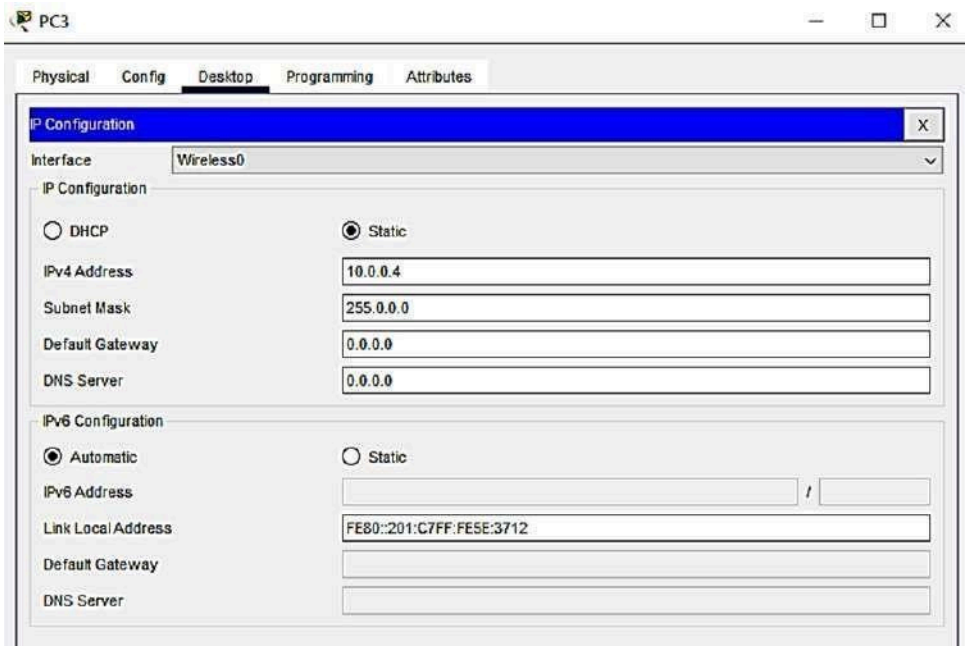
3(B): Now configure the PC 1 IP Address



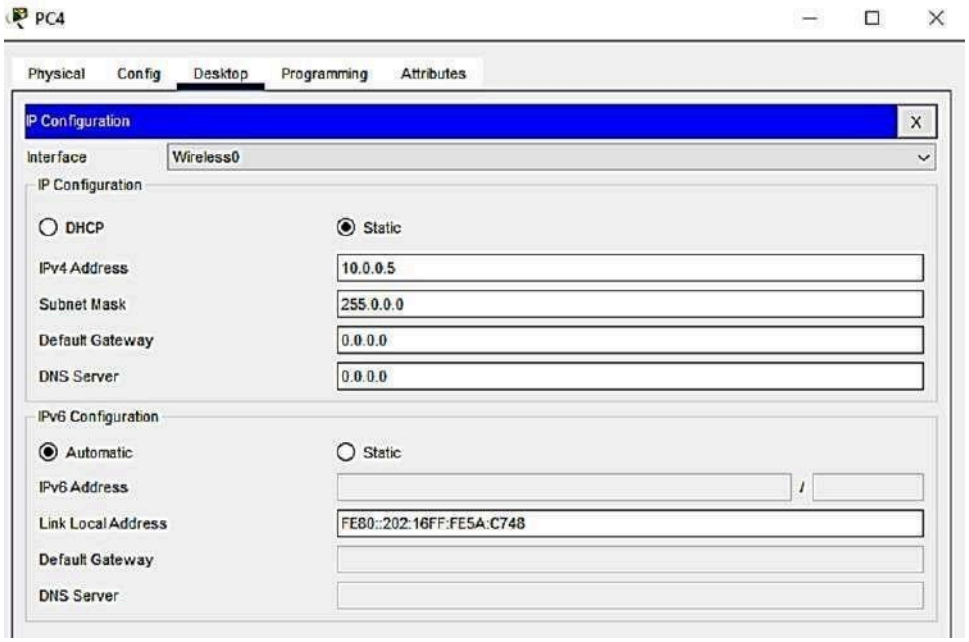
3(C): Now configure the PC 2 IP Address



3(D): Now configure the PC 3 IP Address

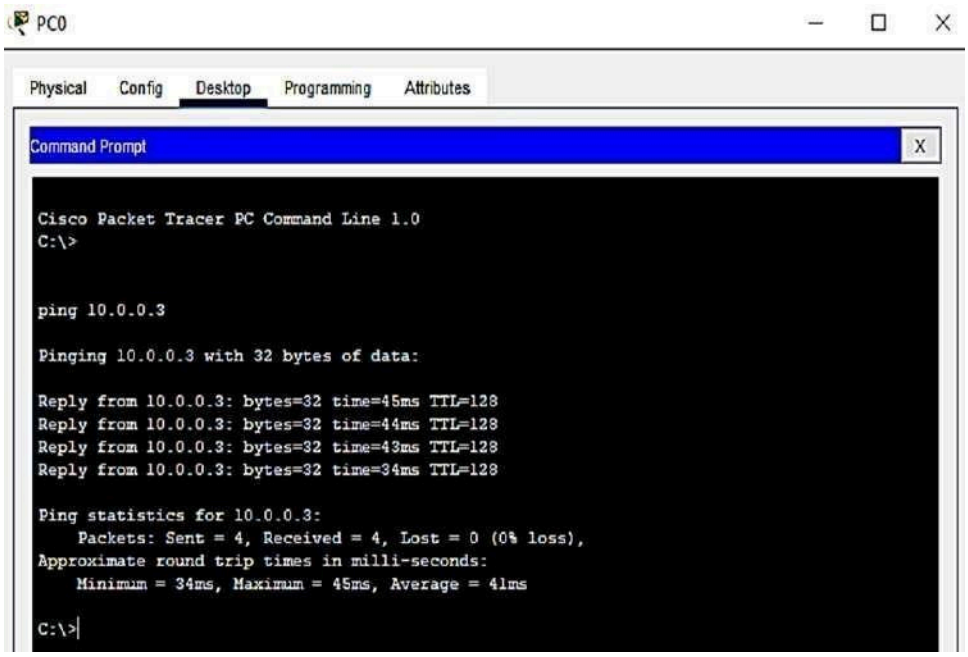


3(E): Now configure the PC 4 IP Address

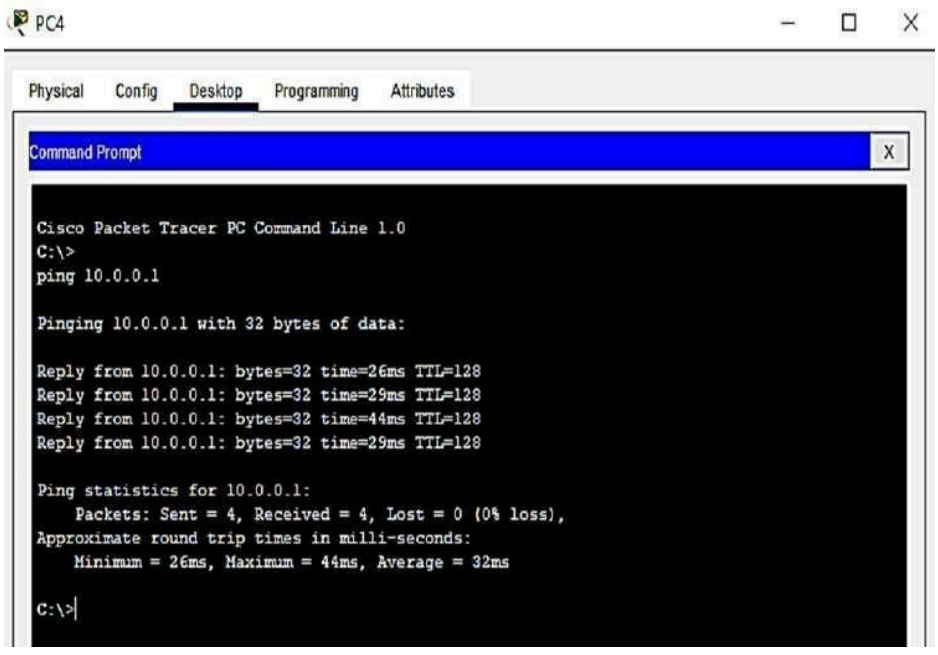


3(F): Now check the connectivity by using ping command with CMD

(i) PC 0 : ping 10.0.0.3


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>
ping 10.0.0.3
Pinging 10.0.0.3 with 32 bytes of data:
Reply from 10.0.0.3: bytes=32 time=45ms TTL=128
Reply from 10.0.0.3: bytes=32 time=44ms TTL=128
Reply from 10.0.0.3: bytes=32 time=43ms TTL=128
Reply from 10.0.0.3: bytes=32 time=34ms TTL=128
Ping statistics for 10.0.0.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 34ms, Maximum = 45ms, Average = 41ms
C:\>

(ii) <u>PC 4 :</u>


PC4
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>
ping 10.0.0.1
Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time=26ms TTL=128
Reply from 10.0.0.1: bytes=32 time=29ms TTL=128
Reply from 10.0.0.1: bytes=32 time=44ms TTL=128
Reply from 10.0.0.1: bytes=32 time=29ms TTL=128
Ping statistics for 10.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 26ms, Maximum = 44ms, Average = 32ms
C:\>