Network Essentials

→ Network Communication (or) internetworking defines a set of protocols (that is rules & standards) that allow application programs to talk with each other without regard to the hardware & operating systems where they are run.

→ Internetworking allows applications programs to communicate independently of their physical network communications.

→ The internetworking technology called TCP/IP is named after its two main protocols. TCP (Transmission control protocol & IP (Internet protocol). It involves the following terms like.

Client :- A process that requests service on the network.

Server :- A process that responds to a request for service from a client.

Datagram:- The basic unit of information, consisting of one or more data packets, which are passed across an Internet at the transport level.

Packet:- The unit or block of a data transmission between a computer & its network.

Networking :-

→ It is the practice of Connecting Multiple Computing device inorder to share resources, exchange files and allow electronic communication.

→ The Computer network can be linked through a medium such as Cables, Telephone lines, Radio waves, Satellites (or) Infrared beams.

→ Building blocks of network are nodes & links.

Basic Terminologies

Nodes :- Devices Connected to network like Router, Modem, Switch & other devices.

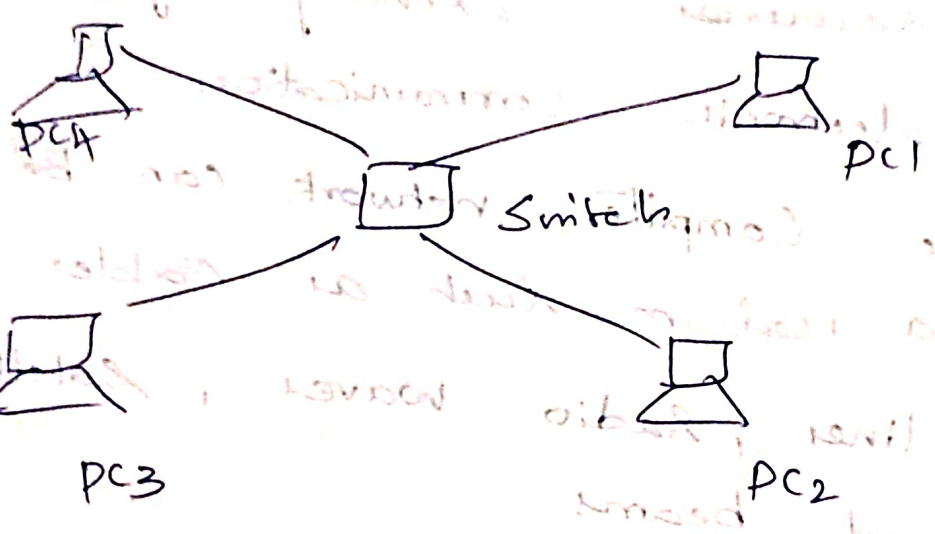
Hub :→ It is physical layer device.

Send data in form of bits.

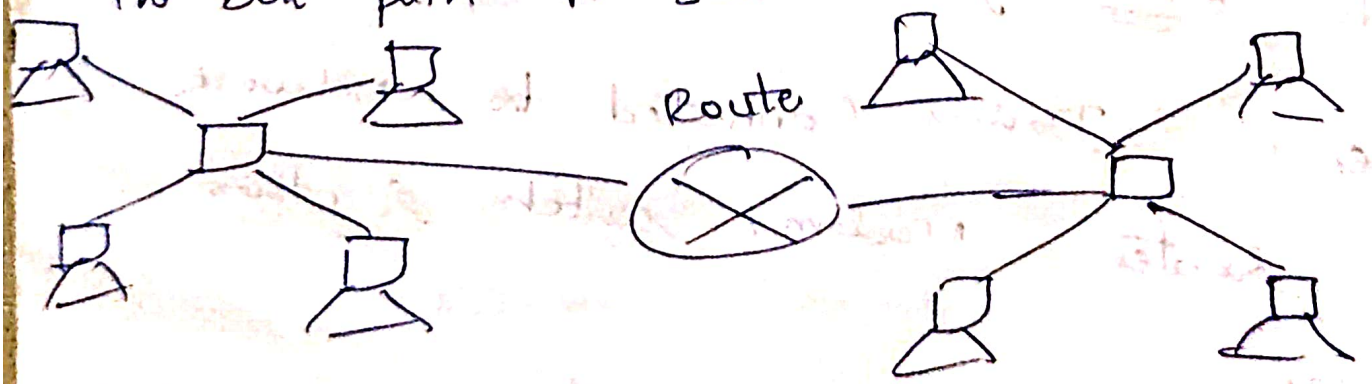
→ Connect multiple computers. & forward data to all. ie, the hub broadcast the data to all connected devices on the network.

→ datalink layer device.

Switch:- → device used to connect multiple computers / devices to form a network. Unlike hub it wont forward data to all. Instead, it forwards data to the destination device..



Router:- → Network layer device.
→ device which forwards data packet from one network to another.
→ uses routing table to determine the best path to send data.



Modem:- → device used to connect with Internet using telephone lines.

Bridge:- → device used to connect to different computing devices and also used to divide a large network in to smaller segments.

Ip Address :- → unique numerical identifier that is assigned to every device on a network.

Protocol:- → Set of rules & standards that govern how data is transmitted over a network. eg:- TCP/IP, HTTP, FTP.

DNS:- → Domain Name System.
→ is a protocol that translates human readable domain names (www.google.com) into Ip address that compute can understand.

Firewall:- → device used to monitor & control incoming & outgoing network traffic & used to protect network from unauthorized access & other security threats.

Network types :-

→ A network is a system that connects 2 or more computing devices for transmitting & sharing information.

→ The key components of a network are

- Network devices
- Links
- Communication protocols
- Network defense.

→ The network types depend on how large they are & how much of an area they cover geographically.

① Network types :-

→ Small home networks connect a few computers to each other as to the internet.

→ The soho (small office home office) network allows computers in a home office to connect to a corporate network (or) a remote office to access centralized, shared resources.

→ Medium to large networks, such as those used by corporations & schools, can have many locations with hundreds of interconnected hosts.

→ The internet is a network of networks that connects hundreds of millions of computers worldwide.

② Mobile Devices :-

→ Smart phones combine the function of many different products together such as telephone, camera, GPS receiver, media player & touch screen computer.

→ Tablets come with on-screen keyboards, so users are able do do

Many of the things that they used to do on their laptop computer such as comparing emails (or) browsing the web.

→ Smartwatch.

→ Wearable computer in the form of glasses.

Connected Home devices:-

→ Connected security system.

→ Household appliances such as ovens, refrigerators ---.

other connected devices:-

→ smart cars.

→ Radio frequency identification tags (RFIDS)

→ Sensors

→ Medical devices such as pacemakers, insulin pumps, hospital monitor---

Types of network:

① LAN :- → restricted to limited area (small n/w) → is a group of computers connected to each other in a small area such as building, office..

Range: upto 2km

Eg:- Home, School Library, office → lab, campus..

② PAN :- → is a network arranged within an individual person, typically within a range of 10 meters.

Wireless personal → is developed by using wireless technologies like WiFi, Bluetooth...

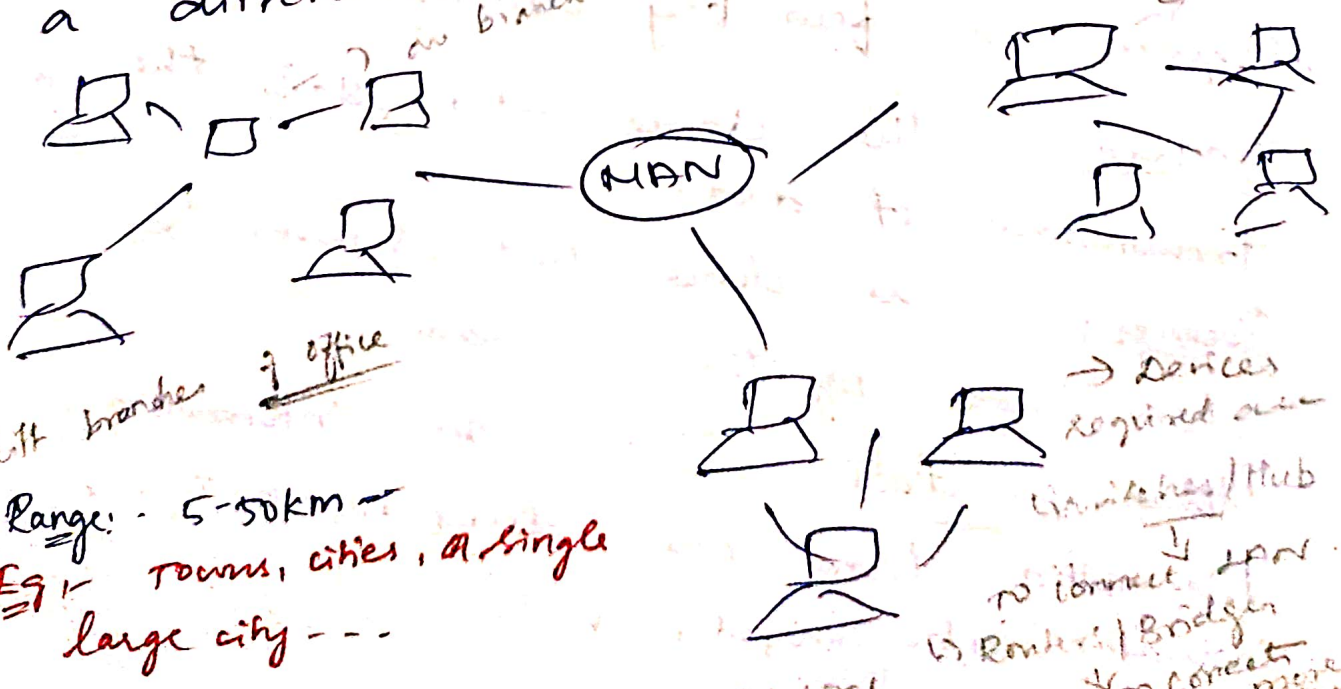
wired personal → is created by using the USB.

Eg:- USB, printer, tablet...

Range:- 1-100m

③ MAN :- → is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.

(restricted to small geographic area like city)



Range:- 5-50km

Eg:- Towns, cities, a single large city...

WAN: → 2 or more LANS can communicate within a ~~country~~.

→ is a network that extends over a large geographical area such as states or countries. (Above 50km) ⇒ Internet.

(Large geographical area within a city.)

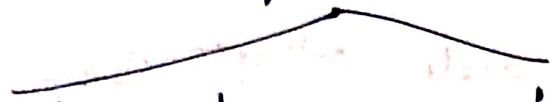
CAN: (Campus Area N/W) (1-5km)

→ is a network that joins 2 or more LANS together within a limited area. Eg: schools, buildings --

Network Topology :-

→ Network topology is how computers connect / relate to one another in a network.

→ It is of 2 types



Physical topology

↓

The way of how computers connect with the help of cables.

Logical topology

↓

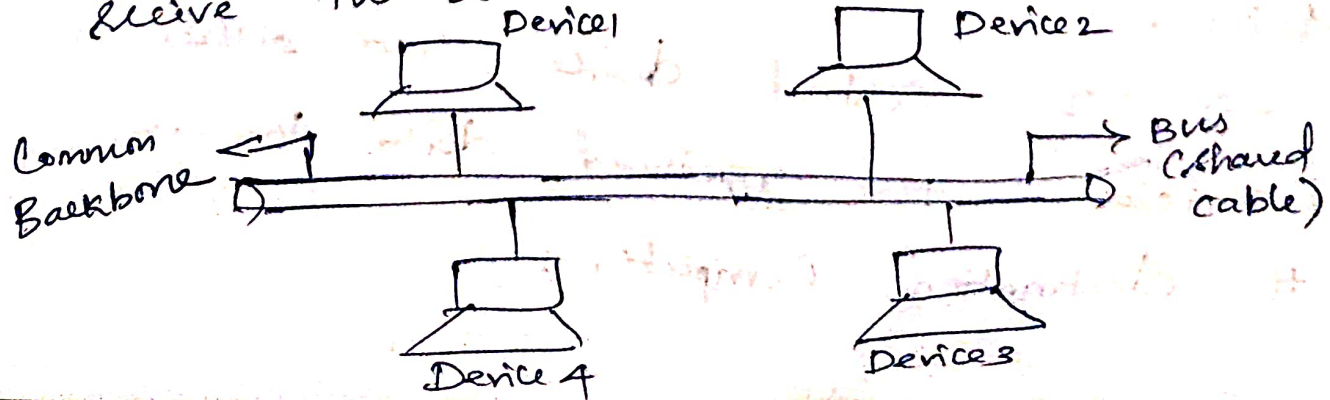
the way of how data flows from one computer to another within a network.

→ Types of topology :-

① Bus topology :-

→ In this type, computers connect to a shared central cable called a bus. ie, all connected computers use the same cable for data transmission.

→ Here, if a computer sends data to a second computer, all other computers connected to the same central cable also receive the data.

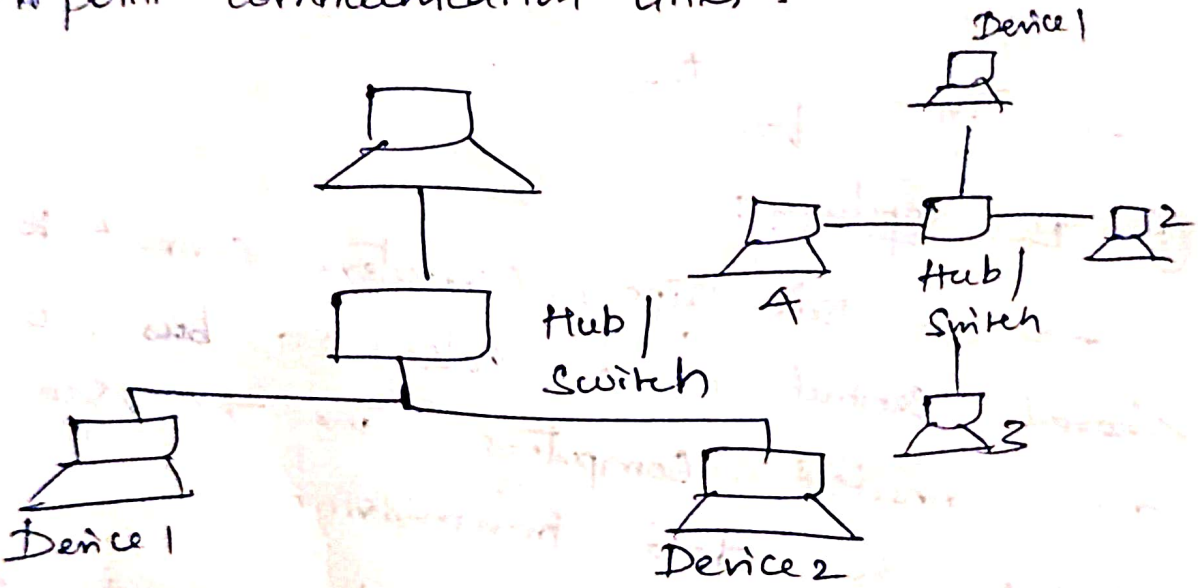


Advantages:- → Less cabling
→ Less expensive

Disadvantage:- → Limited number of computers can connect
→ If central cable fails, then entire network gets collapse.

Star topology

→ In this, the computer connect to a central device called a switch (or hub, with point to point communication links.



→ In this topology, if one computer wants to send some data to another computer, it is first routed to central device.

→ The central device, then either broadcast the received data towards the destination computer.

Advantages:- → Less expensive.

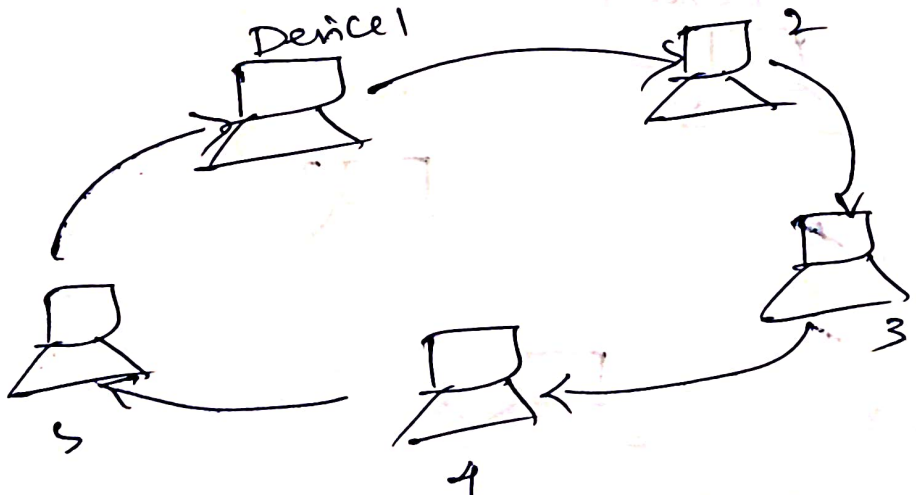
→ Easy to reconfigure.

Disadvantages:- → number of computers are limited based on the number of ports in the central device.

→ If the central device goes down, the whole network gets collapse.

(3). Ring Topology:-

→ In this, each computer connects to 2 adjacent computer to form a ring.



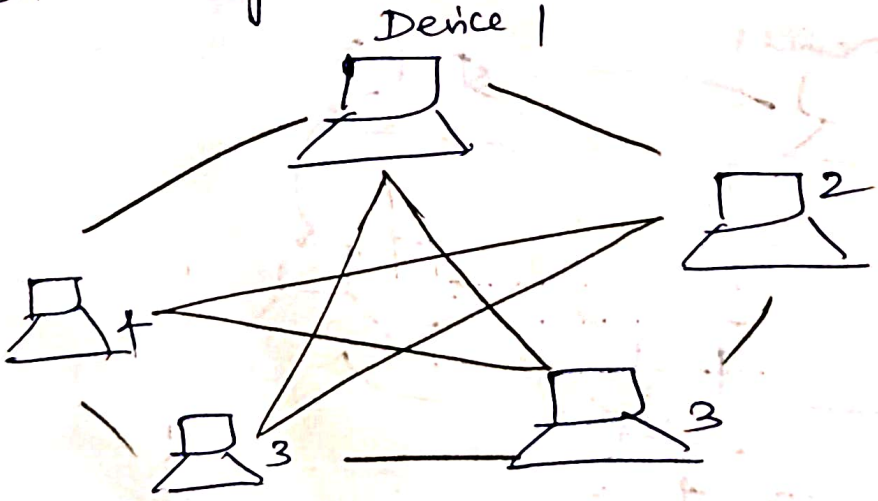
→ Data transmitted by one computer moves from one computer to another in a circular manner to reach its destination.

Advantages:- → Less Cabling.
→ Easy to troubleshoot.

Disadvantages:- → All Computer connect to form a closed loop, one fault paralyzes / collapse the whole network.

4) Mesh Topology:-

→ In this, each node connects to all other nodes; i.e., it is a point-to-point connection, which means that there are multiple paths that data can take between any 2 devices.



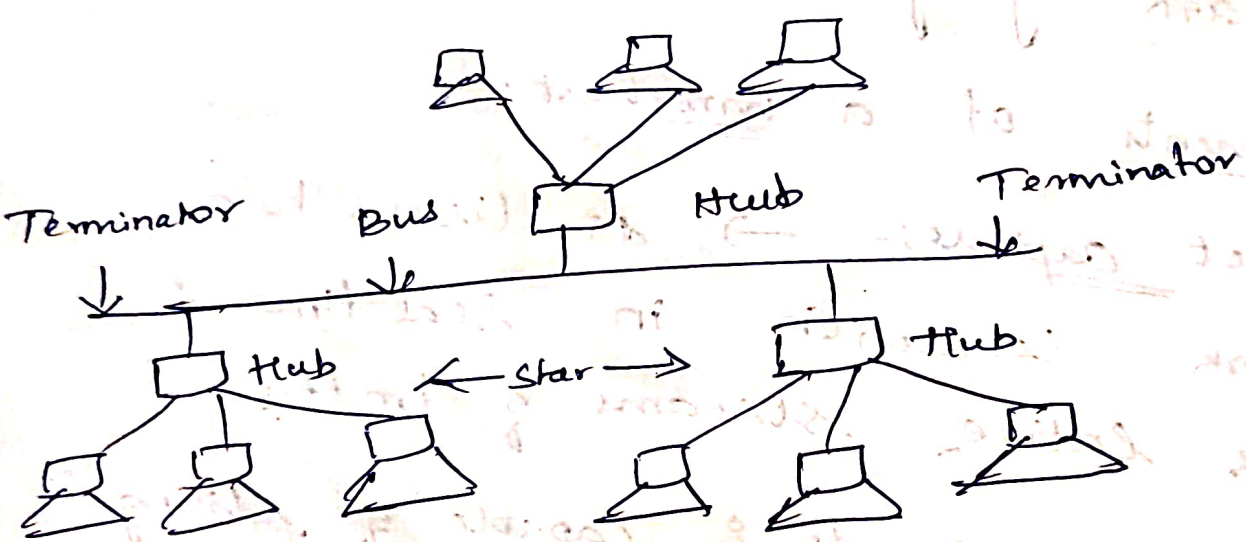
Advantages:- → Fault tolerance

Disadvantages:- → Cost
→ Power Consumption.

(5) Tree Topology:

→ It combines the characteristics of linear bus & star topologies.

→ It consists of groups of star-configured workstations connected to a linear bus backbone cable.



Data Transmission:-

→ It is sending & receiving digital (or) analog data between devices.

→ This can be achieved through different mediums, such as cables, optical fibres (or) wireless signals.

How data transmission work?

→ It involves atleast 2 (or) more digital devices communicating over a network & requires a few key components:

Sender:- The device that starts the transmission of data.

Receiver:- The device that receives the data sent by the sender.

Message (or) data:- This is the information transmitted from one device to another, including text, images, video..

Medium:- The physical path (or) channel through which data is transmitted, such as optical cable (or) wireless transmission.

Protocol:- A set of rules governing the format, timing & sequencing of data transmission.

The different factors in data transmission lower layer are

- The direction of information.
- The level of synchronization.
- The number of bits sent.

Types:-

~~personal data:-~~

Volunteered data:- This is created & explicitly shared by individuals, such as social network profiles, & this type of data might include video files, pictures, text (or) audio files.

observed data:- This is captured by recording the actions of individuals, such as location data taken using cell phones.

Inferred data:- This is data such as a Credit score, which is based on analysis of volunteered (or) observed data.

The bit:-

→ Computers & networks work only with binary digits

→ Each bit can only have one of two possible values 0 (or) 1.

→ The term bit is an abbreviation of "binary digit" & represents the smallest piece of data.

→ Each group of eight bits, such as the representations of letters & numbers is known as a byte.

→ Using (ASCII) American standard code for Information Interchange, each character is represented by eight bits.

eg:- Letter : A = 01000001
Number 9 = 00111001
special character # = 00100011

Common Methods of Data transmission:-

→ After the data is transformed into bits, it must be converted into signals that can be sent across the network media to its destination.

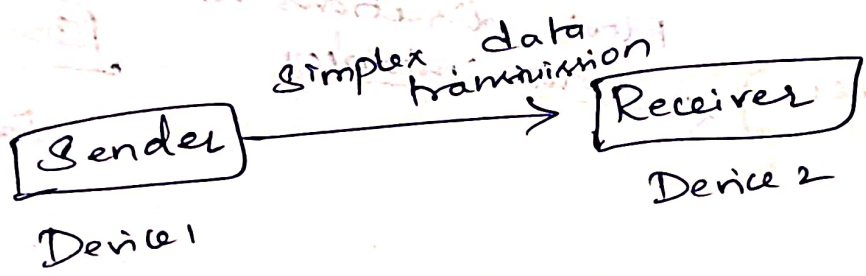
→ Media refers to the physical medium on which the signals are transmitted.

→ A signal consists of electrical or optical patterns that are transmitted from one connected device to another.

Types of data Transmission:-

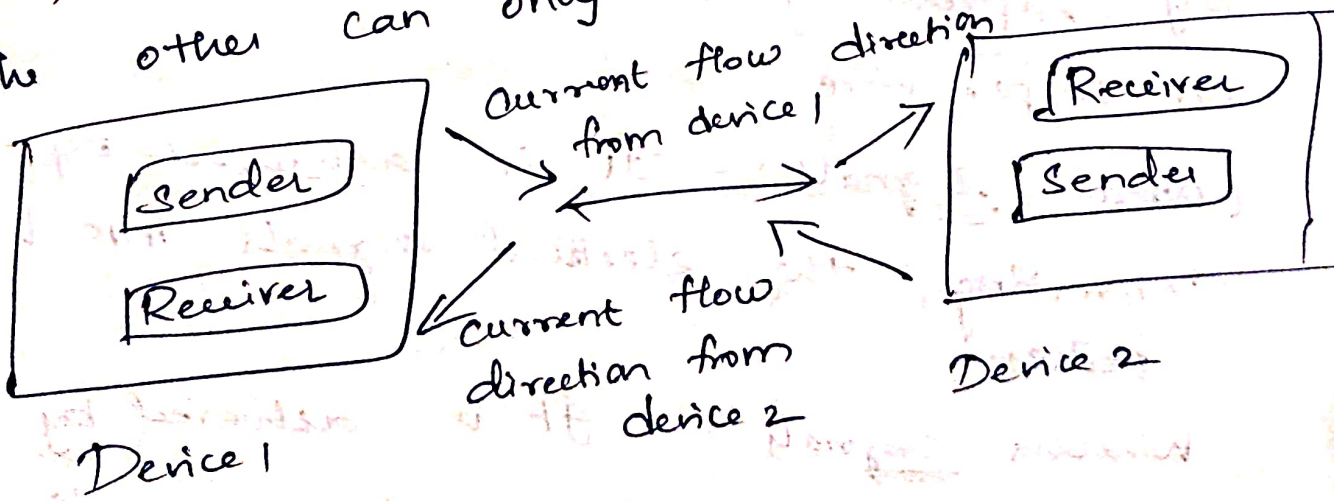
① Simplex Transmission:- (Unidirectional)

→ It's a mode of communication where the data can only flow in one direction.



② Half-duplex transmission:-

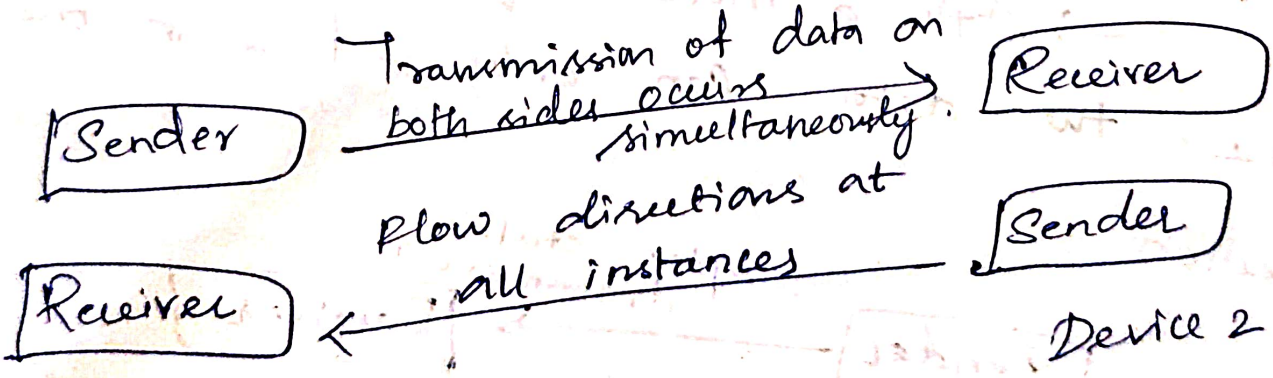
→ Allows data to flow in both directions, but only one direction at a time. i.e., when one device sends data, the other can only receive it & vice versa.



③ Full- duplex Transmission:-

→ Information / data flow in both directions simultaneously, allowing for 2-way Communication.

→ It is bidirectional, as it enables to Transmit & Receive data Concurrently.

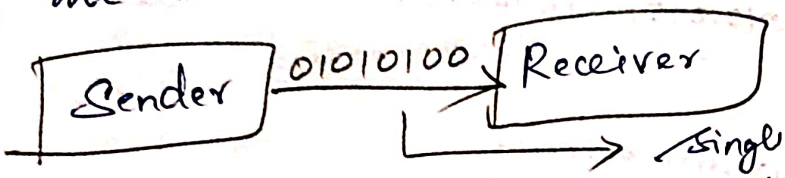


Serial transmission:-

→ It involves sending data bits one at a time over the transmission channel.

→ This means that the bits are sent sequentially rather than in parallel.

→ This type of transmission is slow, because only one-bit can be transmitted at a time.



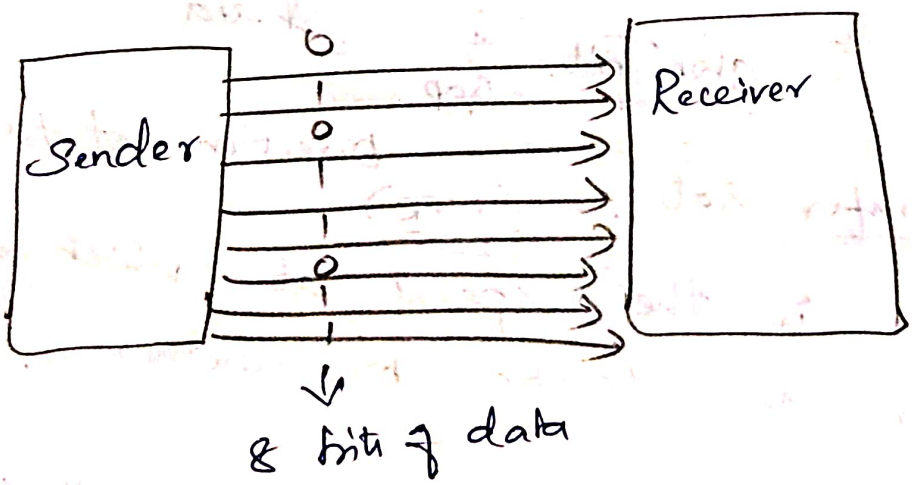
eg:- USB.

Single wire carries the data one bit at time.

Parallel transmission:-

→ It sends multiple data bits at once using parallel channels.

→ It is useful for transfering large amounts of data quickly.



→ It is faster method of data transmission than serial.

→ eg:- printer. (sending data to printer).

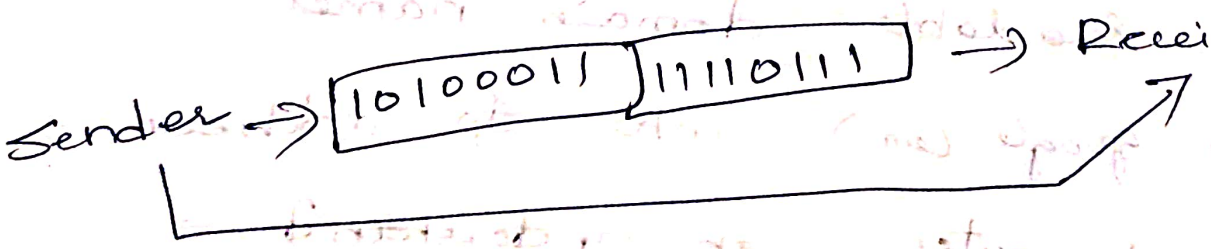
Synchronous Transmission:-

→ It is a full-duplex type of transmission that allows data to be transmitted.

→ Sending bits one after another without start / stop bits (or) gaps.

→ It is the responsibility of the Receiver to group the bits.

→ The Receiver counts the bits as they arrive & group them in eight bit units.

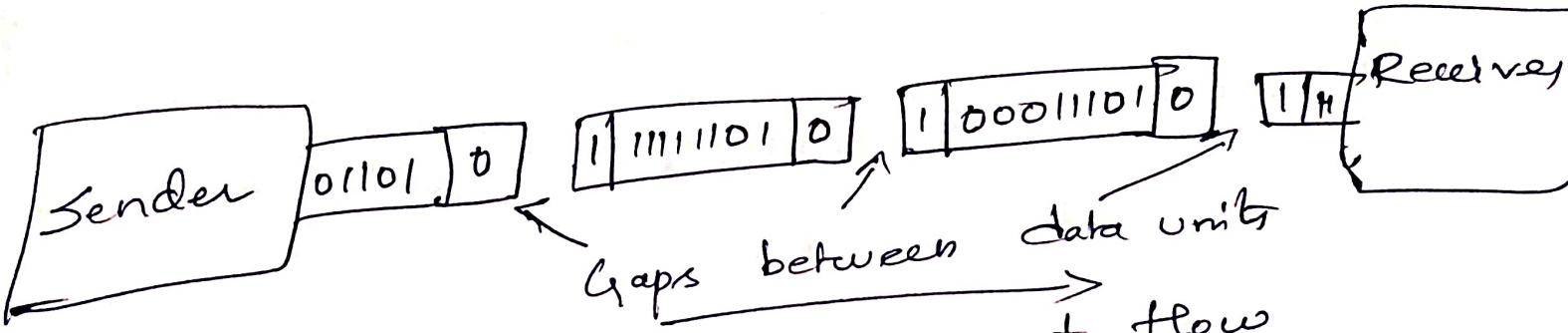


Direction of flow

Asynchronous Transmission:-

→ It is a type of half-duplex transmission that allows data to be transmitted.

→ Send one start bit (0) at the beginning & one (or) more stop bit (1) at the end of each byte.



0 → represents start bit

1 → represents stop bit

Device.

There are 3 common methods of signal transmission used in networks:

Electrical signals :- Transmission is achieved by representing data as electrical pulses on copper wire.

optical signals :- It is achieved by converting the electrical signals into light pulses.

Wireless signals :- It is achieved by using microwave, or radio waves through the air.

Bandwidth :-

→ It is the capacity of a medium to carry data.

→ Digital bandwidth measures the amt of data that can flow from one place to another in a given amt of time.

→ It is typically measured in the number of bits that can be sent across the media in a second.

Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	bps	1bps = fundamental unit of bandwidth.
Kilobyte : Thousands of bits per second.	Kbps	1 Kbps = 1000 bps = 10^3 bps
Megabyte : Millions of bits per second	Mbps	1 Mbps = 1,000,000 bps = 10^8 bps
Gigebyte : Billions of bits per second	Gbps	1 Gbps = 1,000,000,000 bps = 10^9 bps
Terabyte : Trillions of bits per second	Tbps	Tbps = 1,000,000,000,000 bps = 10^{12} bps

Throughput :-

→ Like bandwidth, throughput is the measure of the transfer of bits across the media over a given period of time.

→ However, due to a number of factors,

Throughput does not usually match the specified bandwidth.

→ Many factors influence throughput including:

1) The amt of data being sent & received over the connection.

2) The types of data being transmitted.

3) The latency created by the number of network devices encountered between source & destination.

⇒ Latency refers to the amt of time, including delays, for data travel from one given point to another.

⇒ It is made of four components.

Latency = Propagation time + Transmission time + queuing time + processing delay.

Network performance :-

→ It is measured in following ways

1) Bandwidth
2) Throughput
3) Latency (Delay)

Bandwidth :-

→ The bandwidth of a network is given by the number of bits that can be transmitted over the network in a certain period of time.

→ [i.e., maximum amount of data that can be transmitted per second].

→ Bandwidth is applicable for both wired & wireless network.

↳ Wired measure → bits per second.
↳ Wireless " → hertz

Throughput:-

→ The throughput is a measure of how fast we can actually send through a network.

→ [ie, Actual amount of data that passes through the medium].

Latency (Delay):-

→ It defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.

→ It made of four components

↳ Transmission delay.

↳ Propagation delay.

↳ Queueing delay.

↳ Processing delay.

→ Latency = Transmission delay + propagation delay + Queuing dely + proceing delay.

Data Transfer Rate :- (DTR)

→ It is the speed at which data moves from one location to another.

$$DTR = \frac{\text{Amount of data transmitted}}{\text{Time (seconds)}}$$

Where

→ amount of data is the size of data, measured in bits / bytes.

→ time is the duration of data transfer, measured in seconds.

→ The data transfer rate is usually expressed in bits per second (bps), kilobits per second (kbps), megabits per second (Mbps), or gigabits per second (Gbps), depending on the speed of the transfer.

→ eg. suppose you need to transfer a file that is 10 MB in size & takes 20 seconds to transfer the file.

$$DTR = \frac{10\ MB}{20\ sec} =$$

→ Amount of data, we will convert 10 megabytes to megabits

[1 byte = 8 bits]

[10 × 8 = 80 megabits]

$$DTR = \frac{80}{20} = \boxed{4\ mbs}$$

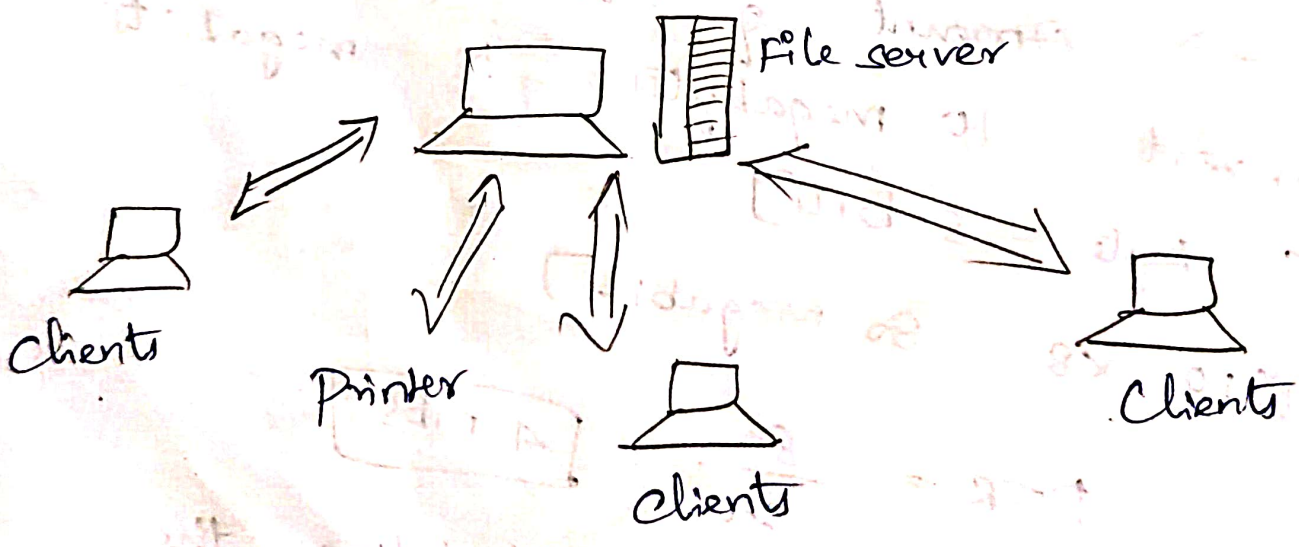
→ Based on this calculation, the data transfer rate for this file transfer is 4 megabits per second.

Client and Servers:-

→ In general, computing Machines Connected together on networks can be Categorized as 2 types, Servers & Clients.

→ A Server is Centralized computer that provides services such as network management processes, access to resource files (or) security to other nodes (computers, printers etc..) in the network.

→ The Machines that requires services from the Server are called clients.



→ A Server is simply a computer that provides the network resources & provides service to other computers when they request.

→ A client is the program that request the service from a server.

→ Local area network (LAN) is based on client-server relationship.

→ A client-server network is a distributed communications architecture in which a centralized server receives & responds to requests for services & data from multiple clients.

Purpose of a client-server network:-

→ To share resources efficiently.

→ This type of network makes the same digital services & data accessible to multiple users across a shared connection, whether it's a LAN, WAN (or) so on--

→ In a client-server network, a central server computer receives a client request & can do the following:-

* Respond to the request directly -
* Route it to another server that can fulfill the request.

Types of Server :-

① File server :- → Stores data & allows clients to remotely access their / shared files. (often through the LAN only)

→ A user can read, write, exchange & manage the files within the help of file servers.

② Printer Server :- Controlling & managing printing on the network.

③ Application Server :-

→ Allows multiple users access to software.

→ often used to access data from a database.

④ Message Server :- → The data can be used in the form of audio, video, binary, text (or graphics.

⑤ Database Server :- → It is type of application server.

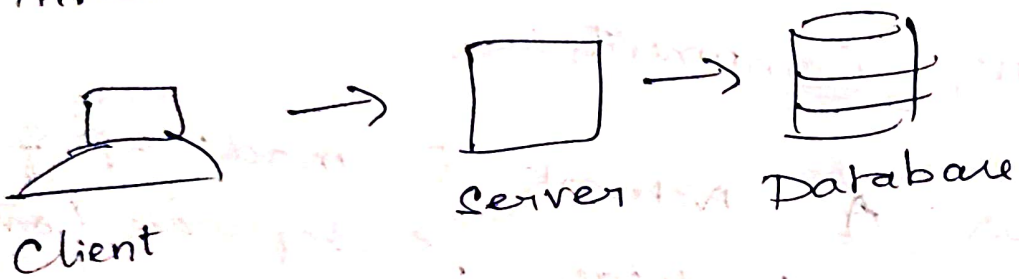
→ Stores large amounts of data.

3-Tier Architecture:-

→ It is also known as the three-layer architecture, is a client-server software architecture

→ The purpose of this architecture is to improve Modularity, Maintability, flexibility of the software system.

Three Tier Architecture



The three layers are:

(1). presentation layer :-

→ This layer represents the user interface of the application & is responsible for presenting data to the user & receiving user input such as web pages, forms...

(2). Application layer :-

→ This layer Contains the business logic of the application & performs the core processing of the data.

→ It is responsible for processing user requests, retrieving & manipulating data

③. Data storage Layer :-

→ This layer is responsible for managing the data storage & retrieval in the system.

Network Components :-

→ A network is made up of several hardware & software components.

→ All components make it possible for transfering data & information from one device to another & make easy communication between different computers.

→ Components of network are:

① Server :- → is a computer that serves the data to other computers & users.

→ The term server usually refers to a computer system that receives a request for a web document & sends the request information to the client.

(2) client:-

→ The device that receive request and response from the server is called a client.

→ When the server & its client work together on the computer, we call it the client / server network.

(3). Transmission media:-

→ It is the medium through which the data is transferred from one device to another in a network.

→ physical transmission medium includes the use of wires & cables like fiber optic cables, coaxial cable etc.-

→ Wireless transmission medium includes the use of media like infra-red waves, electromagnetic etc.-

(4) NIC:- (Network Interface Card):-

→ It is also known as network interface controllers, Network adapter, LAN adapter & physical Network interface.

→ They are hardware components used to connect computer within in the networks.

→ Without NIC computer cannot be connected to the network.

→ It has 2 types

- Internal NIC (Wired NIC)
- External NIC (Wireless NIC)

(5) Hub:-

→ The hub is used to connect multiple connections that come from different branches.

(6) Switch:-

→ It a component that helps to connect multiple devices for data transfer.

(7). Router:-

→ It is a hardware network Component

→ The Router receives the data & forward it to the destination.

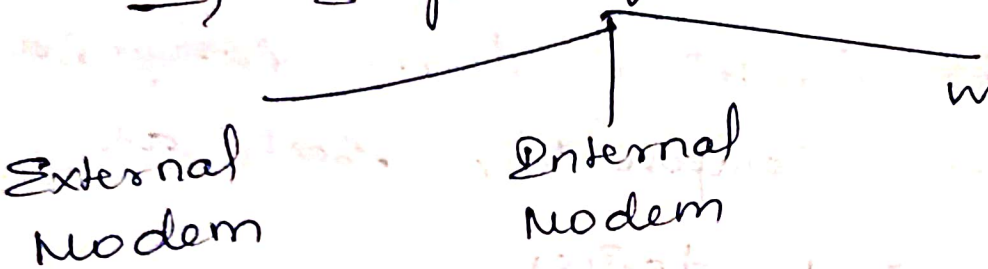
→ It has 2 types

- Broadband Router
- Wireless Router

(8) Modem :- (Modulator / Demodulator)

→ It allows a computer device, such as router or switch to connect to the internet.

→ 3 types of modem as



(9) Repeater :-

→ This component receive signals from cables like optical fiber, coaxial cables --

(10) Bridges :-

→ This component is used to connect two different or same network.

(11) Gateway :-

→ It is a hardware that acts as a gate within two networks. such as firewall ---

Network structure:-

→ It is an organizational blueprint characterized by interconnected nodes.

→ It contains three categories of hardware components, such as

↳ End devices
↳ Intermediate devices
↳ Network media.

Enddevices:- Desktop computer, Laptop, printer, iphone, wireless Tablet.

Intermediate device:-

Wireless Router, LAN switch, Router,

Network Media:-

Wireless media, LAN media, WAN media.

Online Connections :-

Wireless Networks :-

→ Networks that are not Connected by Cables are called wireless networks.

→ They generally use radio waves for Communication between the nodes.

Types :-

① wireless LANs :- Connects two (or) more network devices.

② wireless MANs :- Connects 2 (or) more wireless LANs.

③ wireless WANs :- Connects 2 (or) more wireless (or) large areas Comprising LANs, MANs.

Components of a wireless Network :-

→ To setup a wireless network, need 3 basic components

- ↳ Access points
- ↳ Routers
- ↳ Clients.

Examples :- ↳ Mobile Telephones
- ↳ Cell phone Network (3G, 4G, 5G)
- ↳ Gps
- ↳ Bluetooth
- ↳ wi-fi
- ↳ NFC (Near field communication).

Local Network Connection:-

LAN Components :-

→ There are many components that can be part of a local area network.

→ Some of are personal computers, servers, networking devices & cabling.

→ These components can be grouped into four main categories:

- Host
- Peripherals
- Network devices
- Network media

→ To physically connect to a network, an end-user device must have a network interface card (NIC) & some configuration of the operating system, so that the device can participate in the network.

→ There are three parts of IP configuration through which device can send & receive information on the network.

Ip Address :- This identifies the host of the network.

Subnet Mask :- This is used to identify the network on which the host is connected.

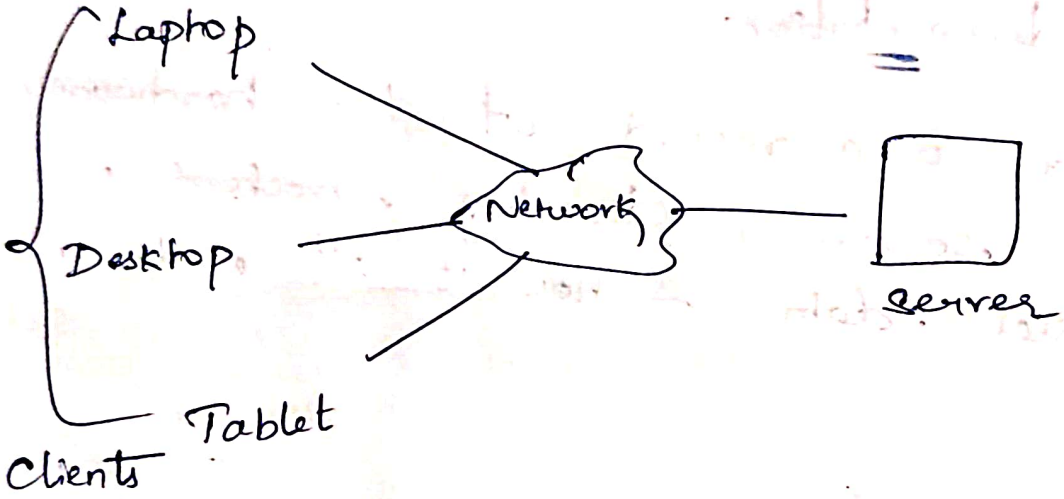
Default gateway :- This identifies the networking device that the host uses to access the internet (or other remote network.

Network documentation :-

→ It is a record of the hardware, software, servers, directory structure, user profiles, data & how it all works together.

Client - Server Network :-

→ In this network, there is atleast one dedicated central server that controls the network & a number of clients connect to the server to carry out specific tasks.



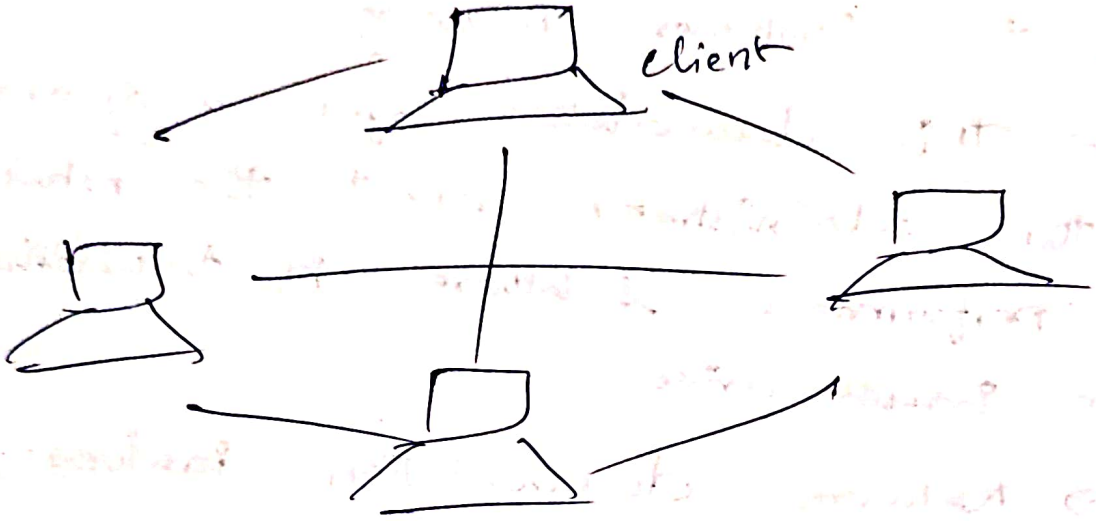
→ A client - server network has multiple clients connected to one central server for communication & resource sharing between devices.

Peer - to - peer network :-

→ In this network, there is no central server controlling the network, instead, all the computers in the network

are connected to one another & share resources, files, applications & programs.

→ In peer-to-peer network, each computer can function as either client (or) server.



Key features of peer-to-peer:

→ Decentralization.
→ Self-Organizing system
→ Resource sharing
→ Privacy & Security
→ Direct Communication.
→ Fault tolerance & Redundancy.

Network Documentation:-

→ It is a type of specialised technical documentation.

→ It is the practice of keeping records relating to the networks of computers that the customer is using.

→ This documentation gives a glimpse to the administrators about the network, its performance & where to troubleshoot when issues arise.

→ Network documentation involves:

↳ how the two networks are connected together & what are the services provided between their connections.

↳ It lists all the devices that are making up the network.

↳ Identifies all network infrastructure elements such as routers, switches, firewalls etc..

Key benefits of network documentation:-

1) Visualization
2) Troubleshooting
3) Budgeting & Forecasting

Wireshark:

→ It is widely used, open source network analyzer that can capture & display real-time details of network traffic.

→ It is particularly useful for troubleshooting network issues, analyzing network protocols and ensuring network security.

→ Wireshark is one such tool, that can offer an in-depth view into network activities, diagnose network performance issues (or) identify potential security threats.

Key features of wireshark:-

→ PCAP (packet capture)
→ Real-time analysis
→ Filtering capabilities
→ GUI (Graphical User Interface).

Uses :- → To Analyze network packets

→ To troubleshoot network issues

→ To check Malicious & hacking possibilities in network.

Why wireshark is so popular:

→ It has a great GUI

→. It offers network monitoring on almost all types of network standards (ethernet, WLAN, Bluetooth etc.)

→ All the necessary components for monitoring, analayzing & documenting the network traffic are present, It is free to use.

Color Coding in wireshark:-

→ The packets in the wireshark are highlighted with blue, black & green color.

→ These colors help users to identify the types of traffic.

→ It is also called packet colorization.

Wireshark User Interface:-

→ It Consists of four parts.

- Main Menu
- Main Menu Toolbar
- Filter Tool
- Interface List

→ wireshark helps you identify packet types by applying common sense color coding.

Color in Wireshark	packet type
Light purple	TCP
Light blue	UDP
Black	packets with errors
Light green	HTTP traffic
Light yellow	windows-specific traffic, including server message Routing
Dark yellow	ACK traffic.
Dark grey	

Components of a wireshark:-

(1). packet capture:- → It listens to a network connection in real time & grabs entire streams of traffic.

(2). Filtering → It is capable of slicing & dicing all data using filters.
→ By applying filter, you can obtain just the information you need to see.

③. Visualizations:- → It allows you to Visualize entire conversations & network streams.

Packets:-

→ Devic A & B are Connected using router.

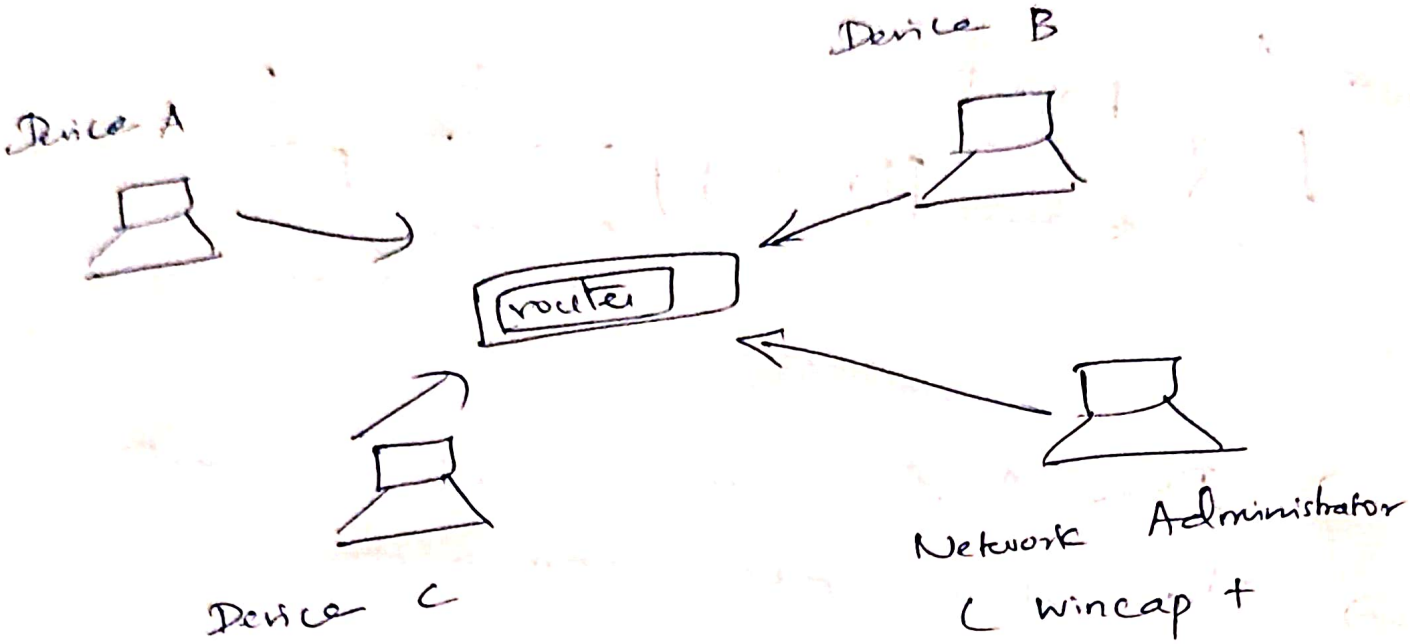
→ Two devices are Communicating by Means of packets.

→ Device A is sending request packet to Router, Router finds a destination address & sends (forwards) to device B.

→ Device B will receive the request packet & based on that request it will forward response packet to Router & Router finds destination address & forwards to device A.

→ Packets Contains informations like Ip & MAC address, data's, Port number. & so on---

Working of Wireshark :



→ Wincap software will take a copy of all packets in this network & send to wireshark tool.

→ By Wireshark tool, can analyze network traffic.

→ Network administrator can monitor network traffic.

→ By this way, any unwanted request can be monitored.