LAB MANUAL

COMPUTER NETWORK LAB

INDEX

Sr. No	Programs	Date	Signature
1.	To study about components and specifications of Laptop and Desktop.		
2.	Familiarization with networking components and devices LAN adapter, Hub, Switches, Routers etc.		
3.	Familiarization with Transmission media and tools: Co-axial cable, UTP cable, Crimping tool, Connectors etc.		
4.	Preparing the UTP cable for cross and direct connection using crimping tool.		
5.	Introduction to various interior and exterior routing protocols.		
6.	Installation and introduction of simulation tools packet tracer/GNS3.		
7.	Study of various LAN topologies and their creation using network devices, cables and Computer.		
8.	Configuration of TCP/IP protocols in Window/LINUX.		
9.	Configuration of TELNET protocols on router for remote access.		

Program 1

Aim:-To study about the components and specifications of Computer and Laptop.

❖ Computer:-

A computer is a machine or device that performs processes, calculations and operations basedon instructions provided by a software or hardware program. It is designed to execute applications and provides a variety of solutions by combining integrated hardware and software components.

❖ Computer Specifications:-

Motherboard:-

- The motherboard is the backbone of your PC and it provides the electrical connections between every component so that they are able to communicate with each other.

Motherboard and their parts:-

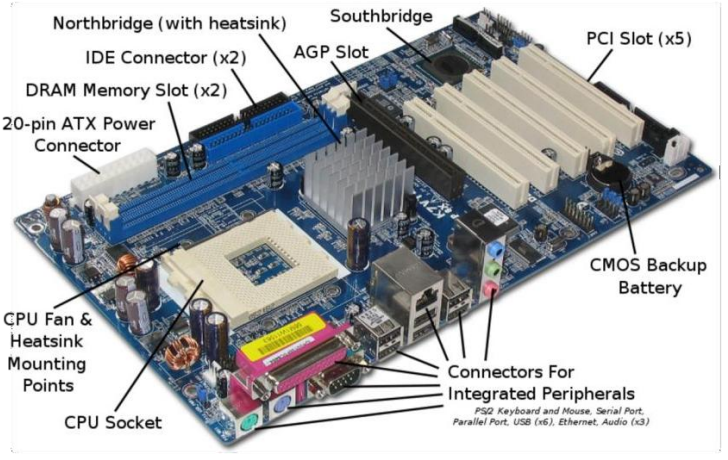


Diagram: Motherboard with Label Diagram

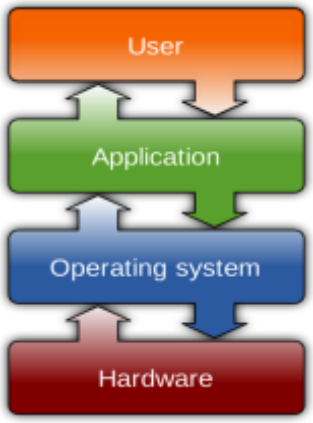
Processors:-

A **processor** (CPU) is the logic circuitry that responds to and processes the basic instructions that drive a computer. The CPU is seen as the main and most crucial integrated circuitry (IC) chip in a computer, as it is responsible for interpreting most of computers commands.

Mentioned computer's processor has **speed of 1.60 GHz**.

Operating System:-

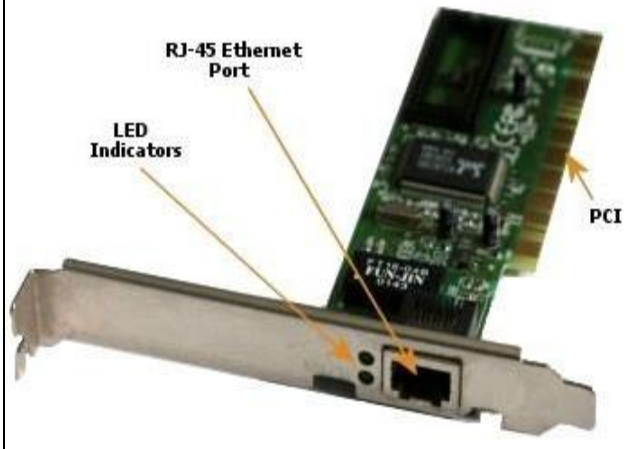
An Operating System (OS) is an interface between a computer user and computer hardware. An operating system is a software which performs all the basic tasks like file management, memory management, process management, handling input and output, and controlling peripheral devices such as disk drives and printers.



The computer has **Window 7 & 32 bit** operating system**.**

Network Interface Card:-

A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.



✓ SMPS:-

Switched-Mode Power Supply (SMPS) is an electronic circuit which converts the power using switching devices that are turned on and off at high frequencies, and storage components such as indicators or capacitors to supply power when the switching device is in its non-conduction state.

✓ Buses used in computer:-

A bus is a high-speed internal connection. Buses are used to send control signals and data between the processor and other components. Three types of bus are used. Address bus - carries memory addresses from the processor to other components such as primary storage and input/output devices.

Memory:-

It is *used to store data and instructions*. Computer memory is the storage space in the computer, where data is to be processed and instructions required for processing are stored. The memory is divided into large number of small parts called cells. Each location or cell has a unique address, which varies from zero to memory size minus one.

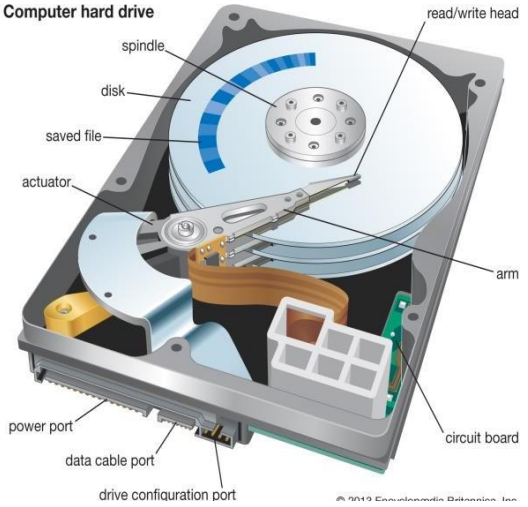
1. RAM:-

RAM is the working memory of your computer. The higher the RAM, the more multi-tasking the computer can do. Mentioned Computer have **1 GB** RAM.

2. Hard Disk drive:-

HDD is an electro-mechanical storage device, which is an abbreviation of Hard Disk Drive. It uses magnetic storage for storing and retrieving the digital data. It is a non-volatile storage device. Mentioned computer have HDD of **1 TB.**

HDD 1TB



Internal architecture of HDD

Laptop:-

Laptop is a small, portable personal computer(pc) with a screen and alphanumeric keyboard. It is also known as laptop computer, notebook computer.

Laptop Specifications:-

View basic information about your computer

Windows edition

Windows 10 Home Single Language

© 2019 Microsoft Corporation. All rights reserved.

Windows 10

System

Processor:	AMD A6-9210 RADEON R4, 5 COMPUTE CORES 2C+3G	2.40 GHz
Installed memory (RAM):	4.00 GB (3.67 GB usable)	
System type:	64-bit Operating System, x64-based processor	
Pen and Touch:	No Pen or Touch Input is available for this Display	

Computer name, domain, and workgroup settings

Computer name:	DESKTOP-P7HEN8N	Change settings
Full computer name:	DESKTOP-P7HEN8N	
Computer description:		
Workgroup:	WORKGROUP	

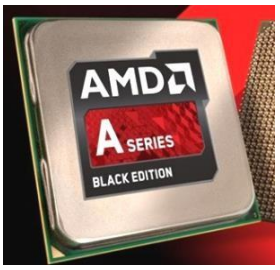
Windows activation

Windows is activated Read the Microsoft Software License Terms

Product ID: 00327-70000-00001-AA386 Change product key

Processor:-

A processor is an integrated electronic circuit that performs the calculations that run a Laptop. A processor performs arithmetical, logical, input/output (I/O) and other basic instructions that are passed from an operating system (OS).



Mentioned laptop **has AMD A6 processor with 2.40 Ghz speed**.

Operating System:-

An operating system is a program that acts as an interface between the user and the computer hardware and controls the execution of all kinds of programs**.**

Mentioned Laptop has **Windows 10 & 64 bit** operating system.

Types of Memory Used:-

✓ Cache Memory:-

It is an extremely fast memory type that acts as a buffer between RAM and the CPU. It holds frequently requested data and instructions so that they are immediately available to the CPU when needed. Cache memory is used to reduce the average time to access data from the Main memory.

Mentioned Laptop has **8 MB** cache Size.

✓ RAM:-

RAM (Random Access Memory) is the internal memory of the CPU for storing data, program, and program result. It is a read/write memory which stores data until the machine is working.

Mentioned Laptop has **4GB RAM** size.

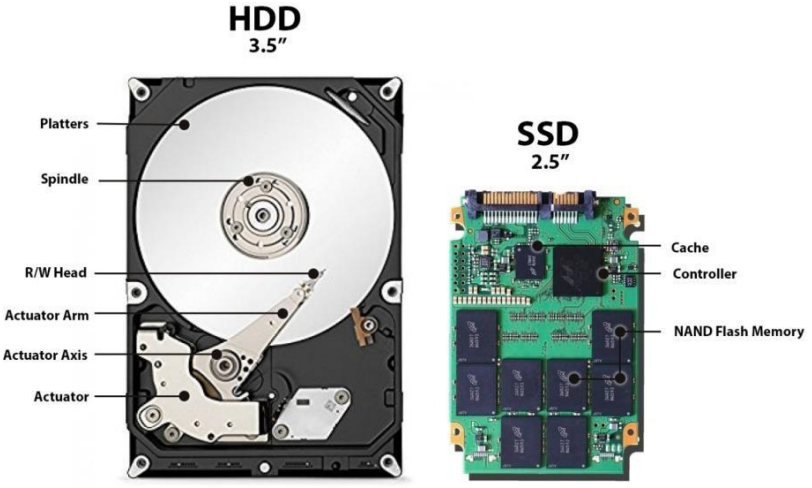
✓ Hard disk drive:-

HDD is used in computer to facilitate the user to store data permanently as it is non volatile.

Mentioned Laptop has **1 TB HDD** Size

✓ Solid State Drive:-

It is a new generation of storage device .It is faster but expensive than HDD.



✓ Screen resolution:-

Mentioned Laptop has 1920 x 1080 screen resolution.

✓ Ports in Laptop:-

Laptops generally have 5 types of ports.

i. Charging port (used to charge laptop).
ii. USB type C port (used for Bidirectional data transfer, taking power supply).
iii. RJ-45 port for Ethernet connection.
iv. HDMI port.
v. Headphone 2.0 port.

Touch:- It allows you to complete intuitive control.

Program 2

Aim:-Familiarization with networking components and devices LAN adapters, hubs, switches, routers etc.

✓ What is a Network?

A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

Networking Components:-

Computer networks components comprise both **Hardware parts as well as the software parts** required for installing computer networks, both at organizations and at home. The hardware components are the server, client, peer, transmission medium, and connecting devices. The software components are operating system and protocols.

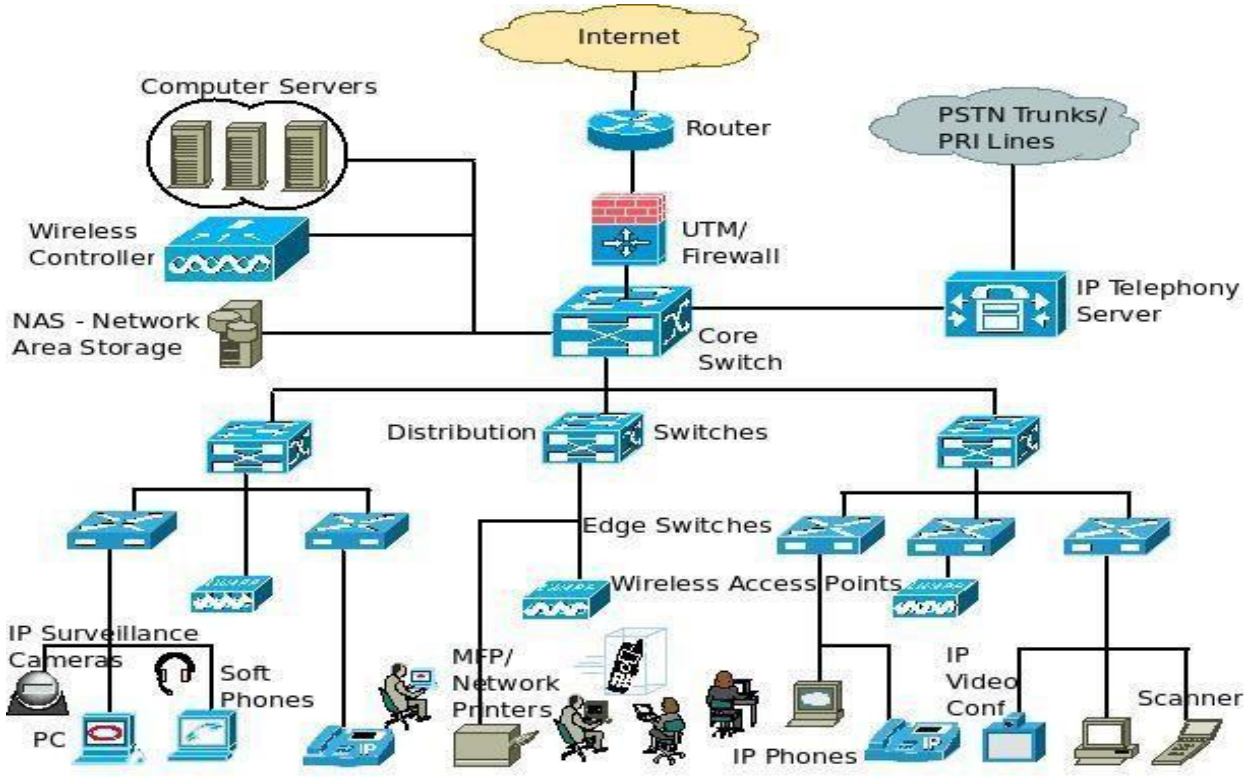


Diagram: Components of Network.

✓ Hardware Components:-

- **Servers**:−Servers are high-configuration computers that manage the resources of the network. The network operating system is typically installed in the server and so they give user accesses to the network resources. Servers can be of various kinds: file servers, database servers, print servers etc.
- **Clients:** − Clients are computers that request and receive service from the servers to access and use the network resources.

- **Peers:-** Peers are computers that provide as well as receive services from other peers in a work group network.
- **Transmission Media:-** Transmission media are the channels through which data is transferred from one device to another in a network. Transmission media may be guided media like coaxial cable, fiber optic cables etc; or maybe unguided media like microwaves, infra-red wave etc.
- **Networking Devices:-** Connecting devices act as middleware between networks or computers, by binding the network media together. Some of the common connecting devices are:
    1. **Routers**
    2. **Hub**
    3. **Switch**
    4. **Bridge**
    5. **Repeater**
    6. **Gateway**

➔ Software Components:-

- ✓ **Operating System** − Network Operating Systems is typically installed in the server and facilitate workstations in a network to share files, database, applications, printers etc.
- ✓ **Protocol Suite** − A protocol is a rule or guideline followed by each computer for data communication. Protocol suite is a set of related protocols that are laid down for computer networks. The two popular protocol suites are−
    - **OSI Model (Open System Interconnections)**
    - **TCP / IP Model**.

➔ LAN Adapter:-

A LAN adapter is an expansion board that is used to connect a computer or computing device to a network. LAN adapter is the most common and generic alternate name for a Network Interface Card(NIC). Similar products, such as Wireless USB LAN Adapter rare referred to as LAN adapters.

LAN ADAPTER

➢ Functions of LAN Adapter:-

The computer and the card must communicate with each other so that they can proceed to exchange information. In this way, the computer allocates part of its memory to cards that have DMA (Direct memory access).The card interface indicates that another computer is requesting data from the computer. The computer bus transfers the data from the computer memory to the network card.

Networking Devices

➔ Router:-

Routers are networking devices operating at layer 3 or a network layer of the **OSI model**. They are responsible for receiving, analyzing, 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.

➢ How a router works:-

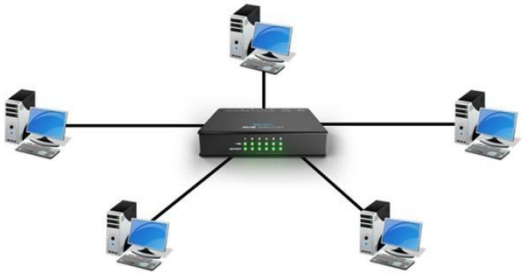
A router examines a packet header's destination IP address and compares it against a routing table to determine the packet's best next hop. Routing tables list directions for forwarding data to particular network destinations, sometimes in the context of other variables, like cost. They amount to an algorithmic set of rules that calculate the best way to transmit traffic toward any given IP address. A routing table often specifies a default route, which the router uses whenever it fails to find a better forwarding option for a given packet. For example, the typical home office router directs all outbound traffic along a single default route to its internet service provider (ISP) Routing tables can be static -- i.e., manually configured -- or dynamic. Dynamic routers automatically updated their routing tables based on network activity, exchanging information with other devices via routing protocols.

➔ Hub:-

A Network Hub is one of the most commonly used networking devices can be easily found on any small networks such as home or office. Hub operates at the physical layer of OSI model. It is the simplest networking device hence has low cost. Basically, a hub is a repeater with multiple ports. The function of a hub in networking is similar to the repeater. It transfers data in the form of binary bits and uses for broadcasting data.

➢ Working of Hubs:-

When a host sends frames, the hub forwards the frames in all the ports. Hubs do not separate the type of the frame, for example, whether the frame unicast should be either multicast or broadcast. Hubs forward all the frames into all the ports. Although a hub sends the frames to all the ports, a computer accepts the ones, whose MAC match matches the destination MAC address field. The rest of the frames are discarded after receiving the required information.

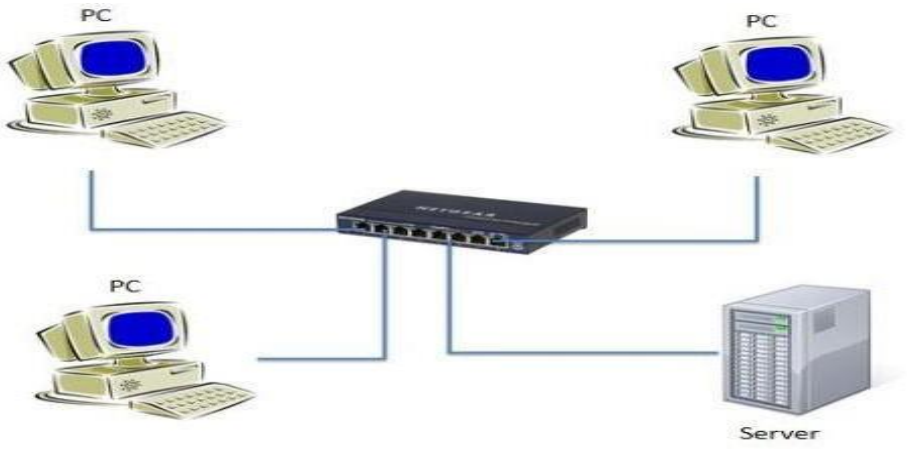


➔ Switch:-

A switch is a Networking device in a computer network that connects other devices together. Multiple data cables are plugged into a switch to enable communication between different networked devices. Switches manage the flow of data across a network by transmitting a received network packet only to the one or more devices for which the packet is intended.

Diagram- Switch

- **Working of Switch:-**Whenever a host sends a frame to any other host, then the source host is stored with the port in the address table of the MAC address switch. A switch always stores the address of the source in the table. Unless a host does send some data, its MAC address and port number will not be stored in the table of the switch. Unless a host does send some data, its MAC address and port number will not be stored in the table of the switch. When you initialize the switch, the switch does not contain any information about any host and its address. In such a situation, when a host frame sends, its MAC address is stored in the table but due to no destination information, the switch sends the frame to all the hosts .When you initialize the switch,the switch does not contain any information about any host and its address. In such a situation, when a host frame sends, its MAC address is stored in the table but due to no destination information, the switch sends the frame to all the hosts. As soon as the second host sends some data, its address also gets stored in the table. As soon as the second host sends some data, its address also gets stored in the table. Whenever a host sends the frames, the switch stores it if its address is not already present in the table. Thus a switch creates its table. When all the hosts' addresses and port numbers come in the switch, the switch delivers the frame to all hosts only, delivering the same host to the host for which the data has been sent.



➔Bridge:-

Bridge is termed as a network device which is helpful in filtering the data load of the traffic by dividing it into segments or packets. They are used to lower the load of traffic on the LAN and other networks. Bridges are passive devices, because there is no interaction between bridged and the paths of bridging. Bridges operate on the second layer of the OSI model that is the data link layer.

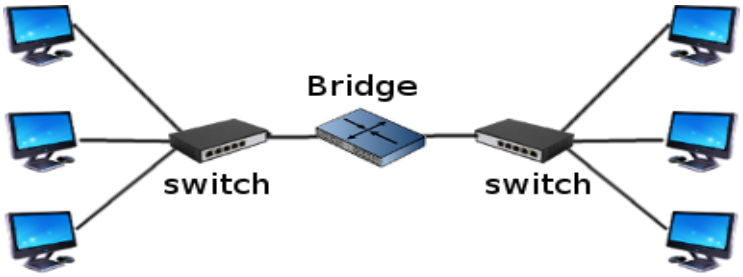


Diagram: Working of Switch

- **Working of Bridge:-**

When various network segments are established at the data link layer of the OSI model, we refer to it as bridge. However when the packets ofdata are transferred along a network , without locating the network addresses this process is termed as bridging. The process of bridging is helpful in locating the addresses of unknown addresses to which it is viable to send data. In bridging the data packets contain a header or a packet header which holds the address to the intended device. Bridge can remember and recall the address of the devices for further transmission. There are two kinds of bridging modes, the transparent bridging and the source routing bridging. When the process of bridging occurs, it makes a bridging table along side where it stores the MAC addresses of the various terminals. Thistable helps the bridges to send the data packet to the exact location next time. However when a specific address does not meet the contents of the bridging table, the data packet is forwarded further ahead to every attached terminal in LAN except from the computer it is connected to. This type of bridging is called transparent bridging. When the source computer presents pathway information within the packet, this typeof bridging is known as source route bridging. It is most commonly used in used on Token Ring networks.

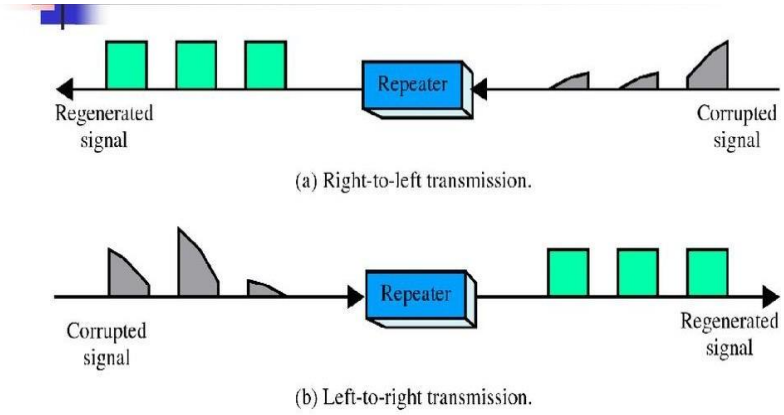
➔ Repeater:-

A repeater is a network device that retransmits a received signal with more power and to an extended geographical or topological network boundary than what would be capable with the original signal repeater is implemented in computer networks to expand the coverage area of the network, re propagate a weak or broken signal and or service remote nodes. Repeaters amplify the received/input signal to a higher frequency domain so that it is reusable, scalable.

Diagram: Repeater

➔ Working of Repeater:-

When an electrical signal is transmitted via a channel, it gets attenuated depending upon the nature of the channel or the technology. This poses a limitation upon the length of the LAN or coverage area of cellular networks. This problem is alleviated by installing repeaters at certain intervals.



Repeaters amplifies the attenuated signal and then retransmits it. Digital repeaters can even reconstruct signals distorted by transmission loss. So, repeaters are popularly incorporated to connect between two LANs thus forming a large single LAN

Diagram: Working of Repeater

➔ Gateway:-

The link between two computers to connect to internet or another network is called gateway. The gateway works like a portal among two programs by means of communications between protocol and permit them to share data on same computers or among different computers. Gateways are also known as protocol converter that can perform at any OSI model layer. The task of a gateway is very complex.

- **Working of Gateway:-**

A gateway is a network point that works as an access to another network. Generally in intranet a node can be either a gateway node or the nodes that join the network are gateways. In large organization where the computers control the traffic between organization networks are gateway nodes. Like that the computers used by ISP to connect different user with each other at a time to the internet are gateway nodes. In a project of any business company computer server work as a gateway nodes and it may be proxy server or firewall some time. A gateway may connected to a router because a router exactly known where to through a given packet of data that appears at the gateway then a switch finalize the actual in and out path of the gateway for the specified packet .A gateway is a compulsory features of routes even though other devices can perform as a gateway. The operating system mostly used this term and internet connection sharing act as a gateway and creating a connection among internal network.

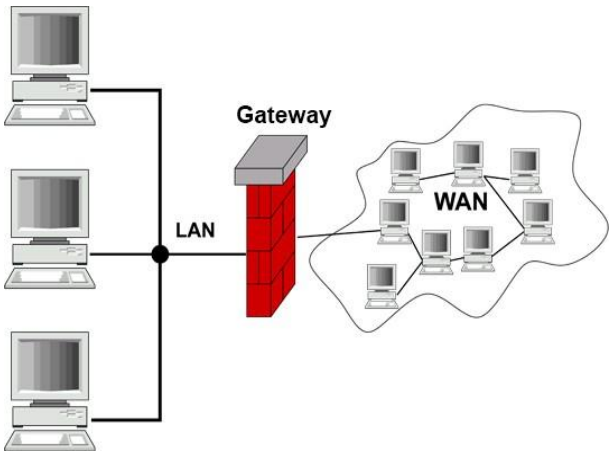


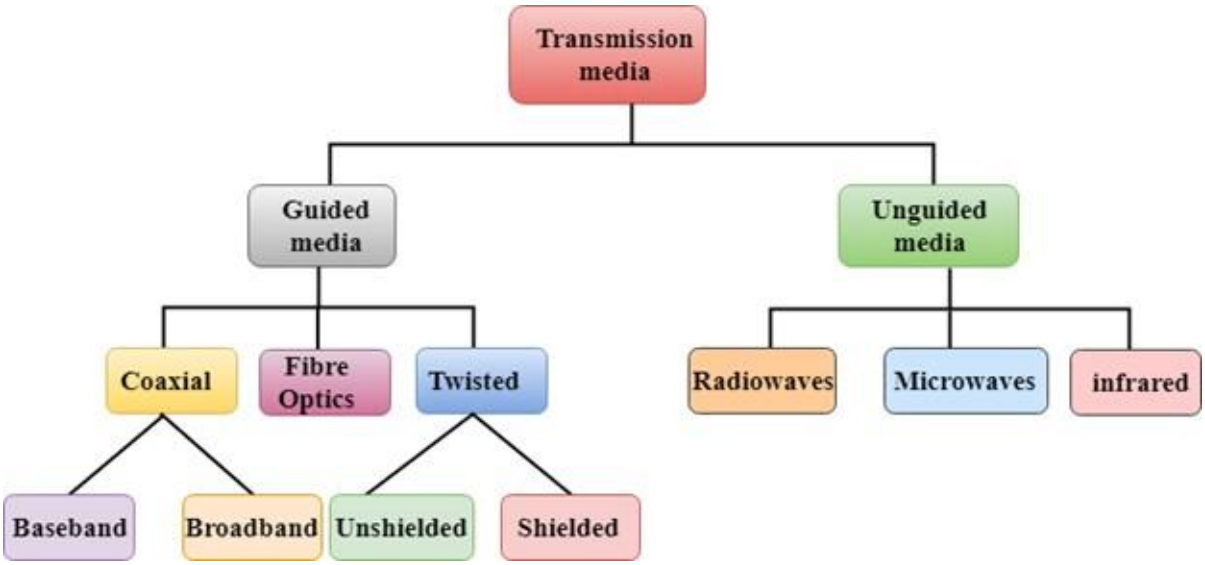
Diagram: Working of Gateways

Program 3

Aim:-Familiarization with Transmission media and Tools Coaxial cable, UTP Cable, Crimping Tools, Connectors etc.

Transmission Medium:

A communication channel that is used to carry the data from one transmitter to the receiver through the electromagnetic signals .The main function of this is to carry the data in the bits form through the Local Area Network(LAN).In data communication, it works like a physical path between the sender & receiver .For instance ,in a copper cable network the bits in the form of electrical signals whereas in a fiber network ,the bits are available in the form of light pulses. The quality as well as characteristics of data transmission ,can be determined from the characteristics of medium &signal. The properties of different transmission media are delay, bandwidth, maintenance, cost and easy installation.

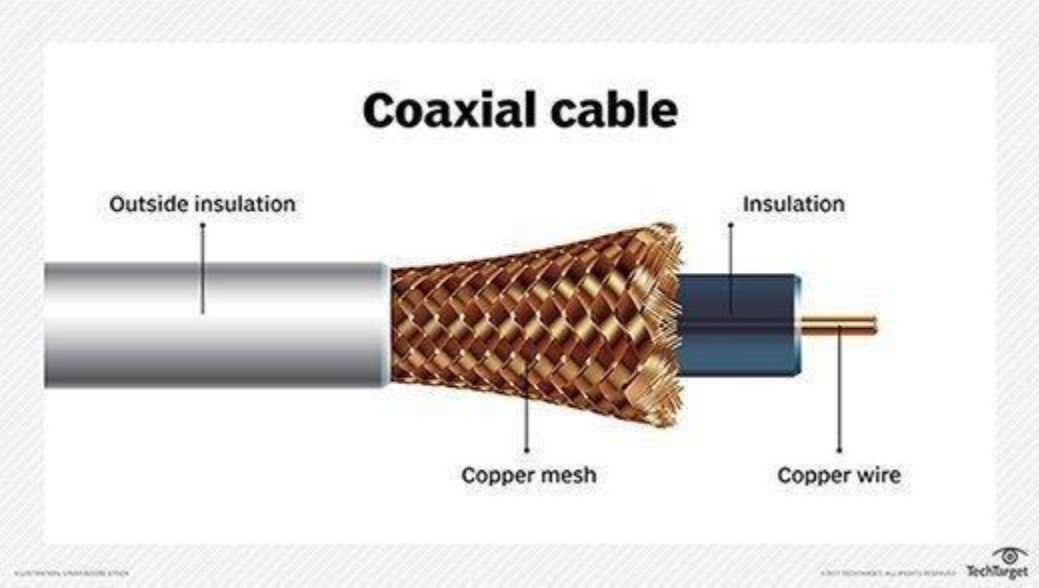


Bounded/Guided Transmission Media:

This kind of transmission media is also known as wired otherwise bounded media. In this type ,the signals can be transmitted directly & restricted in a thin path through physical links.
The types of Bounded /Guided transmission are discussed below.

Coaxial Cable:

Coaxial cable (or *coax)* carries signals of higher frequency ranges than those in twisted pair cable. It has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.



Applications:

1. Coaxial cable was widely used for both analog and digital data transmission.
2. It has higher bandwidth.
3. Inexpensive when compared to fiber optical cables.
4. It uses for longer distances at higher data rates.
5. Excellent noise immunity.
6. Used in LAN and Television distribution.

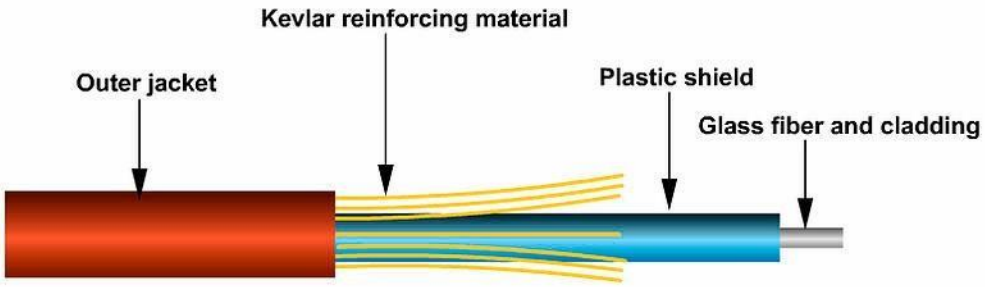
Disadvantage :

1. Single cable failure can fail the entire network.
2. Difficult to install and expensive when compared with twisted pairs.
3. If the shield is imperfect ,it can lead to grounded loop.

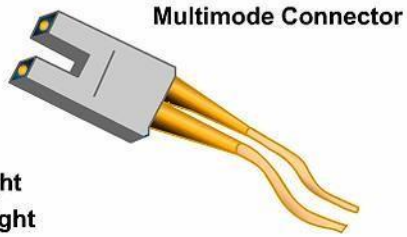
Fibre Optic Cable:

A fiber optic cable is a network cable that contains strands of glass fibers inside an insulated casing. They're designed for long-distance, high-performance data networking, and telecommunications. Compared to wired cables, fiber optic cables provide higher bandwidth and transmit data over longer distances. Fiber optic cables support much of the world's internet, cable television, and telephone systems.

Fiber Optic Cable



Speed and throughput:	100+ Mbps
Average $ per node:	Most Expensive
Media and connector size:	Small
Maximum cable length:	up to 2 Km
Single mode:	One stream of laser-generated light
Multimode:	Multiple streams of LED-generated light



Advantages of Fiber Optic Cables:

1.The loss of signal in optical fiber is less than that in copper wire.

2.Opticalfibers usually have a longer life cycle for over 100 years.

Disadvantage:

1.It is expensive.

2.Difficult to install.

Twisted pair cable:

A twisted pair cable is a type of cable made by putting two separate insulated wires together in a twisted pattern and running them parallel to each other. This type of cable is widely used in different kinds of data and voice infrastructures.

Twisted pair is of two types:

1.Shielded Twisted Pair(STP)

2.Unshielded Twisted Pair(UTP)

Shielded Twisted Pair:

Shielded Twisted Pair (STP) cables additionally have an overall conducting metallic shields covering four twisted pair wires. There may be another conducting metallic shields covering

individual twisted pairs also. These metallic shields blocks out electromagnetic interference to prevent unwanted noise from the communication circuit.

Advantage of Shielded Twisted Pair:

1.The cost of the shielded twisted pair cable is not very high and not very low.

2.An installation of STP is easy.

3.It has higher capacity as compared to unshielded twisted pair cable.

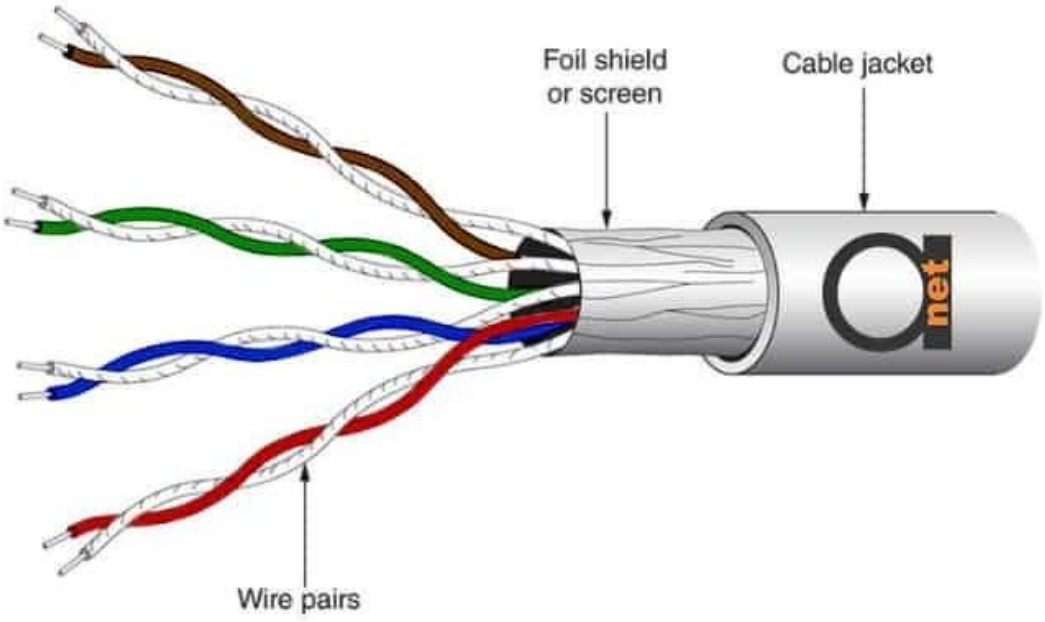
4.It has a higher attenuation.

5.It is shielded that provides the higher data transmission rate.

Disadvantages:

1.It is more expensive as compared to UTP and coaxial cable.

2.It has a higher attenuation rate.



Unshielded Twisted Pair(UTP):

An unshielded twisted pair is widely used in telecommunication. It is most common type when compared with shielded twisted pair cable which consists of two conductors usually copper, each with its own colour plastic insulator.

Categories:

Category 1: Category 1 is used for telephone lines that have low-speed data.

Category 2: It can support up to 4Mbps.

Category 3: It can support up to 16Mbps.

Category 4: It can support up to 20Mbps. Therefore, it can be used for long-distance communication.

Category 5: It can support up to 200Mbps.

Advantages Of Unshielded Twisted Pair:

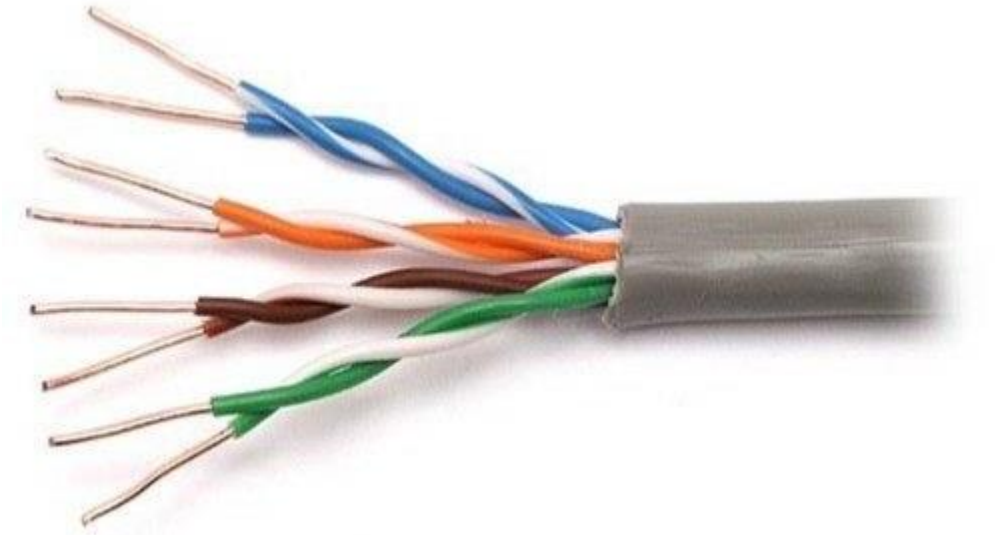
1. It is cheap.

2. Installation of the unshielded twisted pair is easy.

3. It can be used for high-speed LAN.

Disadvantage:

1. This cable can only be used for shorter distances because of attenuation.



Unbounded/Unguided Transmission Media:

Unguided medium transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

Types of unguided Transmission media:

✓ Radio Transmission:

Its frequency is between 10Khz to 1Ghz. It is simple to install and has high attenuation. These waves are used for multicast communication.

Types of propagation:

1. Troposphere
2. Ionosphere

Microwaves:

It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

Infrared:

Infrared waves are used for very short distance communication. They cannot penetrate through

obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

Crimping tool:

A **crimping tool** is a device used to conjoin two pieces of metal by deforming one or both of them to hold each other. The result of the tool's work is called a **crimp**. An example of crimping is affixing a connector to the end of a cable. For instance, network cables and phone cables are created using a crimping tool (shown below) to join RJ-45 and RJ-11 connectors to both ends of phone or Cat 5 cable.

Connector:

A device that terminates a segment of cabling or provides a point of entry for networking devices such as computers, hubs, and routers. Connectors can be distinguished according to their physical appearance and mating properties, such as jacks and plugs (male connectors) or sockets and ports (female connectors).

Program 4

Aim: Preparing the UTP cable for cross and direct connection using Crimping Tools.

Requirements:

Crimping tools, UTP Cable, RJ-45 connector, Cable tester.

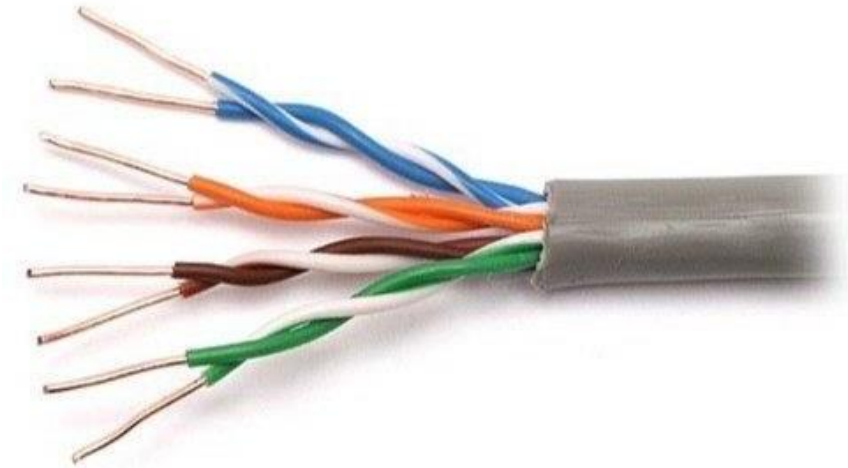
Procedure:

Crimping Tools:

A crimping tool is a device used to conjoin two pieces of metal by deforming one or both of them to hold each other. The result of the tool's work is called a crimp. An example of crimping is affixing a connector to the end of a cable. For instance, network cables and phone cables are created using a crimping tool (shown below) to join RJ-45 and RJ-11 connectors to both ends of phone or Cat 5 cable.

UTP Cables:

UTP stands for Unshielded Twisted Pair cable. UTP cable is a 100 ohm copper cable that consists of 2 to 1800 unshielded twisted pairs surrounded by an outer jacket. They have no metallic shield. This makes the cable small in diameter but unprotected against electrical interference. The twist helps to improve its immunity to electrical noise and EMI.



RJ-45 Connector:

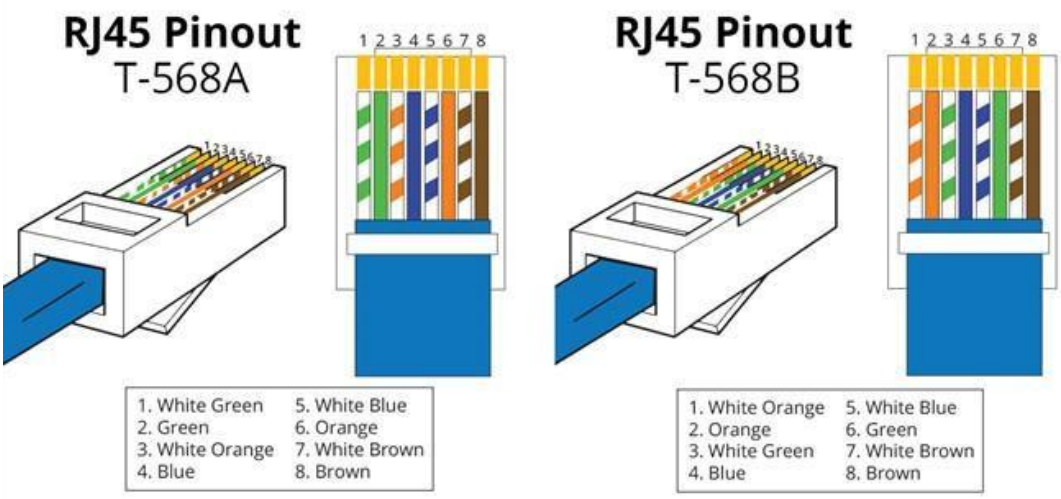
RJ-45 connector is a tool that we put on the end of the UTP cable. With this we can plug the cable in the LAN port.

Cable test:

A cable tester is a electronic device used to verify the electrical connections in a signal cable or other wired assembly. Basic cable testers are continuity tester that verify the existence of a conductive path between ends of the cable, and verify the correct wiring of connectors on the cable.

Straight cable:

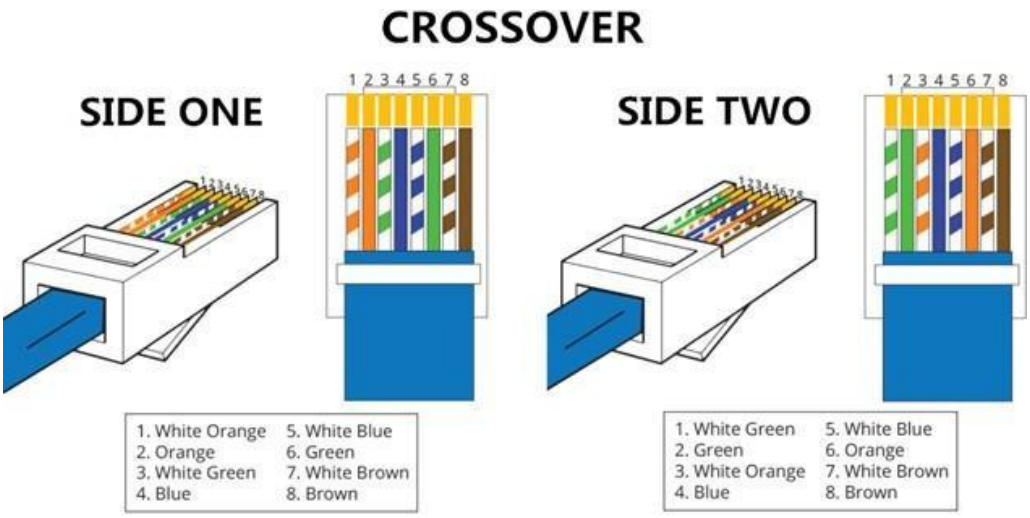
A straight-through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router. This type of cable is also sometimes called a patch cable and is an alternative to wireless connections where one or more computers access a router through a wireless signal. On a straight-through cable, the wired pins match. Straight-through cable use one wiring standard: both ends use T568A wiring standard or both ends use T568B wiring standard. The following figure shows a straight-through cable of which both ends are wired as the T568B standard.



Cross cable:

An Ethernet crossover cable is a type of Ethernet cable used to connect computing devices together directly. Unlike straight-through cable, crossover cables use two different wiring standards: one end uses the T568A wiring standard, and the other end uses the T568B wiring

standard. The internal wiring of Ethernet crossover cables reverses the transmit and receive signals. It is most often used to connect two devices of the same type: e.g. two computers (via network interface controller) or two switches to each other.



Making Straight UTP Cable:

- Peel the end of the UTP cable , approximately 2 cm.

- Open the cable strands , align and follow the arrangement as standard cable image shown below .

- Once the order is according to the standard , cut and flatten the ends of the cable,

- Put the cable is straight and aligned into the RJ - 45 connector , and make sure all cables are in correct position as follows:

Orange White on no 1

Orange on no 2

Green White on no 3

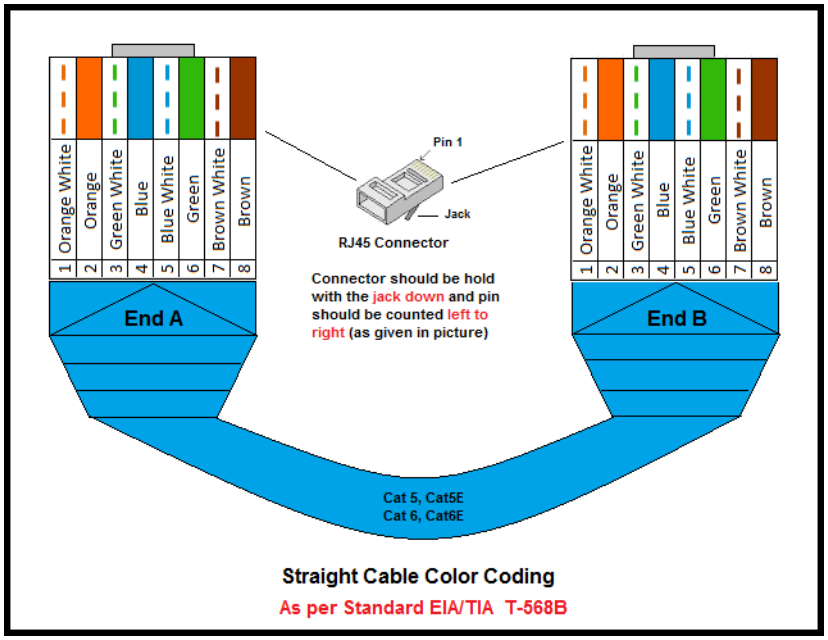
Blue on no 4

Blue White on no 5

Green on no 6

White Brown on no 7

Brown on no 8



- Make crimping using crimp tools , press crimping tool and make sure all the pins (brass) on the RJ - 45 connector has " bite " of each cable . usually when done will sound "click ". Once finished at the end of this one , do it again at the other end cable.

The final step is to check the cable that you created earlier using the LAN tester , enter each end of the cable (RJ- 45) to each LAN port available on the tester , turn and make sure all of the LEDs light up according to the order of the wires we created.

Creating Cross UTP Cable:-

Creating a cross cable has almost the same steps with straight cable , the difference lies only in the colour sequence from both ends of the cable . Unlike the straight cable that has the same colour sequence at both ends of the cable , the cross cable has a different colour sequences at

both ends of the cable.

The first ends is same with straight cable :

Orange White on no. 1

Orange on no. 2

Green White on no. 3

Blue on no. 4

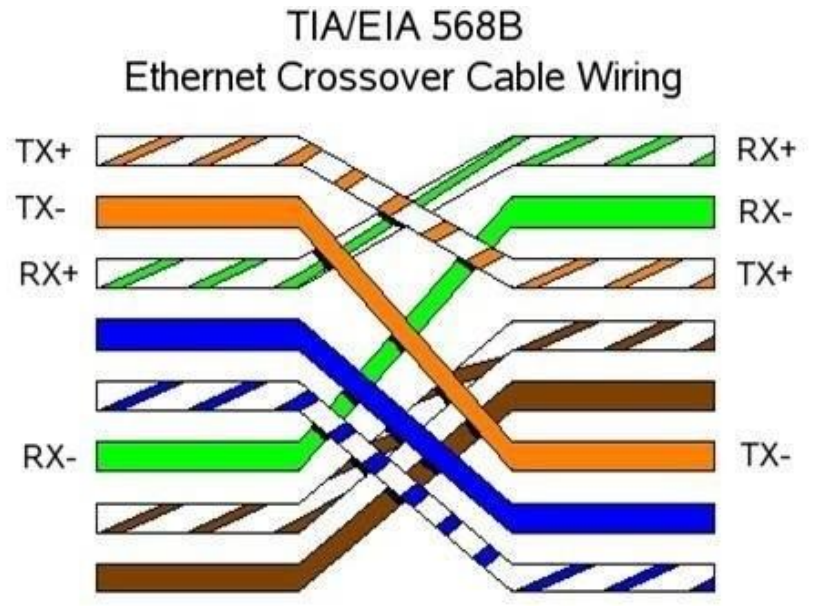
Blue White on no. 5

Green on no. 6 .

White chocolate on no. 7

Brown on no. 8

For the second end of the cable, the colour composition is different from the first . The colour arrangement is as follows



Green White on no. 1

Green on no. 2

Orange White on no. 3

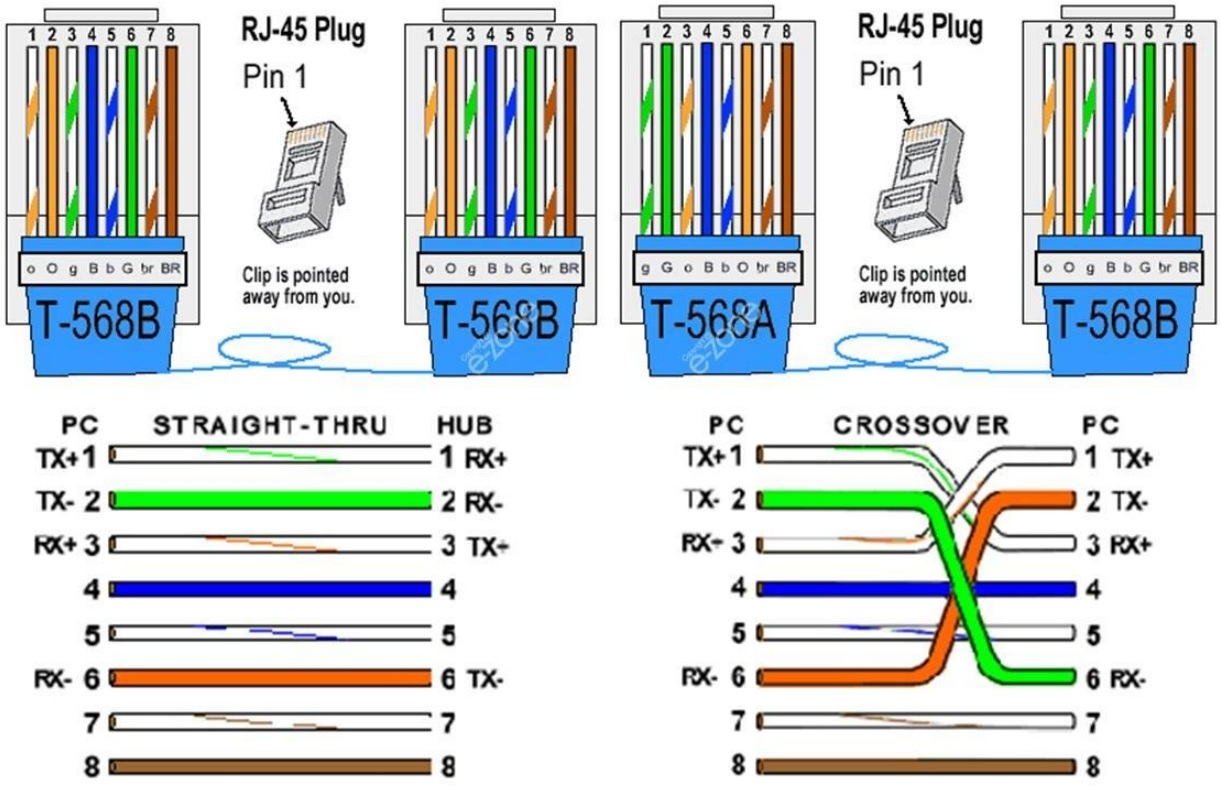
Blue on no. 4

Blue White on no. 5

Orange on no. 6

White chocolate no.7

Brown on no.8



Program 5

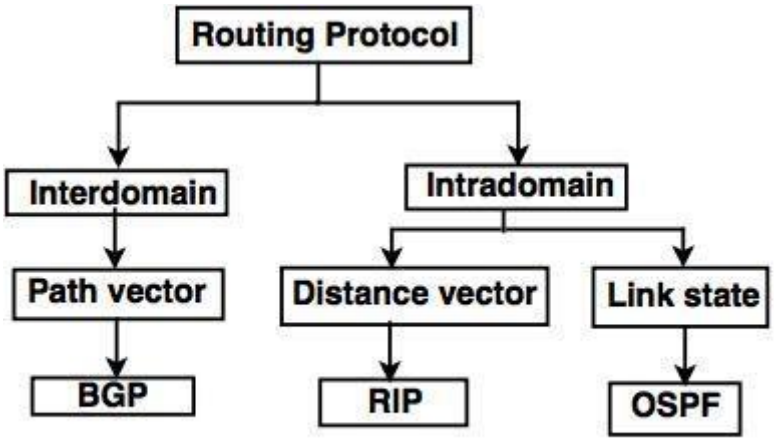
Aim: Introduction to various Interior and Exterior routing Protocols

Routing Protocol:

Routing protocols are set of rules which specify how ***routers communicate*** with each other to distribute information that enables them to select routes between nodes on a computer network.

Types of Routing Protocol:

There are many types of routing protocols, ***two major classes*** are in widespread use on IP networks:-



Classification of routing protocol

1. Interior gateway protocols:-(Intra-Domain)

An interior gateway protocol (IGP) is a type of protocol used for exchanging routing information between gateways (commonly routers) within an autonomous/Independent system (for example, a system of corporate local area networks). This routing information can then be used to route network-layer protocols like IP.

- Interior gateway protocols can be divided into two categories:
  - ➔ Distance-vector routing protocols
  - ➔ Link-state routing protocols.

Distance vector Routing Protocol:

Distance-vector routing protocols use the ***Bellman–Ford*** algorithm. In these protocols, each router does not possess information about the full network topology. It advertises its distance value (DV) calculated to other routers and receives similar advertisements from other routers unless changes are done in the local network or by its neighbours (routers). Using these routing advertisements each router populates its routing table. In the next advertisement cycle, a router advertises updated information from its routing table. This process continues until the routing tables of each router converge to stable values**.**

Examples of distance-vector routing protocols:

- Routing Information Protocol (RIP)
- Routing Information Protocol Version 2 (RIPv2)
- Routing Information Protocol Next Generation (RIPng), an extension of RIP version 2 with support for IPv6
- Interior Gateway Routing Protocol (IGRP)

Link-state routing protocol:

In link-state routing protocols, each router possesses information about the complete network topology. Each router then independently calculates the best next hop from it for every possible destination in the network using local information of the topology. The collection of best-next-hops forms the routing table.

In a link-state protocol, the only information passed between the nodes is the information used to construct the connectivity maps.

Examples of link-state routing protocols:

- Open Shortest Path First (OSPF)
- Intermediate system to intermediate system (IS-IS)

2. Exterior gateway protocols: (Inter-Domain)

Exterior gateway protocols are routing protocols used on the Internet for exchanging routing information between Autonomous Systems, such as **Border Gateway Protocol (BGP)**, **a path-vector routing protocol**. Exterior gateway protocols should not be confused with Exterior Gateway Protocol (EGP), an obsolete routing protocol.

Types of EGP:

- **Path Vector Routing:**

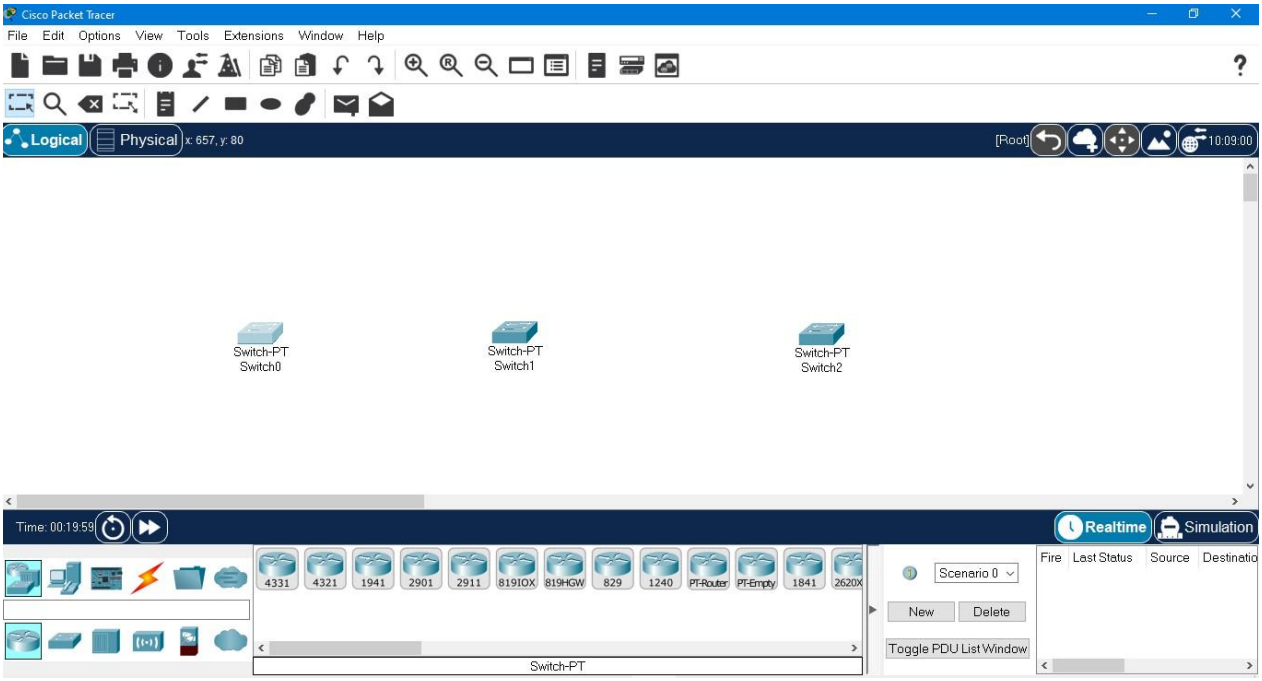
  A path-vector routing protocol is a network routing protocol which maintains the path information that gets updated dynamically. Updates that have looped through the network and returned to the same node are easily detected and discarded. This algorithm is sometimes used in Bellman–Ford routing algorithms to avoid **"Count to Infinity"** problems.

Examples of Path vector Routing:

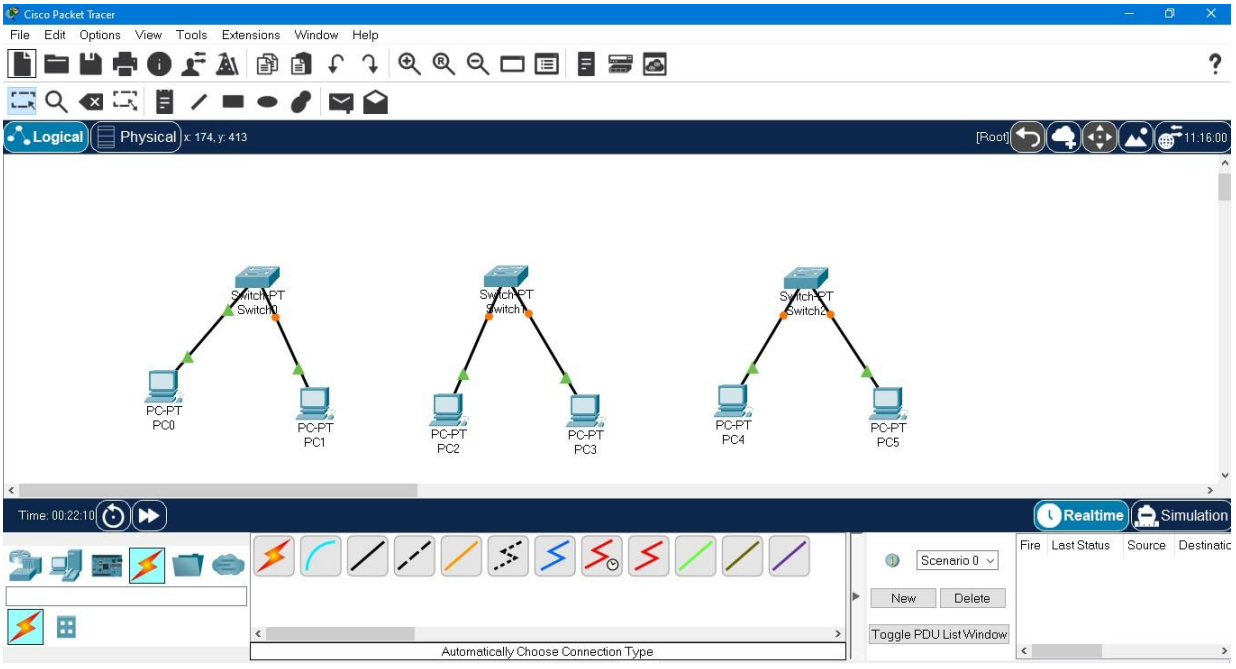
- Border Gateway Protocol (BGP)

➔ Configuration of Routing Information Protocol (RIP) Using Cisco Packet Tracer:-

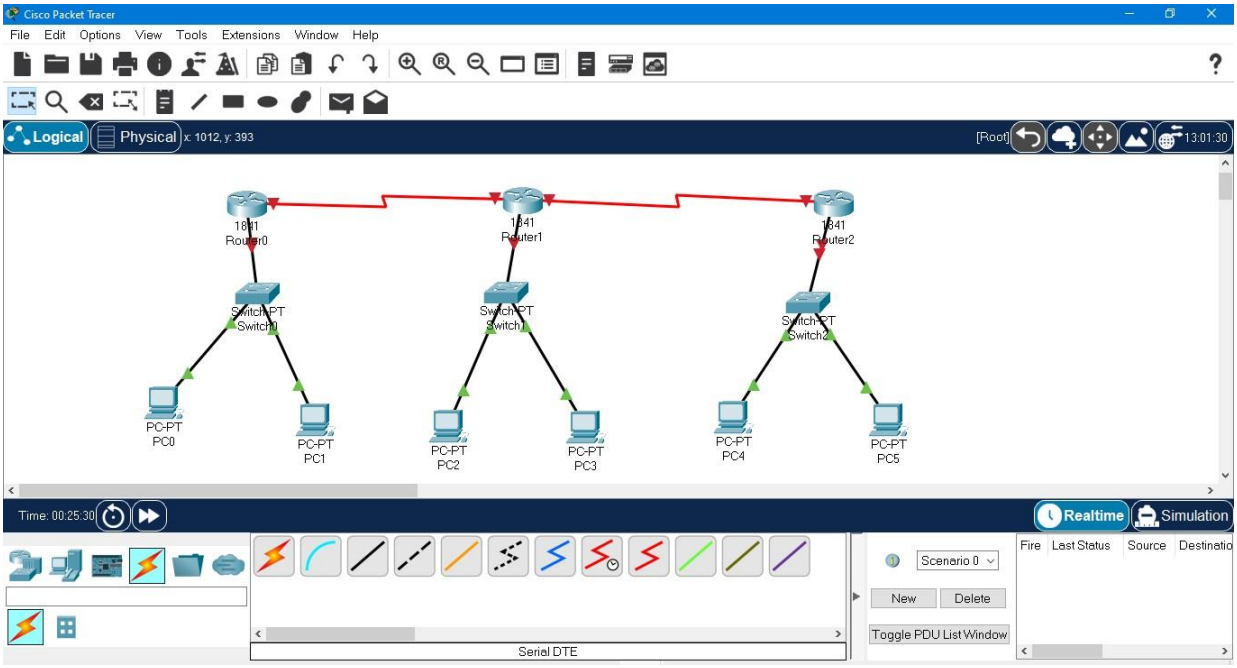
Step 1. Choose Switch and select 3 Switch-PT.As shown:



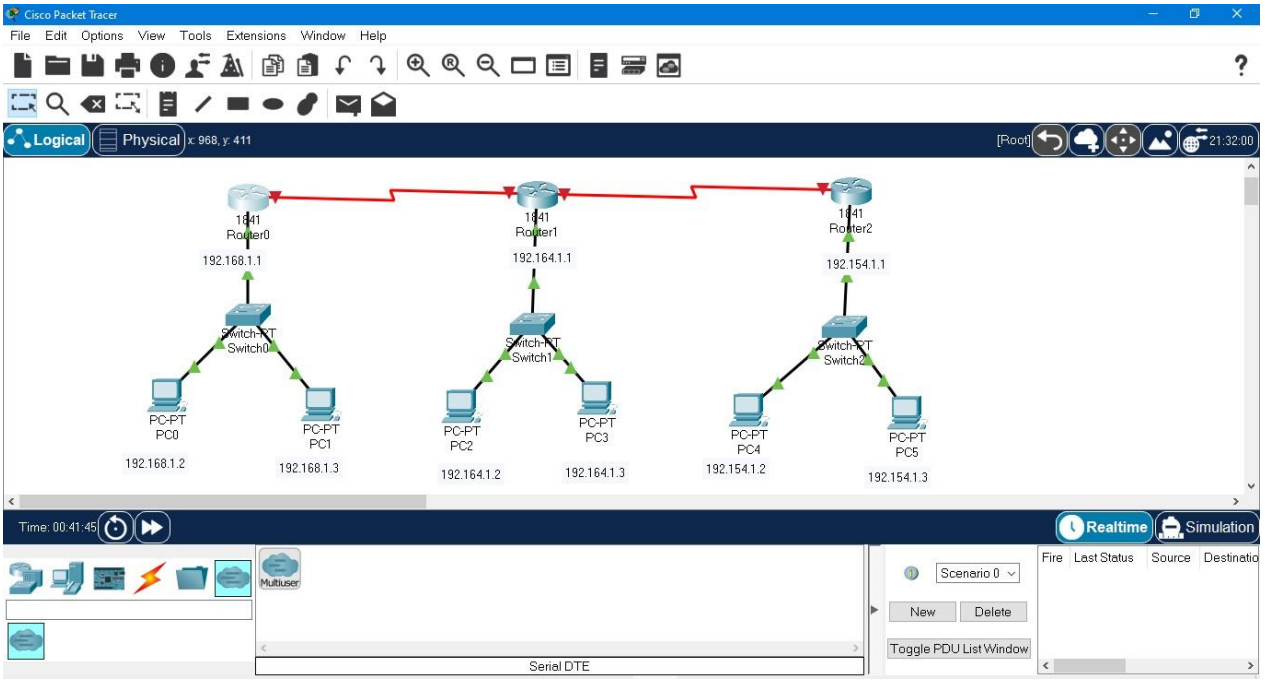
Step 2. Choose PC and select 6 PCs to connect with Switches. Connect each pair of 2 PCs with Switches using Automatic type connection. As shown:



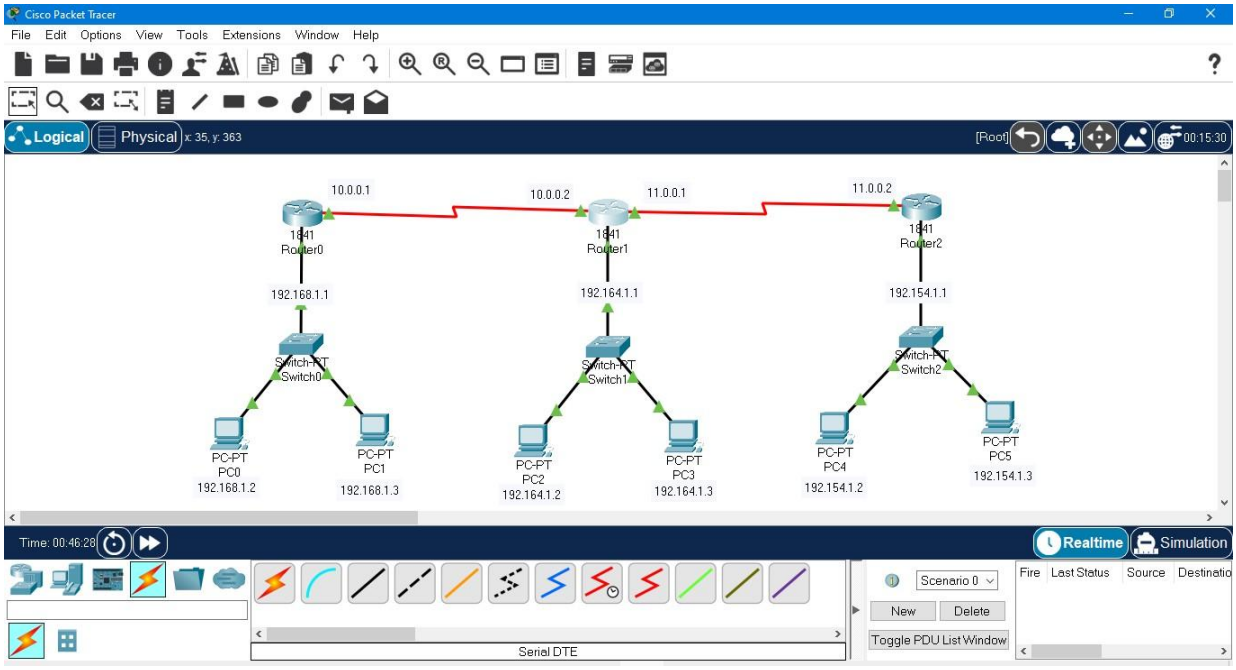
Step 3. Now choose 3 Routers(1841) and connect these with switches using Automatic connection type. Connect router with each other by DTE cable. As shown:



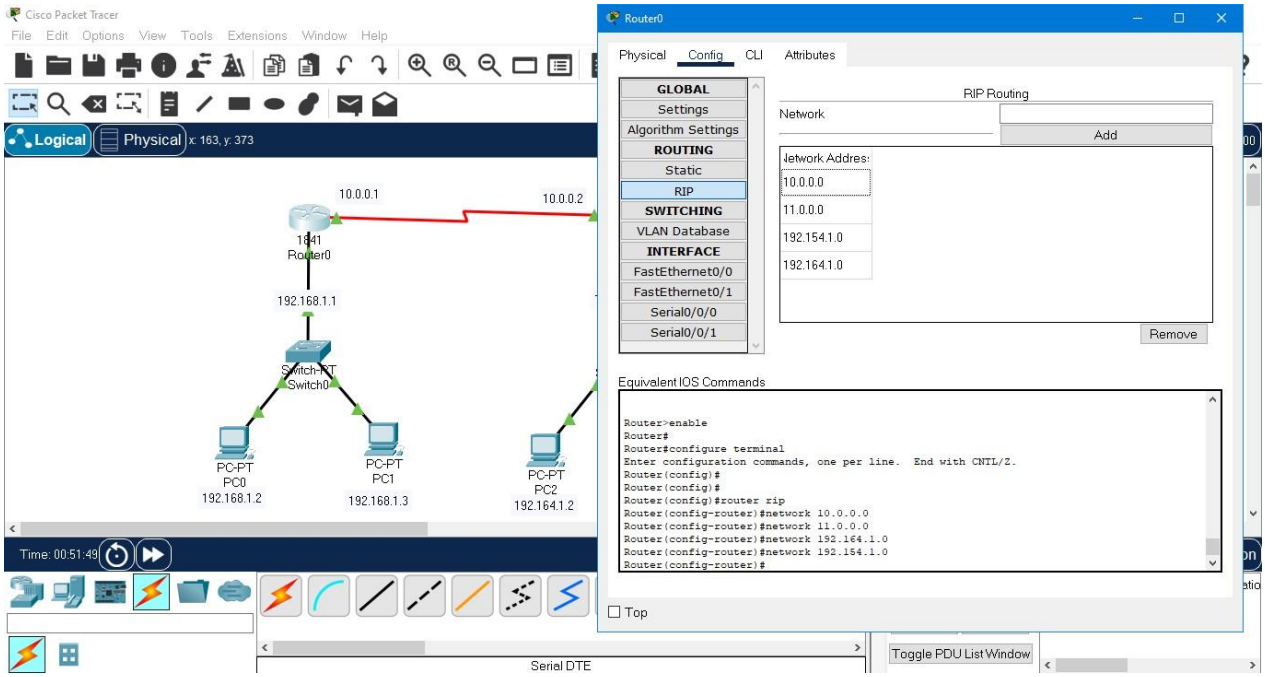
Step 5. Now Assign IP to Routers and PCs connected.



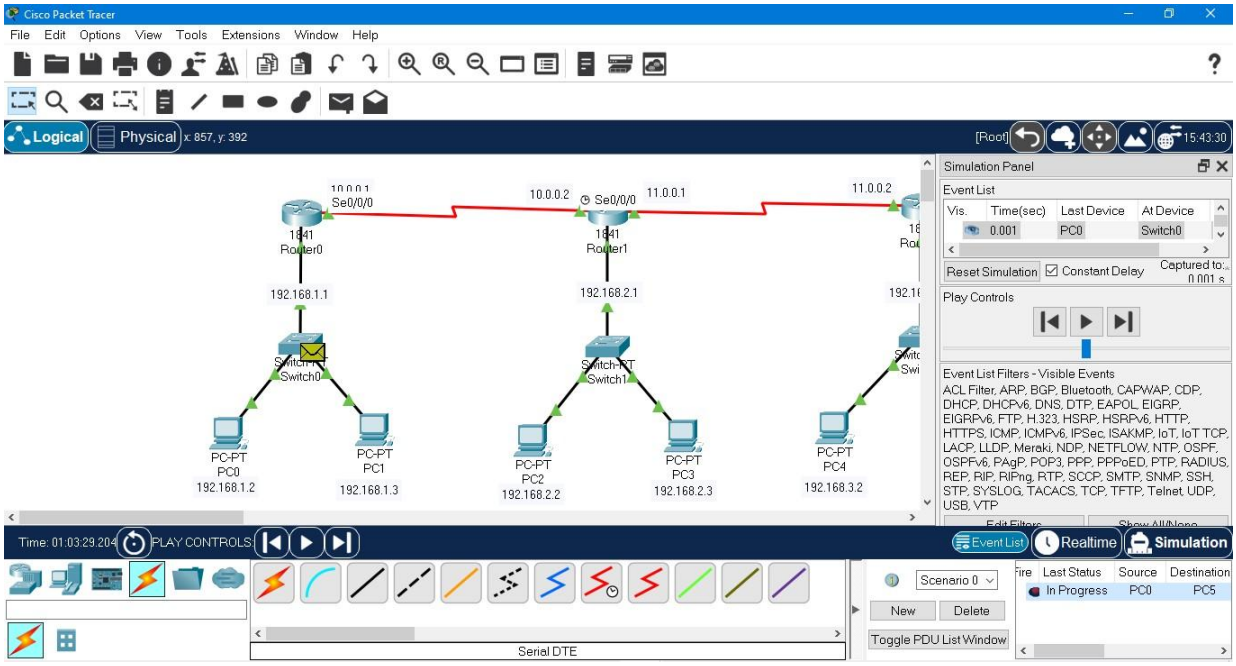
Step 6. Give Serial IPs to router to connect them together. As shown:



Step 7. Updating RIP table of ROUTER 0. As shown:



Step 8.Now Transfer the *message* from PC0 to PC5. As shown:



Program 6

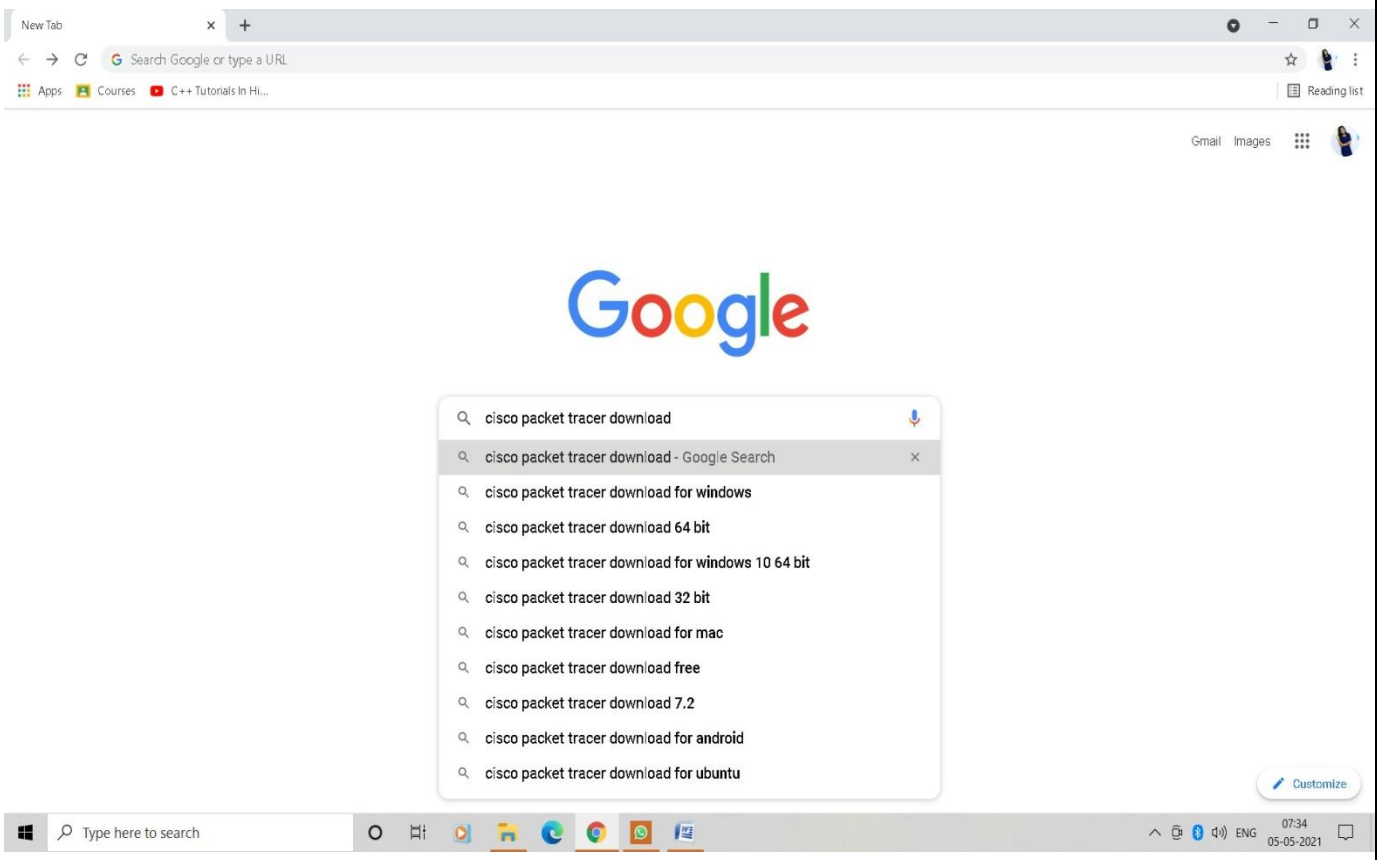
Aim :- Installation and Introduction of simulation tools packet tracer/ GNS3.

GNS3 (Graphical Network Simulator -3) :

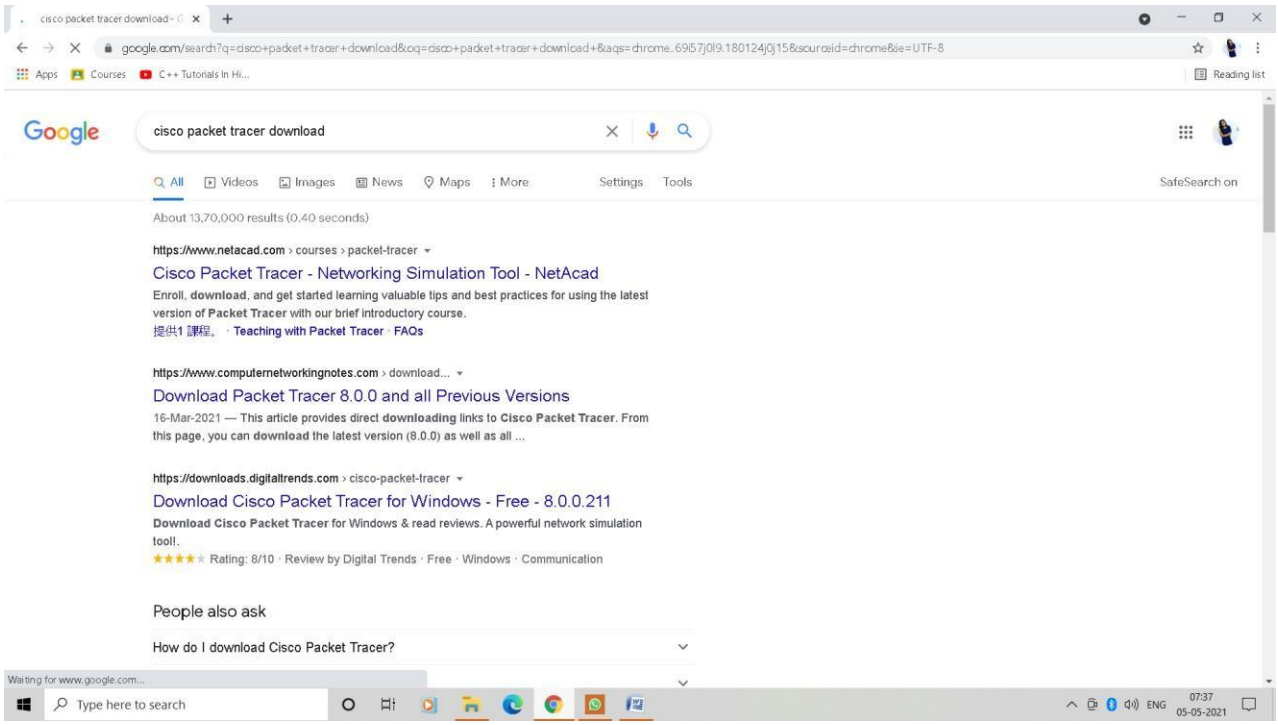
It is a network software emulator first released in 2008. It allows the combination of virtual and real devices , used to simulate complex networks. It uses Dynamips (dynamip s is an emulator computer program that was written to emulate Cisco routers.) emulation software to simulate Cisco IOS**.**

Installation of Packet Tracer:

Step 1 : First serach " cisco packet tracer download " in browser.

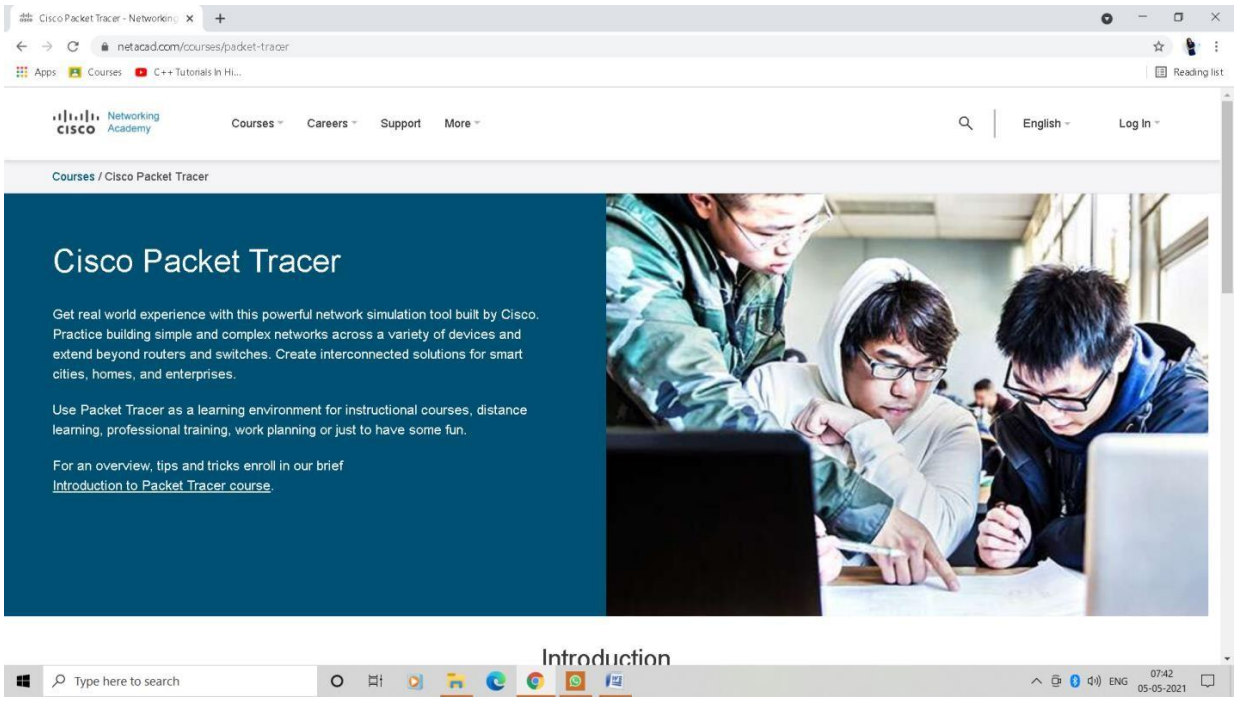


Searching in goggle



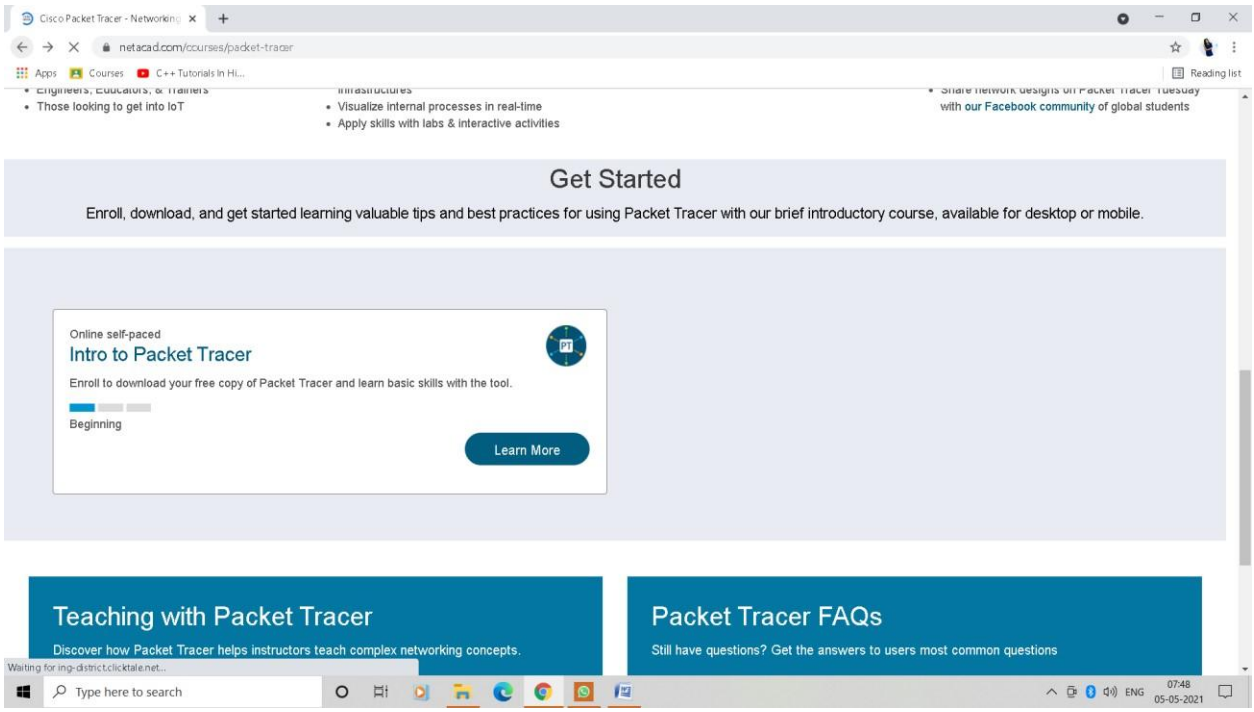
Result of search

Step 2 : Now click on the website [https://www.netacad.com/courses/packet-tracer .](https://www.netacad.com/courses/packet-tracer)

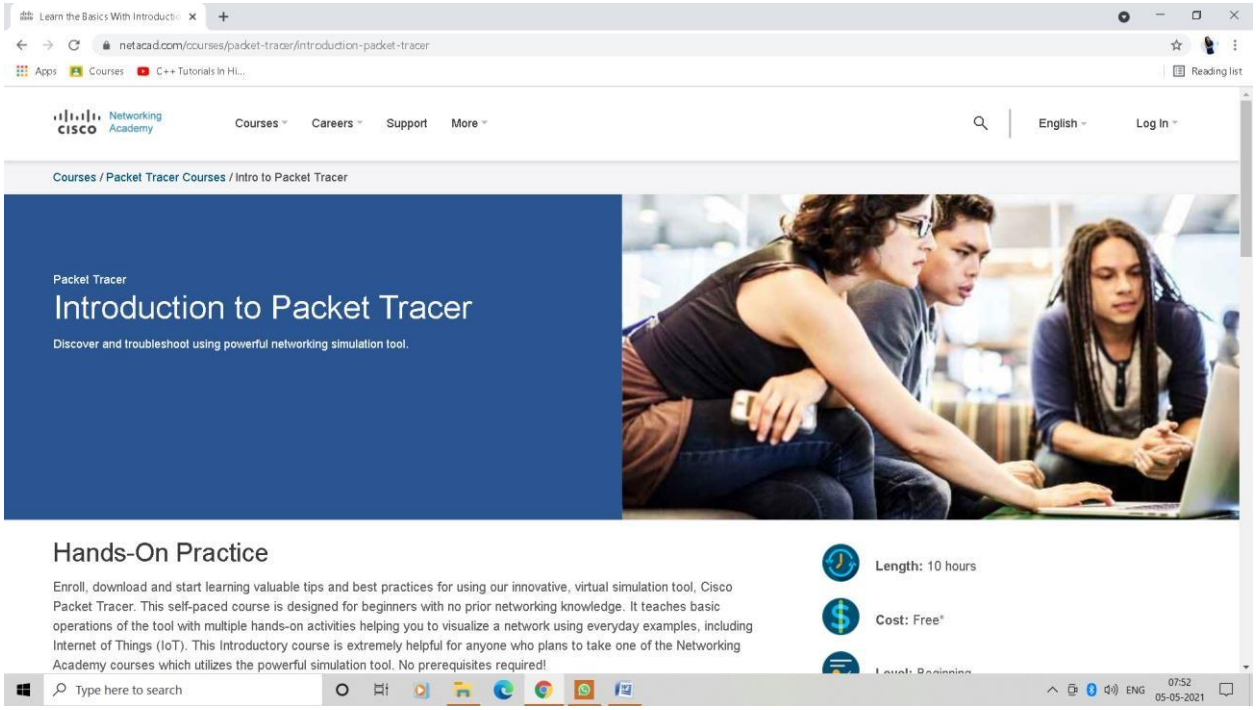


After clicking on the link

Step 3 : Now slide down and then we find page as shown in below and the we click on <u>learn more</u> option.

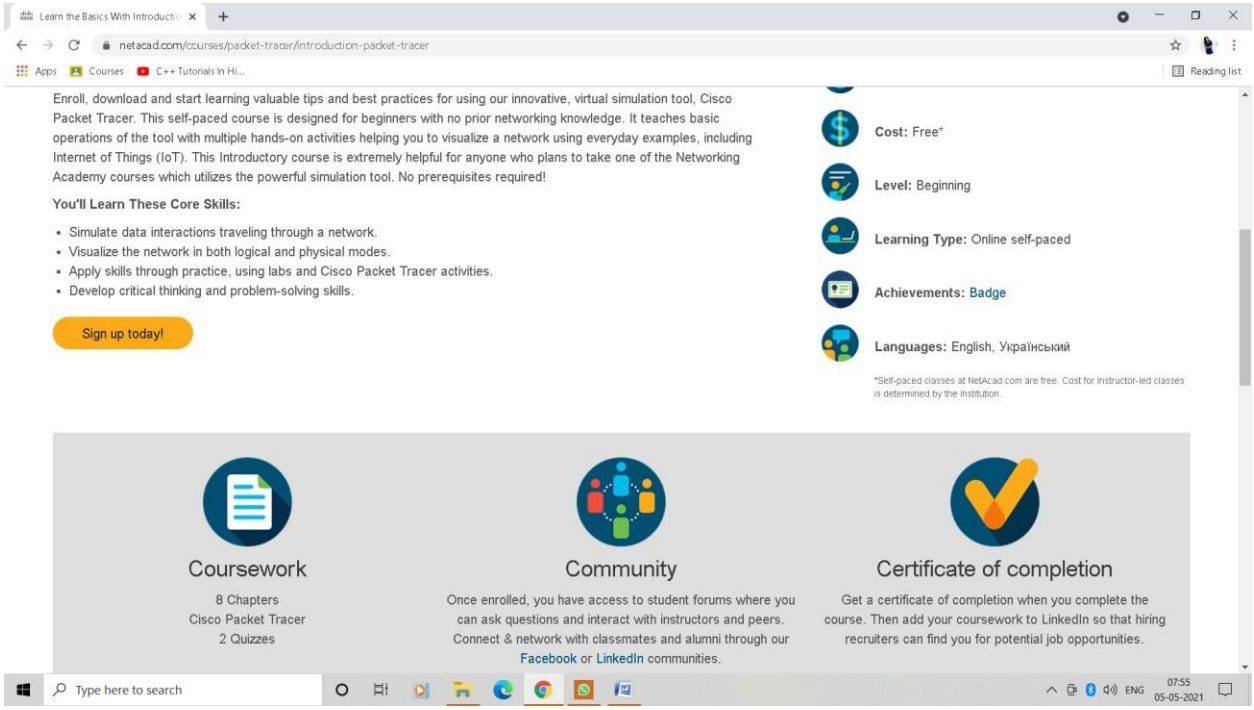


Learn on option

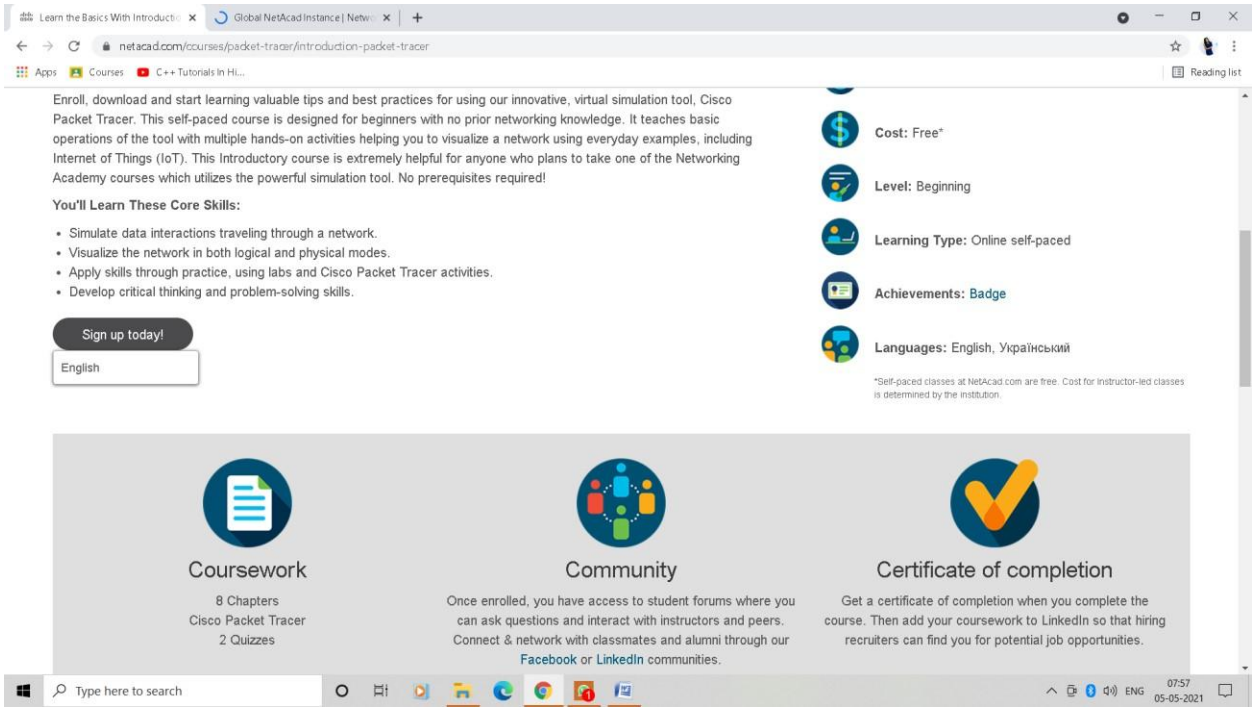


After clicking on learn more option.

Step 3 : To download cisco packet tracer we need to enroll as a student in the free course. For this we click on sign up today option.

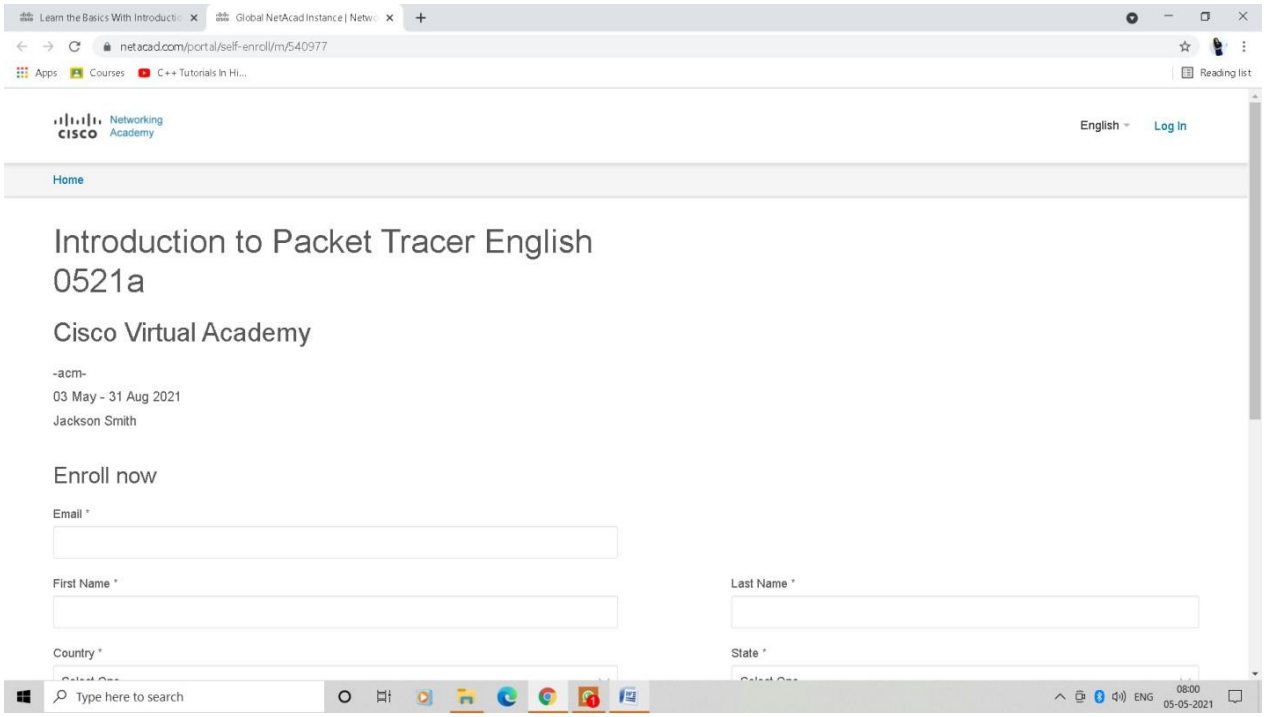


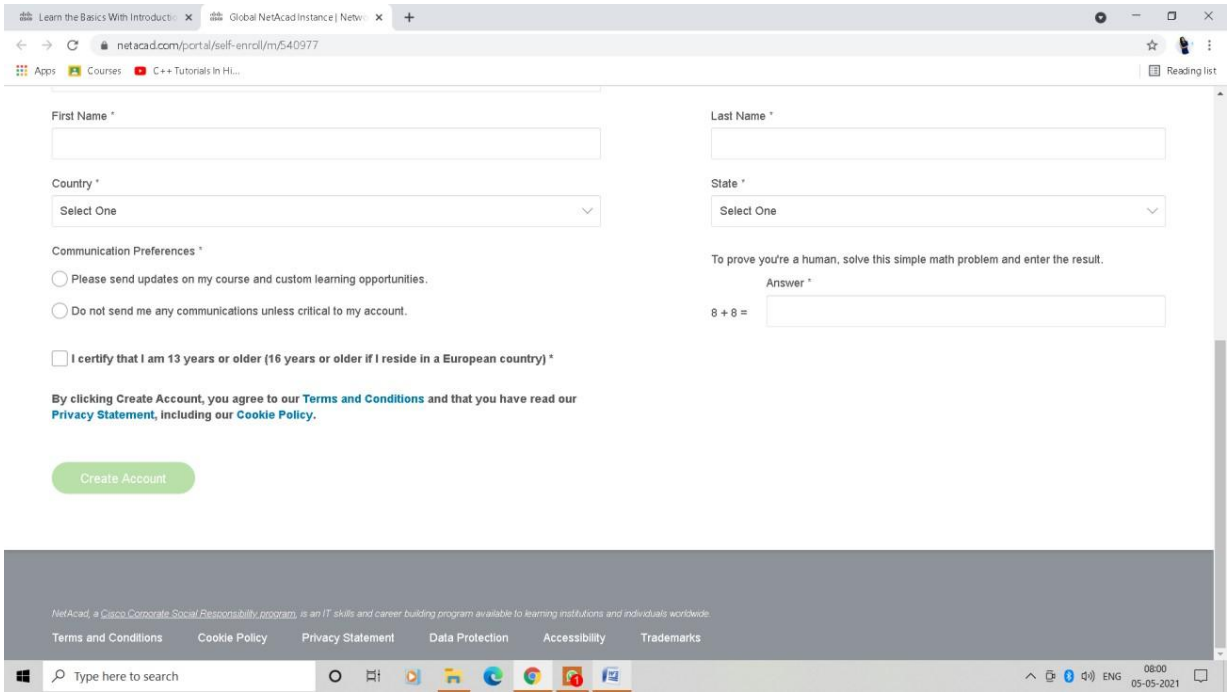
Sign up today option



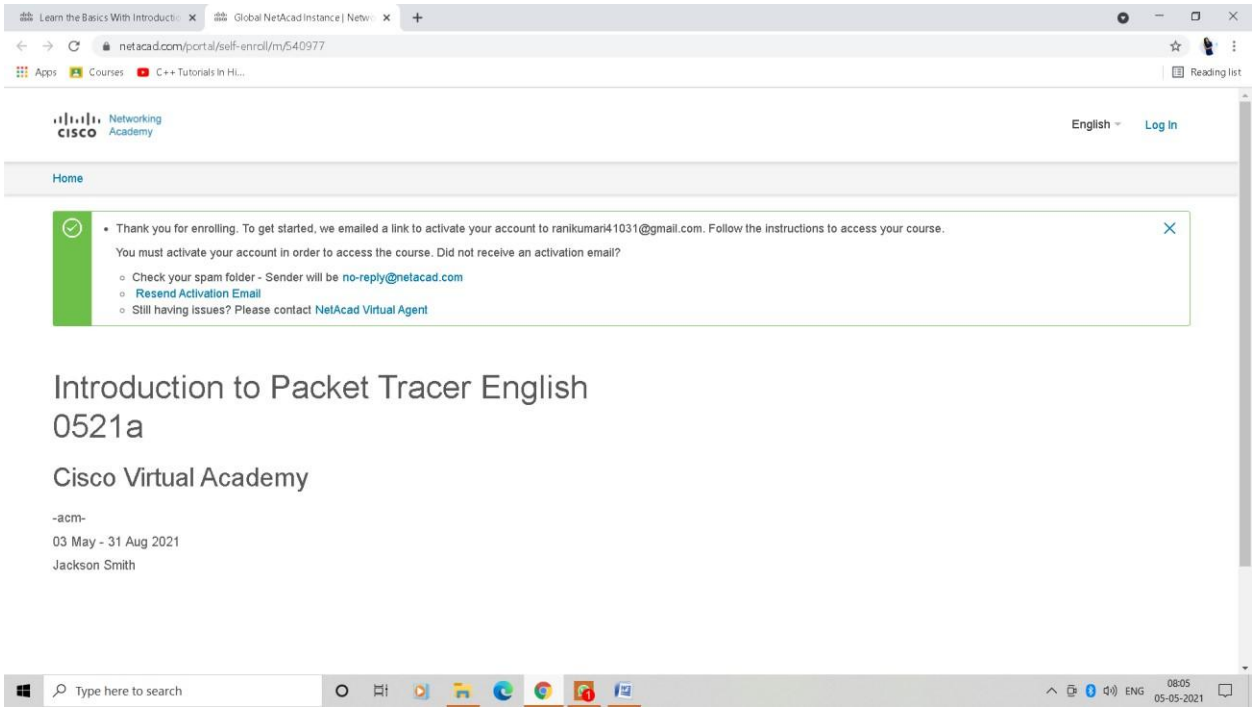
When we go to the sign up today option, it show to choose language as shown in above picture.

Step 4 : After choosing the language we get sign up page as shown in below.





Step 5 : After enrolling we get an mail to active our account.



Networking Academy

Hello Rani Kumari,

Welcome to Cisco Networking Academy!

To activate your account, please click the button below:

Activate account

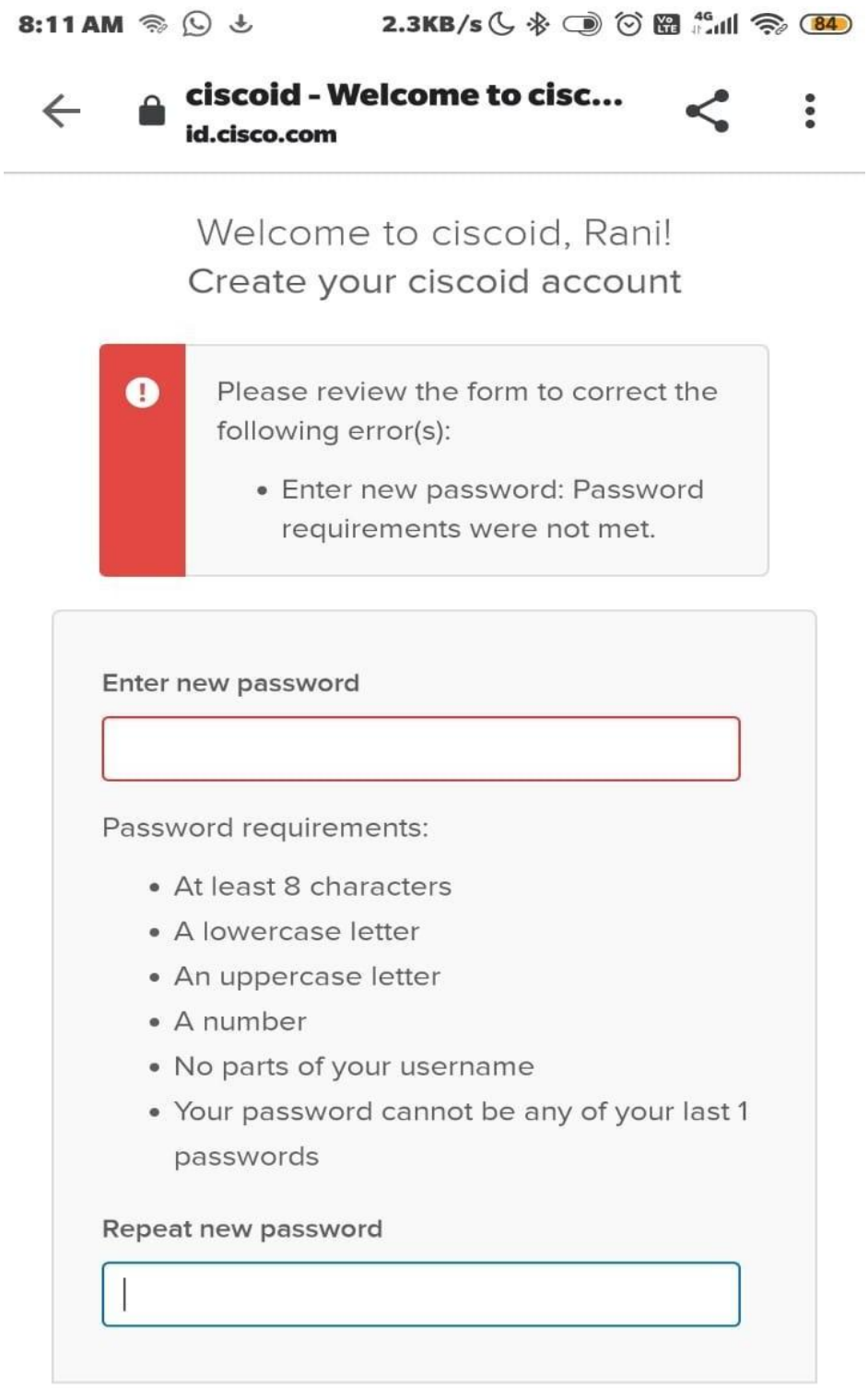
TIPS:

- This link is valid for a limited time. If this link is expired, please go to https://www.netacad.com and click on Log In/Resend Activation Email to get a new link.
- If you do not see Activate account button above, please copy the following link and paste into your browser:

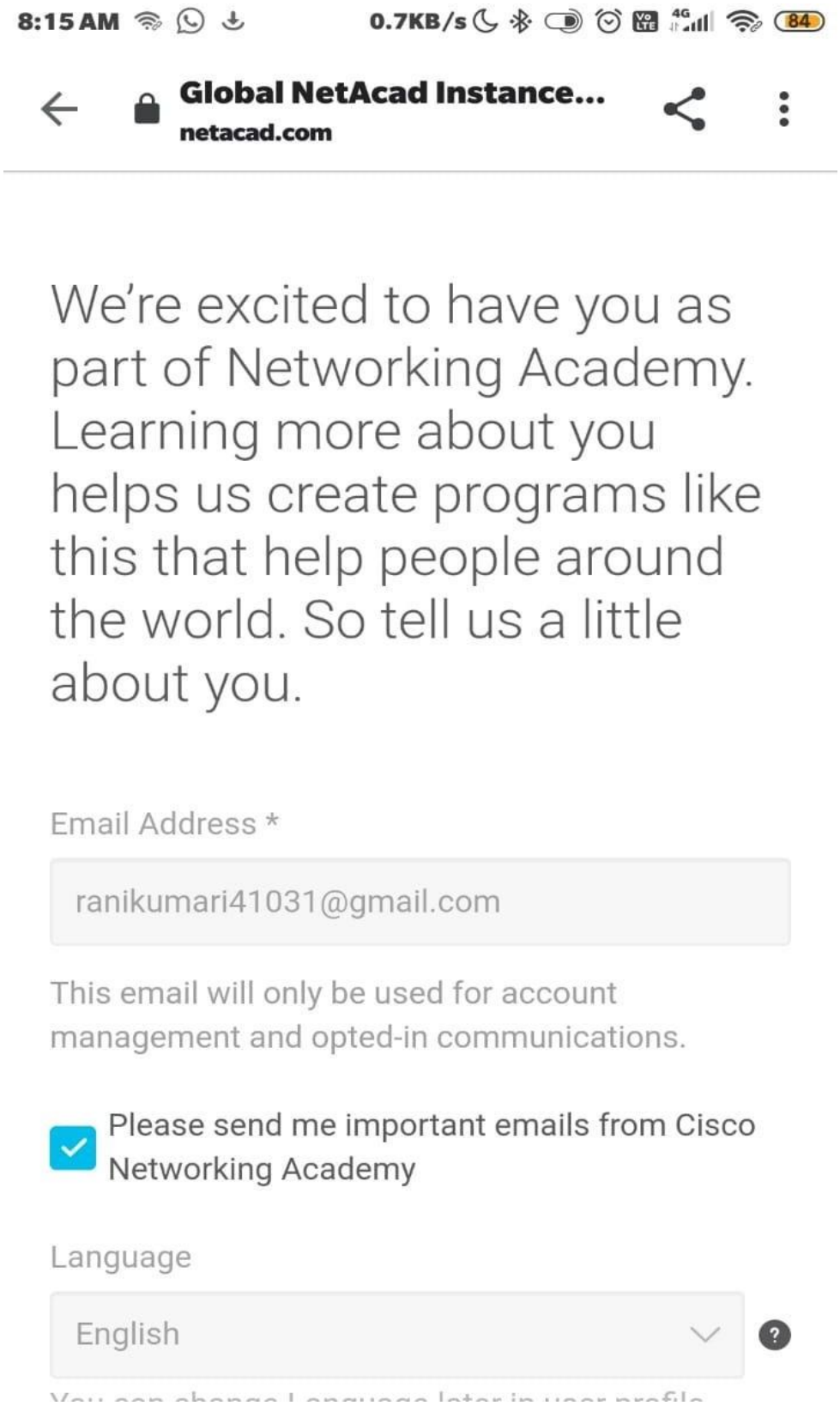
  https://id.cisco.com/welcome/BsJwK0o59Ao5YuXtDqNb?fromURI=https://www.netacad.com/portal/saml_login

- If you already have an account, go to https://www.netacad.com and click Log In to access your courses.
- Your NetAcad ID is 1024764838. Keep this handy in case you ever need support

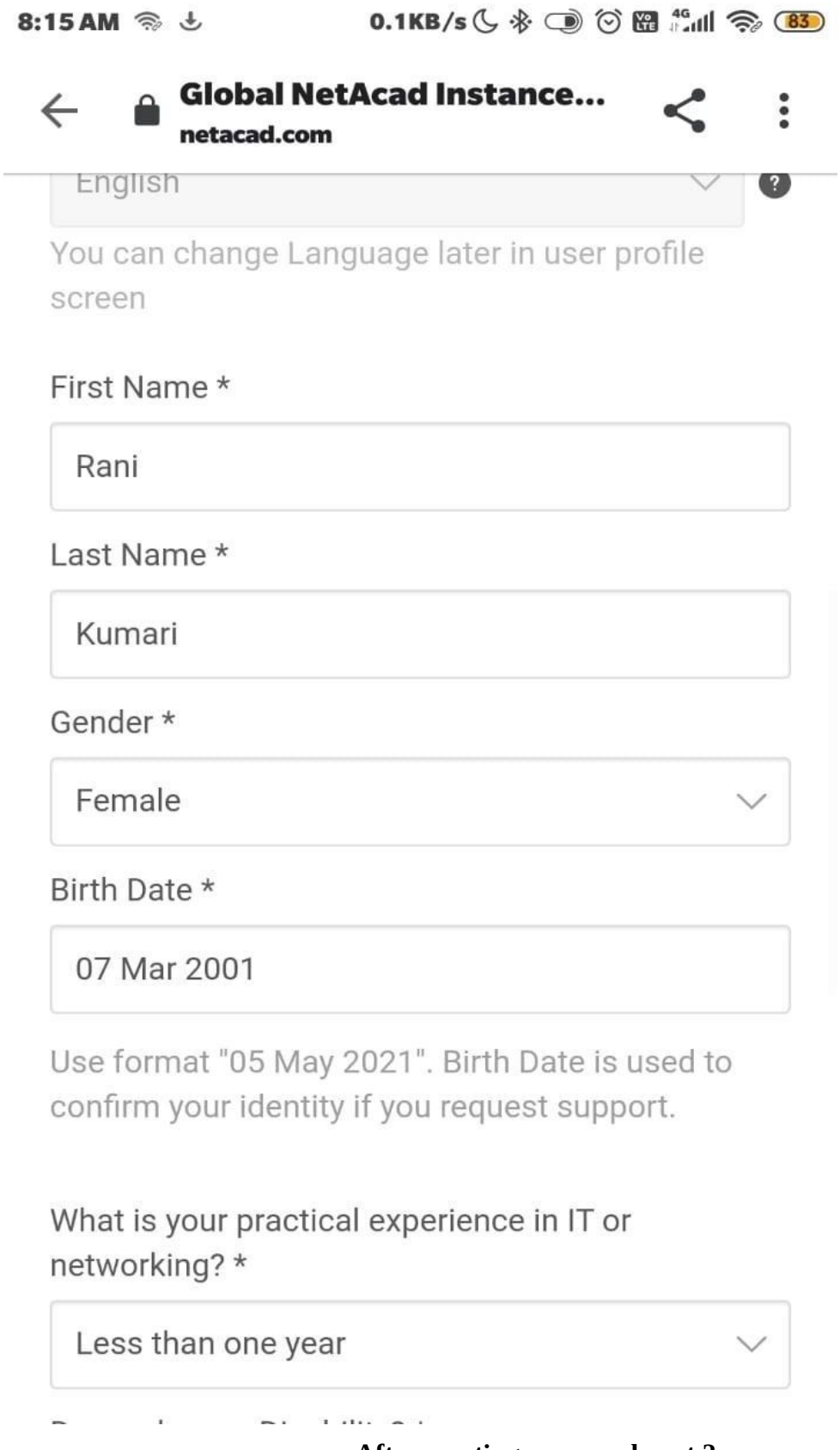
Step 6 : After clicking on active account mail we have to create a password for account and then they ask about personal information like DOB , Gender etc.



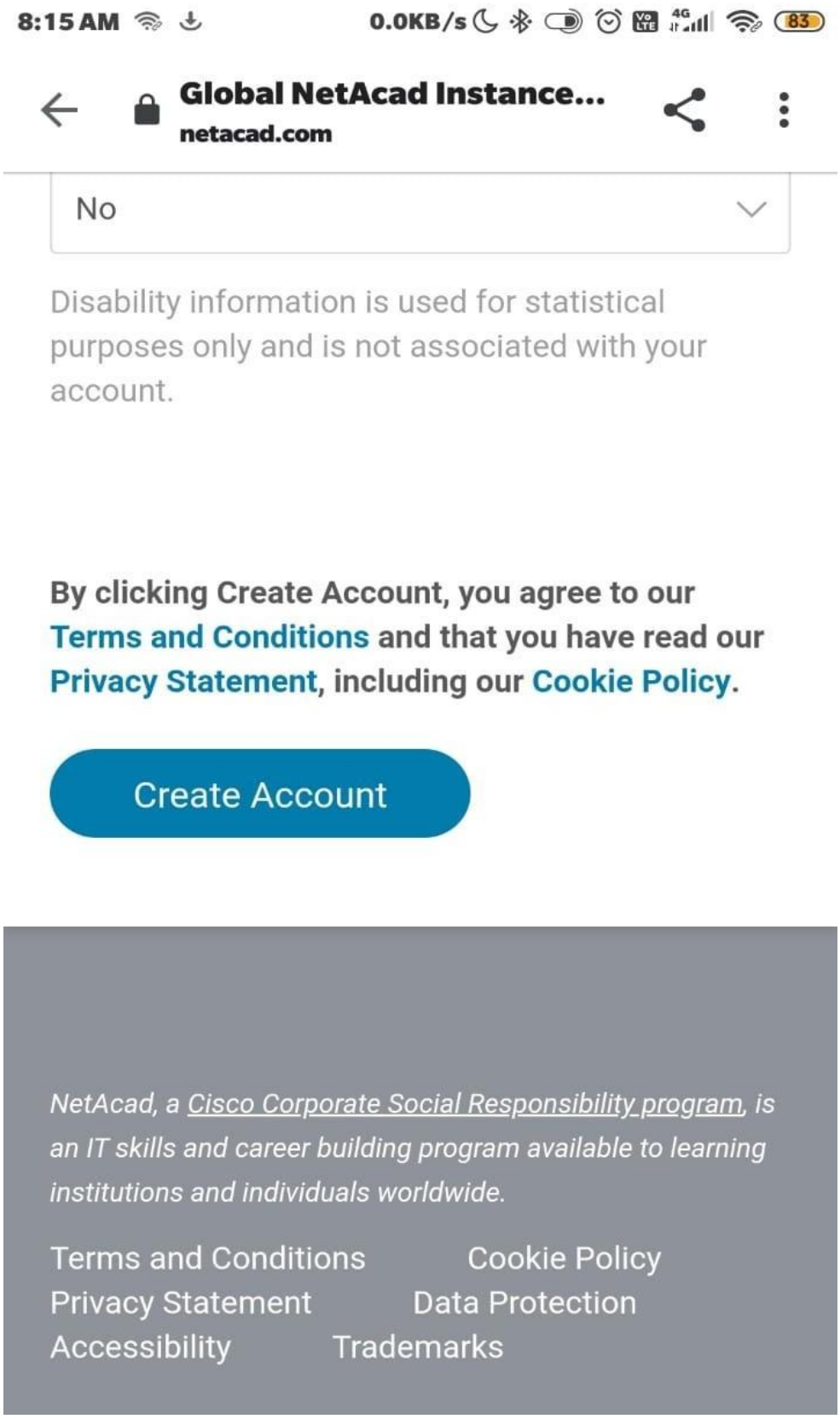
Password Creation



After creating password part 1

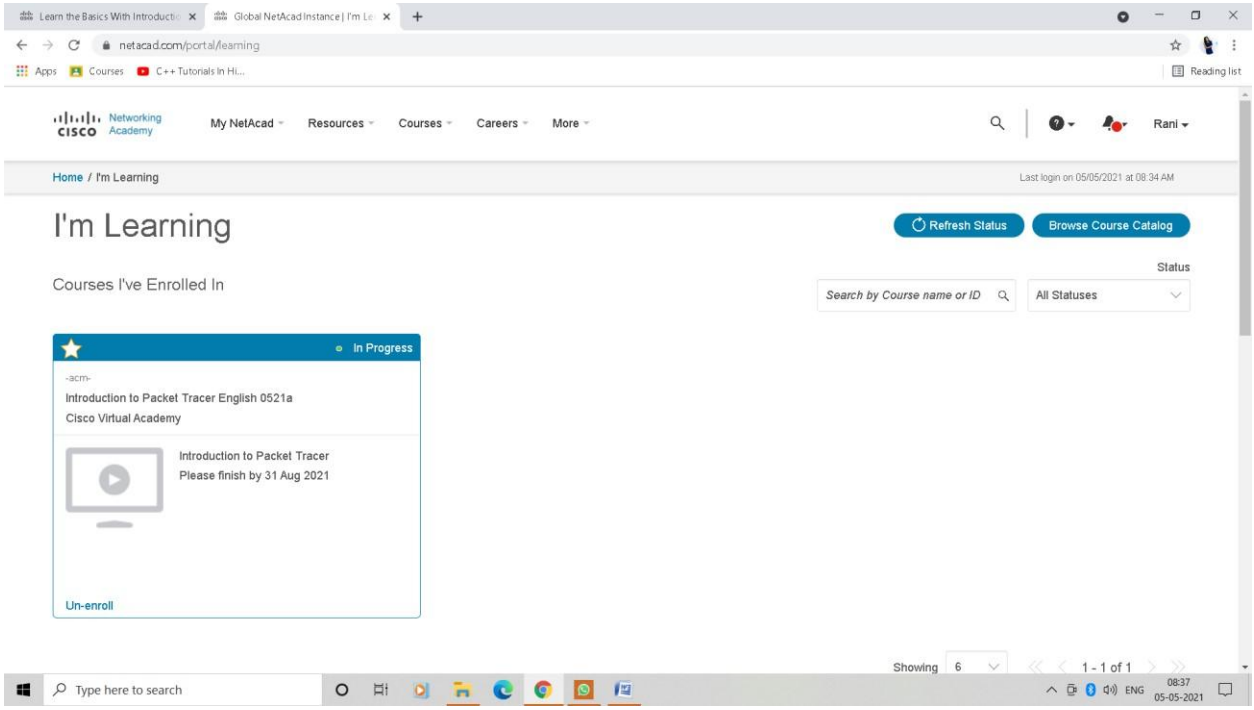


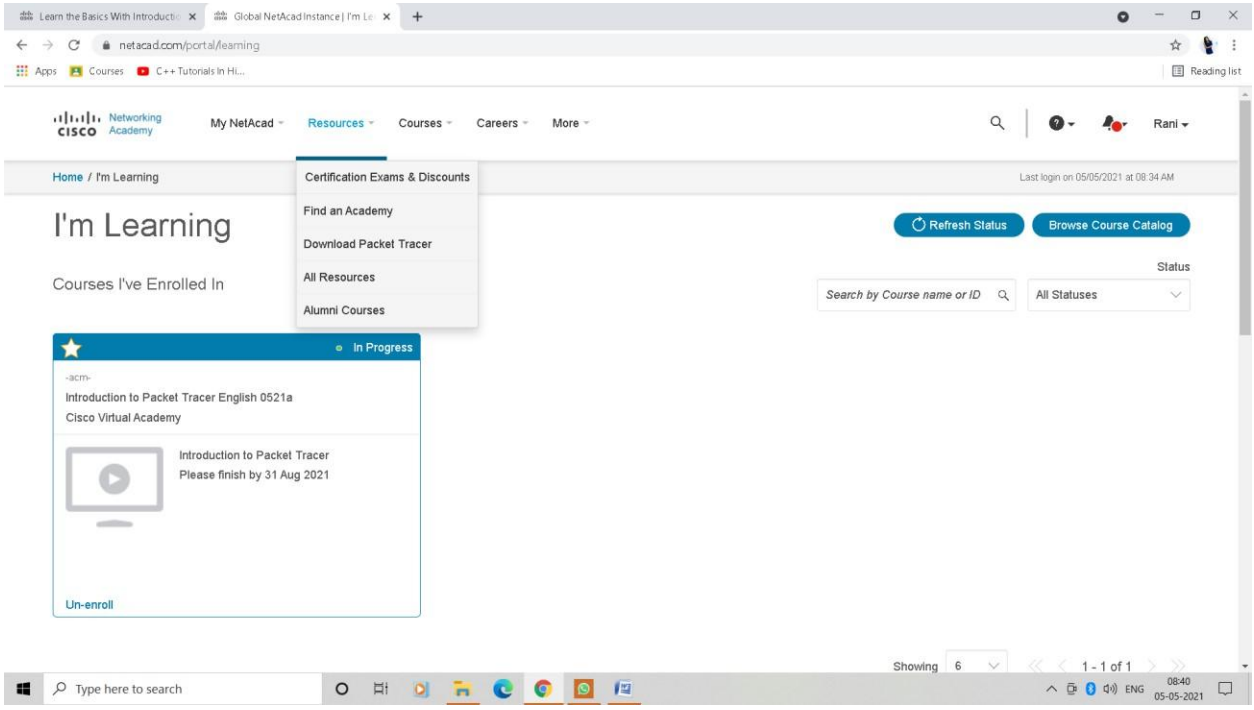
After creating password part 2



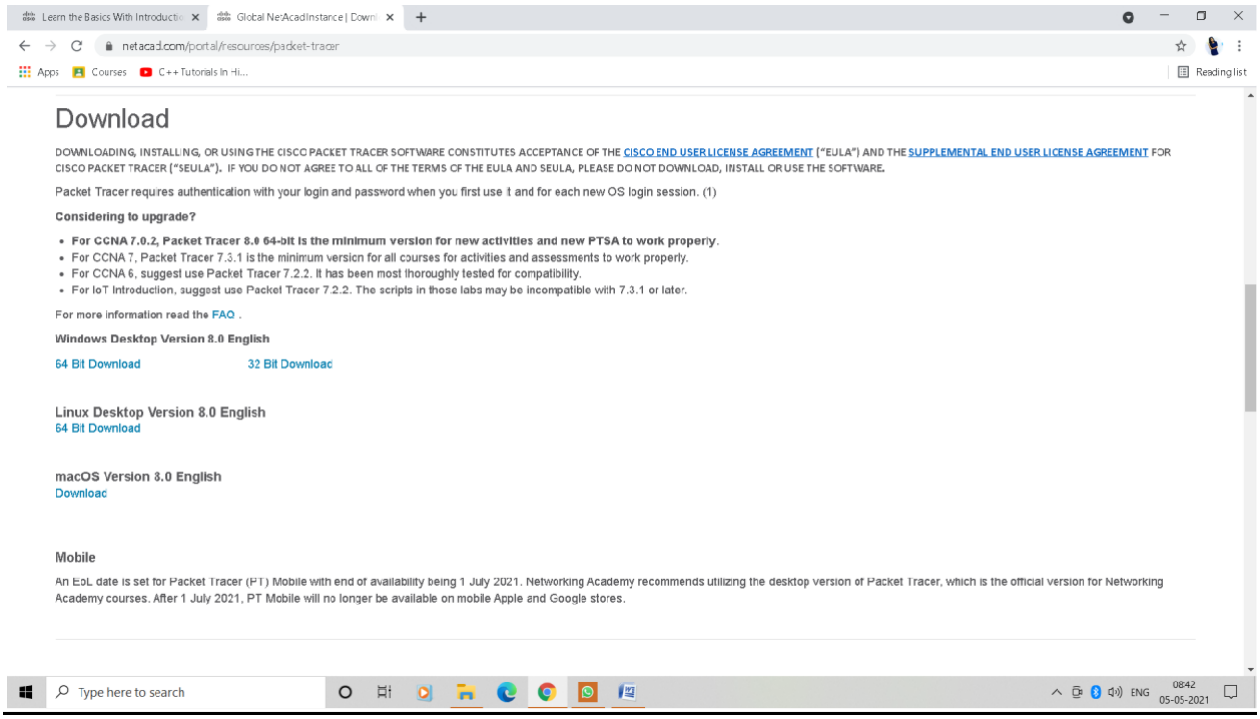
Final part after creating password and now click on create account option

Step 6 : After creating account successfully now we have resources option and we click on resources option and get packet tracer option , click on that.



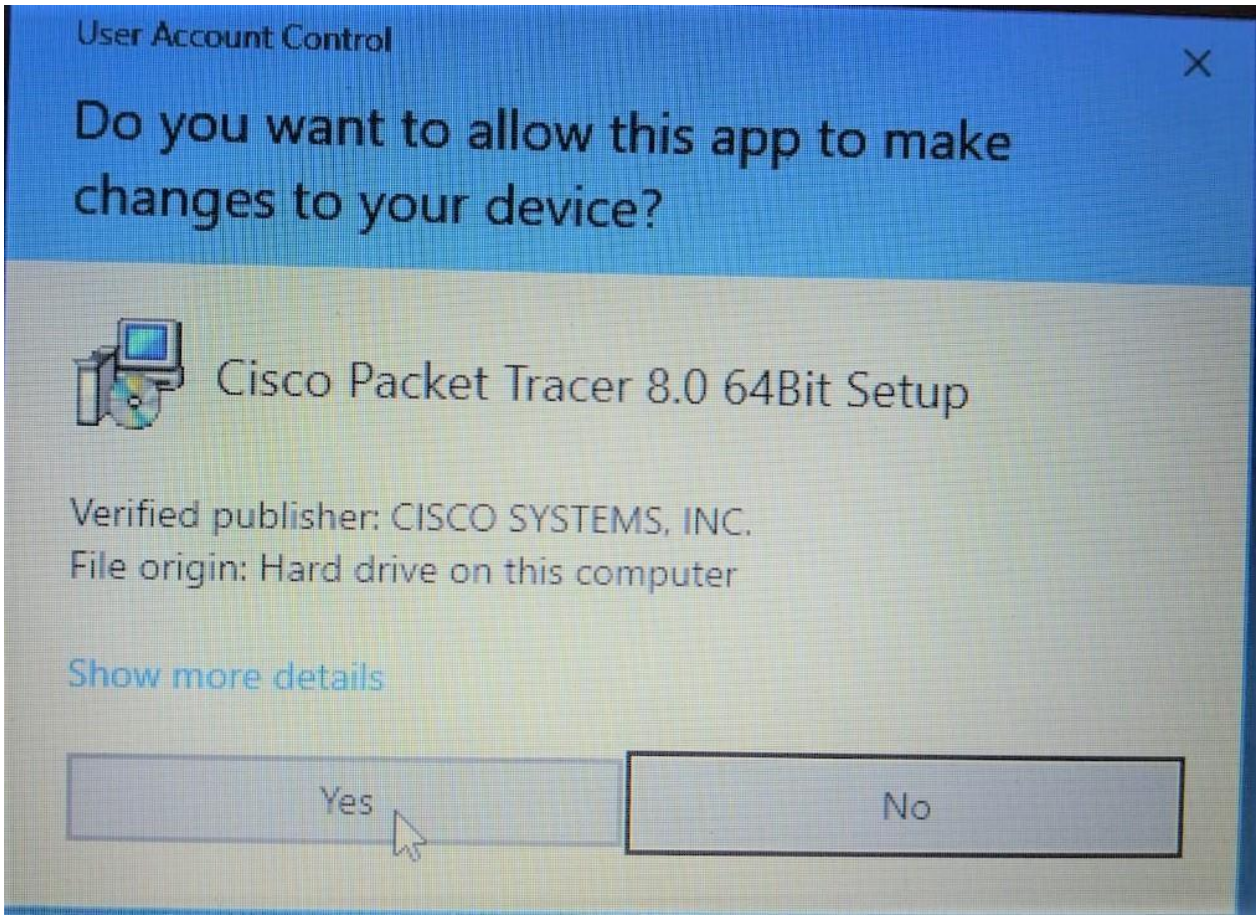


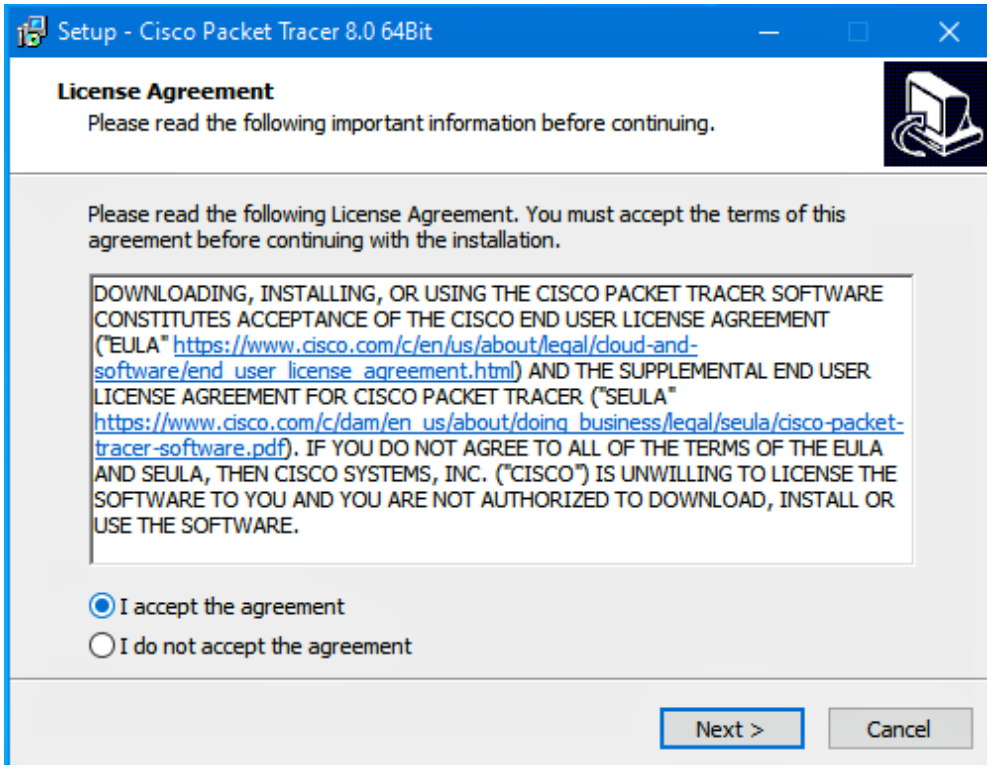
<u>After clicking on resources option we get download packet tracer</u>

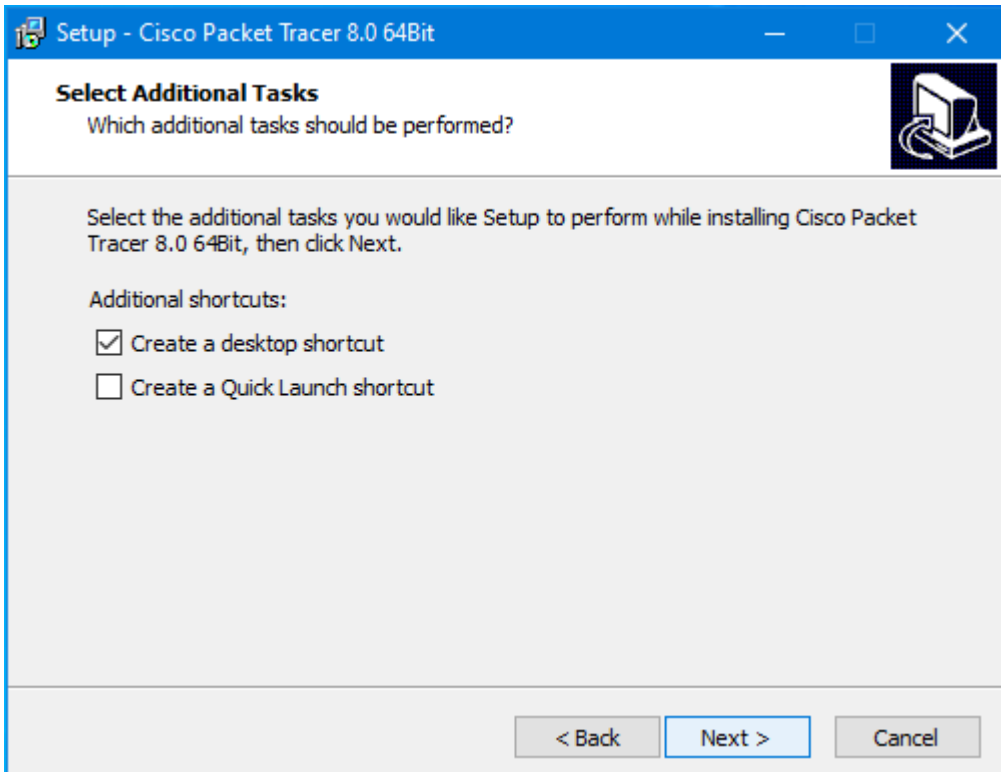


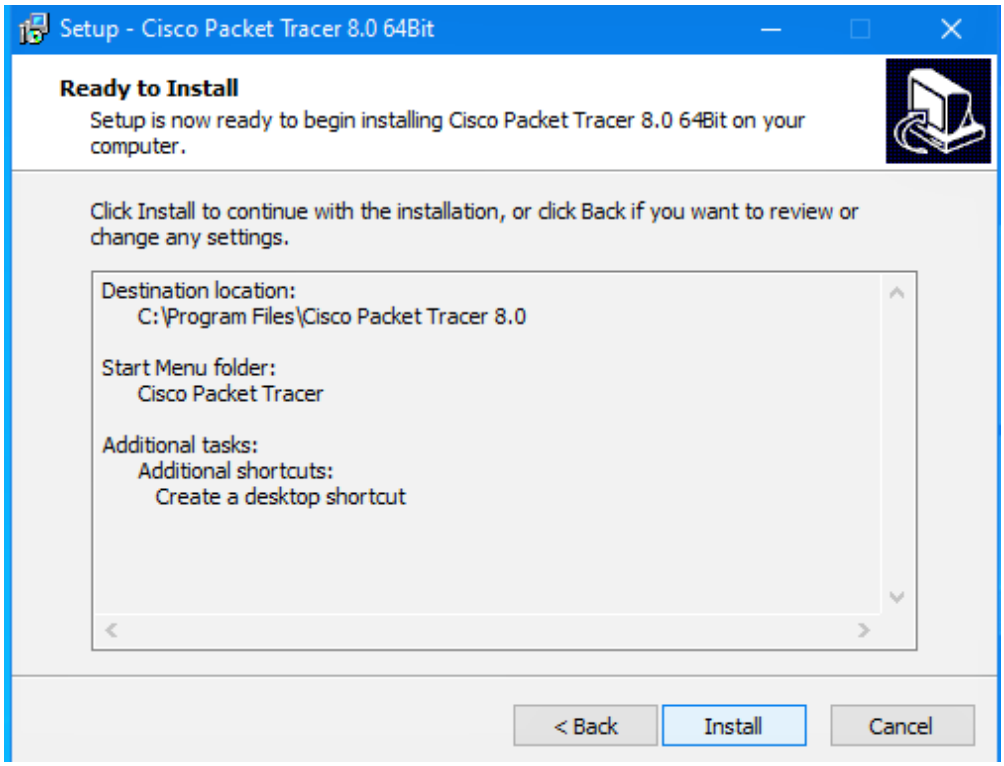
Choose operating system

Step 7 : Installation of cisco packet tracer.

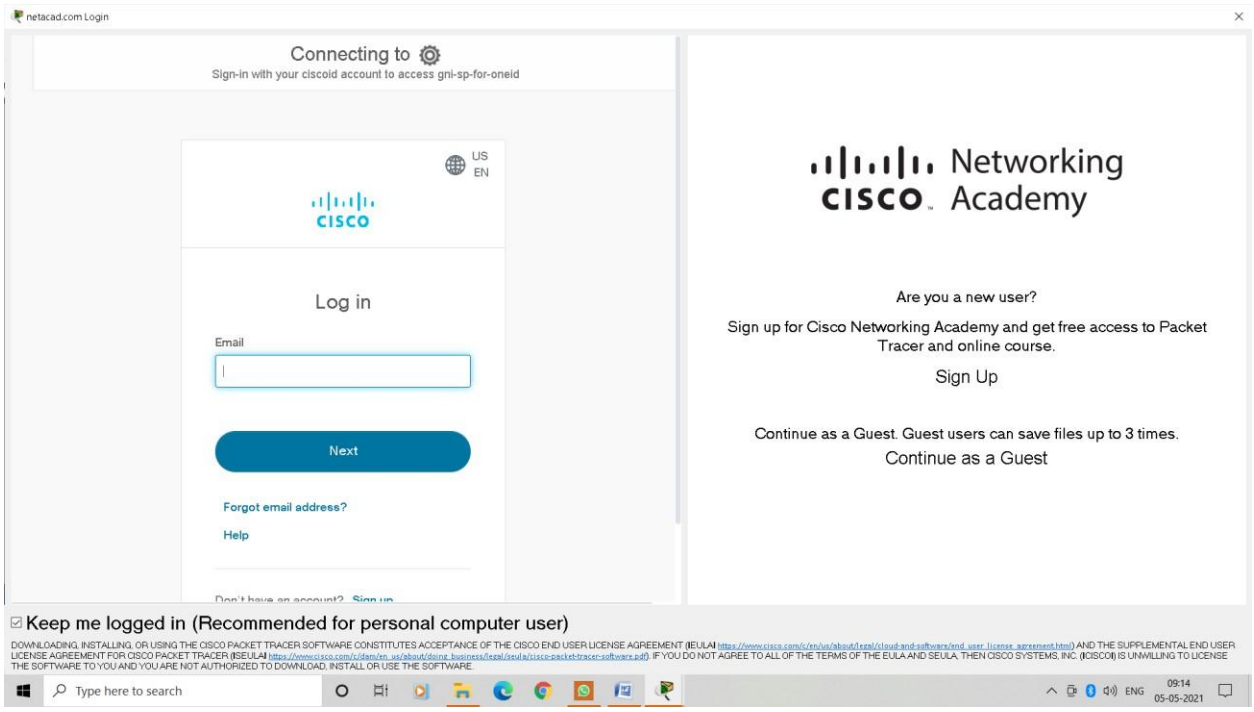

User Account Control
Do you want to allow this app to make changes to your device?
Cisco Packet Tracer 8.0 64Bit Setup
Verified publisher: CISCO SYSTEMS, INC.
File origin: Hard drive on this computer
Show more details
Yes
No


Setup - Cisco Packet Tracer 8.0 64Bit
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
DOWNLOADING, INSTALLING, OR USING THE CISCO PACKET TRACER SOFTWARE CONSTITUTES ACCEPTANCE OF THE CISCO END USER LICENSE AGREEMENT ("EULA" https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end_user_license_agreement.html) AND THE SUPPLEMENTAL END USER LICENSE AGREEMENT FOR CISCO PACKET TRACER ("SEULA" https://www.cisco.com/c/dam/en_us/about/doing_business/legal/seula/cisco-packet-tracer-software.pdf). IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE EULA AND SEULA, THEN CISCO SYSTEMS, INC. ("CISCO") IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND YOU ARE NOT AUTHORIZED TO DOWNLOAD, INSTALL OR USE THE SOFTWARE.
I accept the agreement
I do not accept the agreement
Next >
Cancel

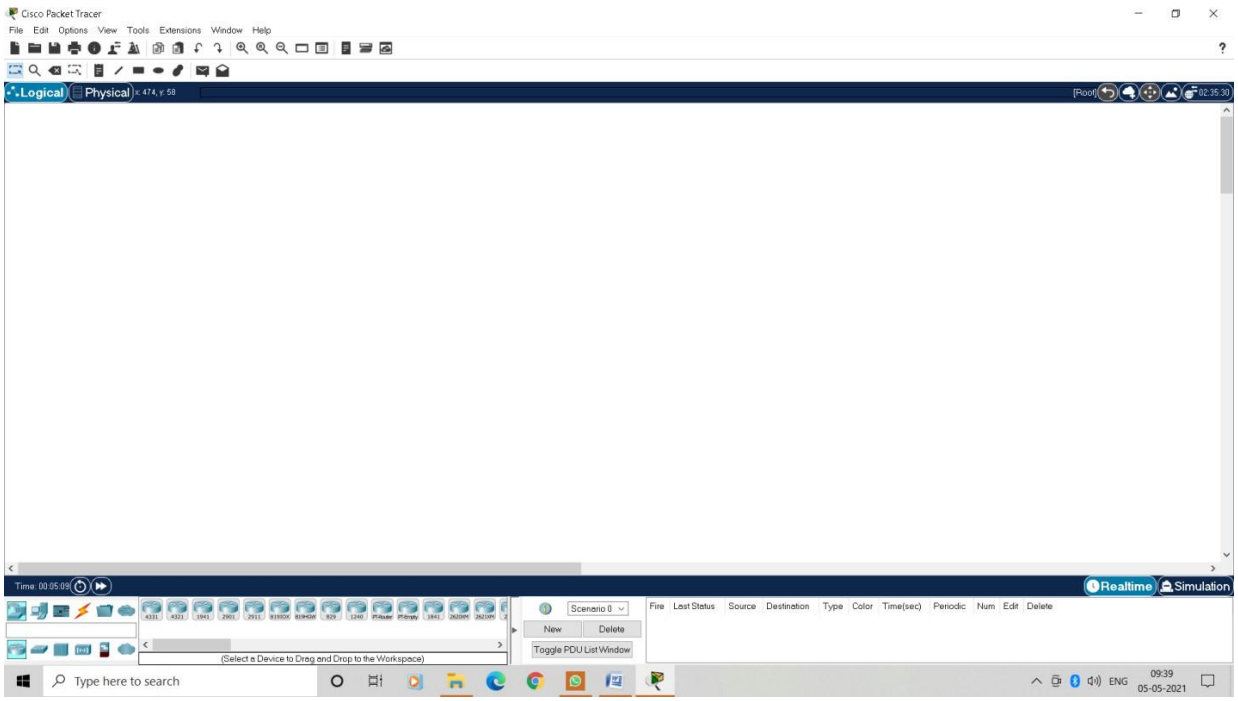

Setup - Cisco Packet Tracer 8.0 64Bit
Select Additional Tasks
Which additional tasks should be performed?
Select the additional tasks you would like Setup to perform while installing Cisco Packet Tracer 8.0 64Bit, then click Next.
Additional shortcuts:
Create a desktop shortcut
Create a Quick Launch shortcut
< Back
Next >
Cancel


Setup - Cisco Packet Tracer 8.0 64Bit
Ready to Install
Setup is now ready to begin installing Cisco Packet Tracer 8.0 64Bit on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files\Cisco Packet Tracer 8.0
Start Menu folder:
Cisco Packet Tracer
Additional tasks:
Additional shortcuts:
Create a desktop shortcut
< Back
Install
Cancel

Step 8 : After choosing operating system packet tracer will be downloaded .



After downloading the login page of cisco packet tracer



Program 7

Aim:- Study of various LAN topologies and their creation using network devices, cables and Computer.

Topology is derived from two Greek words topo and logy, where topo means 'place' and logy means 'study'. In computer networks, a topology is used to explain how a network is physically connected and the logical flow of information in the network. A topology mainly describes how devices are connected and interact with each other using communication links.

In computer networks, there are mainly two types of topologies, they are:

1. **Physical Topology:** A physical topology describes the way in which the computers or nodes are connected with each other in a computer network. It is the arrangement of various elements(link, nodes, etc.), including the device location and code installation of a computer network. In other words, we can say that it is the physical layout of nodes, workstations, and cables in the network**.**
2. **Logical Topology**: A logical topology describes the way, data flow from one computer to another. It is bound to a network protocol and defines how data is moved throughout the network and which path it takes. In other words, it is the way in which the devices communicate internally.

Network topology defines the layout, virtual shape, or structure of the network, not only physically but also logically. A network can have one physical topology and multiple logical topologies at the same time.

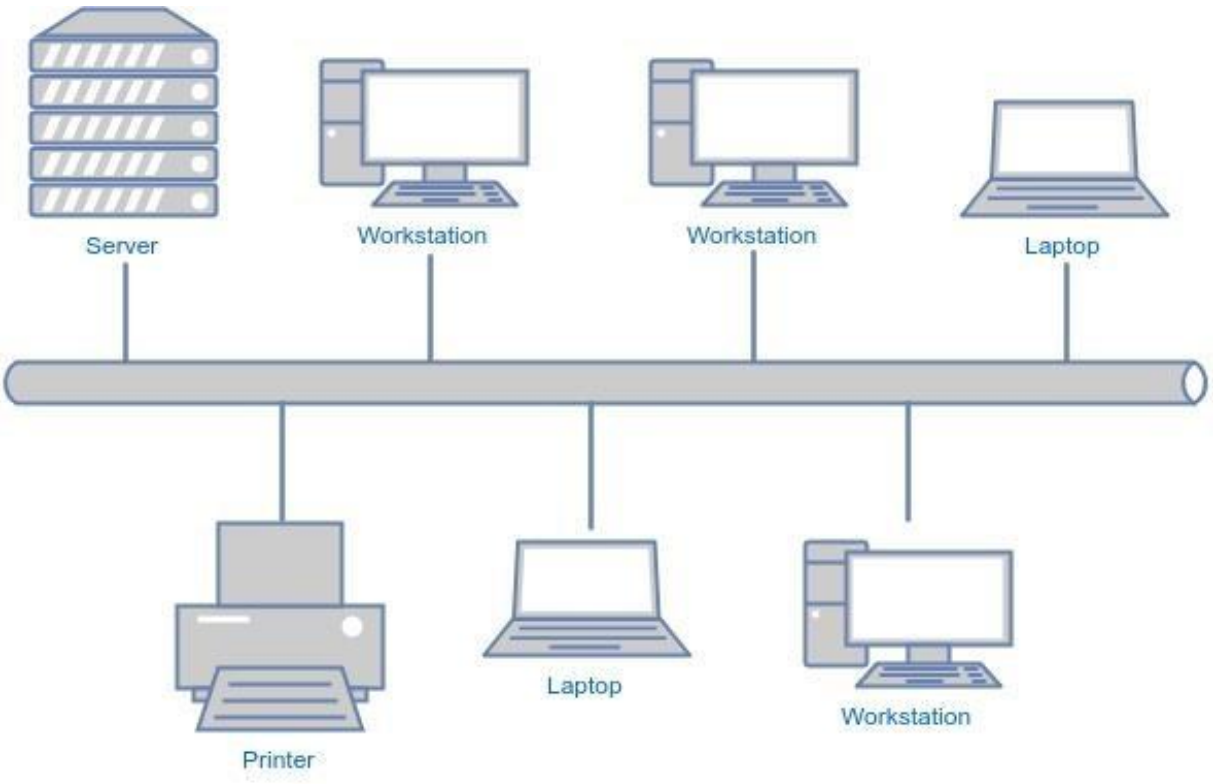
In a computer network, there are mainly six types of physical topology, they are:

1. **Bus Topology**
2. **Ring Topology**
3. **Star Topology**
4. **Mesh Topology**
5. **Tree Topology**
6. **Hybrid Topology**

1. Bus Topology:

Bus topology is the simplest kind of topology in which a common bus or channel is used for communication in the network. The bus is connected to various taps and droplines. Taps are the connectors, while droplines are the cables connecting the bus with the computer. In other words, there is only a single transmission line for all nodes.

In this topology, the bus acts as the backbone of the network, which joins every computer and peripherals in the network. Both ends of the shared channel have line terminators. The data is sent only in one direction and as soon as it reaches the end, the terminator removes the data from the communication line(to prevent signal bounce and data flow disruption).
In a bus topology, each computer communicates to another computer on the network independently. Every computer can share the network's total bus capabilities. The devices share the responsibility for the flow of data from one point to the other in the network.



Bus Topology

Following are the advantages of Bus topology:

1. Simple to use and install.
2. If a node fails, it will not affect other nodes.
3. Less cabling is required.
4. Cost-efficient to implement.

Following are the disadvantages of Bus topology:

1. Efficiency is less when nodes are more(strength of signal decreases).
2. If the bus fails, the network will fail.
3. A limited number of nodes can connect to the bus due to limited bus length.
4. Security issues and risks are more as messages are broadcasted to all nodes.
5. Congestion and traffic on the bus as it is the only source of communication.

2. Ring Topology :

Ring topology is a topology in which each computer is connected to exactly two other computers to form the ring. The message passing is unidirectional and circular in nature. This network topology is deterministic in nature, i.e., each computer is given access for transmission at a fixed time interval. All the nodes are connected in a closed-loop. This topology mainly works on a token-based system and the token travels in a loop in one specific direction.

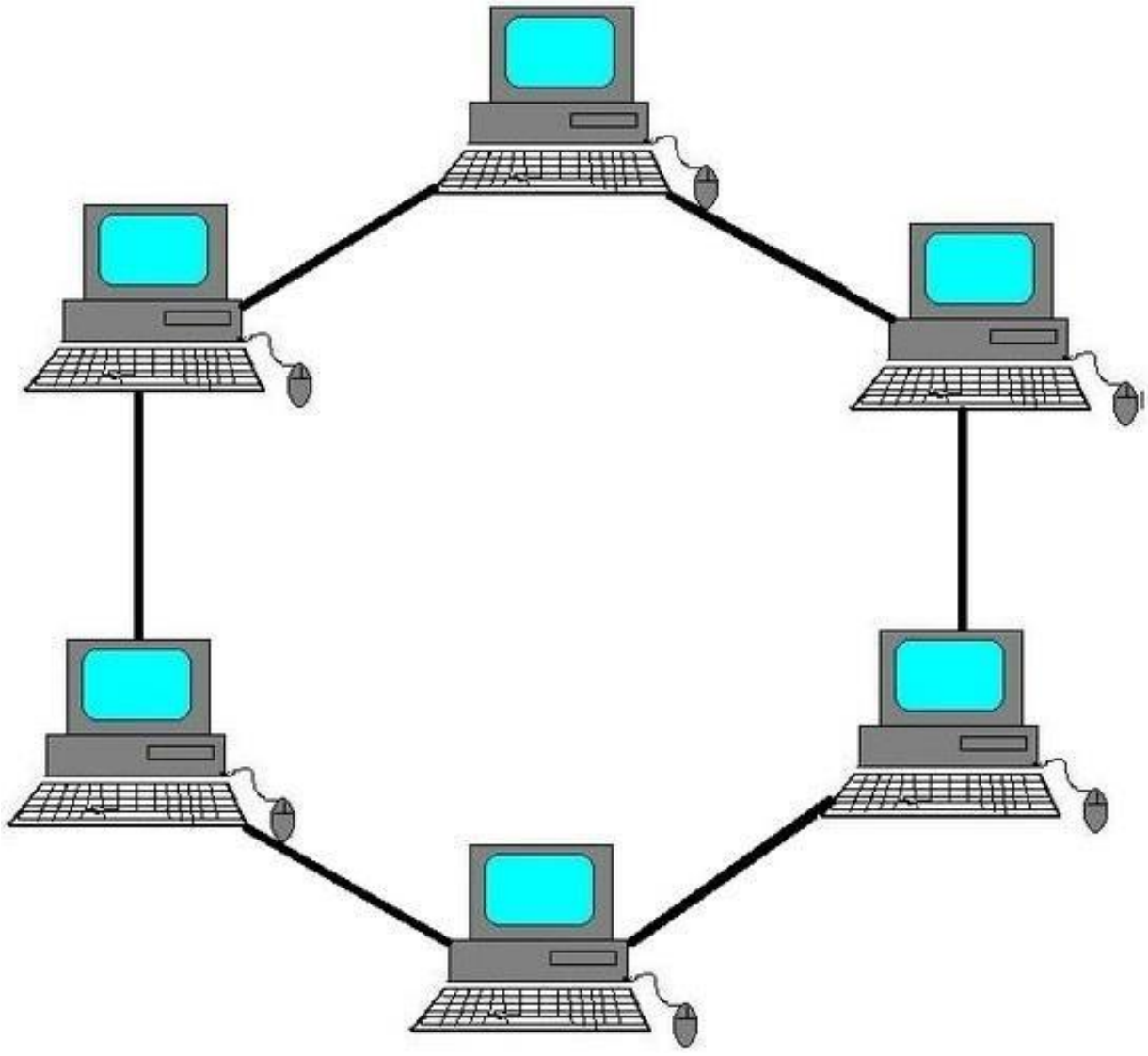
In a ring topology, if a token is free then the node can capture the token and attach the data and destination address to the token, and then leaves the token for communication. When this token reaches the destination node, the data is removed by the receiver and the token is made free to carry the next data.

Following are the advantages of Ring topology:

1. Easy Installation.
2. Less Cabling Required.
3. Reduces chances of data collision(unidirectional).
4. Easy to troubleshoot(the faulty node does not pass the token).
5. Each node gets the same access time.

Following are the disadvantages of Ring topology:

1. If a node fails, the whole network will fail.
2. Slow data transmission speed(each message has to go through the ring path).
3. Difficult to reconfigure(we have to break the ring).

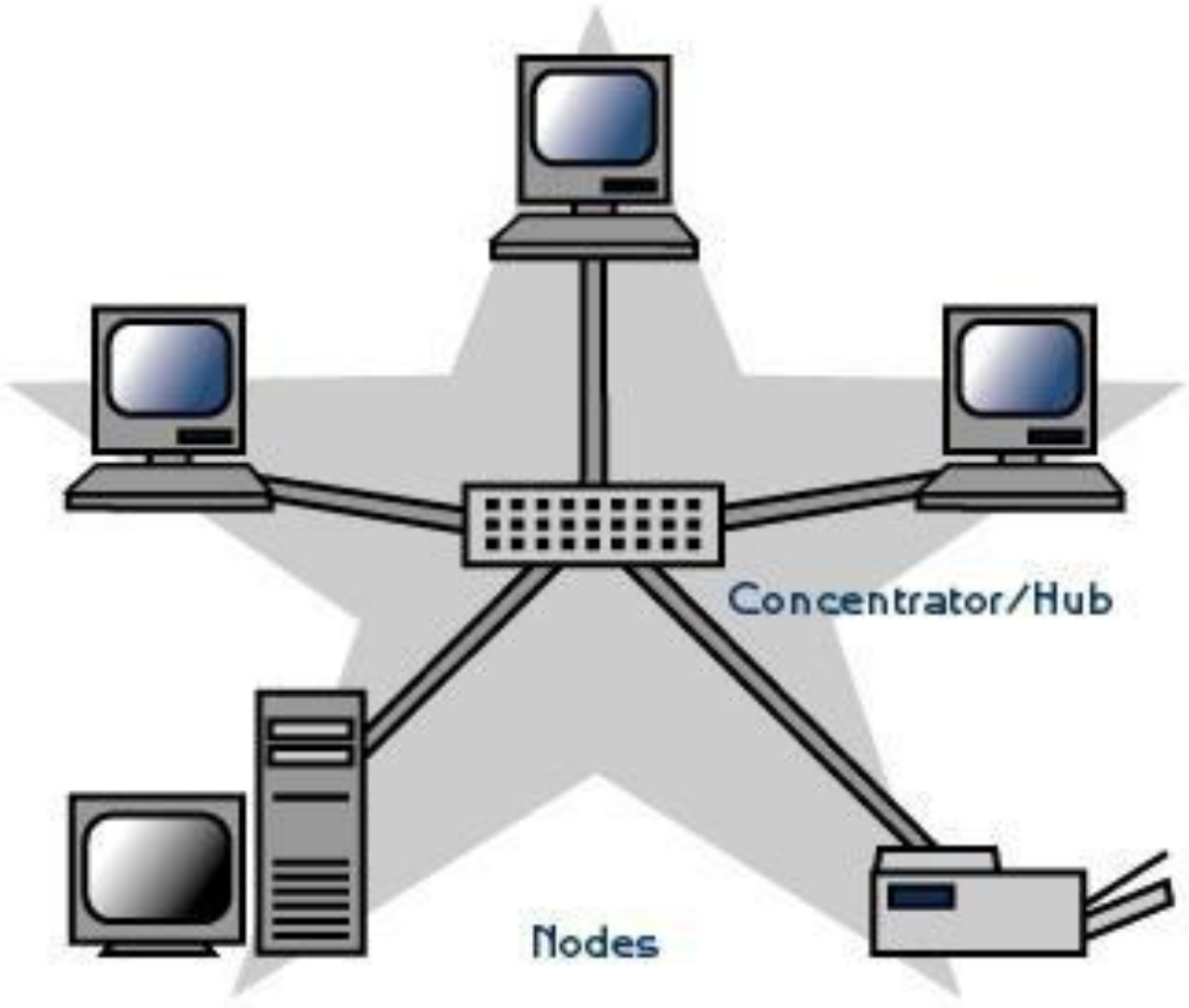


Ring Topology

3.Star Topology :

Star topology is a computer network topology in which all the nodes are connected to a centralized hub. The hub or switch acts as a middleware between the nodes. Any node requesting for service or providing service, first contact the hub for communication. The central device(hub or switch) has point to point communication link(the dedicated link between the devices which can not be accessed by some other computer) with the devices. The central device then broadcast or unicast the message based on the central device used. The hub broadcasts the message, while the switch unicasts the messages by maintaining a switch table. Broadcasting increases unnecessary data traffic in the network.

In a star topology, hub and switch act as a server, and the other connected devices act as clients. Only one input-output port and one cable are required to connect a node to the central device. This topology is better in terms of security because the data does not pass through every node.



Star Topology

Following are the advantages of Star topology:

1. Centralized control.
2. Less Expensive.
3. Easy to troubleshoot(the faulty node does not give response).
4. Good fault tolerance due to centralized control on nodes.
5. Easy to scale(nodes can be added or removed to the network easily).
6. If a node fails, it will not affect other nodes.
7. Easy to reconfigure and upgrade(configured using a central device).

Following are the disadvantages of Star topology:

1. If the central device fails, the network will fail.
2. The number of devices in the network is limited(due to limited input-output port in a central device).

4.Mesh Topology :

Mesh topology is a computer network topology in which nodes are interconnected with each other. In other words, direct communication takes place between the nodes in the network.

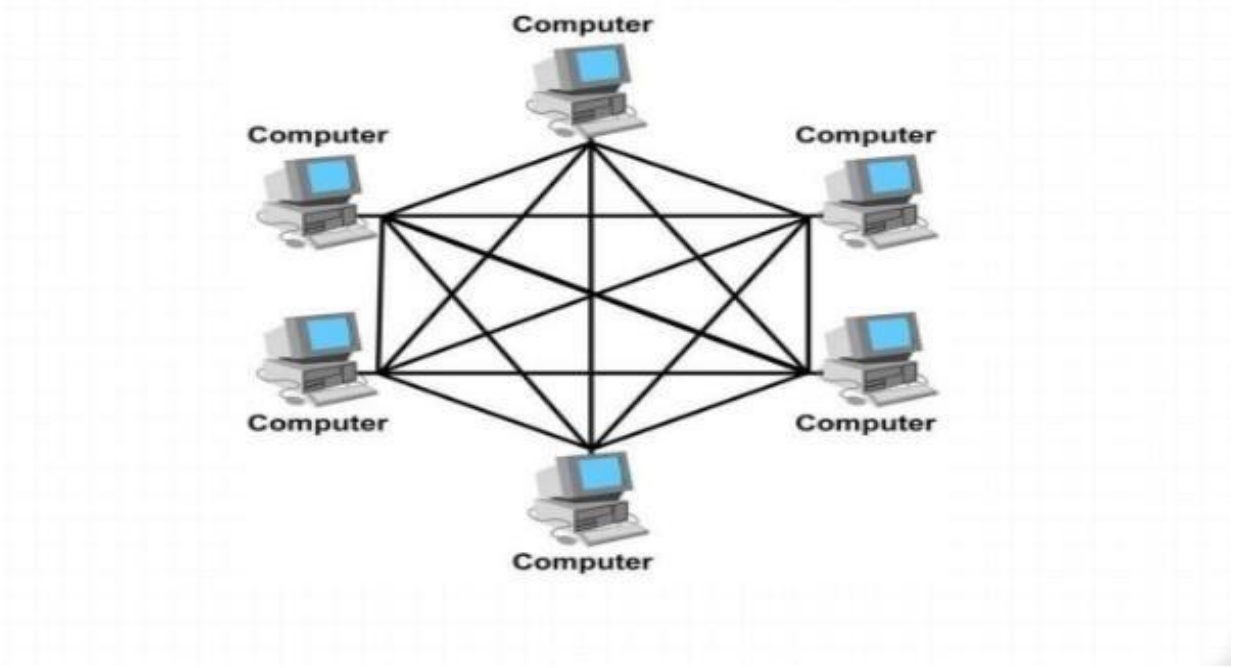
There are mainly two types of Mesh:

4 a). Full Mesh:

In which each node is connected to every other node in the network. In a fully connected mesh topology, each device has a point to point link with every other device in the network. If there are 'n' devices in the network, then each device has exactly '(n-1)' input-output ports and communication links. These links are simplex links, i.e., the data moves only in one direction. A duplex link(in which data can travel in both the directions simultaneously) can replace two simplex links. If we are using simplex links, then the number of communication links will be 'n(n-1)' for 'n' devices, while it is 'n(n-1)/2' if we are using duplex links in the mesh topology.

4 b). Partial Mesh:

In which, some nodes are not connected to every node in the network.



Mesh Topology

Following are the advantages of Mesh topology:

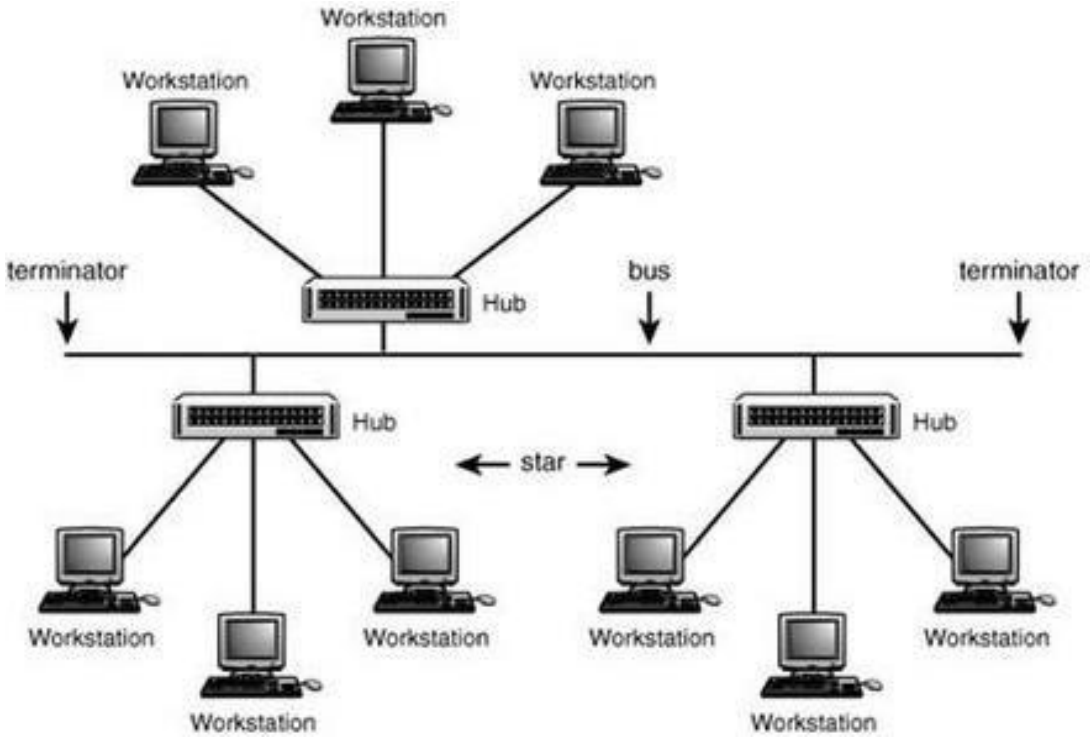
1. Dedicated links facilitate direct communication.
2. No congestion or traffic problems on the channels.
3. Good Fault tolerance due to the dedicated path for each node.
4. Very fast communication.
5. Maintains privacy and security due to a separate channel for communication.
6. If a node fails, other alternatives are present in the network.

Following are the disadvantages of Mesh topology:

1. Very high cabling required.
2. Cost inefficient to implement.
3. Complex to implement and takes large space to install the network.
4. Installation and maintenance are very difficult.

5. Tree Topology:

Tree topology is a computer network topology in which all the nodes are directly or indirectly connected to the main bus cable. Tree topology is a combination of Bus and Star topology. In a tree topology, the whole network is divided into segments, which can be easily managed and maintained. There is a main hub and all the other sub-hubs are connected to each other in this topology.



Tree Topology

Following are the advantages of Tree topology:

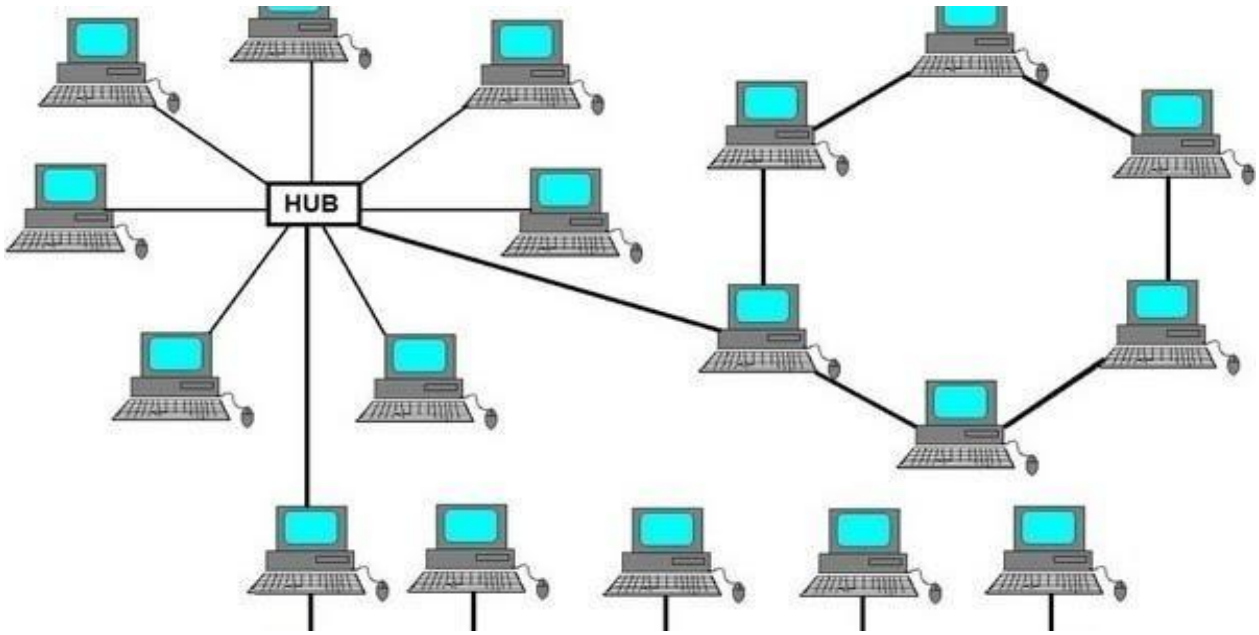
1. Large distance network coverage.
2. Fault finding is easy by checking each hierarchy.
3. Least or no data loss.
4. A Large number of nodes can be connected directly or indirectly.
5. Other hierarchical networks are not affected if one of them fails.

Following are the disadvantages of Tree topology:

1. Cabling and hardware cost is high.
2. Complex to implement.
3. Hub cabling is also required.
4. A large network using tree topology is hard to manage.
5. It requires very high maintenance.
6. If the main bus fails, the network will fail.

6. Hybrid Topology:

A Hybrid topology is a computer topology which is a combination of two or more topologies. In practical use, they are the most widely used.
In this topology, all topologies are interconnected according to the needs to form a hybrid. All the good features of each topology can be used to make an efficient hybrid topology.



Hybrid Topology

Following are the advantages of Hybrid topology:

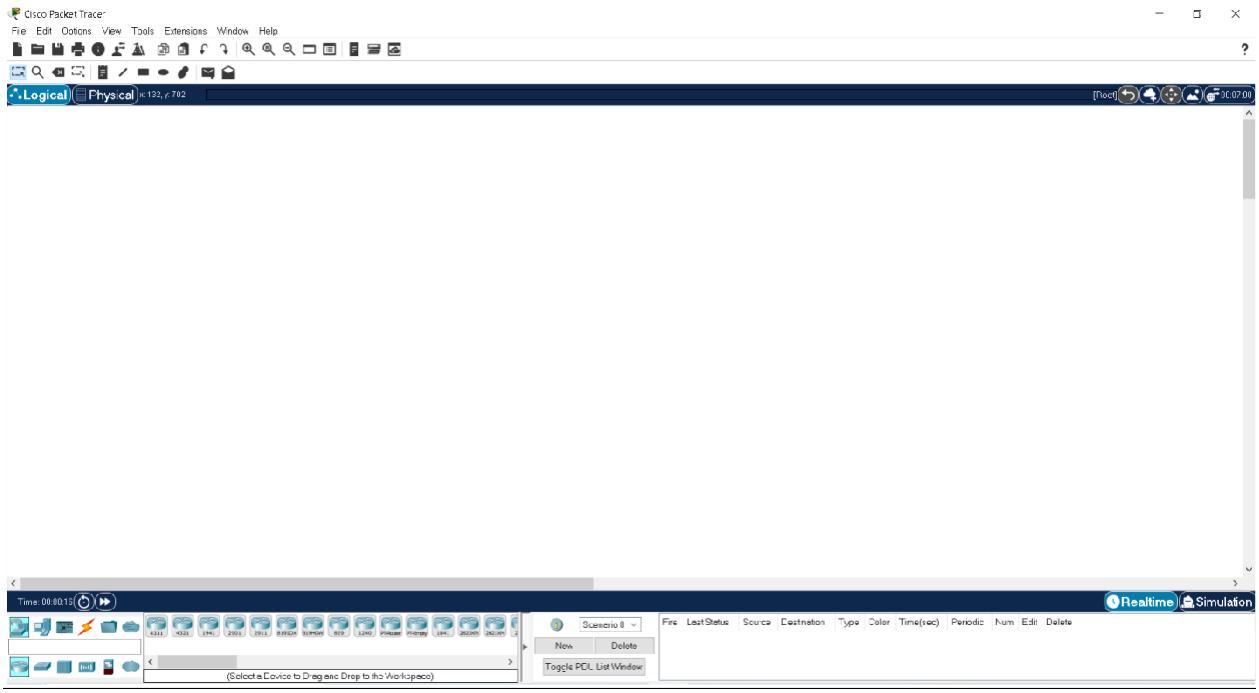
1. It can handle a large volume of nodes.
2. It provides flexibility to modify the network according to our needs.
3. Very Reliable(if one node fails it will not affect the whole network).

Following are the disadvantages of Hybrid topology:

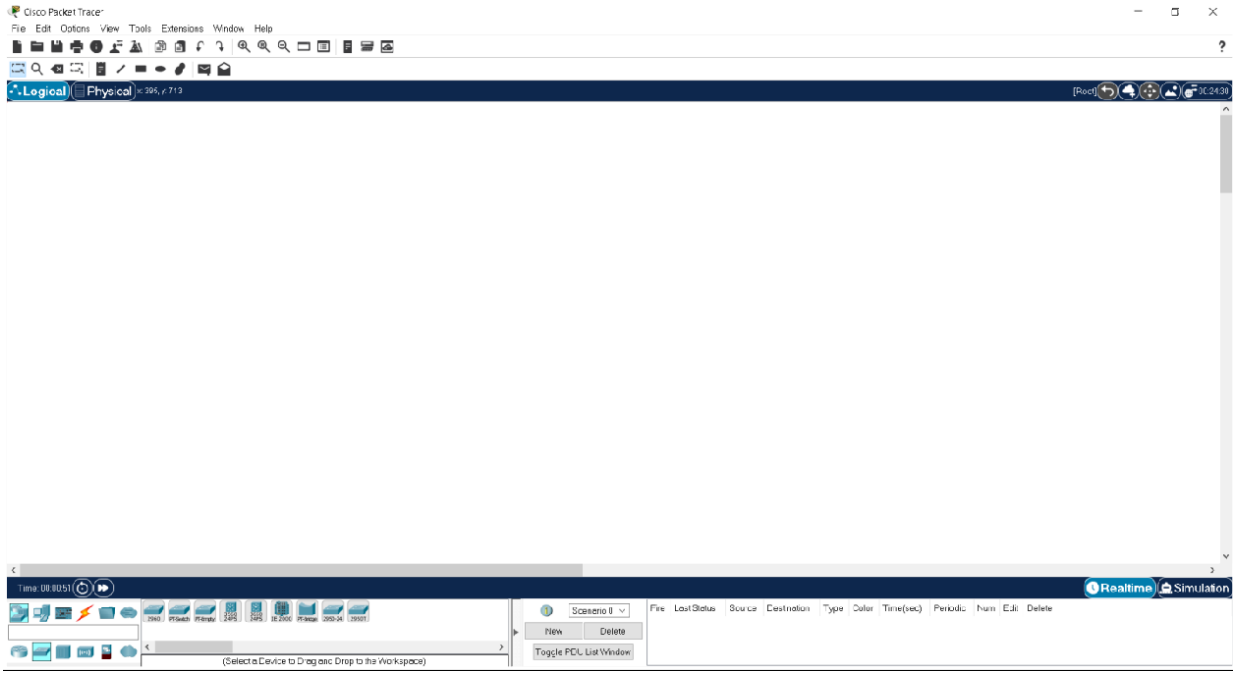
1. Complex design.
2. Expensive to implement.
3. Multi-Station Access Unit(MSAL) required.
4. Hence, after learning the various computer network topologies, we can conclude that some points need to be considered when selecting a physical topology:
5. Ease of Installation.
6. Fault Tolerance.
7. Implementation Cost.
8. Cabling Required.
9. Maintenance Required.
10. Reliable Nature.
11. Ease of Reconfiguration and upgradation.

➔Demonstration of a star topology by using cisco packet tracer

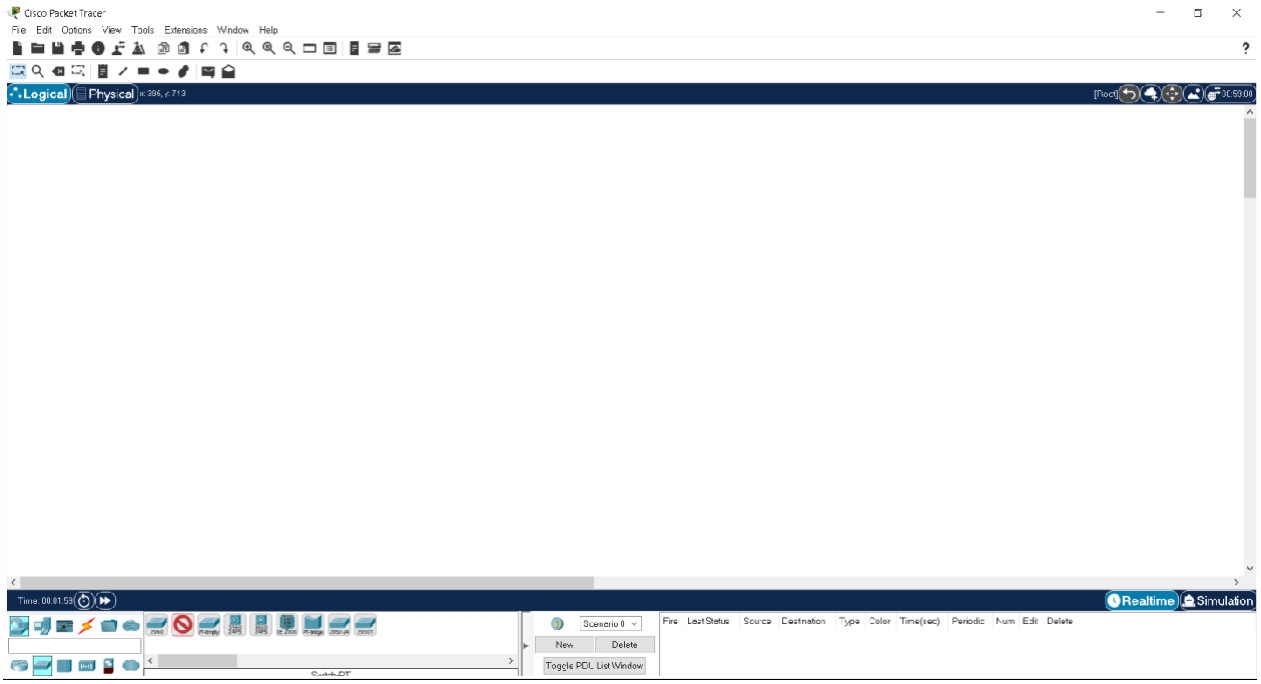
STEP 1: Open cisco packet tracer and choose SWITCH PT with name SWITCH0.



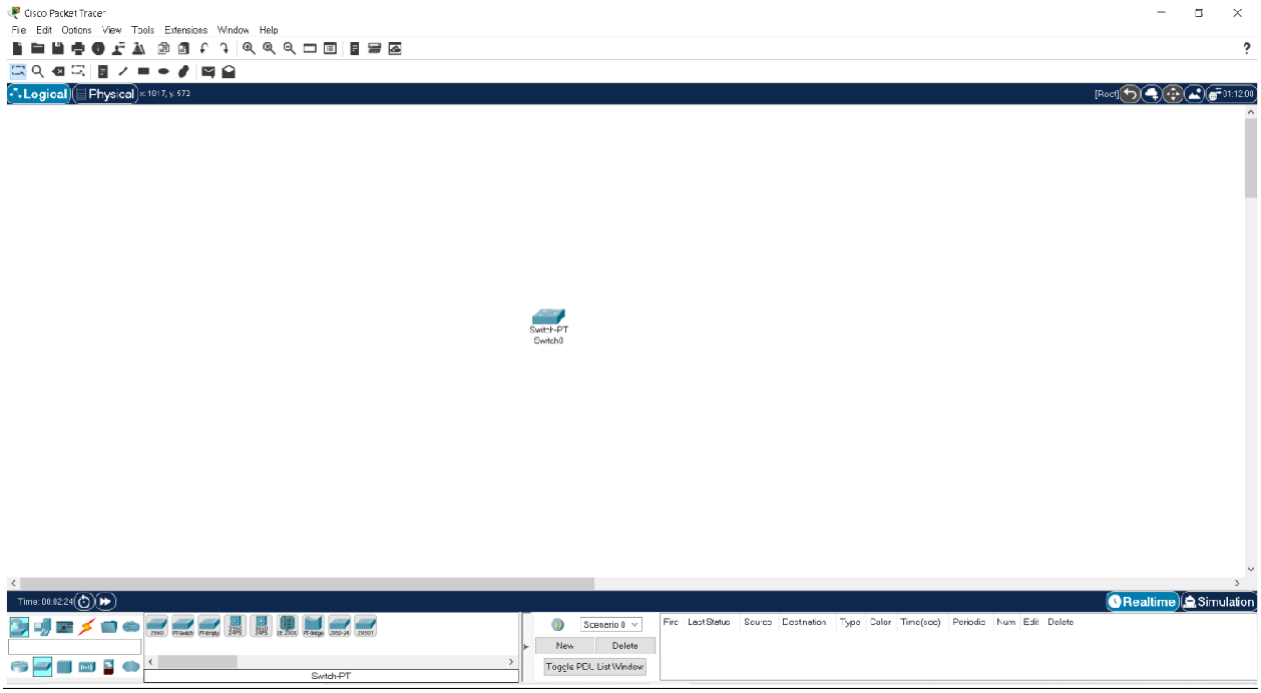
Click on switch option.



Choose SWITCH PT.

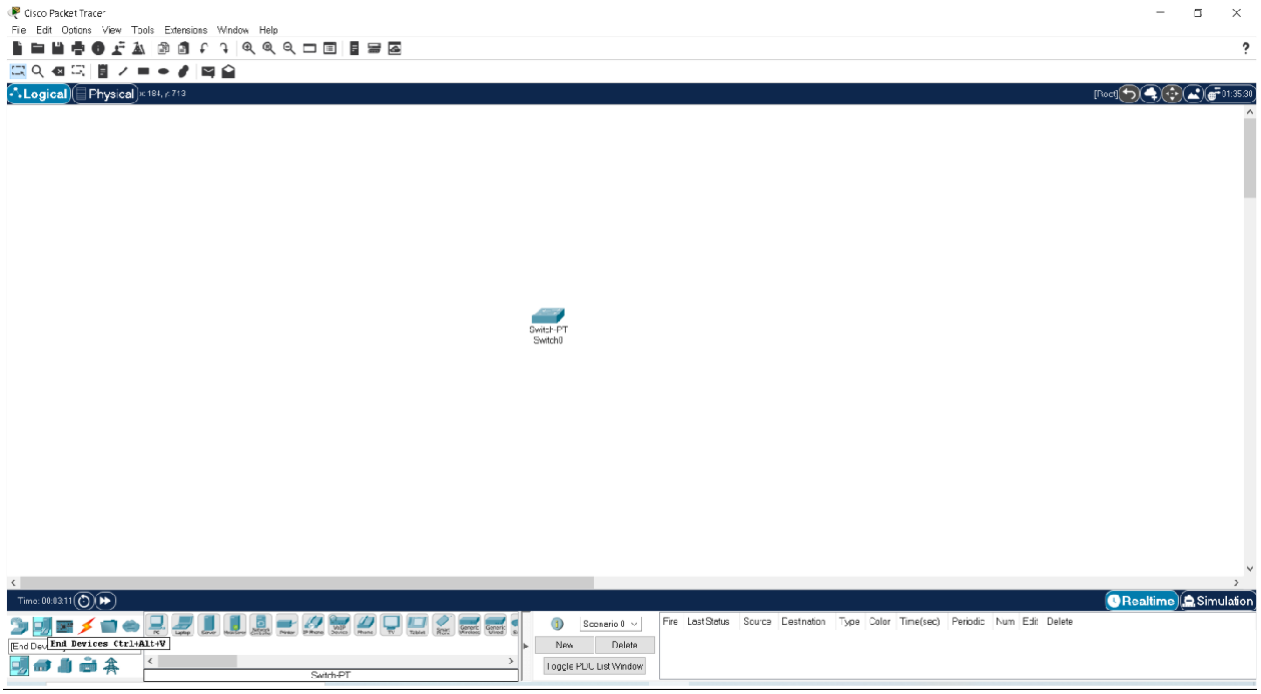


Click on SWITCH PT.

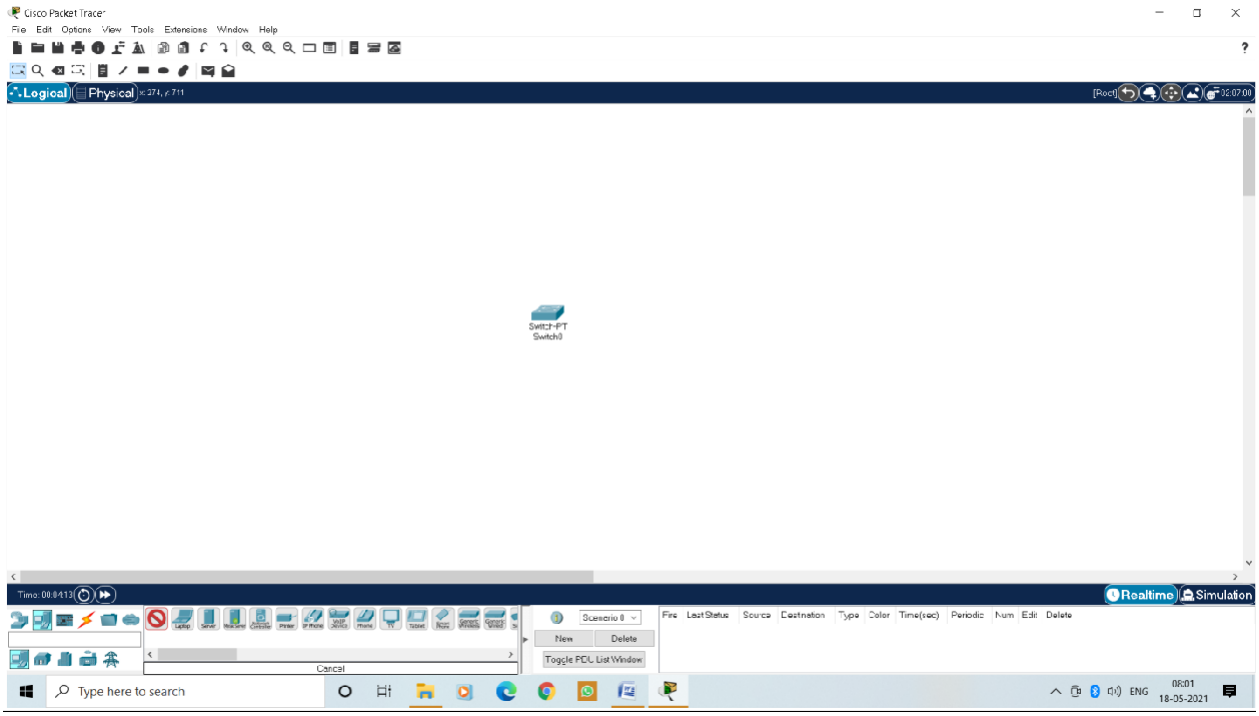


SWITCH PT is selected with name SWITCH 0.

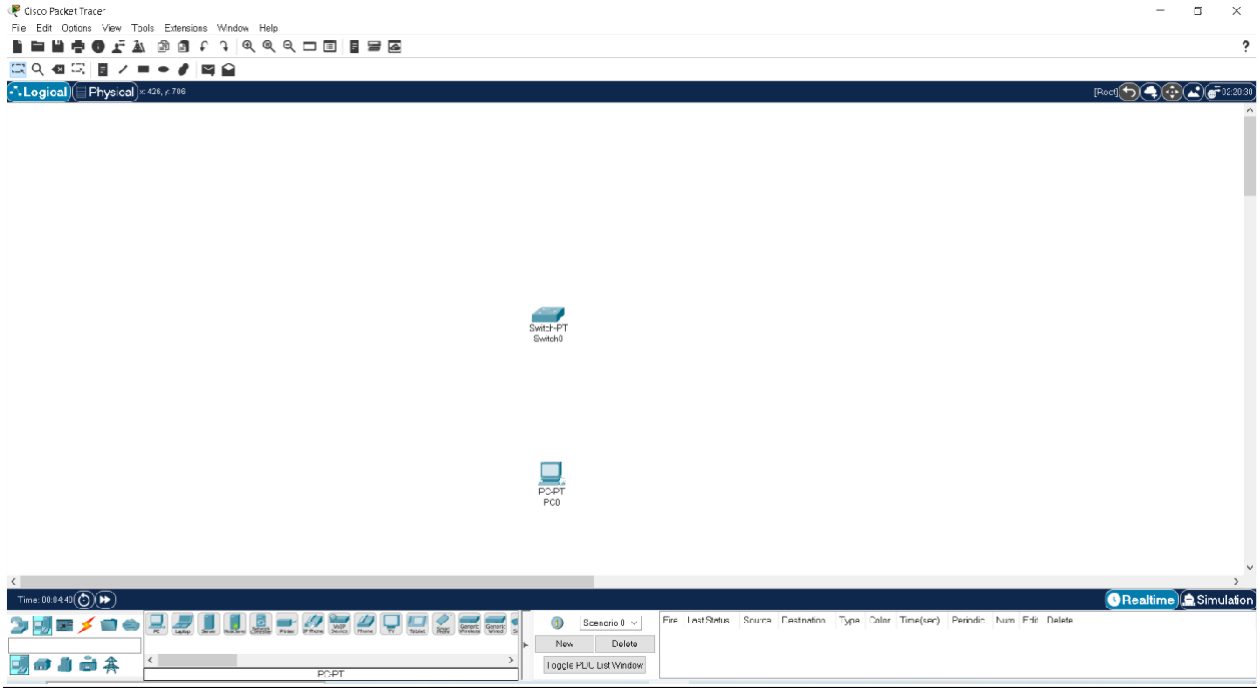
STEP 2 : Now click on end diveces and add PCs .



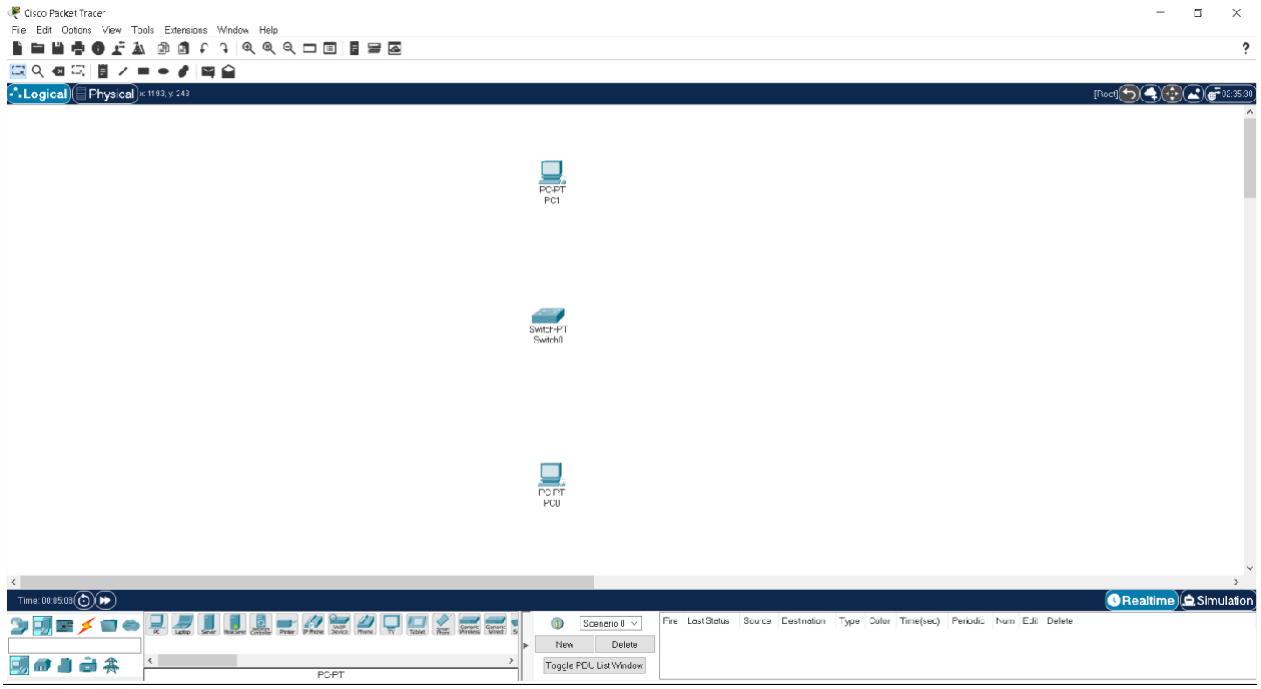
Clicking on end devices.



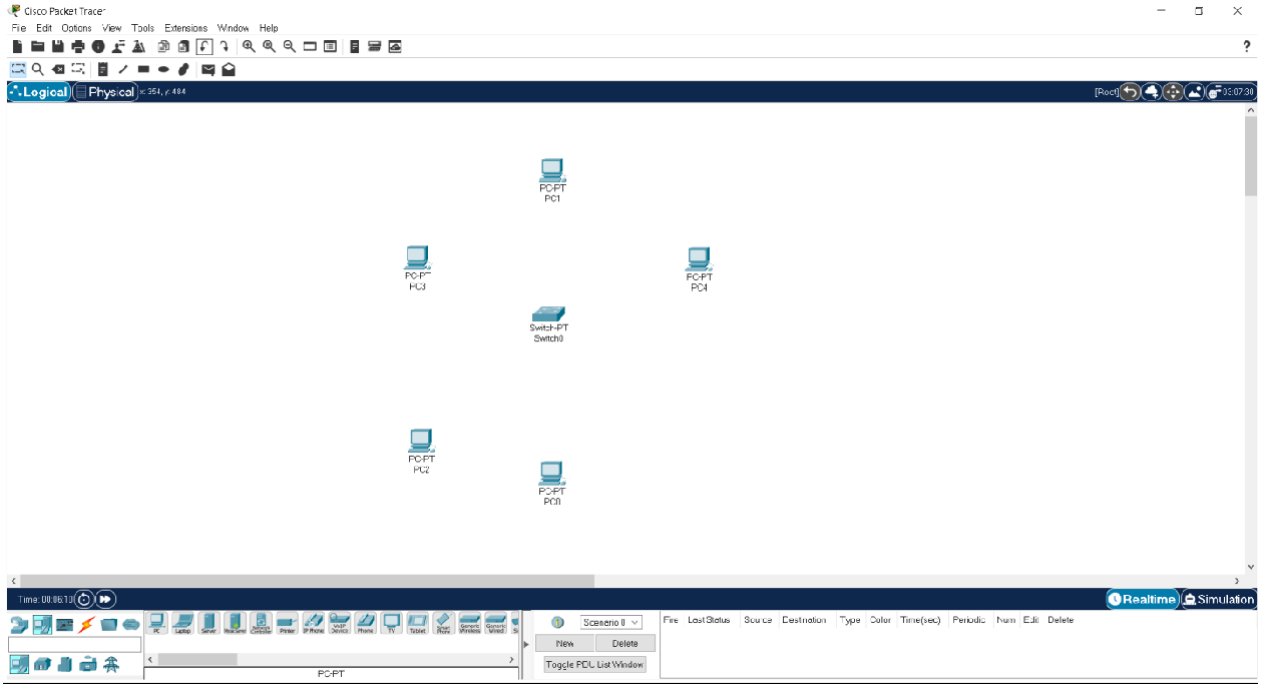
Choose PC as end devices.



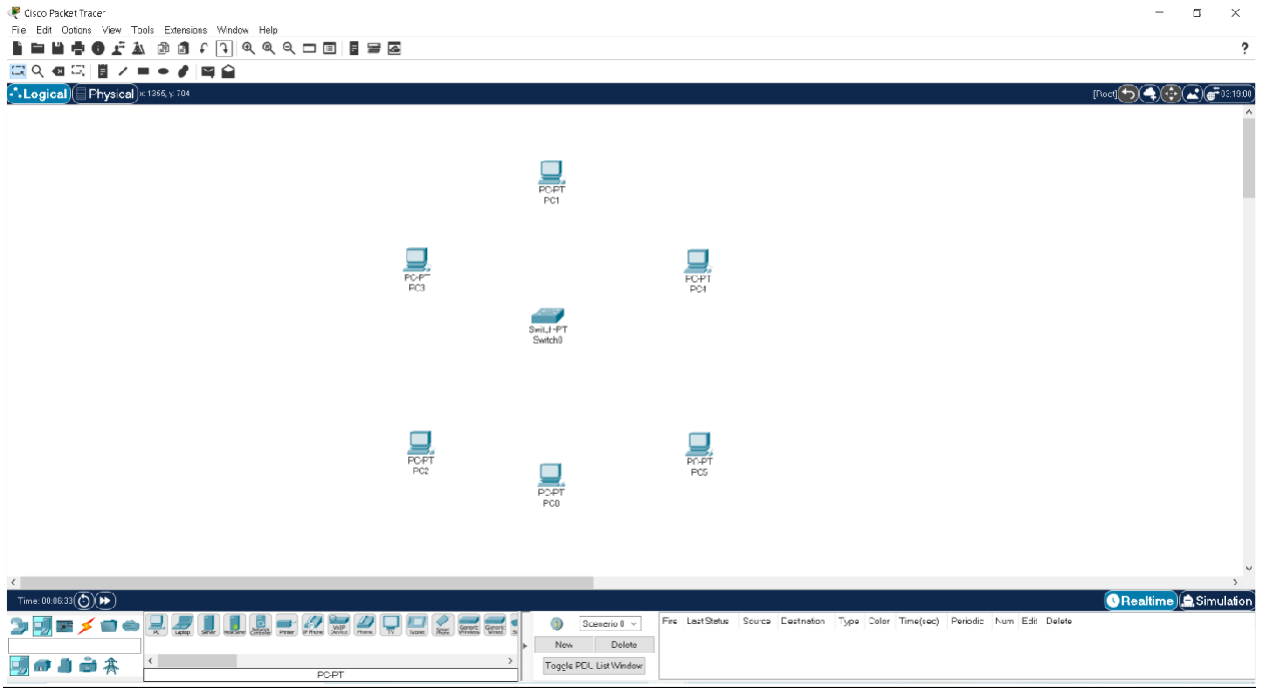
First PC selected.



Second PC selected.

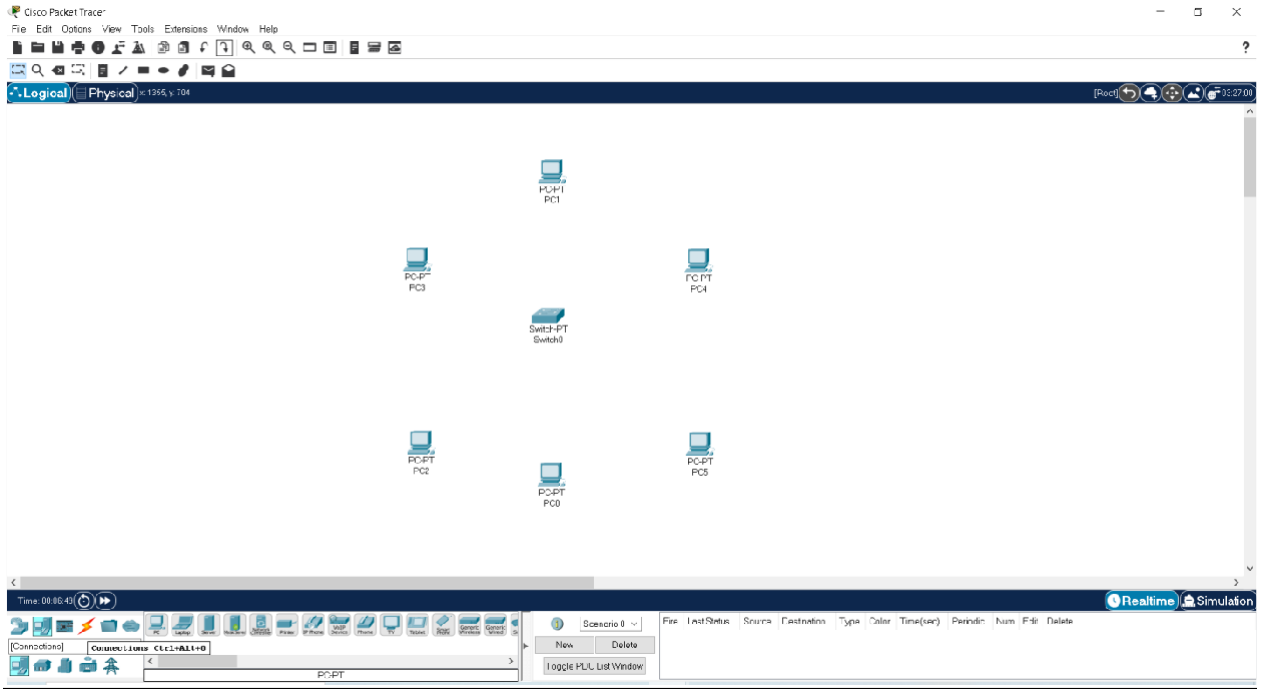


Four PCs are selected.

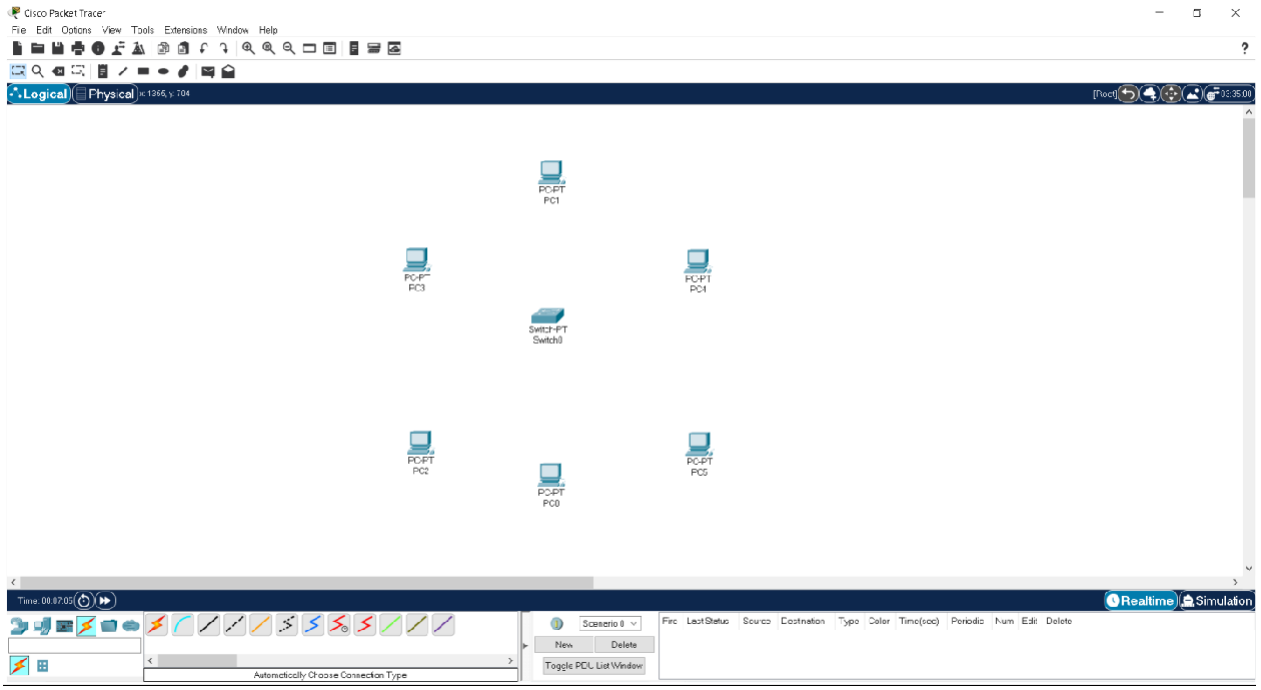


All required PCs are selected and placed in STAR shape.

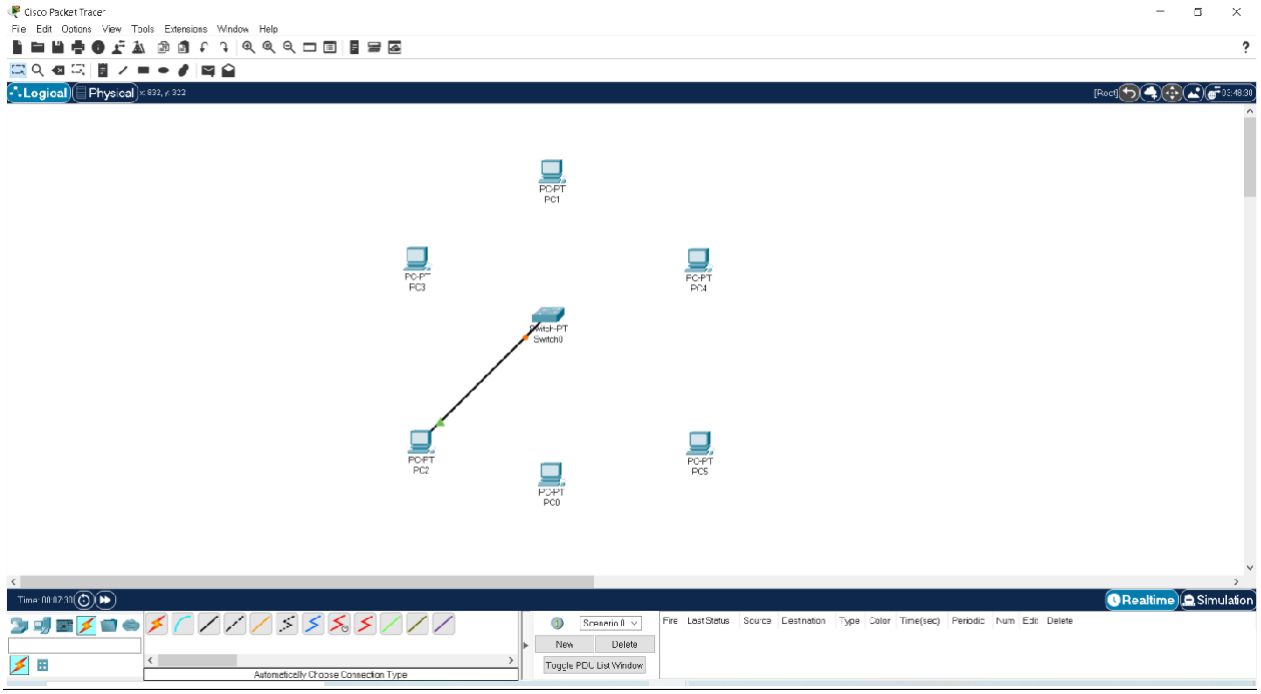
STEP 3 : Click on automatic connection type and connect all the PCs to SWITCH 0.



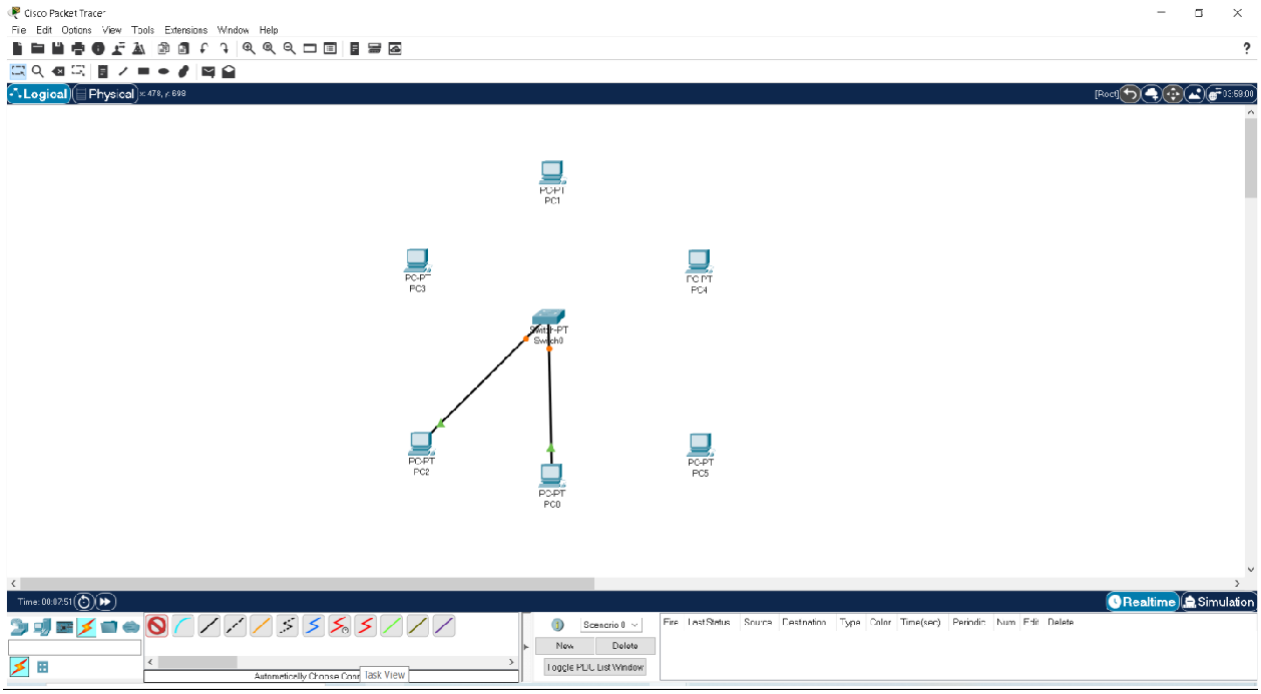
Clicking on connection.



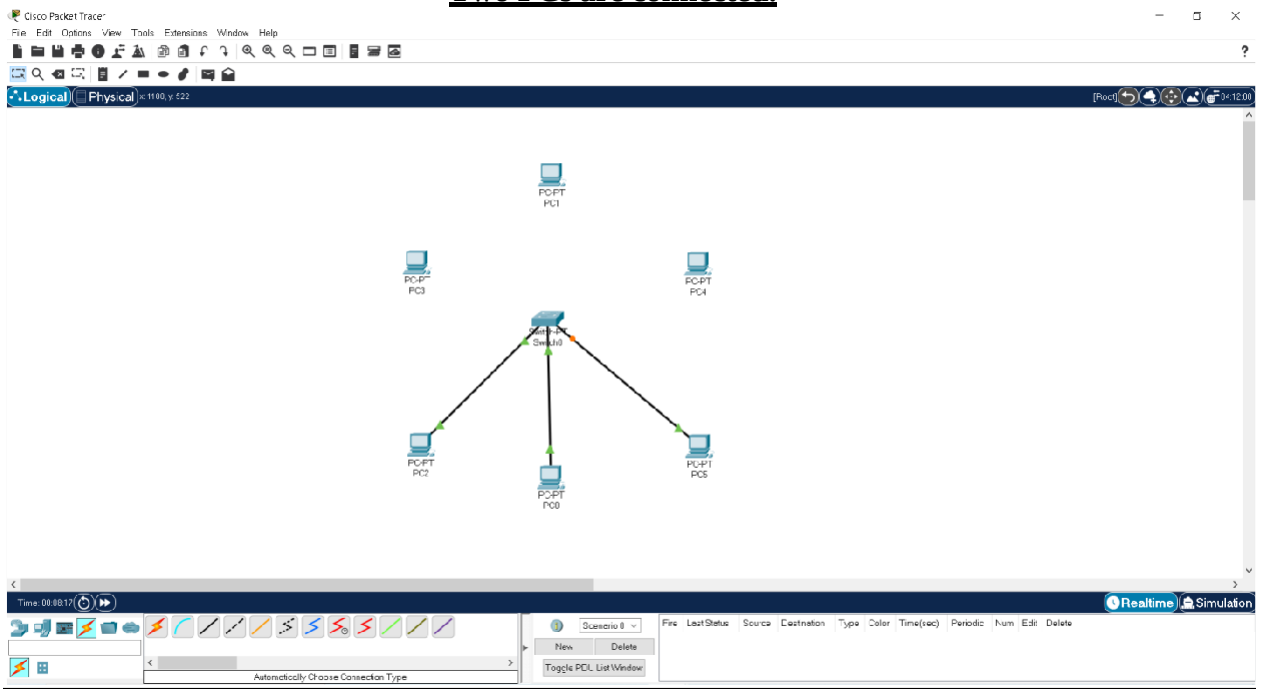
Choosing automatic connection type.



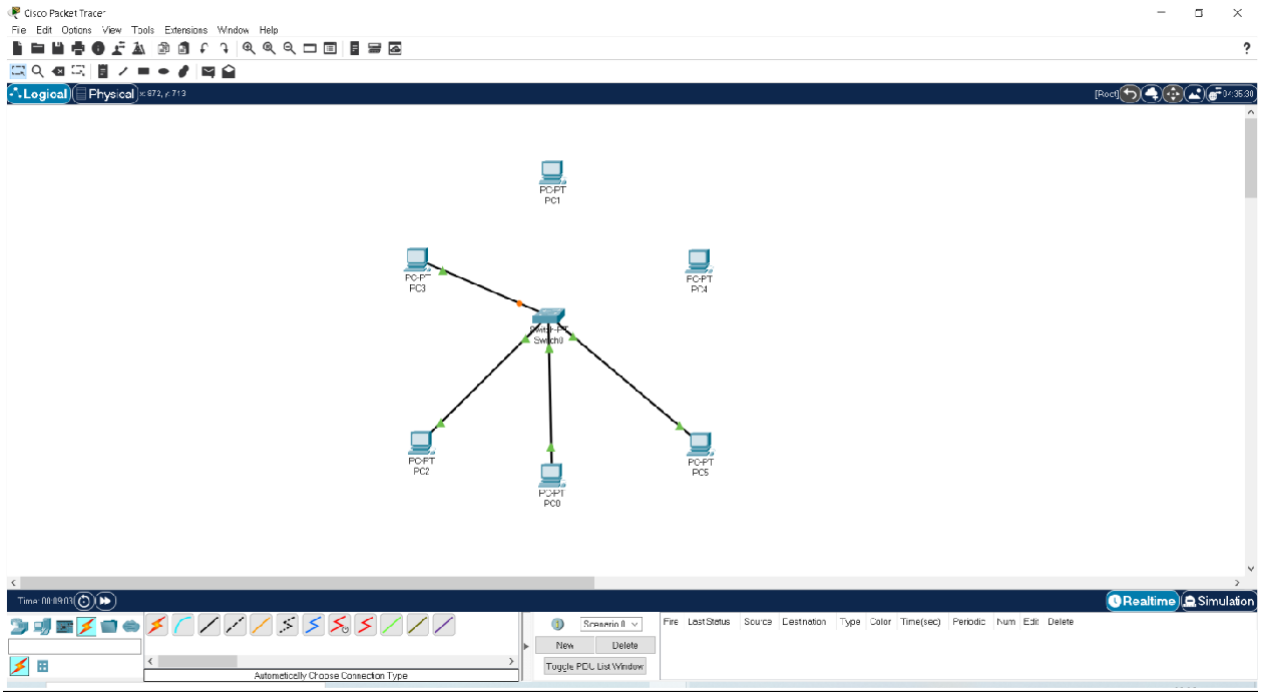
One PC is connected.



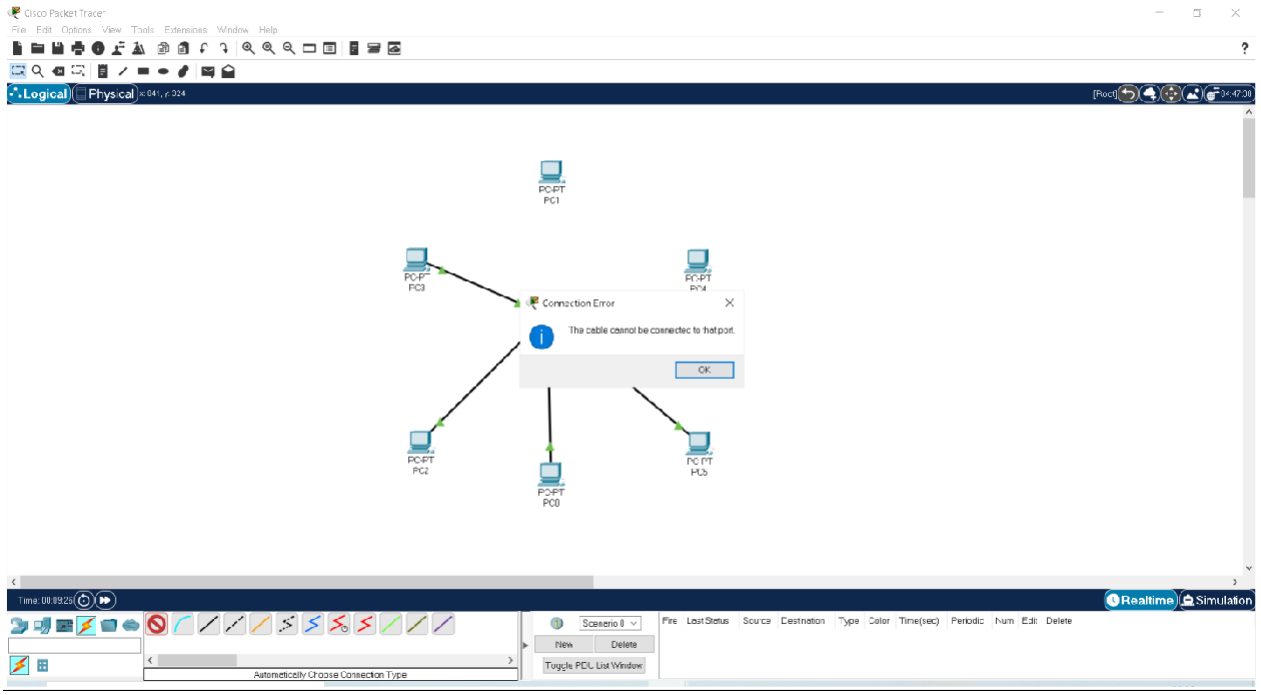
Two PCs are connected.



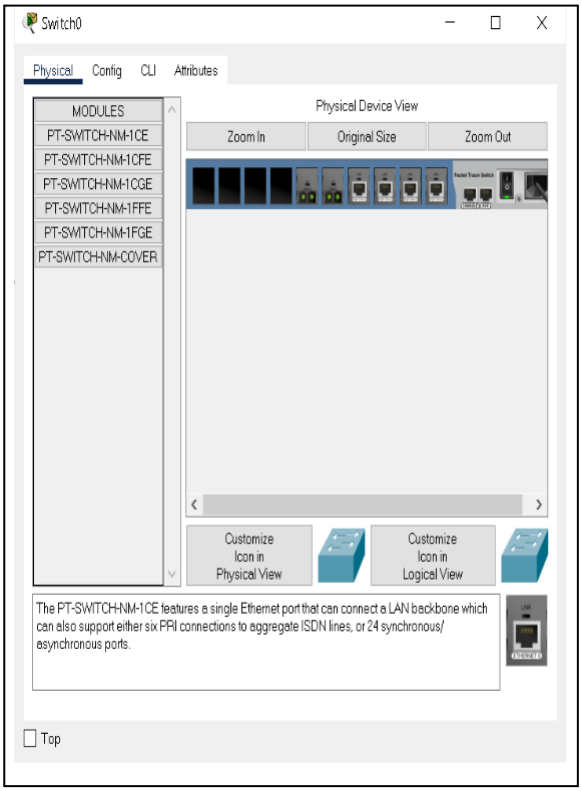
Three PCs are connected.



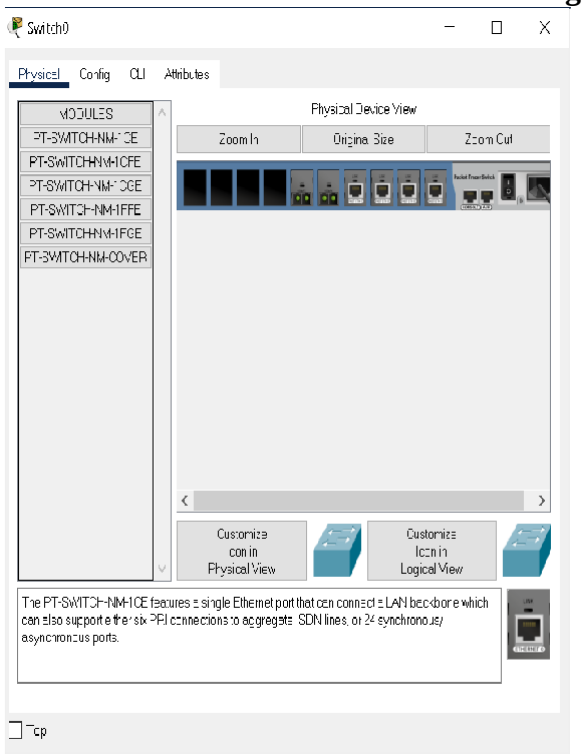
Four PCs are connected.



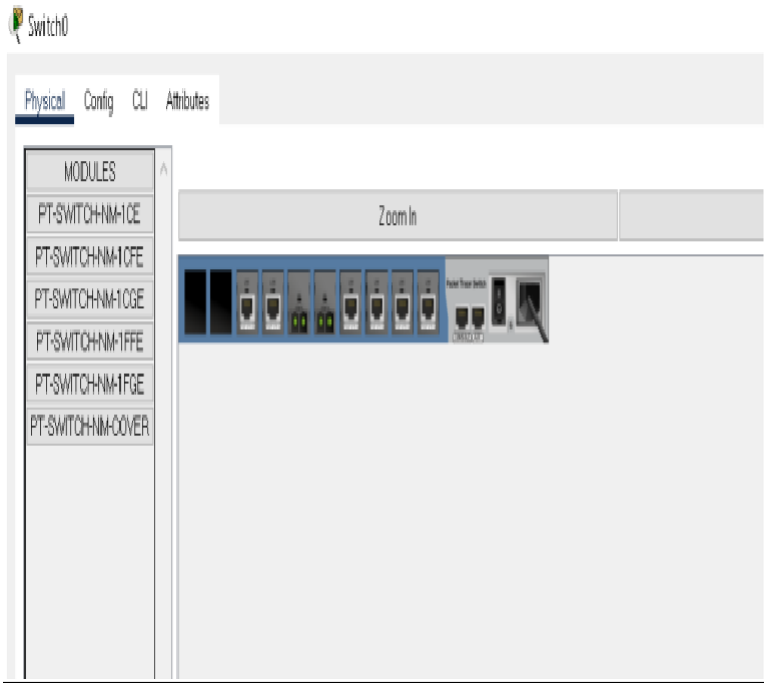
In 5th PC (PC4) connection there will show an error as shown in above picture.
To resolve above error we click on switch PT (SWITCH 0) as shown below then it shows there are only 4 ports are available in SWITCH 0 . Now we need 2 more ports to make a star topology and connecting rest 2 PCs (PC4 & PC5).



STEP 4: Now to add 2 more ports in SWITCH 0 , first power off the SWITCH 0 then click on PT SWITCH-NM-1CFE and drag to Zoom in Options as shown below.

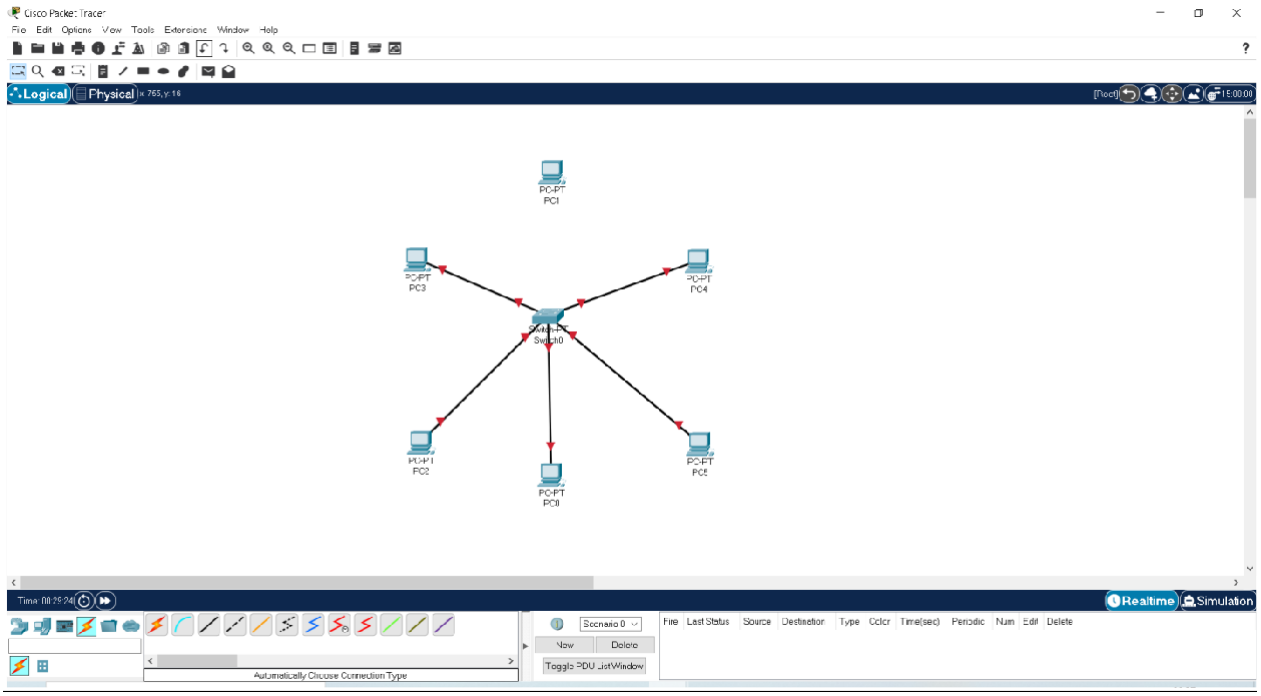


POWER OFF SWITCH 0

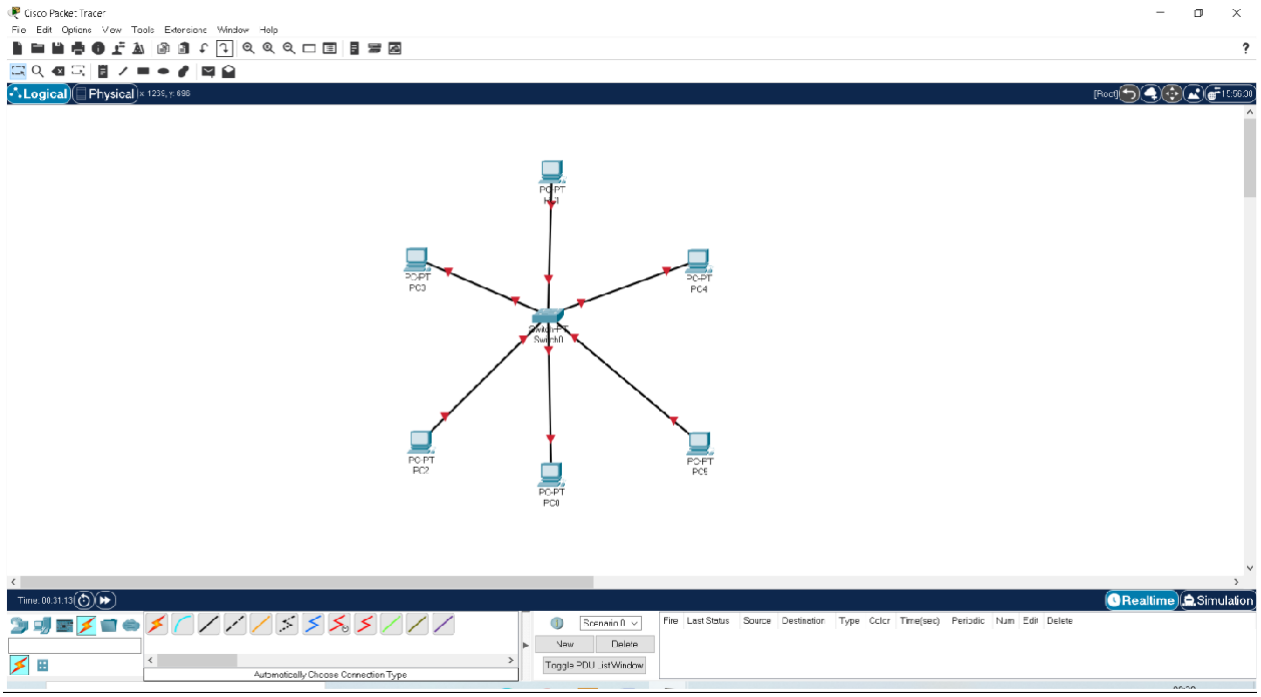


After adding 2 more ports

STEP 5: Now we connect the rest of two PCs (PC4 & PC5) as we connect previous PCs in STEP3 .

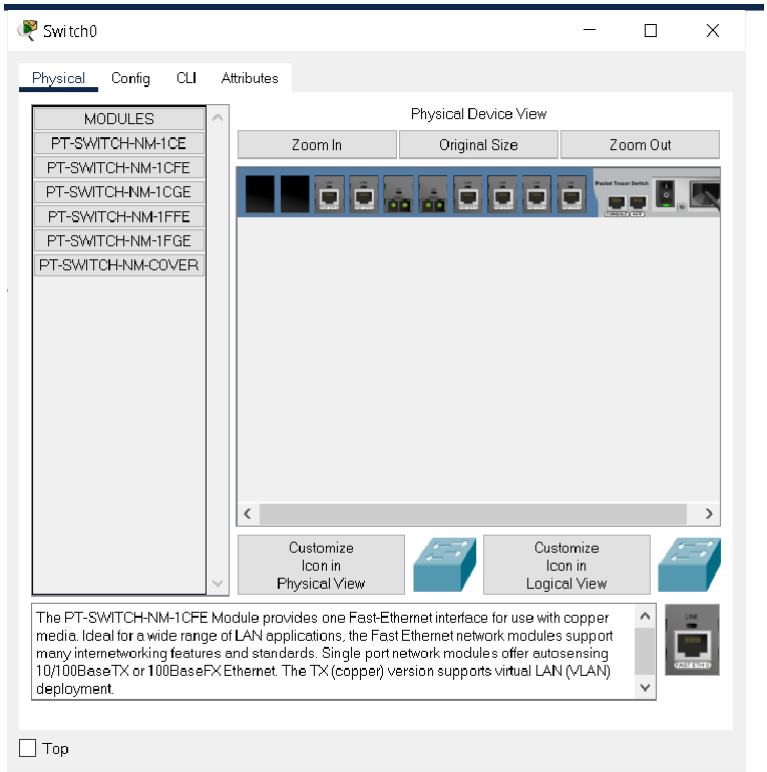


PC4 Connected.

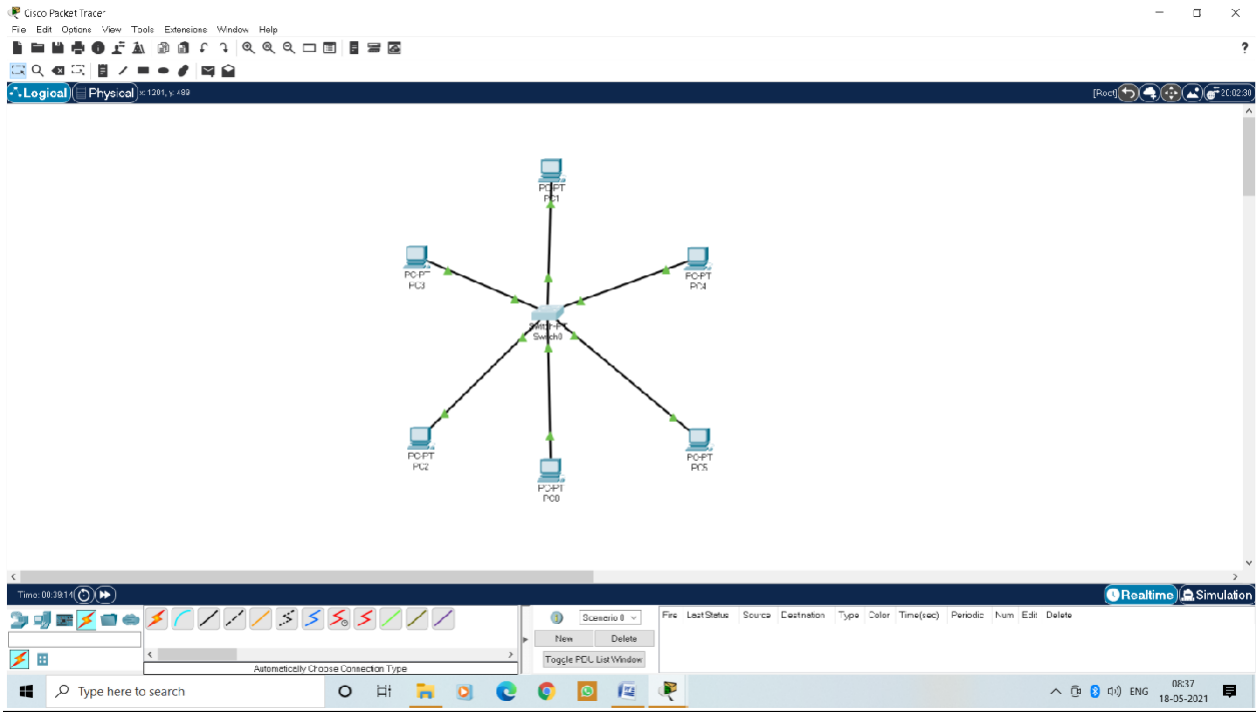


PC5 Connected.

STEP 6 : Now , power on the SWITCH 0 to check topology is working or not.

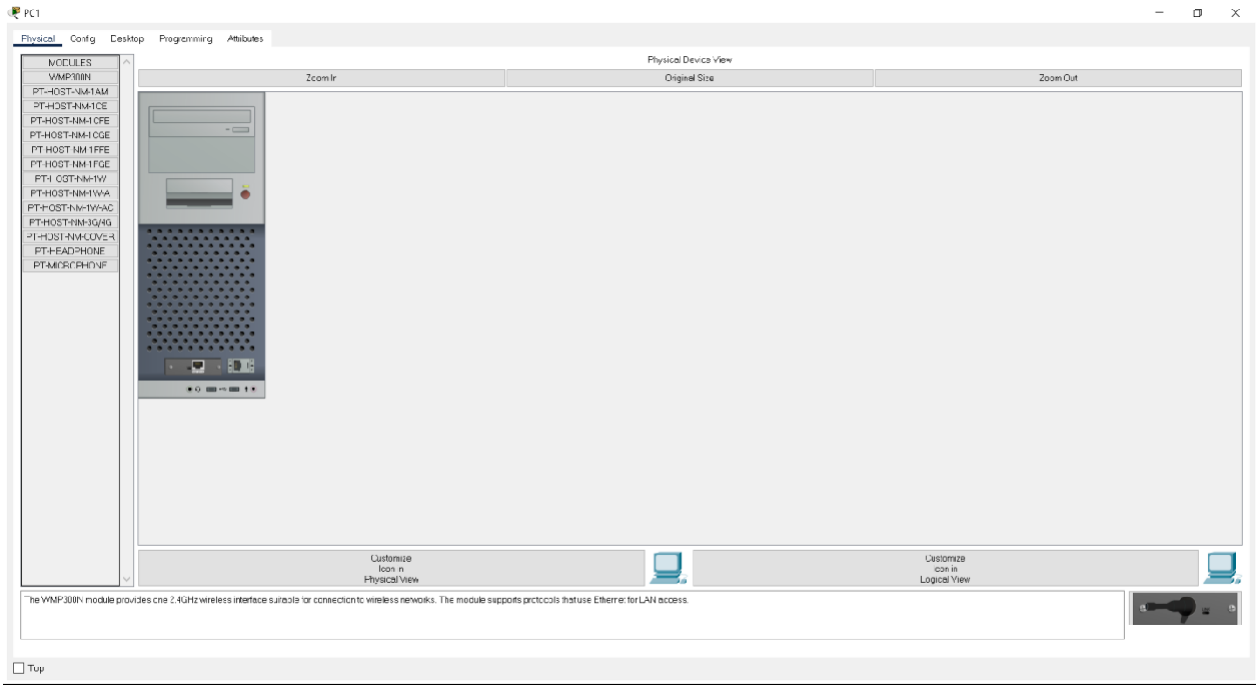


POWER ON SWITCH 0.

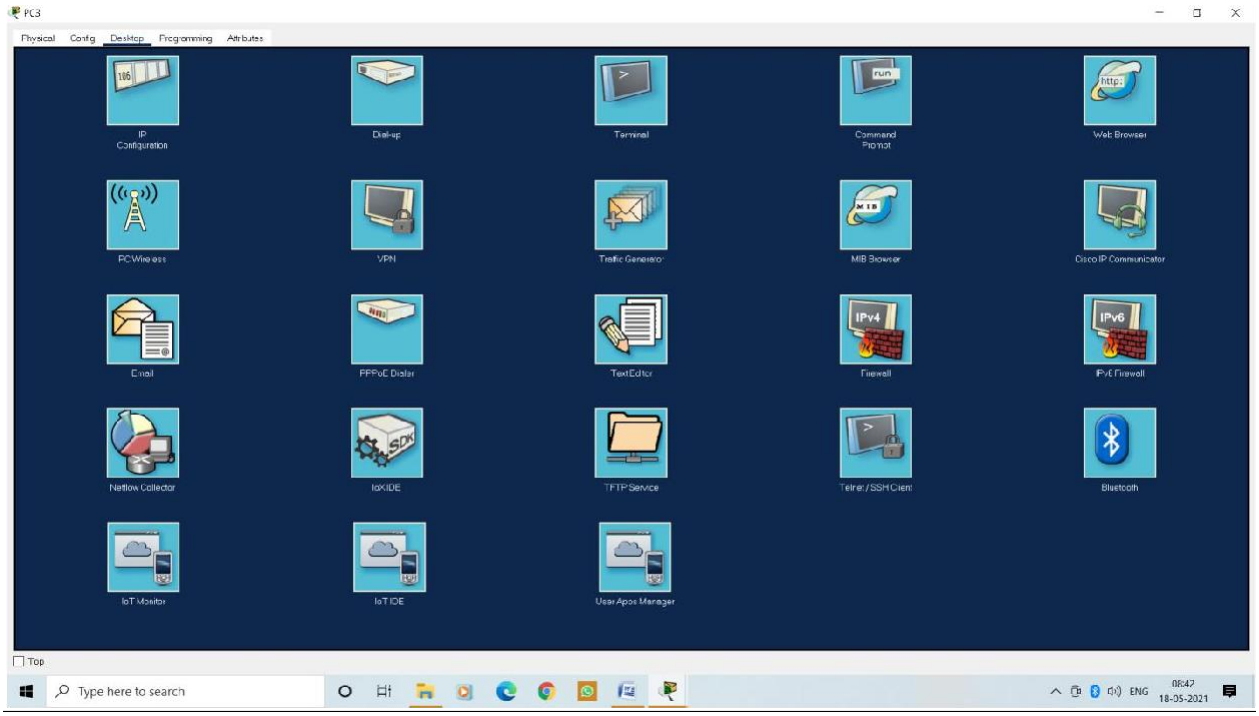


After power on of SWITCH 0 , all the red arrows have became green which means topology is working.

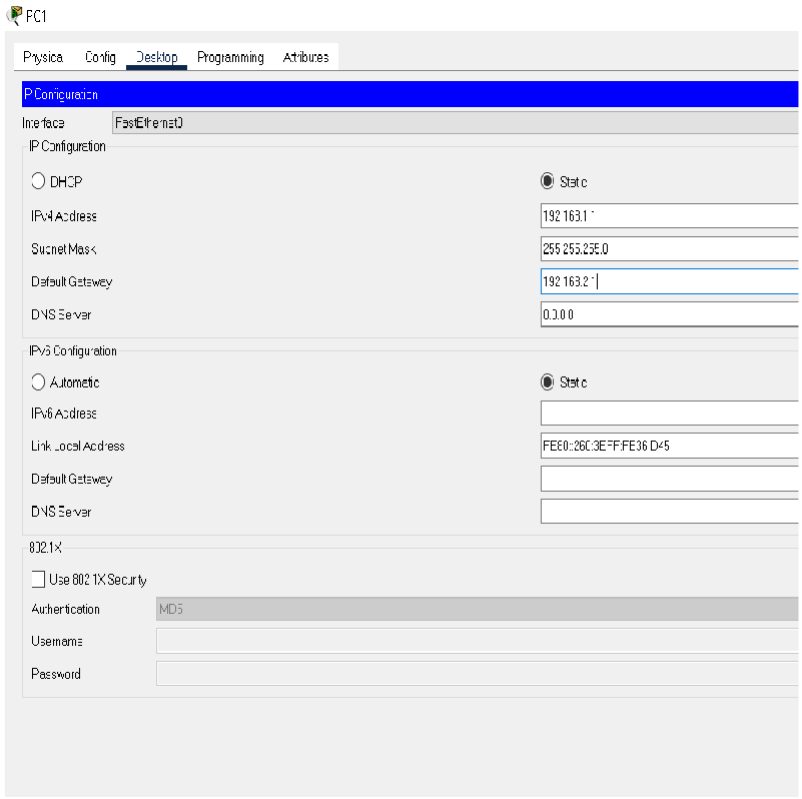
STEP 7 : Now by clicking each PC set their IP address,Subnet Make & Dfault Gateway from the following method.



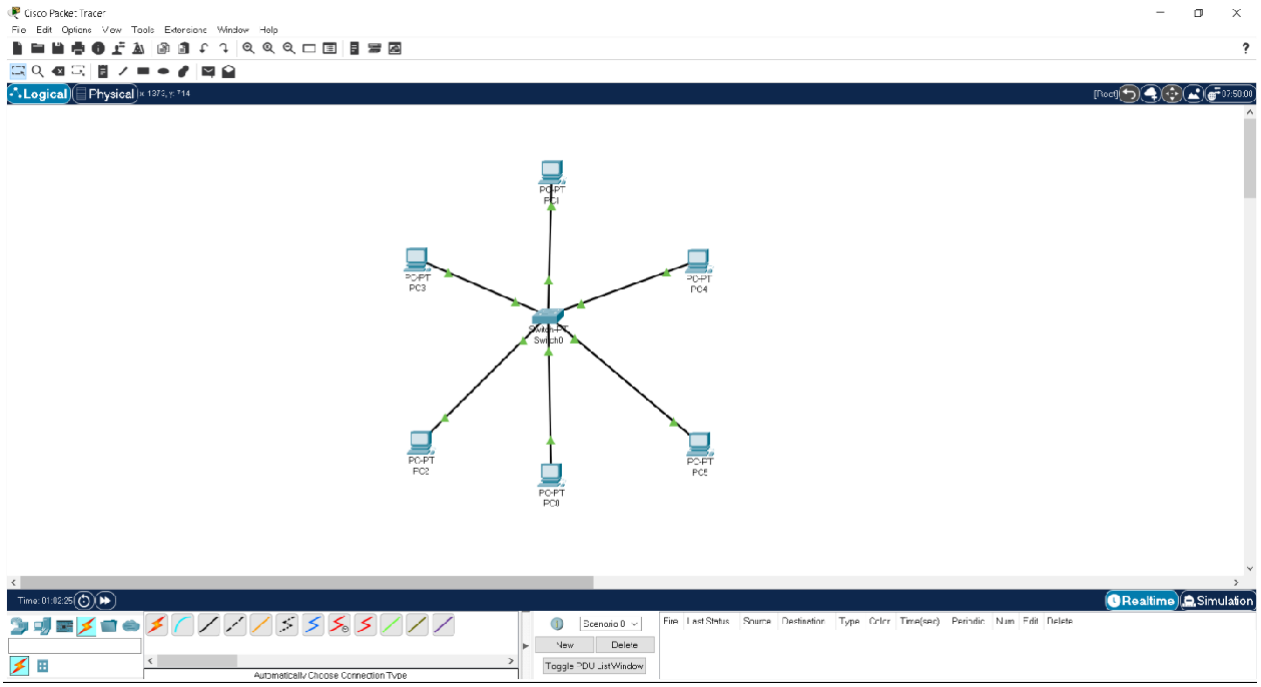
<u>After click on PC and now click on desktop.</u>



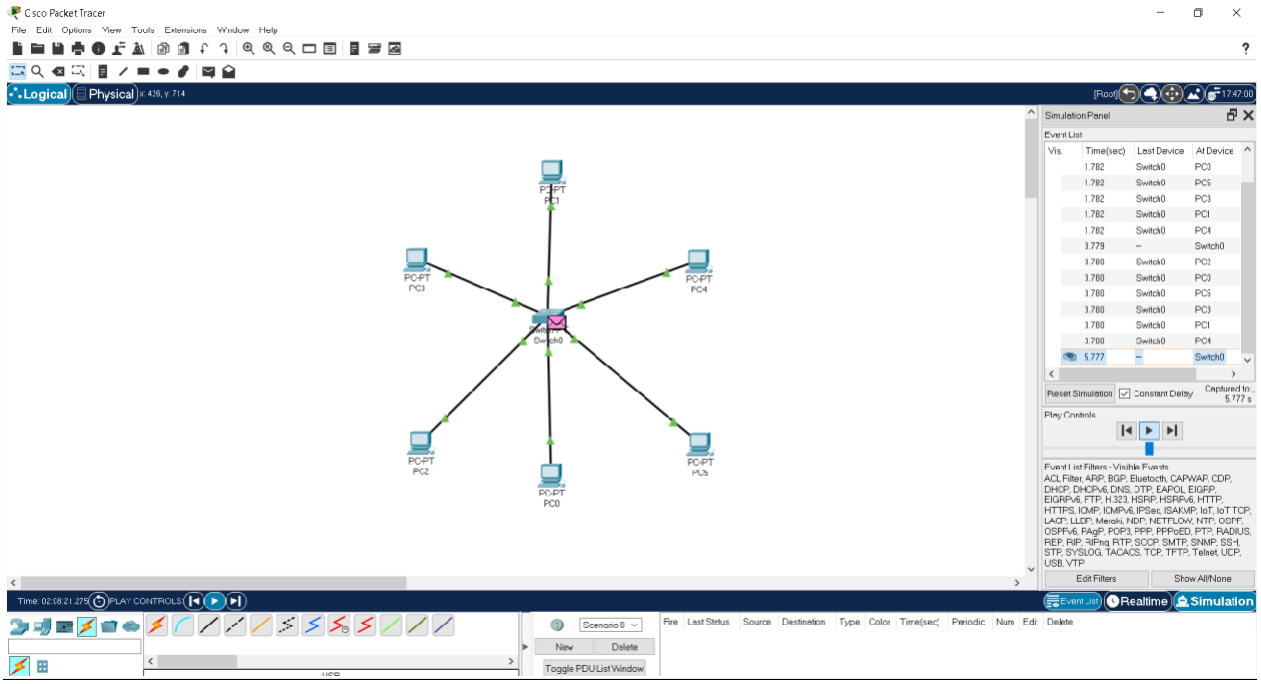
Now select IP configuration.



Now IP configuration is complete for PC1.



Now, star topology is completed.

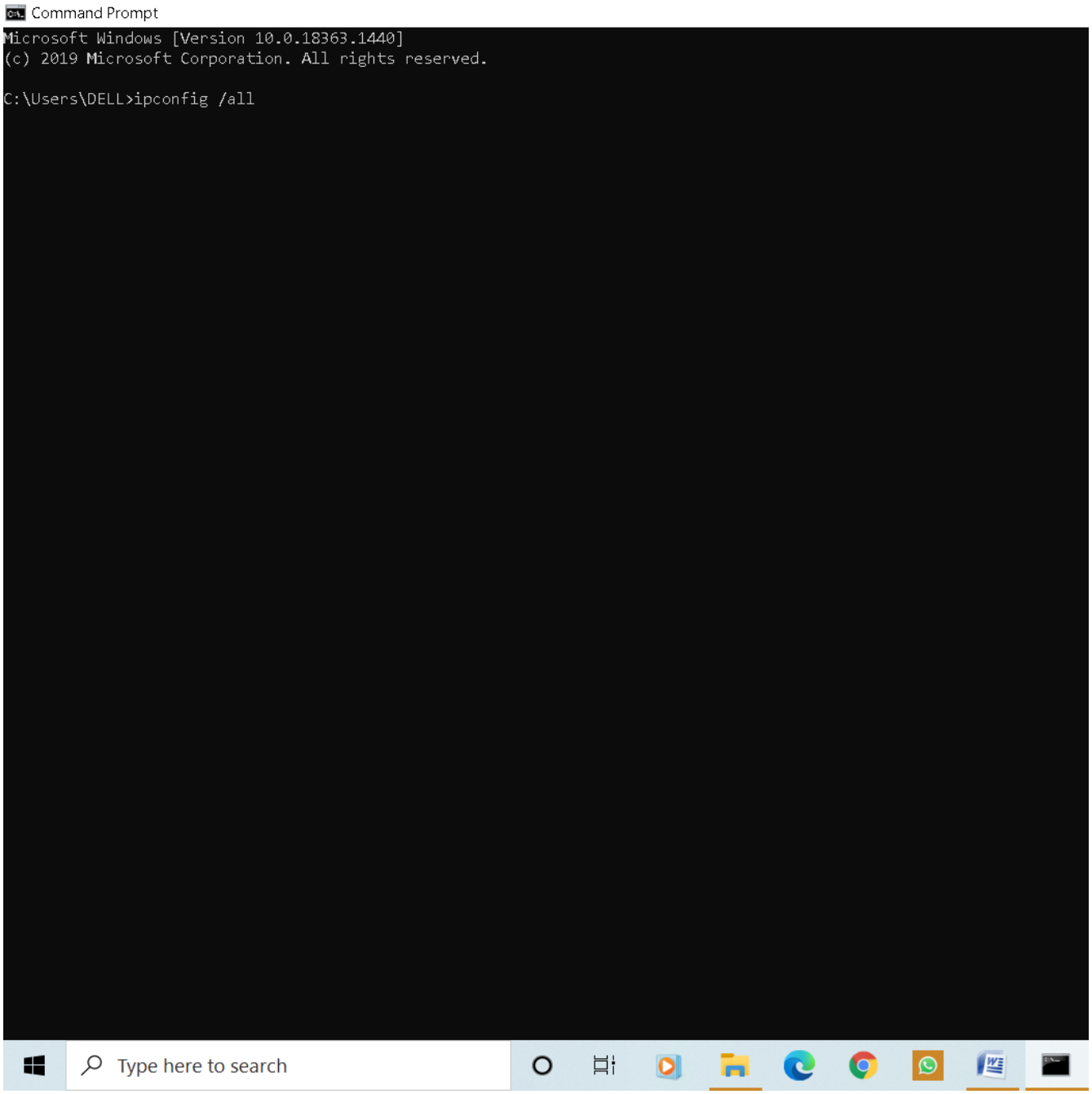


After simulation of star topology.

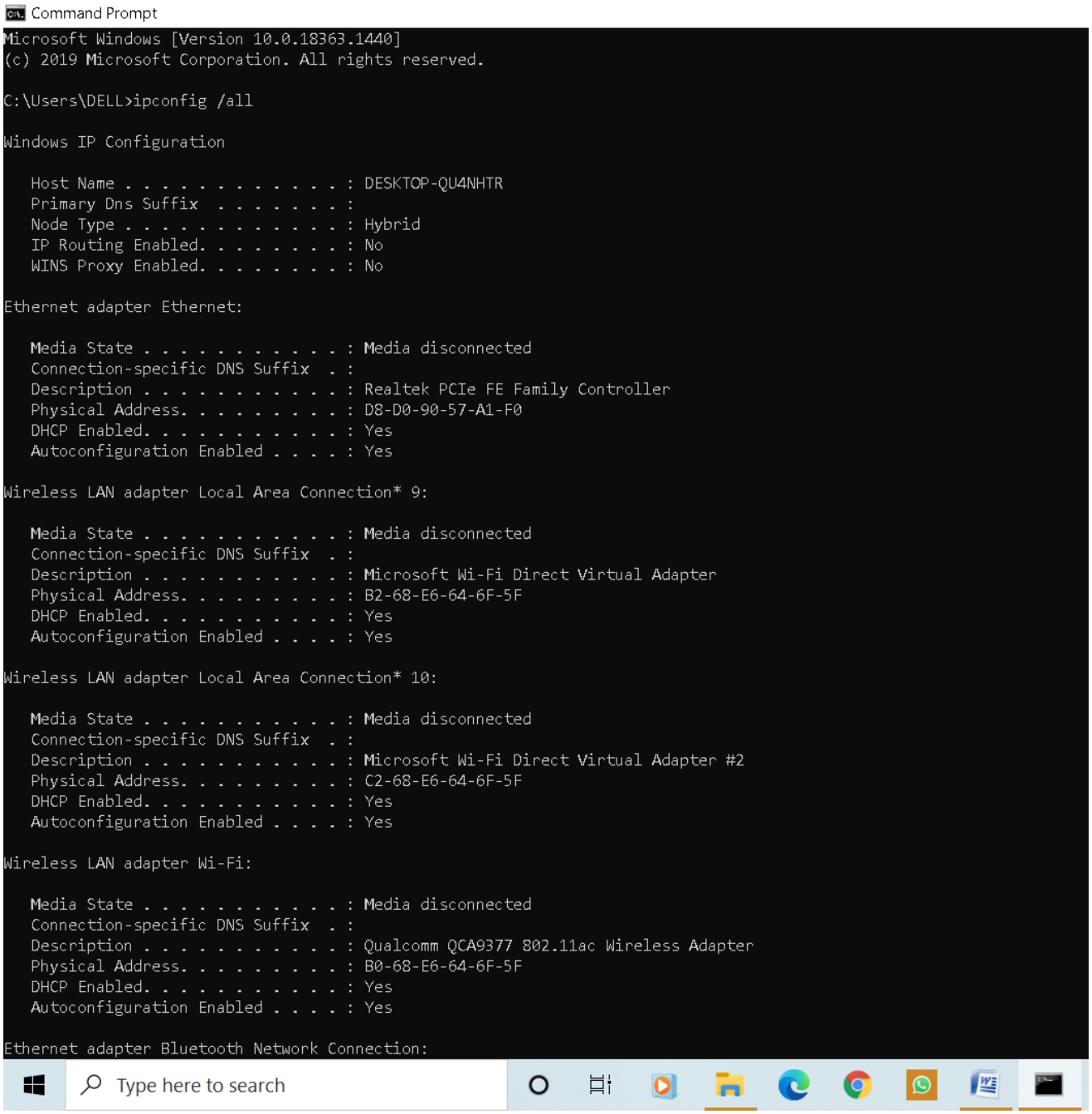
Program 8

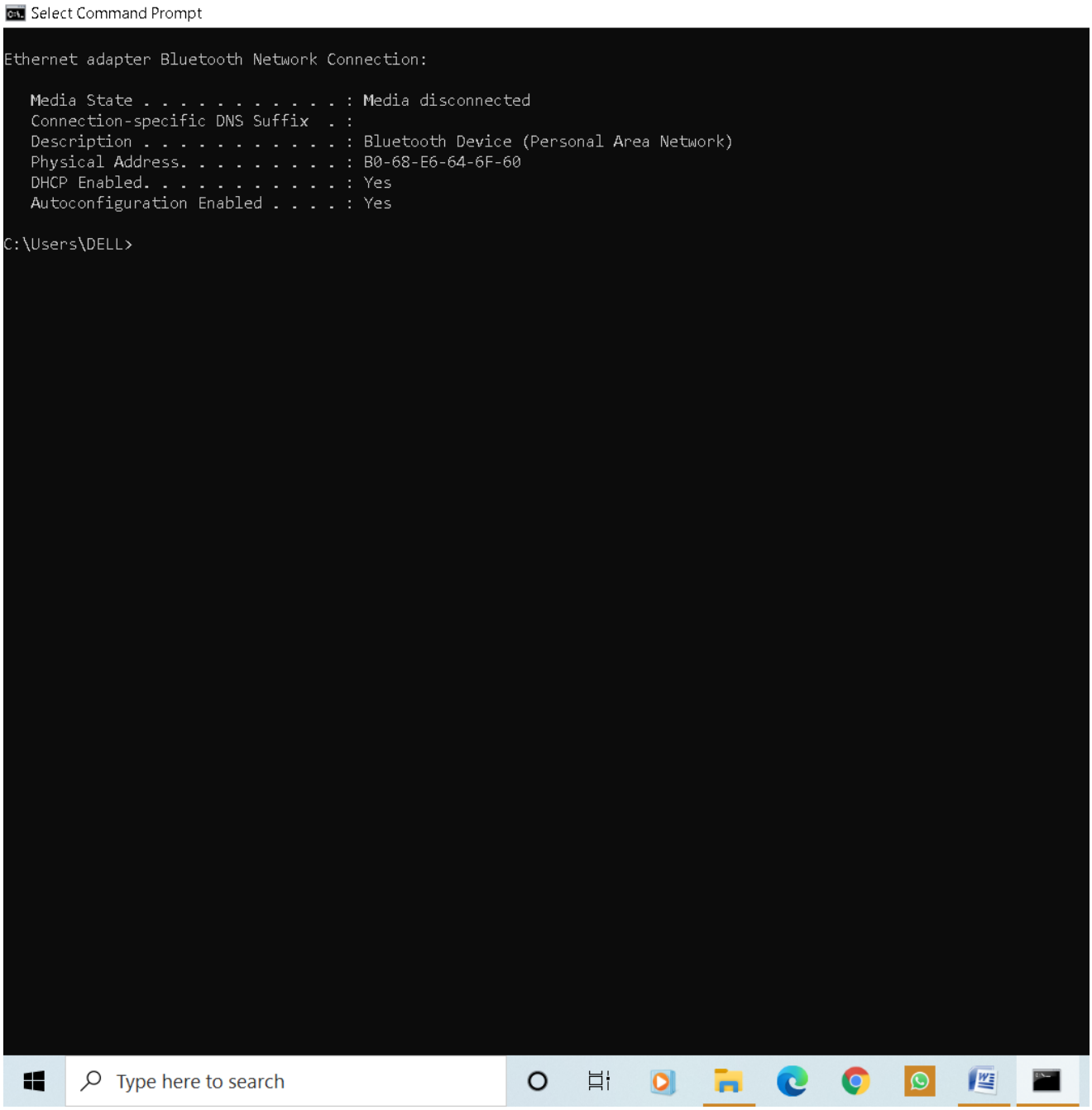
Aim :- Configuration of TCP/IP protocols in Window/LINUX.

Open command prompt then type <u>ipcongif /all</u> and press enter.



After pressing Enter




Select Command Prompt
Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : B0-68-E6-64-6F-60
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
C:\Users\DELL>
Type here to search

Program 9

Aim:-Configuration of TELNET protocols on router for remote access.

Telnet protocol:

Telnet is an application protocol that allows a user to communicate with a remote device. A user on a client machine can use a software (known as a Telnet client) to access a command-line interface of another, remote machine that is running a Telnet server program.Telnet is often used by network administrators to access and manage remote devices. A network administrator can access the device by telnetting to the IP address or hostname of a remote device. The network administrator will then be presented with a virtual terminal that can interact with the remote host. To use telnet, you must have a software (Telnet client) installed. On a remote device, a Telnet server must be installed and running.

Steps to Configure Telnet on Cisco Router

1. First of all, execute the following command to change the current hostname as Switch1.

```
Switch(config)#hostname Switch1
```

2. configure an IP address on the switch. Unlike the routers, typically switch does not require to be configured with an IP address. However, we need to configure an IP address on the switch's VLAN 1 interface.

The following commands will configure 10.0.0.1/8 IP address on the VLAN 1 interface.

```
Switch1(config)#interface vlan 1
Switch1(config-if)#ip address 10.0.0.1    255.0.0.0
Switch1(config-if)#no shutdown
Switch1(config-if)#exit
```

3. Once you have configured the appropriate hostname and IP address on the switch, execute the following commands to enable the Telnet protocol.

```
Switch1(config)#line vty 0 4
Switch1(config-line)#password 123456
Switch1(config-line)#login
Switch1(config-line)#exit
```

4. The following figure shows the Telnet configuration on Switch1

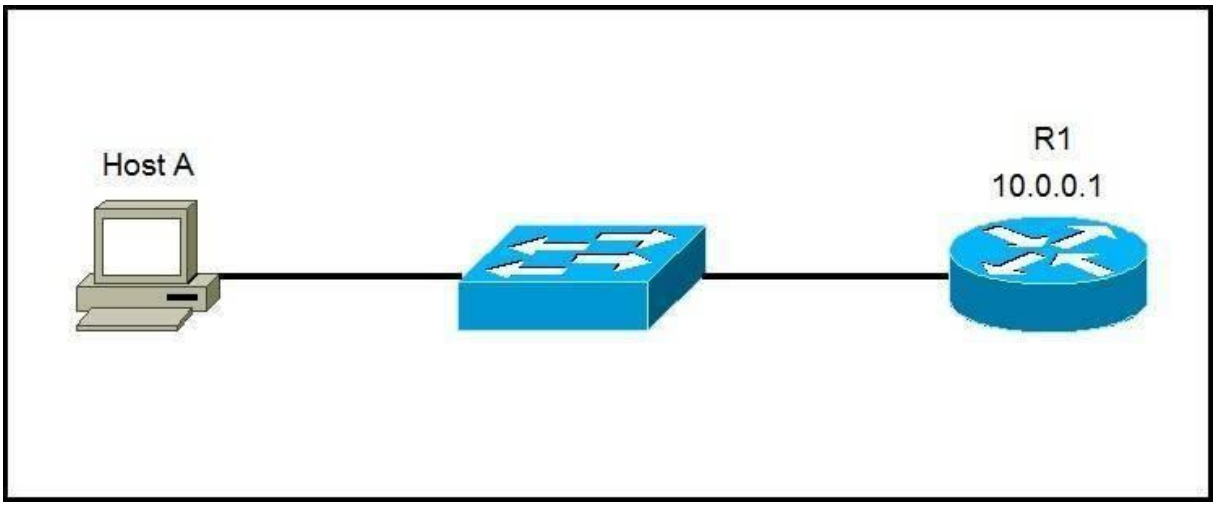
5. In the preceding commands, vty −means virtual terminal and 0 4 means ─total five mm(0 to 4) users can access the switch remotely at a time. 123456 is the password that the remote users need to know in order to connect to the switch.

6. Once you have done your configuration on switch1, move on to PC0. Configure 10.0.0.1/8 IP address on PC0.

7. After configuring the appropriate IP address on the PC, open the Command Prompt window of the PC, type telnet 10.0.0.100 and press Enter.

8. At the Password: prompt, type your telnet password (123456) and verify that you are able to connect to switch's console remotely.

Consider the following example:



The network administrator wants to use his computer (Host A) to access and manage the router (R1). The administrator will start a Telnet client program on Host A and enter the IP address of the router R1 (telnet 10.0.0.1):

```
telnet 10.0.0.1
Trying 10.0.0.1 ...Open


User Access Verification

Password:
```

The administrator can now manage the remote device (R1) from his own computer.
Although Telnet is simple and easy to use, it is not widely used anymore, especially in production environments. This is because Telnet sends all data in clear-text, including usernames and passwords! SSH is commonly used today instead of Telnet. Telnet is only used if SSH is not available on the device, for example on some older Cisco equipment.