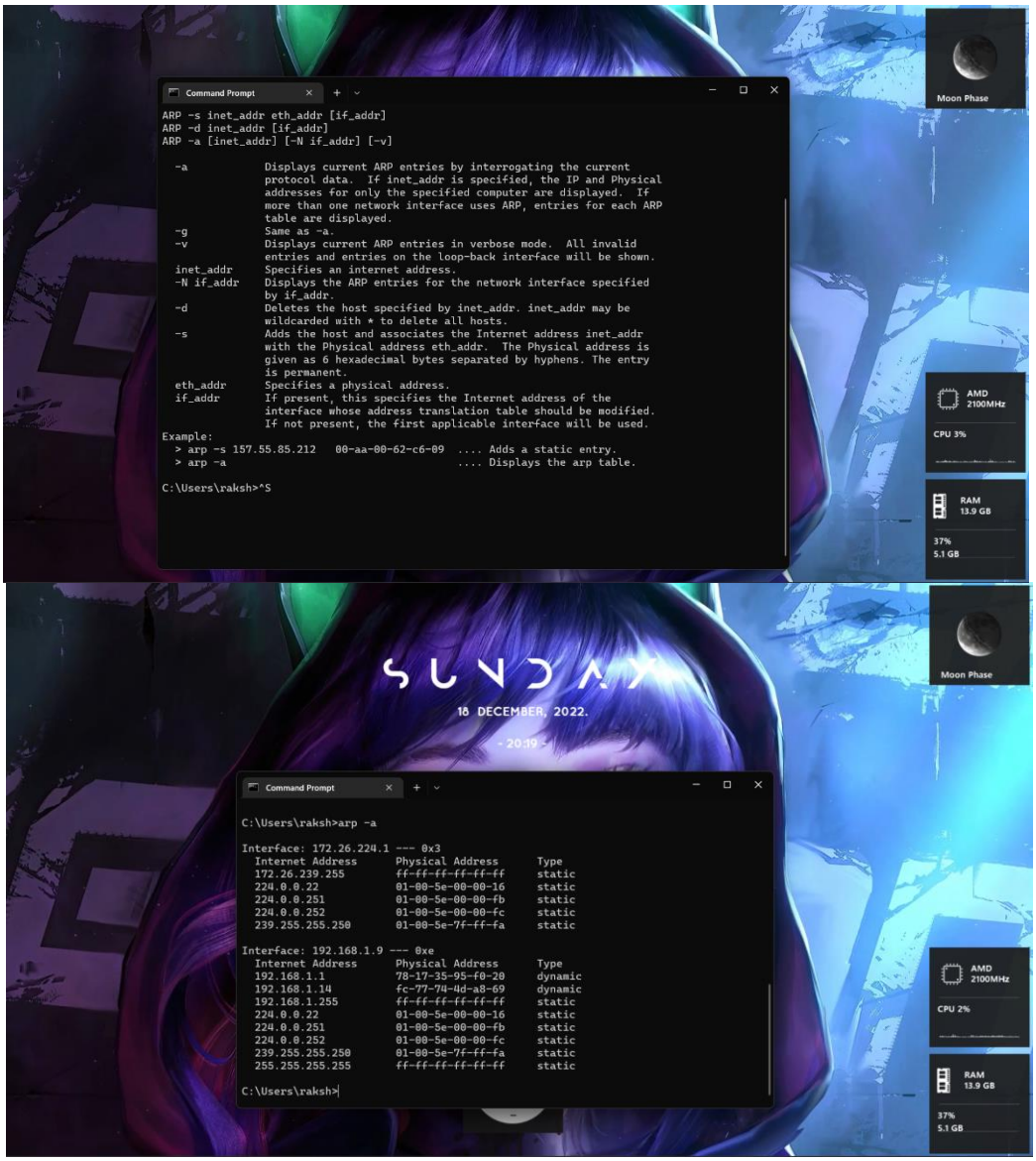
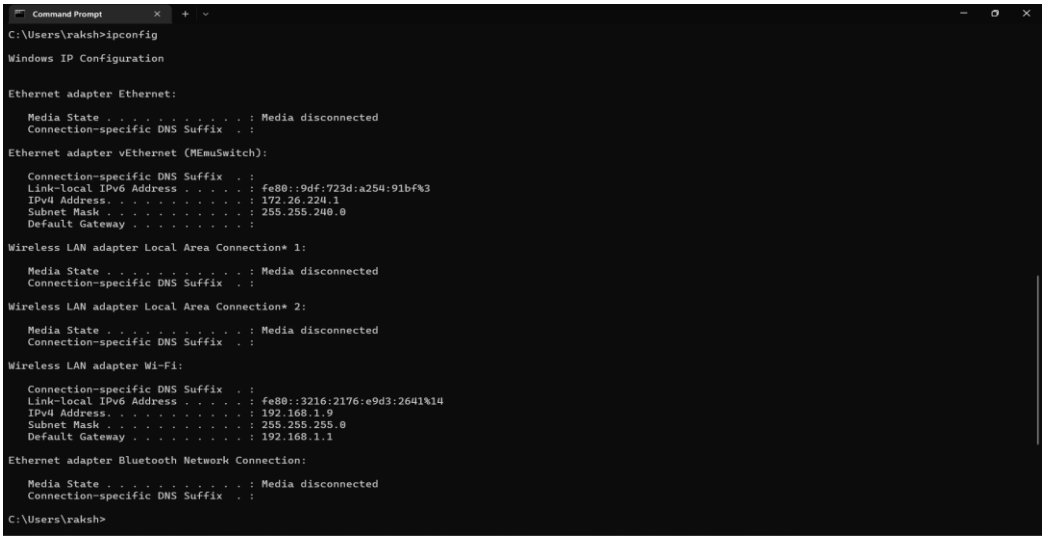
1. Execute the following commands:
   i. arp
   ii. ipconfig
   iii. hostname
   iv. netdiag
   v. netstat
   vi. nslooup
   vii. pathping
   viii. ping route
   ix. tracert

Ans.

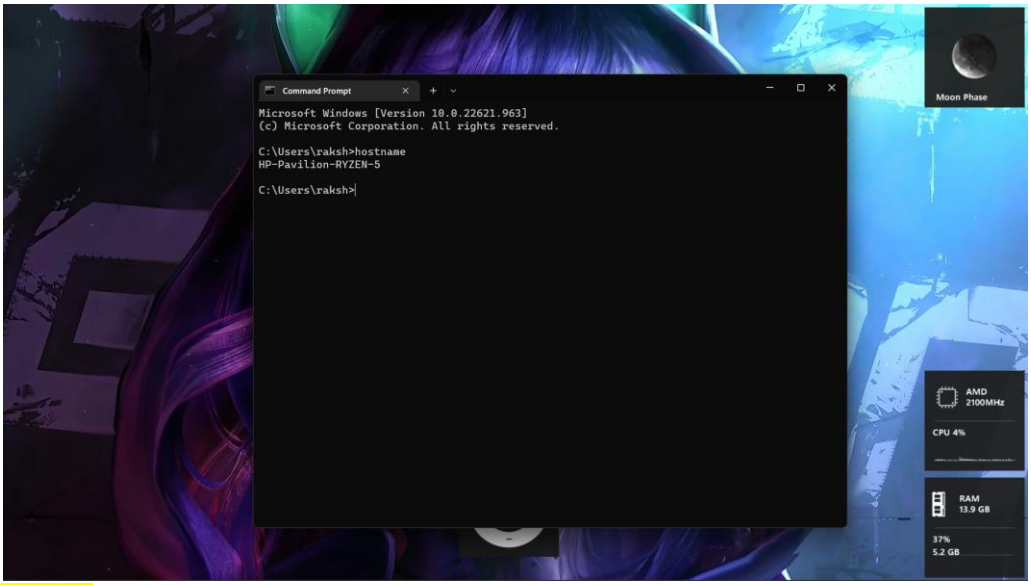
i. arp



ii. ipconfig

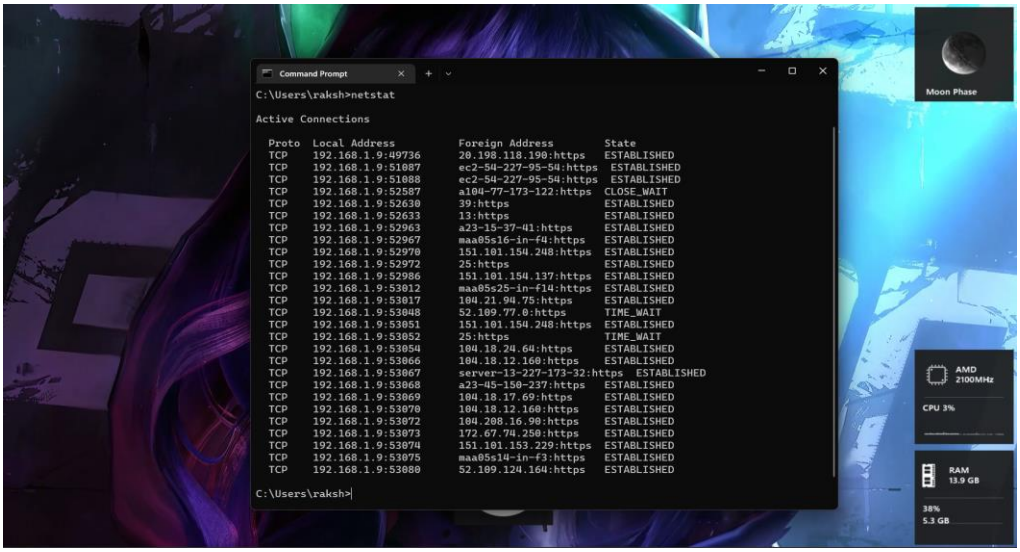


iii. hostname

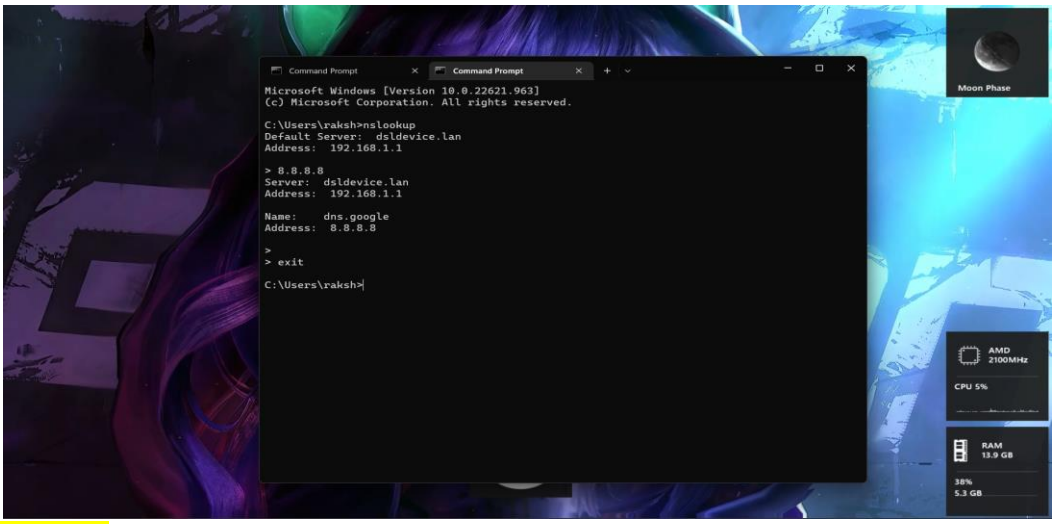


iv. netdiag

v. netstat

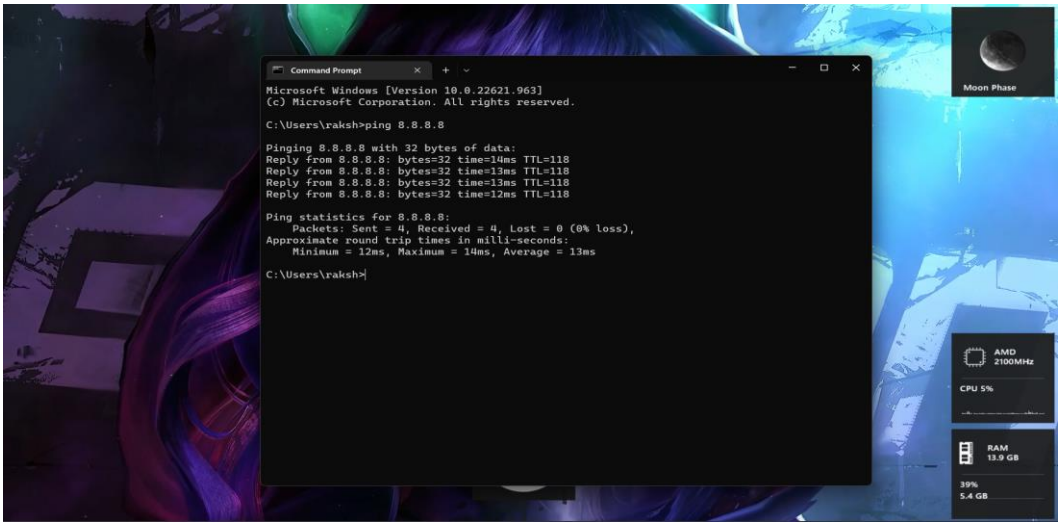


vi. nslooup

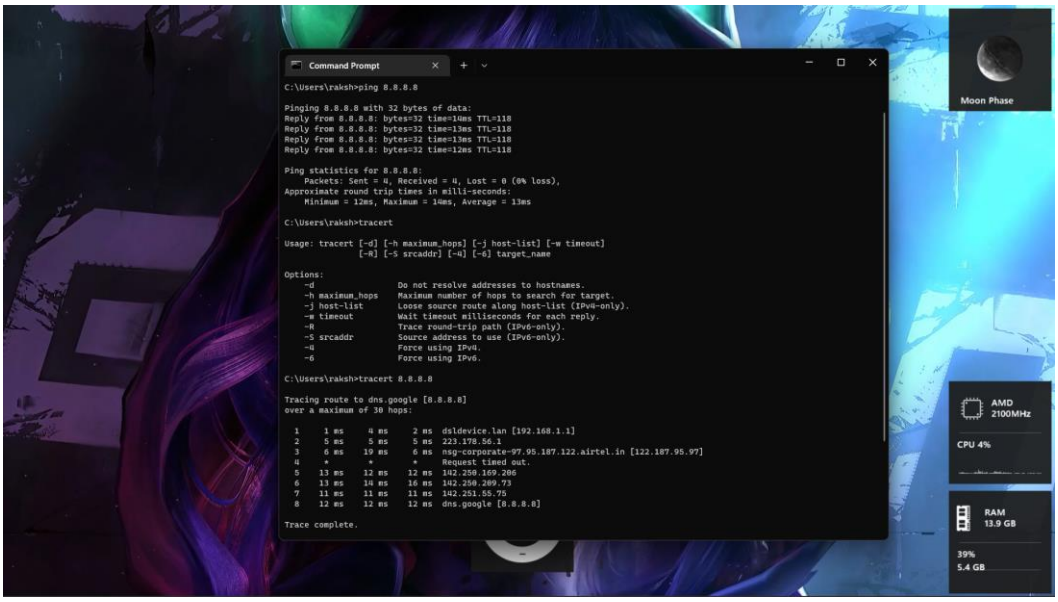


vii. pathping

viii. ping route



ix. tracert



2. Study of different types of network cables

Ans. The function of the media is to carry a flow of information through LAN.

- Wired Media

  Wired communication media are also known as Guided media and are a type of Transmission media. This type of communication is most stable which is why it is considered better than wireless. These connections are less prone to other outer interferences. In wired communication media, wire is used to transfer data from source to destination.

  i. Copper Cable

  Copper wire is used for the electrical wiring. It transmits data in the form of electronic signals. It is the single solid conductor. It offers lower bandwidth compared to Fibre. It is heavier and thicker. It cannot be laid in a different environment because it is more prone to corrosive materials. Attenuation is high. As in this data travel in the form of electric signals, they are affected by the electrical and magnetic interfaces. They do not provide security against the wiretappers, because there is leakage of signals, and are easy to tap. These are prevalent to Cross-talk. In this charge carriers are electrons, they carry a negative charge, so they get affected when they move in a wire. They cannot be easily broken. Installation Cost is less. It is a bandwidth size 10Gbps.

  - Coaxial Cables: - a type of electrical cable consisting of an inner conductor surrounded by a concentric conducting shield, with the two separated by a dielectric (insulating material); many coaxial cables also have a protective outer sheath or jacket. The term *coaxial* refers to the inner conductor and the outer shield sharing a geometric axis.

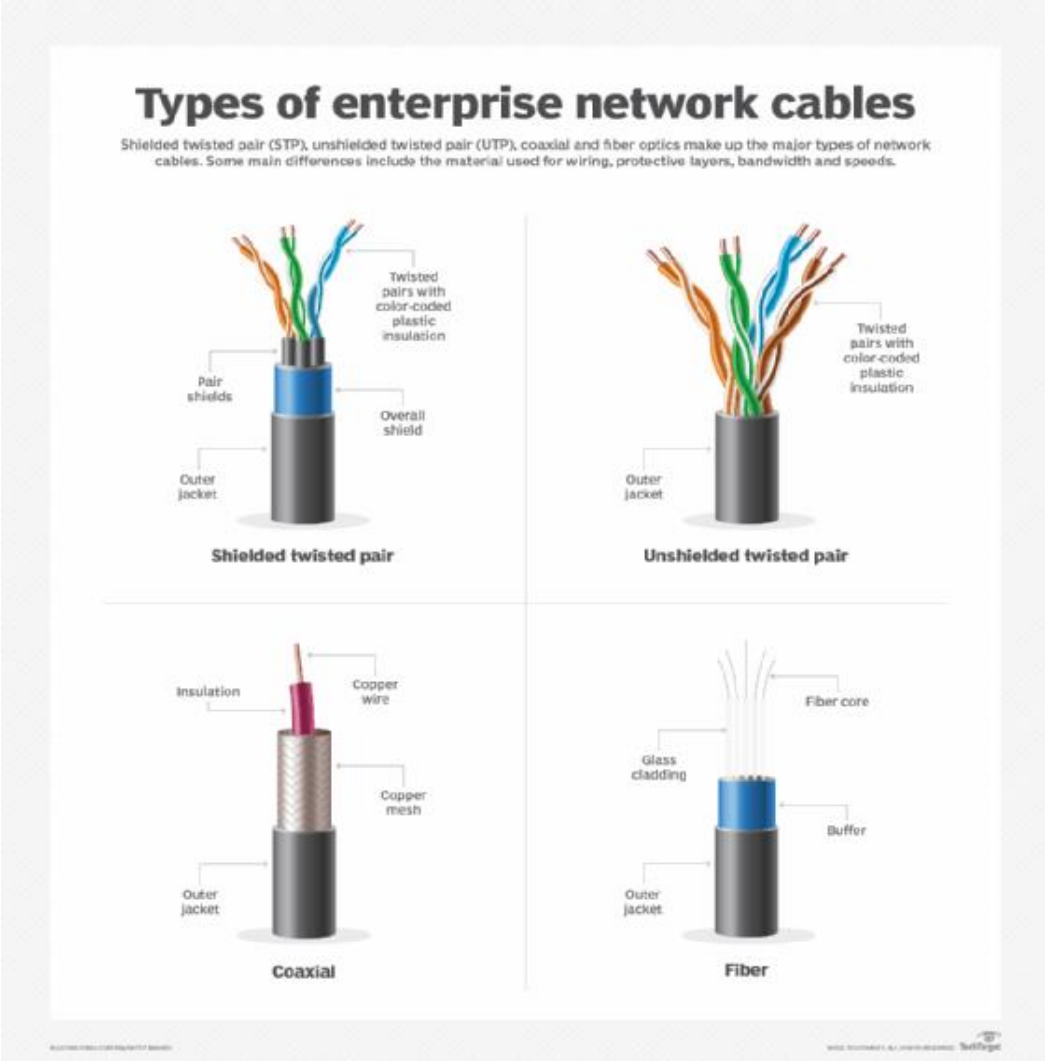
  - Shielded Twisted Pair (STP): - A shielded twisted pair is a type of twisted pair cable that contains an extra wrapping foil or copper braid jacket to protect the cable from defects like cuts, losing bandwidth, noise, and signal to the interference. It is a cable that is usually used underground, and therefore it is costly than UTP. It supports the higher data transmission rates across the long distance.

  - Unshielded Twisted Pair (UTP): - UTP is an unshielded twisted pair cable used in computer and telecommunications mediums. Its frequency range is suitable for transmitting both data and voice via a UTP cable. Therefore, it is widely used in the telephone, computers, etc. It is a pair of insulated copper wires twisted together to reduce noise generated by external interference.

  ii. Fibre Optic Cable

  Fiber Optic Cable is also known as the Optical Fiber Cable. It is made up of plastic or glass. It transmits signals in the form of light. It offers higher

bandwidth compared to copper cables. It is thin, lighter in weight, and smaller in size. It can be laid in different environments because it is more resistant to corrosive materials. Attenuation is very low. As this data travel in the form of light, they are not affected by the electrical and magnetic interfaces. They provide security against the wiretappers, because there is no leakage of light and are difficult to tap. There is no Cross-talk. In this charge carriers are photons, they do not carry any charge, so they do not get affected. They are easily breakable. Installation Cost is high. It is a bandwidth size 60Tps.

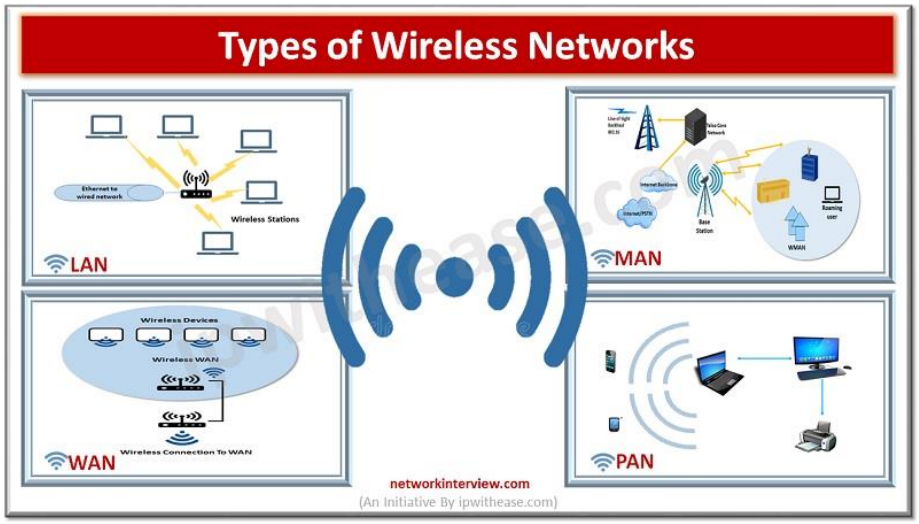


- Wireless Media

  Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.

  When an antenna is attached to electrical circuit of a computer or wireless device, it converts the digital data into wireless signals and spread all over within its frequency range. The receptor on the other end receives these signals and converts them back to digital data.

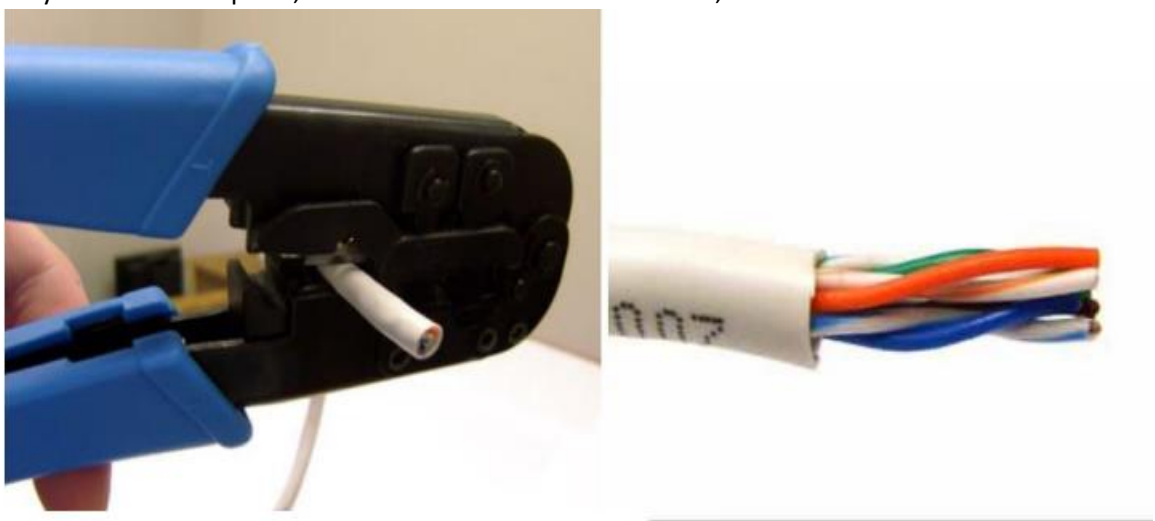
- LAN
- WAN
- MAN
- PAN



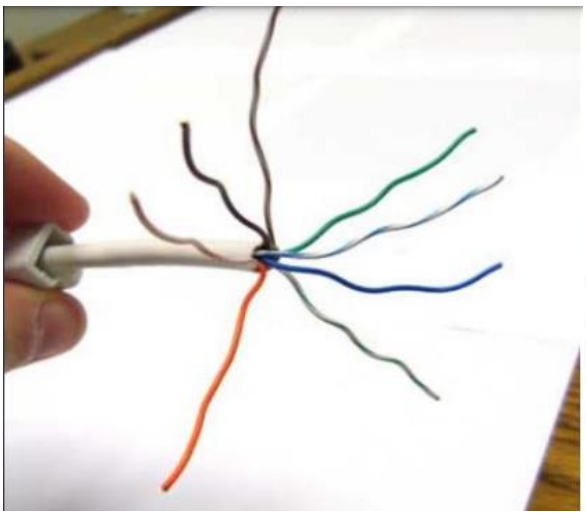
3. Practically implement the cross-wired cable and straight wired cable using Crimping tool

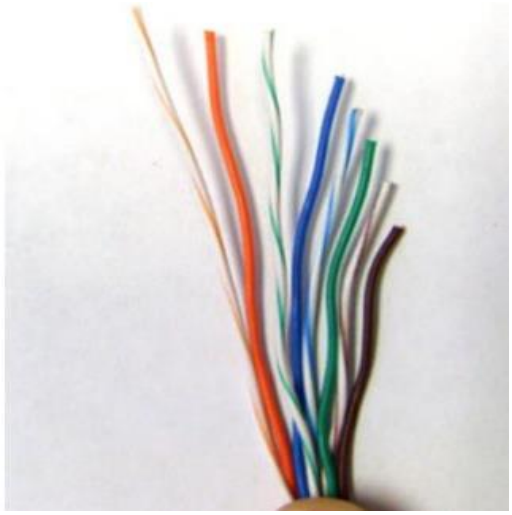
Ans.
Apparatus (Components): RJ-45 connector, Climping Tool, Twisted pair Cable

Step 1: - Start by stripping off about 2 inches of the plastic jacket off the end of the cable. Be very careful at this point, as to not nick or cut into the wires, which are inside.



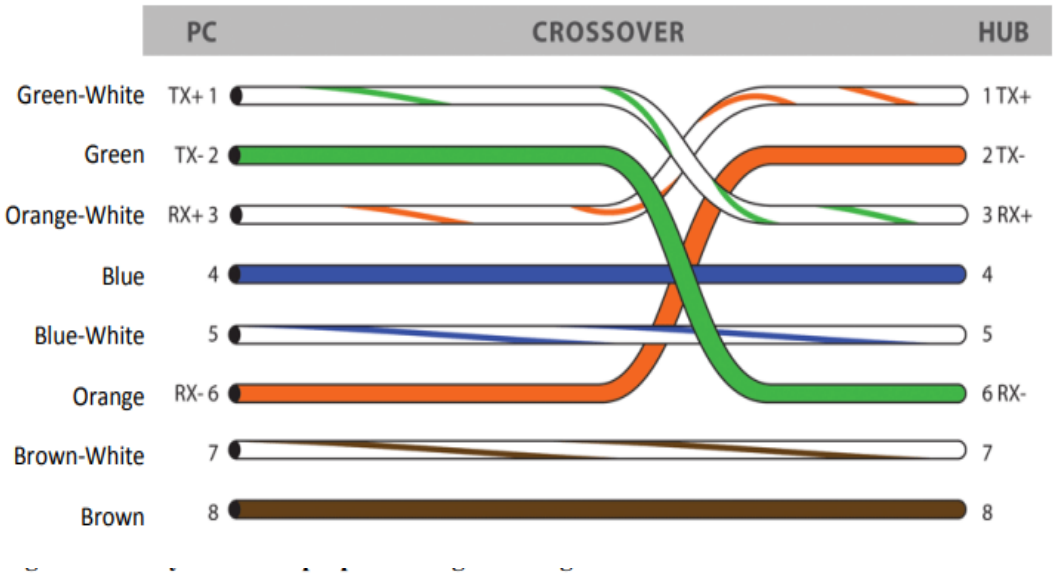
Step 2: - Spread the wires apart but be sure to hold onto the base of the jacket with your other hand. You do not want the wires to become untwisted down inside the jacket.

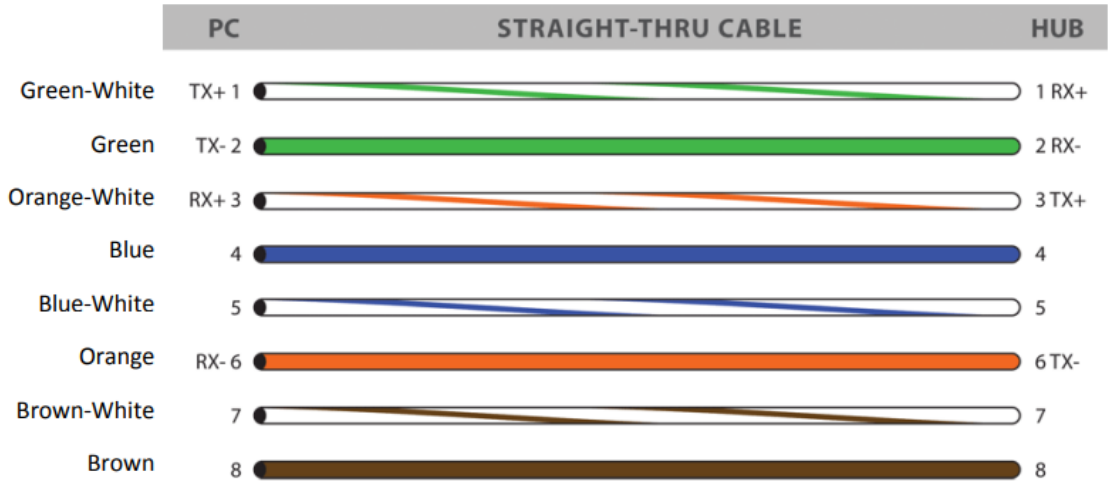




Step 3: - Cut of the Plastic Separator and the thread do that it doesn't impede the implementation.

Step 4: - Arrange the wires accordingly for cross-wired cable and straight wired cable.





Step 5: - Align the 8 exposed wires by snipping a few millimetres of it.
Step 6: - Insert the cable into the RJ-45-connector and make sure all the 8 wires are all inserted into the connector properly.

Step 7: - Use the crimping tool to crimp the connector.

If all the wires are inserted properly then the RJ-45-connector stay connected to the wires, else the connector will slip out and the RJ-45-connector becomes unusable.

4. Study of network IP Address configuration: (Classification of address, static and dynamic address)

   Ans.

   An IP address represents an Internet Protocol address. A unique address that identifies the device over the network. It is almost like a set of rules governing the structure of data sent over the Internet or through a local network. An IP address helps the Internet to distinguish between different routers, computers, and websites. It serves as a specific machine

identifier in a specific network and helps to improve visual communication between source and destination.

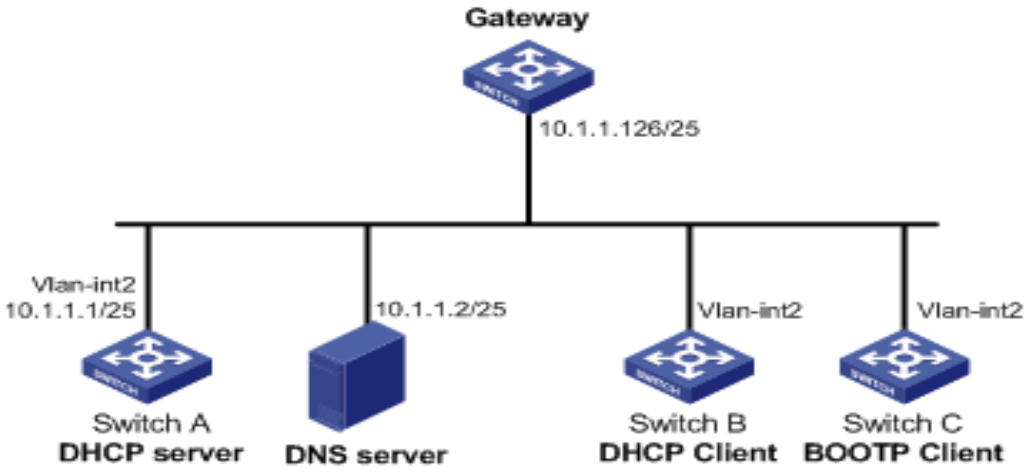
IP address structure: IP addresses are displayed as a set of four digits- the default address may be 192.158.1.38. Each number on the set may range from 0 to 255. Therefore, the total IP address range ranges from 0.0.0.0 to 255.255.255.255.

Classification of IP Address:

- Public IP address
- Private IP address
- Static IP address
- Dynamic IP address

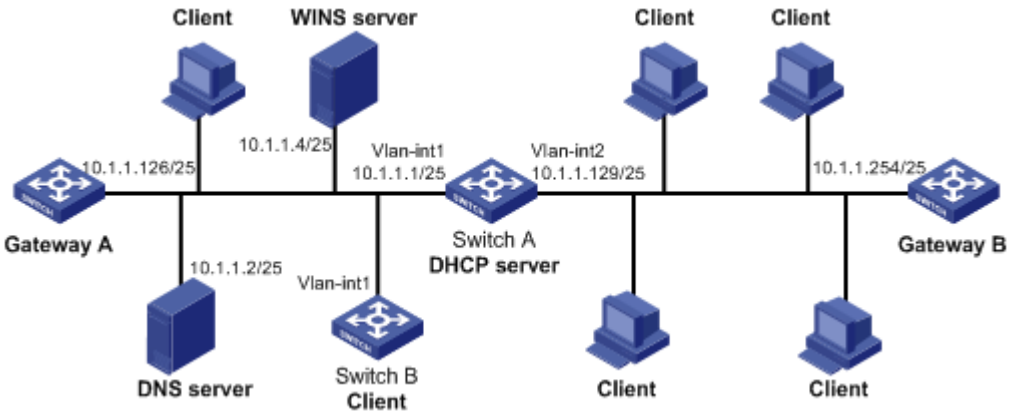
Static IP Address–

A static IP address is an invalid IP address. Conversely, a dynamic IP address will be provided by the Dynamic Host Configuration Protocol (DHCP) server, which can change. The Static IP address does not change but can be changed as part of normal network management. Static IP addresses are incompatible, given once, remain the same over the years. This type of IP also helps you get more information about the device.



Dynamic IP address–

It means constant change. A dynamic IP address changes from time to time and is not always the same. If you have a live cable or DSL service, you may have a strong IP address. Internet Service Providers provide customers with dynamic IP addresses because they are too expensive. Instead of one permanent IP address, your IP address is taken out of the address pool and assigned to you. After a few days, weeks, or sometimes even months, that number is returned to the lake and given a new number. Most ISPs will not provide a static IP address to customers who live there and when they do, they are usually more expensive. Dynamic IP addresses are annoying, but with the right software, you can navigate easily and for free.



5. Study of network configuration: (IPv4 and IPv6, Subnet, Supernet)
   Ans.
   An IP address represents an Internet Protocol address. A unique address that identifies the device over the network. It is almost like a set of rules governing the structure of data sent over the Internet or through a local network. An IP address helps the Internet to distinguish between different routers, computers, and websites. It serves as a specific machine identifier in a specific network and helps to improve visual communication between source and destination.

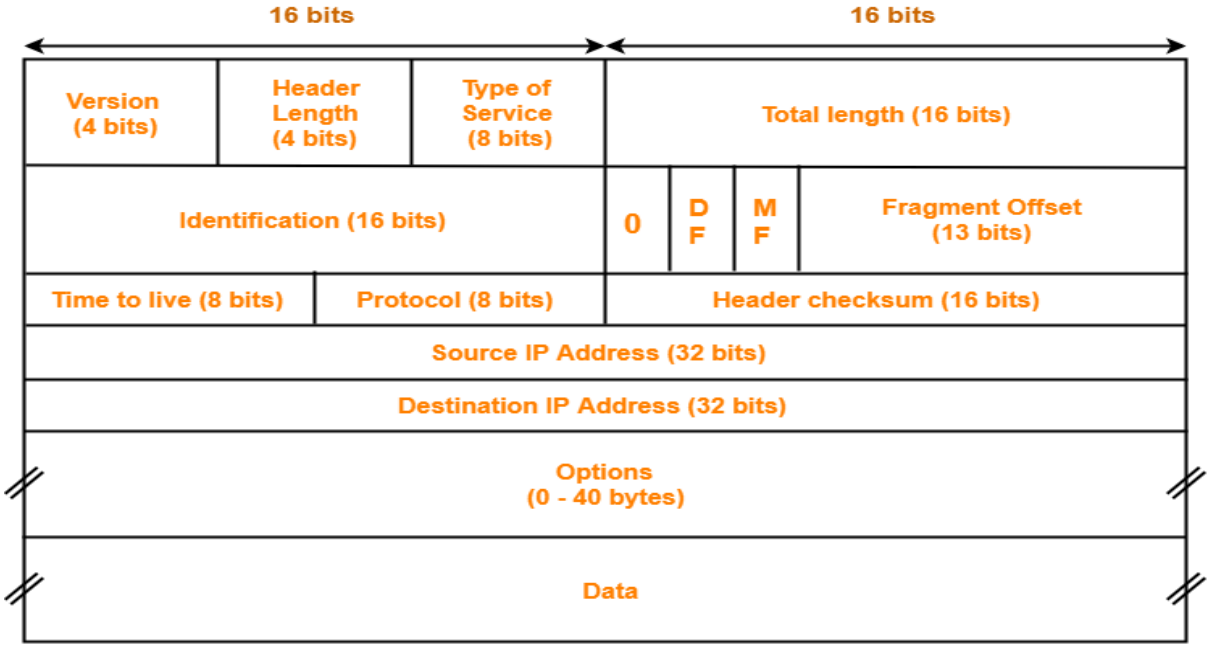
   IP address structure: IP addresses are displayed as a set of four digits- the default address may be 192.158.1.38. Each number on the set may range from 0 to 255. Therefore, the total IP address range ranges from 0.0.0.0 to 255.255.255.255.

   IPv4
   IP stands for **Internet Protocol** and **v4** stands for **Version Four** (IPv4). IPv4 was the primary version brought into action for production within the ARPANET in 1983.
   IP version four addresses are 32-bit integers which will be expressed in decimal notation.
   Example- 192.0.2.126 could be an IPv4 address.
   Parts of IPv4

   Network part:
   The network part indicates the distinctive variety that's appointed to the network. The network part conjointly identifies the category of the network that's assigned.

- **Host Part:**
  The host part uniquely identifies the machine on your network. This part of the IPv4 address is assigned to every host.
  For each host on the network, the network part is the same, however, the host half must vary.
- **Subnet number:**
  This is the nonobligatory part of IPv4. Local networks that have massive numbers of hosts are divided into subnets and subnet numbers are appointed to that.
  Characteristics of IPv4
- IPv4 could be a 32-Bit IP Address.

- IPv4 could be a numeric address, and its bits are separated by a dot.
- The number of header fields is twelve and the length of the header field is twenty.
- It has Unicast, broadcast, and multicast style of addresses.
- IPv4 supports VLSM (Virtual Length Subnet Mask).
- IPv4 uses the Post Address Resolution Protocol to map to the MAC address.



IPv4 Header

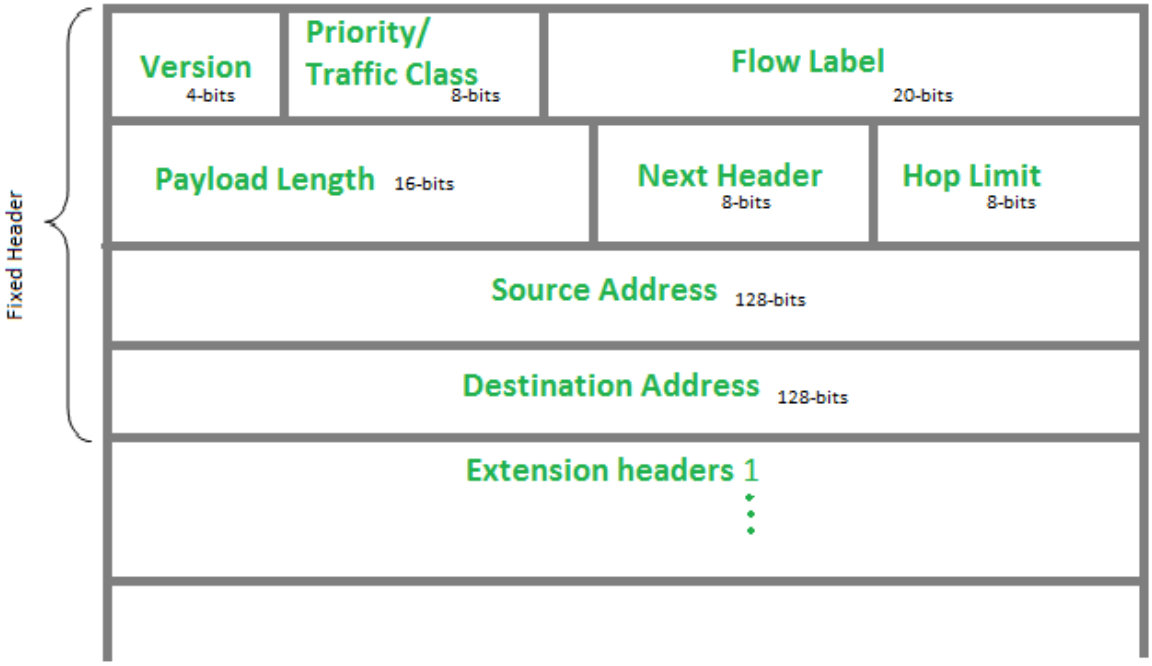
IPv6

IPv6 or Internet Protocol Version 6 is a network layer protocol that allows communication to take place over the network. IPv6 was designed by Internet Engineering Task Force (IETF) in December 1998 with the purpose of superseding the IPv4 due to the global exponentially growing internet users. This new IP address version is being deployed to fulfil the need for more Internet addresses. It was aimed to resolve issues which are associated with IPv4. With 128-bit address space, it allows 340 undecillion unique address space. IPv6 also called IPng (Internet Protocol next generation)

Types of IPv6 Address

Now that we know about what is IPv6 address let's take a look at its different types.

- **Unicast addresses** It identifies a unique node on a network and usually refers to a single sender or a single receiver.
- **Multicast addresses** It represents a group of IP devices and can only be used as the destination of a datagram.
- **Anycast addresses** It is assigned to a set of interfaces that typically belong to different nodes.



IP Subnetting

Subnetting is the process in which you break a network into smaller pieces. This can be done for a variety of reasons. For example, a company having department LANs connected to different interfaces in a router or in different VLANs in a switch can't use the same network part and the same mask for devices in all departments because they would not communicate with each other.

Using different IP network addresses for devices in different LANs within the same company is not recommended because of the large number of IP addresses that might be wasted in the process.

Subnetting is done by choosing an appropriate mask, called a **subnet mask** or NetMask to define the number of hosts in that network. The network address of a subnet can be a valid IP address from the subnetted network that devices will no longer be able to use. By subnetting, you lose some usable IP addresses (two for each subnet).

The Subnet Mask

The subnet mask is a 32 bit sequence of zeros and ones, just like the IP address. The subnet mask has all the bits in the network part of the IP address set to 1, and all the bits in the host part of the IP address set to 0. The subnet mask works like the network mask (it's basically the same thing), except that the subnet mask borrows some bits from the host part to identify the subnet.

IP Supernetting or CIDR

CIDR stands for "Classless Inter-Domain Routing". It is a new addressing scheme for the Internet, intended to replace the old classful (Class A, B, C) address scheme. CIDR allows a more efficient allocation of IP addresses and uses routing aggregation for minimizing the routing table entries, and is also called **supernetting** .

A recapitulation of classful IP addressing shows us the following:

Address Class	Number of Network Bits	Number of Hosts Bits	Decimal Address Range
Class A	8 bits	24 bits	1-126
Class B	16 bits	16 bits	128-191
Class C	24 bits	8 bits	192-223

If a provider needed 10,000 IP addresses for a project, then it would receive a class B network, and 55,534 IP addresses would not be used. If however, the provider had been assigned 40 class C networks for that 10,000 IP addresses, it could not match its needs (not all the IP addresses would be in the same network) and the routing tables of routers on the Internet would grow with 40 new routes.

CIDR is an addressing scheme that supports masks not only of 8, 16, or 24 bits as in classful routing but of arbitrary length. The CIDR notation is:

xxx.xxx.xxx.xxx/n

where xxx.xxx.xxx.xxx is the IP address of the network and "n" is the number of '1' bits in the mask. For example, the class C network 192.168.1.0 with the mask 255.255.255.0 is written in CIDR as 192.168.1.0/24.

Program 6:

Study of network devices. (Switch, Router, Bridge).

Switches:

- A switch is a data link layer networking device which connects devices in a network and uses packet switching to send and receive data over a network
- A switch has many ports, to which computers are plugged in.
- However, when a data frame arrives at any port of a network switch, it examines the destination address and sends the frame to the corresponding devices.
- Thus, it supports both unicast and multicast communications.
- We can have a two-layered switch or a three-layered switch.
- A two-layered switch is a bridge, a bridge with many ports and a design that allows better performance.
- A bridge with a few ports can connect a few LANs together. A bridge with many ports may be able to allocate a unique port to each station, with each station on its own independent entity.
- This means no competing traffic (no collision, as we saw in Ethernet).
- A two-layer switch, as a bridge does, makes a filtering decision based on the MAC Address of the frame it received.
- However, a two-layer switch can be more sophisticated. It can have a buffer to hold the frames for processing.
- It can have a switching factor that forwards the frames faster. Some new two-layer switches, called cut-through switches, have been designed to forward the frame as soon as they check the MAC addresses in the header of the frame.

Routers:

- Routers are networking devices operating at layer 3 or a network layer of the OSI model.
- They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks.
- When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.
- A router is a three-layer device that routes packets based on their logical addresses (host-to-host addressing).
- A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decisions about the route.
- The routing tables are normally dynamic and are updated using routing protocols. Data is grouped into packets, or blocks of data.
- Each packet has a physical device address as well as logical network address. The network address allows routers to calculate the optimal path to a workstation or computer.
- The functioning of a router depends largely upon the routing table stored in it. The routing table stores the available routes for all destinations.
- The router consults the routing table to determine the optimal route through which the data packets can be sent.
- A routing table typically contains the following entities –
    - IP addresses and subnet mask of the nodes in the network
    - IP addresses of the routers in the network
    - Interface information among the network devices and channels

- Routing tables are of two types –
    - Static Routing Table − Here, the routes are fed manually and are not refreshed automatically. It is suitable for small networks containing 2-3 routers.
    - Dynamic Routing Table − Here, the router communicates with other routers using routing protocols to determine the available routes. It is suited for larger networks having large numbers of routers.

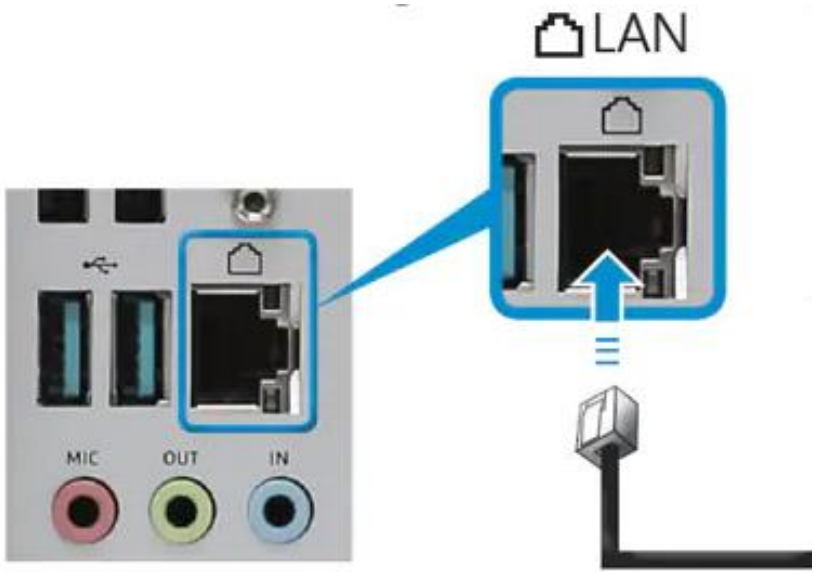
Bridges:

- A bridge operates in the physical layer as well as in the data link layer. It can regenerate the signal that it receives and as a data link layer device, it can check the physical addresses of source and destination contained in the frame.
- The major difference between the bridge and the repeater is that the bridge and the repeater is that the bridge has a filtering capability.
- That means it can check the destination address of a frame and decide if the frame should be forwarded or dropped.
- If the frame is forwarded, then the bridge should specify the port over which it should be forwarded.

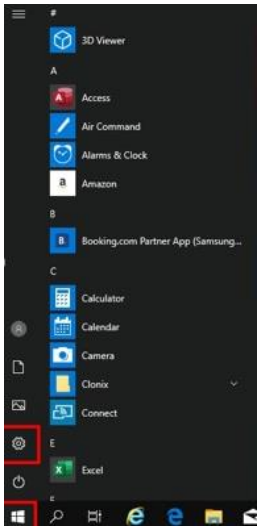
7. Configure and connect the computer to LAN.

A.

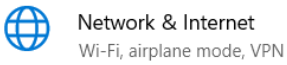
1. Connect a LAN cable to the PC's wired LAN port.



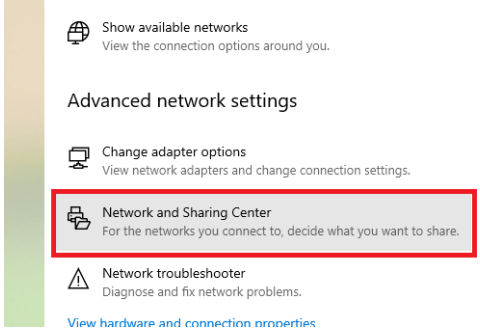
2. Click the Start button on the taskbar and then click Settings.



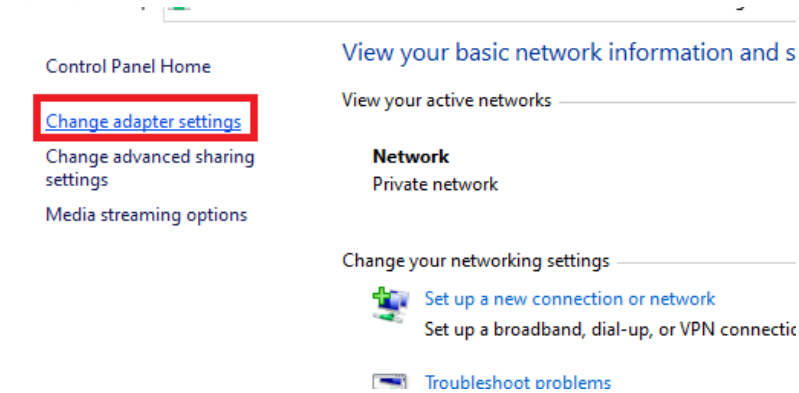
3. Click Network and Internet.



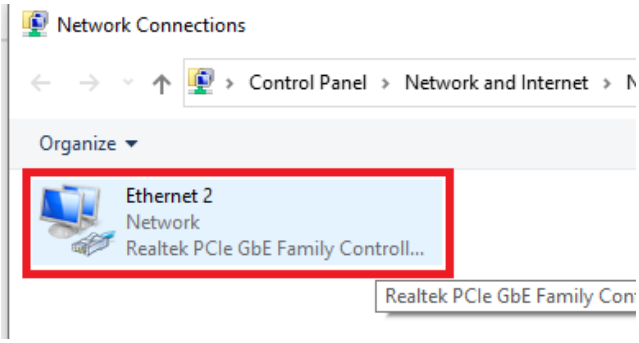
4. In Status, click Network and Sharing Center.



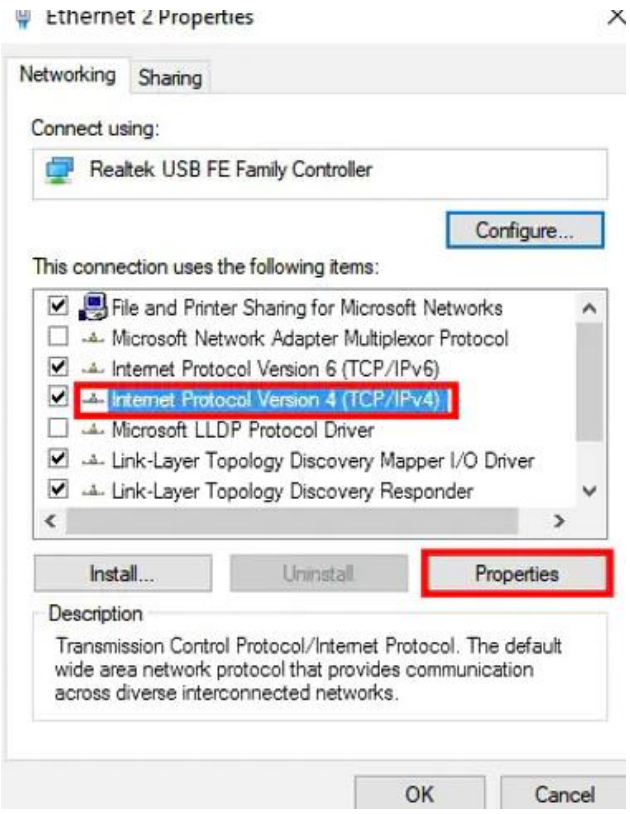
5. Choose Change adapter settings at the upper left.



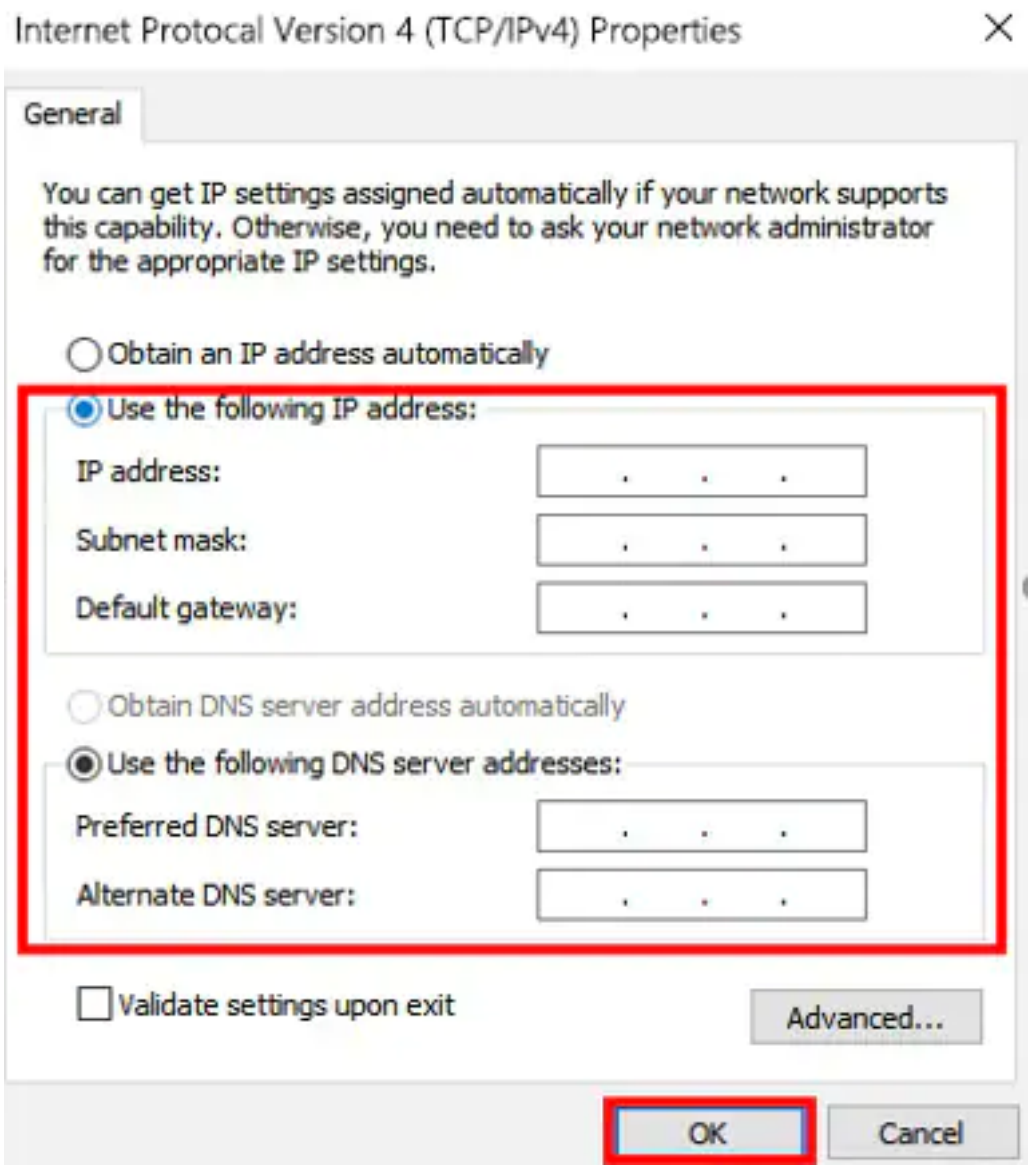
6. Right-click Ethernet and then choose Properties.



7. Select Internet Protocol Version 4 (TCP/IPv4), then click Properties.



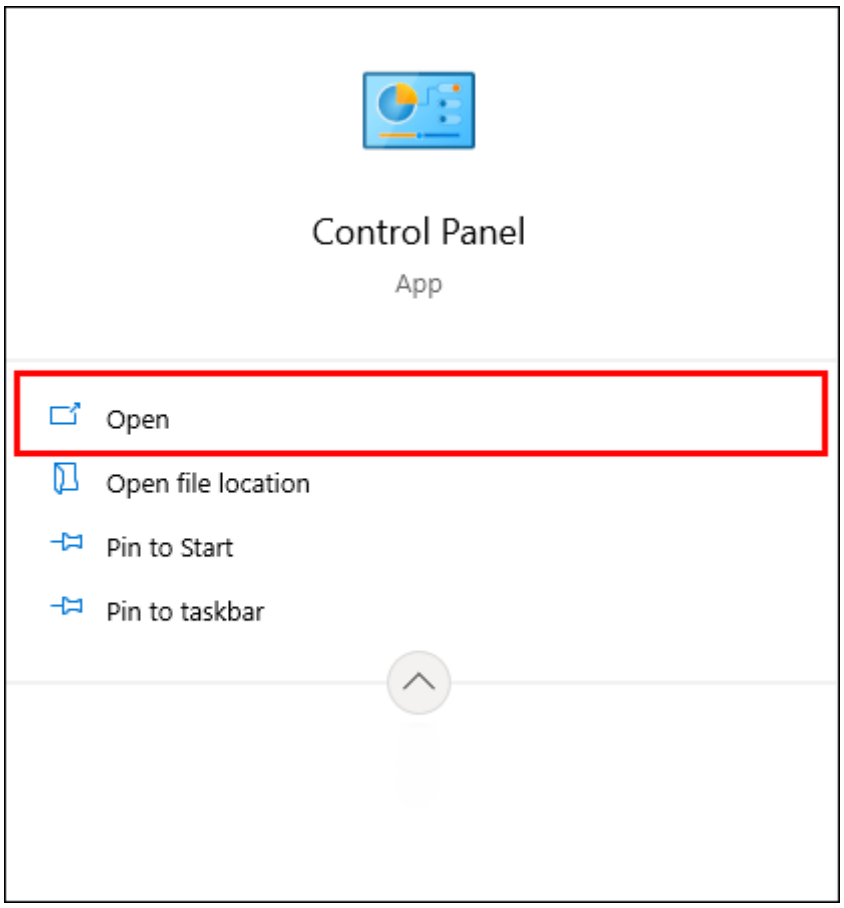
8. Set up the IP to use, then click OK to save your settings.



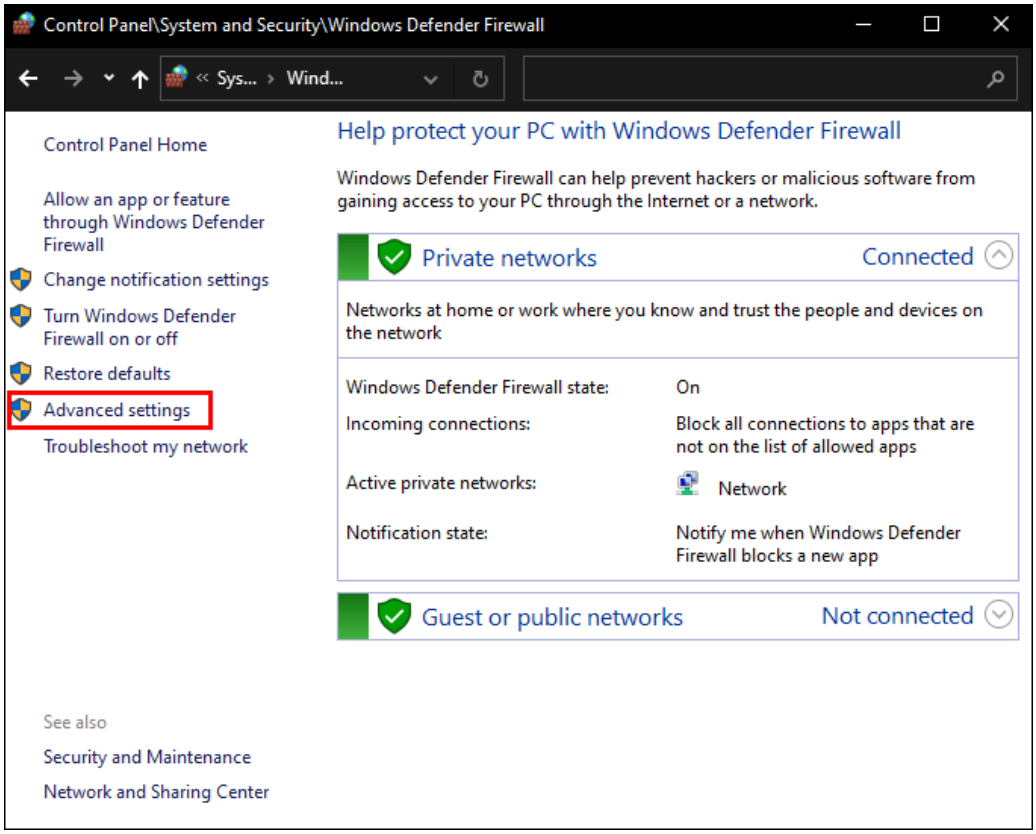
8. Block the Website Using “Windows Defender Firewall” in Windows 10.

A.

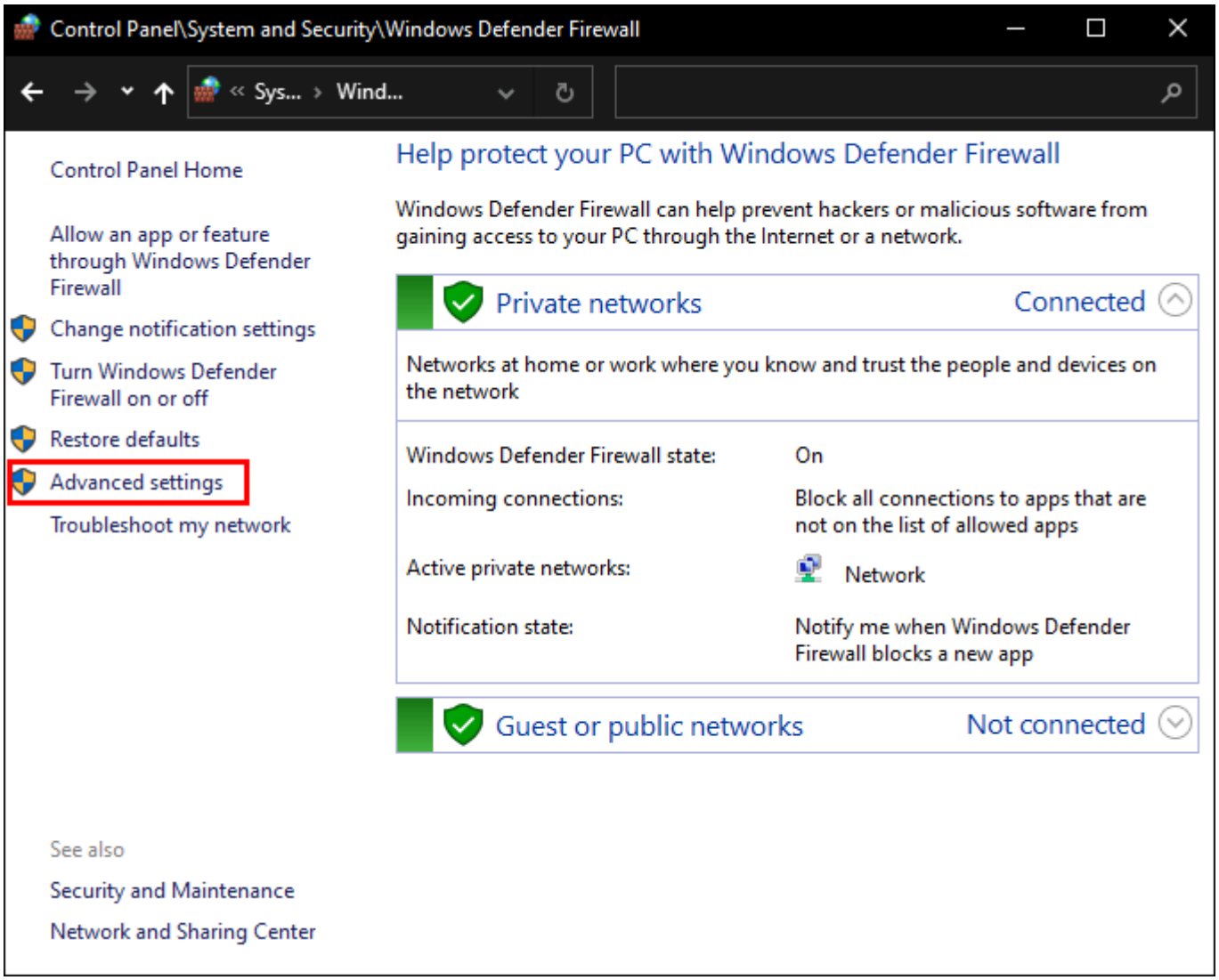
1. Launch the Control Panel on your computer.



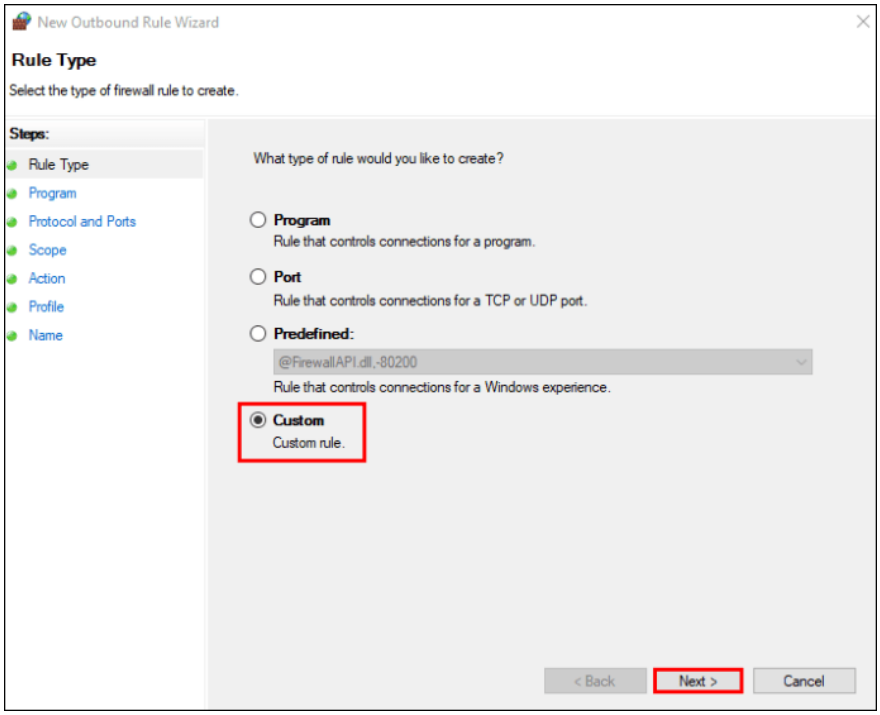
2. Select “Windows Defender Firewall” followed by “Advanced Settings” on the left-side pane.



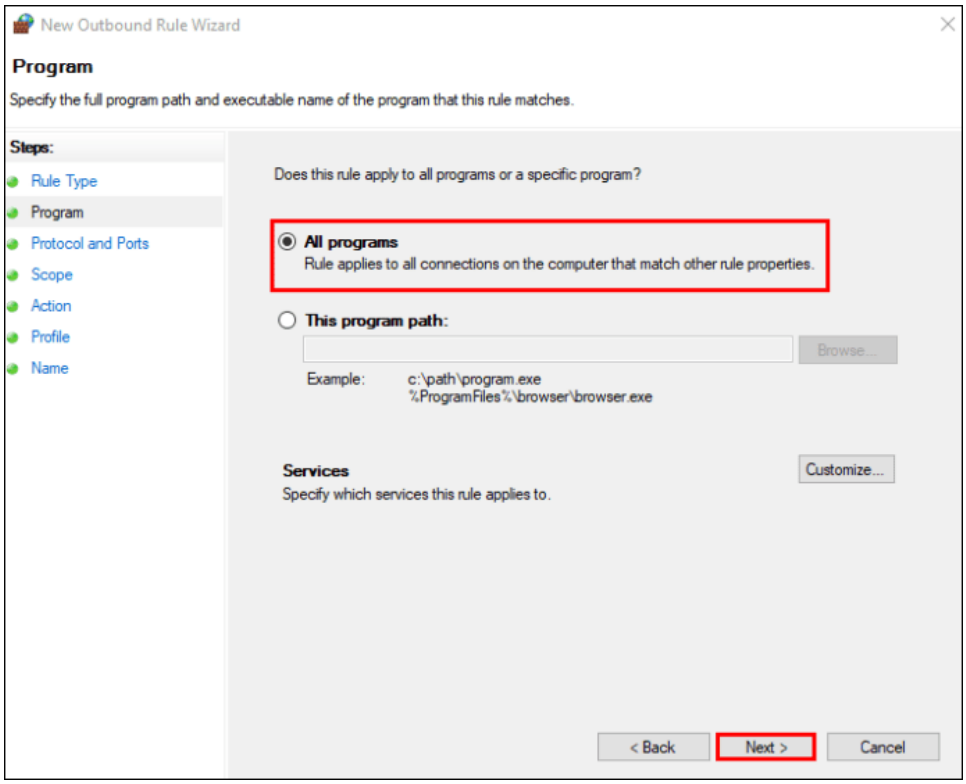
3. Right-click on “Outbound Rules” from the menu on the left and select “New Rule.”



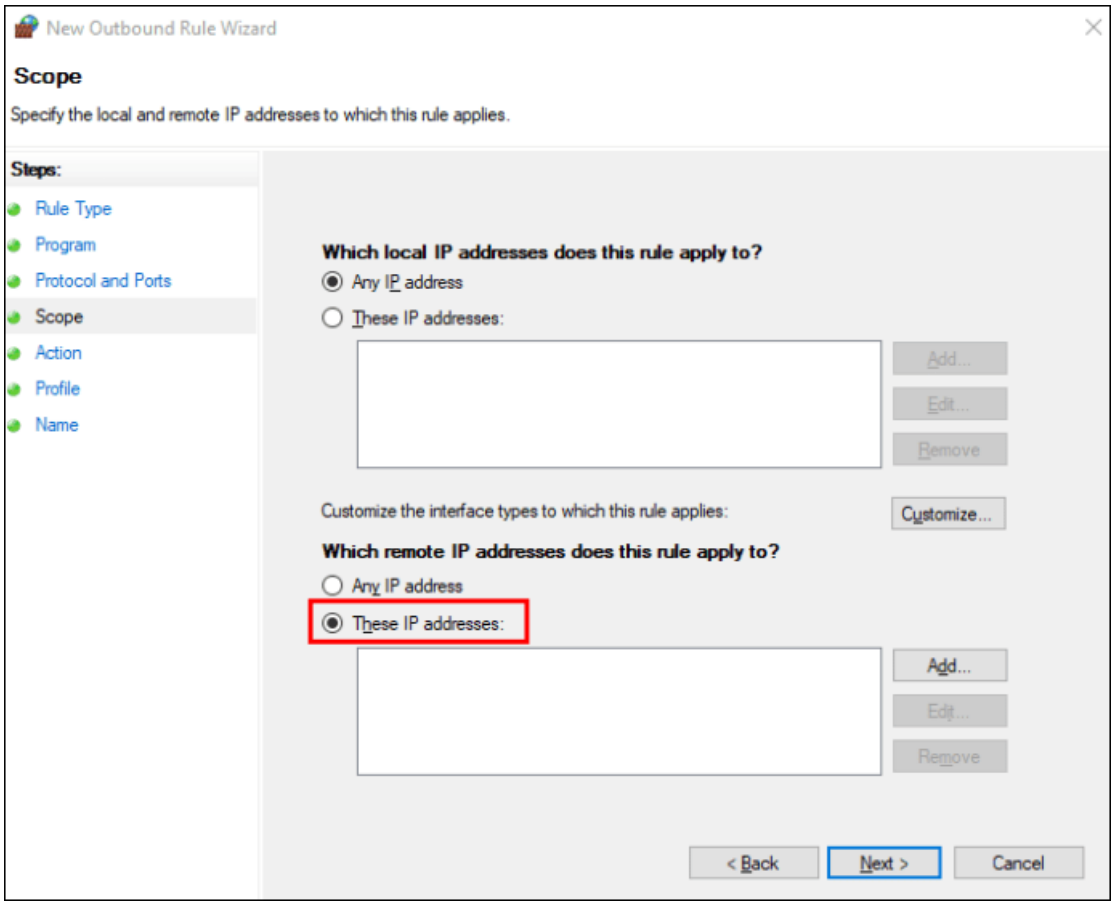
4. When a new window pops up, select the “Custom” option followed by “Next.”



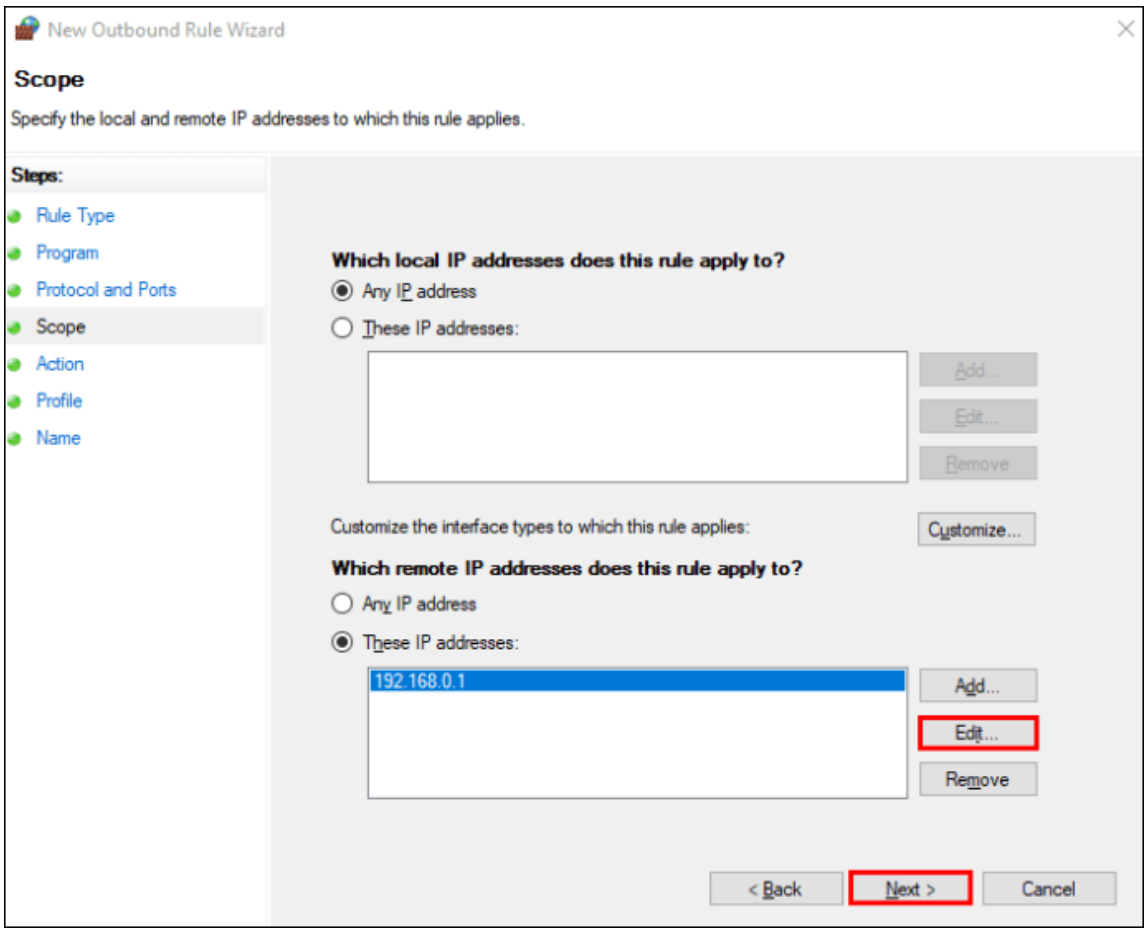
5. On the next window, select “All programs” and again select “Next.”



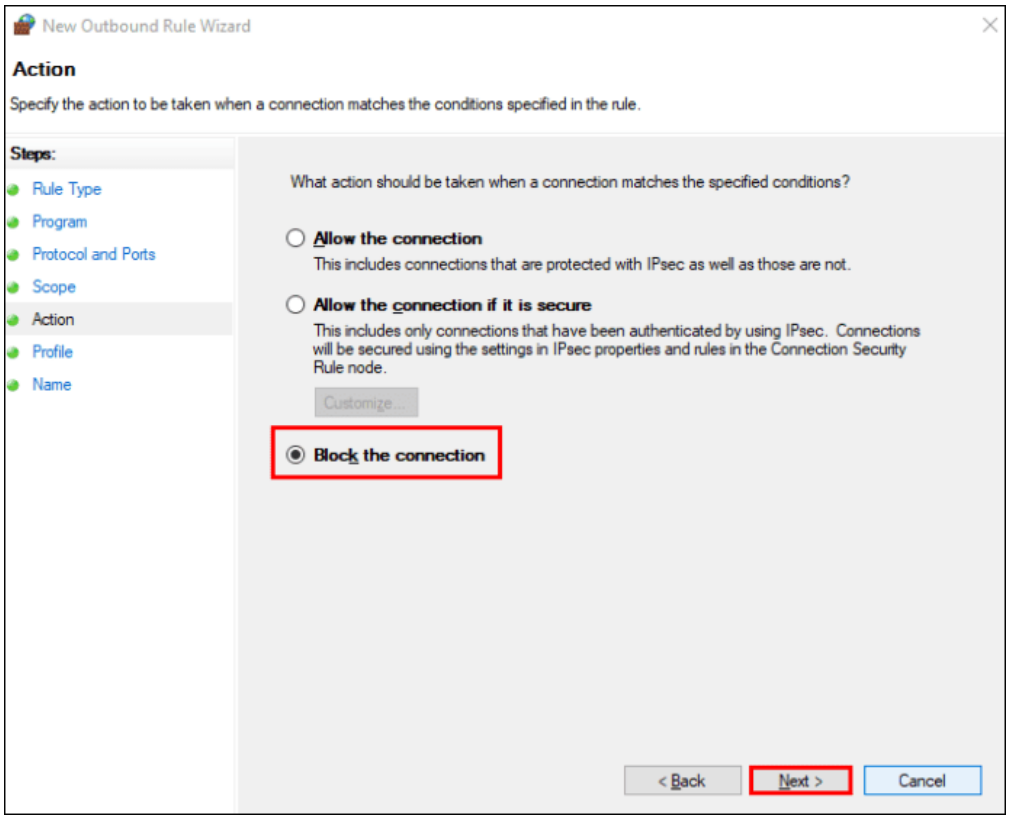
6. Select the” These IP addresses” option under “Which remote IP addresses does this rule apply to?”



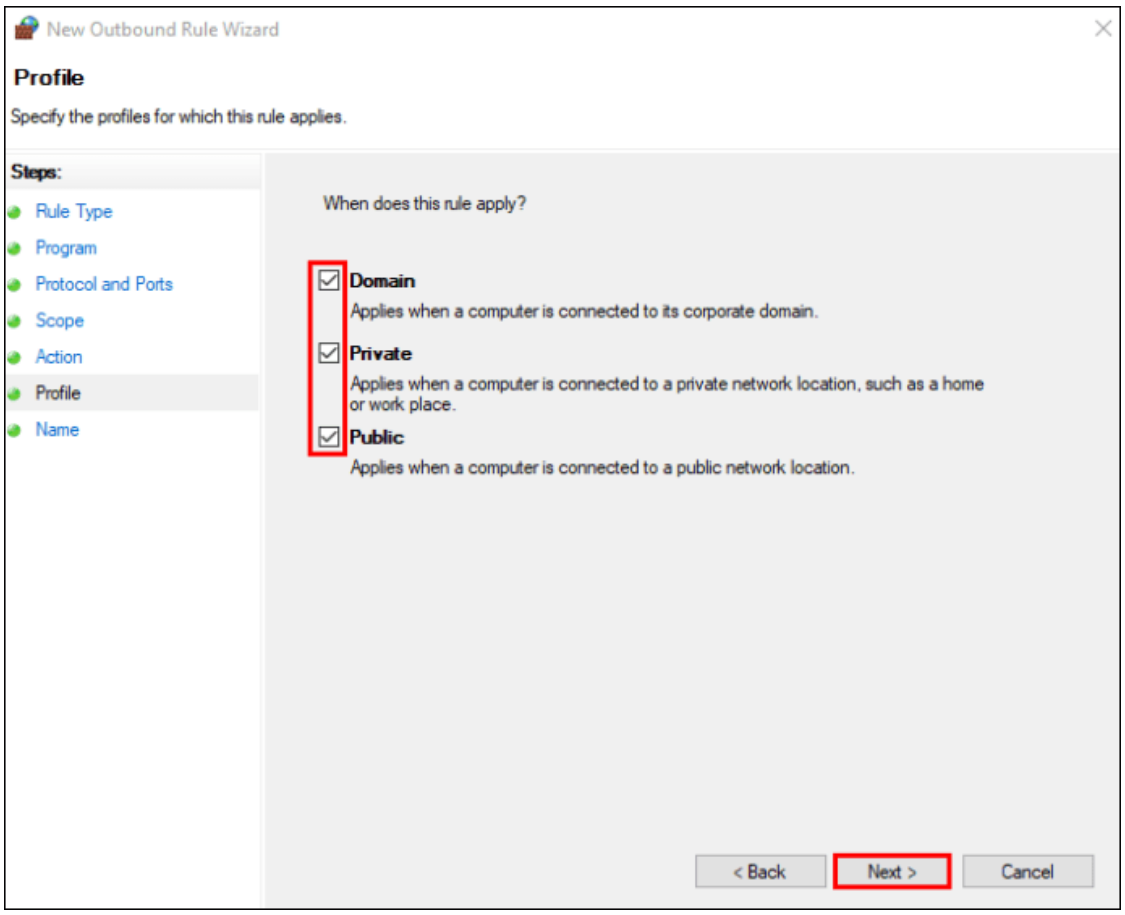
7. Click on “Add” and enter the IP addresses you want to block. Then select “Next.”



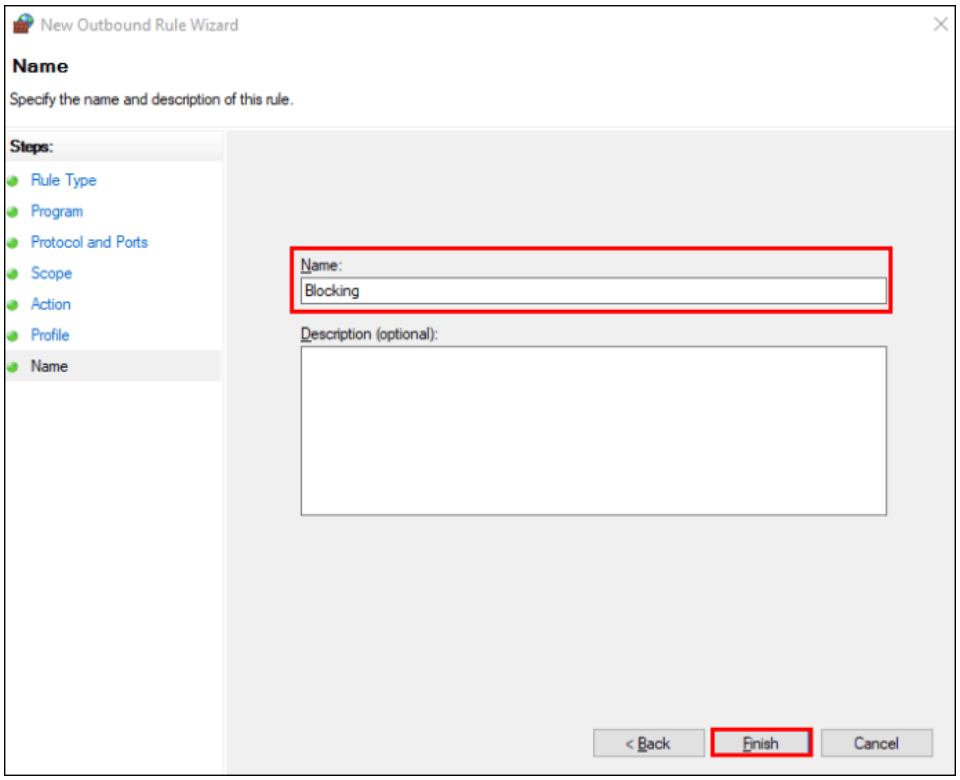
8. Make sure to choose the “Block the connection” option and click on “Next.”



9. Choose whether the rule applies to Domain, Private, or Public. You can also select all three.



10. Select “Next,” add a name or description for this rule, and select “Finish” to complete the action.



9. Share the folder in a system and access the files of that folder from other system using IP address.

A. **First Computer**

1. Open File Explorer.

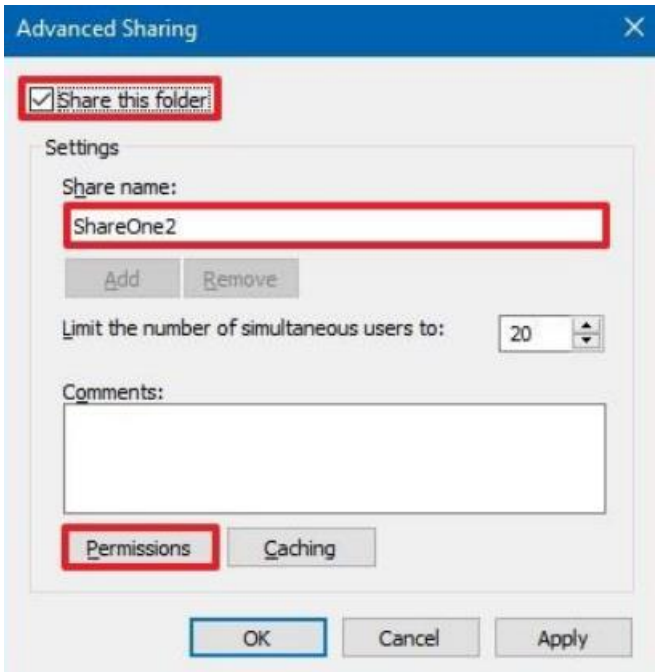
2. Navigate to the folder you want to share.

3. Right-click the folder and select the Properties option.

4. Click the Sharing tab.

5. Click the Advanced Sharing button.

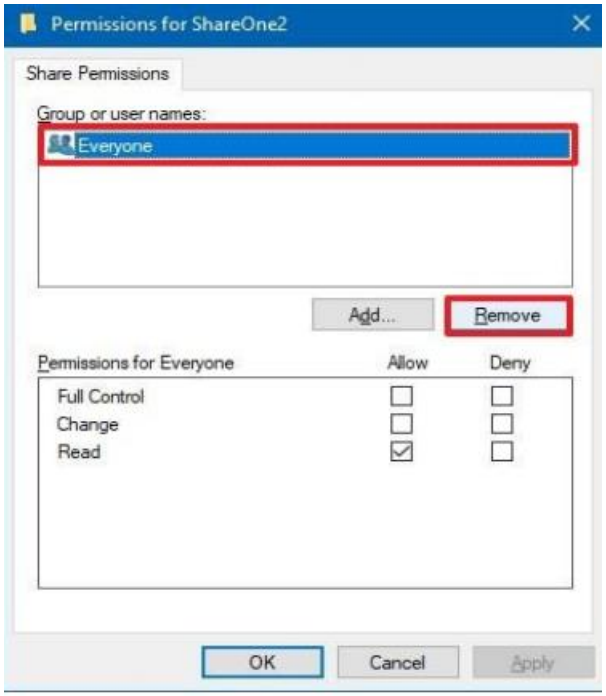
6. Check the Share this folder option.



7. Click the Permissions button.

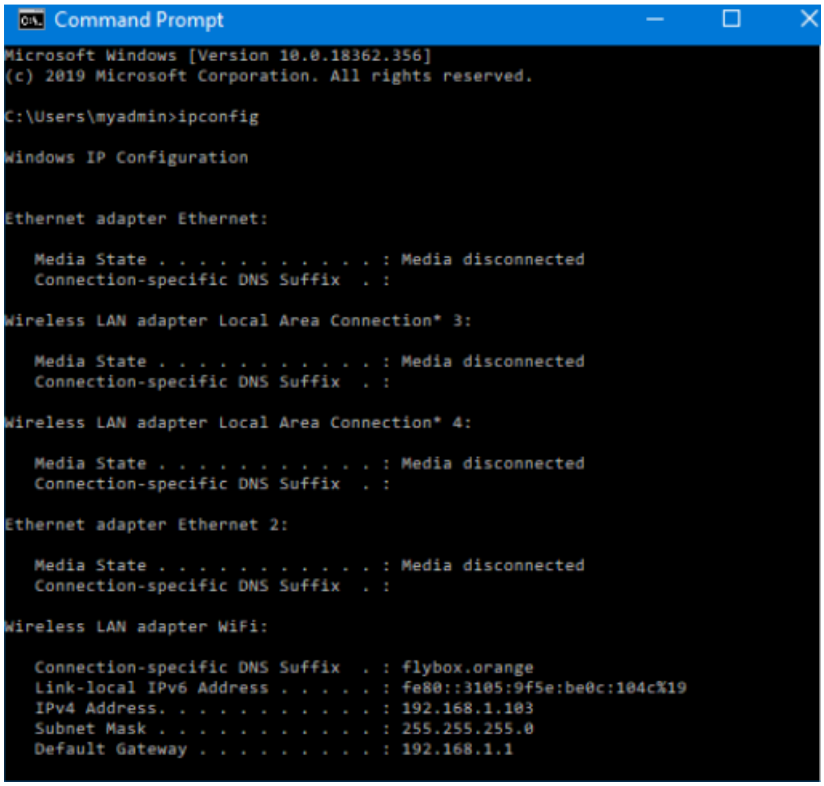
8. Select the Everyone object if you want to share the folder to everyone or Add button to select specific users or group of users

9. Tick the permission boxes to assign users the permission to either read or read and write in the shared folder.

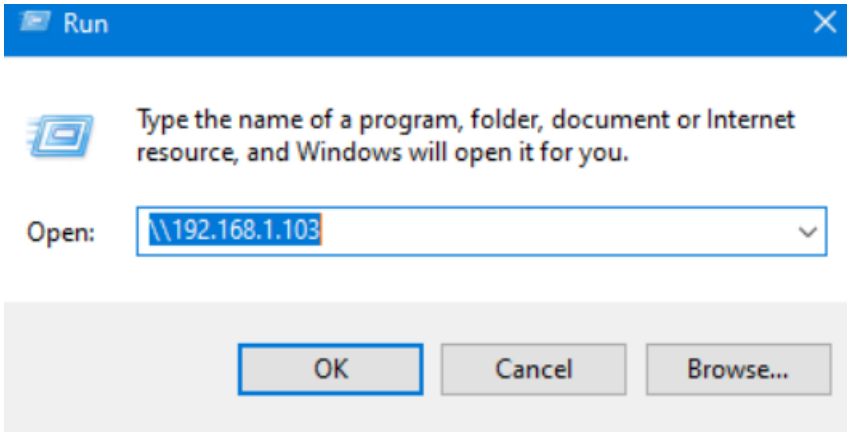


10. Select Apply and then OK buttons.

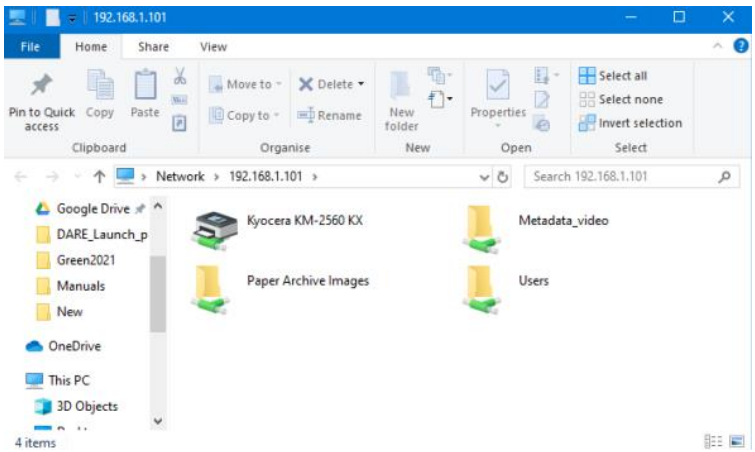
11. Now to test if the shared folder will be accessed over the network, you need to know the IP address of your PC (the computer containing the shared folder). To find the IP address of your computer, go to search and type the command “cmd “to launch the command prompt application and then type “ipconfig” in the command line prompt dialog.



12. On the same Computer, Go to search and type in the command “run” to launch the run App and then type in: \\IP address (e.g.: \\192.168.1.1).

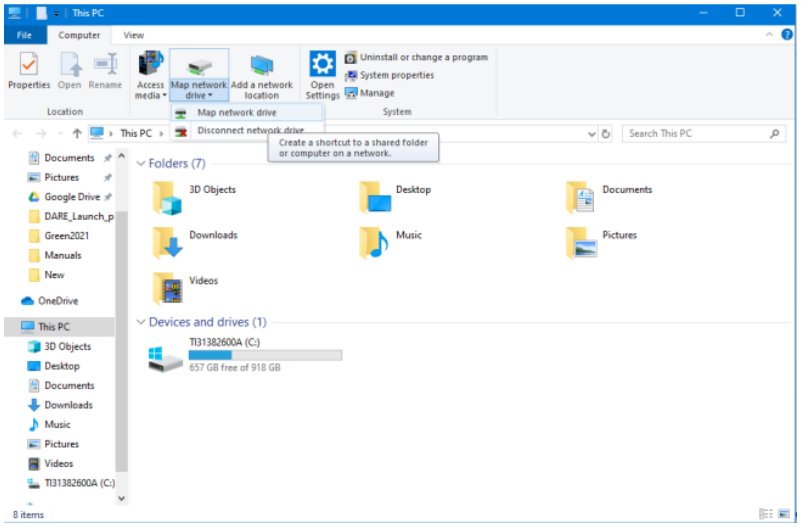


13. Click OK to see the list of shared folders on your computer.

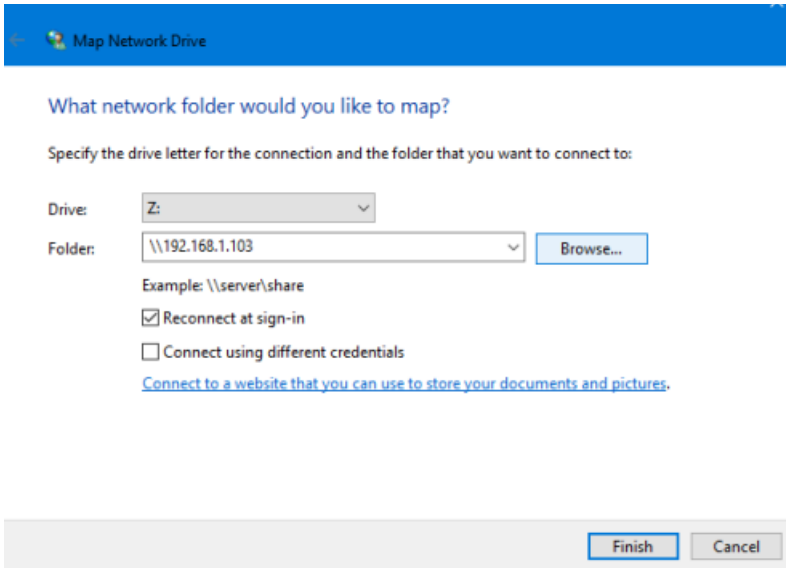


Second Computer

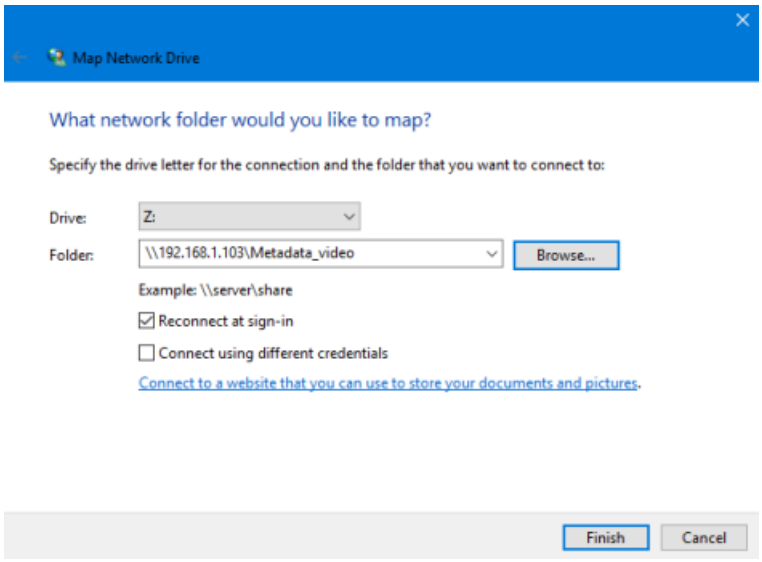
1. Open File Explorer from the taskbar or the Start menu, or press the Windows logo key + E. Alternatively, Select This PC from the left pane. Then, on the computer tab, select Map network drive.



2. Under Drive, choose any letter, in the drop-down box, under Folder, type in \\ IP address of the server computer (i.e. where the shared folder is located).



3. Select Browse to see the IP address and then expand to see the shared folders and select the required shared folder and then click OK, then click Finish.



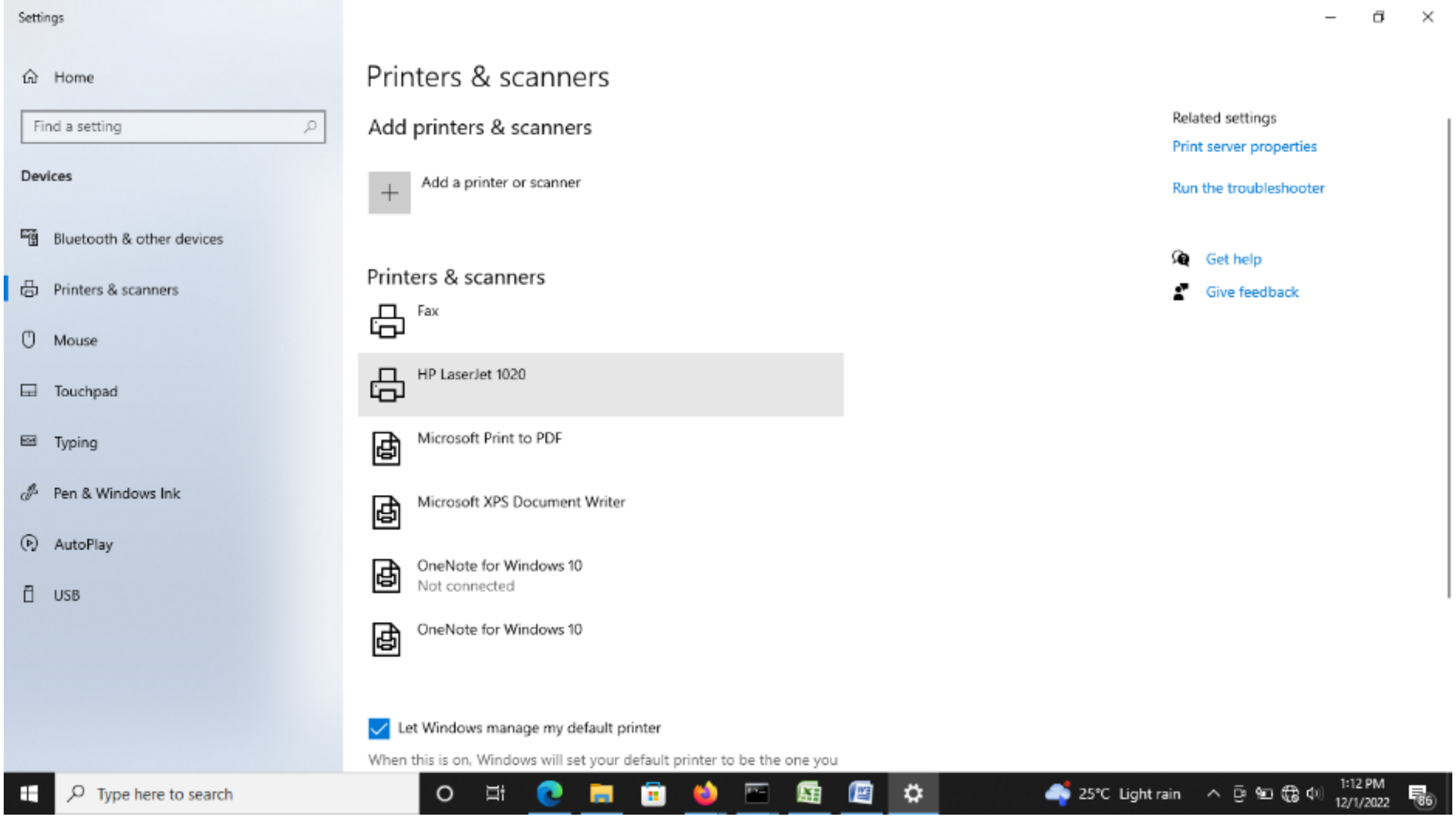
4. Check your network location and you will find the mapped link. End.

Note: If you can't connect to a network drive or shared folder, the computer you're trying to connect to might be turned off, or you might not have the correct permissions. Try to contact your network administrator.

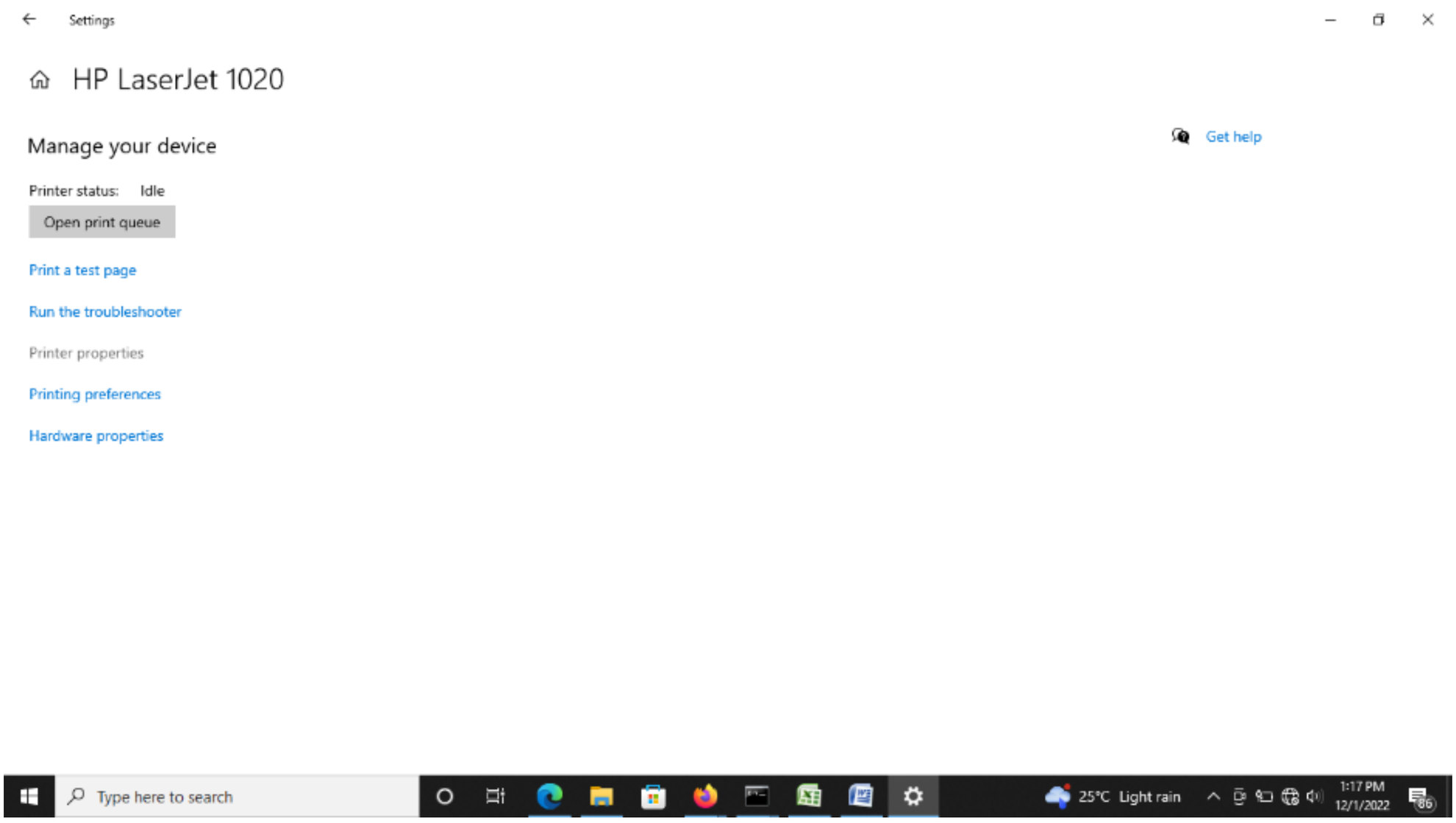
Program 10: Printer sharing

Install the driver of the printer in the PC

Open printer and scanning from pc

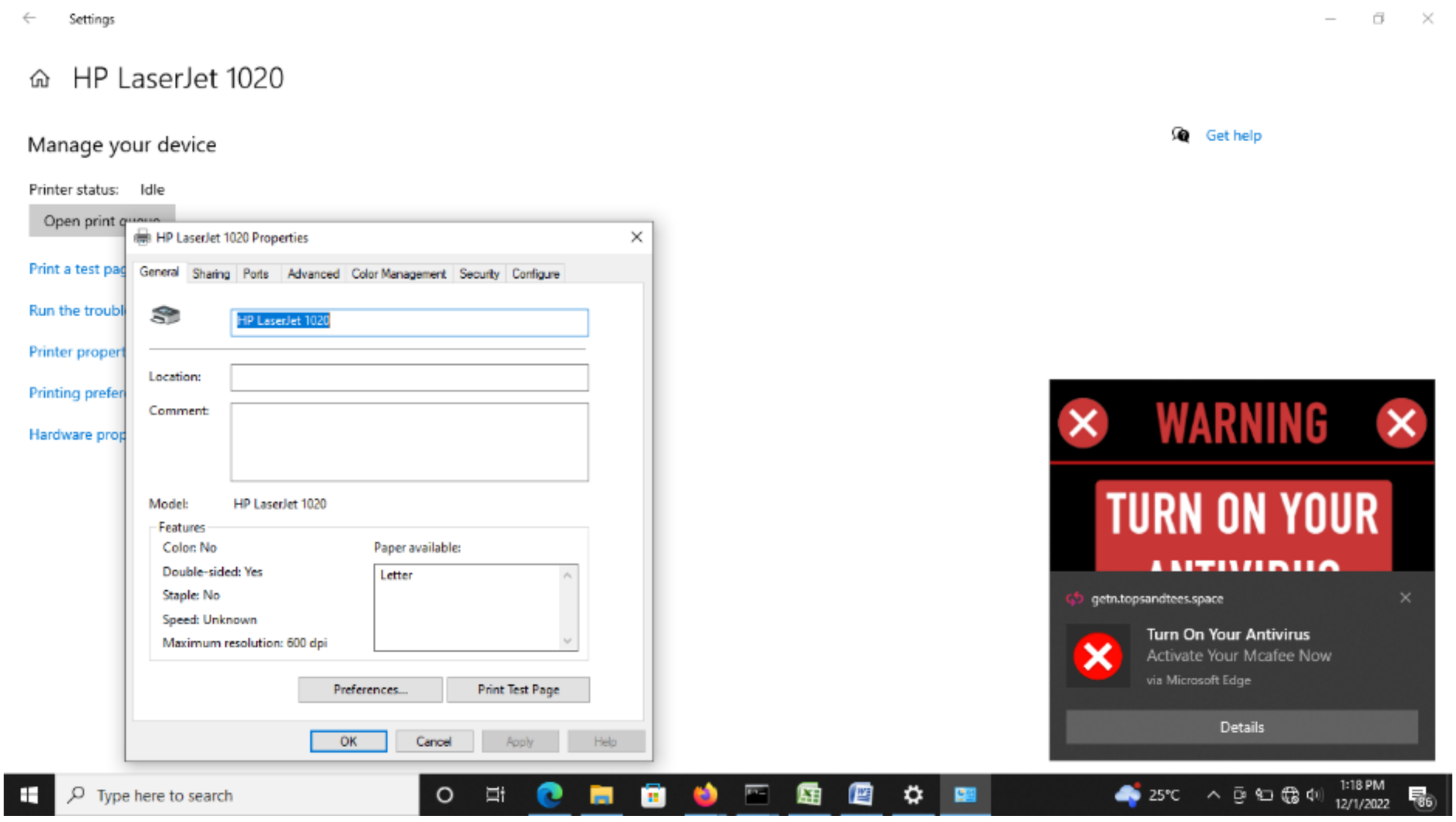


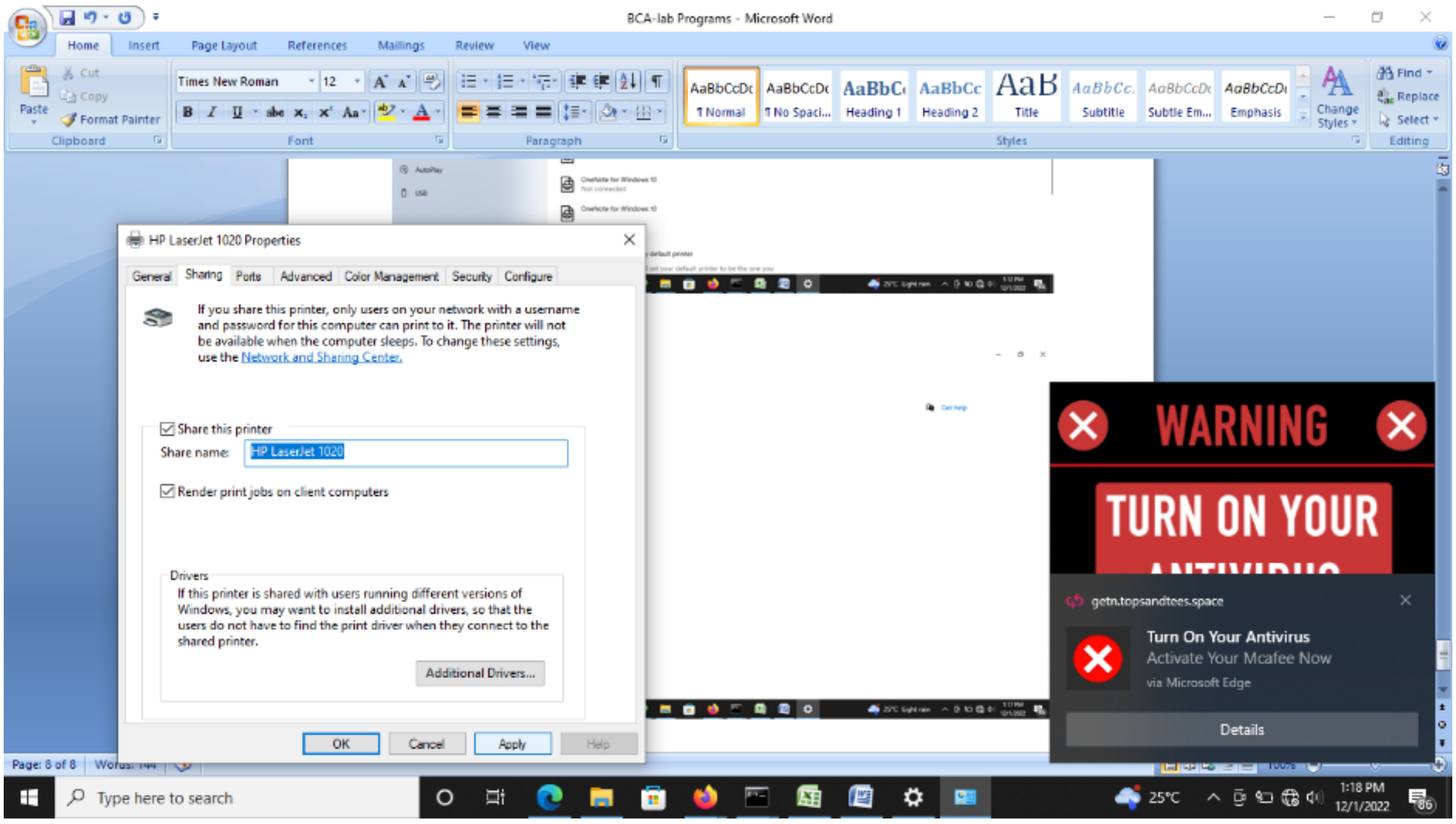
Manage- printer properties



Print and scanners-Share

Printer properties



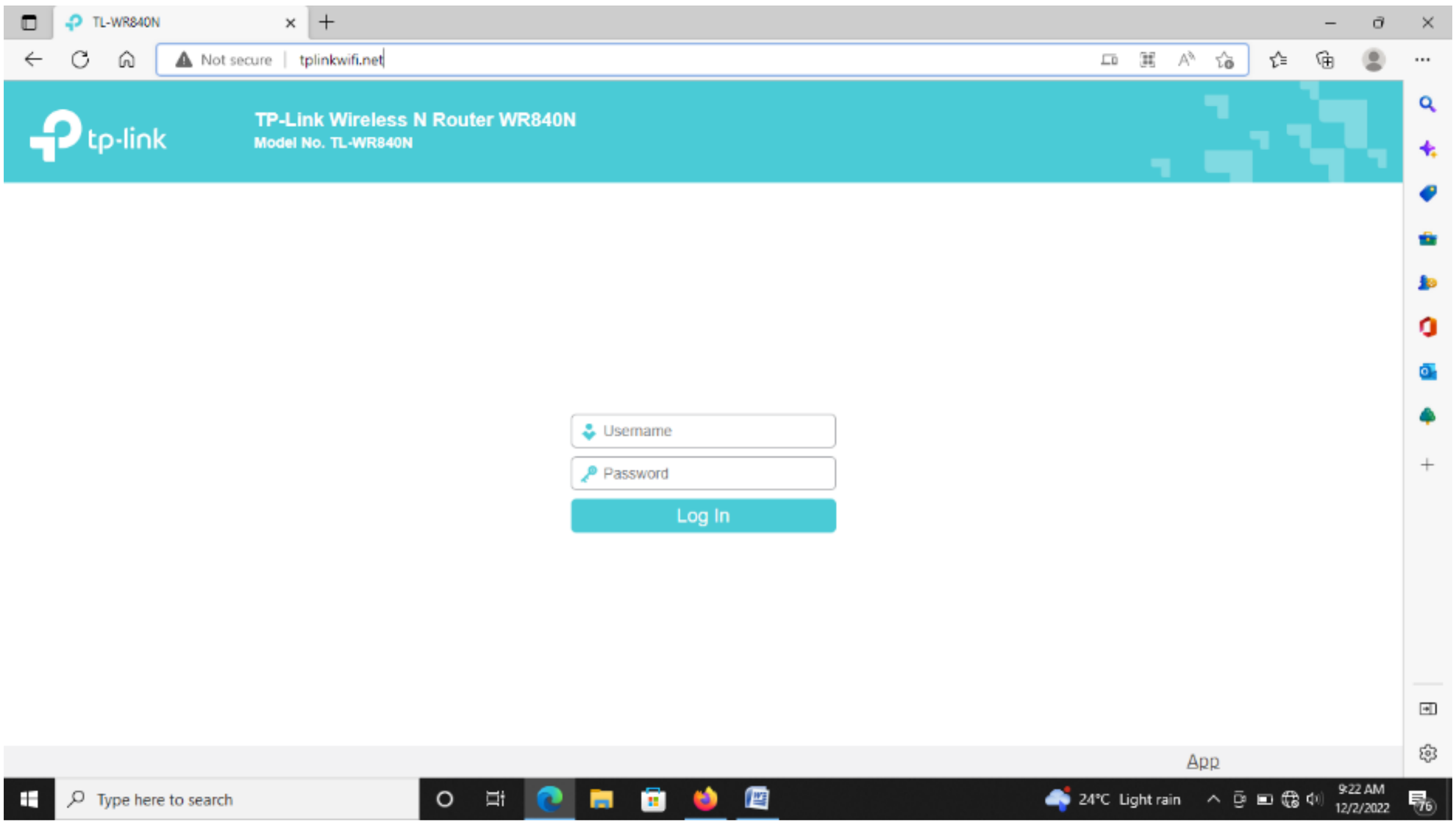

BCA-lab Programs - Microsoft Word
Home
Insert
Page Layout
References
Mailings
Review
View
Paste
Cut
Copy
Format Painter
Clipboard
Times New Roman
12
Font
Paragraph
Normal
No Spaci...
Heading 1
Heading 2
Title
Subtitle
Subtle Em...
Emphasis
Change Styles
Find
Replace
Select
Editing
Styles
HP LaserJet 1020 Properties
General
Sharing
Ports
Advanced
Color Management
Security
Configure
If you share this printer, only users on your network with a username and password for this computer can print to it. The printer will not be available when the computer sleeps. To change these settings, use the Network and Sharing Center.
Share this printer
Share name:
HP LaserJet 1020
Render print jobs on client computers
Drivers
If this printer is shared with users running different versions of Windows, you may want to install additional drivers, so that the users do not have to find the print driver when they connect to the shared printer.
Additional Drivers...
OK
Cancel
Apply
Help
WARNING
TURN ON YOUR
getn.topsandtees.space
Turn On Your Antivirus
Activate Your Mcafee Now
via Microsoft Edge
Details
Page: 8 of 8
Type here to search
25°C
1:18 PM
12/1/2022

Program11: configuring wifi and connect other devices

Connect the wifi access point to the PC through Ethernet port and supply the power

Go to the browser and type: the URL/IP address present on the back of the access point.

Example: http://tplinkwifi.net/ OR default IP address present at the back of the ip address.



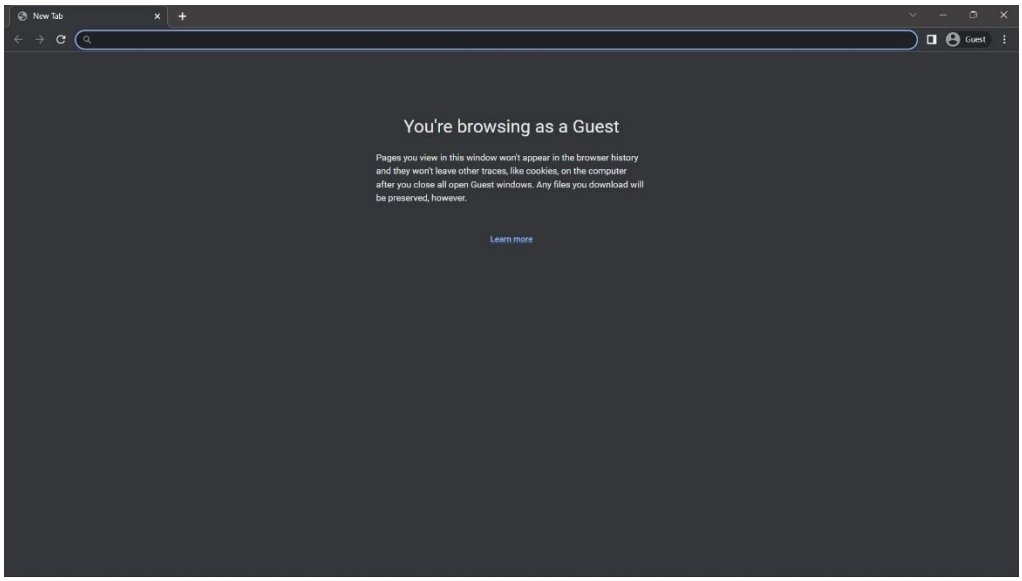
11. Configuration of WIFI hotspot, and connect other Devices (mobile/laptop).

A.

1. Connect the Hotspot Device to the Internet Using the Cable.

2. Connect the Laptop/Mobile to the device using wire/wireless.

3. Open any web Browser.

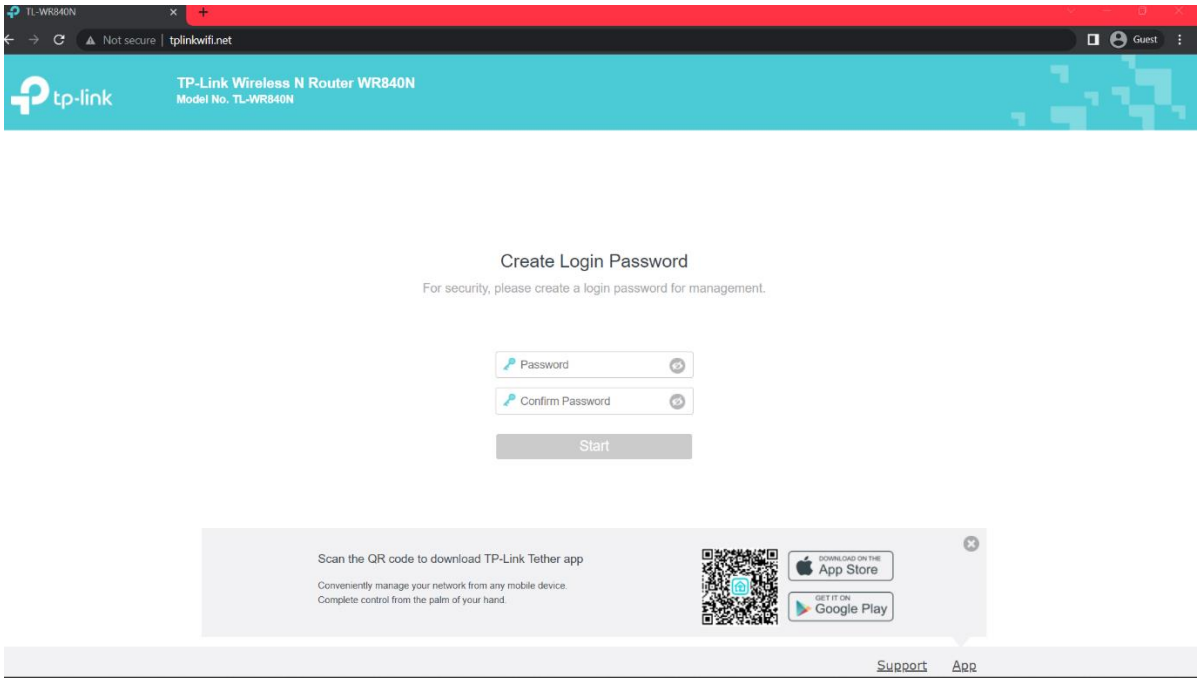


4. Enter the default access address in the browser address bar.

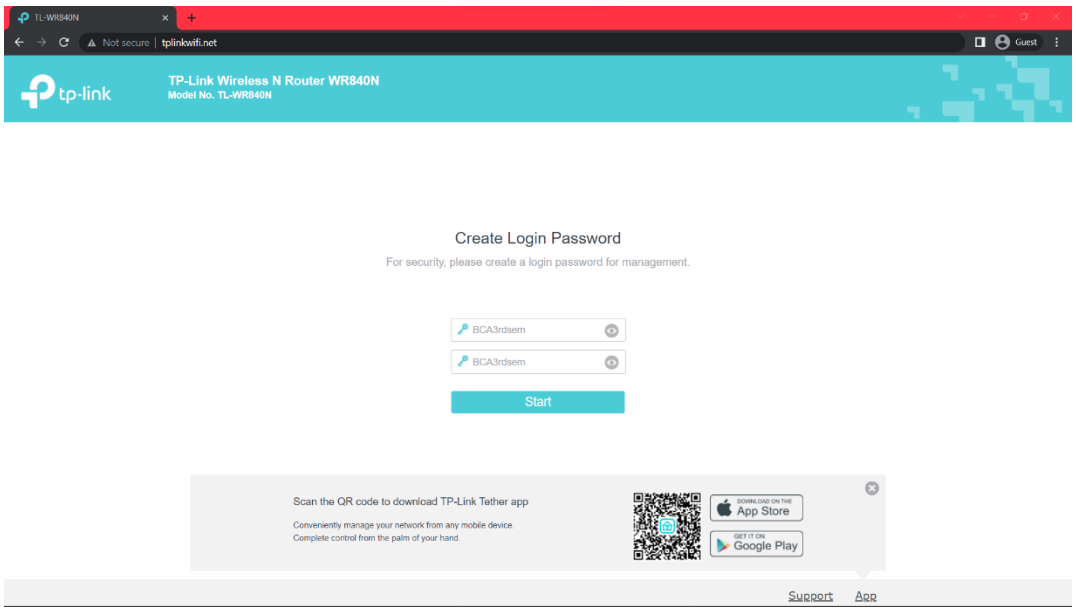
192.168.0.1

192.168.1.1

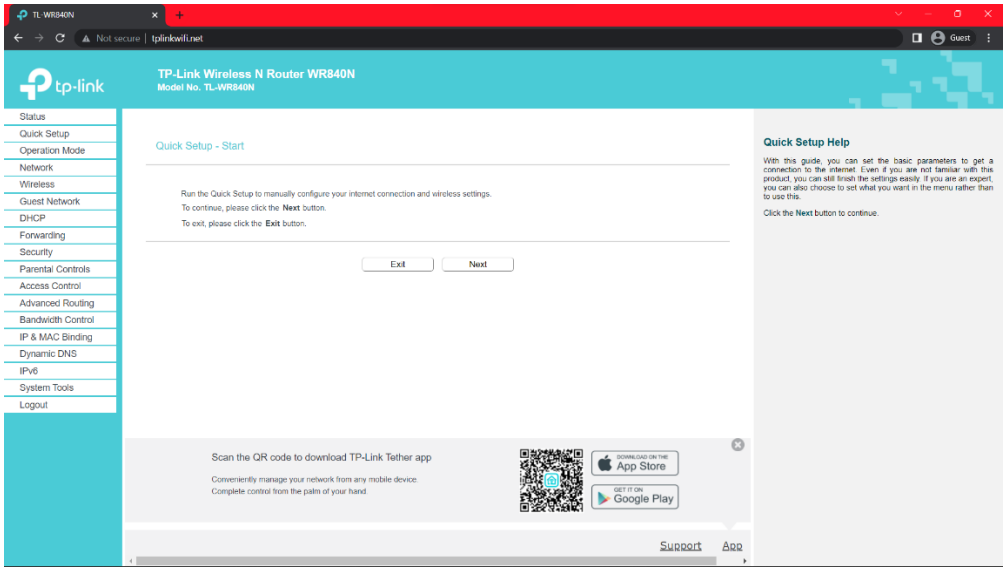
Tplinkwifi.net



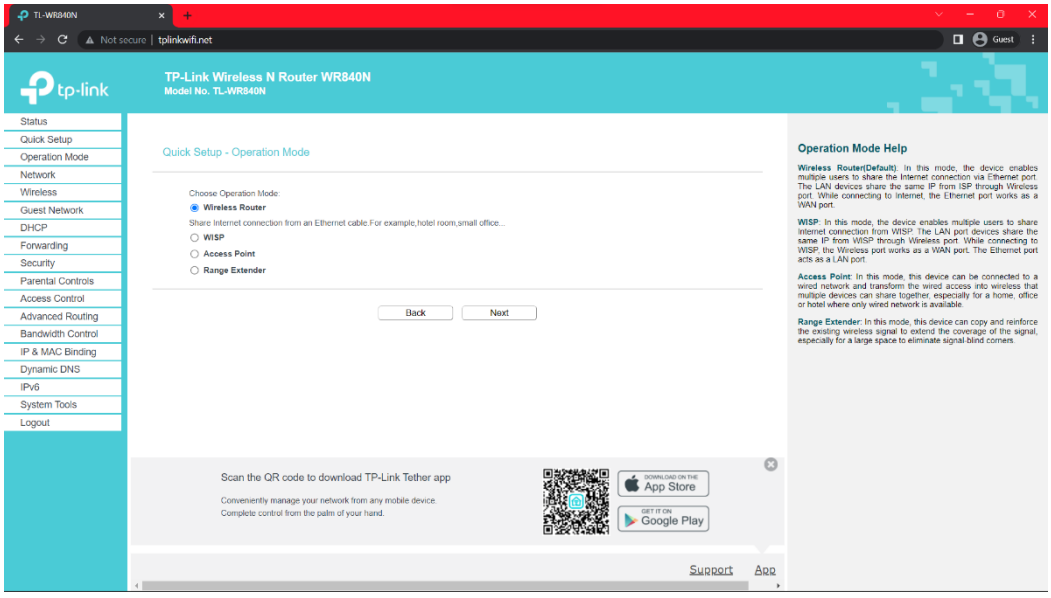
5. Create a new admin password (to access the device settings not WIFI) and click ok (Let's Get Started).



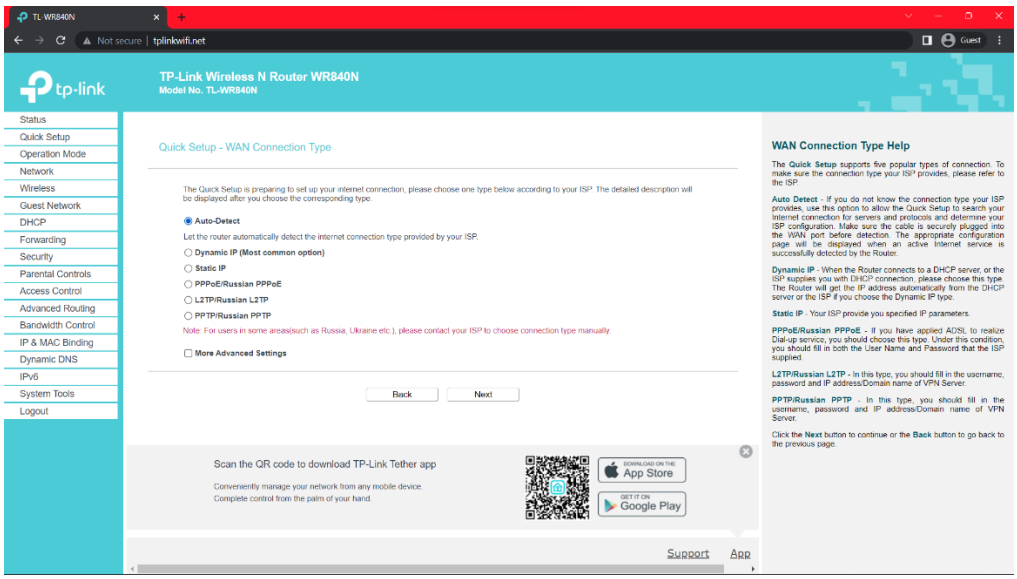
6. Select Quick Setup tab and click next.



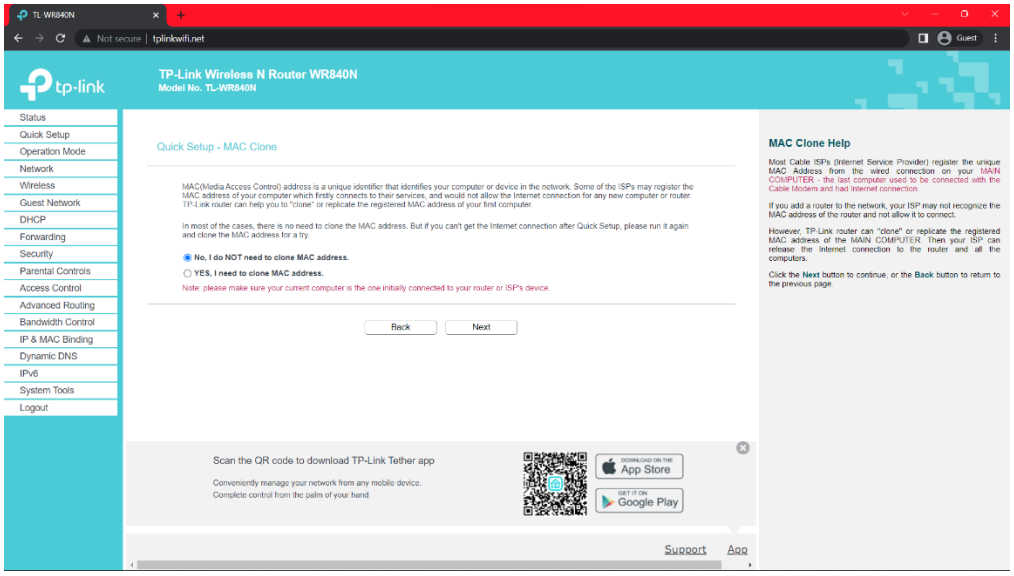
7. In operation mode select Wireless Router and click next.



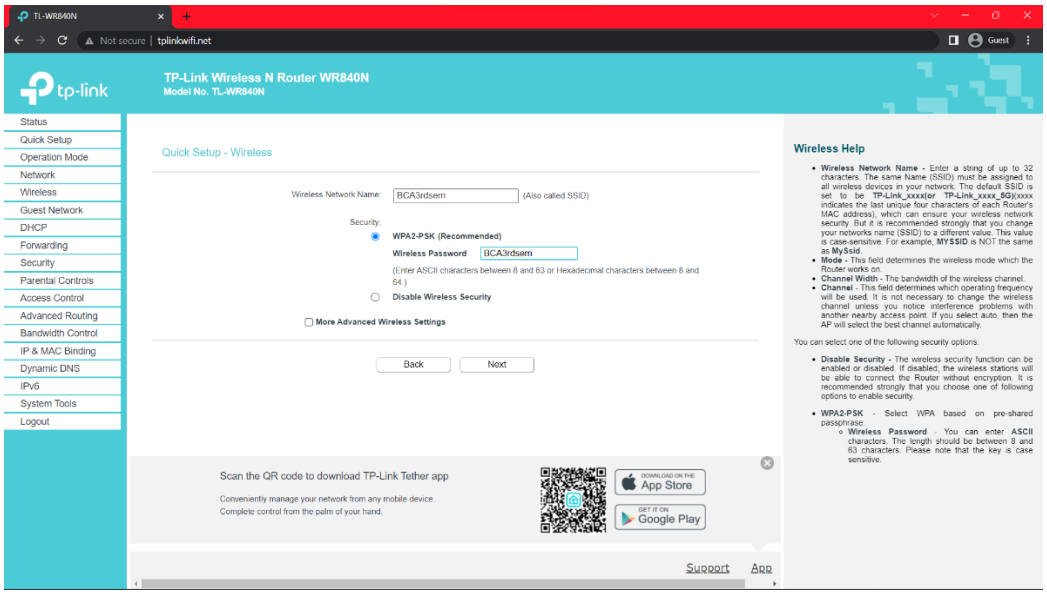
8. In WAN Connection Type click on Auto Detect and then click next.



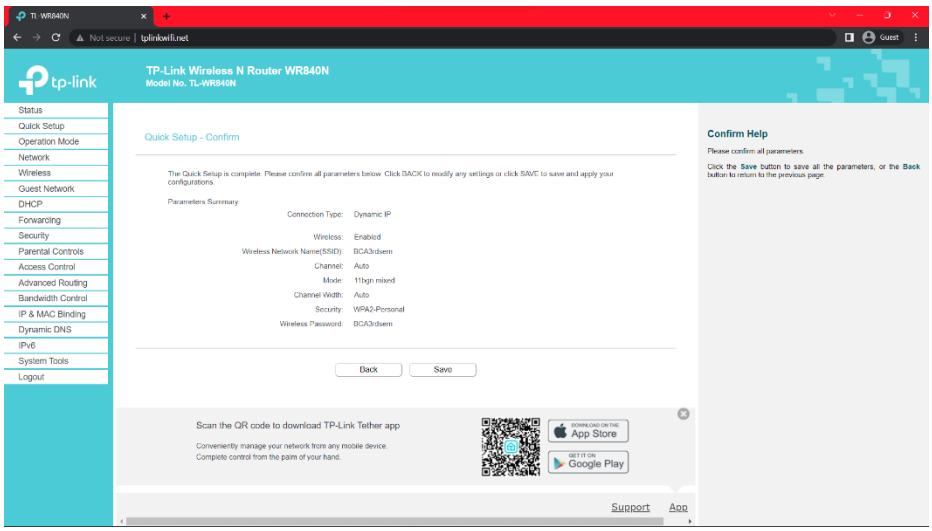
9. in MAC Clone Click on “No, I do NOT need to clone MAC address.” And then click next.



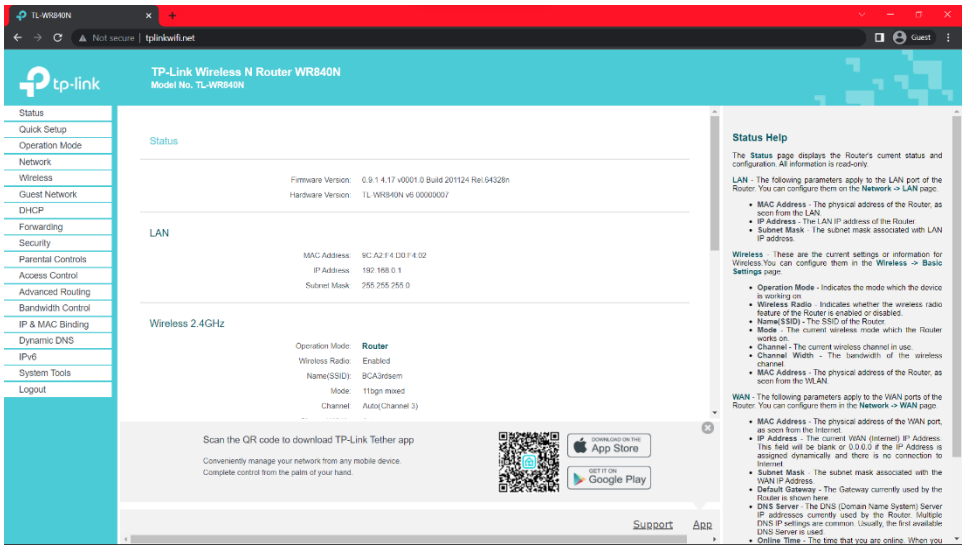
10. In Wireless options set WIFI Name, Password type and password and then click next.



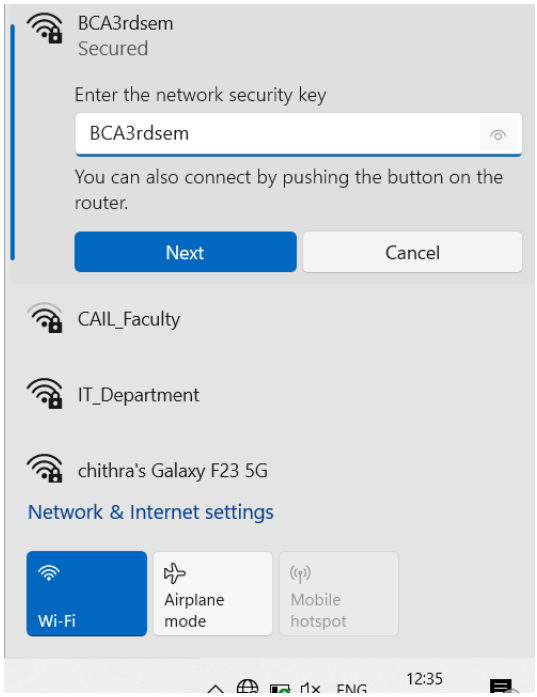
11. Click Save The settings will be set.



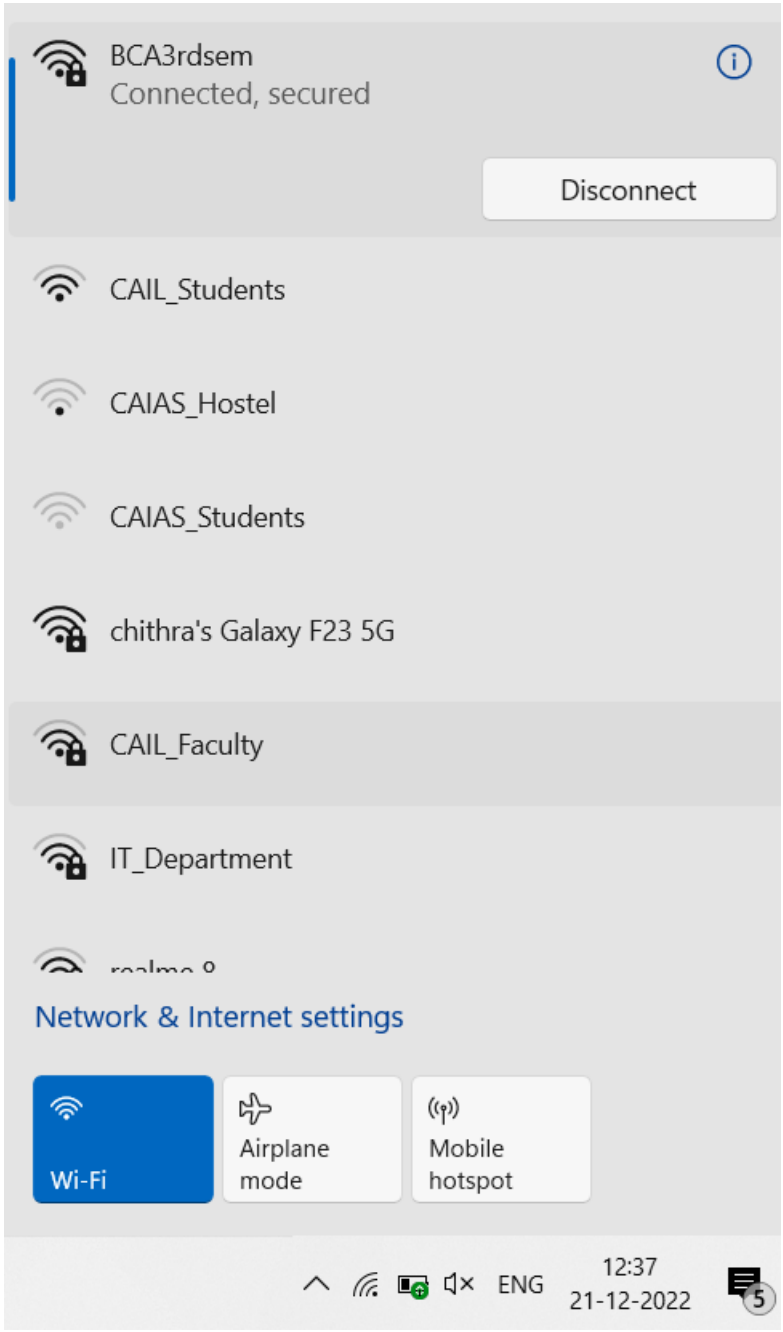
12. The Setting of the Router will be set and seen.



13. Connect the WIFI From other device.



14. The WIFI Gets Connected.

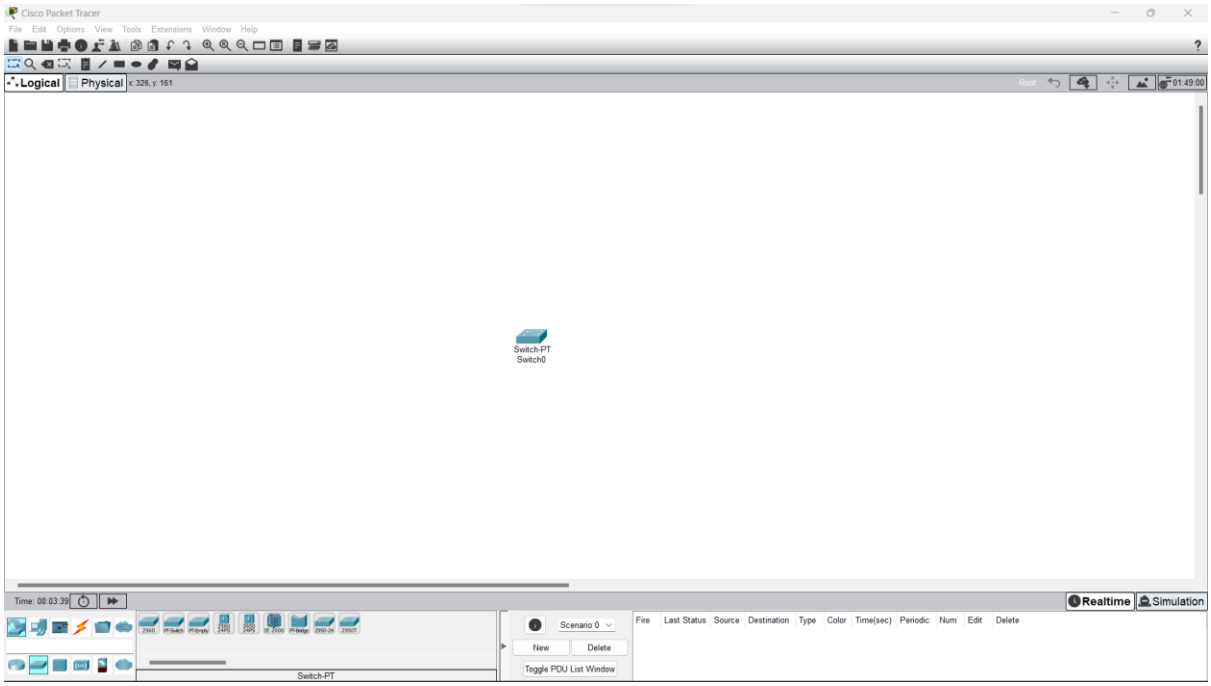

BCA3rdsem
Connected, secured
Disconnect
CAIL_Students
CAIAS_Hostel
CAIAS_Students
chithra's Galaxy F23 5G
CAIL_Faculty
IT_Department
Network & Internet settings
Wi-Fi
Airplane mode
Mobile hotspot
ENG
12:37
21-12-2022
5

Program 12:

Configuration of switches.

Step 1: Open cisco packet tracer.

Step 2: Select a switch from the network devices in the bottom left corner.



Step 3: Configure the Host name of the switch0.

- Click on switch0 and go to Command Line Interface (CLI).
- The change the hostname to “BCA”

Command:

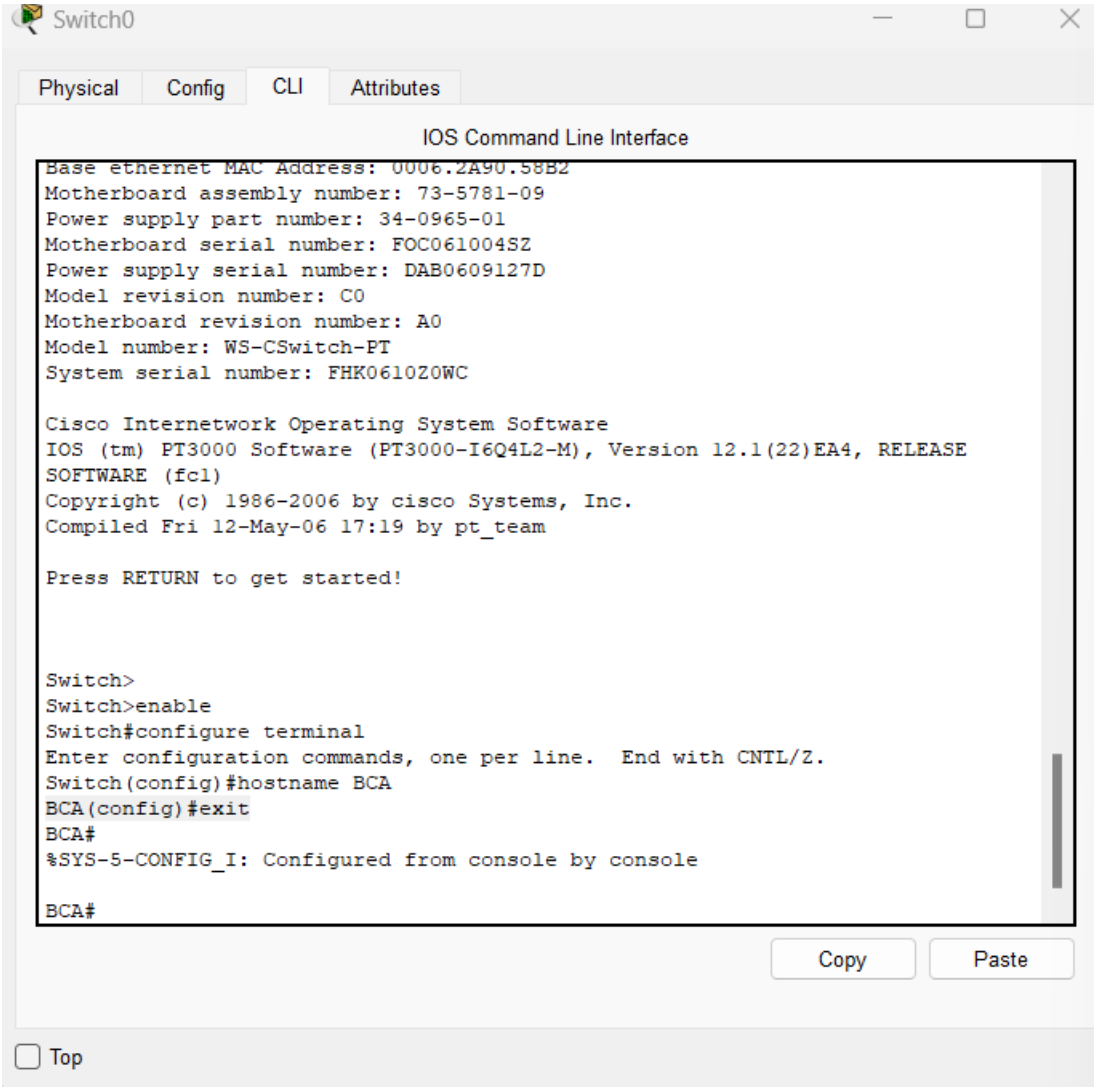
Switch>

Switch>enable

Switch#configure terminal

Switch(config)#hostname BCA

BCA(config)#exit



Step 4: Set up line control password and enable secret password

Commands:

BCA(config)#line con 0

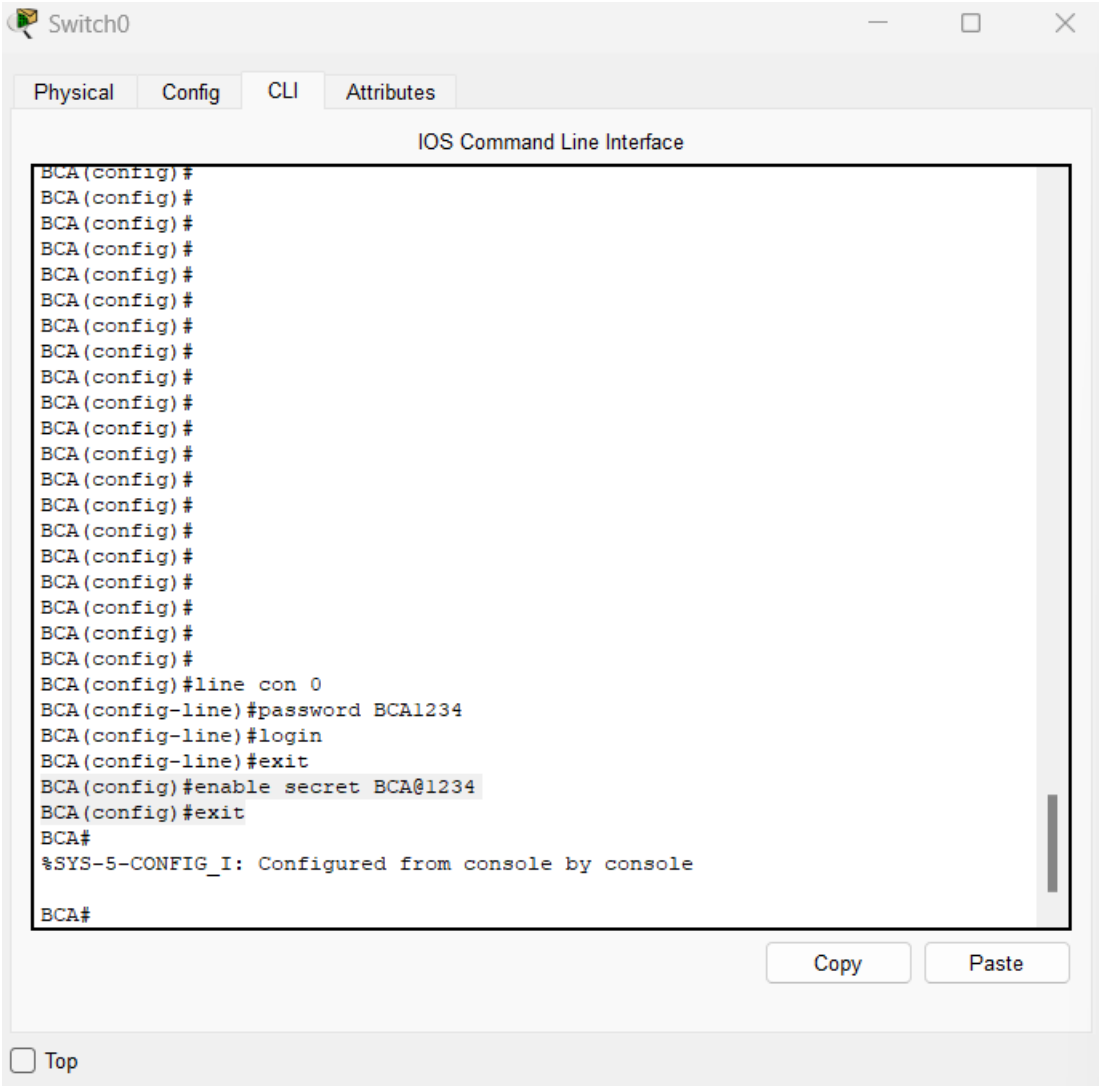
BCA(config-line)#password BCA1234

BCA(config-line)#login

BCA(config-line)#exit

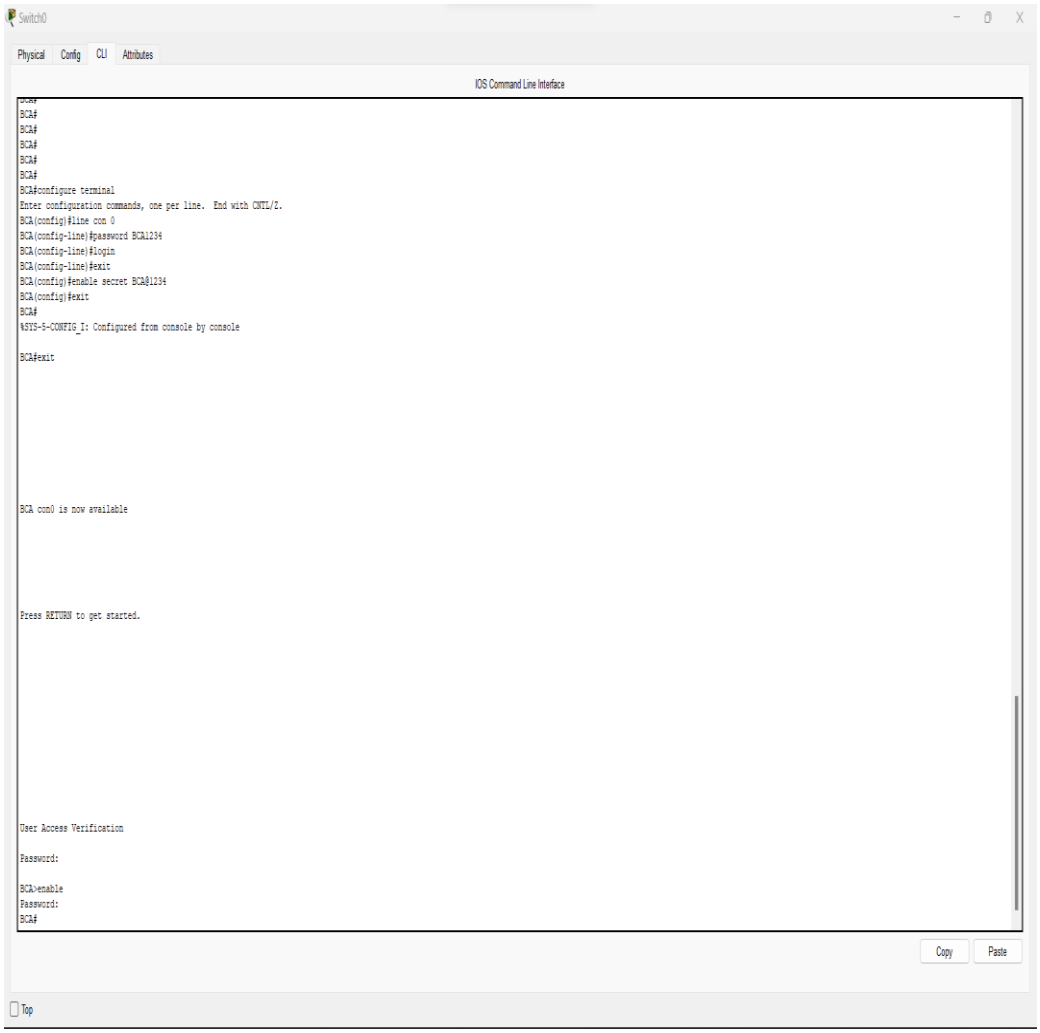
BCA(config)#enable secret BCA@1234

BCA(config)#exit



Step 5: Verify the password

- When you try to log in first it will ask for the line control password.
- Then, to configure terminal it will ask enable a secret password.


Switch0
Physical
Config
CLI
Attributes
IOS Command Line Interface
BCA#
BCA#
BCA#
BCA#
BCA#
BCA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BCA(config)#line con 0
BCA(config-line)#password BCA1234
BCA(config-line)#login
BCA(config-line)#exit
BCA(config)#enable secret BCA@1234
BCA(config)#exit
BCA#
%SYS-5-CONFIG_I: Configured from console by console
BCA#exit
BCA con0 is now available
Press RETURN to get started.
User Access Verification
Password:
BCA>enable
Password:
BCA#
Copy
Paste
Top

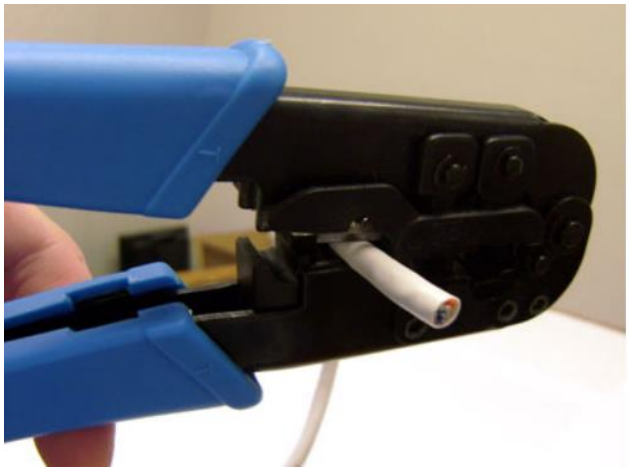
PROGRAM 16:

Making your own patch cord.

Tools and parts you need:

- Cat5e or Cat6e Cable
- RJ45 connector
- Crimping Tool

Step 1: Stripping out the outer jacket

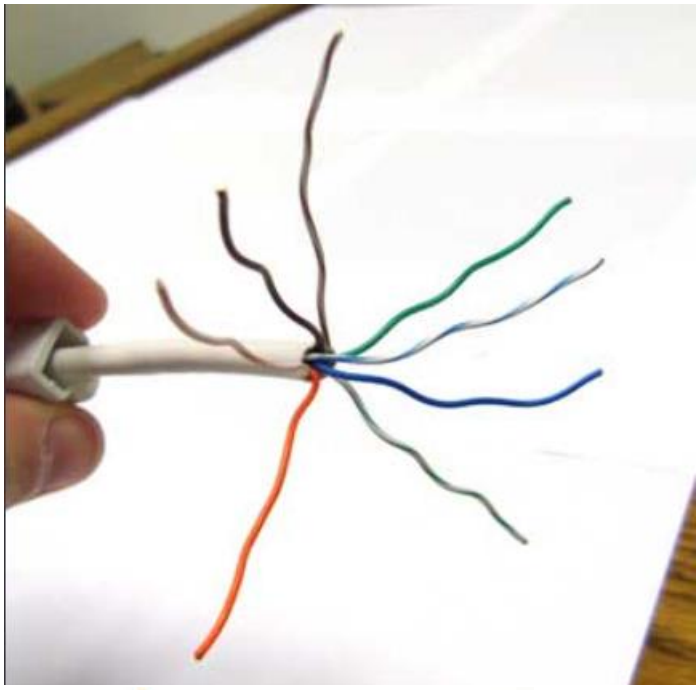


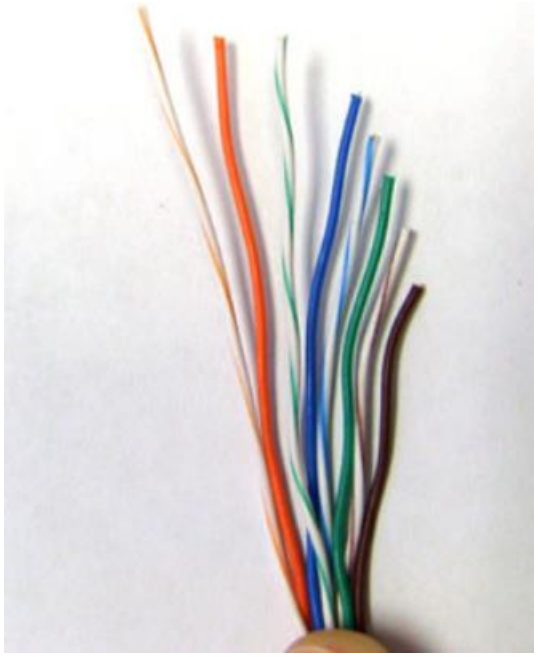
After striping out the outer jacket with the crimping tool we will have four twisted pairs exposed with enough room to straighten them out and organize them.

Step 2: Organising and Lining up the wire

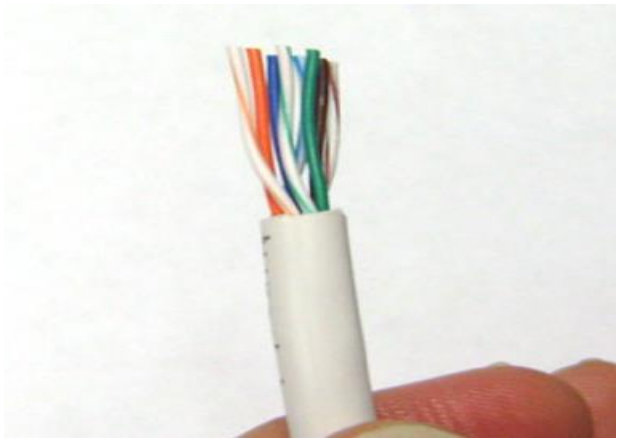
Straighten the twisted pairs and arrange in in the following colour code:

- Orange/white
- Orange
- Green/White
- Blue
- Blue/White
- Green
- Brown/White
- Brown



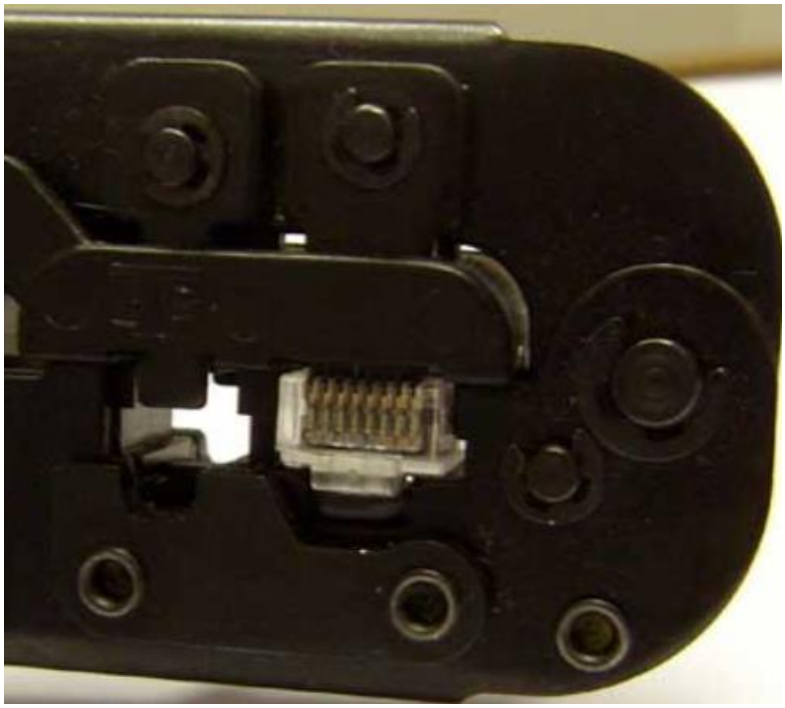


Step 3: Trim the wires with the crimping tool to make all of them even



Step 4: Insert the wires carefully into the RJ45 connector

Step 5: Crimp the connector with the crimping tool.



The cable is finished

Repeat the same steps from 1 to 5 on the opposite side of the cable to finish making your own patch cord.

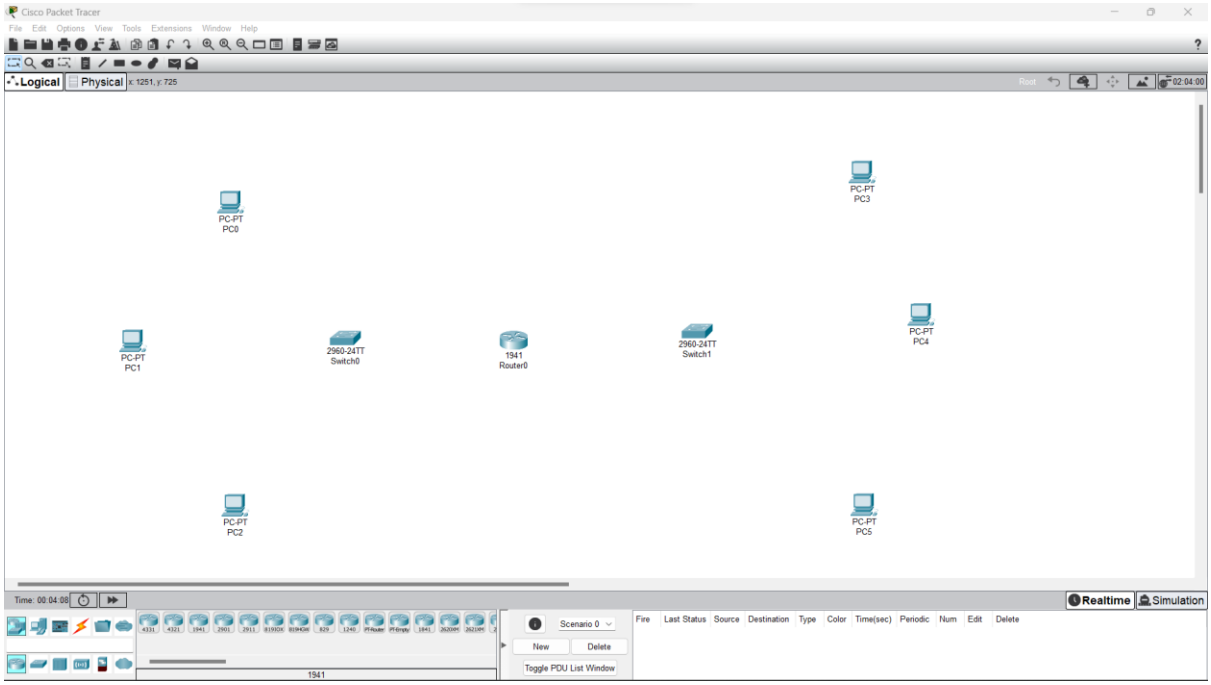
Program 15:

Configure VLAN using Packet Tracer/GNS3

Step 1: Open cisco packet tracer.

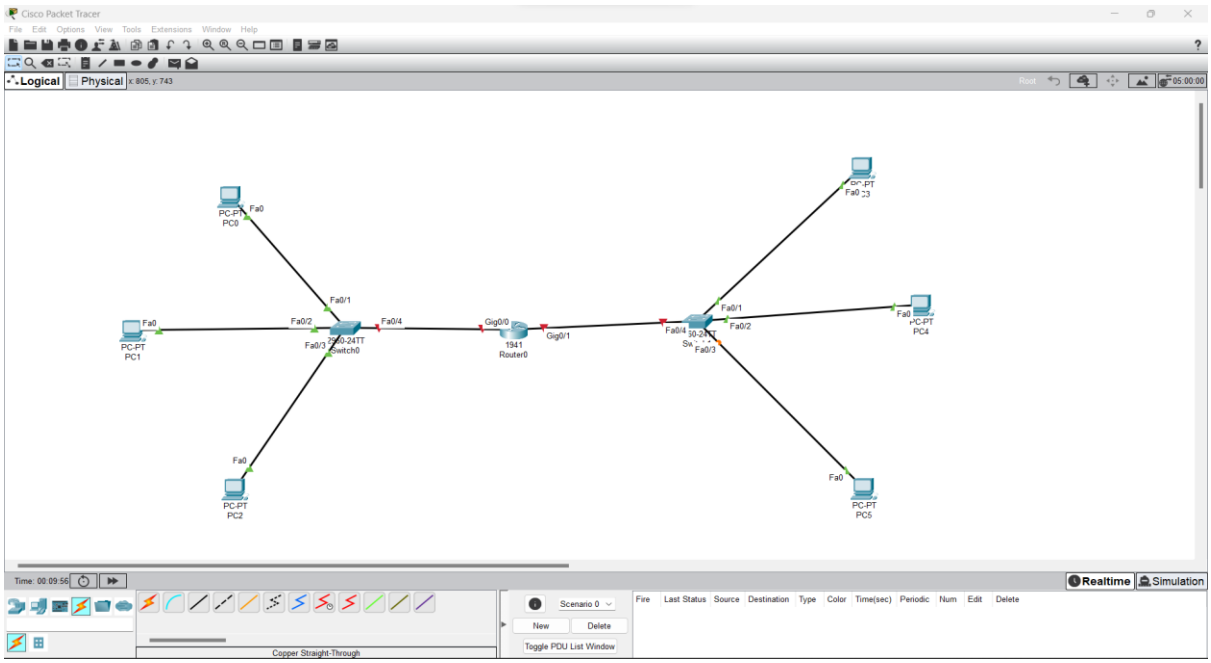
Step 2: Insert six PCs, 2 Switches and 1 router(1941).

The devices are available in the bottom right corner of the window.



Step 3: Connect all the devices using copper straight through cables.

Use the fast ethernet ports for connecting PCs to switches (fast Ethernet 0 to fast Ethernet 0/1 or 0/2 or 0/3 depending on the free ports)and fast Ethernet port to Gigabit ethernet port to connect switch to router.

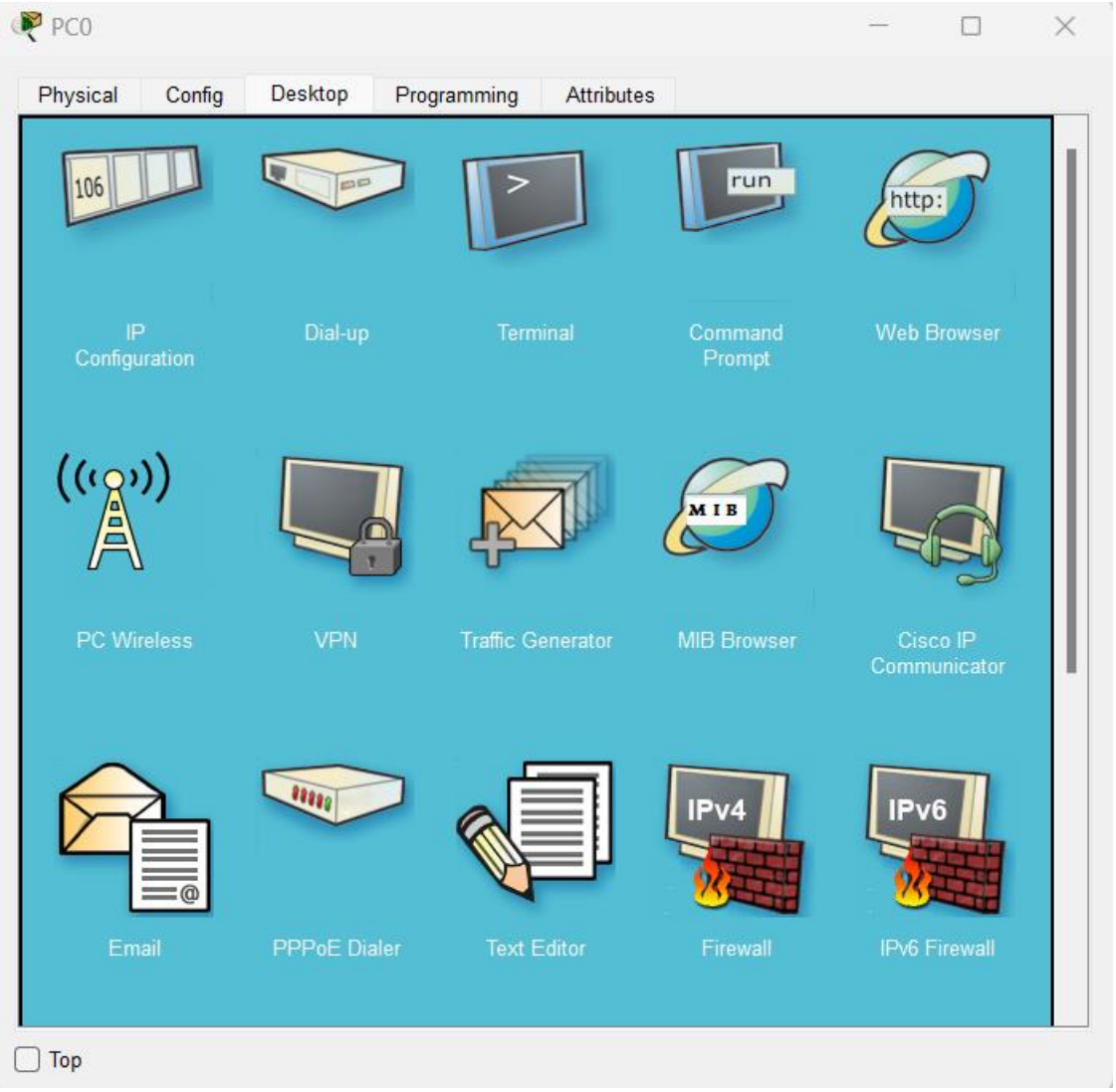


Step 4: Start configuring the devices:

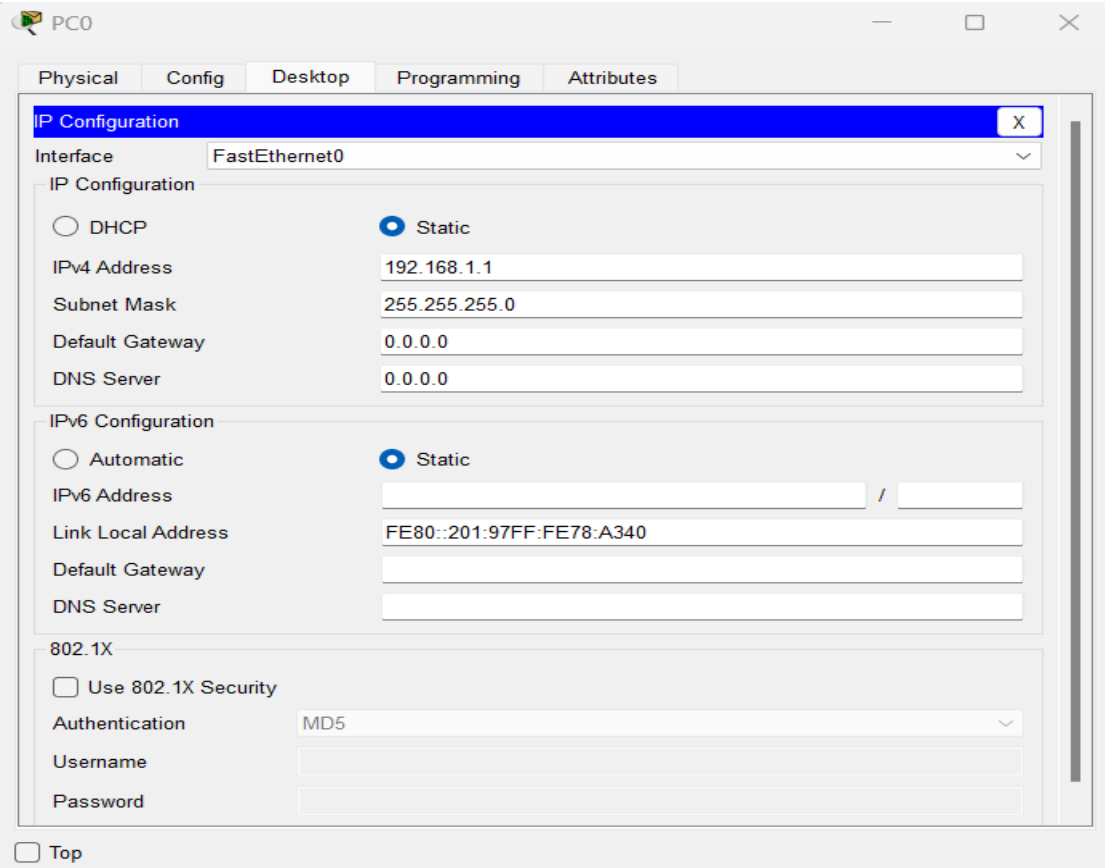
For PCs connected to Switch0(LAN A):

- We can set ip addresses from Class A range
- PC0 will be 192.168.1.1
- PC1 will be 192.168.1.2
- PC2 will be 192.168.1.3

Now leftclick on PC0 and then chose the desktop tab and then ip configuration



Now fill in the IPv4 Address as 192.168.1.1 and the subnet mask will fill automatically

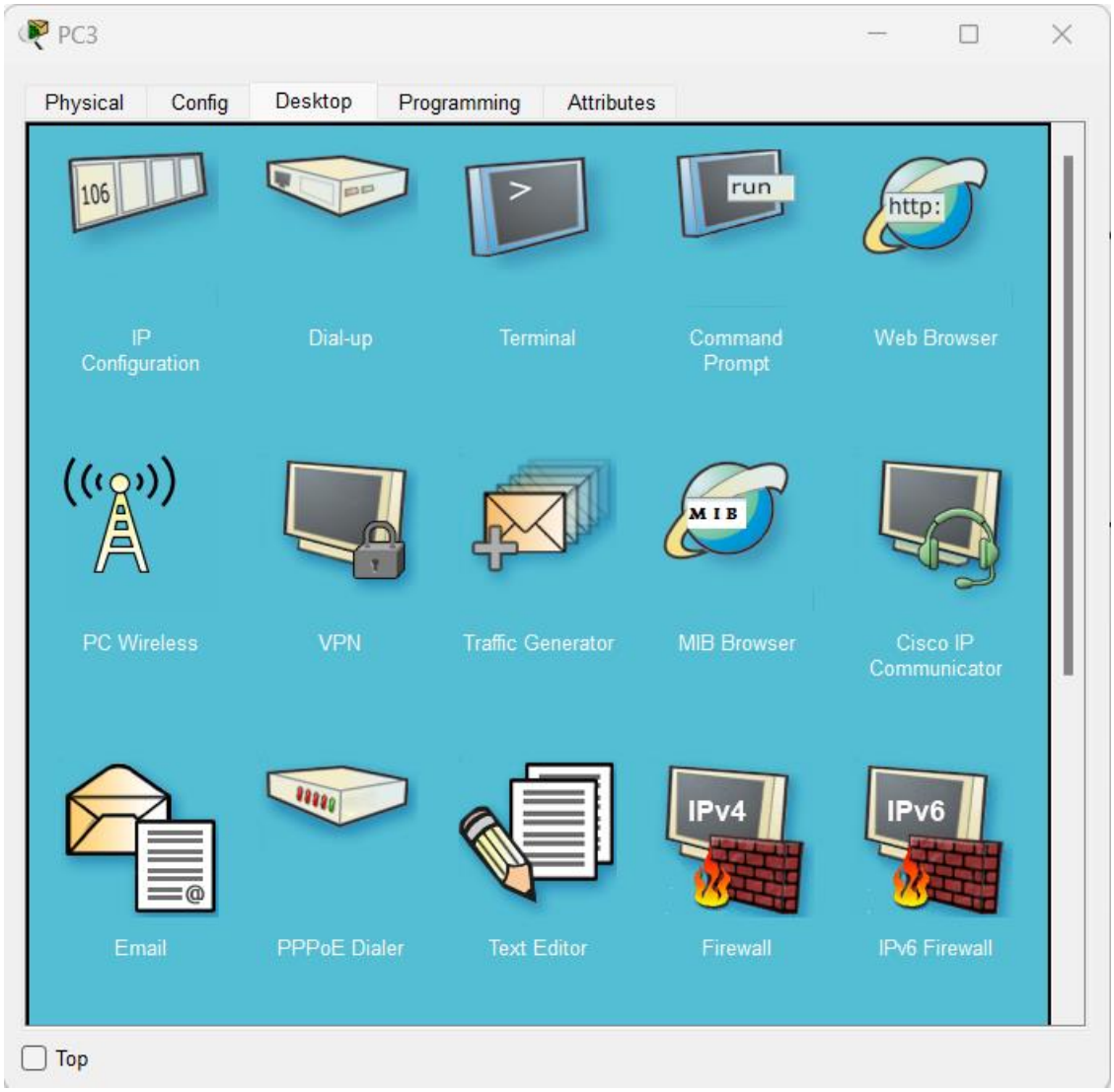


Repeat the steps for all the other PCs connected to Switch0

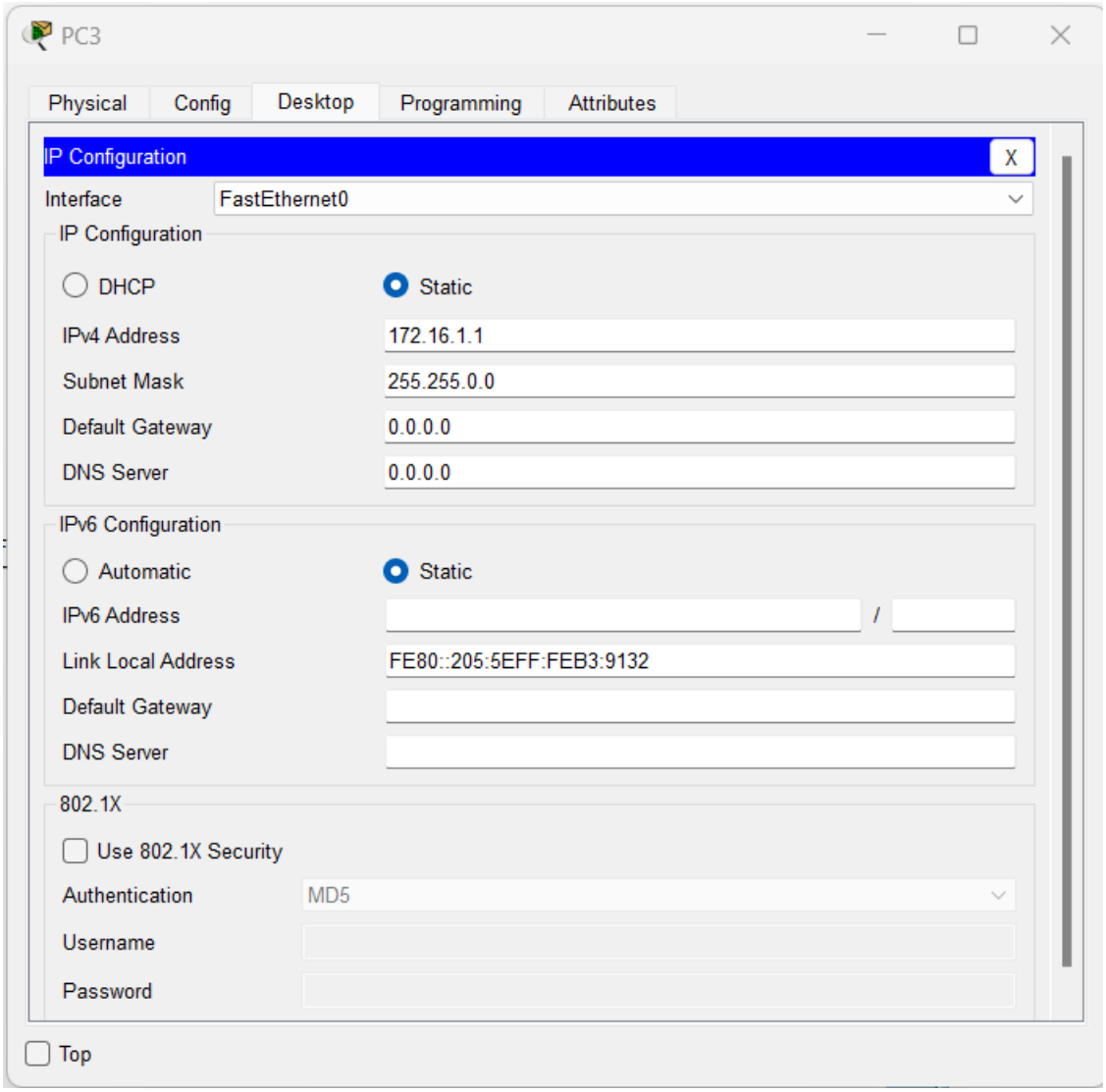
For PCs connected to Switch1(LAN B):

- We can set ip addresses from Class B range
- PC3 will be 172.16.1.1
- PC4 will be 172.16.1.2
- PC5 will be 172.16.1.3

Now leftclick on PC3 and then chose the desktop tab and then ip configuration



Now fill in the IPv4 Address as 172.16.1.1 and the subnet mask will fill automatically.



Repeat the steps for all the other PCs connected to Switch1

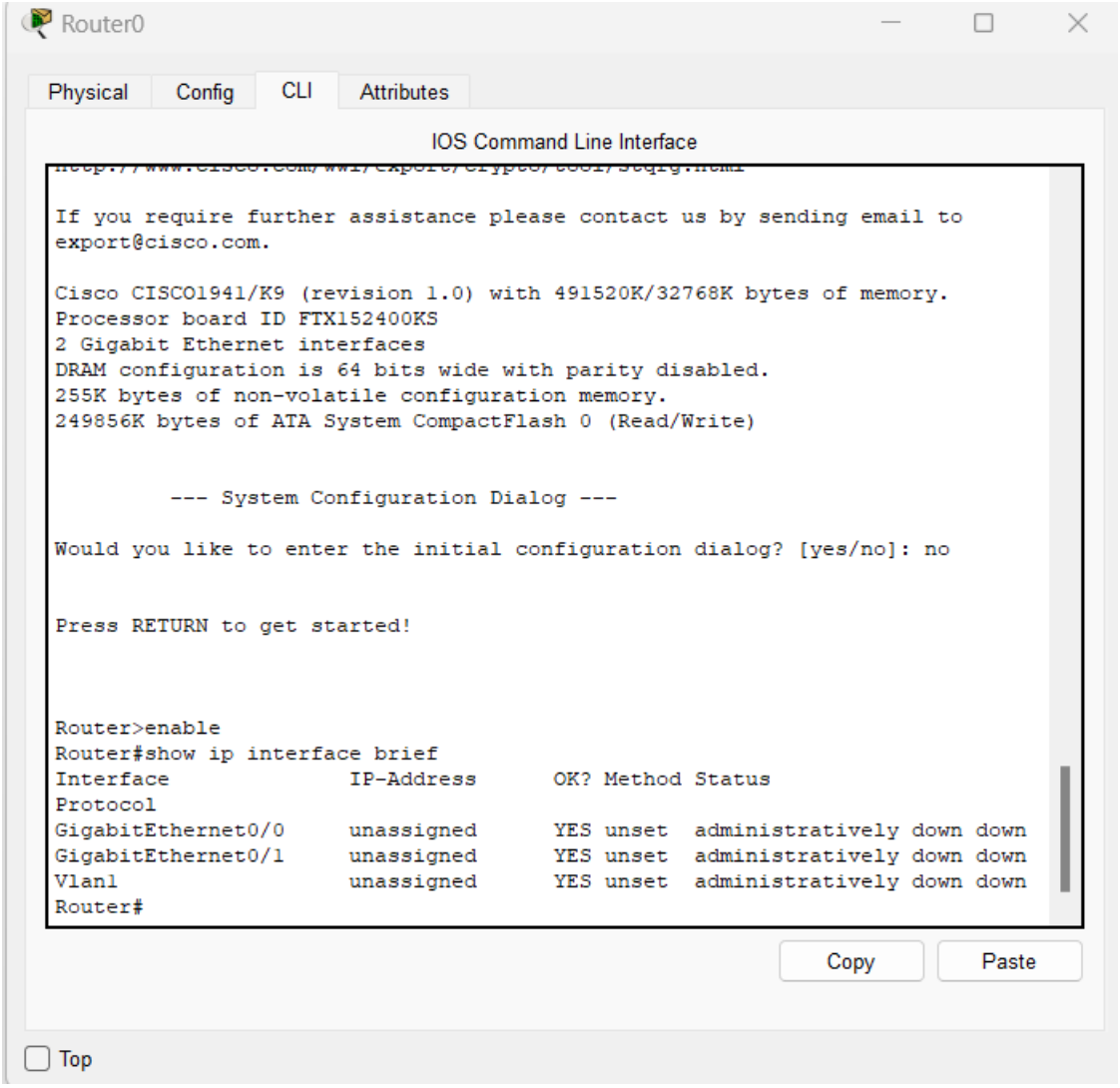
Step 5: Configure the router

Leftclick on the router and go to the CLI tab.

Use the following commands

Router>enable

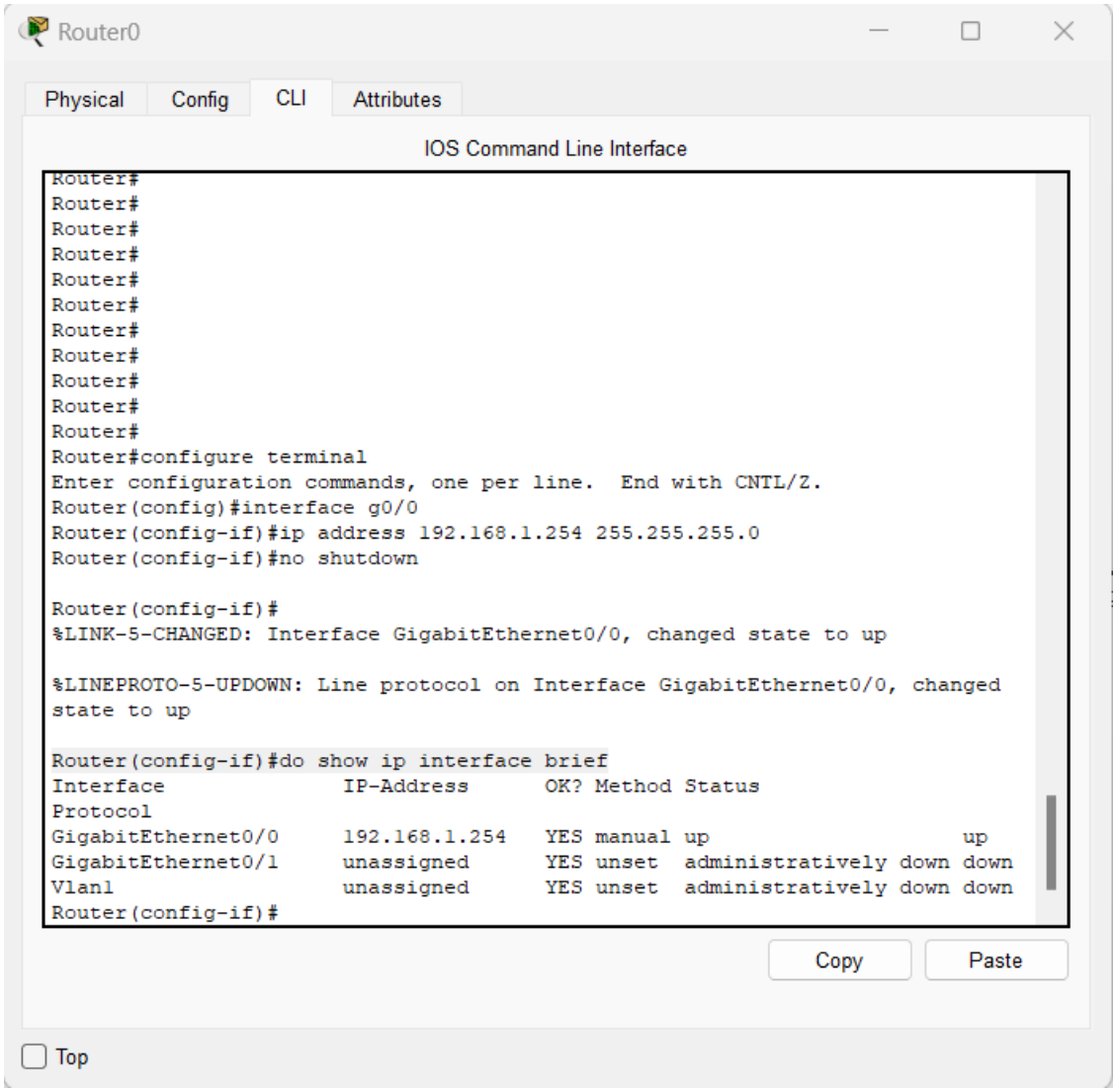
Router#show ip interface brief



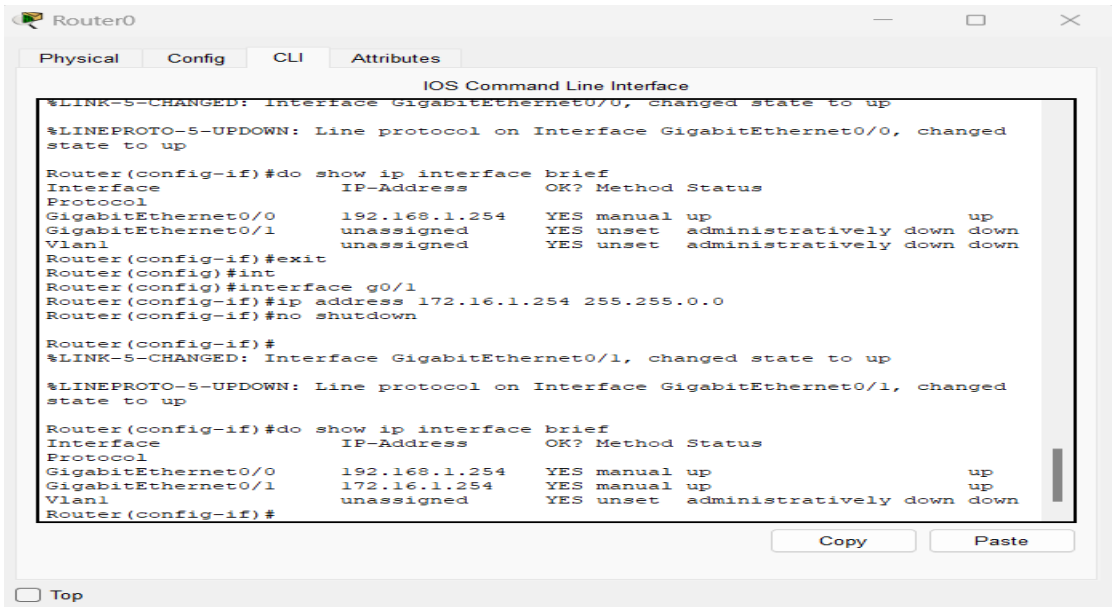
You can see that the gateways are not assigned and the status is down

Now we have to assign ip address first to GigabitEthernet0/0 then to GigabitEthernet0/1

- GigabitEthernet0/0:
  Use the following commands:
  Router#configure terminal
  Router(config)#interface g0/0
  Router(config-if)#ip address 192.168.1.254 255.255.255.0
  Router(config-if)#no shutdown
  Router(config-if)#do show ip interface brief



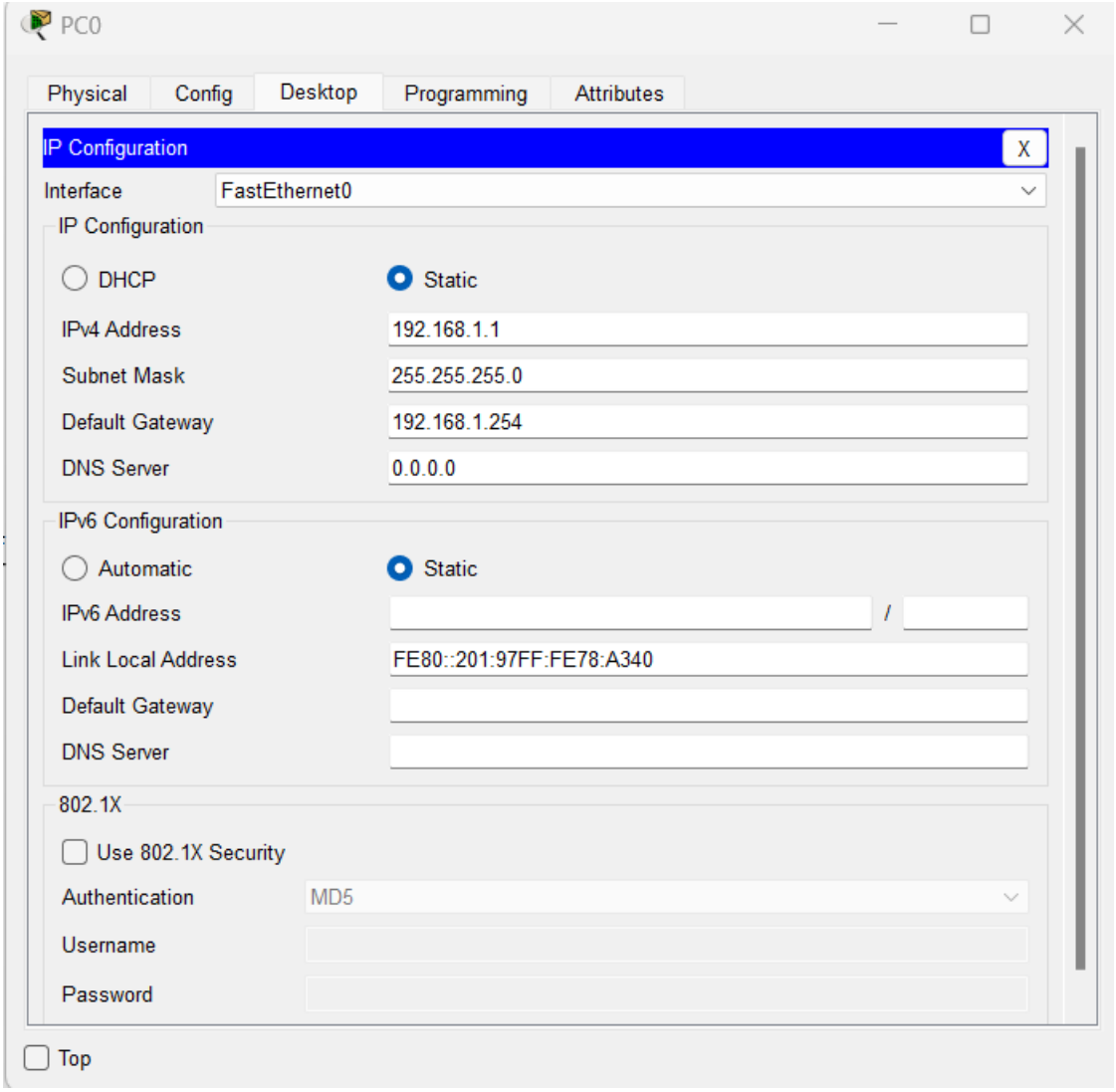
Repeat the same steps for g0/1

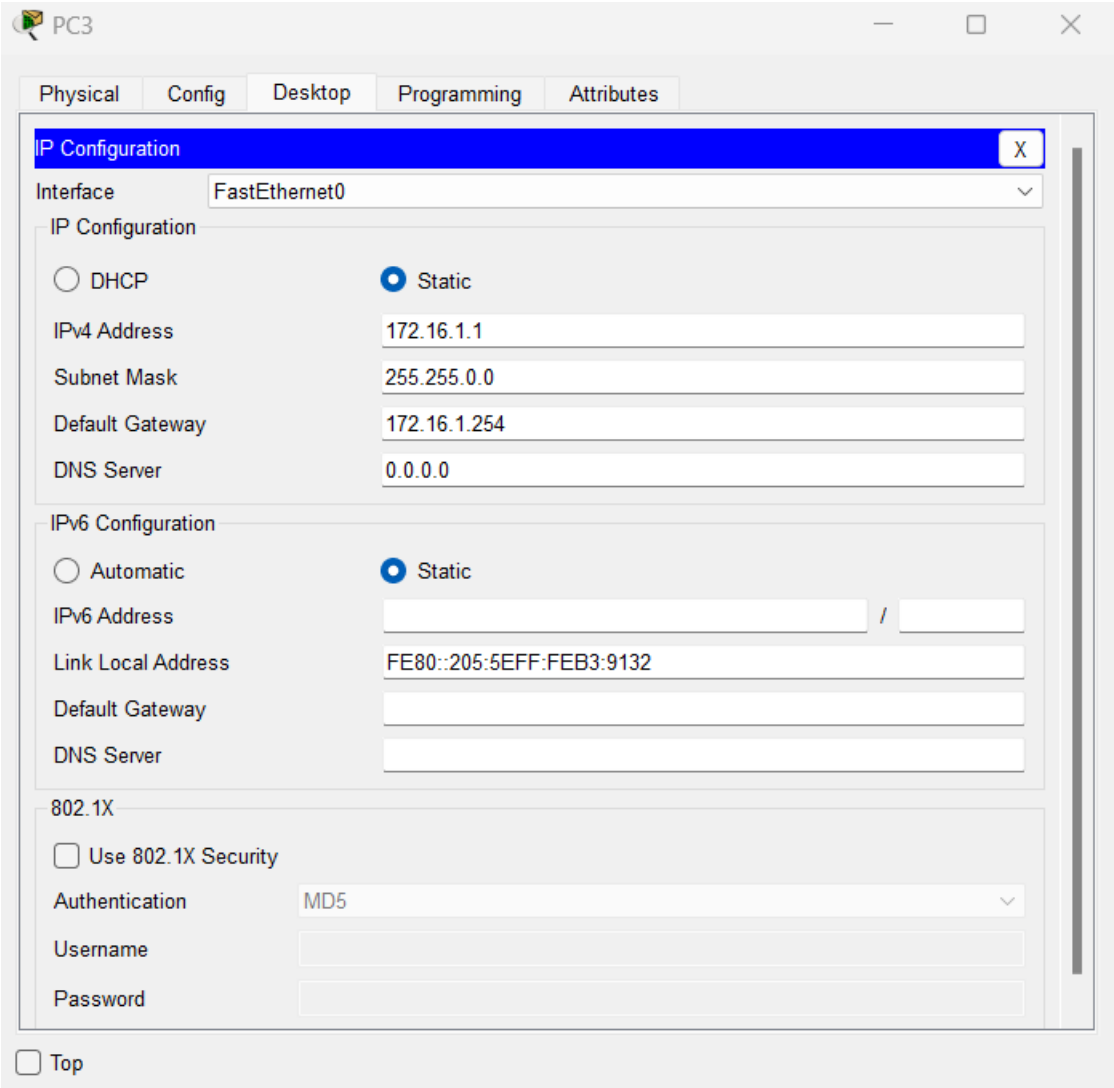


Now both the gateways are assigned with an ip address.

Step 6: assign the gateways to each PC.

- Leftclick on the PC
- Select Desktop Tab
- Select IP Configuration and assign the gateways as 192.168.1.254 for PCs connect to Switch0 and 172.16.1.254 for PCs connected to Switch1

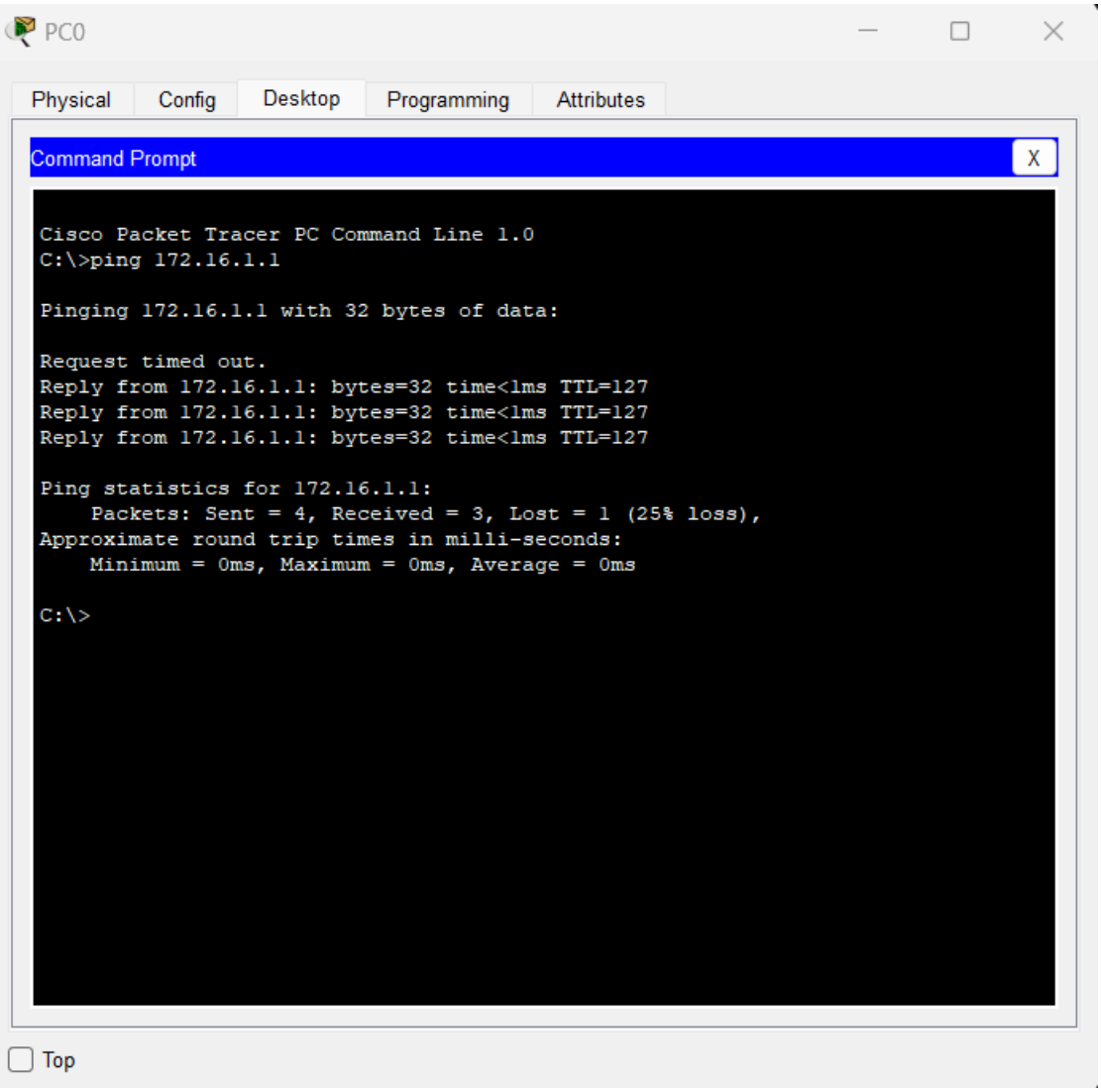




Step 7: check the connections between the two LANs

- Rightclick on PC0 select Desktop tab
- Then select Command Prompt and use the following command
  C:\>ping 172.16.1.1

You should receive the following output



Repeat this for all the ip addresses that you have assigned for each PC.

This shows that LAN A is connected to LAN B

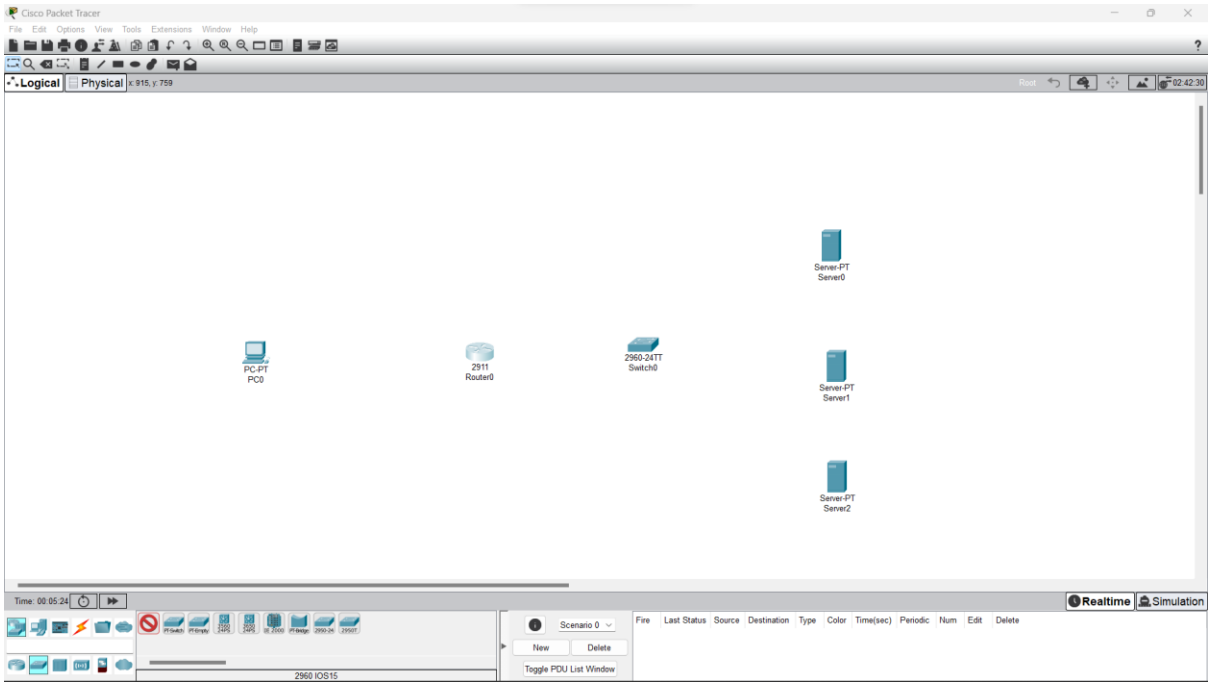
PROGRAM 16:

Configure VPN using Packet Tracer/GNS3

Step 1: Open cisco packet tracer.

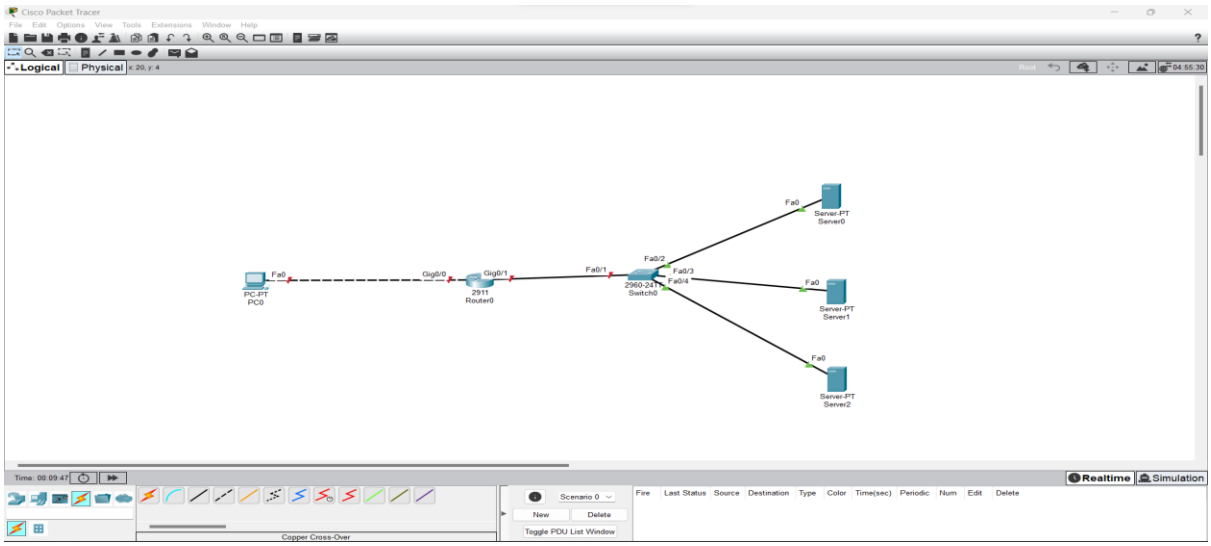
Step 2: Insert the following devices from the bottom left corner of the window.

- 1 router (2911)
- 1 switch
- 3 servers
- 1 Pcs



Step 3: connect all the devices

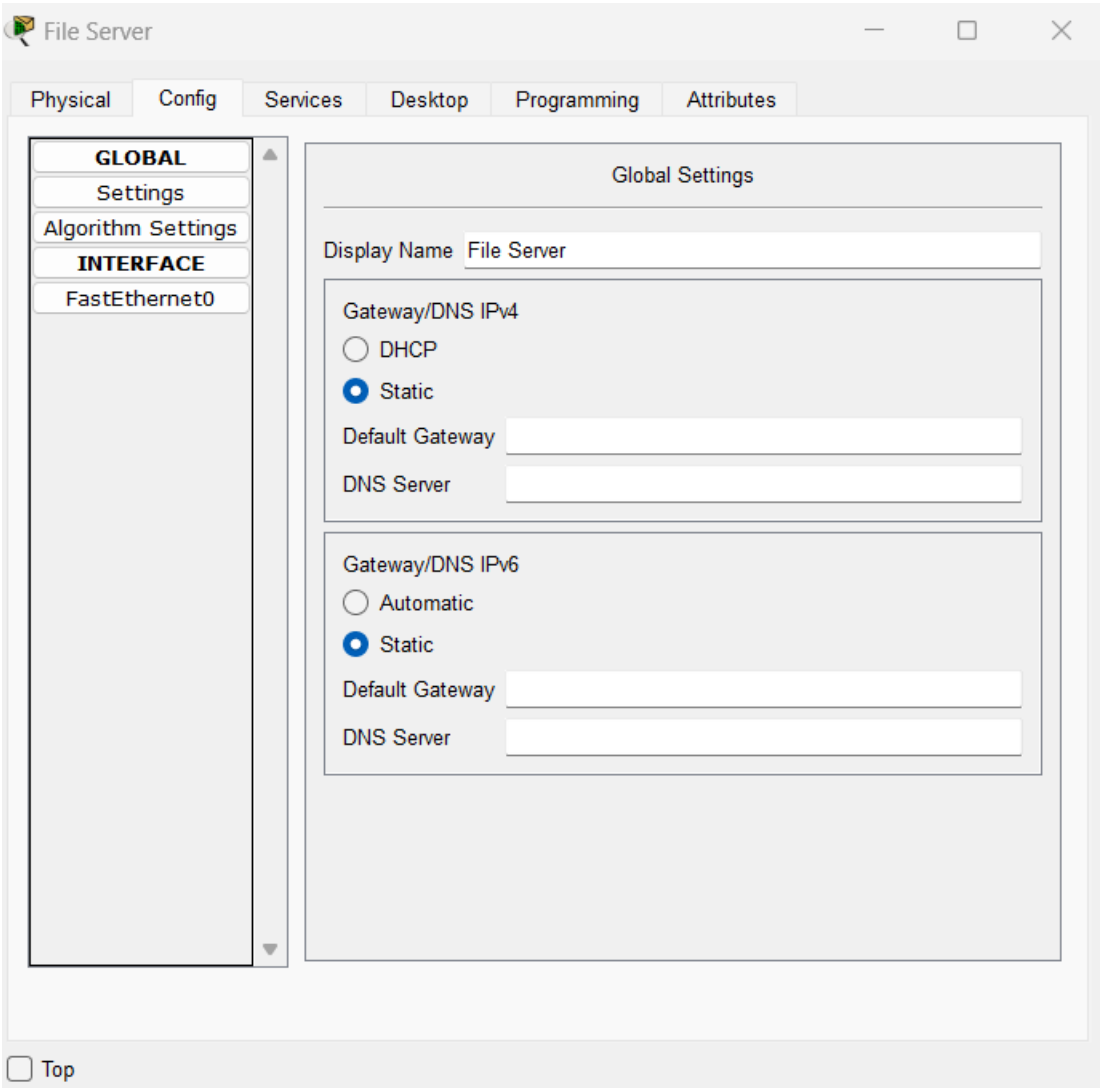
- Use copper straight through cable to connect the servers to the switch and the switch to the router.
- Use copper cross-over cable to connect the PC to router.



Step 4: Rename the servers as the following:

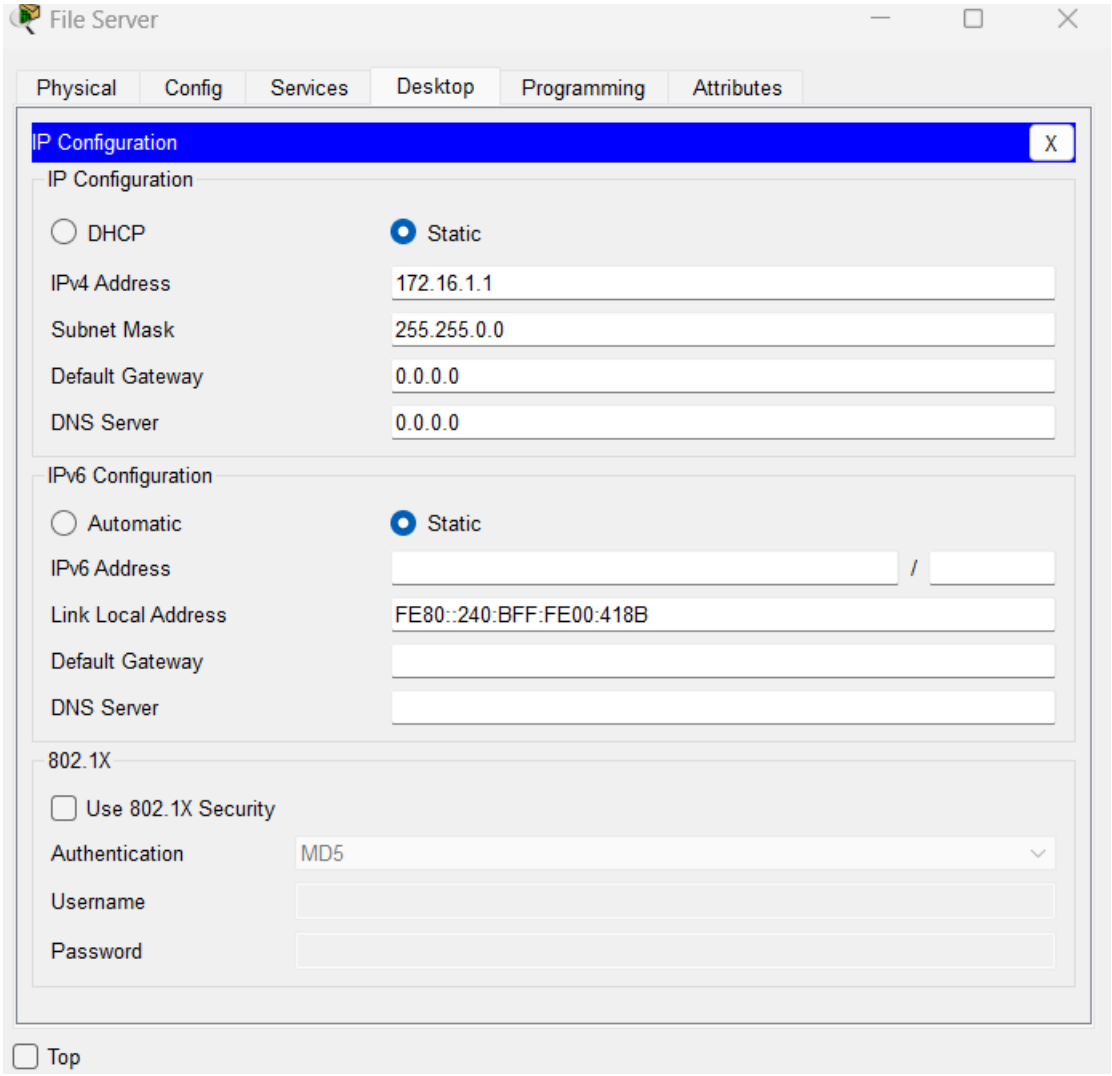
- File server
- Web server
- Mail Server

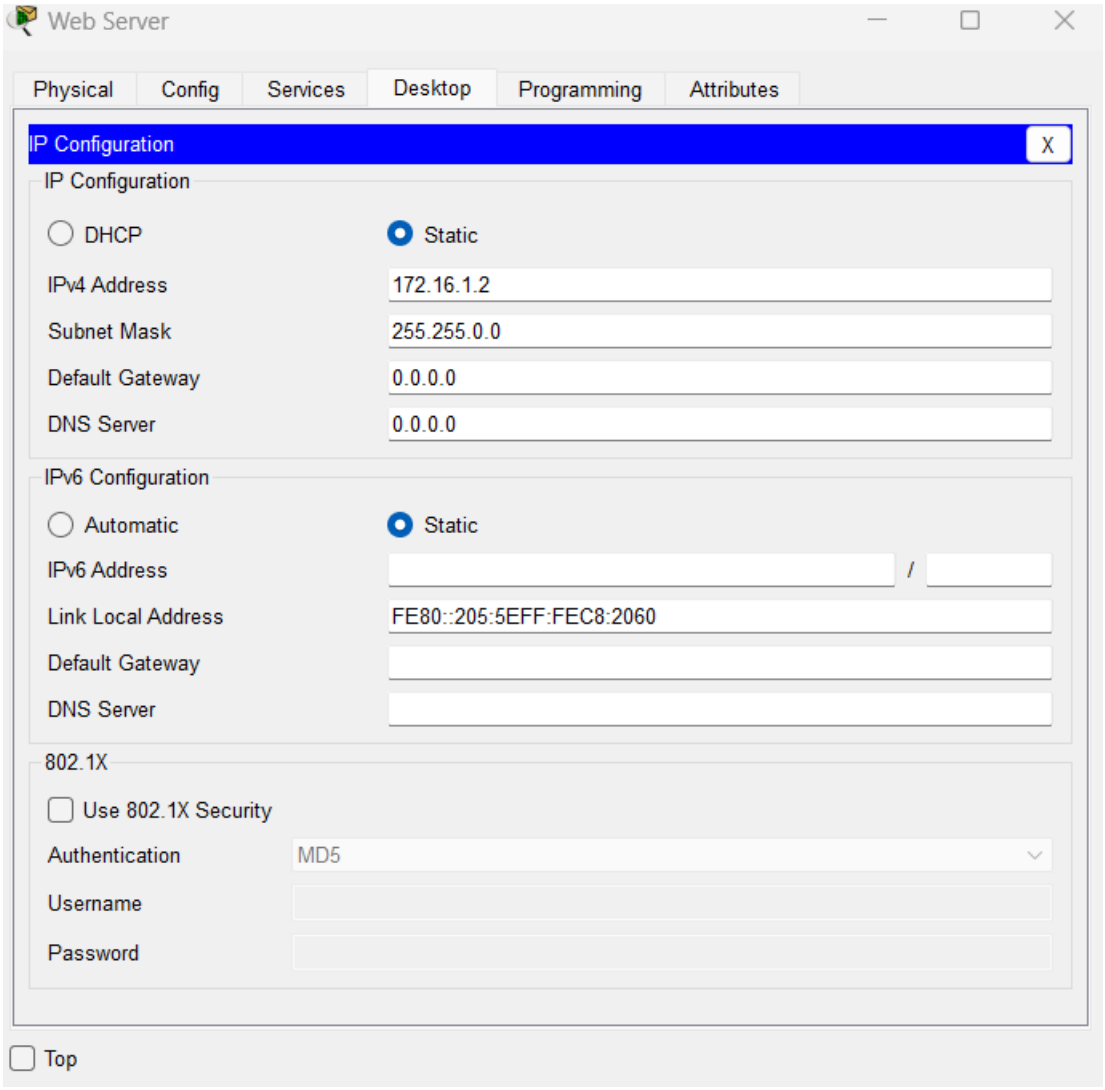
To do the above click on the server and then chose “config tab” and in “Display Name” change the name to the required name

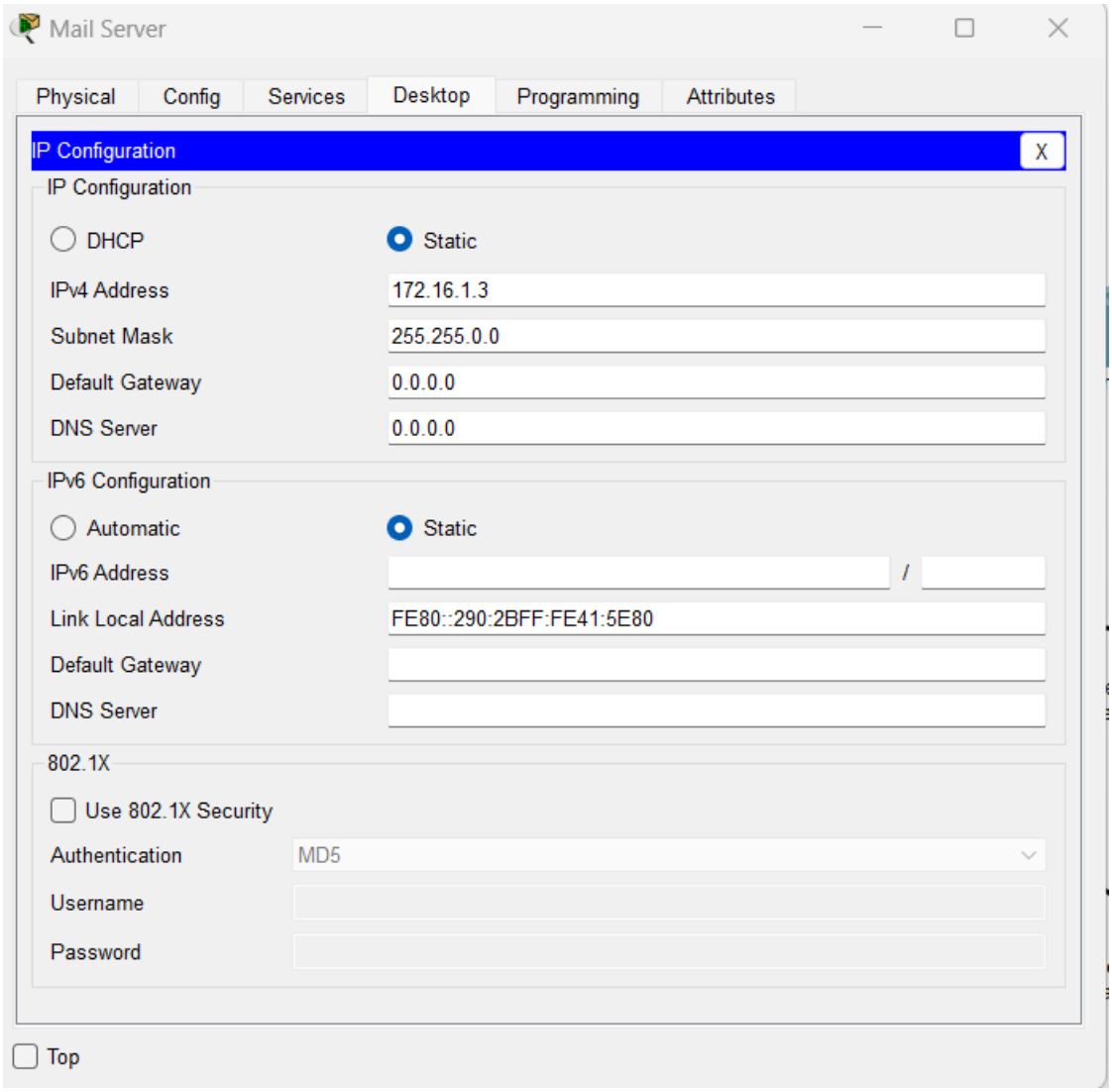


Step 5: Assign ip addresses to the servers

- Click on the server chose the “Desktop tab” then chose “IP Configuration” and set the following IP addresses
  - File Server- 172.16.1.1
  - Web server-172.16.1.2
  - Mail Server-172.16.1.3
- The subnet mask will be auto filled after the IP address is assigned.

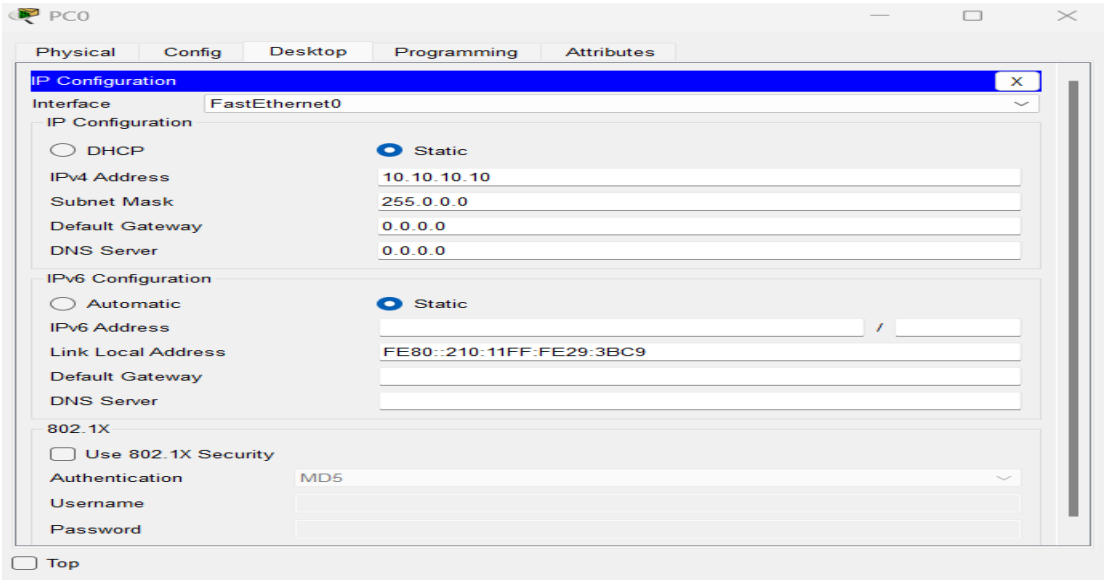

File Server
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
172.16.1.1
Subnet Mask
255.255.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::240:BFF:FE00:418B
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


Web Server
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
172.16.1.2
Subnet Mask
255.255.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::205:5EFF:FEC8:2060
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top



Step 6: Assign an IP address 10.10.10.10 to the PC

- Click on PC then chose “Desktop Tab” and then chose IP Configuration and then set IP address as 10.10.10.10 subnet mask will be auto filled.



Step 7: Assign an ip address to the routers Gigabit ethernet ports 0/0 and 0/1.

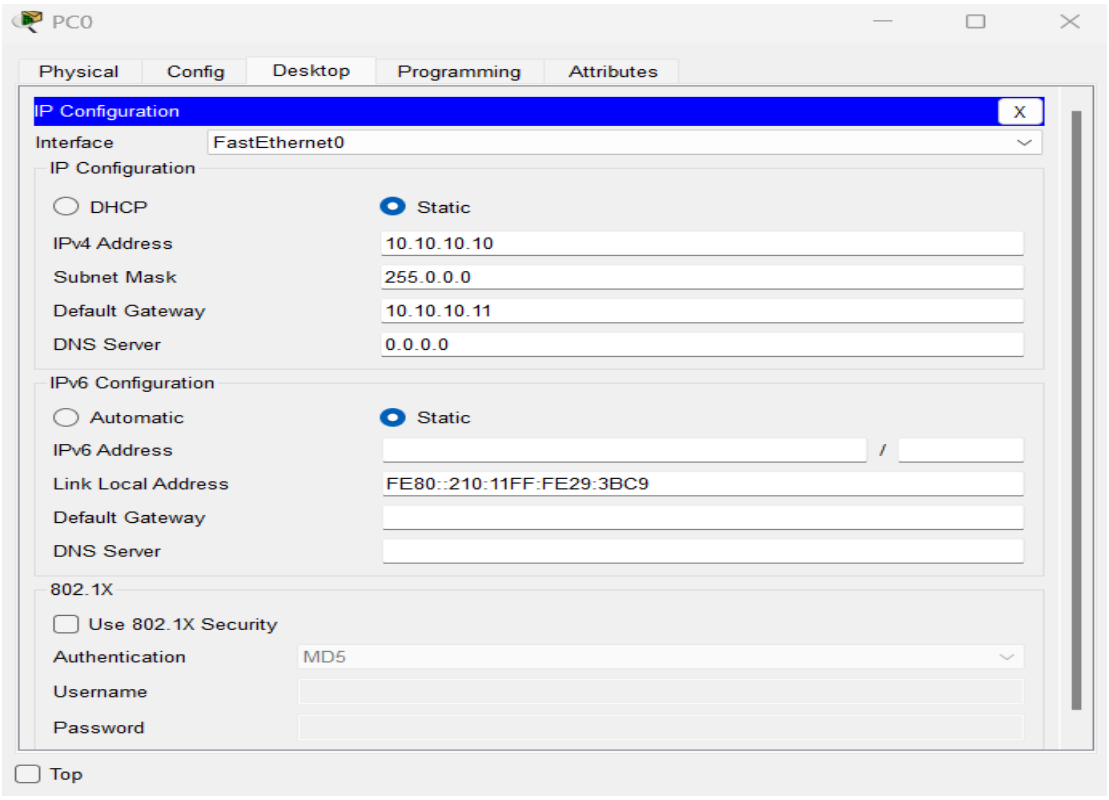
- Click on router then select CLI tab and run the following commands.
  - Router>enable
  - Router#config ter
  - Router(config)#do show ip int br
  - Router(config)#interface g0/0
  - Router(config-if)#ip address 10.10.10.11 255.0.0.0
  - Router(config-if)#no shutdown
- This sets the IP address of the Gigabit ethernet 0/0 as 10.10.10.11 and its subnet mask as 255.0.0.0

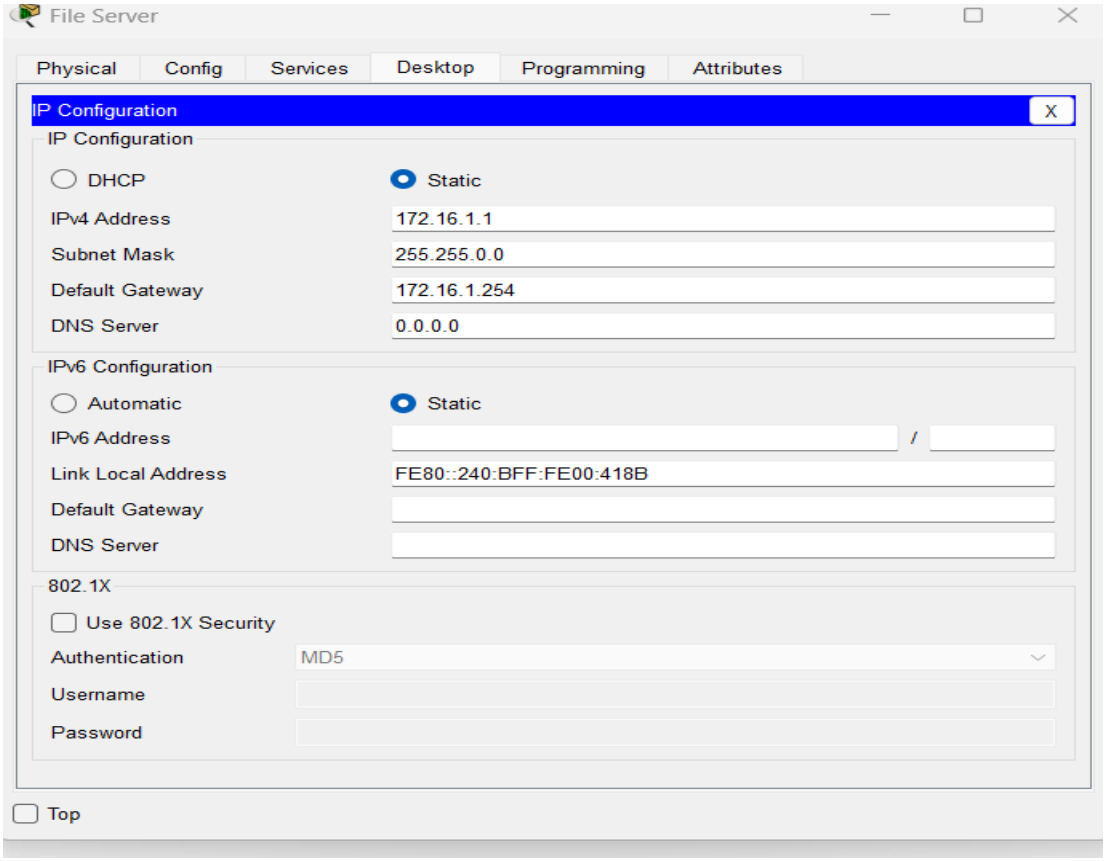
Repeat the step for Gigabit ethernet g0/1

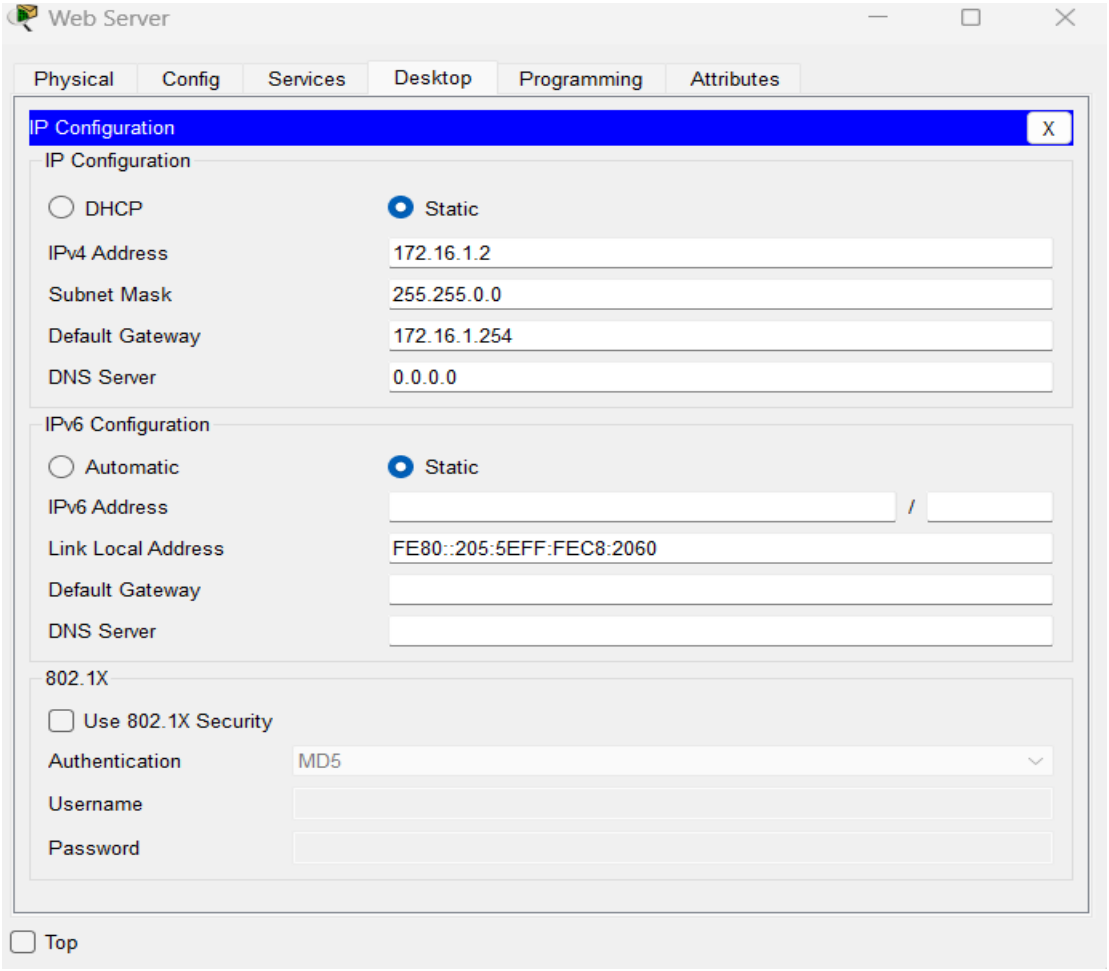
```
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#int
Router(config)#interface g0/1
Router(config-if)#ip address 172.16.1.254 255.255.0.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router(config-if)#exit
Router(config)#do show ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     10.10.10.11     YES manual up                    up
GigabitEthernet0/1     172.16.1.254    YES manual up                    up
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router(config)#
```

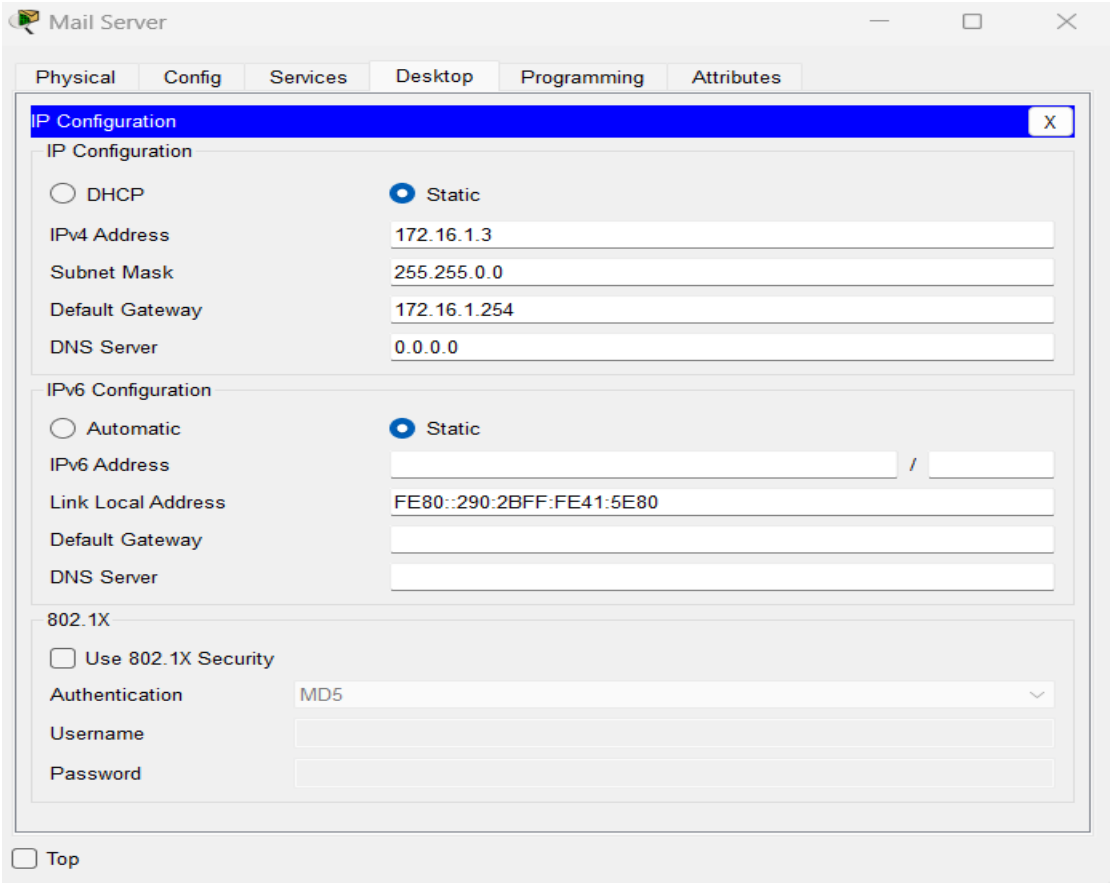
Step 8: Set the gateway for the PC and servers as the following :

- PC- 10.10.10.11
- Servers(File server, Web Server, Mail Server)- 172.16.1.254



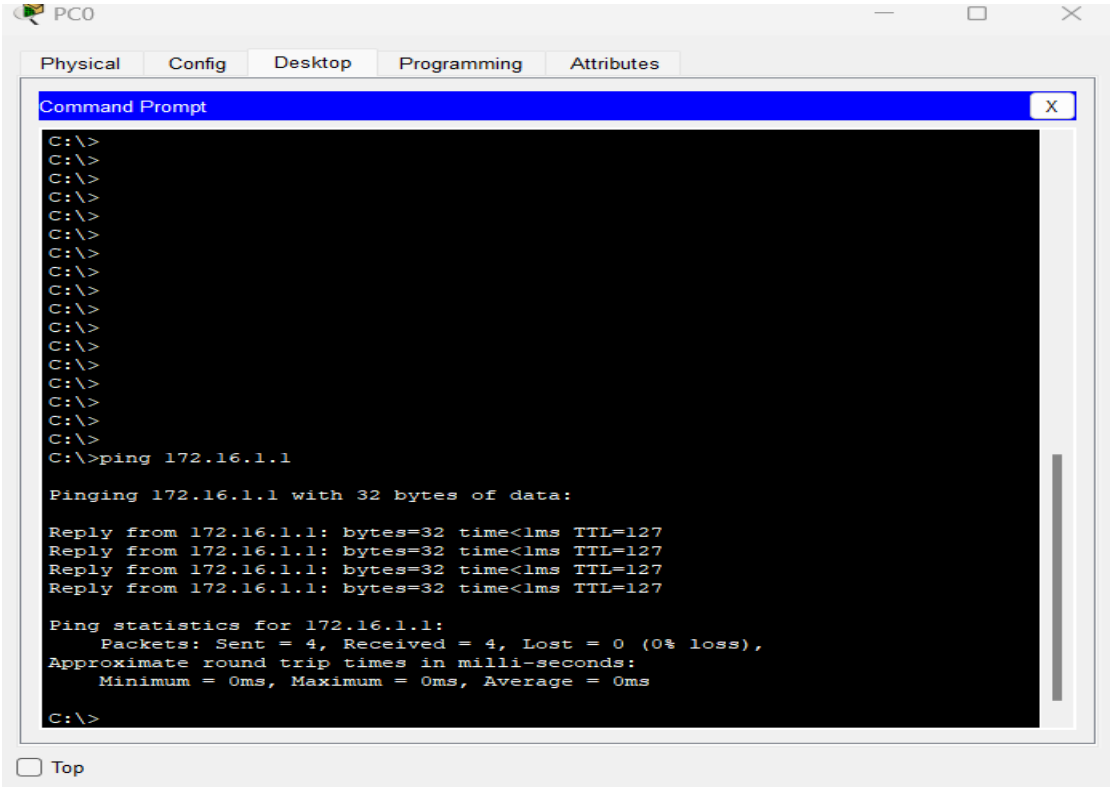

File Server
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
172.16.1.1
Subnet Mask
255.255.0.0
Default Gateway
172.16.1.254
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::240:BFF:FE00:418B
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

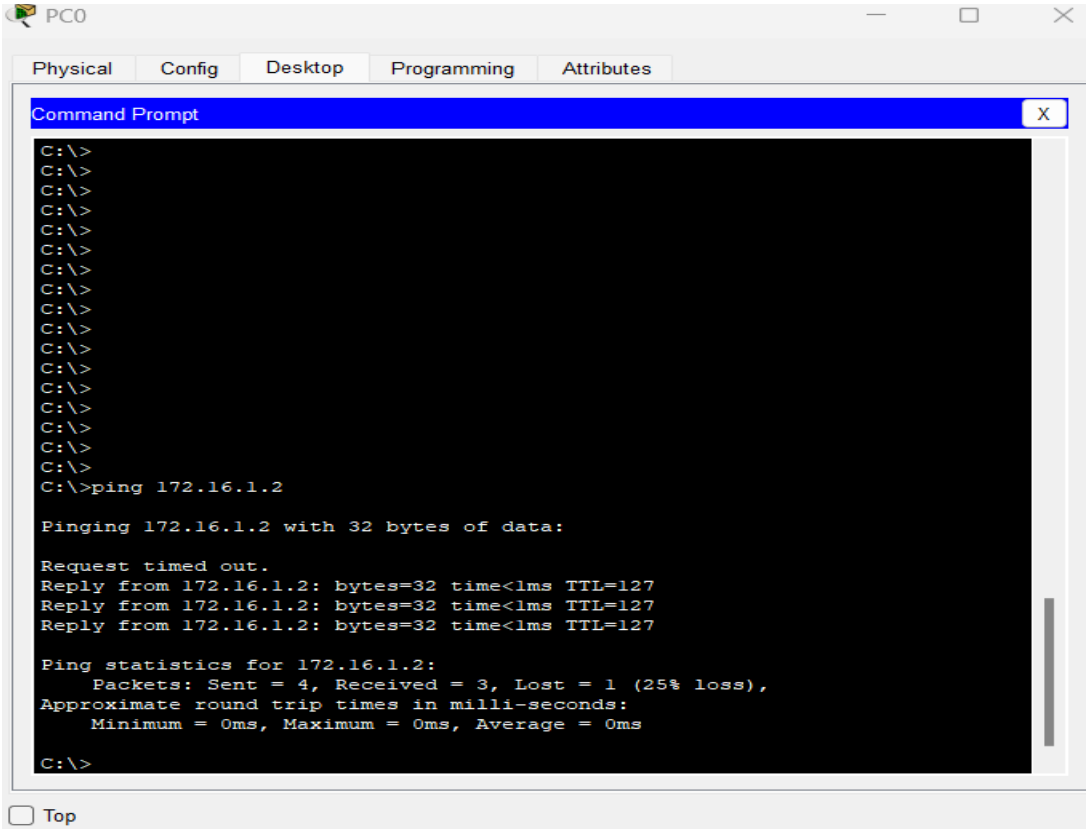

Web Server
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
172.16.1.2
Subnet Mask
255.255.0.0
Default Gateway
172.16.1.254
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::205:5EFF:FEC8:2060
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

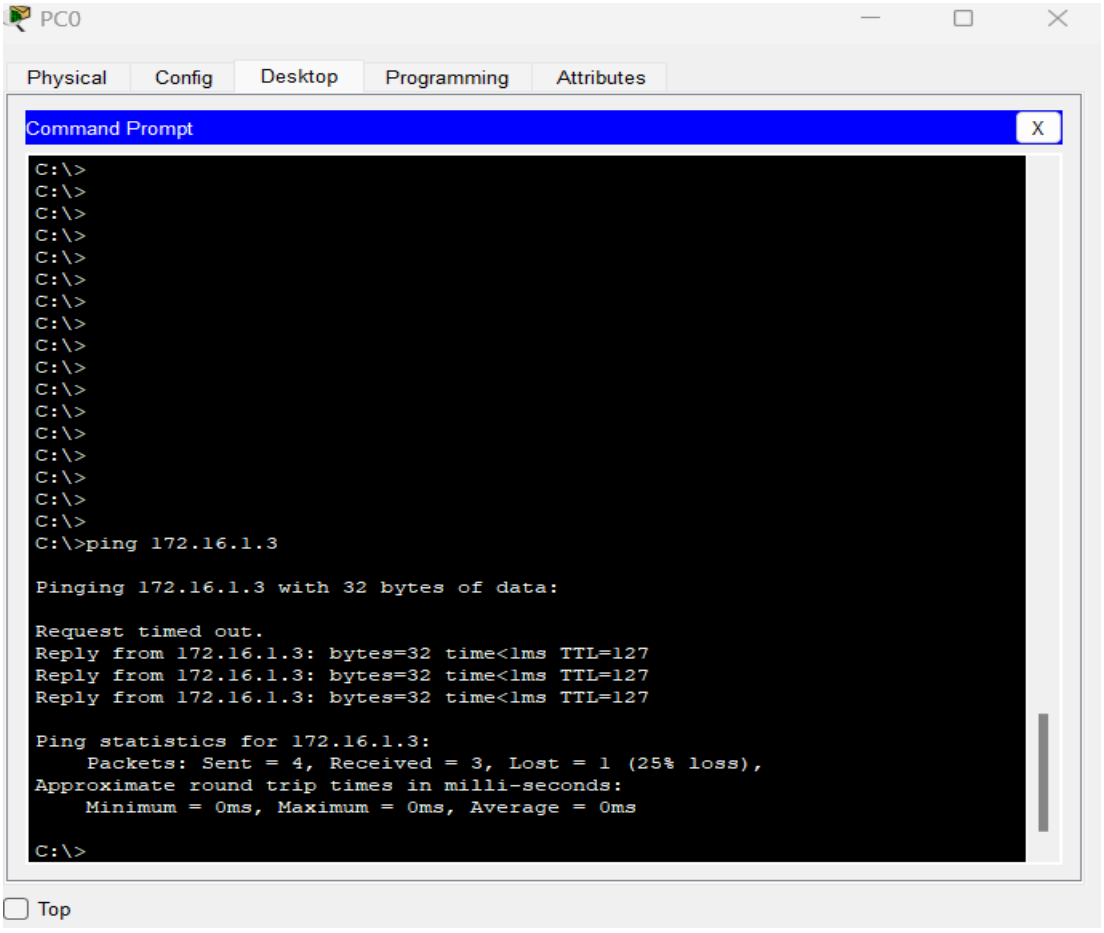


Step 9:Check the connectivity to each system in the network

- Click on PC then Desktop a nd then run the ping command along with destination ip address.




PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 172.16.1.2
Pinging 172.16.1.2 with 32 bytes of data:
Request timed out.
Reply from 172.16.1.2: bytes=32 time<1ms TTL=127
Reply from 172.16.1.2: bytes=32 time<1ms TTL=127
Reply from 172.16.1.2: bytes=32 time<1ms TTL=127
Ping statistics for 172.16.1.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 172.16.1.3
Pinging 172.16.1.3 with 32 bytes of data:
Request timed out.
Reply from 172.16.1.3: bytes=32 time<1ms TTL=127
Reply from 172.16.1.3: bytes=32 time<1ms TTL=127
Reply from 172.16.1.3: bytes=32 time<1ms TTL=127
Ping statistics for 172.16.1.3:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top

If you get a reply from all the systems the connection is confirmed.