COMPUTER NETWORKS

WHAT IS A COMPUTER NETWORK? ITS FEATURES

A system of interconnected computers and devices seeking to share resources is known as a computer network.

FEATURES OF COMPUTER NETWORK

1) THEY FACILITATE RESOURCE SHARING

The primary use of a network is to share the resources. It helps in sharing the location regardless of the physical location of the devices.

2) THEY REDUCE COST OF COMMUNICATION

They reduce the cost of communication as more devices connect the cost of communicating data cuts down.

3) THEY ENSURE SCALABILITY

WHAT IS SCALABILITY?

Scalability refers to the capacity of something to change its size.

Scalability ensures that new device or computer can be added so that it is feasible both in terms of cost and effort in future.

4) REDUCE REDUNDANCY OF DATA

WHAT IS CALLED REDUNDANCY IN COMPUTER SCIENCE?

It is the duplication of data. Networks reduce the duplication of data by sharing the resources so that we can easily find the duplicates.

5) INCREASES RELIABILITY OF DATA

The data can be stored in a different device so that the data stored is backed up in a different device reducing the chance of losing the data when hardware fails.

TYPES OF NETWORKS

The networks can be classified into many heads depending upon how we classify them. They can be classified on the basis of geographical spread, the purpose like general or specific etc. Let us classify the network on the basis of geographical spread.

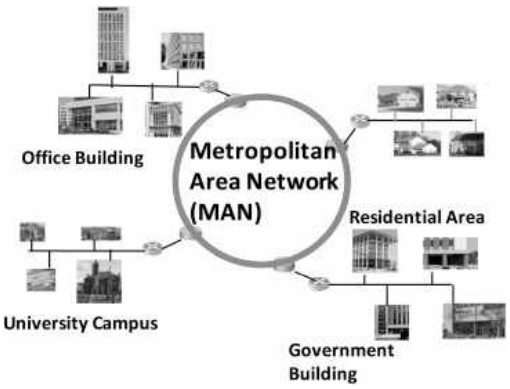
PAN- PERSONAL AREA NETWORK

- These are the smallest networks that have connectivity range up to 10 m.
- It is typically used for personal purposes.
- It can provide data transmission between mobiles, computers, computer peripherals and personal digital assistants.
- Some of the wired PAN includes USB and thunderbolt.
- Some of the wireless PAN includes infrared and Bluetooth.

LAN- LOCAL AREA NETWORK

- A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home.
- A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school. It can also be a group of buildings.

- Regardless of size, a LAN's single defining characteristic is that it connects devices that are in a single, limited area.
- It usually consists at least two computers.
- When the connection is wireless, it is called WLAN (Wireless LAN)
- The common wired connections include hardware like Twisted pair cable, hub, and network adapters (NIC).



MAN- METROPOLITAN AREA NETWORK

- It is a collection of devices which are interconnected in the range larger than the LAN. Here, it covers the size of a metropolitan city or group of cities. I.e., interconnected LANs in group of cities is known as MAN.
- The owner of the MAN who can access the data of the network is usually a single entity of the government or an organisation. This entity is called the **Service Provider**.
- The speed of the network is moderate to high since there can be more traffic and data collisions.
- They facilitate sharing of regional resources.
- Examples of MAN are Cable TV, Local telephone network and Wi-MAX.

WAN- WIDE AREA NETWORK

- It is a network consisting of group of LANs and MANs. It covers a large geographical area.
- The routers connect LANs to WANs.
- They facilitate movement of resources to many computers cutting the cost.
- Internet is an example of WAN. In fact, internet is the largest WAN in the world.
- Since the number of nodes are high, the data speed is low because of network congestion.
- It is one of the complex networks.
- The satellite communication is used in WANs.

COMPONENTS OF A COMPUTER NETWORK:

1) HOSTS OR NODES:

It is a computer or any other device that is connected to a network and shares (or seeks to share) its resources to other computer.

2) SERVERS

Servers are computers that hold shared files, programs, and the network operating system. Servers provide access to network resources to all the users of the network.

3) CLIENTS

Clients are computers that access and use the network and shared network resources. Client computers are basically the customers(users) of the network, as they request and receive services from the servers.

4) TRANSMISSION MEDIA/ COMMUNICATION CHANNELS

The medium through which the nodes interact and communicate with each other is known as a transmission media or communication channel.

5) CONNECTING NETWORK DEVICES OR HARDWARE

NETWORKING HARDWARE, also known as NETWORK equipment or computer NETWORKING DEVICES, are electronic DEVICES which are needed for communication and interaction between DEVICES on a computer NETWORK.

6) NETWORK SOFTWARE

Set of software helping devices in the network to share information with each other is known as a network software. NETWORK SOFTWARE encompasses a broad range of SOFTWARE used for design, implementation, and operation and monitoring of computer NETWORKS.

HISTORY OR EVOLUTION OF NETWORKS

ARPANET- THE FIRST NETWORK FOR BASIS OF INTERNET

ARPA NET: **A**dvanced **R**esearch **P**roject **A**gency **NET**work

Designed By: ARPA and then handed over to Defence communication agency.

Year: 1969

Connections: Computers of few universities and then used by US defence communication agency

NSFNET- THE INTELLECTUAL LEAP.

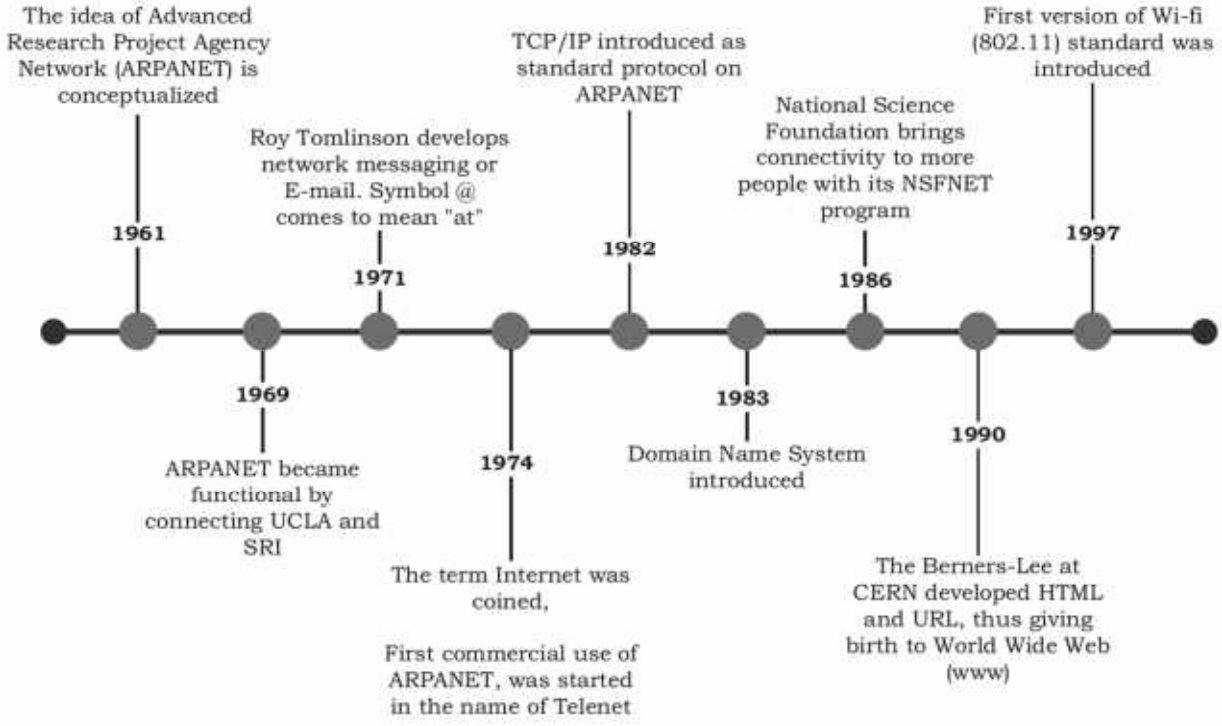
NSFNET (**N**ational **S**cience **F**ederation **NET**work) created a new network which was more capable than ARPANET and became the first backbone infrastructure for the commercial public Internet. Its main aim was to use network only for academic research and not for any kind of private business activity. Later, many privately owned businesses with their very own private systems joined with ARPANET and NSFNET to make more capable and wider network, the Internet.

So, **ARPANET + NSFNET + Private networks= Internet**

THE INTERNET

Interconnected network of networks forms the internet.

The **Internet** is the global system of interconnected computer networks that uses the Internet protocol suite (TCP/IP) to communicate between networks and devices. Millions of domestic, business and government networks are connected with each other for the purpose of sharing files, data, email, etc. They are not directly connected rather they are connected through gateways.



HOW DOES THE INTERNET WORK?

Internet is a global collection of networks, both big and small. These networks connect together in many different ways to form the single entity known as internet.

INTERSPACE

It is a client server program allowing users to communicate through internet. It is also an application environment for interconnecting spaces to manipulating information over networks.

SENDING DATA ACROSS NETWORKS USING SWITCHING TECHNIQUES

WHAT IS SWITCHING?

Network switching is the process of directing data received from any number of input ports to another designated port that will transmit the data to its desired destination.

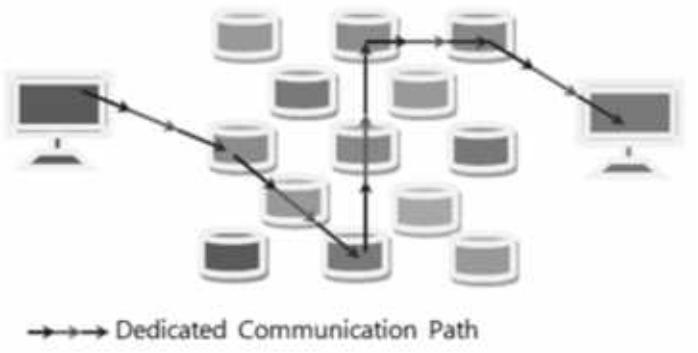
TYPES OF SWITCHING

There are two Types of Switching namely

1) Circuit Switching 2) Packet Switching

CIRCUIT SWITCHING

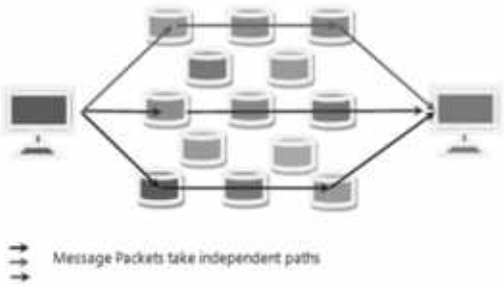
Figure 1: Circuit switching



Circuit switching is defined as the establishment of a dedicated communication path between the two parties, or nodes, within a physical network. This path (circuit) is established and maintained for the duration of the session. No matter the length of the communication session, the circuit will remain, and the data paths maintained. The circuit is only terminated when the session ends. The session consists of three phases: circuit establishment, data transfer, and circuit termination/disconnect.

1) A request signal is sent by the sender to set up the connection with the receiver. It establishes a physical connection between the two participants.
2) All intermediate nodes are identified. These nodes are also called switching nodes.
3) If the destination node is available, it sends back the acknowledgement of receiving a signal. Hence, data transmission begins.
4) When the data transmission is complete, the call can be terminated.

PACKET SWITCHING



Packet switching is defined as the process of breaking down messages into small components, called packets. Switching information (source and destination) is then included in the header information of the packet. Each packet then independently navigates its way using the information, through the network to its destination.

MESSAGE SWITCHING

It is the mode of data transmission in which a message is sent as a complete unit and switched via number of intermediate nodes which stores the data as a buffer and then forwarded towards destination host.

To note:

1) Entire message is sent. No breakdown of messages
2) The message is stored and forwarded to the nearby hosts until the message reaches the destination hosts.
3) Has increases access time.
4) There is no direct link btw sender and receiver.

CIRCUIT AND PACKET SWITCHING ADVANTAGES AND DISADVANTAGES

Circuit Switching	Packet Switching

Advantages	Disadvantages	Advantages	Disadvantages
No need for complex paths	Resources(the available bandwidth) are not fully utilised	Delay in delivery of packets is less	Needs complex protocols
No network congestion over a line. Suitable for long period continuous transmission	Not suitable except calls	Many connections can be established	High-volume networks can lose data packets during high-traffic times.
Dedicated line for communication	Set up time is long	Efficient usage of bandwidth	The data sent may be vulnerable to security issues.
Less chance of retransmission of data than packet switching.	A dedicated connection makes it impossible to transmit other data even if the channel is free.	Data delivery can continue even if some parts of the network faces link failure.	

DATA COMMUNICATION TERMINOLOGY

BANDWIDTH

Bandwidth refers to the capacity of a transmitting media to carry the signals across a connection during a certain period of time.

Measurement Unit: 1) Bits per second [In case of digital media]

2) Hz [In case of analogue media]

UNITS

For Frequency

Frequency	No of Cycles per second	Exp
HZ- Hertz	1	10^0 Hz
KHz- Kilo Hertz	1,000	10^3 Hz
MHz- Mega Hertz	10,00,000	10^6 Hz
Ghz- Giga Hertz	100,00,00,000	10^9 Hz
Thz- Tera Hertz	10,00,00,00,00,000	10^{12} Hz

for Data transmission rate

Data rate	Abbreviation	Equivalent
Bit per second	bps	-
Bytes per second	Bps	8 bps
Kilobits per second	Kbps	1000 bps / 10^3 bps
Megabits per second	Mbps	1000000 bps / 10^6 bps
Gigabits per second	Gbps	1000000000 bps / 10^9 bps
Terabits per second	Tbps	1000000000000 bps / 10^{12} bps

CHANNEL

A **channel** is a communication medium, the path that data takes from source to destination.

BAUD

The number of times that a signal changes per second is known as **Baud.** It is measuring rate of data speed.

SIGNAL

A **signal** is an electrical or electromagnetic current that is used for carrying data from one device or **network** to another.

DATA

Data is the entity which is processed and stored in the computer.

TRANSMISSION MEDIA

Pathway that can transmit information from a sender to a receiver.

DATA TRANSMISSION RATE OR THROUGHPUT

The **data transmission rate** is the volume of **data transmitted** over a **transmission** channel within a specified unit of time.

NOISE

Noise is the **unwanted signal** which interferes with the original message signal and corrupts the parameters of the message signal.

THE PHYSICAL LAYER-TRANSMISSION MEDIA, NETWORK DEVICE AND TOPOLOGIES

The purpose of the physical layer is to transport bits from one machine to another.

TRANSMISSION MEDIA OR THE COMMUNICATION CHANNEL

Transmission media is divided into two:

1) Guided Media 2) Unguided Media

1) GUIDED/BOUNDED/WIRED MEDIA

- It is the physical medium trough which signals are transmitted.
- Here, **Physical medium** like wires and cables are used.
- The data is secure since data is oriented towards the intended nodes.
- Used for **point-to-point** communication.
- Has higher transmission rate than the unguided media.

Some of the Guided media

TWISTED PAIR CABLE

- Transmits data **electrically.**
- Has pairs of cable. Each pair makes a **circuit** that can transmit data.
- Typically has 4 pairs.

WHY IS EACH PAIR TWISTED?

As electricity flows through a media, it produces electrical magnetic field. It may produce **noise.** A twisted pair nullifies by creating opposite magnetic forces.

TYPES OF TWISTED PAIR CABLE:

1) Unshielded Twisted Pair (UTP) 2) Shielded Twisted Pair (STP)

1) UNSHIELDED TWISTED PAIR (UTP)

Here, Each **Eight** individual wire (i.e., **Four pairs**) is insulated by an insulating material and twisted out. They are covered by an outer jacket.

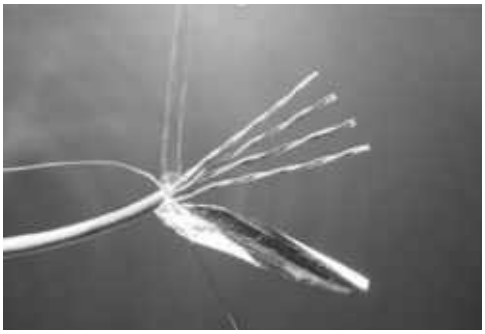
Some of the features of UTP:

- Its cost is less i.e. It is **cheap.**
- **More prone to EMI** (Electro Magnetic Interference)
- **Grounding** is **not** required.

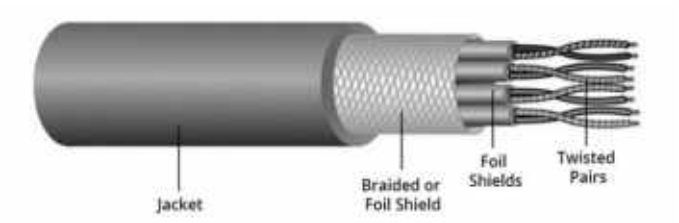
If they are insulated by a twisted material, why is it called unshielded Twisted Pair?

These cables are **more prone** to **Electromagnetic interference** than Shielded Twisted pair cables.

2) SHIELDED TWISTED PAIR (STP)



Here, each individual wire is insulated by an insulating material, twisted out. They have an extra layer of protection that has thick wires (overall shield) and an insulator (for each pair) protecting them from EMI.



Some of the features of STP:

- It is costlier to install as well as maintain the STP.
- Needs Grounding
- Less prone to EMI

ADVANTAGES AND DISADVANTAGES OF USING TWISTED PAIR CABLE

ADVANTAGES

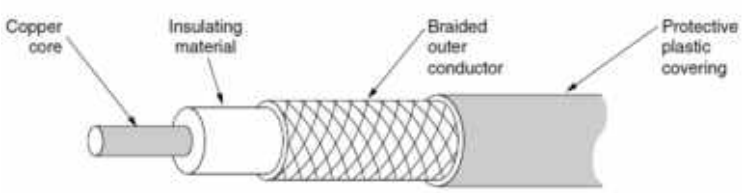
1) The cost of twisted pair cable is low, it has low weight, and it is flexible.
2) Since it is flexible, it is easy to install and maintain.

DISADVANTAGES

1) Apt only for short distances
2) More suspectable to induced EMI's.

COAXIAL CABLE OR COAX

- Transmits data **Electrically.**
- Has 4 parts
  1) The Outer Plastic covering for protecting against the weather.
  2) The braided outer conductor acting as a **return signal** agent as well as a protector against external noise or signal leak.
  3) Insulating material (dielectric insulator)for reducing signal loss and noises.
  4) Copper core for conducting the signal



ADVANTAGES OF COAX

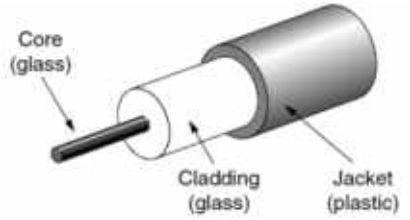
1) Can carry signals over longer distances.
2) Offers higher bandwidth.
3) Less prone to EMI

DISADVANTAGES OF COAX

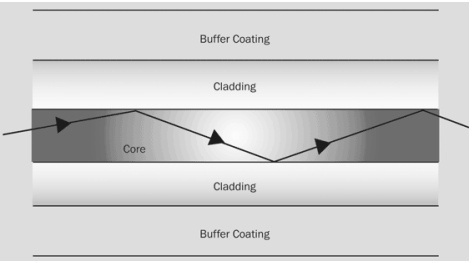
1) It is stiff and hence it is less flexible.
2) It is difficult to install.
3) To limit interference, endpoints need to be grounded.
4) They are bulky.

FIBRE-OPTIC CABLE

- Transmits data using **lights.**
- Uses **optical fibres made of glass** rather than metals.



- Has mainly three parts



1) Core

It carries the light and is typically made of glass.

2) Cladding

It is a layer that has low refractive index causing internal reflection.

3) Jacket and Coating

It is a layer that protects the cladding and the core from shocks, moisture, and corrosive environments.

ADVANTAGES OF OFC

1) Free from EMI
2) Offers higher bandwidth.
3) Secure since there are less chances of signal leak.
4) No risk of getting electric shocks.
5) Longer lifespan of wire
6) Less signal degradation

DISADVANTAGES OF OFC

1) It is quite expensive.
2) Two cables cannot be joined.
3) Additional hardware is required.
4) Wires are fragile so we cannot bend it too much.

WHICH OF THESE THREE IS APT?

Factor	Twisted Pair	Coax	OFC
Data speed	Up to 10Gbps (Depends upon type)	Up to 10 Mbps	Can be greater than 100 Gbps too. (record of 255 Tbps)
Distances	Shortest (Up to 100m)	Up to 500m	10 km and few up to 100 km
Cost	Cheapest	Costlier than twisted pair	Costliest for short distances but can be efficient over long distances

2) UNGUIDED OR WIRELESS MEDIA

- The signal gets transmitted without a physical medium.
- The data is not secure since the signal propagates without any physical media. The media is the air which can be eavesdropped.
- Communication is not point to point. It is range based communication.
- Transmission rate may degrade due to many factors like distance, objects, weather etc.
- Mainly uses **Electromagnetic Spectrums.**

Some of the unguided media

RADIO WAVES

- Radio waves are part of Electromagnetic spectrums that has highest wavelength and lowest frequency.
- They have frequency between 3 KHz (wavelength of 10 Km) and 3 GHz (10 Cm)
- They are omnidirectional (Travel in all directions)

ADVANTAGES OF RADIO WAVES

- Signals can be passed to longer distances at a good speed.
- Being omnidirectional, it is useful.
- They penetrate solid walls of buildings.
- They are cheaper for long distance communication.

DISADVANTAGES OF RADIO WAVES

- The signals sent are prone to weather effects causing degradation.
- The signals sent are unsecure.

MICROWAVES

- Has frequency more than 3 GHz but less than 300 GHz.
- It has line of sight communication.

- It has lower wavelength than the radio waves and hence have more frequency.

ADVANTAGES OF MICROWAVES

- Can be used for point-to-point communication.
- Higher data rates
- Smaller antenna due to higher frequency

DISADVANTAGES OF MICROWAVES

- Cost of installing towers is high.
- Uses more power than radio waves.
- More suspectable to EMI than Radio waves
- Water absorbs these frequencies hence microwave propagation is affected during storms, rain etc.

INFRARED WAVES

- They are used for short range communication.
- They have frequency between 300 GHz to 400 THz.
- They have Line of sight communication.
- They do not cross solid objects.

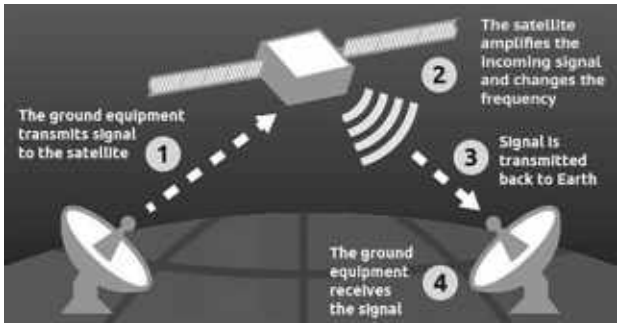
ADVANTAGES OF INFRARED WAVES

- Line of Sight communication (Good as well as bad)
- Good for short distances communication

DISADVANTAGES OF INFRARED WAVES

- Line of Sight communication
- Do not cross walls and solid objects.
- Performance degrades as distance rises.

SATELLITE LINK



- Uses Microwaves typically of frequency 1.5 GHz to 20 GHz.
- Satellite links are used to provide communications over exceptionally large distances (global coverage).
- This is achieved by using the satellite as a repeater.
- A ground station relays a signal up to the satellite at a frequency known as the **uplink frequency**.
- The satellite receives this signal and re-broadcasts it on a **downlink frequency** to another ground station.

ADVANTAGES OF USING SATELLITES

- Covers large geographical area.
- Good and consistent quality of signals
- No line-of-sight constraints (no problem of mountains, buildings etc)
- The earth stations (both sender and receiver) can be kept mobile.
- The cost of ground stations can be cut.

DISADVANTAGES OF USING SATELLITES

- Manufacturing and sending satellites to the orbit **costs huge**.
- The maintenance is complex.
- The speed of communication is slower than normal microwave transmission since signal has to travel to a long distance, needs to be regenerated and then needs to be received.
- Acquiring legal permissions is costly and tough.
- It is subjective to constraint of external interferences.

NETWORK DEVICES

To see what a network device is, see components of a computer network. Some of the network devices are

MODEM

A MODEM (Modulator DE-Modulator) is an electronic device that enables a computer to transmit data over telephone lines. The **modulator** part of the modem converts digital signals to analogue signals, and the **demodulator** part converts analogue signals to digital signals.

TYPES OF MODEM

Modems can be classified on basis of **location**: internal or external, **direction** of sending data, data bits handling capability: synchronous and asynchronous etc. Let us see the first 2 types.

LOCATION

INTERNAL MODEM

A modem connected using PCI express in the motherboard is called internal modem. It does not need external power supply since PCI provides electricity for it. Internal modem does not have indicators and hence we cannot find whether connection is established or not unless we boot up the pc.

EXTERNAL MODEM

An external modem is a standalone modem that does not contain a router. It is an explicit hardware which needs power source from adapters. It may have indicators regarding the status of the connection.

COMBO OF MODEM AND ROUTER

A router/modem combo is a modem that is contained within a router, which allows multiple computers /devices to connect within one network. It is quite common to see them nowadays.

DIRECTION OF SENDING DATA

HALF DUPLEX MODEM

These are the modems which are capable to send and receive signals in **both directions but only one at a time.**

FULL DUPLEX MODEM

These are the modems capable of transmitting signals in both directions simultaneously. They make use of two carrier frequencies (one for each direction).

RJ-45 CONNECTOR

A registered jack (RJ) is a standardized physical network interface for connecting telecommunications or data equipment.

- It has 8 pins.
- Used in connecting LANs particularly the ethernet.
- Also known as a data jack
- It is similar to a telephone jack but is wider.
- It is used commonly in Unshielded twisted pair cables.

ETHERNET CARD OR WIRED NIC

NIC- NETWORK INTERFACE CARD

It is a hardware component that connects a computer to a computer network. The card has a permanent address (called a **MAC (Media Access Control) Address**).

ETHERNET CARD

As a connection can be wired as well as wireless, the hardware component that enables a computer to connect to other computers or internet through guided media is known as an ethernet card.

WIFI CARD

It is a card connecting a computer to a computer network trough wireless media is known as a Wi-Fi card.

ROUTER

- Router is a hardware that forwards data packets between two networks so that the data packets reach the destination in the most efficient path. However, the process done by router comes under network layer (layer concerned with getting packets from the source all the way to the destination).
- A router **regulates data** over two **similar networks.**
- Works along IP Addresses

SWITCH

- A network switch is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device.
  Do you know?
  The switch does not accept corrupted signals, it asks the sender to resend the signal.
- A switch **creates** a network.
- Works along MAC addresses

GATEWAY

A gateway is a piece of networking hardware used in telecommunications for telecommunications networks that allows data to flow from **one discrete network to another.**
It is a key access point that acts as a "gate" between an organisation's network and the outside world of the Internet.

- Gateway forms a passage **between two different networks.**
- Converts protocols which are between two networks.

HUB

A hub is the most basic networking device that connects multiple computers or other network devices together. Unlike a network switch or router, a network hub has no routing tables or intelligence on where to send information and broadcasts all network data across each connection.

- Connects multiple computers.
- It sends the received data to all of its computers **(broadcast)** hence does not require any addresses like IP or MAC.

NETWORK TOPOLOGIES

The layout pattern of the interconnections between computers in a network is called **network topology**. Or, **Network topology** is the way a network is arranged, including the physical or logical description of how links and nodes are set up to relate to each other.

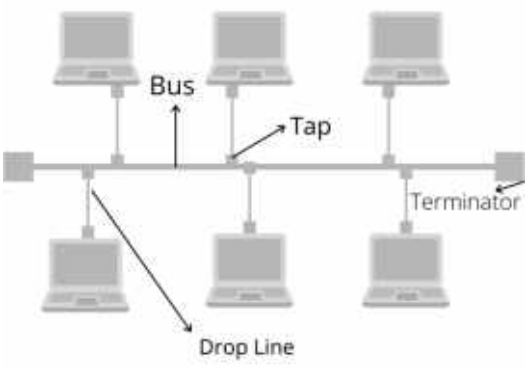
In least and simple words, it is the way of connecting several nodes with each other on a network.

PHYSICAL AND LOGICAL TOPOLOGY

- A **physical topology** describes how network devices are **physically** connected - in other words, how devices are actually plugged into each other.
- A **logical topology** describes how network devices **appear** to be connected to each other.

BUS TOPOLOGY

- It is a network topology where all nodes are connected by a single backbone cable called a **bus.**
- The line connecting the node to the bus cable is known as the **Drop Cable.**
- The connector of Bus and the Drop is known as a **Tap.**
- At end of the bus, there is a device called **terminator** to terminate the signals so that signals do not reflect back to the bus.
- The data is sent to every node, if the address does not match the address, packet is ignored.



ADVANTAGES OF BUS TOPOLOGY

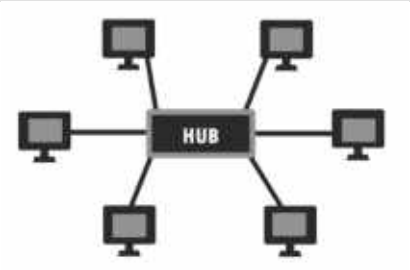
- It is cheaper to install since the cables required are quite less.
- Works well in small networks
- Up to certain limit, nodes can be easily added.

DISADVANTAGES OF BUS TOPOLOGY

- As more devices connect, they get prone to data collision.
- As more devices connect, the performance degrades.
- If main cable fails, the whole network collapses.
- Each node receives the data. So, it poses a data security risk.
- It is difficult to identify the faults in nodes if any.

STAR TOPOLOGY

- It is a network topology where all nodes are centrally connected to a device called a **hub**.
- Each device that needs to share data sends data to the hub and then hub **broadcasts** the data to all devices. The intended recipient accepts the data received and all other nodes ignore the data. Thus, all the devices are **indirectly connected** with each other.



ADVANTAGES OF STAR TOPOLOGY

- It is easier to locate the faults in nodes or wires connecting nodes since each node is independently connected to hub.
- The data transfer rate is good since all data is transferred trough a central hub.
- The data collision chances are lower.
- It needs fewer wires than mesh topology (topology where all nodes are connected to each other with independent wires).
- Problem in one node does not affect the whole network.

DISADVANTAGES OF STAR TOPOLOGY

- An extra hardware is required (The hub)
- Since the hub **broadcasts** data, the data security is compromised. (This can be solved by using switches rather than the hubs)
- Problem in hub disrupts the entire network.
- Needs more wiring than bus topology hence cost rises.

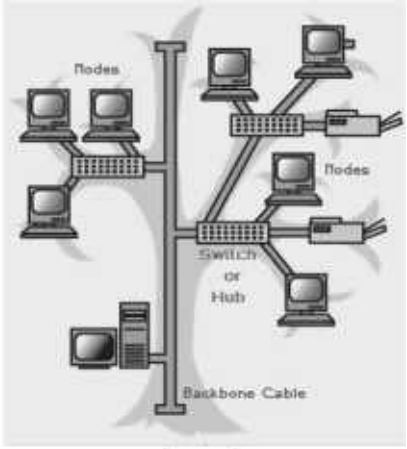
TREE TOPOLOGY

- Other names of this topology are **Star-Bus Topology and Parent-Child Topology.**
- It is a **hybrid** version of star topology and bus topology.
- Here, nodes are connected to switches or hubs. The nodes are then connected to the hubs or switches.
- Usually in tree topology, switches are preferred over hubs since broadcasting is not desirable in tree topology.

ADVANTAGES OF TREE TOPOLOGY

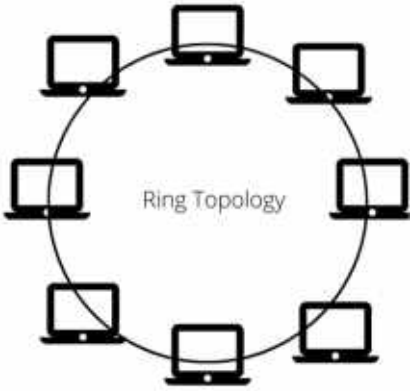
- Fault identification is easier.
- A problem in one node does not affect the other.
- It is scalable and flexible to add extra nodes.
- It is useful in areas where bus and star topologies cannot be implemented individually.
- If direct link to a node is required, we can connect a node directly rather than using a switch (Useful for server placement)

DISADVANTAGES OF TREE TOPOLOGY



- It is quite complex to implement upon
- It needs several external hardware like switch or hubs.
- If bus fails, network shuts down.
- If switch or hub fails, the children's network is disrupted.
- Data security can be compromised if switches are hampered. If hubs are used, data security is doubtful.
- Even if it is scalable, if network's size is large, it is tough to manage. The data speed decreases.

RING TOPOLOGY



- It is a topology where nodes are connected in a circular path.
- Each node connects itself to two other nodes (Typically adjacent nodes)
- Data packets travel from one node to another, then the node forwards the data packets to another node until the intended recipient node receives the information.
- The ring topology is classified into **Unidirectional and Bidirectional Ring topology.**
- In unidirectional ring topology, data packets are sent only in one direction.
- In bidirectional ring topology, data packets are sent in both directions.
- In bidirectional ring topology, if data packets are duplicated, TCP/IP would detect them and ignore the duplicate data packets.
- Usually, unidirectional ring topology are used.

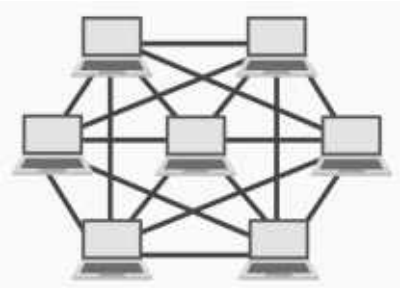
ADVANTAGES OF RING TOPOLOGY

- As data is passed typically unidirectionally, data collision is reduced.
- No separate network hardware is required.
- The transmission rate is increased.
- Fault identification is easy.
- Ring network is less costly.
- Adding nodes is easy.
- It is relatively cheaper than mesh and tree topology.

DISADVANTAGES OF RING TOPOLOGY

- Fault in nodes can disrupt the whole network.
- As number of nodes increases, data speed falls.
- If one cable has an issue, entire system fails.
- Data passes through each node.

MESH TOPOLOGY



- It is a topology where all nodes are connected to each other .
- There is a point-to-point communication.
- The data is sent to the node without any intermediate node.
- There are $\frac{n(n-1)}{2}$ links in a "**n**" number of nodes network.

HOW N(N-1)/2?

Let us recall the combination formula.

Let there be "**n"** number of items that can be selected "**r"** at a time. Then, the number of items that can occur (without considering the order) is ${}^{n}C_{r} = \frac{n!}{(n-r)!\,r!}$ Where "!" means multiply recursively the predecessors until it gets to one.

i.e., n! = n* (n-1) * (n-2) * (n-3) ……*3*2*1

- Here, a link can connect **two** nodes, hence r=2.

- Applying r=2, we get ${}^{n}C_2 = \frac{n!}{(n-2)!\,2}$, we can write n! as n*(n-1) (n-2)!

  We get $\frac{n*(n-1)*\cancel{(n-2)!}}{\cancel{(n-2)!}\,2} = \frac{n(n-1)}{2}$

ADVANTAGES OF MESH TOPOLOGY

- Owing to dedicated link, the traffic is less.
- A failure in one link or node does not affect the whole network.
- Data is security is good since there are no intermediates between the data transmission.
- Mode nodes can be added without disturbing the other nodes.
- Faults can be easily detected.

DISADVANTAGES OF MESH TOPOLOGY

- The wiring is quite complex and can incur great cost.
- To add a new node, many wires are needed hence scalability is doubtful.
- Maintenance of this type of network is tough.
- The number of ports for connecting might be inadequate, in many times external hardware is required.

NETWORK PROTOCOLS

WHAT IS A PROTOCOL?

It is a system of rules that allow two or more devices to transmit data with each other. These rules include what type of data is transmitted, how data transfers are confirmed, how data is transmitted etc.

PROTOCOLS THAT ARE COMMONLY USED IN NETWORKING

Some of the protocols that are used in networking are **TCP/IP, FTP, PPP, HTTP, SMTP, POP3, Telnet,** and other mobile communication protocols like **GSM, GPRS and WLL.**

TCP/IP- TRANSMISSION CONTROL PROTOCOL/ INTERNET PROTOCOL

It is a combination of two separate protocols which are widely used. The TCP compliments the IP hence the entire suite is referred as TCP/IP.

TCP

- It is the most widely used protocol for communication.
- It establishes connection between hosts and then maintains the connection.
- It checks for errors during transmission. It filters out the duplicate data which is received.
- Comes under **Transmission Layer** in OSI model

IP

- It is the supplement of TCP.
- It delivers packets from source host to destination host based on the **IP Addresses** which are enclosed in data packets.
- It can also deliver data from source host to destination host by routing through various addresses.
- There are two major versions of IP, namely **IP v4** and **IP v6**.
- The IP comes under the **Network Layer** in OSI model.

FTP- FILE TRANSFER PROTOCOL

- It is standard protocol to transfer files from a server to a client over the **TCP/IP**. It is the protocol that severs, and client use to transfer files from one to each other on a TCP/IP.
- This protocol also allows to upload data into the **FTP-Server**. The software used to upload or modify data to an FTP- server is known as **FTP-Client.**
- The server uses port 20 and 21 for communication.
- The protocol is not designed to be secure. It is suspectable to brute force attacks, packet capturing etc.
- It comes under **Application Layer in** OSI model.

WHY FTP IS IN APPLICATION LAYER?

- The FTP enables the user to remotely access the files in a server over the TCP/IP.
- The FTP enables the practical use of the TCP/IP (coming under transmission and network layer).

PPP- POINT TO POINT PROTOCOL

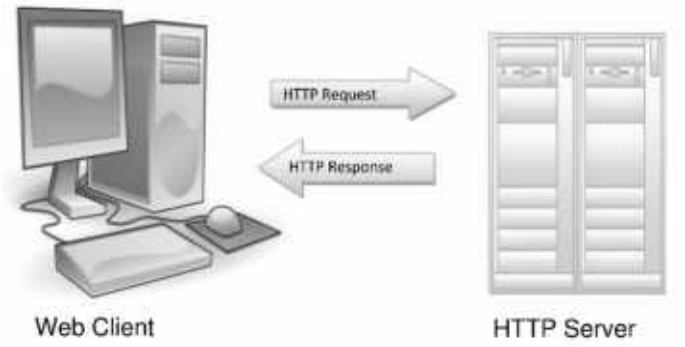
- It is a protocol for point-to-point communication. i.e., There are no nodes in between the connection.
- This protocol offers connection authentication, encryption during transmission.
- The PPP defines format of frames through which the transmission occurs.
- It establishes the link between the nodes.
- It encapsulates the other protocols.
- Comes under the **Data Link Layer.**

PPP AROUND US

1) PPP connects the modem to the server of ISP. When this connection is made through ethernet, it is called PPPoE (Point to Point Protocol over Ethernet). Even nowadays it is used widely.
2) Commonly used in Dial up connections

HTTP- HYPER TEXT TRANSFER PROTOCOL

- It is a protocol for interacting with web resources by transmitting hypertext messages. Its primary function is to establish a connection with the server and send HTML pages back to the user's browser.
- It allows users to transmit data over the world wide web.
- It uses IP suite to transmit data.



- HTTP functions as a request–response protocol in the client–server computing model. The request made is called HTTP request and the response given by server is known as http response. The response may be positive or negative. Like 1xx- under process, 2xx- successful 3xx-redirection ,4xx- Client error, 5xx- Server-side error.
- This protocol uses the port **80**.
- It is an **Application Layer** protocol.

SMTP- SIMPLE MAIL TRANSFER PROTOCOL

- It is a communication protocol for **Email transmission.**
- Mail servers and other transfer agents rely on this protocol for email transmission.
- It works closely with the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox.
- This protocol **facilitates** the **transmission and delivery of messages** to destination hosts.

- It is to be noted that the email, which is to be transmitted, arrives to the mail server and not the person directly.
- It is an **Application Layer** Protocol
- The SMTP can facilitate transmission of text messages only.
- Nowadays, Extended Simple Mail Transfer Protocol (ESMTP) is used, and it allows multimedia files to be transmitted through emails.

POP- POST OFFICE PROTOCOL

- It is a protocol for retrieving messages from email server to local computer.
- It downloads the messages from the Mail server's storage and saves them in local storage of the computer.
- It does not allow more than one simultaneous connection.
- As soon as the local computer gets the mails, the mails present in mail server storage gets deleted.
- The POP3 is a version of POP which is common.
- It uses the port 109 and 110.
- POP has a server which manages the authentication and manages the connection.

IMAP- INTERNET MESSAGE ACCESS PROTOCOL

- It is a protocol for retrieving messages from email server to local computer.
- IMAP allows you to access your email from any device. The emails are not actually downloaded. They are just read from email service. Unless the user manually deletes the message, the emails are stored in the server.
- IMAP only downloads a message when you click on it, and attachments are not automatically downloaded. Hence it is faster.
- It allows many devices to read emails.

TELNET

- Stands for teletype network.
- It is a remote login protocol enabling remote access to a host computer.
- A Telnet program allows a user on one system to log in to a remote system and issue commands in a command window of the remote system. So, a remote user can execute commands.
- It provides command line communication.
- However, the data sent including the remote username, host name and password are not encrypted hence has a serious security concern.

WIRELESS/ MOBILE COMMUNICATION PROTOCOLS

GSM- GLOBAL SYSTEM FOR MOBILE COMMUNICATION

- GSM is a globally accepted standard for digital cellular communications.
- It is used for transmitting voice and data services through mobiles.
- It uses TDMA for transmitting signals. The available bandwidth is given to various users on time basis (in terms of microseconds)
- Here, a SIM is needed for communication.
- The data of a customer is stored in a SIM (Subscriber Identity Module)

CDMA- CODE DIVISION MULTIPLE ACCESS

- It is a technology where users can communicate simultaneously using division of codes.
- Here, usually a device is adhered to its network and cannot be changed.
- CDMA provides better capacity for voice and data communications but is not widely used as that of GSM.
- More users can be connected than that of GSM.
- In CDMA, the signals are automatically encrypted and hence it's security against eavesdropping is strong.

GPRS- GENERAL PACKET RADIO SERVICE

- It is a service for internet access on 2g and 3g cellular communication on GSM.
- It allows to transmit IP packets to external networks.
- It offers services like SMS message and broadcast, Multimedia messaging service, always on internet access, etc.
- It has theoretical speed of 120 Kbps and in real world it has speed about 30-40 Kbps.
- It is also known as 2.5 G

WLL- WIRELESS IN LOCAL LOOP

- It is It is a technology in which the mobile network subscriber gets connected to the nearest local exchange using radio waves.
- It is the wireless link or that connects from point of the customer premises to the edge of the common carrier or service provider's network.
- It is an edge over the copper lines hence it reduces cost. But the problem is that as the distance increases, radio wave degrades.
- It is also known as Radio In The Loop (RITL) and Fixed Radio Access (FRA).
- This is based on full-duplex radio network system.

OTHER TECHNOLOGIES FOR MOBILE COMMUNICATION THE 1G,2G,3G,4G AND SO ON

1G- THE FIRST GENERATION

- It is a wireless cellular technology introduced 1890s.
- It could transmit only voice calls
- It uses analogue signals to transmit voice
- The voice data security is not good since the data is not encrypted
- It had a basic voice quality
- The devices were quite large

2G- THE SECOND GENERATION

- This wireless cellular technology came in 1991
- Primarily could communicate voice, fax ,MMS ,and SMS
- It used digital signals to transmit data. Hence call quality enhanced
- GPRS enabled wireless internet access
- It enabled more people to communicate.
- After EDGE (Enhanced Data rate for GSM Evolution) was introduced and hence data speeds rose.
- But still, the speed was inadequate to send videos.
- GPRS had speed (theoretical) of 40 Kbps and EDGE had theoretical speed of 384 Kbps.

3G- THE THIRD GENERATION

- This wireless cellular technology was introduced in late 1990's but it was commercially available only after 2001.
- It natively offered voice and data services
- It offered data speeds up to few megabits per second.
- It was the era in which the data speeds rose up rapidly.
- Many technologies were introduced to increase the data speeds.
- First, CDMA2000, UMTS etc were used giving speeds up to 2 Mbps, later HSPA (High Speed Packet Access or 3.5G) came giving theoretical speeds up to 14 Mbps, then HSPA evolved into HSPA+(3.75G) making the way to 56 Mbps.
- It made the path for video communication and other faster internet services.

4G- THE FOURTH GENERATION

- It is the technology which have peak speeds ranging from 100-1000 Mbps
- It was commercially introduced in 2009 and in India it was commercially introduced by Airtel in 2013.
- It has made wireless networking to a great level.
- 4g offers less video buffering time, higher voice quality etc.
- LTE(Long Term Evolution) is a technology which is widely used. VoLTE (Voice Over LTE) is also part of 4G which offers good voice quality and speeds.

5G- THE FIFTH GENERATION

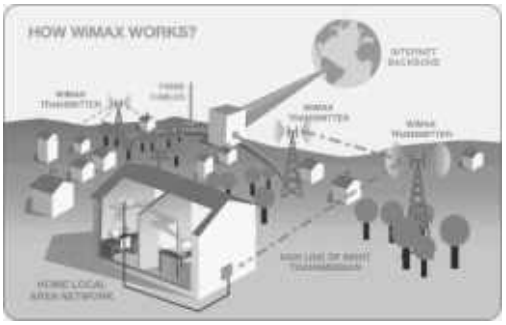
- The fifth generation or 5G is currently under development. As on 21 May 2020, Nokia has announced the highest speed of 5g offering 4.7 Gbps.
- However, the latest phones are ready to adopt 5g.
- It is expected to be a milestone development for the success of IoT and Machine to Machine (M2M) communications. Machine to machine (M2M) is direct communication between devices — wired and wireless, IOT's and so on.

OTHER WIRELESS COMMUNICATION TECHNOLOGIES- WIMAX AND WIFI

WIMAX

- It stands for **Worldwide Interoperability for Microwave Access**
- It allows users over a geographical area up to 50 Km to get access to internet without wires.
- It forms an MAN (Metropolitan area network) or a WAN (Wide area network).

HOW DOES WIMAX WORK?



- The Wi-max setup has mainly two parts
    - Wi-Max tower / the base station- It acts as a transmitter between the subscriber's area and establishes connection to the internet service provider.
    - The Wi-Max receiver or the Wi-max subscriber unit establishes link between the LAN of home, office etc and the Wi-Max tower.
- Just like a wired connection, it provides internet connection to all. But it uses wireless connection.
- Advantages are that they are scalable, have good quality of service, they are cost effective, and they are easier and faster to deploy.
- Disadvantages: It is power intensive; the cost of maintenance is high and is suspectable to weather effects.

WI-FI

- It stands for wireless fidelity.
- It uses radio waves to connect. The frequency which are commonly used are 2.4 GHz (Has 11 channels) and 5 GHz.
- It creates a wireless local area network.
- The Wi-Fi router connects the local area network to the internet.
- The area which the Wi-Fi connects is known as Wi-Fi hotspot.
- Wi-Fi repeaters are the devices which are used to repeat the radio signals hence increasing the range of Wi-Fi.

MOBILE COMMUNICATION PROCESSORS

WHAT IS A PROCESSOR?

A processor is a piece of hardware that processes the binary data and produces the output.

SOME OF THE FEATURES OF MOBILE PROCESSORS

- They are small so that they can be fitted into small devices.
- They are designed to use less power than normal processors.
- They have less speed than normal processors and are designed to dissipate less heat.
- They usually have Image Processing Unit, GPU (Graphical Processing Unit) and nowadays, they also have Neural processing unit for neural operations together known as SOC (System on a Chip)
- Common mobile processor manufacturers are Qualcomm, Exynos , Hi-silicon, Intel (Atom series and M series processor), MediaTek, Apple, Nvidia (Tegra) and Spread Trum.

SOME OF THE MOBILE PROCESSORS

QUALCOMM SNAPDRAGON

- Qualcomm is a US based company mainly known for its processor series Snapdragon.
- Snapdragon is a mobile based processor.
- As on 2021 April beginning, sd 888 is the flagship with upto 2.84 Ghz speed and an improved GPU. It is paired with enhanced ISP and supports 5G. It makes 26 TOPS (Trillion Operations Per Second). It also supports Wi-Fi 6

APPLE

Apple does not simply manufacture processors; it contracts with processor makers to build its own custom processors to suit its needs. They are SOC (System on chip) processors. “A” series is used for iPhone, iPad, and iPods. The latest one is A14 which is used in iPhone 12 series and iPad air 2020. “S” series is for apple watches. “U” series was introduced in 2019 smart devices and from iPhone 11 series to enable short field communication between apple devices.

HISILCON KIRIN

HiSilicon is a Chinese semiconductor manufacturing company owned by Huawei. It’s Kirin processors are used in Honor and Huawei’s smartphones. Kirin’s ISP is one of the best which is used in Huawei’s p30 pro.

EXYNOS BY SAMSUNG

Exynos is a brand of Samsung which is used widely. Their transistors emit less radiation compared to other transistors. They also have good reception capacity.

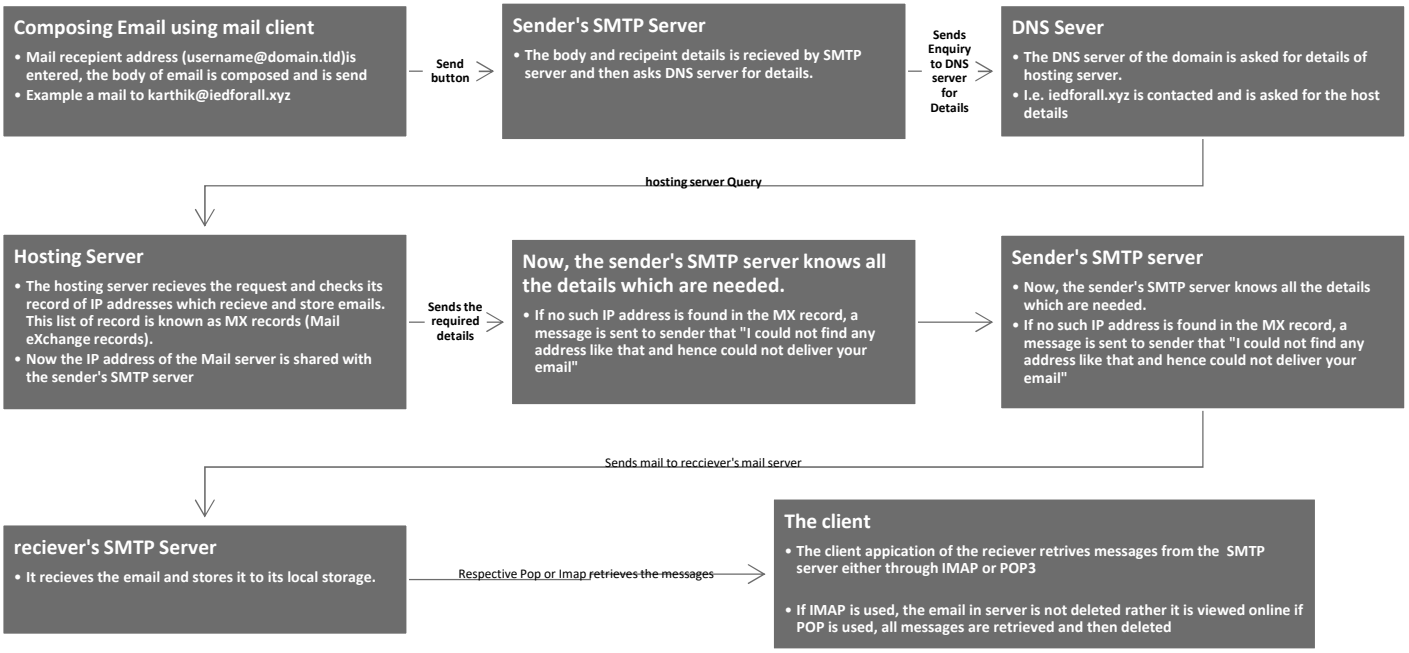
MEDIATEK

It is a Taiwanese microprocessor company that produces processor chips for TVs, smartphones and IOT devices. Its TV chips are quite popular and are widely used. The smartphone processor series is known as Helio. Th mid-range of Helio processors are little AI oriented.

INTEL

Intel is a US based processor manufacturing and designing company. It is a major player in processors except the smartphone industry. Intel Atom series is a power efficient series used for mobiles. U series is used in light laptops for power efficiency . T series is the one which use less power and deliver less performance. H series mobile processors give high graphical performance

THE WORKING OF EMAIL



CHAT AND VIDEO CONFERENCING PROTOCOLS

CHAT CONFERENCING PROTOCOLS

WHAT IS A CHAT?

It is generally a textual communication between two or many peoples.

PROTOCOLS USED FOR CHATTING

IRC- INTERNET RELAY CHAT

- Was introduced in early 1980's
- Internet Relay Chat (IRC) is an application layer protocol that facilitates communication in the form of text.
- It is based on client server architecture.
- Client sends messages to server and then server sends the message to respective client.
- It can allow more than two participants to receive a message. The channel through which more than two people can send chat is known as a room or commonly as a chat room.

XMPP-EXTENSIBLE MESSAGING AND PRESENCE PROTOCOL

- It was introduced as an open-source project.
- It could allow other protocols to be used too.
- Multimedia services are present. Many other implementations like voice calls, video calls, read responses, online status were introduced because it was an open-source project.
- WhatsApp is an example for this.

VIDEO CONFERENCING PROTOCOLS

SESSION INITIATION PROTOCOL

- It is a protocol for establishing, modifying, and terminating session-based multimedia (video or audio) conferences.
- It is an application layer protocol which works over the TCP/IP. It works well in both IPv4 and IPv6.
- It performs the following works,
    - Establishes connection between callers by inviting people and acknowledging the response of the invitees.

- Facilitates the communication between the callers and if any modification in the session is needed, it does the needful.
- Terminates the calls when needed or when the person is unreachable.

H. 323

- It is a standard for video conferencing which has components, protocols, and procedures to provide real-time multimedia sessions including the audio, video, and data transmissions over switched networks.
- It was designed by ITU (International telecommunication union)
- It is a binary protocol (sends binary data rather than text data)
- First, H323 was used to make the telephones speak through internet. Later, it was used in internet telephony, video conferencing and various video and data communications.

NETWORK SECURITY CONCEPTS

WHAT IS NETWORK SECURITY?

Network security is any activity designed to protect the usability and integrity of a network and its data.

WHY IS NETWORK SECURITY NEEDED?

- As the networks have evolved, the quantity of data that is being transferred have rose exponentially. The data which is sent may have some importance to end users.

If the data sent is breached, it can have several adverse effects. The network security is needed regardless of the business needs or personal needs.

- Network security practices are important since they can ensure that the shared data is kept safe, and the data does not fall into other's hands.
- We live in a digital era which understands that our private information is more vulnerable than ever before. We all live in a world which is networked together, from internet banking to government infrastructure, where data is stored on computers and other devices.
- A portion of that data can be sensitive information which unauthorized access or exposure could have negative consequences.

GOALS OF CYBERSECURITY

- Ensuring the confidentiality of data
- Preserving the integrity of data
- Promoting the availability of data to intended users.

A NETWORK THREAT

A threat is a potential negative action or event that results in an unwanted impact to a computer system or application. The threats can be classified to two heads.

Natural network threats Deliberate network threats

Natural security threats are those which can occur naturally. For example, equipment failure, accidental physical damage caused due to various factors, loss of power supply etc.
The deliberate security threats are those which are deliberately made to have adverse effect on a network.

SOME OF THE NETWORK SECURITY THREATS

The two major deliberate network security threats are

1) Malwares 2) Spams

MALWARES

- Malware is a short term used for MALicious softWARE.
- Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network.
- There are many types of malwares. They are classified om the basis of their ways to infect a target.
- Some of the malwares are Viruses, Worms, Trojan horses, Ransomwares, Spywares, adware and keyloggers.

VIRUSES

1) This term was coined by Fred Cohen in 1985.
2) A virus is a piece of software code created to perform malicious activities and hamper resources of a computer system like CPU time, memory, personal files, or sensitive information.
3) Virus self-replicates itself and attaches itself to a host program. As the infected program is executed, the dormant virus starts replicating and starts causing damage.
4) The first known virus is the program called “CREEPER” which simply displayed the message to user “*I'm the creeper: catch me if you can*”. Some of the viruses are CryptoLocker, ILOVEYOU, MyDoom, Sasser and Netsky, Slammer and Stuxnet
5) Viruses can be further classified some of them are
    - Boot sector viruses- Viruses that reside in boot sector of disk and gets loaded when computer boots up
    - Macro viruses- The viruses designed to replicate using macro language, which is used in text processing applications like word, excel etc.
    - File viruses- The viruses which target an executable file and then infects the computer that can cause permanent damage to a file or a file system
    - Stealth viruses- Those viruses which hides themselves after infecting a computer

WORMS

- A worm is a malware which is similar function to that of a virus, but the difference is that it is a standalone program which does not require any host to replicate itself.
- Viruses need a trigger to infect and replicate while worms do not need a trigger.
- Worms are capable of infecting hosts by themselves.
- Some prominent examples of worms include Storm Worm, Sobig, MS Blast, Code Red, Nimda and Morris Worm.

RANSOMWARE

- It is a type of malware that targets user data. It either blocks the user from accessing their own data or threatens to publish the personal data online and demands ransom payment against the same.
- The ransomwares encrypt the user’s data in a special format and can demand payment for getting back their data.
- The most common example for ransomware is the WannaCry ransomware which encrypted data and demanded the ransom in form of Bitcoin.

TROJAN

- A trojan is a malware that seems or claims to a legit software. Once installed, they can either damage the data or can provide a back door for malware to infect a computer. Or a trojan can provide backdoor access for it’s programmer to gain remote access to a computer
- The name trojan horse is from the Greek history that the ancient Greeks could not infiltrate the city of Troy using traditional warfare methods, they gifted the king of Troy with a big wooden horse with hidden soldiers inside and eventually defeated them. Hence the name of Trojan Horse was titled to programs performing in a similar manner.

- There are several trojans which are designed to perform various tasks. Some of them include DDos, identity stealing trojans, exploit kit trojans and Backdoor trojans.

ZOMBIE COMPUTER AND BOTNET

A computer is known as zombie computer if a computer has been compromised by a hacker.

SPYWARE

- It is a malware which is designed to spy and collect the information about their victims.
- They collect information without consent of their user and sends the information to external entity.
- Spyware usually tracks internet usage data and sells them to advertisers. They can also be used to track and capture credit card or bank account information, login and password information or user's personal identity.
- The common example for spywares is a keylogger.

KEYLOGGER

A keylogger is a computer program that records every keystroke made by a computer user, especially in order to gain fraudulent access to passwords and other confidential information.

A keylogger can be either a hardware or a malware. There are many implementations of hardware keyloggers. One of them is by implementing a small layer of thin transparent keyboard on the actual keyboard.

SPAM

Spam is any kind of unwanted, unsolicited digital communication, often an email, that gets sent out in bulk. These messages lead to phishing, scamming, personal identity theft etc.

These spams are one of the modes of communication of potentially unwanted programs.

MODES OF DISTRIBUTION OF MALWARES AND OTHER THREATS

The four common modes of distribution of malwares are,

1) Downloading software from unknown sources in internet
2) Spam emails
3) Removable storage medias
4) Networks

1) Downloading software from unknown sources of internet

   The internet is the archive of many files. While downloading a software, we must check it's origin and we must trust only a verified company. We must read the terms and conditions when we download a software. The freeware which seem lurky is the most common source of malware.

2) Spam emails

   The spam emails are the other sources of malware. There are many spam emails like one claiming to give freebies, proprietary paid software for free, free money etc either steal our personal information or they prompt users to install malwares in their system.

3) Removable storage medias
   The removable storage medias are capable to transfer malware from one computer to another. So the antivirus check before executing any application from them is recommended
4) Networks
   Many worms are capable to replicate themselves over networks. A network firewall can help in protecting from such malwares.

SYMPTOMS OF GETTING INFECTED BY MALWARES

- Computer runs slower than normal
- The resource usage is higher than normal and is suspicious
- The bootup time for the computer is longer than usual
- Frequent error notifications from apps or windows services
- Unknown start-up programs are present in start-up services and apps
- Files appear or disappear randomly or without your knowledge
- Change in network proxy servers and network configuration
- Frequent ads in sites asking to visit some sites (without proper ad analytics)
- Change in home page of web browsers
- Unexplained full disk usage and lack of space in hard disk
- Redirections to other sites even while browsing normally

SOME OF THE MEASURES TO PROTECT OURSELVES FROM MALWARES

- Using antiviruses and updating the system with security patches
- Using open source or legitimate licensed software rather than pirated software
- Configuring the network settings properly
- Using sandbox environment to test suspicious apps
- Not installing apps from unknown sources. Not giving administrative privileges to unknown apps
- Regularly taking backups and roll up points so that even if computer gets infected, the files can be restored
- Avoid clicking links from unknown senders
- Scan the removable media with antivirus software before executing any application from it
- Removing all unknown apps from system
- Using task manager to monitor activities and killing the unknown instances and then removing suspicious apps.

NOTE

Please note that this work is not cited. So, please do not publish it. It might become as a plagiarism. This work is taken from various sources like
1) Youtube videos
2) Video tutorials from Amazon AWS
3) Our school textbook
4) sites like geek to geek, javatpoint, study.com etc
It is also taken from books whose name i do not remember. So, please use it responsibly.
(All the images used are either licensed by me or are open source. So no issues to copy them....)