

1.1 DATA COMMUNICATIONS

- ❖ **Network:** Is two or more devices connected through links.

- ❖ When we communicate, we are sharing information. This sharing can be local or remote. Between individuals, local communication usually occurs face to face, while remote communication takes place over distance. The term *telecommunication*, which includes telephony, telegraphy, and television, means communication at a distance.

- ❖ Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

- ❖ Network computer devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices are said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other.

- ❖ Computer networks support applications such as access to the World Wide Web, shared use of application and storage servers, printers, and fax machines,

and use of email and instant messaging applications. Computer networks differ in:-

- 1.The physical media used to transmit their signals
- 2.The communications protocols to organize network traffic
- 3.The network's size, topology and organizational intent.

➤ **The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.**

1. Delivery: The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

2. Accuracy: The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

3. Timeliness: The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

4. Jitter: Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30 ms. If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.

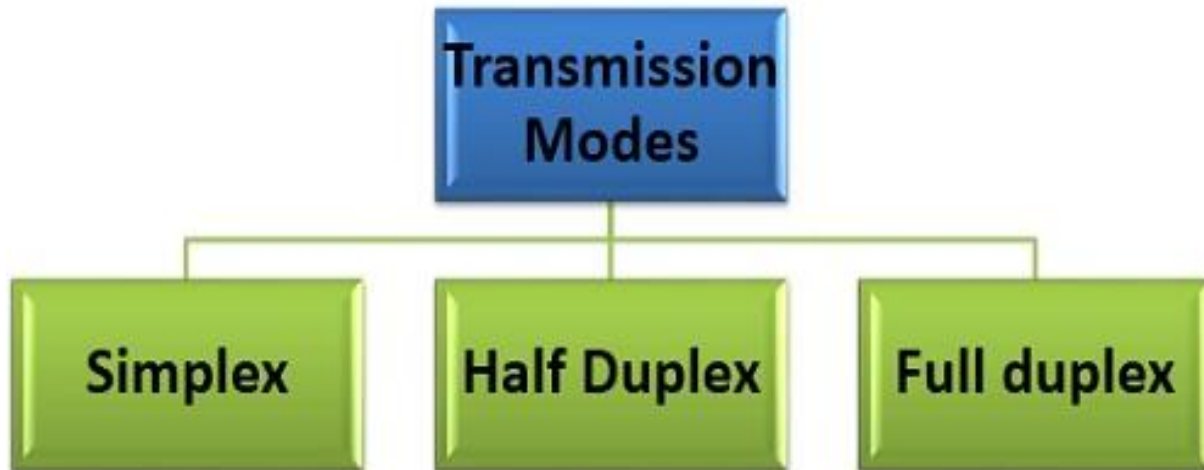
A data communications system has five components (see Figure 1.1).

Figure 1.1 Five components of data communication



- 1. Message:** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
- 2. Sender:** The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
- 3. Receiver:** The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
- 4. Transmission medium:** The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
- 5. Protocol:** A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

1.2 Data Flow (Data Transmission Modes)



Communication between two devices can be simplex, half-duplex, or full-duplex:

1. Simplex: In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive

Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

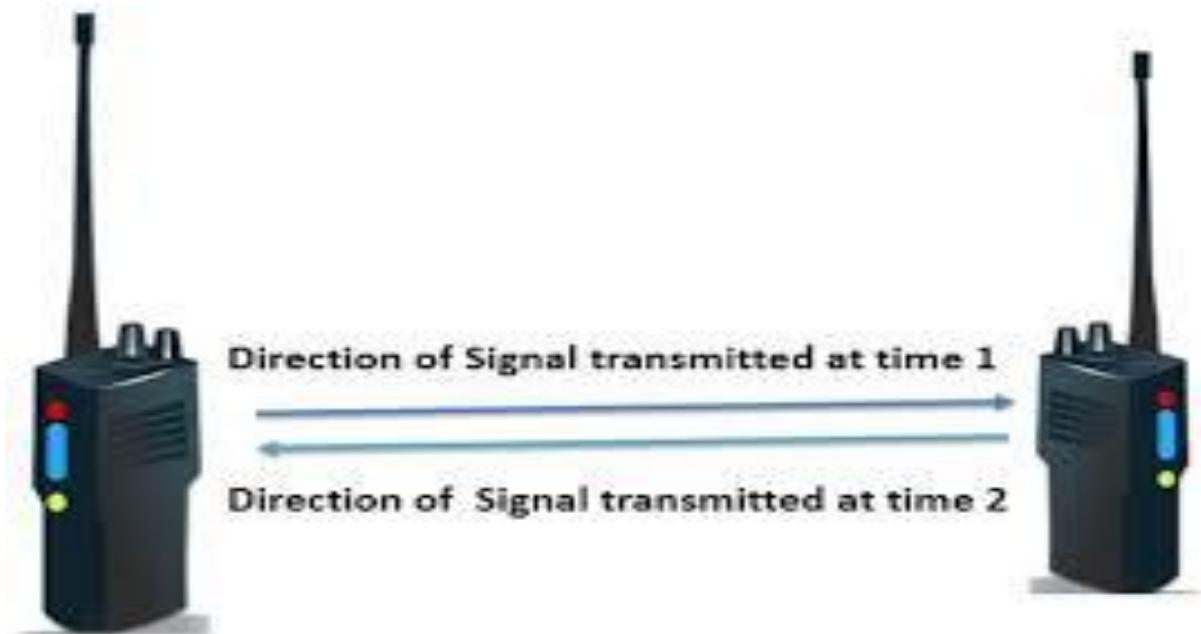


Direction of communication.

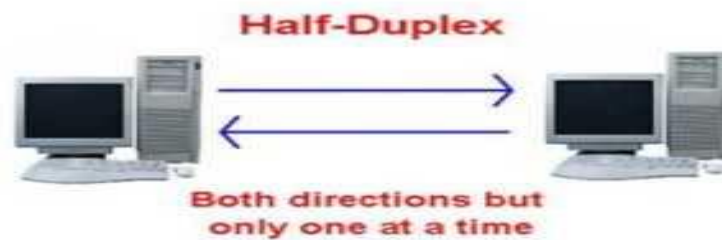


By Natcha Phohan

2. Half-Duplex: In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa (see Figure 1.2b). Walkie-talkies and CB (citizens band) radios are both half-duplex systems. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time.



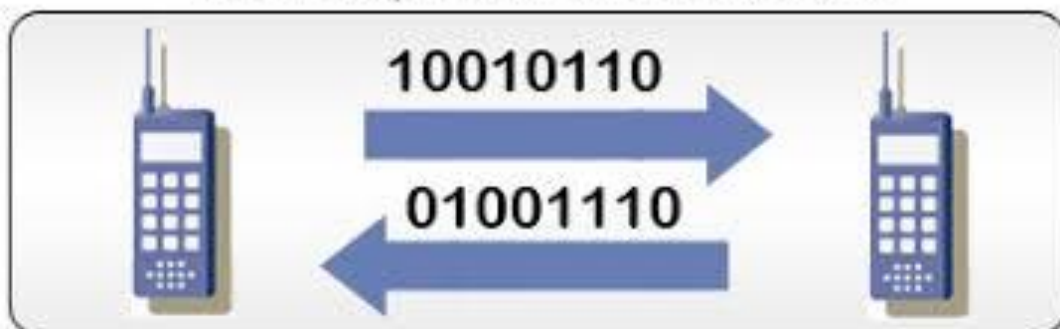
Example



3.Full-Duplex: In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously (see Figure 1.2c). In full-duplex mode, signals going in one direction share the capacity of the link with signals going in the other direction.

One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

Full-Duplex Transmission

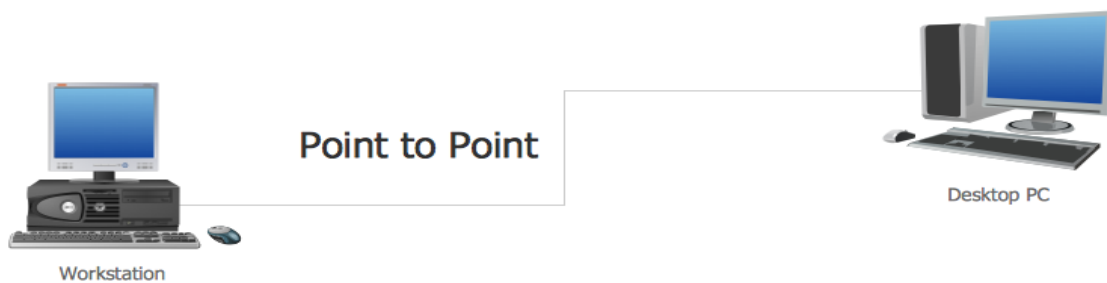


1.3 Type of Connection

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For communication to occur, two devices must be connected in some way to the same link at the same time.

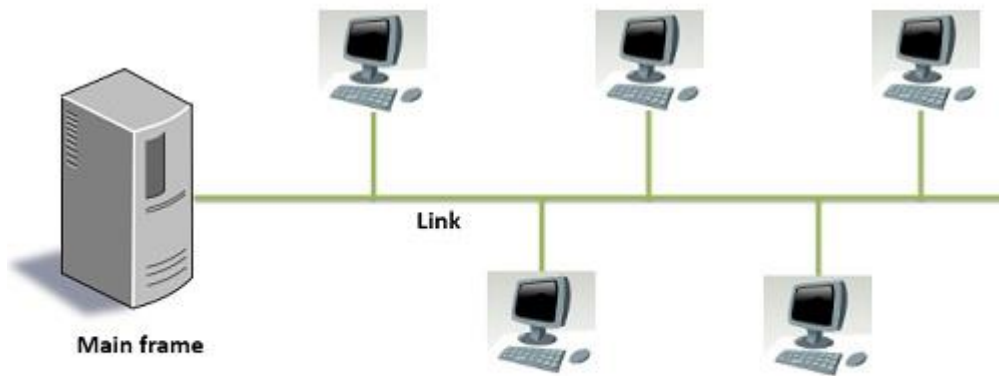
There are two possible types of connections: point-to-point and multipoint.

1. Point-to-Point: A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible (see Figure 1.3a). When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.



(Figure 1.3a)

2. Multipoint: A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link (see Figure 1.3b). In a multipoint environment, the capacity of the channel is shared.



Multipoint Connection
(Figure 1.3b)

➤ Advantages of Computer Networks

- 1- **File sharing:**– become easily share data between different users, or access it remotely if you keep it on other connected devices.
- 2- **Resource sharing:**– using network-connected peripheral devices like printers, scanners and copiers, or sharing software between multiple users, saves money.
- 3- **Sharing a single internet connection:**– it is cost- efficient and can help protect your systems if you properly secure the network.
- 4- **Increasing storage capacity:**– you can access files and multimedia, such as images and music, which you store remotely on other machines or network-attached storage devices.

➤ Disadvantages of Computer Networks

Following are some of the major disadvantages of computer networks

- 1- **Security Issues:** One of the major drawbacks of computer networks is the security issues involved. If a computer is a standalone, physical access becomes necessary for any kind of data theft. However, if a computer is on a network, a computer hacker can get unauthorized access by using different tools. In case of big organizations, various network security software are used to prevent the theft of any confidential and classified data.
- 2- **Rapid Spread of Computer Viruses:** If any computer system in a network gets affected by computer virus, there is a possible threat of other systems getting affected too. Viruses get spread on a network easily because of the interconnectivity of workstations. Such spread can be dangerous if the computers have important database which can get corrupted by the virus.

- 3- **Expensive Set Up:** The initial set up cost of a computer network can be high depending on the number of computers to be connected. Costly devices like routers, switches, hubs, etc., can add up to the bills of a person trying to install a computer network. He will also have to buy NICs (Network Interface Cards) for each of the workstations, in case they are not inbuilt.
- 4- **Dependency on the Main File Server:** In case the main File Server of a computer network breaks down, the system becomes useless. In case of big networks, the File Server should be a powerful computer, which often makes it expensive.

Network Components:

- **NIC: (Network Interface Card):** Is used to enable a network device, (a computer or other network equipment) to connect to a network. Every NIC (Network Interface Card) has a 48-bit globally unique identifier called as MAC Address (Media Access Control Address) burned into its ROM chip. This MAC address is used to deliver Ethernet Frames (packets) to a computer.



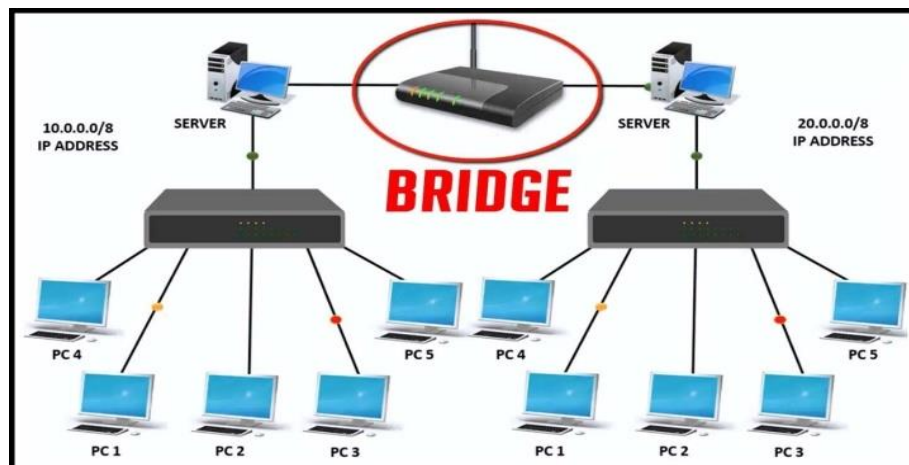
- **Repeater: Repeater** is a powerful network device which is used to regenerate the signals, when they travel over a longer distance, so that the strength of the signal remains the same. A repeater connects two or more cable segments and retransmits any incoming signal to all other segments. A repeater operates at Layer 1 (physical layers).



- **HUB:** A hub is a central network device that connects network nodes Such as workstation and servers in a star topology. A network hub is a device that allows multiple computers to communicate with each other over a network. For example, if five devices are connected to an 8-port hub, all data received by the hub is relayed to the five active ports. A Hub works at Physical layer or Layer 1



- **Bridge:** A bridge is a network device that sends information between two local area network. a bridge is a product that connects a local area network (LAN) to another local area network that uses the **same** protocol. A bridge operates at Layer 2 (data link layer).



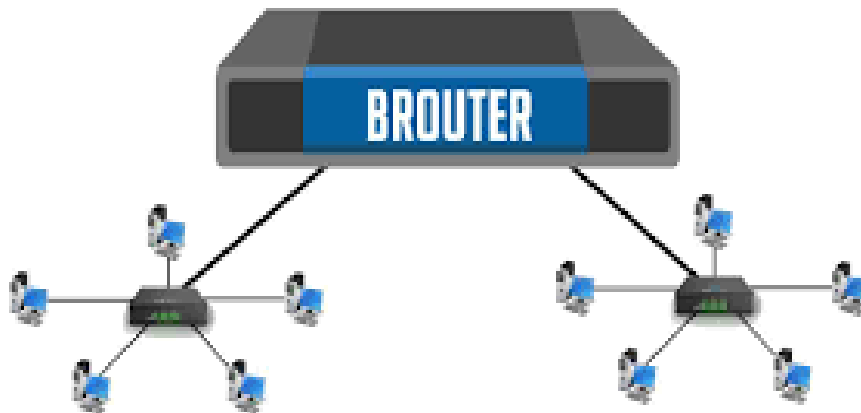
- **Router:** Routers are devices that direct traffic between hosts (A network host may offer information resources, services, and applications to users or other nodes on the network). A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. A packet is typically forwarded from one router to another router through the networks until it reaches its destination node. A router operates at Layer 3(network layer).



➤ **BRouter:** A brouter is a device that functions as both a bridge and a router. It can forward data between networks (serving as a bridge), but can also route data to individual systems within a network (serving as a router).

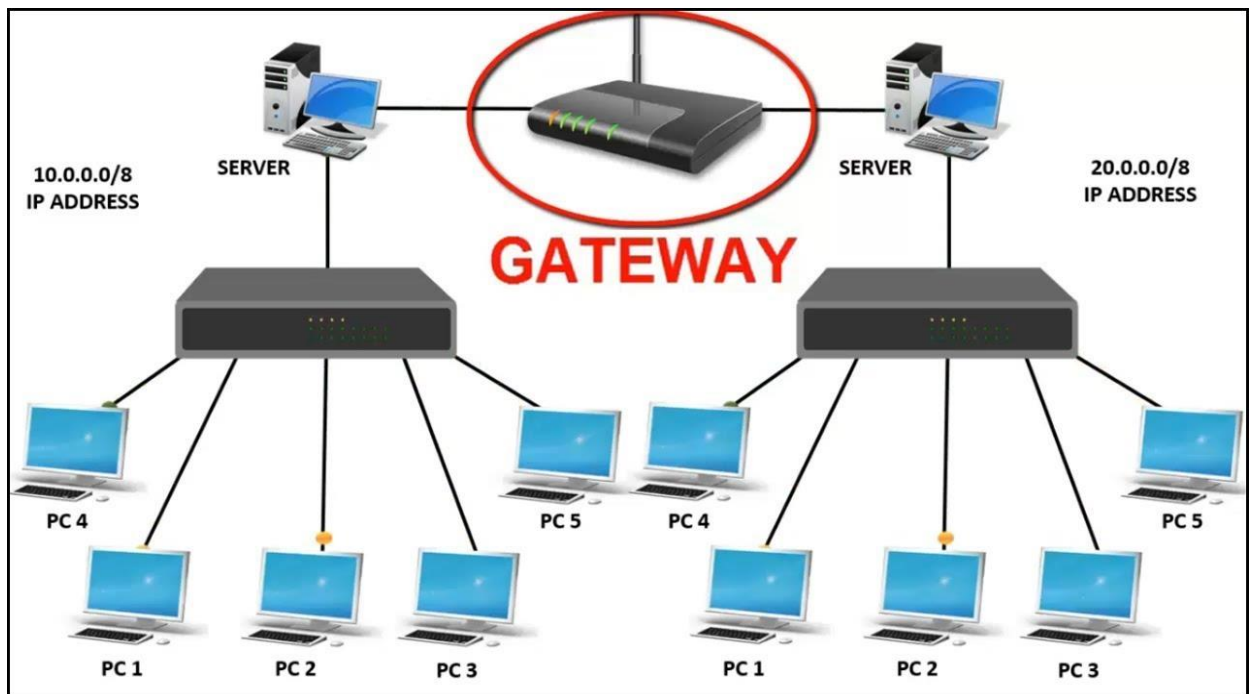
The main purpose of a bridge is to connect two separate networks. It simply forwards the incoming packets from one network to the next. A router, on the other hand, is more advanced since it can route packets to specific systems connected to the router. A brouter combines these two functions by routing some incoming data to the correct systems, while forwarding other data to another network. In other words, a brouter functions as a filter that lets some data into the local network, while redirecting unrecognized data to another network.

Is used on networks that operate with several different protocols.



- **Gateway:** A network gateway joins two networks so the devices on one network can communicate with the devices on another network. Without gateways, you couldn't be able to access the internet, communicate and send data back and forth. A gateway can be implemented completely in software, hardware, or a combination of both. Because a network gateway by definition appears at the edge of a network.

Gateways are network protocol converters. Often the two networks that a gateway joins use different base protocols. The gateway facilitates compatibility between the two protocols. network gateways can operate at any level of the OSI model.



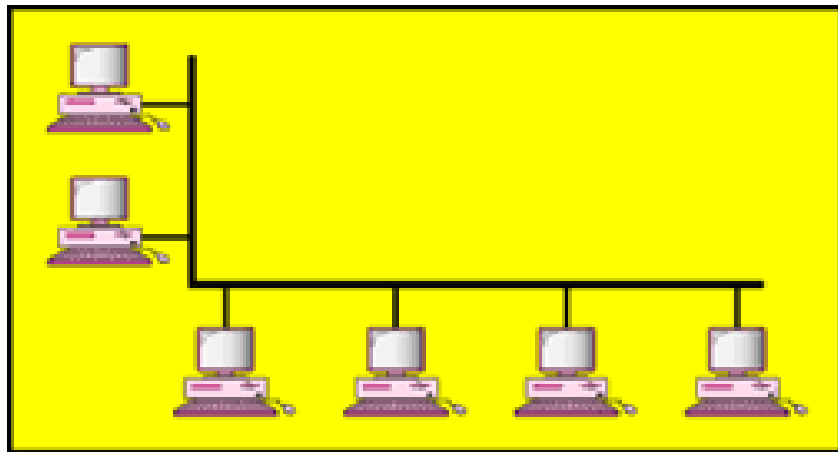
- **Switch:** A network switch (also called switching hub, bridging hub, officially MAC bridge[1]) is a computer networking device that connects devices together on a computer network by using packet switching to receive, process, and forward data to the destination device. A network switch is a multiport network bridge that uses hardware addresses to process and forward data at layer 2 (data link layer).



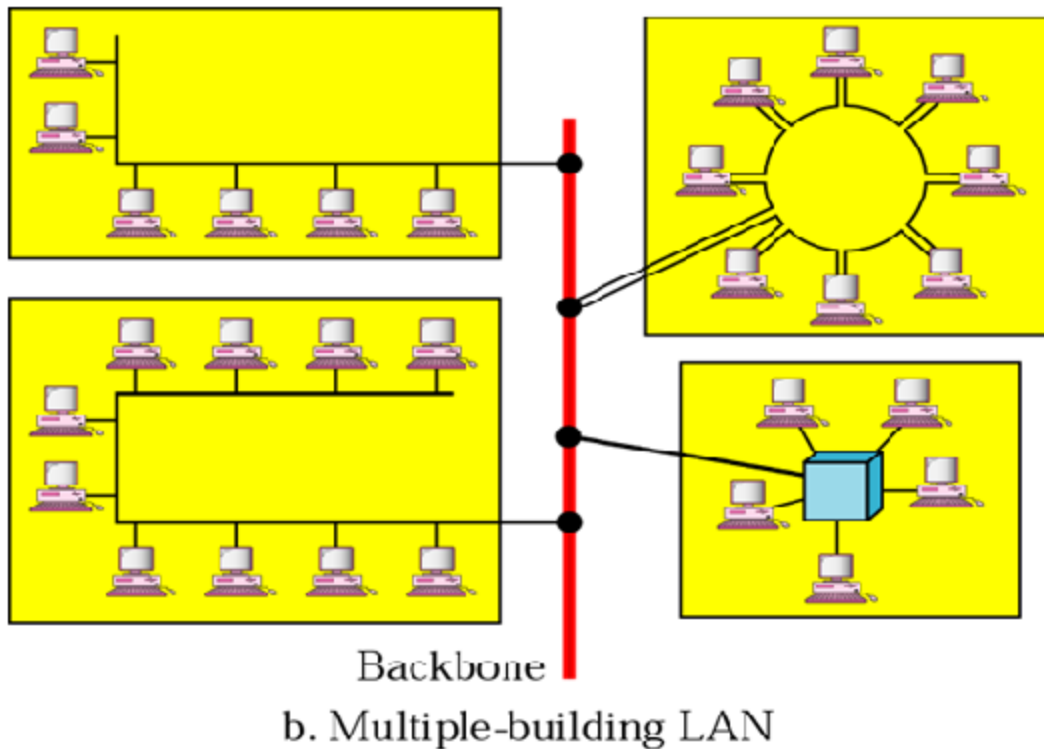
✚ Network Classification(Categories):

1- A local area network (LAN) :

Is usually privately owned and links the devices in a single office, building, or campus (see Figure below a ,b). Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals. Currently, LAN size is limited to a few kilometers. In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star. Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps.



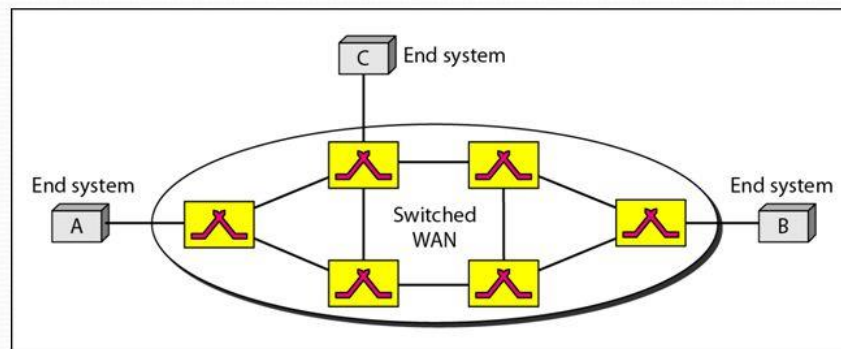
a. Single-building LAN



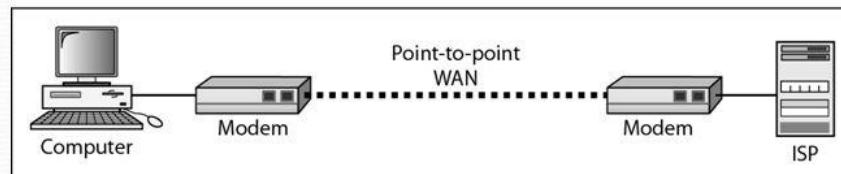
2- Wide Area Network(WAN):

Support long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continental, or even the whole world. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet. We normally refer to the first as a switched WAN and to the second as a point-to-point WAN (see Figure). The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN. The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a Home computer or a small LAN to an Internet service provider (ISP). world wide web (WWW) is an example of WAN Network.

WANs: a switched WAN v. a point-to-point WAN



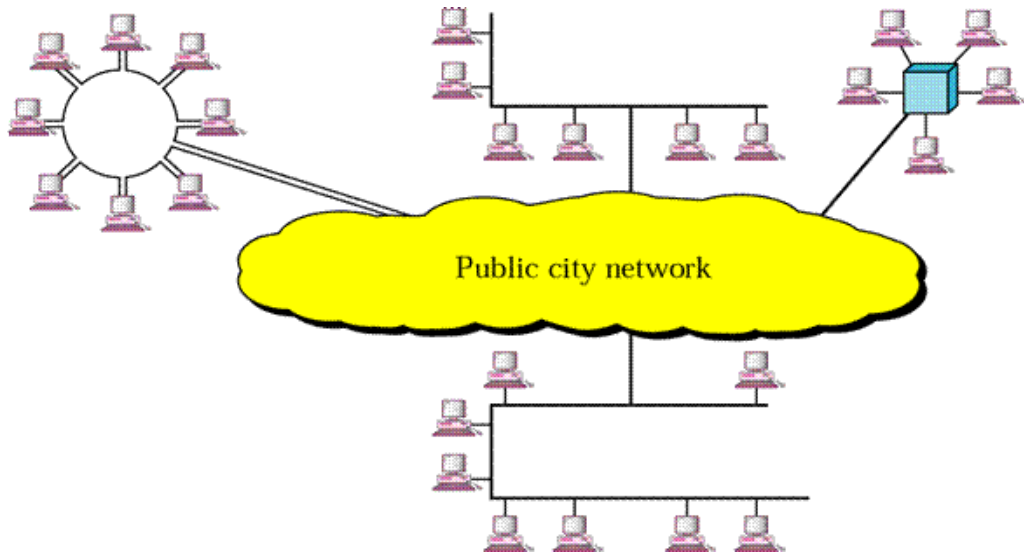
a. Switched WAN



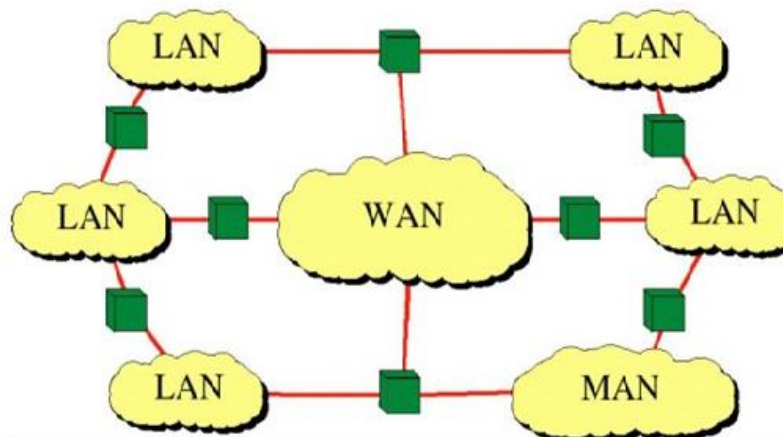
b. Point-to-point WAN

3-Metropolitan Area Networks (MAN):

A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the Internet, and have end points spread over a city or part of city. A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer. Another example is the cable TV network that originally was designed for cable TV.



But Today can also be used for high-speed data connection to the Internet as shown in figures below



LAN Vs WAN

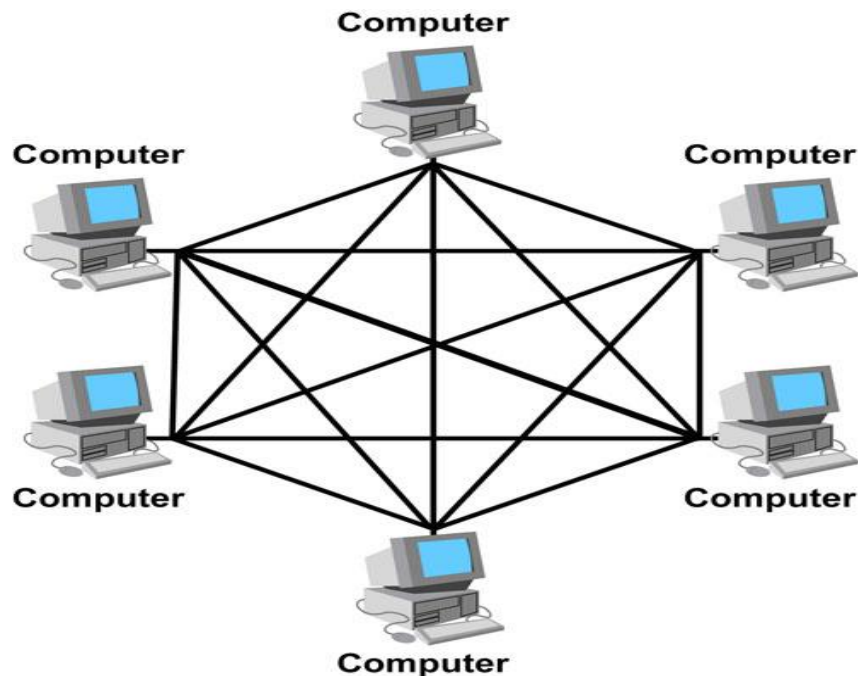
LAN	WAN
Connects host within a relatively small geographical area. <ul style="list-style-type: none">• Same Building• Same room• Same Campus	Hosts may be widely dispersed. <ul style="list-style-type: none">• Across Campuses• Across Cities/countries/continent
Faster	Slower
Cheaper	Expensive
Under a control of single ownership.	Not under a control of a single person.
Typical Speeds: 10 Mbps to 10Gbps	Typical Speed: 64 Kbps to 8 Mbps

Network topology :

Topology refers to the shape of the network or in other terms it is the network layout. The way the computers in a network are physically linked to each other and how they communicate with each other is determined by the network topology.

1. Mesh Topology:

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to $n - 1$ node, node 2 must be connected to $n - 1$ nodes, and finally node n must be connected to $n - 1$ nodes. We need $n(n - 1)$ physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. See figure below



The Advantages of Mesh Topology:

- 1-** The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
- 2-** a mesh topology is robust
- 3-** the advantage of privacy or security
- 4-** Point-to-point links make fault identification and fault isolation easy.

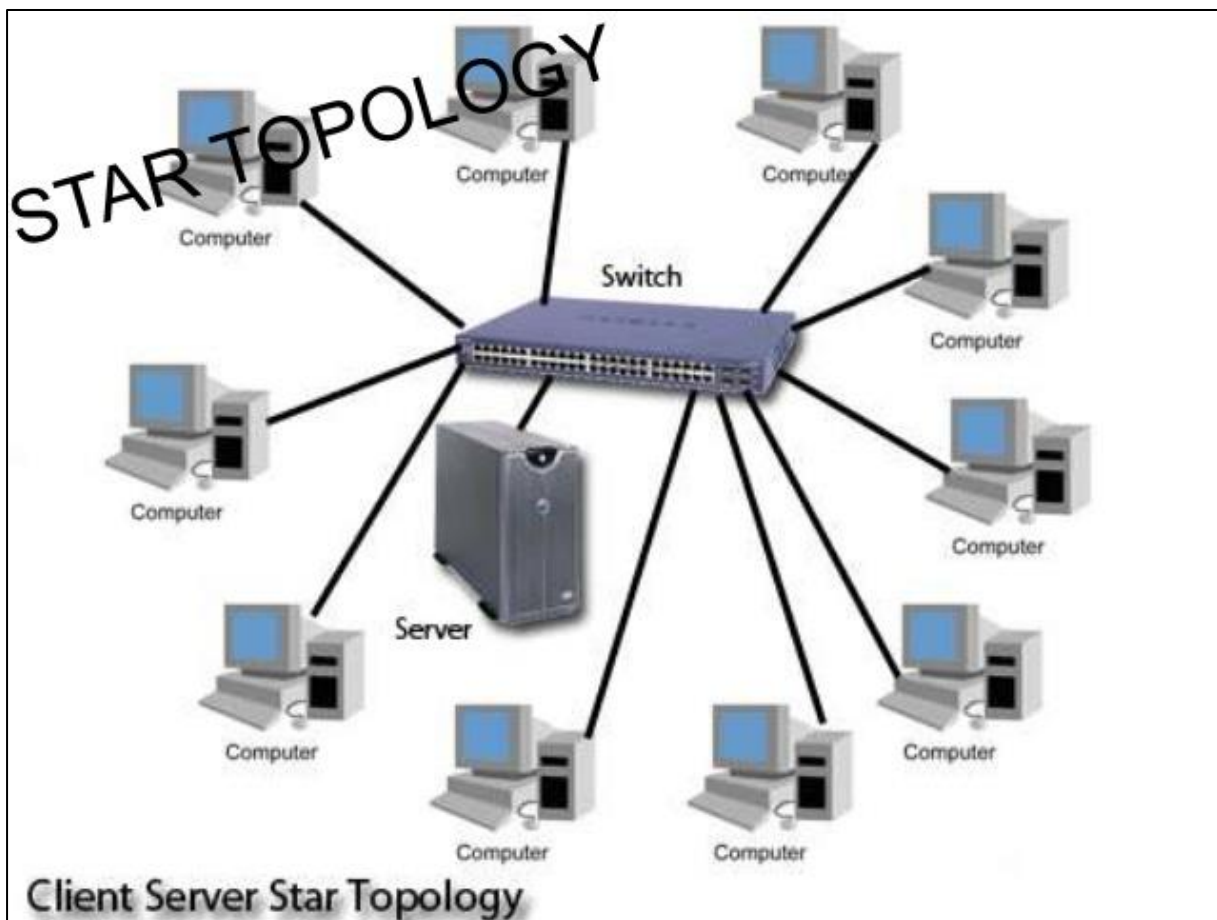
The disadvantages of Mesh topology related to the amount of cabling and the number of I/O ports required:

- 1-** Every device must be connected to every other device, installation and reconnection are difficult.
- 2-** The sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
- 3-** The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

2. Star Topology:

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device. See figure below



The Advantages of Star topology :

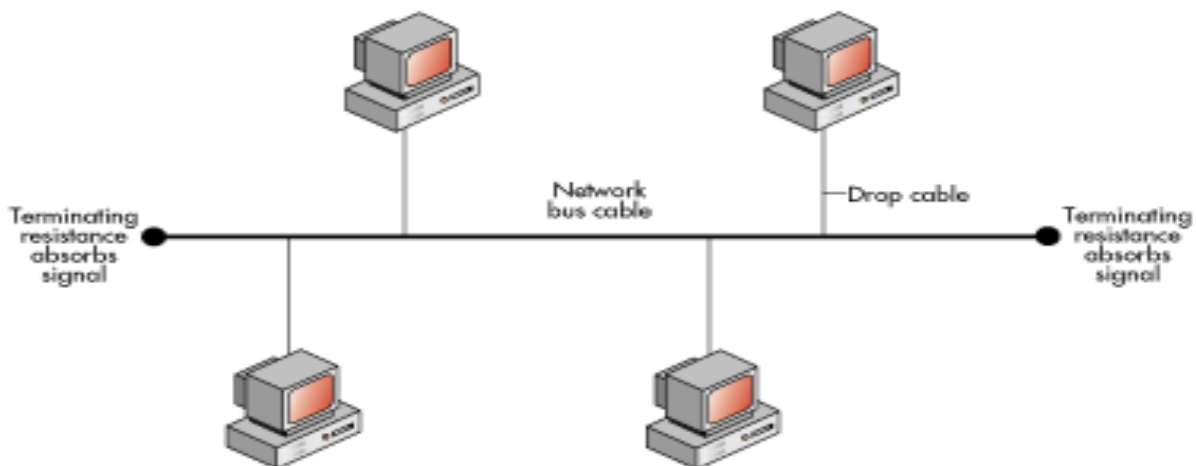
1. A star topology is less expensive than a mesh topology
2. It easy to install and reconfigure
3. Include robustness. If one link fails, only that link is affected. All other links remain active.
4. Easy fault identification and fault isolation.

The Disadvantages of Star topology:

1. One big disadvantage of a star topology is the dependency of the Whole topology on one single point, the hub. If the hub goes down, the whole system is dead.
 2. Each node must be linked to a central hub. For this reason, often, more cabling is required in a star than in some other topologies (Such as ring or bus).
- The star topology is used in local-area networks (LANs).

3. Bus Topology:

The preceding examples all describe point-to-point connections. A bus topology, on the other hand, is multipoint. One long cable acts as a backbone to link all the devices in a network. Nodes are connected to the bus cable by drop lines and taps. See figure below



The advantages of Bus topology:

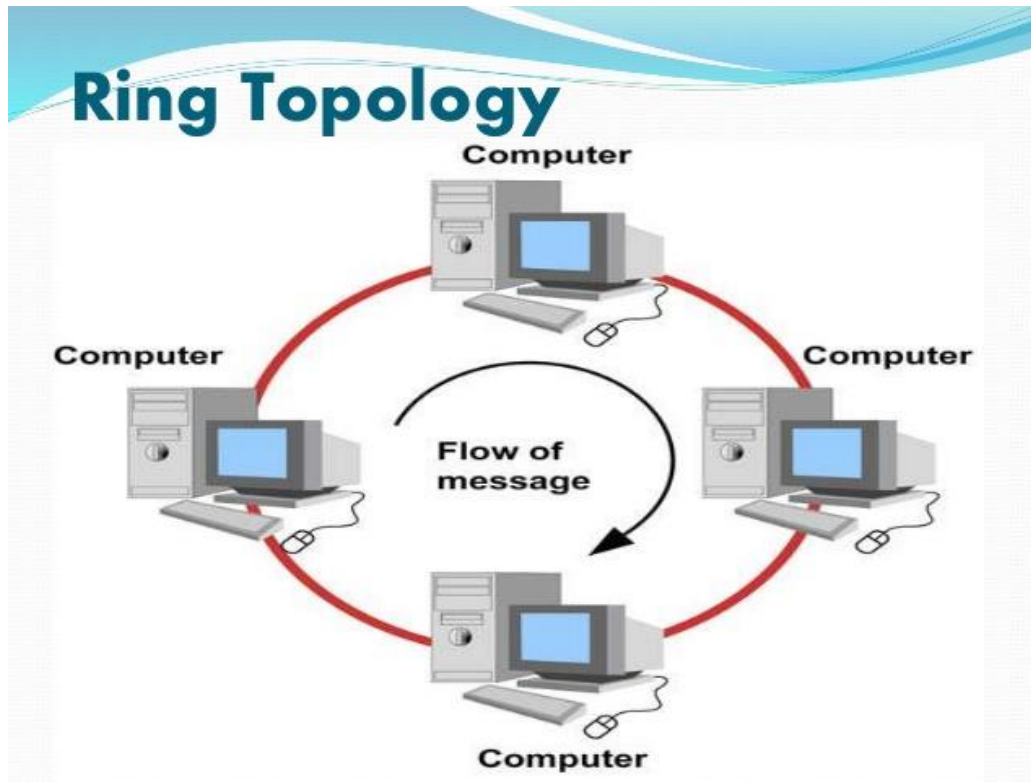
1. Ease of installation. Backbone cable can be laid along the most efficient path, and then connected to the nodes by drop lines of various lengths.
2. In this way, a bus uses less cabling than mesh or star topologies.

The Disadvantages of Bus topology:

1. Include difficult reconnection and fault isolation, fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.
2. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable.
 - Bus topology was the one of the first topologies used in the design of early local area networks.

4. Ring Topology:

In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along. see Figure below

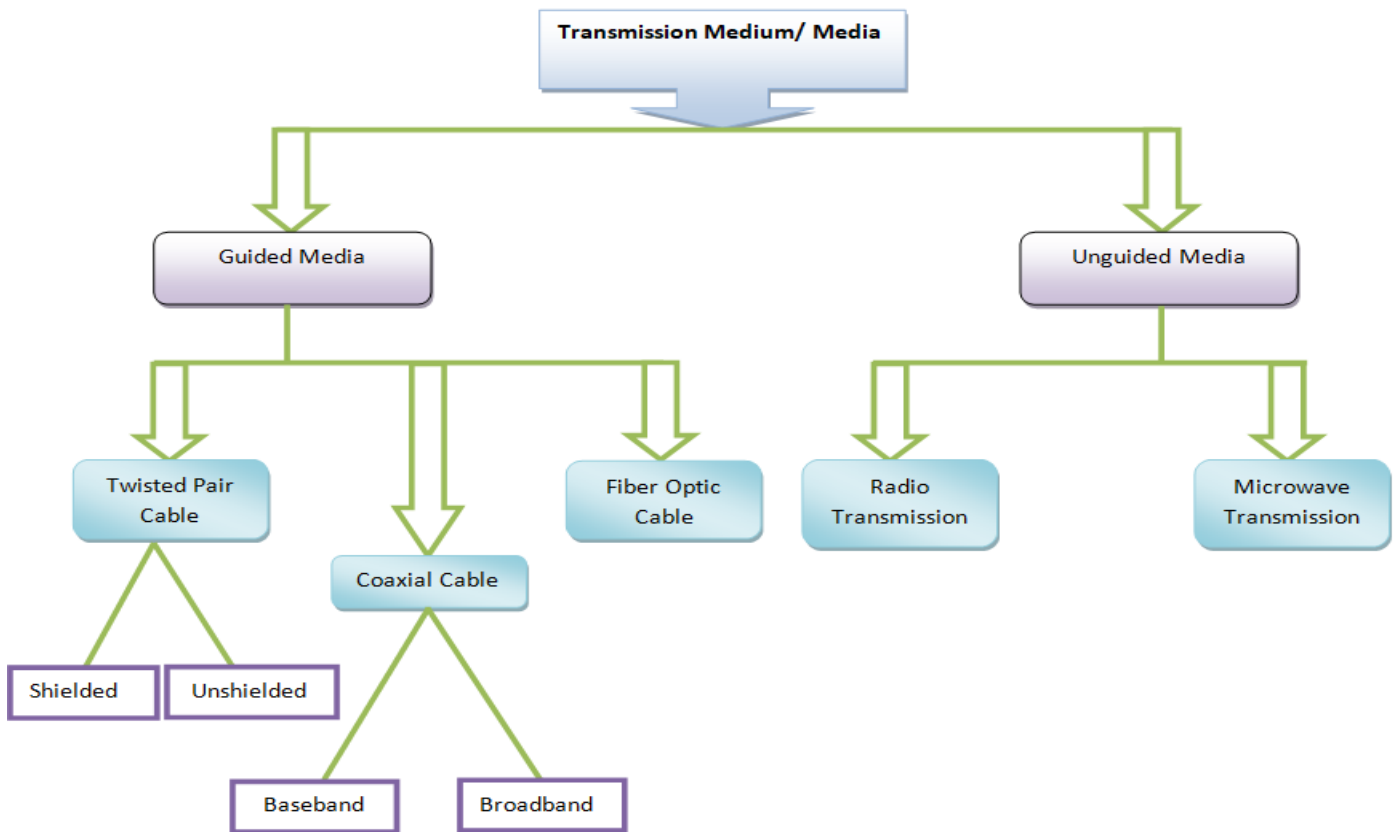


The Advantages of ring topology:

1. Easy to install and reconfigure.
2. To add or delete a device requires changing only two connections.
3. Fault isolation is simplified.

The Disadvantages of ring topology: Unidirectional traffic can be a disadvantage in a simple ring, a break in the ring (such as a disabled station) can disable the entire network.

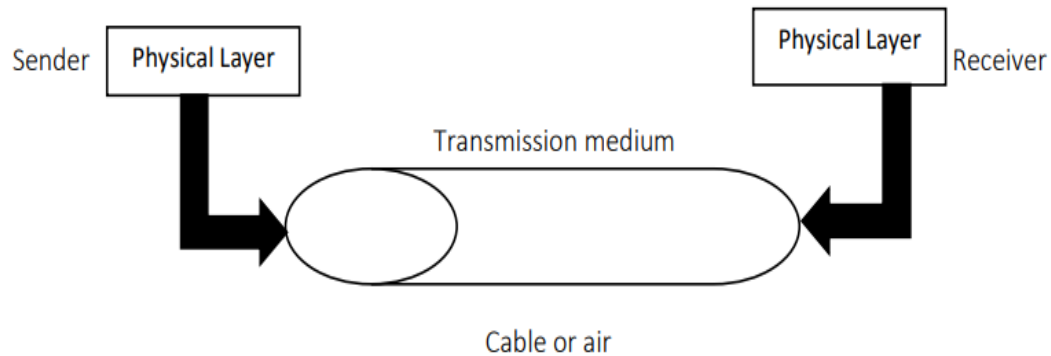
Transmission Medium



✚ Transmission Medium

The transmission medium is the physical path between transmitter and receiver in a data transmission system. Various physical media can be used for the actual transmission. Each one has its own bandwidth, delay, cost, and ease of installation and maintenance. Transmission media can be classified as “**guided or unguided**”. In both cases, communication is in the form of electromagnetic waves. With guided media, the waves are guided along a solid medium, such as **copper twisted pair, copper coaxial cable, and optical fiber.**

The purpose of the physical layer is to transport a raw bit stream from one machine to another.



The atmosphere , outer space , laser and radio are examples of unguided media that provide a means of transmitting electromagnetic signals but do not guide them; this form of transmission is usually referred to as wireless transmission.

The characteristics and quality of a data transmission are determined both by **the characteristics of the medium and the characteristics of the signal**. **In the case of guided media, the medium itself is more important in determining the limitations of transmission.**

For unguided media, the bandwidth of the signal produced by the transmitting antenna is more important than the medium in determining transmission characteristics.

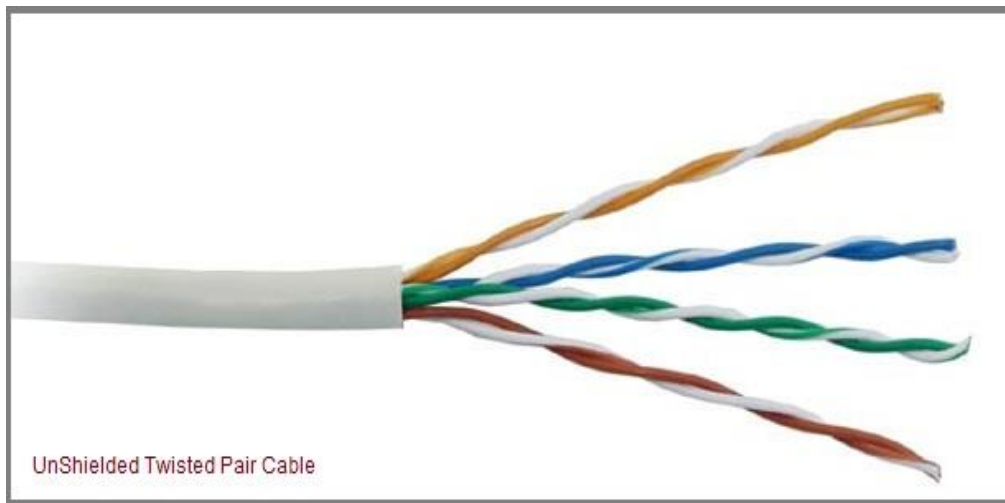
One key property of signals transmitted by antenna is directionality. In general, **signals at lower frequencies are omnidirectional (not having a specific direction)**, that is, the signal propagates in all directions from the antenna. **At higher frequencies**, it is possible to focus the signal into a directional beam.

In considering the design of data transmission systems, a key concern, is **data rate and distance**: greater data rate and distance, is the better. A number of design factors relating to the transmission medium and to the signal determine the data rate and distance.

➤ Guided media

Which are those that provide conduit from one device to another include **twisted-pair cable, coaxial cable and fiber optic cable** . A signal traveling along any of these media is directed and contained by physical limits of the medium. Twisted-pair and coaxial cable use metallic(copper) conductor that accept and transport signals in the form of electric current. **Optical fiber** is a cable that accepts and transport signals in the form of **light**.

1. Twisted Pair



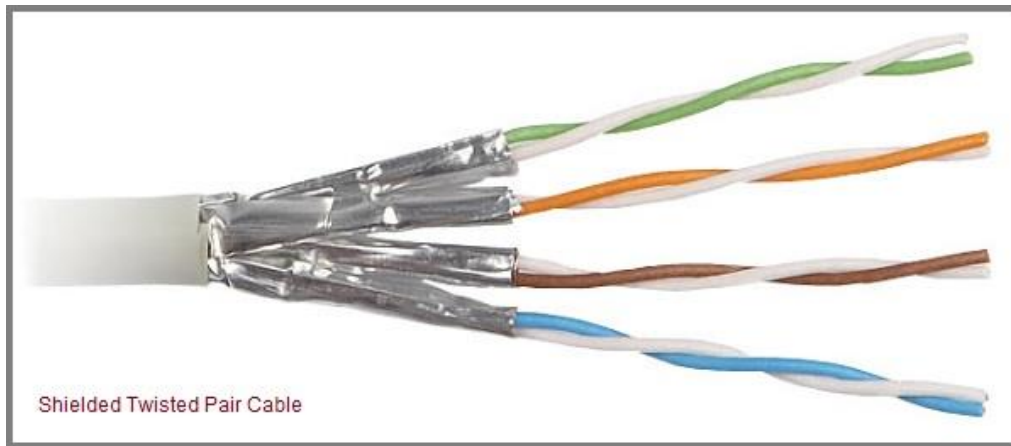
The oldest and still most common transmission medium is twisted pair. A twisted pair consists of two insulated copper wires, typically 1mm thick. The wires are twisted together in a helical form, just like a DNA molecule. The purpose of twisting the wires is to reduce electrical interference from similar pairs close by. The most common twisted-pair cable used in communications is referred to as **unshielded twisted-pair (UTP)**. Due to its low cost, UTP cabling is used extensively for local-area networks (LANs) and telephone connections.

UTP cabling does not offer as high bandwidth or as good protection from interference as coaxial or fiber optic cables, but it is less expensive and easier to work with. There are several UTP categories, which increase in bandwidth, for example:

CAT1 = up to 1Mbps | **CAT2** = up to 4 Mbps | **CAT5e** = up to 1Gbps



Also there is a version of twisted-pair cable used called **shielded twisted pair (STP)**. **STP** cable has a metal foil jacket to cancel any external interference covering each pair of insulated conductors. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk noise, it is bulkier and more expensive. **STP** cabling often is used in Ethernet networks, especially fast data rate Ethernets.



The most common application of the twisted pair is the telephone system. Twisted pairs can run several kilometers without **amplification**, but for longer distances, repeaters are needed. Twisted pairs can be used for either analog or digital transmission. The bandwidth depends on the thickness of the wire and the distance traveled. Due to their adequate performance and low cost, twisted pairs are widely used and are likely to remain so for years to come. Twisted pair cabling comes in several varieties, two of which are important for computer networks.

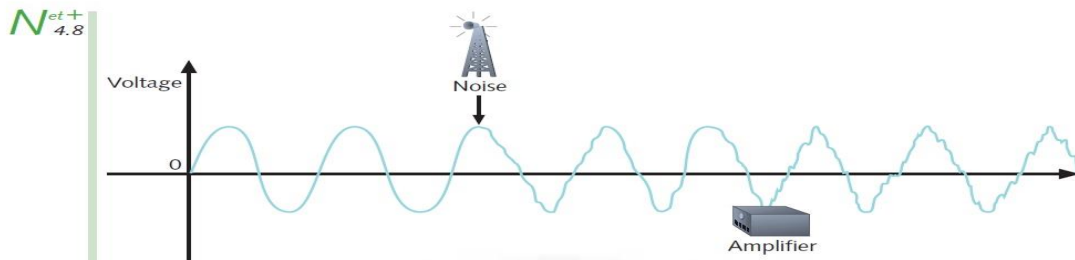


Figure 3-12 An analog signal distorted by noise and then amplified

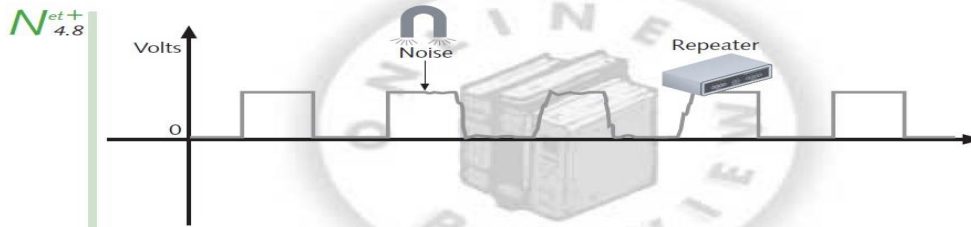


Figure 3-13 A digital signal distorted by noise and then repeated

- **Category 3** twisted consist of two insulated wires gently twisted together. Four such pairs are typically grouped together in a plastic sheath for protection and to keep the eight wires together.
- **Category 5** twisted pairs are similar to category 3 pairs, but with more twists per centimeter and Teflon insulation, which results in less crosstalk and a better quality of signal over longer distances, making them more suitable for high-speed computer communication. Both of these wiring types are often referred to as **UTP (Unshielded Twisted Pair)**.

2.Coaxial Cable

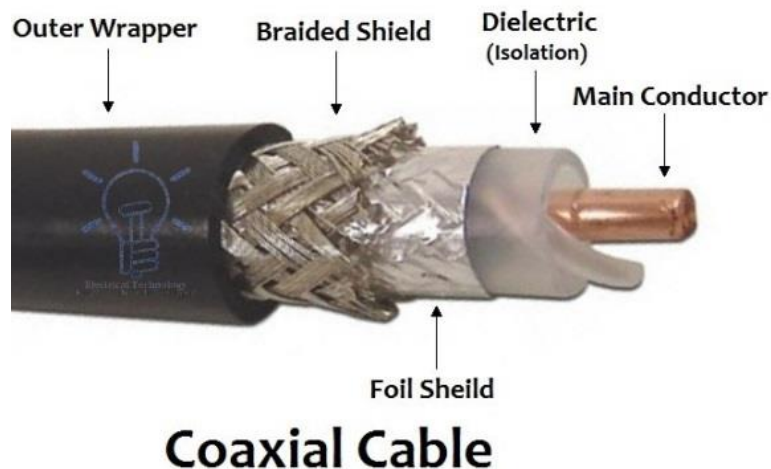
Another common transmission medium is the coaxial cable (known as coax), it has better shielding than twisted pair, so it can span longer distances at higher speeds, Coaxial cables are high-frequency transmission cables made up of a single solid-copper core. Data is transferred electrically over the inner conductor and has **80X more transmission capacity** than twisted pair cables.

Coaxial cables do not produce external electric and magnetic fields and are not affected by them, This makes them ideally suited, although more expensive, for transmitting signals. This cable is suitable for point to point or point to multipoint applications.

➤ Two kinds of coaxial cables are widely used:

1. One kind, 50-ohm cable is commonly used for digital transmission.
2. The other kind, 75-ohm cable is commonly used for analog transmission.

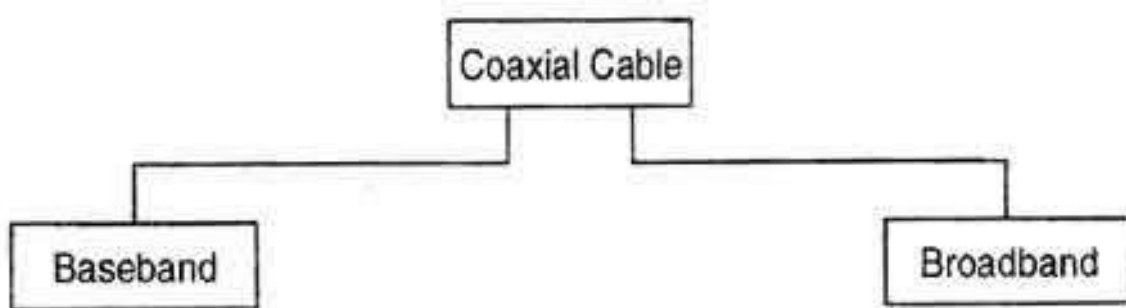
A coaxial cable consists of a stiff copper wire as the core, surrounded by an insulating material. Insulating material is encased by a cylindrical conductor, often as a closely woven braided mesh. The outer conductor is covered in a protective plastic sheath. A cutaway view of a coaxial cable is shown in the figure below:



The construction and shielding of the coaxial cable give it a good combination of high bandwidth and excellent noise immunity. The bandwidth possible depends on the cable length. Coax is still widely used for cable television and some local area networks.

➤ Types of Coaxial Cables

There are two types of coaxial cables:

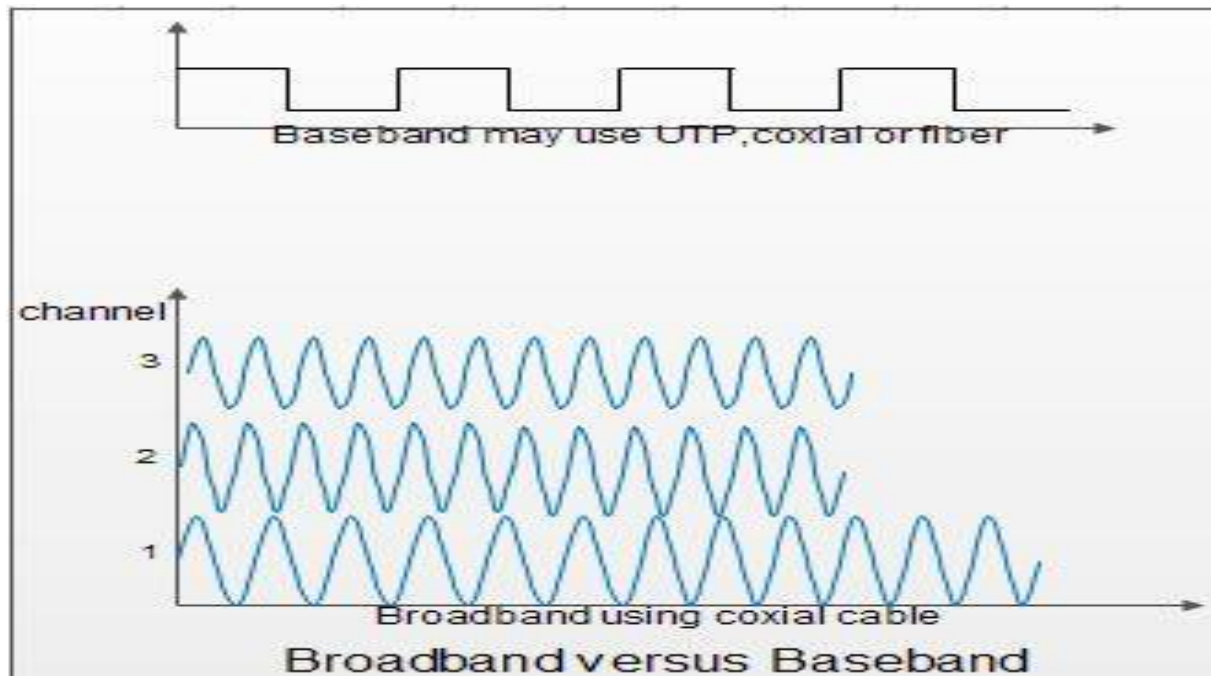


1. A baseband coaxial cable

- Baseband coaxial cables are 50 ohm cables used for 'digital transmission'.
- Transmits a single signal at a time at very high speed.
- Baseband coaxial cable supports frequency range of a-4kHz and are used for digital signaling.

2. A broadband coaxial cable

- Broadband coaxial cables are 75 ohm cables used for analog transmission.
- Can transmit many simultaneous signals using different frequencies. A baseband cable is mainly used for LANs.
- Broadband coaxial cable supports the frequency range above 4kHz and are used for analog signals.



Advantages of Coaxial Cables:

1. It can be used for both analog and digital transmission.
2. It offers higher bandwidth as compared to twisted pair cable and can span longer distances.
3. Because of better shielding in coaxial cable, loss of signal or attenuation is less.
4. Better shielding also offers good noise immunity.
5. It is relatively inexpensive as compared to optical fibers.
6. It has lower error rates as compared to twisted pair.
7. It is not as easy to hack as twisted pair because copper wire is contained in plastic jacket.

Disadvantages of Coaxial Cables:

1. It is usually more expensive than twisted pair.
2. High installation cost. High maintenance cost.

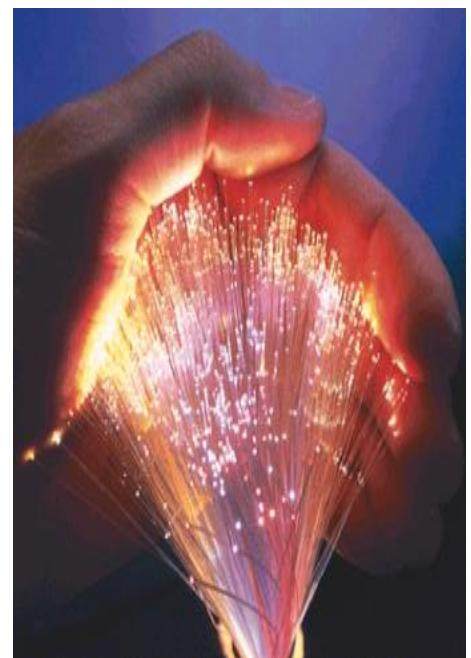
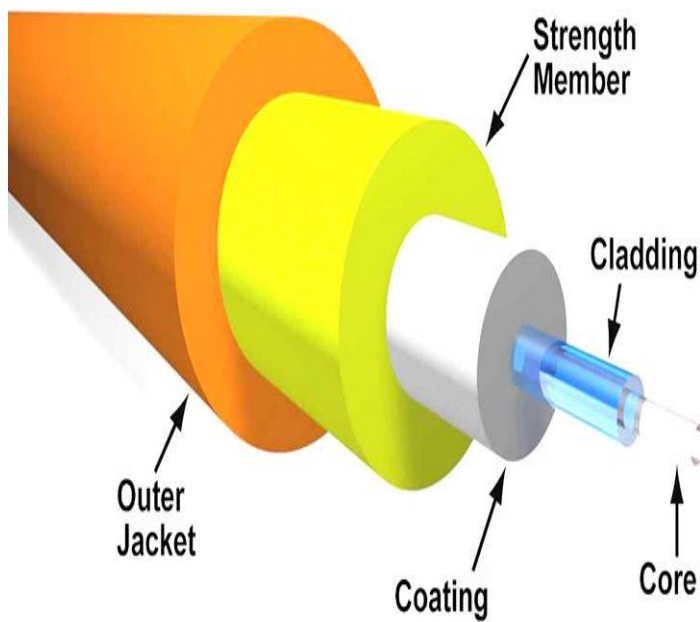
3.Fiber Optics (Optical Fiber)

Introduction:

While copper wire cables were the traditional choice for telecommunication, networking and cable connections for years, fiber optics has become a common alternative. Optical fiber carries more information than conventional copper wire, due to its higher bandwidth and faster speeds. Because glass does not conduct electricity, fiber optics is not subject to electromagnetic interference, and signal losses are minimized. In addition, fiber optic cables can be flooded in water and are used in more at-risk environments like undersea cable. Fiber optic cables are also stronger, thinner and lighter than copper wire cables and do not need to be maintained or replaced as frequently.

Fiber optics, refers to the medium and the technology associated with the transmission of information as **light pulses** along a glass or plastic strand or fiber. A fiber optic cable can contain a varying number of these glass fibers from a few up to a couple hundred.

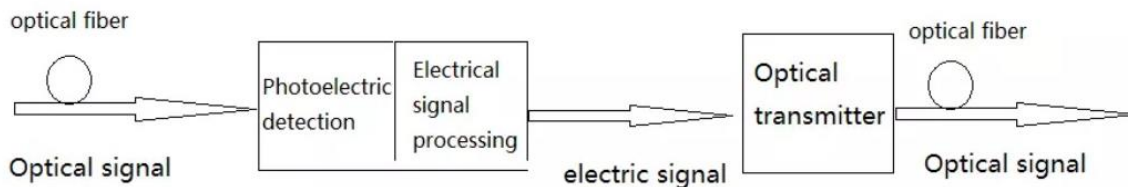
Surrounding the **glass fiber core** is another glass layer called **cladding**. A layer known as a **buffer tube** protects the cladding, and a **jacket layer** acts as the final protective layer for the individual strand or fiber.



How Fiber Optics Works

Fiber optics transmit data in the form of light particles or photons that pulse through a fiber optic cable. The glass fiber core and the cladding each have a different refractive index that bends incoming light at a certain angle. When light signals are sent through the fiber optic cable, they reflect off the core and cladding in a series of zig-zag bounces, this process called **Total Internal Reflection (TIR)**. The light signals do not travel at the speed of light because of the denser glass layers, instead traveling about 30% slower than the speed of light.

To renew, or boost, the signal throughout its journey, fiber optics transmission sometimes requires repeaters at distant intervals to regenerate the optical signal by converting it to an electrical signal, processing that electrical signal and retransmitting the optical signal as shown in the figure below:

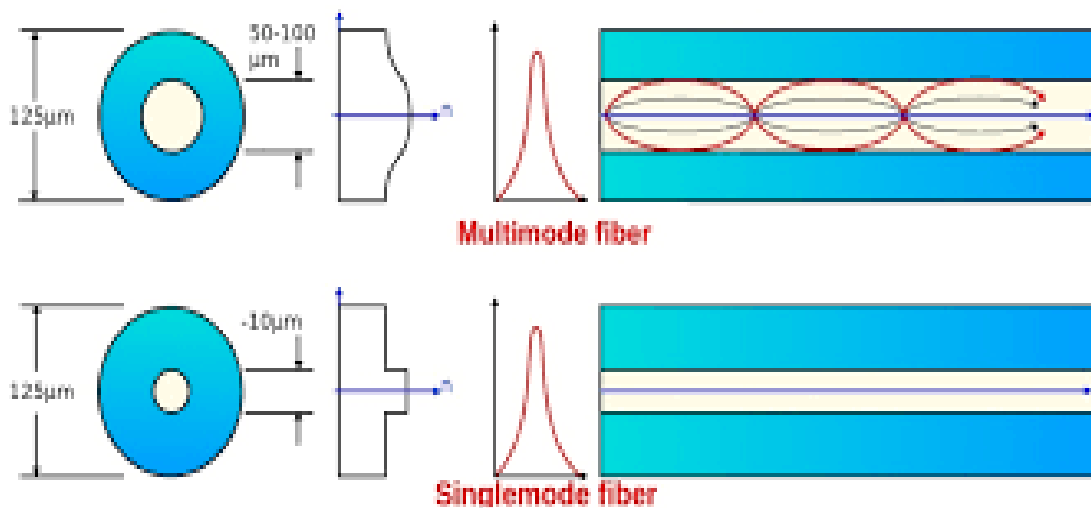
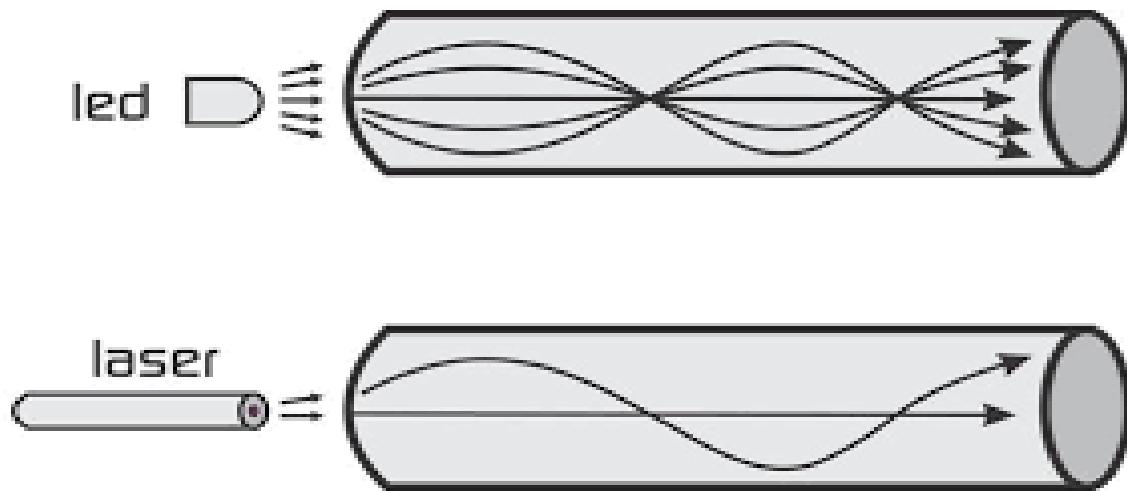


Types of Fiber Optic Cables

Multimode fiber and single-mode fiber are the two primary types of fiber optic cable.

1. [Single-mode fiber](#) (SMF): Is used for longer distances due to the smaller diameter of the glass fiber core, which lessens the possibility for [attenuation](#) the reduction in signal strength. The smaller opening isolates the light into a single beam, which offers a more direct route and allows the signal to travel a longer distance. Single-mode fiber also has a considerably higher [bandwidth](#) than multimode fiber. The light source used for single-mode fiber is typically a [laser](#). Single-mode fiber is usually more expensive because it requires precise calculations to produce the laser light in a smaller opening.

2. Multimode fiber (MMF): Is used for shorter distances because the larger core opening allows light signals to bounce and reflect more along the way. The larger diameter permits multiple light pulses to be sent through the cable at one time, which results in more data transmission. This also means that there is more possibility for signal loss, reduction or interference, however. Multimode fiber optics typically use an [LED](#) to create the light pulse.



➤ **Optical Transmission System has three components:**

1. The light source: A pulse of light indicates a 1-bit and the absence of light indicates a Zero bit.

2. The transmission medium: The transmission medium is an ultra-thin fiber of glass.

3. The detector: The detector generates an electrical pulse when light falls on it, by attaching a light source to one end of an optical fiber and a detector on the other, we have a unidirectional data transmission system that accepts an electrical signal, converts and transmits it by light pulses, and then reconverts the output to an electrical signal at the receiving end.

➤ Two different types of light source are used in fiber optic systems: the **light emitting diode (LED)** and the **injection laser diode (ILD)**. Both are semiconductor devices that emit a beam of light when a voltage is applied. The LED is less costly, operates over a greater temperature range, and has a longer operational life. The ILD, which operates on the laser principle, is more efficient and can support greater data rates.

➤ **Advantages and Disadvantages of Optical Fiber**

✚ **Advantages Fiber-optic cable has several advantages over metallic cable (twisted pair or coaxial):**

1. Higher bandwidth. Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable. Currently, data rates and bandwidth utilization over fiber-optic cable are **limited** not by the medium but by the signal generation and reception technology available.
2. Less signal attenuation. Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.
3. Immunity to electromagnetic interference. Electromagnetic noise cannot affect fiber-optic cables.
4. Resistance to corrosive materials. Glass is more resistant to corrosive materials than copper.
5. Light weight. Fiber-optic cables are much lighter than copper cables.
6. Greater immunity to tapping. Fiber-optic cables are more immune to tapping than copper cables. Copper cables create antenna effects that can easily be tapped.

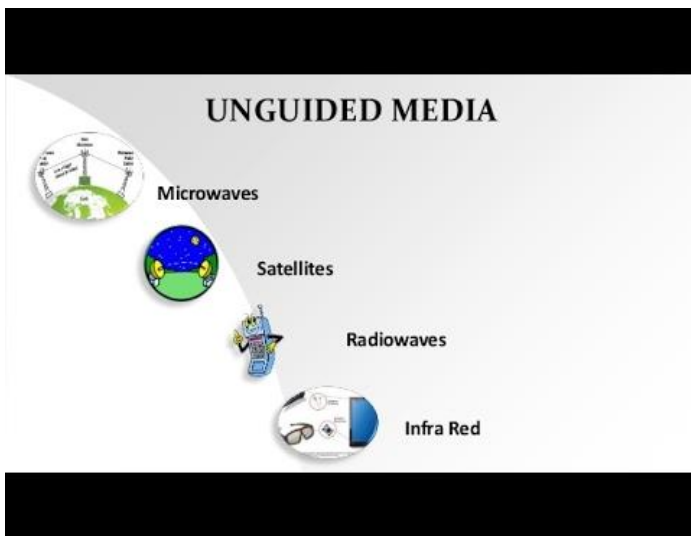
✚ **Disadvantages There are some disadvantages in the use of optical fiber.**

1. Installation and maintenance. Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
2. Unidirectional light propagation. Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
3. Cost. The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.

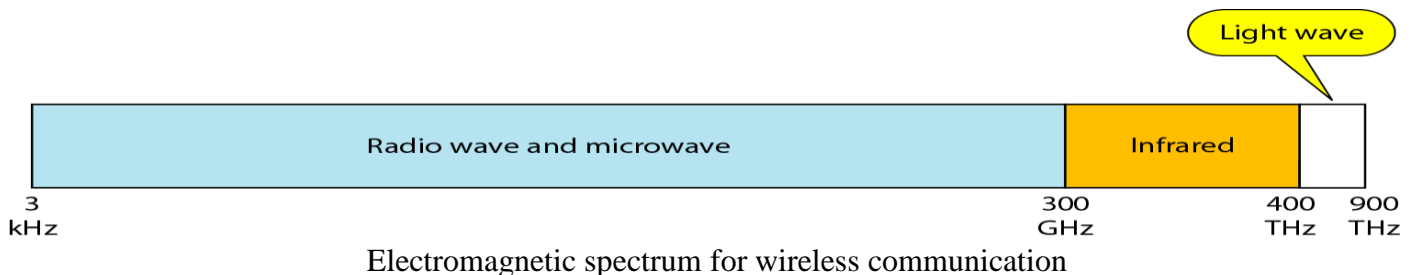
UNGUIDED MEDIA: WIRELESS

Unguided media transport electromagnetic waves without using a physical conductor, for unguided media, transmission and reception are achieved by means of an antenna. For transmission, the antenna radiates electromagnetic energy into the medium (usually air), and for reception, the antenna picks up electromagnetic waves from the surrounding medium. This type of communication is often referred to as wireless communication.

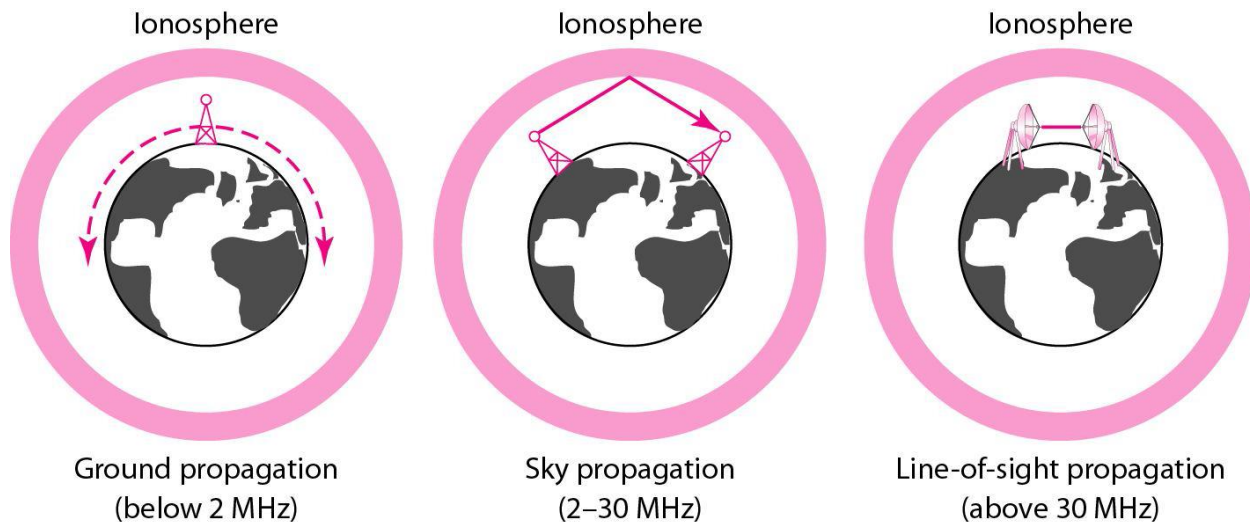
There are basically two types of configurations for wireless transmission: directional and omnidirectional. For the directional configuration, the transmitting antenna puts out a focused electromagnetic beam; the transmitting and receiving antennas must therefore be carefully aligned. In the omnidirectional case, the transmitted signal spreads out in all directions and can be received by many antennas. In general, the higher the frequency of a signal, the more it is possible to focus it into a directional beam.



The figure below shows the part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication.



➤ Unguided signals can travel from the source to destination in several ways: **ground propagation, sky propagation, and line-of-sight propagation**, as shown in figure below:



- **In ground propagation**, radio waves travel through the lowest portion of the atmosphere, hugging the earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet. Distance depends on the amount of power in the signal: The greater the power, the greater the distance.
- **In sky propagation**, higher-frequency radio waves radiate upward into the ionosphere (the layer of atmosphere where particles exist as ions) where they are reflected back to earth. This type of transmission allows for greater distances with lower output power.
- **In line-of-sight propagation**, very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other, Line-of-sight propagation is tricky because radio transmissions cannot be completely focused.

The section of the electromagnetic spectrum defined as radio waves and microwaves is divided into eight ranges, called bands. These bands are rated from very low frequency (VLF) to extremely high frequency (EHF). Table lists these bands, their ranges, and propagation methods.

<i>Band</i>	<i>Range</i>	<i>Propagation</i>
VLF (very low frequency)	3–30 kHz	Ground
LF (low frequency)	30–300 kHz	Ground
MF (middle frequency)	300 kHz–3 MHz	Sky
HF (high frequency)	3–30 MHz	Sky
VHF (very high frequency)	30–300 MHz	Sky and line-of-sight
UHF (ultrahigh frequency)	300 MHz–3 GHz	Line-of-sight
SHF (superhigh frequency)	3–30 GHz	Line-of-sight
EHF (extremely high frequency)	30–300 GHz	Line-of-sight

We can divide wireless transmission into three broad groups: radio waves, microwaves, and infrared waves. See Figure below:

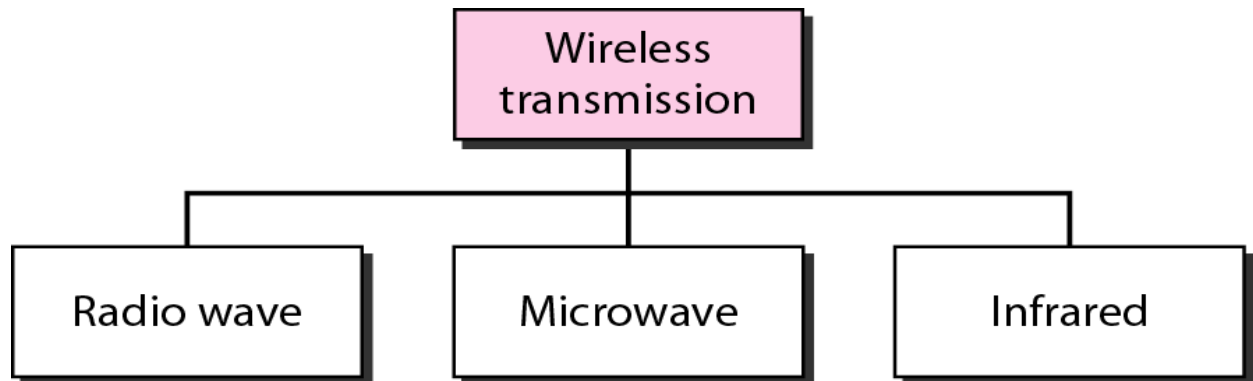


Figure show Wireless transmission waves

1. Radio Waves

Although there is no clear limit distinction between radio waves and microwaves, electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves; waves ranging in frequencies between 1 and 300 GHz are called microwaves. However, the behavior of the waves, rather than the frequencies, is a better criterion for classification.

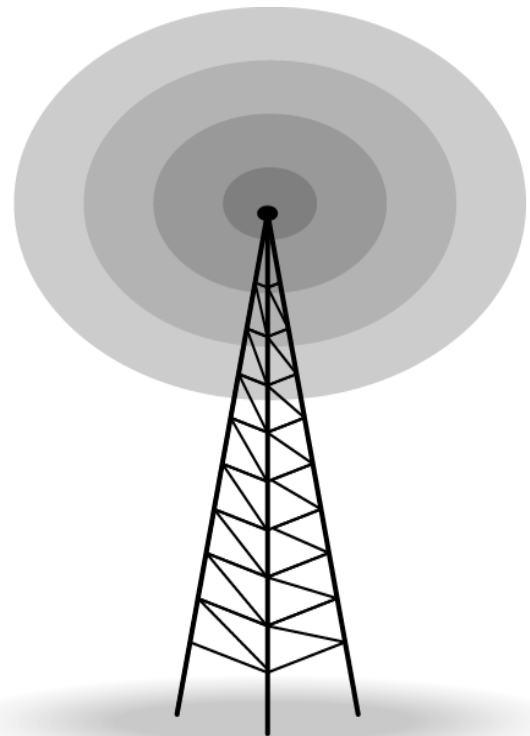
Radio waves, for the most part, are **omnidirectional**. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna sends waves that can be received by any receiving antenna. The omnidirectional property has a disadvantage, too.



The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band. Radio waves, particularly those waves that propagate in the sky mode, can travel long distances. This makes radio waves a good candidate for long-distance broadcasting such as AM radio (AM radio ranges from 535 to 1705 kHz). Radio waves, particularly those of low and medium frequencies, can penetrate walls. This characteristic can be both an advantage and a disadvantage. It is an advantage because, for example, an AM radio can receive signals inside a building. It is a disadvantage because we cannot isolate a communication to just inside or outside a building. The radio wave band is relatively narrow, just under 1 GHz, compared to the microwave band. Using any part of the band requires permission from the authorities.

➤ **Omnidirectional Antenna**

Radio waves use omnidirectional antennas that send out signals in all directions. Based on the wavelength, strength, and the purpose of transmission, we can have several types of antennas. Figure below shows an omnidirectional antenna:



Applications

The omnidirectional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. AM and FM radio (FM radio band goes from 88 to 108 MHz), television, and maritime radio are examples of multicasting.

2. Microwaves

Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves. Microwaves are **unidirectional**. When an antenna transmits microwave waves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.

➤ **The following describes some characteristics of microwave propagation:**

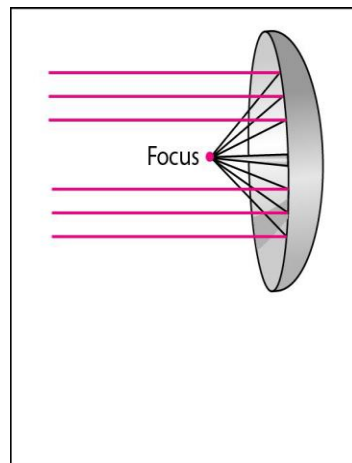
1. Microwave propagation is line-of-sight. Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall. The curvature of the earth as well as other blocking obstacles does not allow two short towers to communicate by using microwaves. Repeaters are often needed for long-distance communication.
2. Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside buildings.
3. The microwave band is relatively wide, almost 299 GHz, and hence it provides a higher data rate rather than data rate provided by radio wave band.
4. Use of certain portions of the band requires permission from authorities.

Unidirectional Antenna

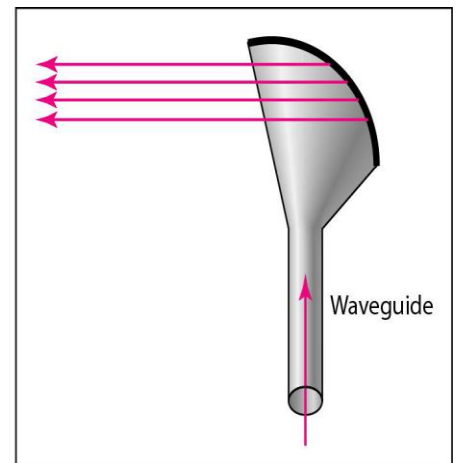
Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: the parabolic dish and the horn see figure below:

Applications

Microwaves, due to their unidirectional properties, are very useful when unicast (one-to-one) communication is needed between the sender and the receiver. The cellular phones, and wireless LANs are examples of the applications that use the microwave signals.



a. Dish antenna



b. Horn antenna

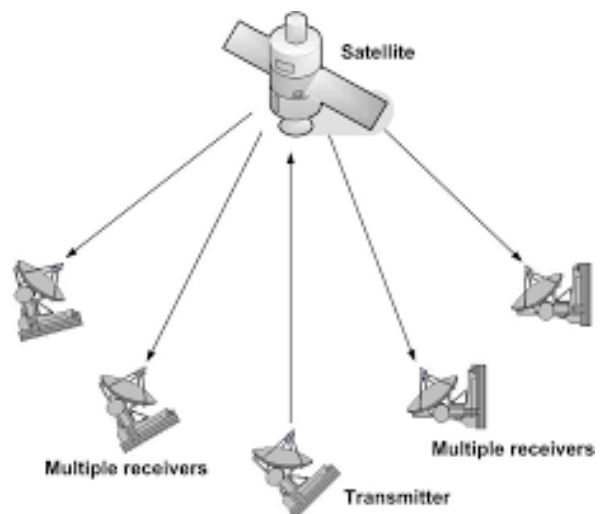
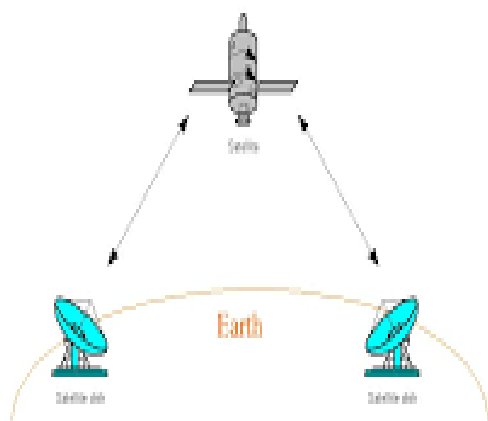
2.1 Satellite Microwave

A communication satellite is, in effect, a microwave relay station. It is used to link two or more ground-based microwave transmitter/receivers, known as earth stations, or ground stations. **The** satellite receives transmissions on one frequency band (uplink), amplifies or repeats the signal, and transmits it on another frequency (downlink). A single orbiting satellite will operate on a number of frequency bands, called transponder channels, or simply transponders. Figure below depicts, in a general way, two common configurations for satellite communication. In the first, the satellite is being used to provide a point-to-point link between two distant ground-based antennas. In the second, the satellite provides communications between one ground-based transmitter and a number of ground-based receivers.

To remain stationary, the satellite must have a period of rotation equal to the earth's period of rotation. The communication satellite is a technological revolution as important as fiber optics. Among the most important applications for satellites are:

- Television distribution
- Long-distance telephone transmission
- Private business networks

Point-to-Point Link via Satellite Microwave



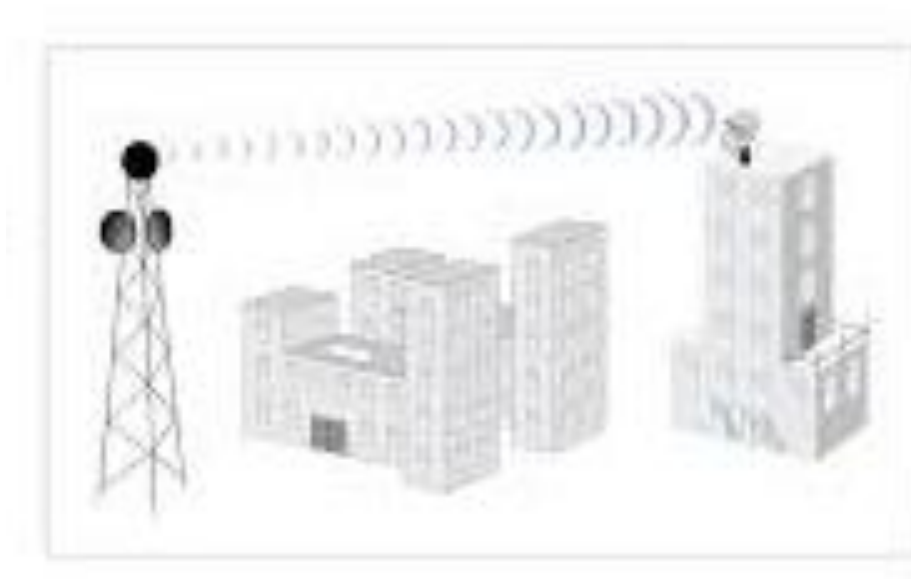
(b) Broadcast link via satellite microwave

The optimum frequency range for satellite transmission is 1 to 10 GHz. Below 1 GHz, there is significant noise from natural sources, including galactic, solar, and atmospheric noise, and human-made interference from various electronic devices. Above 10 GHz, the signal is severely attenuated by atmospheric absorption and precipitation.

2.2 Terrestrial Microwave

The antenna is fixed rigidly and focuses a narrow beam to achieve line-of-sight transmission to the receiving antenna. To achieve long-distance transmission, a series of microwave relay towers is used; point-to-point microwave links are strung together over the desired distance.

The primary use for terrestrial microwave systems is in long-haul telecommunications service, as an alternative to coaxial cable or optical fiber. The microwave facility requires far fewer amplifiers or repeaters than coaxial cable over the same distance, but requires line-of-sight transmission.



3. Infrared (IR)

Infrared waves, with frequencies from 300 GHz to 400 THz can be used for short- range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another; a short-range communication system in one room cannot be affected by another system in the next room.

When we use our infrared remote control, we do not interfere with the use of the remote by our neighbors. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Applications

The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate. The Infrared Data Association (IrDA), an association for use of infrared waves, has established standards for using these signals for communication between devices such as keyboards, mice, PCs, and printers.

For example, some manufacturers provide a special port called the IrDA port that allows a wireless keyboard to communicate with a PC. Infrared signals defined by IrDA transmit through **line of sight**.

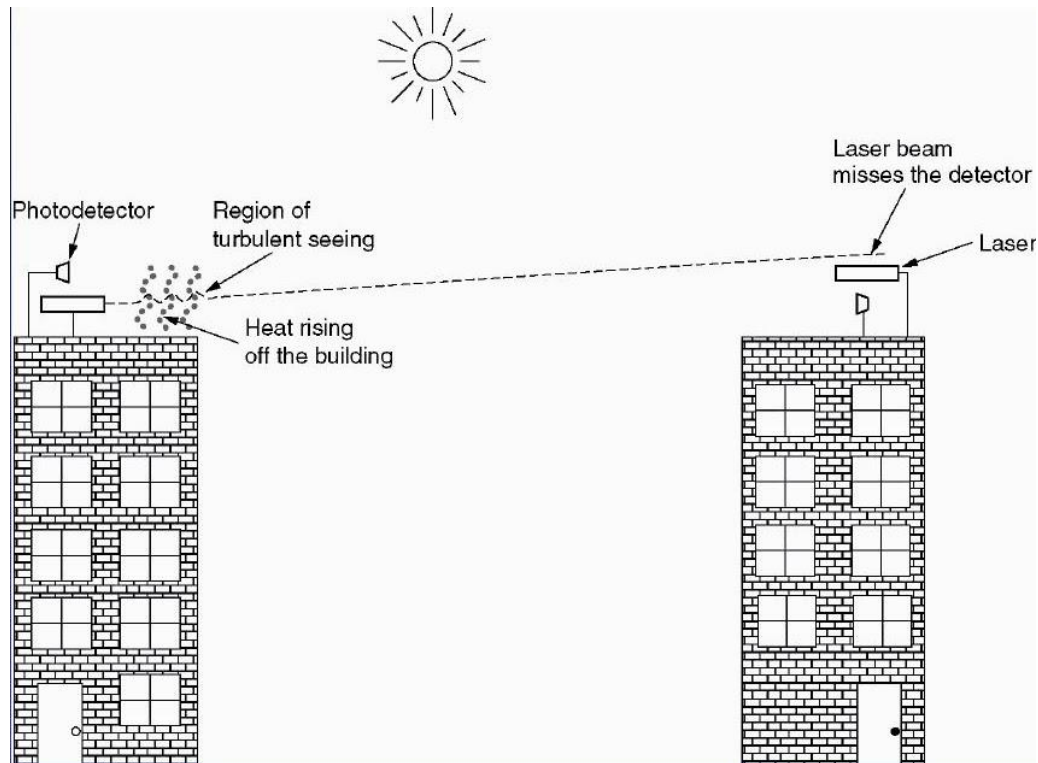


4. Lightwave transmission:

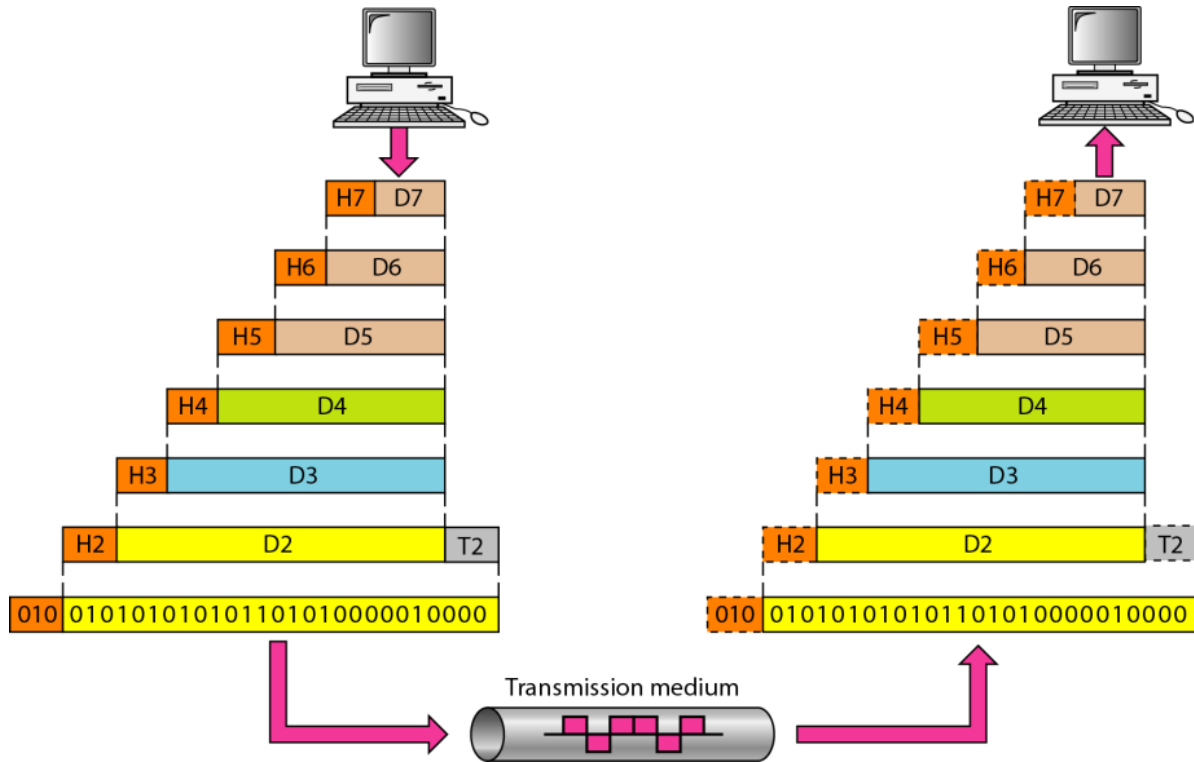
Unguided optical signaling has been in use for centuries, it offers

1. very high bandwidth.
2. very low cost.
3. It is also relatively easy to install.

A disadvantage is that laser beams cannot penetrate rain or thick fog, but they normally work well on sunny days. Heat from the sun during the daytime causes convection currents to rise up from the roof of the building, this turbulent air, diverts the beam and make it dance around the detector.



Network Standards and OSI Model



✚ Network Criteria معايير الشبكات

A network must be able to meet a certain number of criteria. The most important of these are **performance, reliability, and security**.

يجب أن تكون الشبكة قادرة على تلبية عدد معين من المعايير. أهمها الأداء والموثوقية والأمان.

a) Performance can be measured in many ways, including transit time and response time. Transit time is the **amount of time** required for a message to travel from one device to another. Response time is the **elapsed time** between an inquiry and a response.

يمكن قياس الأداء بطرق عديدة ، بما في ذلك وقت الإرسال ووقت الاستجابة.

وقت الإرسال هو مقدار الوقت المطلوب للإرسال من جهاز إلى آخر. وقت الاستجابة هو الوقت المنقضي بين الطلب والرد.

The performance of a network depends on a number of factors:

- 1) Number of users.
- 2) Type of transmission medium.
- 3) Capabilities of the connected hardware.
- 4) Efficiency of the software.

Performance is often evaluated by two networking metrics: **throughput and delay**. We often need more throughput and less delay.

غالبًا ما يتم تقييم الأداء من خلال مقياسين للشبكة: الإنتاجية والتأخير. غالبًا ما نحتاج إلى إنتاجية أكبر وتأخير أقل.

b) Reliability **الموثوقية** network reliability is measured by the:

- 1) Accuracy of delivery.
- 2) Frequency of failure.
- 3) The time it takes a link to recover from a failure.
- 4) Network's robustness in a catastrophe.

c) Security **الامنية** Network security issues include:

- 1) Protecting data from unauthorized access
- 2) Protecting data from damage and change.
- 3) Implementing policies for recovery from data losses.

Protocols and Standards

A) Protocol

A protocol defines **what** is communicated, **how** it is communicated, and **when** it is communicated. The key elements of a protocol are **syntax, semantics, and timing**.

يحدد البروتوكول ما يتم توصيله ، وكيفية توصيله ، ومتى يتم توصيله. العناصر الرئيسية للبروتوكول هي بناء الجملة قواعدياً ، والمعنى ، والتوقيت.

Syntax It refers to the structure or format of the data, meaning the order in which they are presented.

For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

Semantics It refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation?

For example, does an address identify the route to be taken or the final destination of the message?

Timing It refers to two characteristics: when data should be sent and how fast they can be sent.

For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

B) Standards

Standards are essential in creating an open and competitive market for equipment manufacturers and in guaranteeing national and international telecommunications.

المعايير أو المقاييس ضرورية في إنشاء سوق مفتوحة وتنافسية لمصنعي المعدات ولضمان الاتصالات الوطنية والدولية.

Standards Creation Committees لجان وضع المعايير

Most data telecommunications rely primarily on the standards published by the following committees:

- International Organization for Standardization (ISO).
- American National Standards Institute (ANSI).
- Institute of Electrical and Electronics Engineers (IEEE).
- Electronic Industries Association (EIA).

Network Models

The layered model that dominated data communications and networking literature before 1990 was the Open Systems Interconnection (OSI) model. Everyone believed that the OSI model would become the ultimate standard for data communications, but this did not happen. The TCP/IP protocol suite became the dominant commercial architecture because it was used and tested extensively in the Internet; the OSI model was never fully implemented.

كان النموذج الطبقي الذي سيطر على اتصالات البيانات ووثائق الشبكات قبل عام 1990 هو نموذج ربط الأنظمة المفتوحة (OSI). اعتقد الجميع أن نموذج OSI سيصبح المعيار النهائي لاتصالات البيانات ، ولكن هذا لم يحدث. أصبحت مجموعة بروتوكولات TCP / IP هي البنية التجارية السائدة لأنه تم استخدامها واختبارها على نطاق واسع في الإنترنت ؛ لم يتم تنفيذ نموذج OSI بالكامل.

The Open Systems Interconnection (OSI) model is introduced in the late 1970s by the International Standards Organization (ISO).

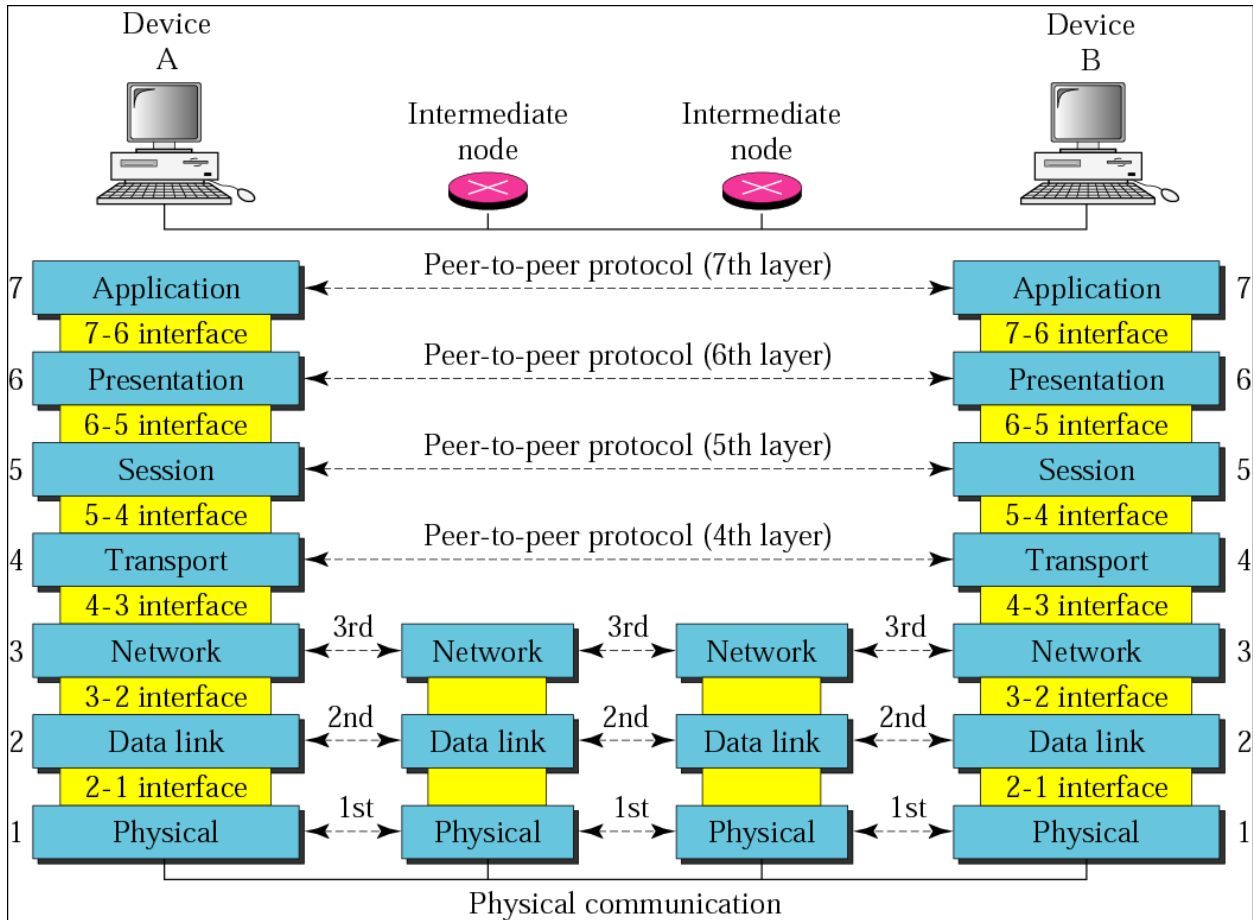
(Note: ISO is the organization. OSI is the model.)

The OSI model is a layered model for the design and understands of network systems that allows communication between all types of computer systems.

إن نموذج OSI هو نموذج متعدد الطبقات لتصميم وفهم أنظمة الشبكة التي تسمح بالاتصال بين جميع أنواع أنظمة الكمبيوتر.

OSI consists of seven separate but related layers, each of which defines a part of the process of moving information across a network (see Figure 2.1). When a message is sent for example from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes, called routers. These intermediate nodes usually involve only the first three layers of the OSI model.

يتكون OSI من سبع طبقات منفصلة ولكنها ذات صلة ، تحدد كل منها جزءاً من عملية نقل المعلومات عبر الشبكة (انظر الشكل 2.1). عندما يتم إرسال رسالة على سبيل المثال من الجهاز A إلى الجهاز B. أثناء انتقال الرسالة من A إلى B ، فقد تمر عبر العديد من العقد الوسيطة ، تسمى الموجهات. عادةً ما تتضمن هذه العقد الوسيطة الطبقات الثلاث الأولى فقط من نموذج OSI.



The interaction between layers in the OSI model

Each layer defines a family of functions distinct from those of the other layers. Each layer at the sending site uses the services of the layer immediately below it. The sender at the higher layer uses the services of the middle layer. The middle layer uses the services of the lower layer. The lower layer uses the services of the carrier. Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4.

تحدد كل طبقة مجموعة من الوظائف تختلف عن تلك الخاصة بالطبقات الأخرى. تستخدم كل طبقة في موقع الإرسال خدمات الطبقة التي تحتها مباشرة. يستخدم المرسل في الطبقة العليا خدمات الطبقة الوسطى. تستخدم الطبقة الوسطى خدمات الطبقة السفلية. تستخدم الطبقة السفلية خدمات الناقل. فالطبقة 3 ، على سبيل المثال ، تستخدم الخدمات التي توفرها الطبقة 2 وتوفر الخدمات للطبقة 4.

The processes on each machine that communicate at a given layer are called peer-to-peer processes. Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.

تسمى العمليات الموجودة على كل جهاز والتي تتواصل في طبقة معينة بعمليات نظير إلى نظير. وبالتالي ، يعد الاتصال بين الأجهزة عملية نظير إلى نظير باستخدام البروتوكولات المناسبة لطبقة معينة.

The interfaces between layers are to define the information and services that each layer must provide for the layer above it.

يجب أن تحدد الواجهات بين الطبقات المعلومات والخدمات التي يجب أن توفرها كل طبقة للطبقة الموجودة فوقها.

The seven layers are belonging to three subgroups. Layers 1, 2, and 3 are the network support layers; they deal with the physical aspects of moving data from one device to another (such as electrical specifications, physical connections, and physical addressing). Layers 5, 6, and 7 are the user support layers; they allow interoperability among unrelated software systems. Layer 4, the transport layer, links the two subgroups.

الطبقات السبع تنتمي إلى ثلاث مجموعات فرعية. الطبقات 1 و 2 و 3 هي طبقات دعم الشبكة ؛ تتعامل مع الجوانب المادية لنقل البيانات من جهاز إلى آخر (مثل المواصفات الكهربائية ، والتوصيلات المادية ، والعنونة المادية). الطبقات 5 و 6 و 7 هي طبقات دعم المستخدم ؛ أنها تسمح بالتشغيل البيئي بين أنظمة البرامج غير ذات الصلة. الطبقة 4 ، طبقة النقل ، تربط المجموعتين الفرعيتين.

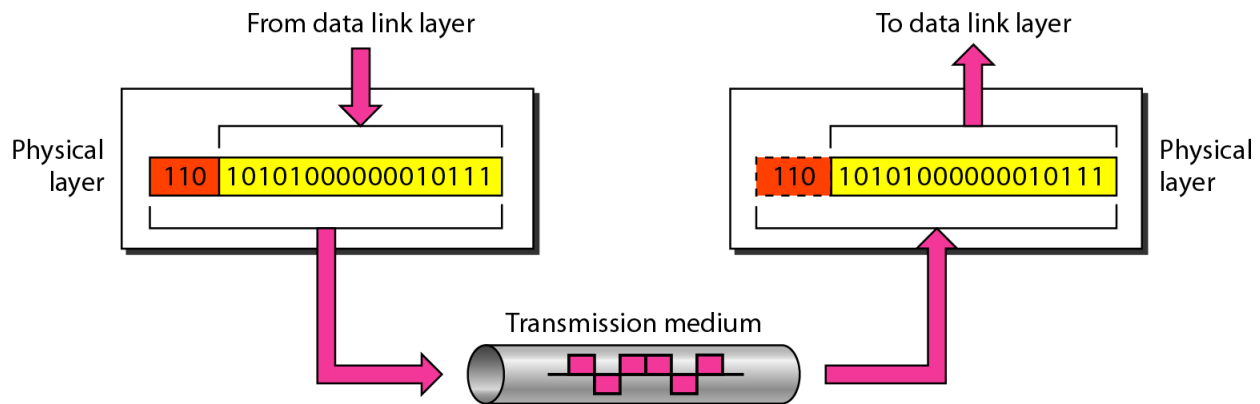
Layers in the OSI Model

In the following we describe the functions of each layer in the OSI model.

1. Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physical medium.

تنسق الطبقة المادية (الفيزيائية) الوظائف المطلوبة لحمل سبيل من ال Bits على وسط مادي.



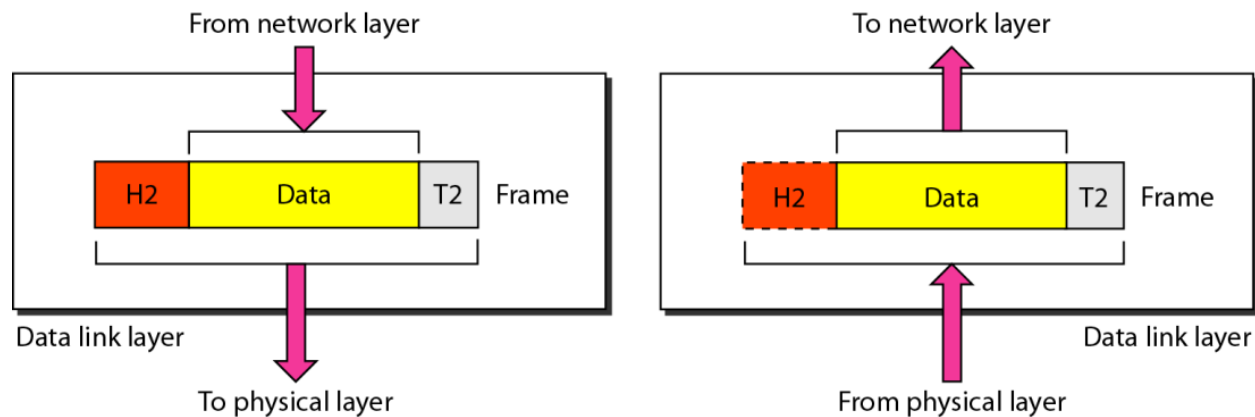
The physical layer is concerned with the following:

- Physical characteristics of interfaces and medium.
- Representation of bits (sequence of 0s or 1s) with defining the type of encoding (how 0s and 1s are changed to signals).
- Data rate or the transmission rate (the number of bits sent each second)
- Synchronization of bits. The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level.
- Line configuration (point-to-point or multipoint configuration).
- Physical topology (mesh, star, bus, etc.).
- Transmission mode (simplex, half-duplex, or full-duplex).

2. Data Link Layer

The data link layer makes the physical layer appear error-free to the upper layer (network layer). The figure shows the relationship of the data link layer to the network and physical layers.

تجعل طبقة ارتباط البيانات الطبقة المادية (الفيزيائية) خالية من الأخطاء للطبقة العليا (طبقة الشبكة). يوضح الشكل علاقة طبقة ارتباط البيانات بالشبكة والطبقات المادية.



The data link layer is responsible for moving frames from one hop (node) to the next. Other responsibilities of the data link layer include the following:

- Framing. The data link layer divides the stream of bits received from the network layer into manageable data units called **frames**.
- Physical addressing. The data link layer adds a header to the frame to define the sender and/or receiver devices of the frame. The devices are defined by the physical address (or MAC address).
- Flow control. The data link layer ensures the rate at which data are produced in the sender and arrived in the receiver.
- Error control. The data link layer adds mechanisms to detect and retransmit damaged or lost frames. Error control is normally achieved through a **trailer** added to the end of the frame (see the **T2** in Figure).
- Access control. The data link layer controls the access to the link when two or more devices are connected to the same link.

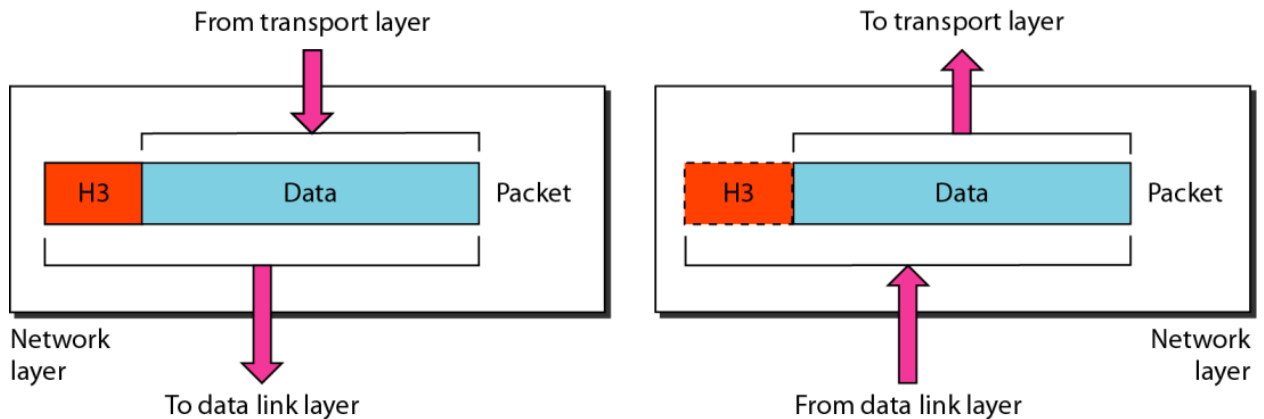
3. Network Layer

The network layer is responsible for the source-to-destination delivery of a packet (see Figure), possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links).

طبقة الشبكة مسؤولة عن تسليم الحزمة من المصدر إلى الوجهة (انظر الشكل) ، ربما عبر عدة شبكات متعددة. بينما تشرف طبقة وصلة البيانات (data link layer) على تسليم الحزمة بين نظامين على نفس الشبكة (الروابط).

Other responsibilities of the network layer include the following:

- Logical addressing. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses (IP address) of the sender and receiver.
- Routing. When independent networks or links are connected to create internetworks, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.



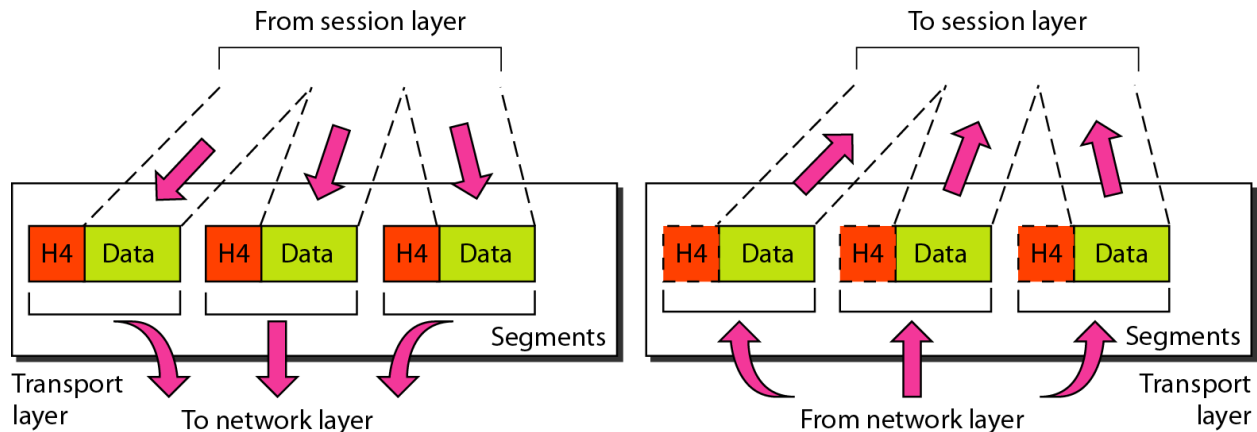
4. Transport Layer

The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets.

طبقة النقل مسؤولة عن تسليم الرسالة بأكملها من عملية إلى عملية. العملية عبارة عن برنامج تطبيق يعمل على مضيف. بينما تشرف طبقة الشبكة على تسليم الحزم الفردية من المصدر إلى الوجهة.

Other responsibilities of the transport layer include the following:

- Service-point addressing. Computers often run several programs at the same time. The transport layer header includes a type of address called a service-point address (or port address) in order to deliver the entire message to the correct process on that computer.
- Segmentation and reassembly. A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly at the destination.
- Flow control. Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.
- Error control. Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to-process rather than across a single link.



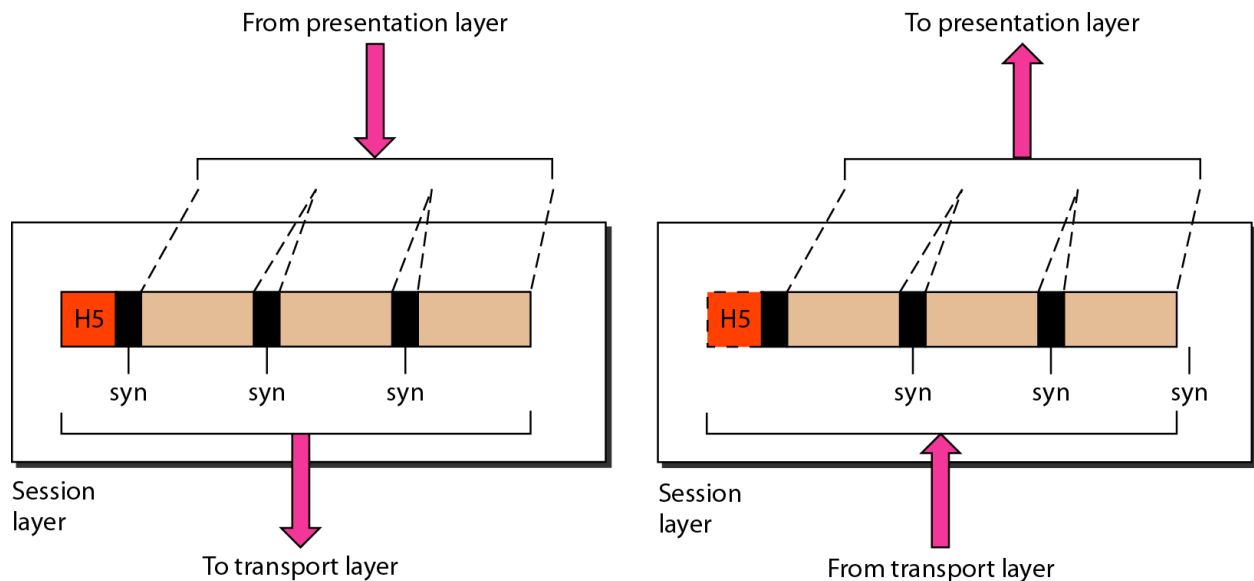
5. Session Layer

The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is responsible for dialog control and synchronization.

الخدمات التي تقدمها الطبقات الثلاث الأولى (المادية ، وصلة البيانات ، والشبكة) ليست كافية لبعض العمليات. طبقة الجلسة مسؤولة عن التحكم في الحوار والمزامنة.

Specific responsibilities of the session layer include the following:

- Dialog control. The session layer allows the communication between two processes to take place in either half-duplex (one way at a time) or full-duplex (two ways at a time) mode.
- Synchronization. The session layer allows a process to add checkpoints, or synchronization points, to a stream of data (see Figure). For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages.



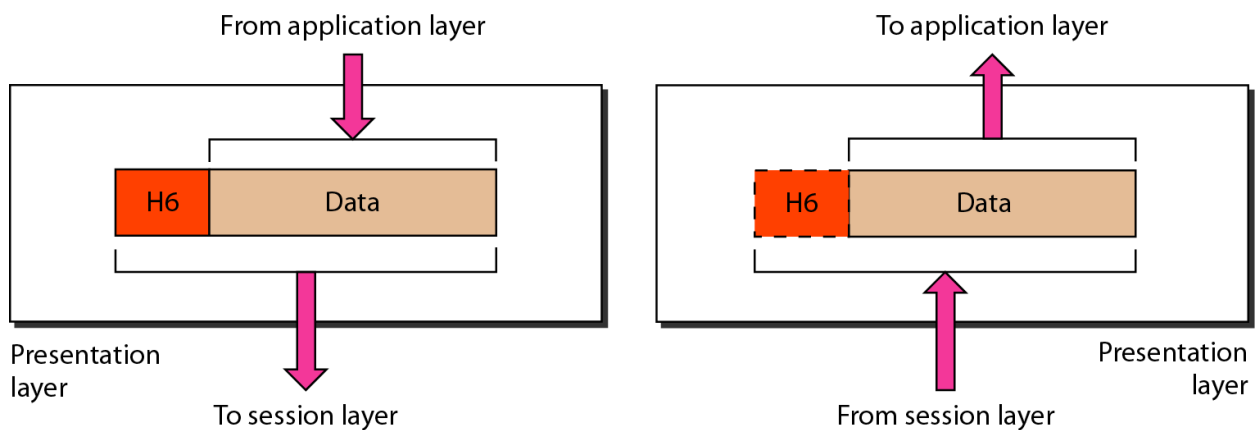
6. Presentation Layer

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

تهتم طبقة العرض التقديمي بالقواعد ودلالات المعنى للمعلومات المتبادلة بين نظامين.

Specific responsibilities of the presentation layer include the following:

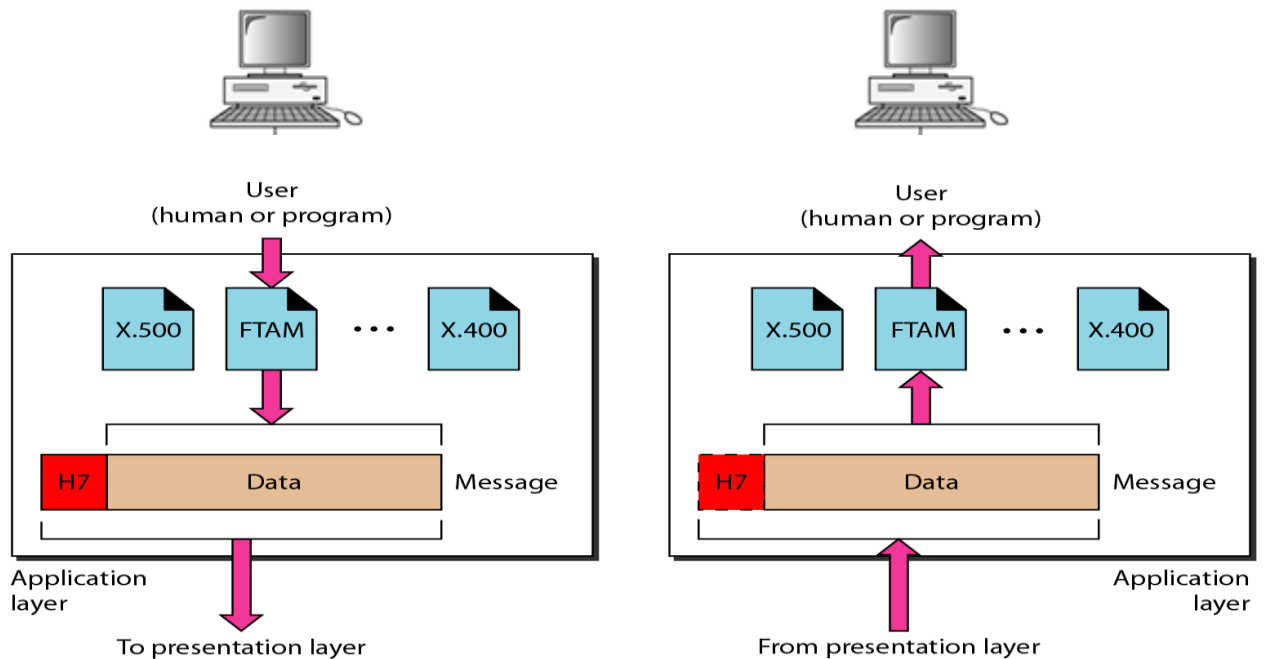
- Translation. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods.
- Encryption. To carry sensitive information, a system must be able to ensure privacy.
- Compression. Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the data transmission.

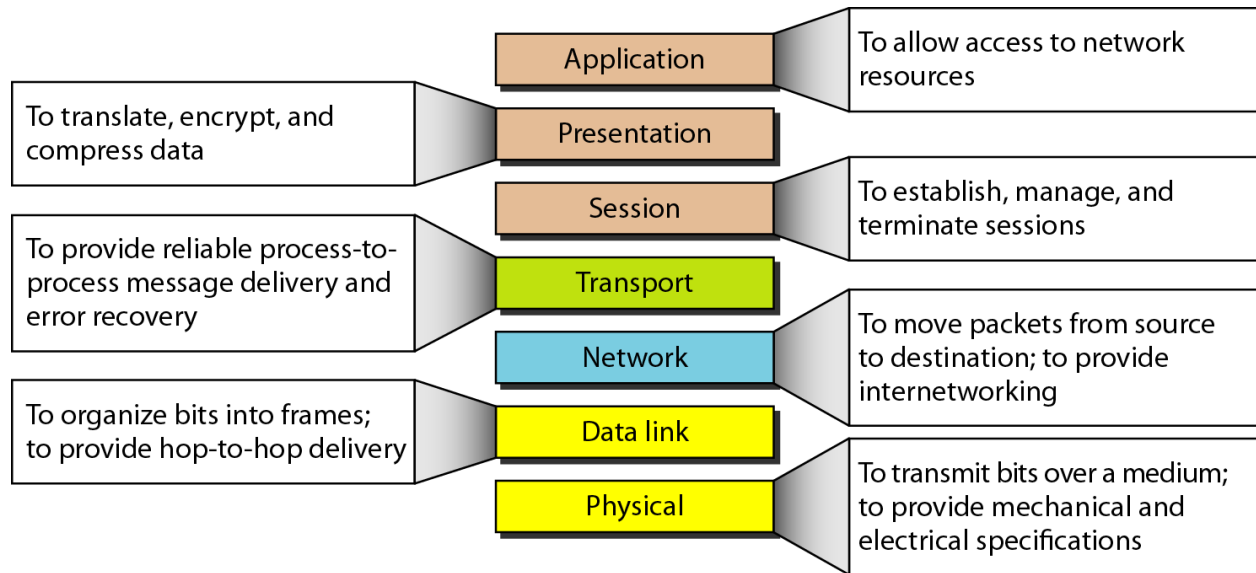


7. Application Layer

The application layer is responsible for providing services to the user. It enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, and other types of distributed information services.

طبقة التطبيق مسؤولة عن تقديم الخدمات للمستخدم. إنها تمكن المستخدم ، سواء كان الإنسان أو البرمجيات ، من الوصول إلى الشبكة. يوفر (واجهات المستخدم) و(الدعم) لخدمات مثل البريد الإلكتروني ، والوصول إلى الملفات عن بعد ونقلها ، وأنواع أخرى من خدمات المعلومات الموزعة.





Summary of OSI layers