Name : Jiten Sidhpura

Date : 13/8/2020

UID : 2018130051

Data Communication and Computer Networks Lab

EXPERIMENT 1

Aim : Study of different types of physical layer wired/wireless connections

Theory :

Basics of Computer Networking

1. Open system:

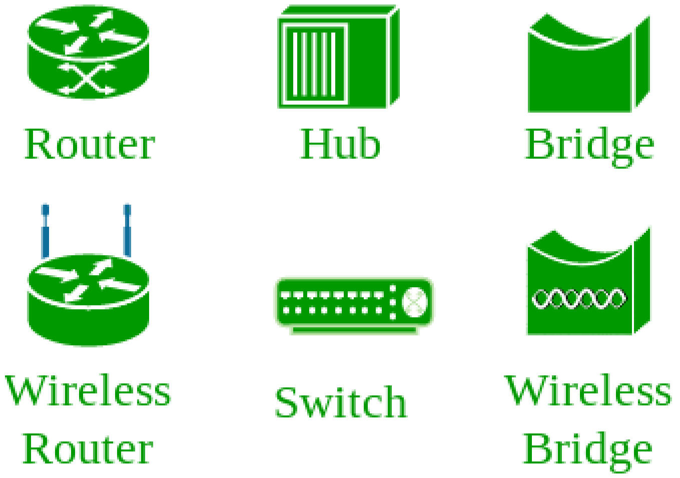
A system which is connected to the network and is ready for communication.

2. Closed system:

A system which is not connected to the network and can't be communicated with.

Computer Network:

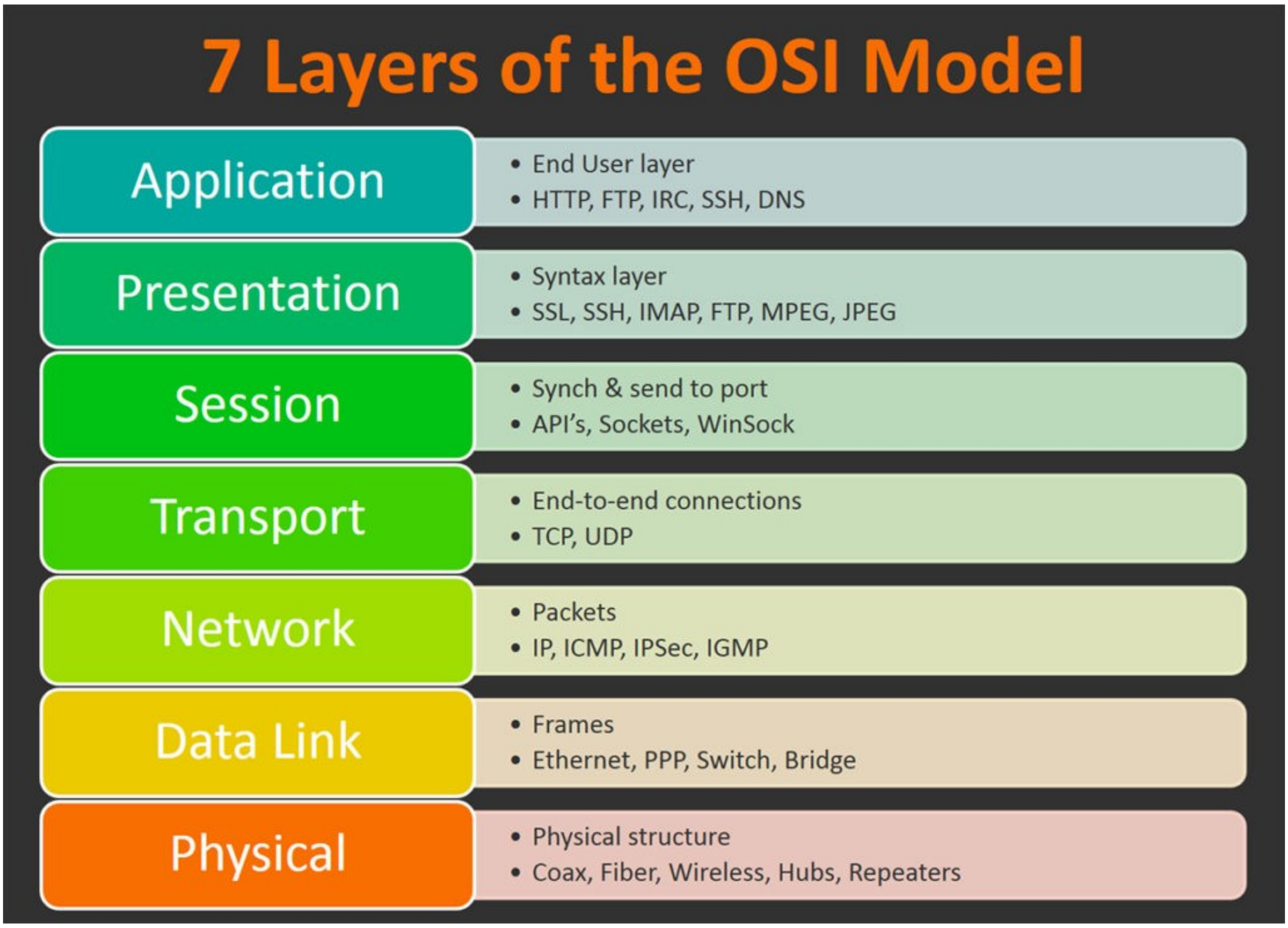
An interconnection of multiple devices, also known as hosts, that are connected using multiple paths for the purpose of sending/receiving data or media. Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as Network devices and include things such as routers, switches, hubs, and bridges.



OSI:

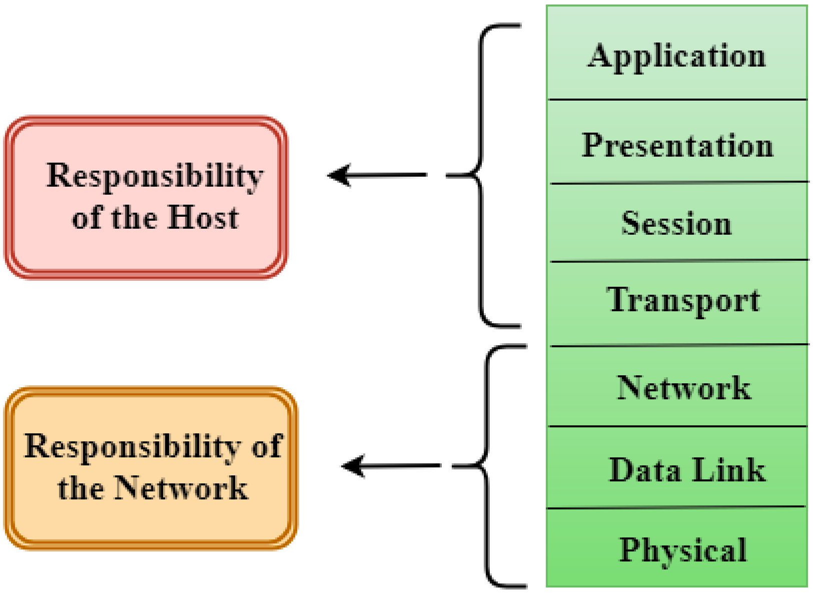
OSI stands for **Open Systems Interconnection**. It is a reference model that specifies standards for communications protocols and also the functionalities of each layer.

It has been developed by ISO – '**International Organization of Standardization**', in the year 1984. It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe. OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.Each layer is self-contained, so that task assigned to each layer can be performed independently.



7 Layers of the OSI Model

Application	• End User layer • HTTP, FTP, IRC, SSH, DNS
Presentation	• Syntax layer • SSL, SSH, IMAP, FTP, MPEG, JPEG
Session	• Synch & send to port • API's, Sockets, WinSock
Transport	• End-to-end connections • TCP, UDP
Network	• Packets • IP, ICMP, IPSec, IGMP
Data Link	• Frames • Ethernet, PPP, Switch, Bridge
Physical	• Physical structure • Coax, Fiber, Wireless, Hubs, Repeaters

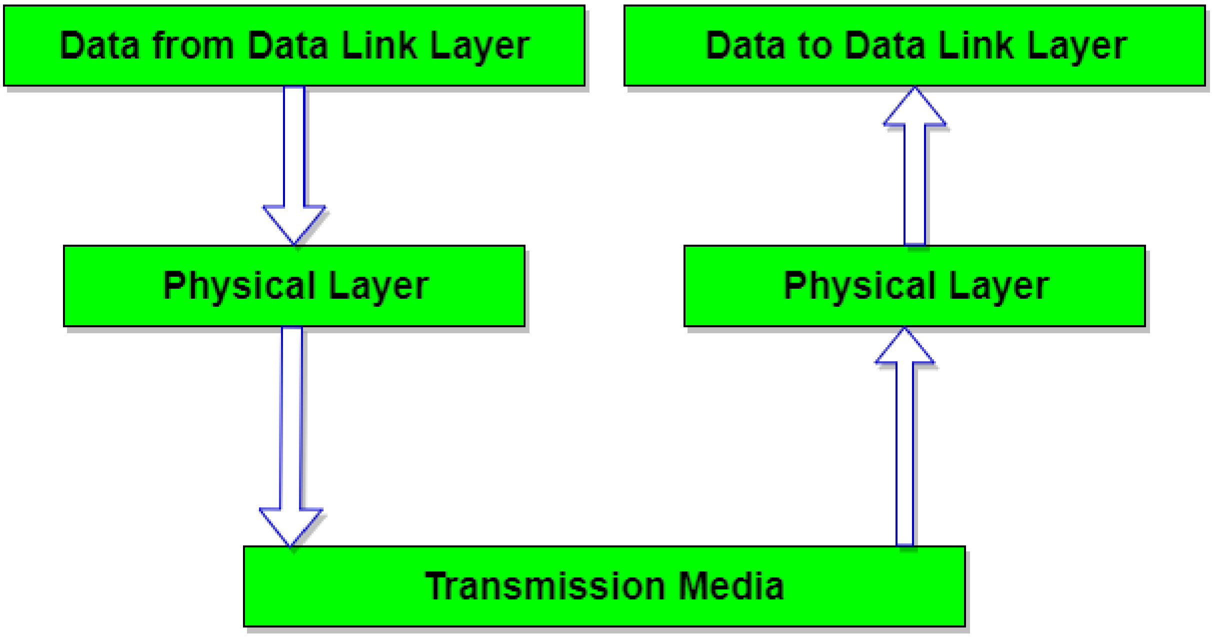


The OSI model is divided into two layers: Upper layers and Lower layers.

- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.

- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

Physical Layer:



The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits**.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

The functions of the physical layer are :

1. **Bit synchronization:**

   The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.

2. **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
3. **Physical topologies:**Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topolgy.
4. **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

The physical layer is responsible for thetransmission of a raw bit-stream over the physical medium. The transmission medium can either be wired or wireless.

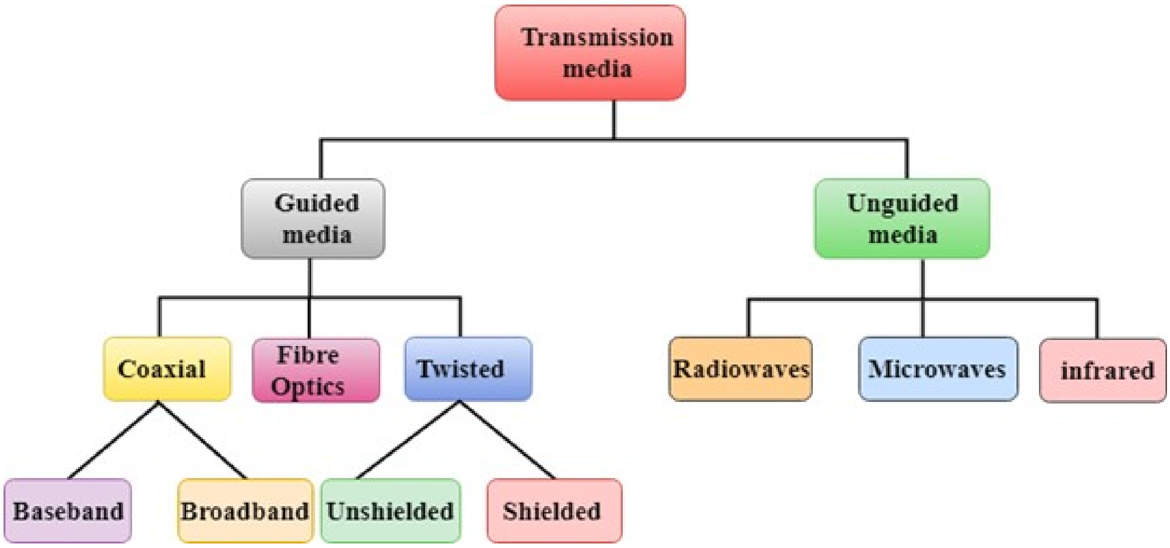
Transmission Media:

Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.

- The main functionality of the transmission media is to carry the information in the form of bits through **LAN**(Local Area Network).
- It is a physical path between transmitter and receiver in data communication.
- In a copper-based network, the bits in the form of electrical signals.
- In a fibre based network, the bits in the form of light pulses.
- In **OSI**(Open System Interconnection) phase, transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 component.
- The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum.
- The characteristics and quality of data transmission are determined by the characteristics of medium and signal.
- Transmission media is of two types are wired media and wireless media. In wired media, medium characteristics are more important whereas, in wireless media, signal characteristics are more important.
- Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.
- The transmission media is available in the lowest layer of the OSI reference model, i.e., **Physical layer.**

Types of Transmission Media:

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types:



WIRED CONNECTIONS:

Wired communication refers to the transmission of data over a wire-based communication technology. Wired communication is also known as wireline communication. Examples include telephone networks, cable television or internet access, and fiber-optic communication.Most wired networks use Ethernet cables to transfer data between connected PCs. Also waveguide (electromagnetism), used for high-power applications, is considered wired line. Local telephone networks often form the basis for wired communications and are used by both residential and business customers in the area. Many networks today rely on the use of fiber optic communication technology as a means of providing clear signaling for both inbound and outbound transmissions and are replacing copper wire transmission. Fiber optic technology is capable of accommodating far more signals than copper wiring while still maintaining the integrity of the signal over longer distances.

In general, wired communications are considered to be the most stable of all types of communications services. They are relatively impervious to adverse weather conditions in comparison to wireless communication solutions. These characteristics have allowed wired communications to remain popular even as wireless solutions have continued to advance.

Coaxial cable:

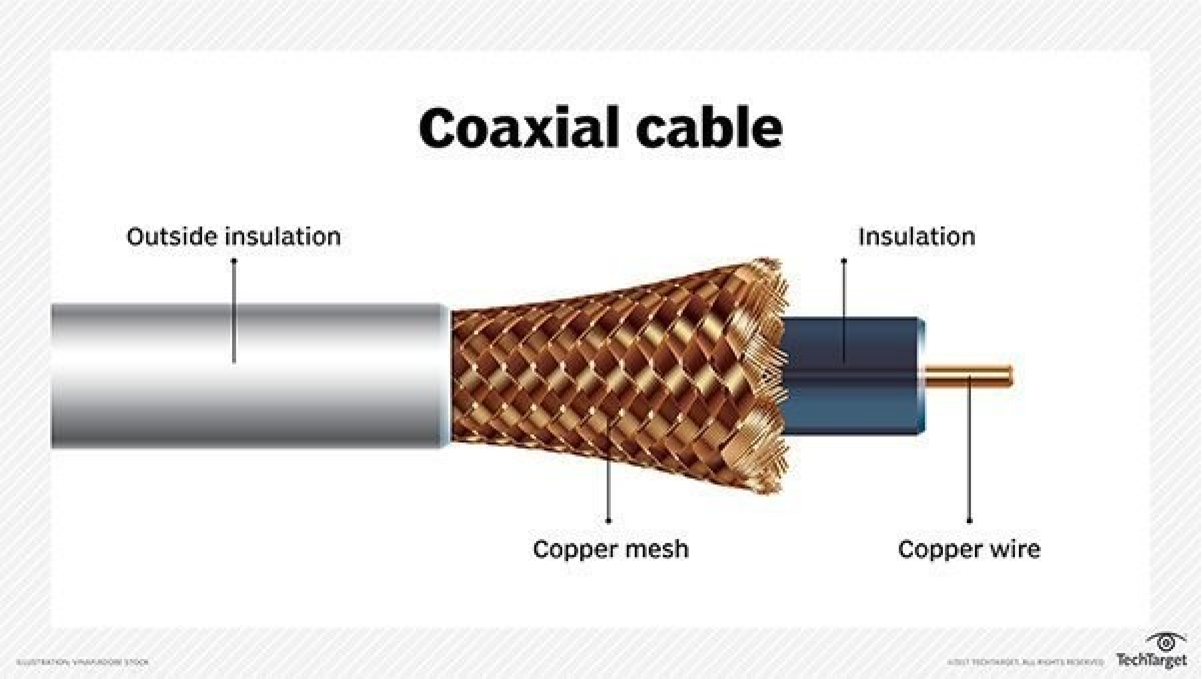
Coaxial cable is a type of copper cable specially built with a metal shield and other components engineered to block signal interference. It is primarily used by cable TV companies to connect_their satellite antenna facilities to customer homes and businesses. It is also sometimes used by telephone companies to connect central offices to telephone poles near customers. Some homes and offices use coaxial cable, too, but its widespread use as an Ethernet connectivity medium in enterprises and data centers has been supplanted by the deployment of twisted pair cabling.

Coaxial cable received its name because it includes one physical channel that carries the signal surrounded -- after a layer of insulation -- by another concentric physical channel, both running along the same axis. The outer channel serves as a ground. Many of these cables or pairs of coaxial tubes can be placed in a single outer sheathing and, with repeaters, can carry information for a great distance.

Coaxial cable was invented in 1880 by English engineer and mathematician Oliver Heaviside, who patented the invention and design that same year. AT&T established its first cross-continental coaxial transmission system in 1940. Depending on the carrier technology used and other factors,twisted pair copper wire and optical fiber are alternatives to coaxial cable.

How coaxial cables work:

Coaxial cables have concentric layers of electrical conductors and insulating material. This construction ensures signals are enclosed within the cable and prevents electrical noise from interfering with the signal.



The center conductor layer is a thin conducting wire, either solid or braided copper. A dielectric layer, made up of an insulating material with very well-defined electrical characteristics, surrounds the wire. A shield layer then surrounds the dielectric layer with metal foil or braided copper mesh. The whole assembly is wrapped in an insulating jacket. The outer metal shield layer of the coaxial cable is typically grounded in the connectors at both ends to shield the signals and as a place for stray interference signals to dissipate.

A key to coaxial cable design is a tight control of cable dimensions and materials. Together, they ensure the characteristic impedance of the cable takes on a fixed value. High-frequency signals are partially reflected at impedance mismatches, causing errors.

Characteristic impedance is sensitive to signal frequency. Above 1 GHz, the cable maker must use a dielectric that does not attenuate the signal too much or change the characteristic impedance in a way that creates signal reflections.

Electrical characteristics of coaxial cables are application-dependent and crucial for good performance. Two standard characteristic impedances are 50 ohms, used in moderate power environments, and 75 ohms, common for connections to antennas and residential installations.

Advantages of coaxial cable :-

1. Coaxial cable is used for both analog and digital data transmission.
2. It has higher bandwidth, hence it can support mixed range of services.
3. Because of its insulation, coaxial cable has lower error rates.
4. Greater spacing between amplifier is possible.
5. It uses for longer distances at higher data rates.
6. Easy to handle.
7. Relatively inexpensive as compared to optic fibre cables.

Disadvantages of coaxial cable :-

1. The bus topology in which coaxial cable is deployed is susceptible to congestion, noise and security risks.
2. Susceptible to damage from lightening strikes.
3. Number of node connection is limited.

Optical Fiber Cable:

Optical fiber is the technology associated with data transmission using light pulses travelling along with a long fiber which is usually made of plastic or glass. Metal wires are preferred for transmission in optical fiber communication as signals travel with fewer damages. Optical fibers are also unaffected by electromagnetic interference. The fiber optical cable uses the application of total internal reflection of light. The fibers are designed such that they facilitate the propagation of light along with the optical fiber depending on the requirement of power and distance of transmission. Single-mode fiber is used for long-distance transmission, while multimode fiber is used for shorter distances. The outer cladding of these fibers needs better protection than metal wires.

Main element of Fiber Optics:

1. **Core:**

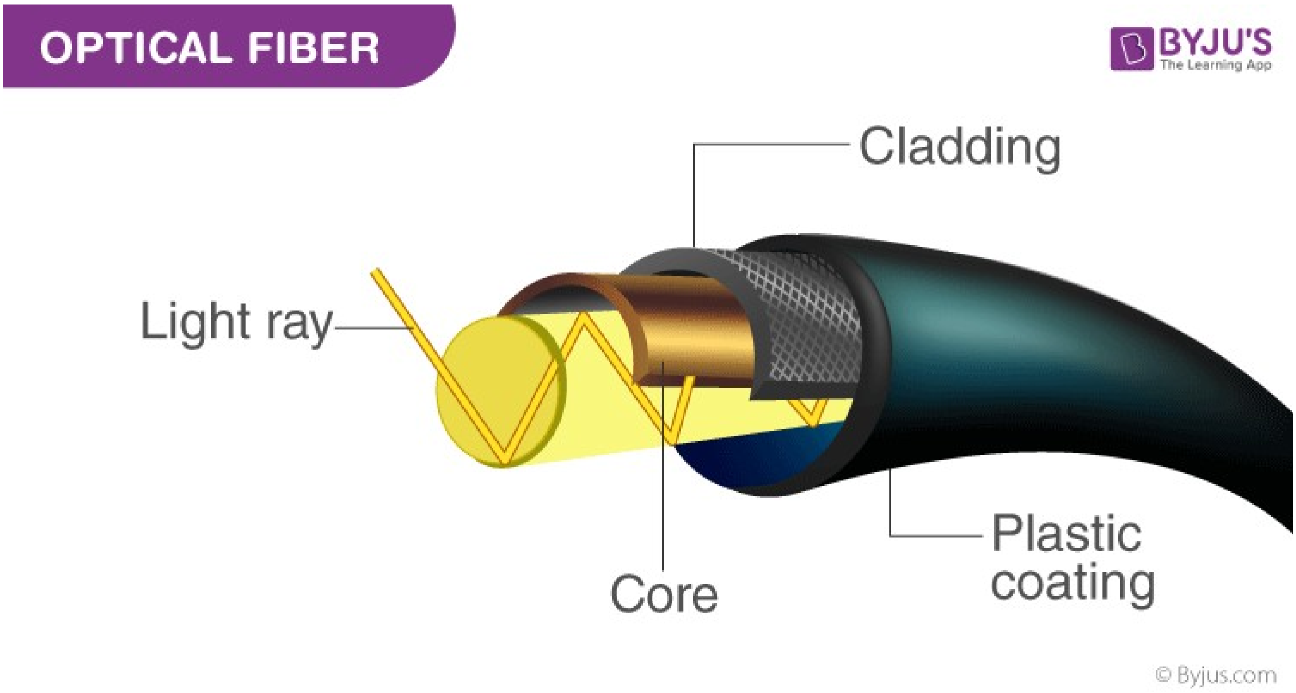
   It is the central tube of very thin size made of optically transparent dielectric medium and carries the light transmitter to receiver and the core diameter may vary from about 5um to 100 um.

2. **Cladding:**

   It is outer optical material surrounding the core having reflecting index lower than core and cladding helps to keep the light within the core throughout the phenomena of total internal reflection.

3. **Buffer Coating:**

   It is a plastic coating that protects the fiber made of silicon rubber. The typical diameter of the fiber after the coating is 250-300 um.



Advantages of Optical Fibre Communication:

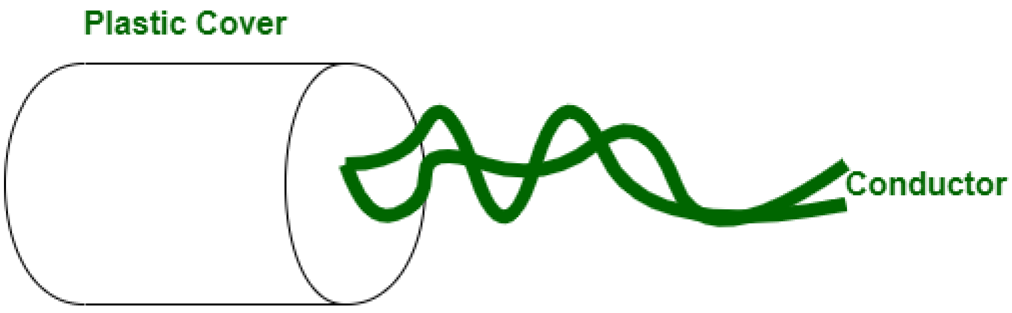
1. The optical fibers have greater information carrying capacities than metallic conductors.
2. Optical fiber is well protected from external interference.
3. It has greater bandwidth.
4. Resistances to high temperature.
5. The optical fibers and fiber cables are very strong and flexible.

Disadvantages of Optical Fibre Communication:

1. It is a high investment cost or installation is costly.
2. It is need more expansive transmitter and receiver equipments.
3. It cannot carry electrical power to operate terminal devices.
4. At higher optical powers, fiber is more prone to fiber flux, so optical fiber may get damaged.

Twisted-Pair Cable:

Twisted Pair Cable is a category of guided media in which circuit is made by twisting two wires to perform transmission. Twisted pair cable constitutes of a combination of insulated copper wires. In twisted pair cable, metallic copper wire helps in transmitting the signals in the form of electrical signals. Twisted Pair Cable are mostly used in telephone networks and cable shielding.



Twisted Pair Cable

Unshielded Twisted Pair (UTP):

This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

Advantages of Unshielded Twisted Pair (UTP):

1. Least expensive
2. Easy to install
3. High speed capacity
4. Susceptible to external interference
5. Lower capacity and performance in comparison to STP
6. Short distance transmission due to attenuation

Shielded Twisted Pair (STP):

This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.

Advantages of Shielded Twisted Pair (UTP):

1. Better performance at a higher data rate in comparison to UTP
2. Eliminates crosstalk
3. Comparitively faster
4. Comparitively difficult to install and manufacture
5. More expensive
6. Bulky

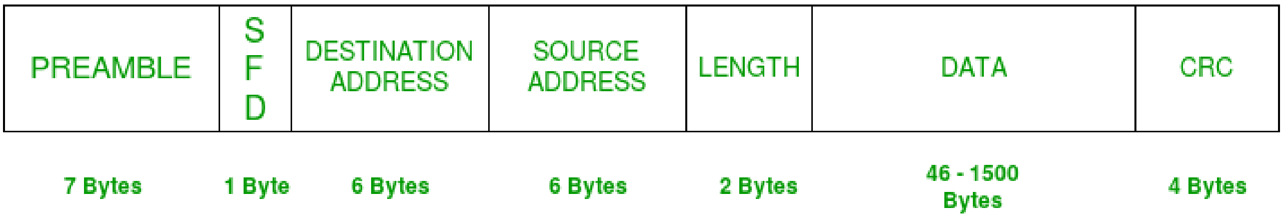
Ethernet:

Ethernet is the traditional technology for connecting devices in a wired local area network (LAN) or wide area network (WAN), enabling them to communicate with each other via a protocol a set of rules or common network language. Ethernet describes how network devices can format and transmit data so other devices on the same local or campus area network segment can recognize, receive and process the information. An Ethernet cable is the physical, encased wiring over which the data travels.

Connected devices accessing a geographically localized network with a cable -- that is, with a wired rather than wireless connection -- likely use Ethernet. From businesses to gamers, diverse end users depend on the benefits of Ethernet connectivity, which include reliability and security.

Ethernet is used to connect devices in a network and is still a popular form of network connection. For local networks used by specific organizations -- such as company offices, school campuses and hospitals.Ethernet is used for its high speed, security and reliability.

Ethernet initially grew popular due to its inexpensive price tag when compared to the competing technology of the time, such as IBM's Token Ring. As network technology advanced, Ethernet's ability to evolve and deliver higher levels of performance, while also maintaining backward compatibility, ensured its sustained popularity. Ethernet's original 10 megabits per second throughput increased tenfold to 100 Mbps in the mid-1990s, and the Institute of Electrical and Electronics Engineers Inc. IEEE continues to deliver increased performance with successive updates. Current versions of Ethernet can support operations up to 400 gigabits per second (Gbps).



PREAMBLE	SFD	DESTINATION ADDRESS	SOURCE ADDRESS	LENGTH	DATA	CRC
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46 - 1500 Bytes	4 Bytes

IEEE 802.3 ETHERNET Frame Format

Advantages:

1. Relatively low cost.
2. Generally resistant to noise.
3. Good data transfer quality.
4. Data security common firewalls can be used.

Disadvantages:

1. Mobility is limited.
2. It is intended for smaller, shorter distance networks.
3. Increased traffic makes the Ethernet speed go down.
4. Receivers do not acknowledge the reception of data packets.
5. When troubleshooting, it is hard to trace which specific cable or node is causing the issue.

WIRELESS CONNECTIONS:

A wireless network is a computer network that uses wireless data connections between network_nodes.

Wireless networking is a method by which homes, telecommunications networks and business installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations.admin telecommunications networks are generally implemented and administered using radio_communication. This implementation takes place at the physical level (layer) of the OSI_model network structure.

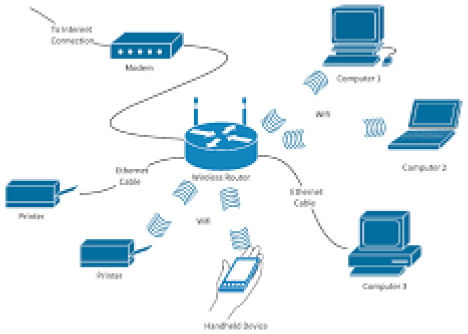
Examples of wireless networks include cell_phone_networks, wireless_local_area networks (WLANs), wireless sensor networks, satellite communication networks, and terrestrial microwave networks.

The first professional wireless network was developed under the brand ALOHAnet in 1969 at the University of Hawaii and became operational in June 1971. The first commercial wireless network was the WaveLAN product family, developed by NCR in 1986.

WIFI:

Wi-Fi stands for Wireless Fidelity. It is a technology for wireless local area networking with devices based on **IEEE 802.11** standards. Wi-Fi compatible devices can connect to the internet via WLAN network and a wireless access point abbreviated as AP. Every WLAN has an access point which is responsible for receiving and transmitting data from/to users. IEEE has defined certain specifications for wireless LAN, called **IEEE 802.11** which covers physical and data link layers.

Wi-Fi (Wireless Fidelity) is a generic term that refers to the communication standard for the wireless network which works as Local Area Network to operate without using the cable and any types of wiring. It is known as **WLAN**. The communication standard is **IEEE 802.11**. Wi-Fi works using Physical Data Link Layer. Nowadays in all mobile computing devices such as laptops, mobile phones, also digital cameras, smart TVs has the support of Wi-Fi. The Wi-Fi connection established from the access point or base station to the client connection or any client to client connection within a specific range, the range depends on the router which provides the radio frequency through Wi-Fi. These frequencies operate on 2 types of bandwidth at present, 2.4 GHz and 5 GHz. All the modern laptops and mobiles are capable of use both the bandwidths, it depends on the Wi-Fi adapter which is inside the device to catch the Wi-Fi signal. 2.4 GHz is the default bandwidth supported by all the devices. 2.4 GHz can cover a big range of areas to spread Wi-Fi signal but the frequency is low, so in simple words, the speed of the internet is less and 5 GHz bandwidth is for a lower range of area but the frequency is high so the speed is very high. Let’s say, if there is an internet connection of 60 MB/s bandwidth, then for 2.4 GHz bandwidth, it provides approx 30 to 45 MB/s of bandwidth connection and for 5 GHz bandwidth, it provides approx 50 to 57 MB/s bandwidth.



Advantages of Wi-Fi:

1. It is a flexible network connection, no wiring complexities. Can be access from any where in the Wi-Fi range.
2. It does not require regulatory approval for individual users.
3. It is salable, can be expanded with using Wi-Fi Extenders.
4. It can be set up in a easy and fast way. Just need to configure the SSID and Password.
5. Security in high in Wi-Fi network, its use **WPA** encryption to encrypt radio signals.
6. It is also lower in cost and supports roaming.
7. It also can provide Hotspots.

Disadvantages of Wi-Fi:

1. Power consumption is high while using Wi-Fi in any device which has a battery, such as mobile, laptops, etc.
2. Many times there may be some security problems happen even it has encryption. Such as many time known devices become unknown to the router, Wi-Fi can be hacked also.
3. Speed is lower than direct cable connection.
4. Wi-Fi signals may be affected by climatic conditions like thunderstorm.
5. Unauthorized access to Wi-Fi can happen, because it does not has firewall.
6. To use Wi-Fi we need a router, which needs a power source, so at the time of power cut we cannot access the internet.

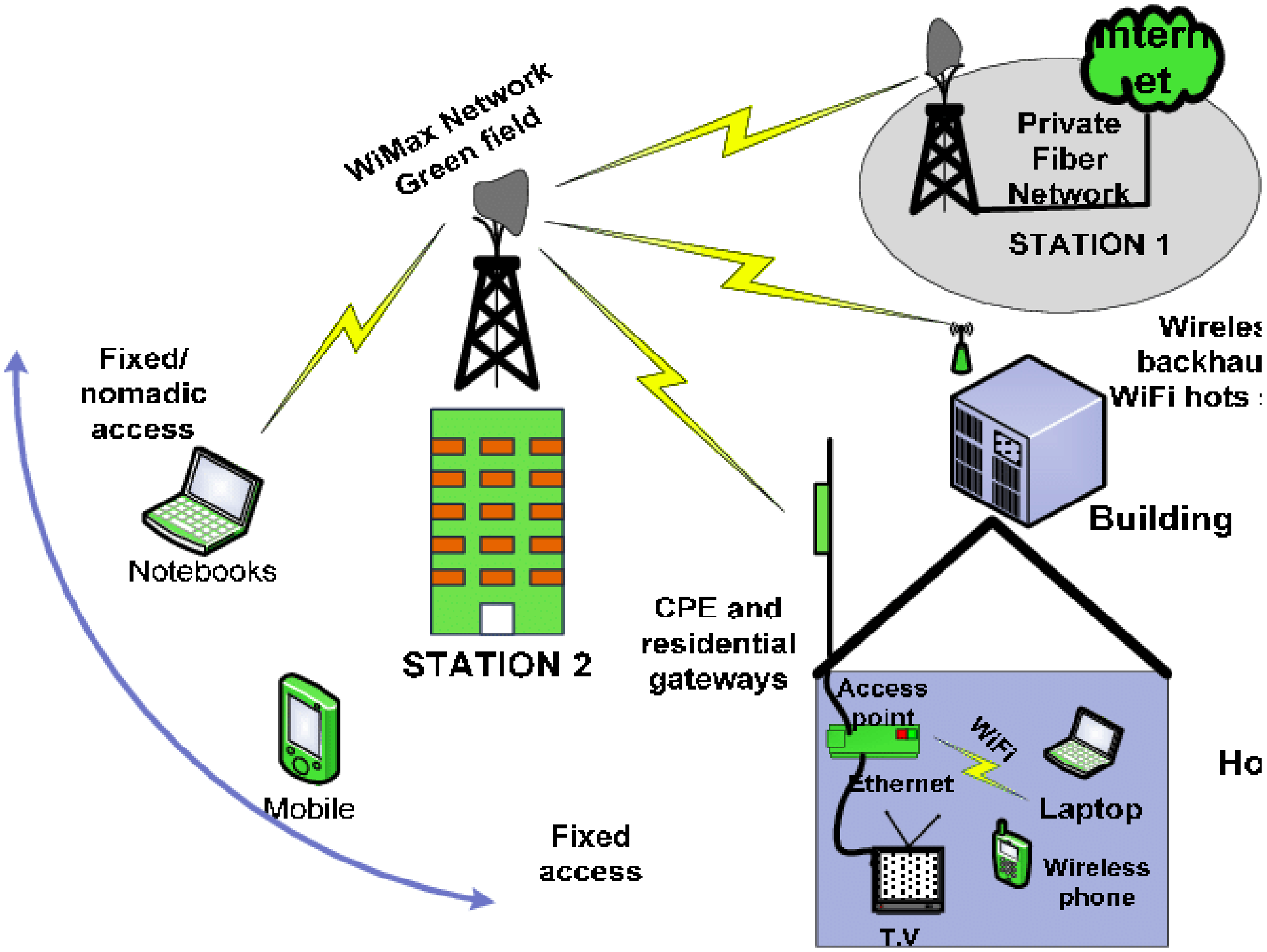
WiMAX:

WiMAX (Worldwide Interoperability for Microwave Access) is a family of wireless broadband communication standards based on the IEEE 802.16 set of standards, which provide multiple physical layer (PHY) and Media Access Control (MAC) options.

The name "WiMAX" was created by the WiMAX Forum, which was formed in June 2001 to promote conformity and interoperability of the standard, including the definition of predefined system profiles for commercial vendors.The forum describes WiMAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL". IEEE 802.16m or WirelessMAN-Advanced was a candidate for the 4G, in competition with the LTE Advanced standard.

WiMAX can provide at-home or mobile Internet access across whole cities or countries. In many cases, this has resulted in competition in markets which typically only had access through an existing incumbent DSL (or similar) operator.

ess to network subscribers etc., as seen in Fig. 1.



Advantages of WiMAX:

1. Single station can serve hundreds of users.
2. Much faster deployment of new users comparing to wired networks.
3. Speed of 10 Mbps at 10 kilometers with line-of-site.
4. It is standardized, and same frequency equipment should work together.

Disadvantages of WiMAX:

1. Line of site is needed for longer connections.
2. Big installation and operational cost.
3. Higher latency and Unreliable service.
4. Big delay and spectral limitation.

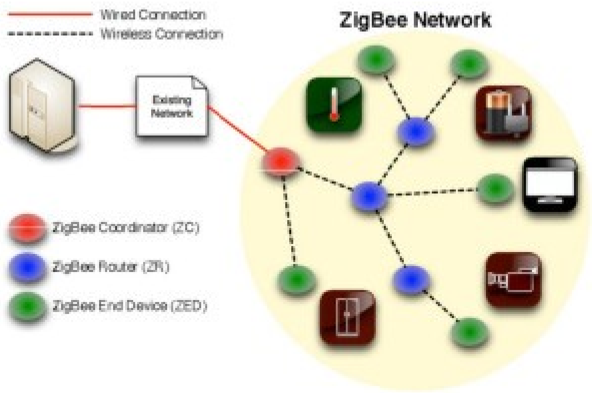
ZIGBEE:

Zigbee is a wireless technology developed as an open global standard to address the unique needs of low-cost, low-power wireless IoT networks. The Zigbee standard operates on the IEEE 802.15.4 physical radio specification and operates in unlicensed bands including 2.4 GHz, 900 MHz and 868 Mhz.

The technology defined by the Zigbee specification is intended to be simpler and less expensive than other wireless personal area networks (WPANs), such as Bluetooth or more general wireless networking such as Wi-Fi. Applications include wireless light switches, home energy monitors, traffic management systems, and other consumer and industrial equipment that requires short-range low-rate wireless data transfer.

Its low power consumption limits transmission distances to 10–100 meters line-of-sight, depending on power output and environmental characteristics. Zigbee devices can transmit data over long distances by passing data through a mesh network of intermediate devices to reach more distant ones. Zigbee is typically used in low data rate applications that require long battery life and secure networking (Zigbee networks are secured by 128 bit symmetric.

Zigbee supports different network configurations for master to master or master to slave communications. And also, it can be operated in different modes as a result the battery power is conserved. Zigbee networks are extendable with the use of routers and allow many nodes to interconnect with each other for building a wider area network.



Advantages of ZIGBEE:

1. The zigbee has flexible network structure.
2. It has a very long battery life.
3. It is low power consumption and easy to install and cheap.
4. It supports large number of nodes i.e. 6500 nodes approximately.

Disadvantages of ZIGBEE:

1. It is so highly risky to be used for official private information.
2. The zigbee has low transmission rate.
3. Replacement with zigbee compliant appliances can be costly.
4. It is not secure like wi fi based secured system.

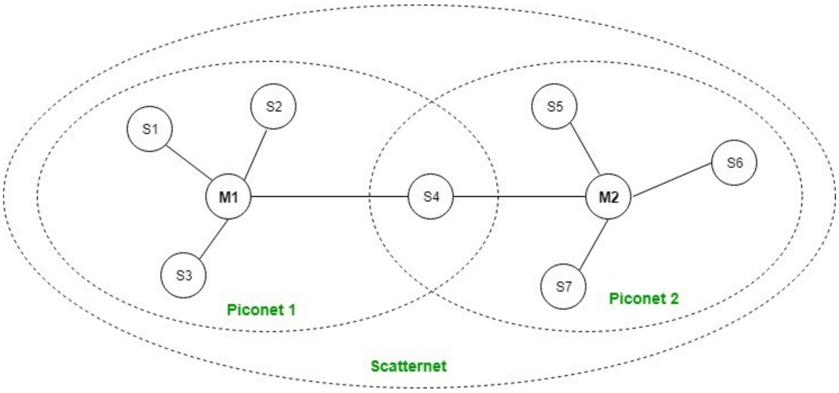
BLUETOOTH:

It is a Wireless Personal Area Network (WPAN) technology and is used for exchanging data over smaller distances. This technology was invented by Ericson in 1994. It operates in the unlicensed, industrial, scientific and medical (ISM) band at 2.4 GHz to 2.485 GHz. Maximum devices that can be connected at the same time are 7. Bluetooth ranges upto 10 meters. It provides data rates upto 1 Mbps or 3 Mbps depending upon the version. The spreading technique which it uses is FHSS (Frequency hopping spread spectrum). A bluetooth network is called piconet and a collection of interconnected piconets is called scatternet.

Bluetooth Architecture:

The architecture of bluetooth defines two types of networks:

1. Piconet
2. Scatternet

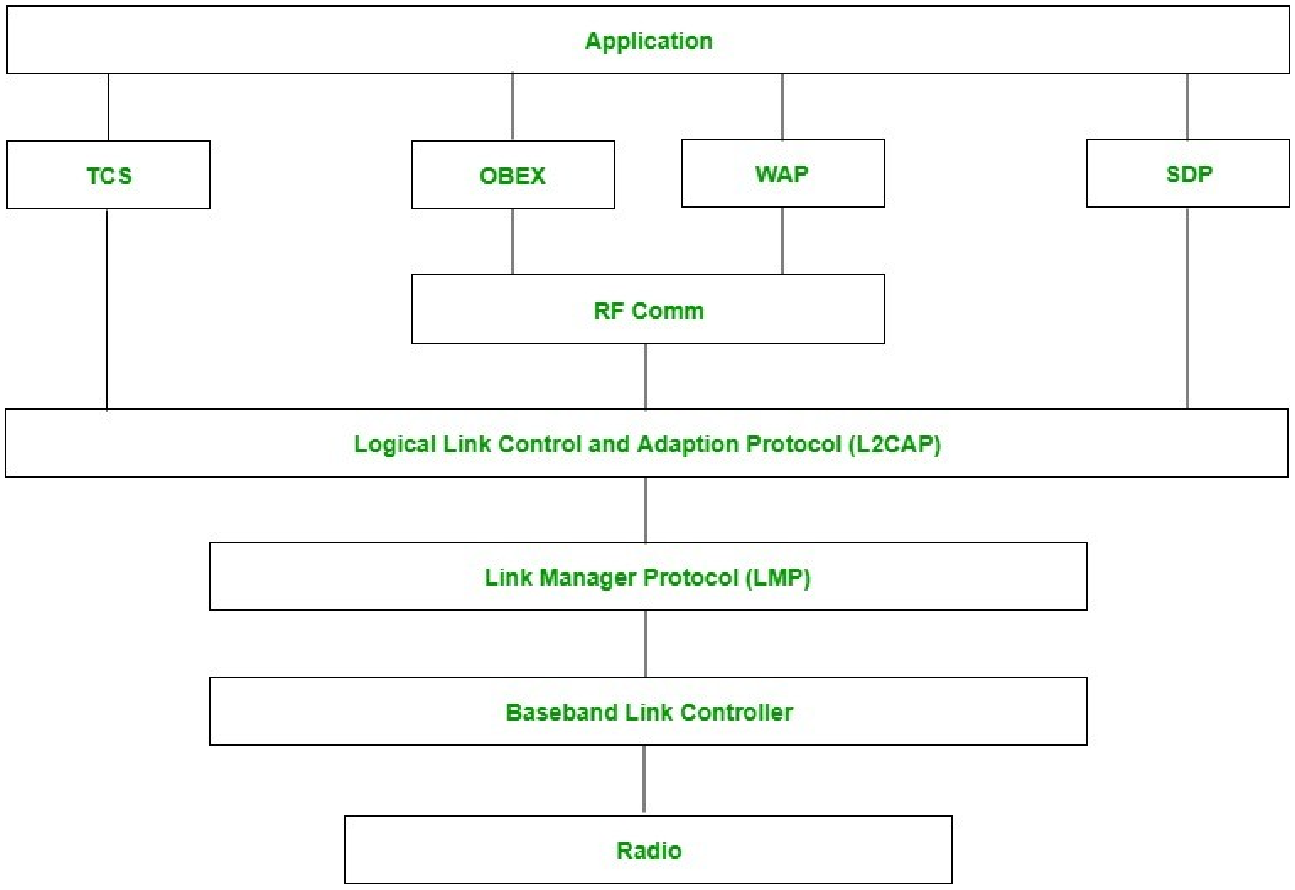


Piconet:

Piconet is a type of bluetooth network that contains one primary node called master node and seven active secondary nodes called slave nodes. Thus, we can say that there are total of 8 active nodes which are present at a distance of 10 metres. The communication between the primary and secondary node can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. It also have 255 parked nodes, these are secondary nodes and cannot take participation in communication unless it get converted to the active state.

Scatternet:

It is formed by using various piconets. A slave that is present in one piconet can be act as master or we can say primary in other piconet. This kind of node can receive message from master in one piconet and deliver the message to its slave into the other piconet where it is acting as a slave. This type of node is refer as bridge node. A station cannot be master in two piconets.


Application
TCS
OBEX
WAP
SDP
RF Comm
Logical Link Control and Adaption Protocol (L2CAP)
Link Manager Protocol (LMP)
Baseband Link Controller
Radio

Advantages of Bluetooth:

1. It avoids interference from other wireless devices.
2. It has lower power consumption.
3. It is easily upgradeable.
4. No line of sight hence can connect through any obstacles.
5. Free to use if the device is installed with Bluetooth.
6. The technology is adopted in many products such as head set, in car system, printer, web cam, GPS system, keyboard and mouse.

Disadvantages of Bluetooth:

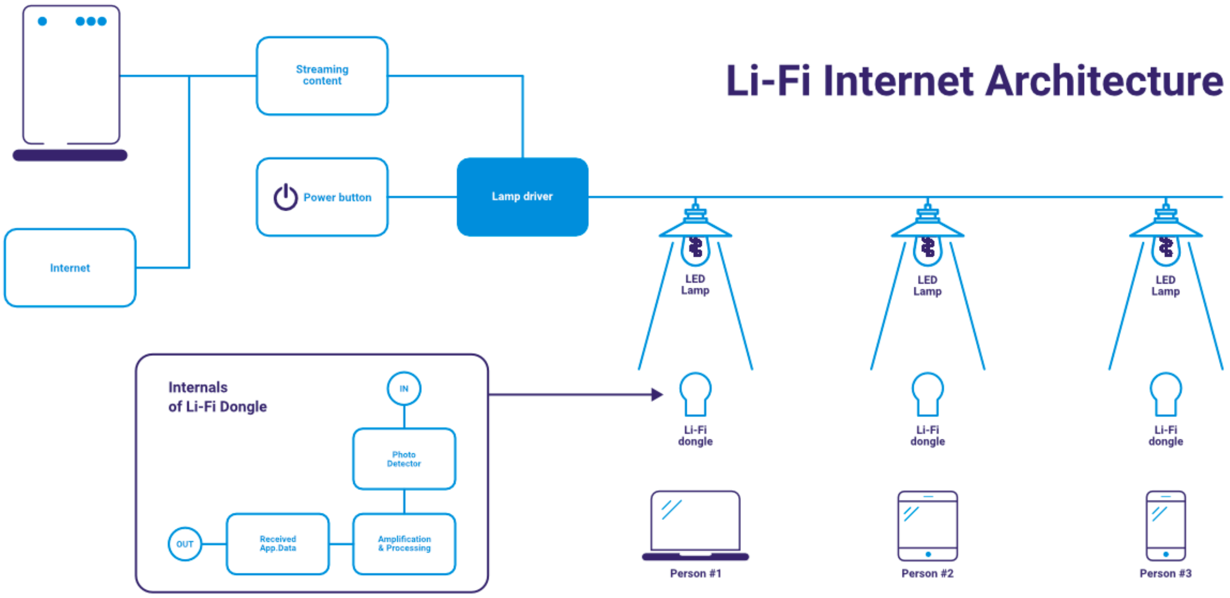
1. It can lose connection in certain conditions.
2. It has low bandwidth as compared to Wi-Fi.
3. It allows only short range communication between devices.
4. Security is a very key aspect as it can be hacked.

LIFI:

Li-Fi is wireless communication technology which utilizes light to transmit data and position between devices. The term was first introduced by Harald Haas during a 2011 TEDGlobal talk in Edinburgh.In technical terms, Li-Fi is a light communication system that is capable of transmitting data at high speeds over the visible light, ultraviolet, and infrared spectrums. In its present state, only LED lamps can be used for the transmission of visible light.

Li-Fi is a derivative of optical wireless communications (OWC) technology, which uses light from light-emitting diodes (LEDs) as a medium to deliver network, mobile, high-speed communication in a similar manner to Wi-Fi.The Li-Fi market was projected to have a compound annual growth rate of 82% from 2013 to 2018 and to be worth over $6 billion per year by 2018.[5] However, the market has not developed as such and Li-Fi remains with a niche market, mainly for technology evaluation.

In this technology, Wi-Fi signals are converted into light form and if your device is under this light then Wi-Fi works on your mobile. The main advantage of this technology is that when you turn on the light of your room, your Wi-Fi will limit only to your room and to your device, no other person will be able to use it and not like router the whole house would be under Wi-Fi signals when only you want to use it in your room. You might think that if you want to close the light and then use this Wi-Fi technology, then scientists have solved your problem too. You can use this Light Wi-Fi in its very dim light also, so next time you want to text in dark, it will not be much of a problem. This technology will reach most of the places soon and will replace routers.



Advantages of LiFi:

1. Faster Data Transmission than Wi-Fi
2. Easy and Inexpensive to Deploy
3. Immune From Electromagnetic Interferences
4. Expansive Future Applications

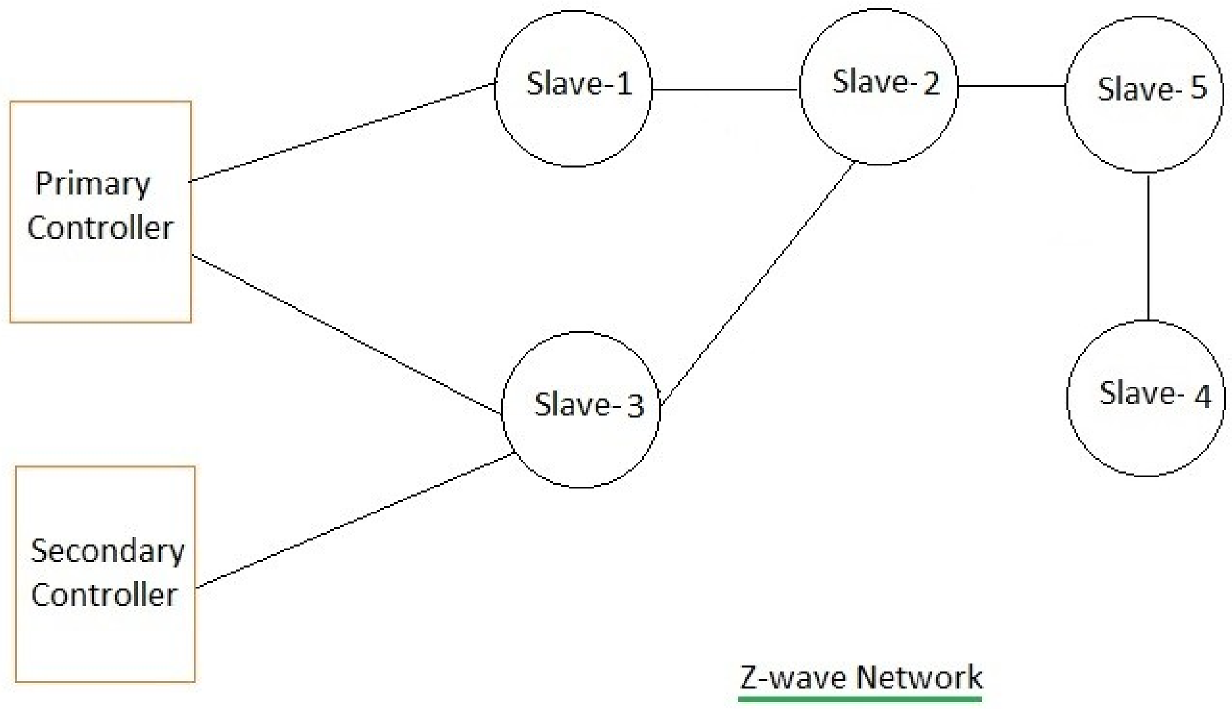
Disadvantages of LiFi:

1. Limited Range and Connectivity
2. Unavailability of Compatible Technologies
3. Light Interference and Light Pollution
4. Possible Cost Implications

Z-Wave:

Z-Wave is a wireless communications protocol used primarily for home automation. It is a mesh network using low-energy radio waves to communicate from appliance to appliance,allowing for wireless control of residential appliances and other devices, such as lighting control, security systems, thermostats, windows, locks, swimming pools and garage door openers. Like other protocols and systems aimed at the home and office automation market, a Z-Wave system can be controlled via the Internet from a smart phone, tablet or computer, and locally through a smart speaker, wireless keyfob, or wall-mounted panel with a Z-Wave gateway or central control device serving as both the hub controller and portal to the outside.[2][4] Z-Wave provides the application layer inter operability between home control systems of different manufacturers that are a part of its alliance. There are a growing number of inter operable Z-Wave products; over 1,700 in 2017,[5] and over 2,600 by 2019.

A Z-Wave network consists of internet of things (IoT) devices and a primary controller, also known as a smart home hub, which is the only device in a Z-Wave network that is usually connected to the internet. When a Z-Wave hub receives a command from a smart home application on a user's smartphone, tablet or computer, it routes the command to its destination device across networks of up to 232 devices -- including the hub. Using source-routed mesh network technology, Z-Wave signals can hop through other Z-Wave devices to reach the device a user intends to control. Each Z-Wave network accommodates a maximum of four hops. The Z-Wave protocol operates on the low-frequency 908.42 band in the U.S . and the 868.42 MHz band in Europe. Though interference with other home electronics, such as cordless phones, is possible, the protocol avoids interference with the 2.4 GHz band where Wi-Fi and Bluetooth operate. Z-Wave offers transmission rates of small data packets using throughput rates of 9.6 kbps, 40 kbps or 100 kbps. The Z-Wave PHY and MAC layers are based on the ITU-T G.9959 global radio standard, and the protocol uses GFSK modulation and Manchester encoding. It also includes AES 128 encryption, IPv6 multichannel operation.



Advantages of Z-wave:

1. Installation is simple and easy. It is also easy to add/remove z-wave devices in the once installed system.
2. Consume less power.
3. AES-128 encryption for secure wireless network.
4. Devices are interoperable with other wireless devices in the IoT space.

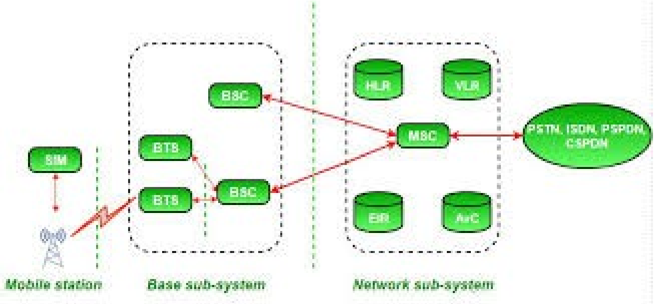
Disadvantages of Z-wave:

1. Supports only tree topology structure.
2. Supports limited number of nodes i.e. 232 which is less than 65000 nodes as supported by zigbee standard.
3. Less data communication speed up to 100 kbps.

GSM:

The Global System for Mobile Communications (GSM) is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation digital cellular networks used by mobile devices such as mobile phones and tablets. It was first deployed in Finland in December 1991. By the mid-2010s, it became a global standard for mobile communications achieving over 90% market share, and operating in over 193 countries and territories. GSM is basically an open, digital cellular radio network and operates in almost all the countries. It is not only used for voice calls but also for data computing and text messages. While CDMA(Code Division Multiple Access) doesn't support calls and data computing at the same time.

GSM makes use of the narrow band Time Division Multiple Access (TDMA) technique for transmitting signals. GSM is a circuit-switching system that works by dividing each 200 kHz channel into eight 25 kHz time-slots. GSM operates on the mobile communication bands 900 MHz and 1800 MHz in most parts of the world.



Advantages of GSM:

1. It is highly secured as facilities cannot be duplicated as all the information is stored on a sim card.
2. It is compatible with a wide range of devices.
3. Allows use of voice calls and data at the same time, unlike CDMA technology.
4. Clarity of voice calls is another interesting and demanding feature.

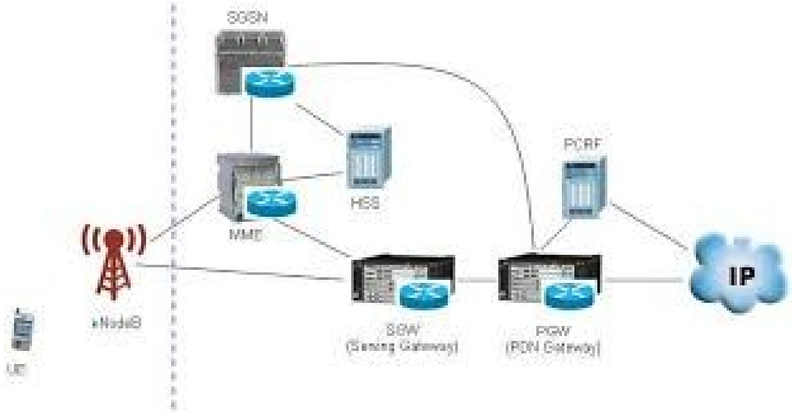
Disadvantages of GSM:

1. As multiple users share same bandwidth, the transmission can face interference. Due to these newer cellular networks like 3G makes use of CDMA technology.
2. It can also interfere with electronics equipment as it makes use of pulse transmission technology.Therefore we are told to put our cellphones on airplane mode in airplanes and hospitals so as to avoid this electronic interference.
3. Also it is a highly complicated system.

4G LTE:

Long-Term Evolution (LTE) is a standard for wireless broadband communication for mobile devices and data terminals, based on the GSM/EDGE and UMTS/HSPA technologies. It increases the capacity and speed using a different radio interface together with core network improvements. LTE is the upgrade path for carriers with both GSM/UMTS networks and CDMA2000 networks. The different LTE frequencies and bands used in different countries mean that only multi-band phones are able to use LTE in all countries where it is supported.

The standard is developed by the 3GPP (3rd Generation Partnership Project) and is specified in its Release 8 document series, with minor enhancements described in Release 9. LTE is sometimes known as **3.95G** and has been marketed both as "4G LTE" and as "Advanced 4G" but it does not meet the technical criteria of a 4G wireless service, as specified in the 3GPP Release 8 and 9 document series for . The requirements were originally set forth by the ITU-R organisation in the IMT Advanced specification. However, due to marketing pressures and the significant advancements that WiMAX, Evolved High Speed Packet Access, and LTE bring to the original 3G technologies, ITU later decided that LTE together with the aforementioned technologies can be called 4G technologies. The LTE Advanced standard formally satisfies the ITU-R requirements to be considered IMT-Advanced.To differentiate LTE Advanced and WiMAX-Advanced from current 4G technologies, ITU has defined them as "True 4G".



Advantages of 4G LTE:

1. Network is very fast & 10 times faster than the 3G network.
2. High voice quality and very fast while downloading huge files.
3. Higher bandwidth

Disadvantages of 4G LTE:

1. Higher data prices for the consumers.
2. Consumers are forced to buy a new device to support 4G LTE.
3. Consumes a lot of battery.
4. Requires complex hardware.

Types of Networks:

1. Personal Area Network (PAN):

The smallest and most basic type of network, a PAN is made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building. These types of networks are typically found in small offices or residences, and are managed by one person or organization from a single device.

2. Local Area Network (LAN):

LANs are the most frequently discussed networks, one of the most common, one of the most original and one of the simplest types of networks. LANs connect groups of computers and low-voltage devices together across short distances (within a building or between a group of two or three buildings in close proximity to each other) to share information and resources. Enterprises typically manage and maintain LANs.

Using routers, LANs can connect to wide area networks (WANs, explained below) to rapidly and safely transfer data.

3. Wireless Local Area Network (WLAN):

Functioning like a LAN, WLANs make use of wireless network technology, such as Wi-Fi. Typically seen in the same types of applications as LANs, these types of networks don’t require that devices rely on physical cables to connect to the network.

4. **Campus Area Network (CAN):**

Larger than LANs, but smaller than metropolitan area networks (MANs, explained below), these types of networks are typically seen in universities, large K-12 school districts or small businesses. They can be spread across several buildings that are fairly close to each other so users can share resources.

5. **Metropolitan Area Network (MAN):**

These types of networks are larger than LANs but smaller than WANs – and incorporate elements from both types of networks. MANs span an entire geographic area (typically a town or city, but sometimes a campus). Ownership and maintenance is handled by either a single person or company (a local council, a large company, etc.

6. **Wide Area Network (WAN):**

Slightly more complex than a LAN, a WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other over one large network to communicate even when they’re miles apart.

The Internet is the most basic example of a WAN, connecting all computers together around the world. Because of a WAN’s vast reach, it is typically owned and maintained by multiple administrators or the public.

7. **Storage-Area Network (SAN):**

As a dedicated high-speed network that connects shared pools of storage devices to several servers, these types of networks don’t rely on a LAN or WAN. Instead, they move storage resources away from the network and place them into their own high-performance network. SANs can be accessed in the same fashion as a drive attached to a server. Types of storage-area networks include converged, virtual and unified SANs.

Conclusion : Understood about OSI layer and about various wireless and wired connectors.

References :

1. https://www.geeksforgeeks.org/basics-computer-networking/
2. https://www.geeksforgeeks.org/layers-of-osi-model/
3. https://www.javatpoint.com/osi-model
4. https://www.studytonight.com/computer-networks/osi-model-physical-layer
5. https://www.geeksforgeeks.org/types-transmission-media/
6. https://www.javatpoint.com/transmission-media
7. https://en.wikipedia.org/wiki/Wired_communication
8. https://en.wikipedia.org/wiki/Coaxial_cable

9. https://searchnetworking.techtarget.com/definition/coaxial-cable-illustrated
10. https://www.polytechnichub.com/advantages-disadvantages-bluetooth/
11. https://www.belden.com/blog/smart-building/network-types
12. https://www.quora.com/What-are-the-advantages-and-disadvantages-of-a-coaxial-cable
13. https://www.omnisecu.com/basic-networking/advantages-and-disadvantages-of-fiber-optic-cable.php
14. https://www.geeksforgeeks.org/introduction-of-zigbee/
15. https://www.polytechnichub.com/advantages-disadvantages-zigbee/
16. https://en.wikipedia.org/wiki/WiMAX
17. https://en.wikipedia.org/wiki/Li-Fi
18. https://www.quora.com/What-are-the-advantages-and-disadvantages-of-
19. https://www.geeksforgeeks.org/ethernet-frame-format/
20. https://en.wikipedia.org/wiki/Z-Wave
21. https://internetofthingsagenda.techtarget.com/definition/Z-Wave

22. https://www.rfwireless-world.com/Terminology/Advantages-and-Disadvantages-of-z-wave.html
23. https://en.wikipedia.org/wiki/LTE_(telecommunication)
24. https://www.online-sciences.com/technology/4g-technology-uses-features-advantages-and-disadvantages/