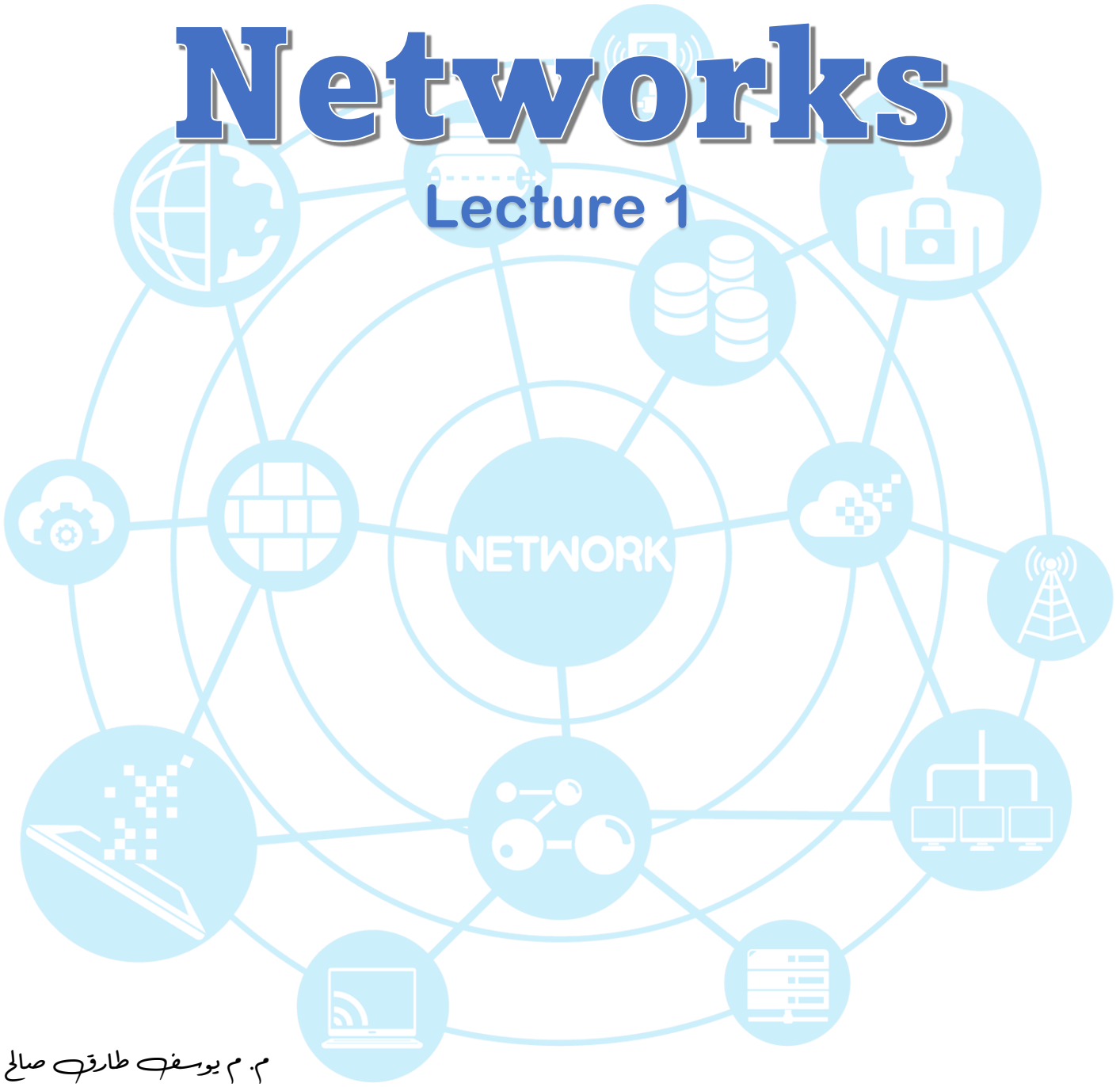
Introduction to Computer Networks

Lecture 1



م.م يوسف طارق صالح

Network Topologies

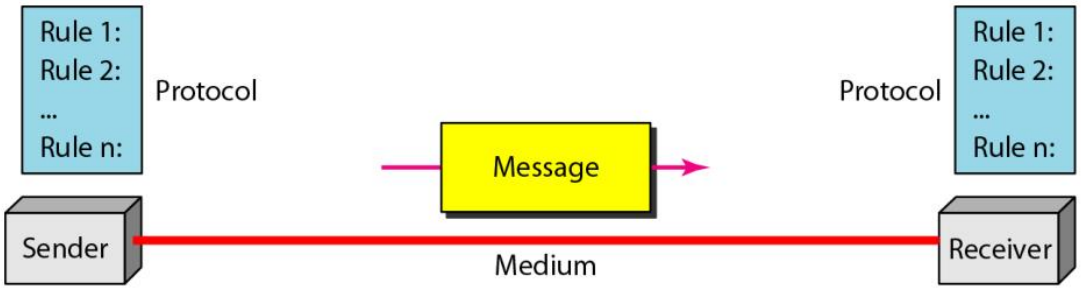
Introduction:

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

A network is a group of connected communicating devices such as computers and printers. An internet (note the lowercase letter i) is two or more networks that can communicate with each other. The most notable internet is called the Internet (uppercase letter I), a collaboration of more than hundreds of thousands of interconnected networks. Private individuals as well as various organizations such as government agencies, schools, research facilities, corporations, and libraries in more than 100 countries use the Internet. Millions of people are users. Yet this extraordinary communication system only came into being in 1969. In the mid-1960s, mainframe computers in research organizations were standalone devices. Computers from different manufacturers were unable to communicate with one another. The Advanced Research Projects Agency (ARPA) in the Department of Defense (DoD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort. In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an interface message processor (IMP). The IMPs, would be connected to one another. Each IMP had to be able to communicate with other IMPs as well as with its own attached host. By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network. Software called the Network Control Protocol (NCP) provided communication between the hosts. In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the Internet ting Projec1. Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end-to-end delivery of packets. This paper on Transmission Control Protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway. Shortly thereafter, authorities made a decision to split TCP into two protocols: Transmission Control Protocol (TCP) and Internetworking Protocol (IP). IP would handle datagram routing while TCP would be responsible for higher-level functions such as Segmentation, reassembly, and error detection. The internetworking protocol became known as TCPIIP.

Components:

A data communications system has five components.



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, just as a person speaking French cannot be understood by a person who speaks only Japanese

Distributed Processing:

Most networks use distributed processing, in which a task is divided among multiple computers. Instead of one single large machine being responsible for all aspects of a process, separate computers (usually a personal computer or workstation) handle a subset.

Network Criteria:

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

Performance: Performance can be measured in many ways, including transit time and response time.

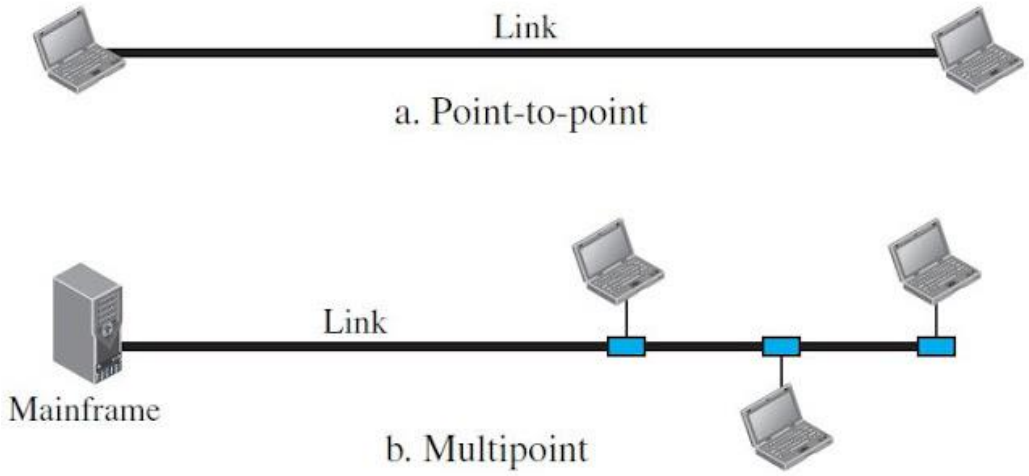
Reliability

Security:

Physical Structures:

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 visualization purposes, it is simplest to imagine any link as a line drawn between two points. 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.

a) Point-to-Point: connection provides a dedicated link between two devices.
b) Multipoint: (also called multi drop) connection is one in which more than two specific devices share a single link.



Uses of Computer Networks:

Had it not been of high importance, nobody would have bothered connecting computers over a network. Computer Networks with some traditional use cases at companies and for individuals and then move on to the recent developments in the area of mobile users and home networking.

1. **Business Applications**
   a) Resource Sharing:
   b) Server-Client model:
   c) Communication Medium
   d) E commerce
2. **Home Applications**
   a) Access to remote information
   b) Person-to-person communication
   c) Interactive entertainment.
   d) Electronic commerce.

Types / Categories of Networks:

Local Area Networks:

Local area networks, generally called LANs, are privately-owned networks within a single building or campus of up to a few kilometers in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information. LANs are distinguished from other kinds of networks by three characteristics: (1) Their size, Their transmission technology, and Their topology. LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance. want to transmit simultaneously. The arbitration mechanism may be centralized or distributed. IEEE 802.3, popularly called Ethernet, for example, is a bus-based broadcast network with decentralized control, usually operating at 10 Mbps to 10 Gbps. Computers on an Ethernet can transmit whenever they want to; if two or more packets collide, each computer just waits a Random time and tries again later.

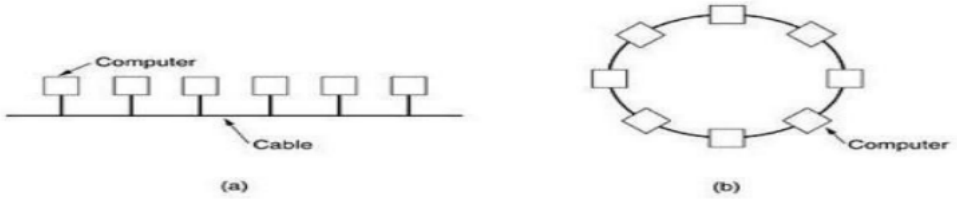


Fig.1: Two broadcast networks . (a) Bus. (b) Ring.

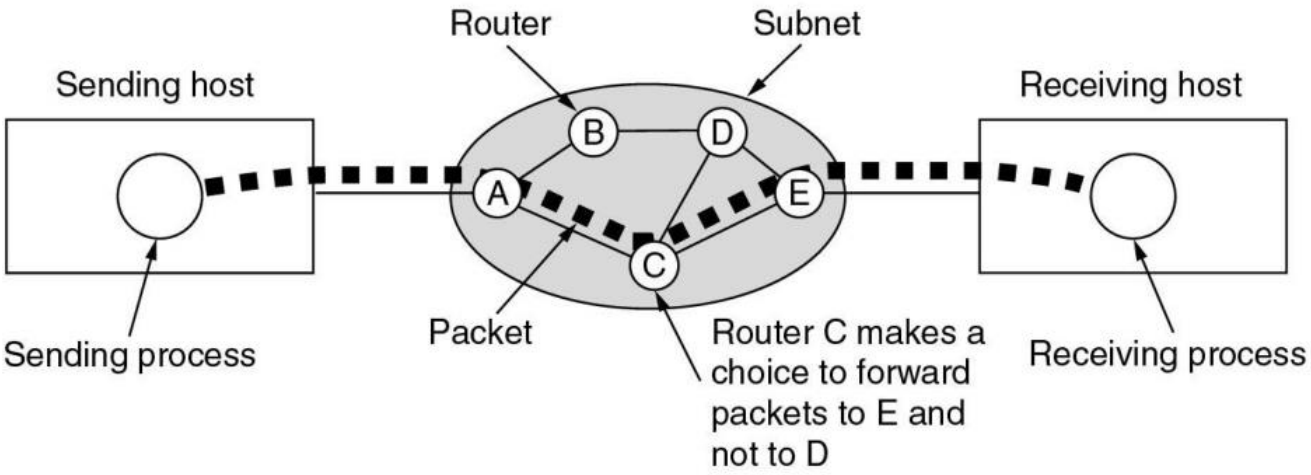
A second type of broadcast system is the ring. In a ring, each bit propagates around on its own, not waiting for the rest of the packet to which it belongs. Typically, each bit circumnavigates the entire ring in the time it takes to transmit a few bits, often before the complete packet has even been transmitted. As with all other broadcast systems, some rule is needed for arbitrating simultaneous accesses to the ring. Various methods, such as having the machines take turns, are in use. IEEE 802.5 (the IBM token ring), is a ring-based LAN operating at 4 and 16 Mbps. FDDI is another example of a ring network.

Metropolitan Area Network (MAN):

A metropolitan area network, or MAN, covers a city. The best-known example of a MAN is the cable television network available in many cities. A MAN is implemented by a standard called DQDB (Distributed Queue Dual Bus) or IEEE 802.16. DQDB has two unidirectional buses (or cables) to which all the computers are attached.

Wide Area Network (WAN):

A wide area network, or WAN, spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user (i.e., application) programs. These machines are called as hosts.. . Of course, if ACE is the best route, all packets may be sent along it, even if each packet is individually routed.



A stream of packets from sender to receiver.

Intranet:

Internet:

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. Count the ways you've used the Internet recently. Perhaps you've sent electronic mail (e-mail) to a business associate, paid a utility bill, read a newspaper from a distant city, or looked up a local movie schedule-all by using the Internet. Or maybe you researched a medical topic, booked a hotel reservation, chatted with a fellow or comparison-shopped for a car. The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.

Internet Today:

The Internet has come a long way since the 1960s. The Internet today is not a simple hierarchical structure. It is made up of many wide- and local-area networks joined by connecting devices and switching stations. It is difficult to give an accurate representation of the Internet because it is continually changing-new networks are being added, existing networks are adding addresses, and networks of defunct companies are being removed. Today most end users who want Internet connection use the services of Internet Service Providers (ISP).

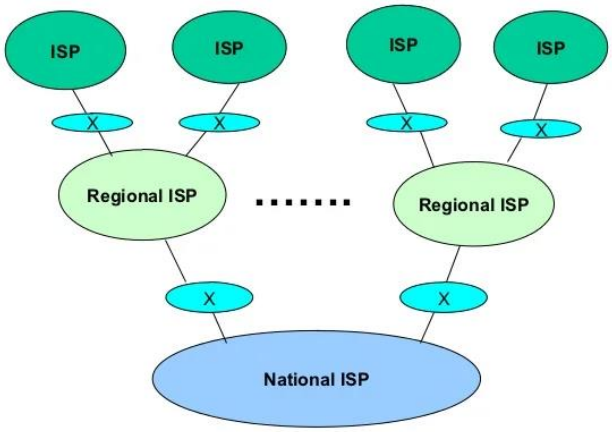


Fig 1.Structure of a national ISP

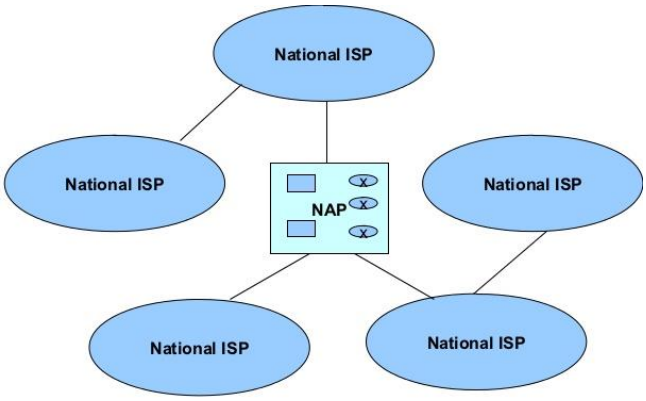


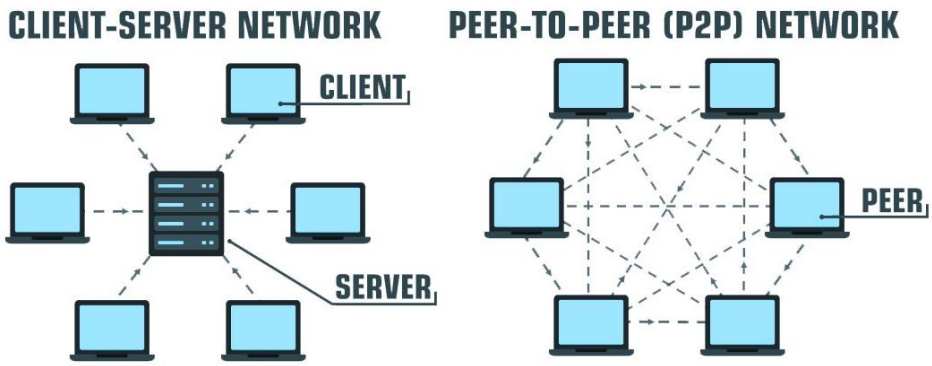
Fig.2.Interconnection of national ISPs

Architecture of Internet:

Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer

The two types of network architectures are used

- Peer-To-Peer network
- Client/Server network



Peer-To-Peer network:

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.

Advantages Of Peer-To-Peer Network:

1. It is less costly as it does not contain any dedicated server.
2. If one computer stops working but, other computers will not stop working.

Disadvantages Of Peer-To-Peer Network:

1. In the case of Peer-To-Peer network, it does not contain the centralized system. Therefore, it cannot back up the data as the data is different in different locations.
2. It has a security issue as the device is managed itself.

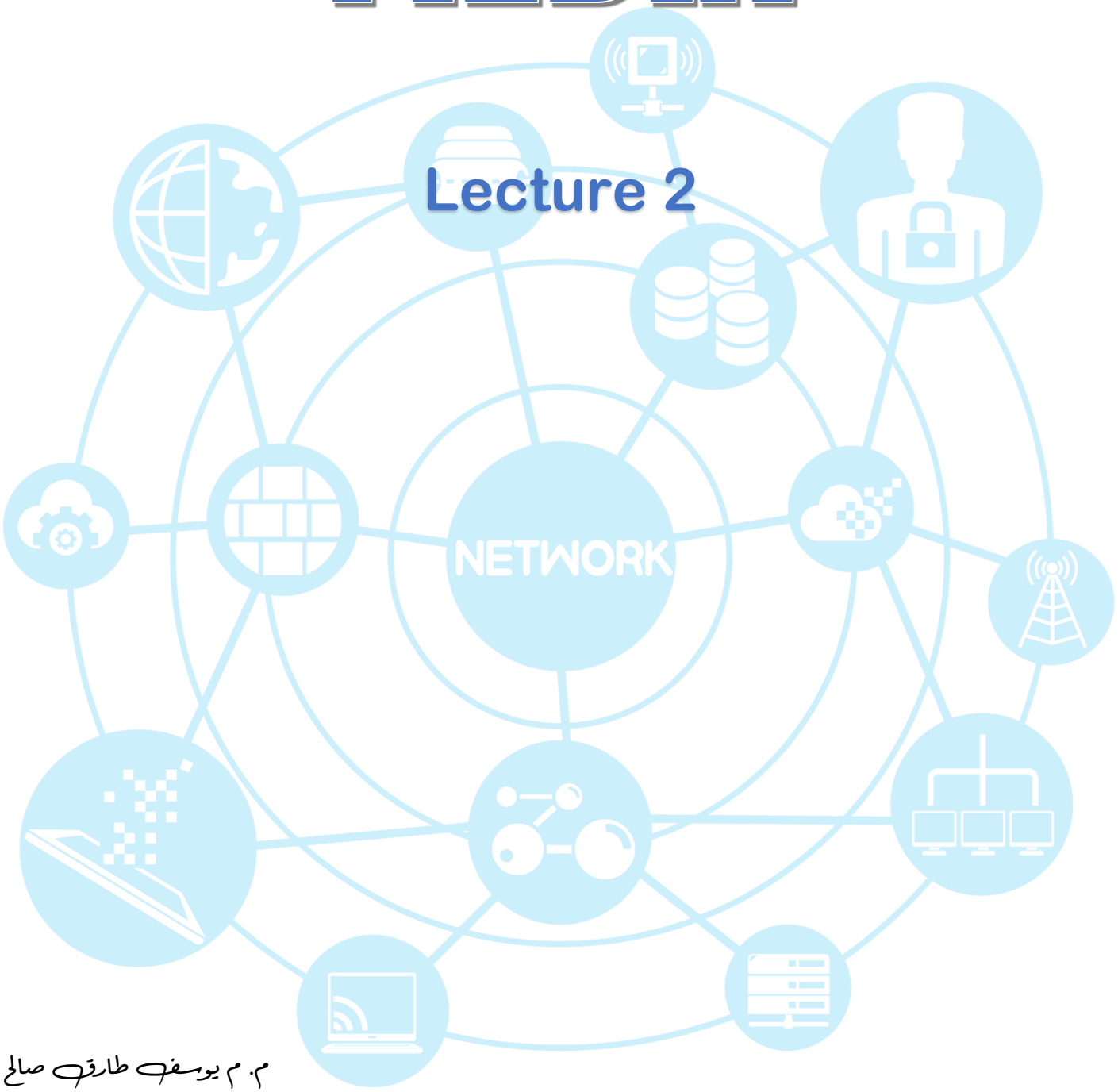
Client/Server Network:

Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.

The central controller is known as a ***server*** while all other computers in the network are called ***clients.***

TRANSMISSION MEDIA

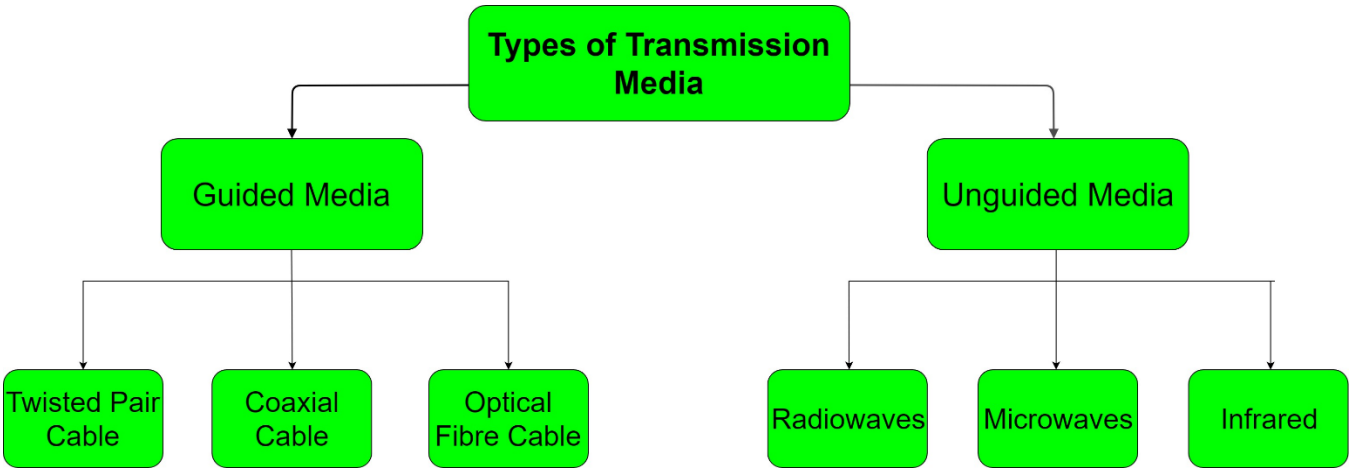
Lecture 2



م.م يوسف طارق صالح

TRANSMISSION MEDIA

A transmission medium can be broadly defined as anything that can carry information from a source to a destination. For example, the transmission medium for two people having a dinner conversation is the air. The air can also be used to convey the message in a smoke signal or semaphore. For a written message, the transmission medium might be a mail carrier, a truck, or an airplane. In data communications the definition of the information and the transmission medium is more specific. The transmission medium is usually free space, metallic cable or optical cable. The information is usually a signal that is the result of conversion of data from another form. Transmission Media is broadly classified into the following types:

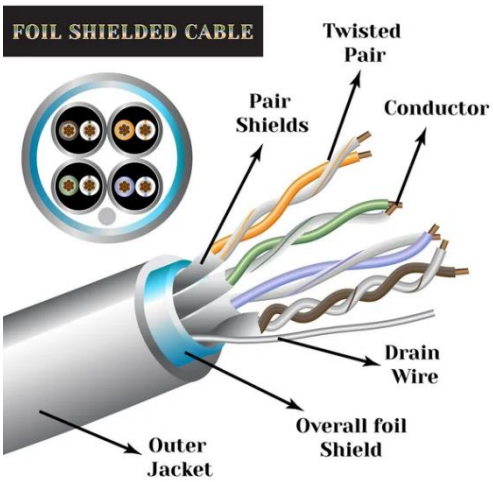


Guided Media:

Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable.

1. Twisted-Pair Cable

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together, as shown below figure.



One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals. If the two wires are parallel, the effect of these unwanted

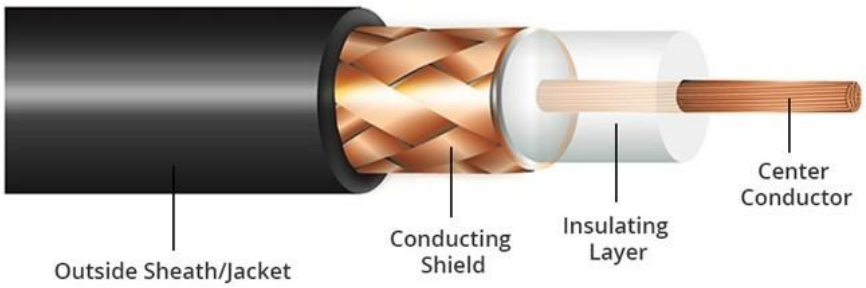
signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources (e,g., one is closer and the other is farther).

Applications

Twisted-pair cables are used in telephone lines to provide voice and data channels. The local loop-the line that connects subscribers to the central telephone office-commonly consists of Unshielded twisted pair cables. The DSL line that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twistedpair cables. Local-area networks, such as 10Base-T and 100Base-T, also use twisted-pair cables.

2. Coaxial Cable

Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover (below figure).

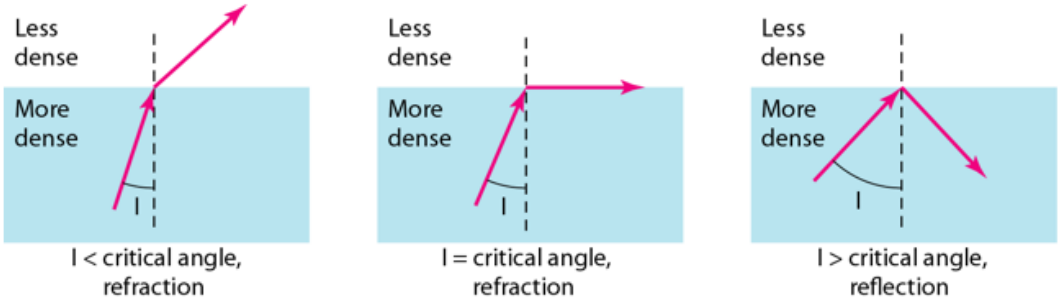


Applications

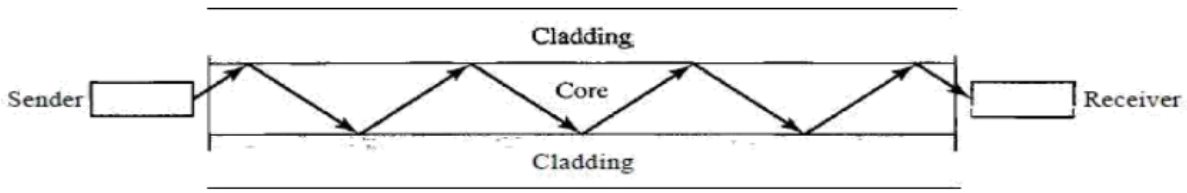
Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10,000 voice signals. Later it was used in digital telephone networks where a single coaxial cable could carry digital data up to 600 Mbps. However, coaxial cable in telephone networks has largely been replaced today with fiber-optic cable. Cable TV networks also usecoaxial cables. In the traditional cable TV network, the entire network used coaxial cable.

3. Fiber Optic Cable:

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. To understand optical fiber, we first need to explore several aspects of the nature of light. Light travels in a straight line as long as it is moving through a single uniform If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes direction. The figure below shows how a ray of light changes direction when going from a denser to a less dense substance.

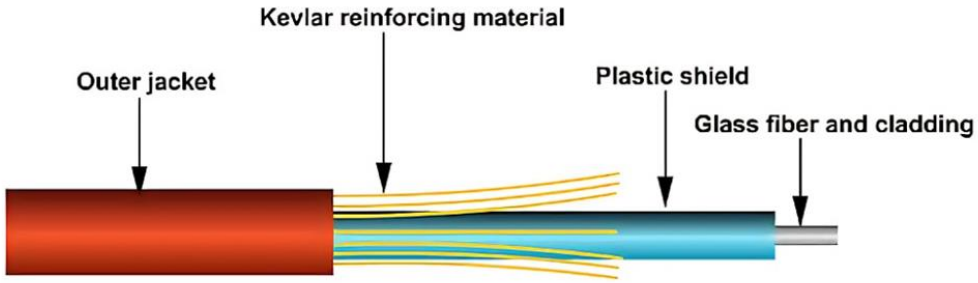


As the figure shows, if the angle of incidence I (the angle the ray makes with the line perpendicular to the interface between the two substances) is less than the critical angle, the ray refracts and moves closer to the surface. If the angle of incidence is equal to the critical angle, the light bends along the interface. If the angle is greater than the critical angle, the ray reflects (makes a turn) and travels again in the denser substance. Note that the critical angle is a property of the substance, and its value differs from one substance to another



Cable Composition:

The figure below shows the composition of a typical fiber-optic cable. The outer jacket is made of either PVC or Teflon. Inside the jacket are Kevlar strands to strengthen the cable. Kevlar is a strong material used in the fabrication of bulletproof vests. Below the Kevlar is another plastic coating to cushion the fiber. The fiber is at the center of the cable, and it consists of cladding and core



Applications

Fiber-optic cable is often found in backbone networks because its wide bandwidth is costeffective. Today, with wavelength-division multiplexing (WDM), we can transfer data at a rate

of 1600 Gbps. The SONET network provides such a backbone. Some cable TV companies use a

combination of optical fiber and coaxial cable, thus creating a hybrid network. Optical fiber

provides the backbone structure while coaxial cable provides the connection to the user premises.

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

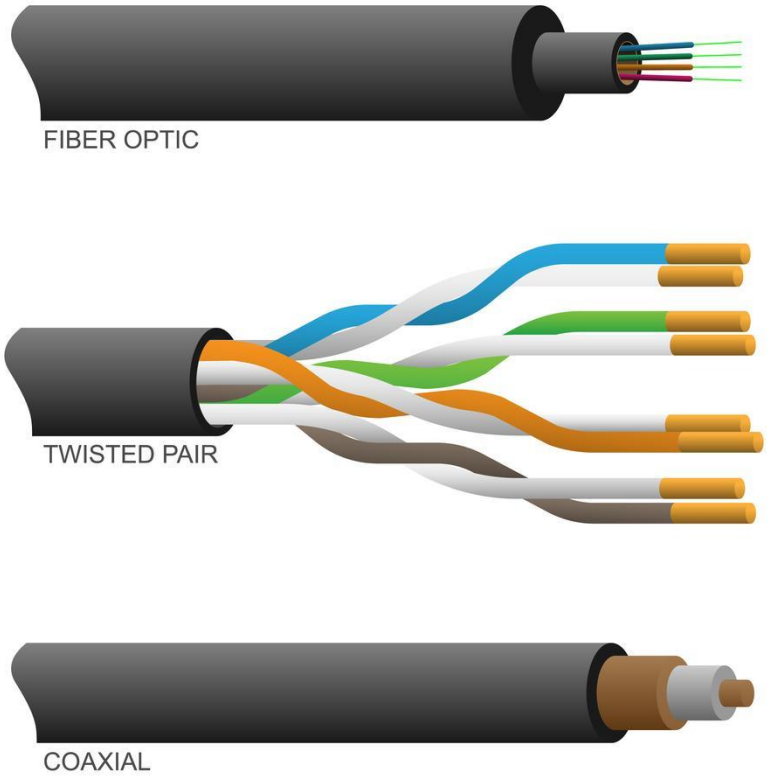
bandwidth utilization over fiber-optic cable is limited not by the medium but by the

signal generation and reception technology available.

✓ **Disadvantages**

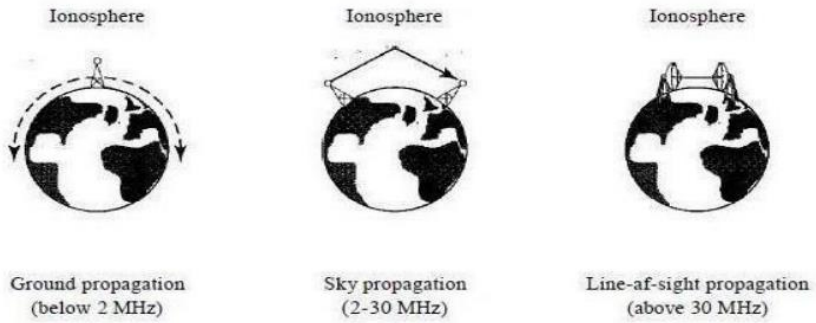
1. Installation and maintenance. Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.

2. Unidirectional light propagation. Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.



UNGUIDED MEDIA: WIRELESS

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



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 7.18. 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 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, and either tall enough or close enough together not to be affected by the curvature of the earth. Line-of-sight propagation is tricky because radio transmissions cannot be completely focused.

1. Radio Waves

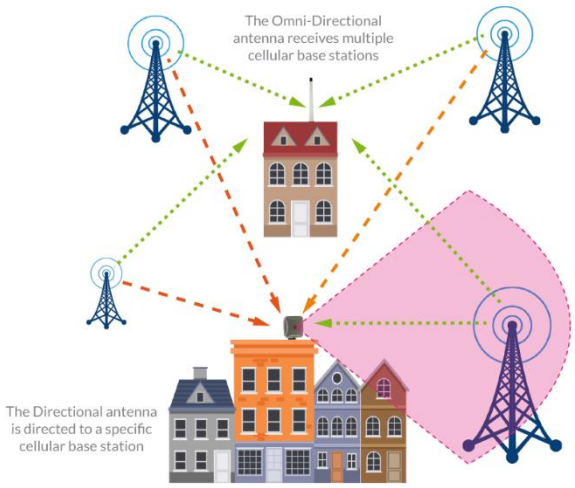
Waves ranging in frequencies between 3 kHz and 1 GHz are called radio waves. Radio waves, for the most part, are omni directional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna sends waves that can be received by any receiving antenna.

Omni directional Antenna

Radio waves use omni directional 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. Below figure 7.20 shows an omni directional antenna.

Applications

The omni directional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting.



2. Microwaves

Electromagnetic waves having frequencies between I 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

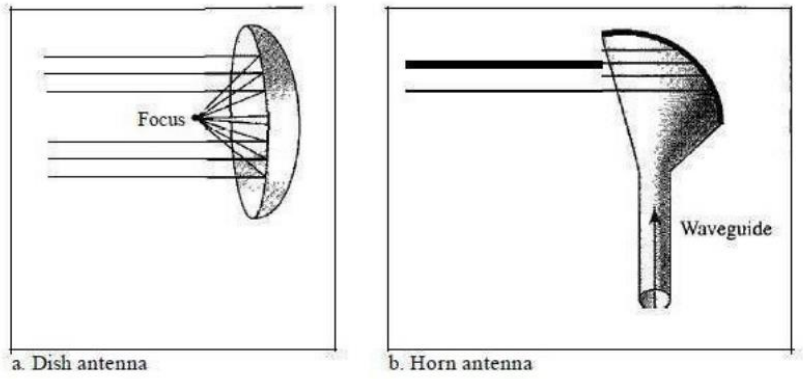
microwave propagation:

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 do 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.

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 below figure). A parabolic dish antenna is based on the geometry of a parabola: Every line parallel to the line of symmetry (line of sight) reflects off the curve at angles such that all the lines intersect in a common point called the focus.



a. Dish antenna b. Horn antenna

3. Infrared

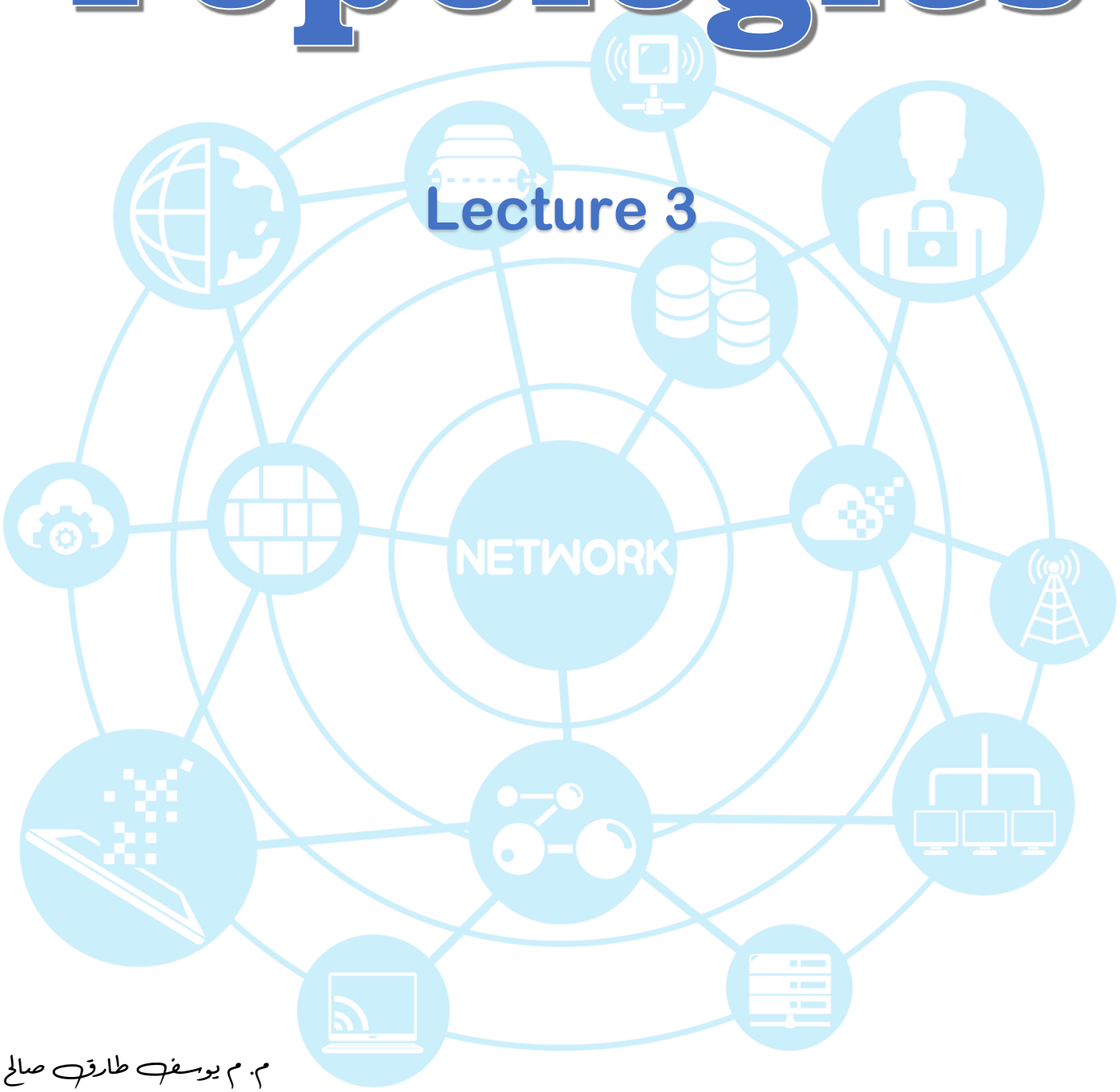
Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another; a short-range 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 communication.

Applications

The infrared band, almost 400 THz, has 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 sponsoring the 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.

Network Topologies

Lecture 3



م.م يوسف طارق صالح

Network Topologies

Introduction:

A computer network defined as a group of computers or any other network devices (network nodes) such as phones, servers, or peripheral devices that are connected to each other to achieve transferring data, exchanging information, and sharing the network resources.

Network topology is the way in which various components of that network are connected and arranged. Network topologies define the layout, virtual shape, or structure of the network, not only physically but also logically. The physical way the computer network is wired may not actually be the way the computer network works logically so; it is good to know about network topologies because different types of networking standards may use one type of physical topology but use an entirely different logical topology.

There are two types of topologies, the physical topology and the logical topology. Physical topology is concerned with the physical layout of the devices on the network and how they are physically connected while Logical topology deals with how data is transferred and flows on the network, apart from physical design.

Topology Types:

Topology refers to the way in which the component of the network is connected. Each topology is suited to specific tasks and has its own advantages and disadvantages.

1. Bus Topology:

Bus topology uses a common backbone to connect all devices, a single cable. The backbone functions as a shared communication medium that devices attach or tap into with an interface connector, figure (1).

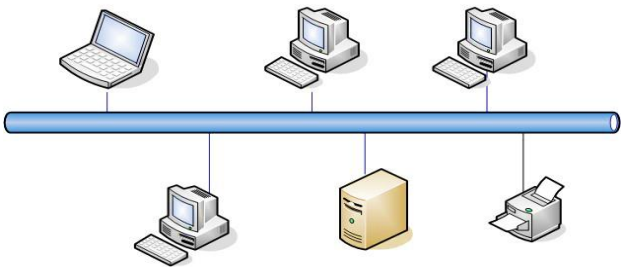


Figure 1: Bus Topology

Also, there is a terminator at each end of the cable, which absorbs any signal, preventing reflection of the signal from the endpoints. Where the terminator is not present, the endpoint acts as a mirror and reflects the signal causing interference and other problems.

A device that wants to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient accepts and processes the message. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network.

Advantages

- Simplicity in setup and expansion, due to it uses a single communication line.
- Less costly because less cabling is needed.

Disadvantages

- A single communication line for data transmission makes it easier for a collision to occur.

- The whole network breaks down when the single network cable has a problem or disconnection.
- The difficulty of identification of the problem when occurs.
- Poor efficiency because all devices receive all signals from every other host.

2. Star Topology:

Star topology uses a central connecting device. All other devices on the network are connecting to that central device with network cables. Each device sends the information to the central connecting device which replicates the information and forwards it to the appropriate host, figure (2).

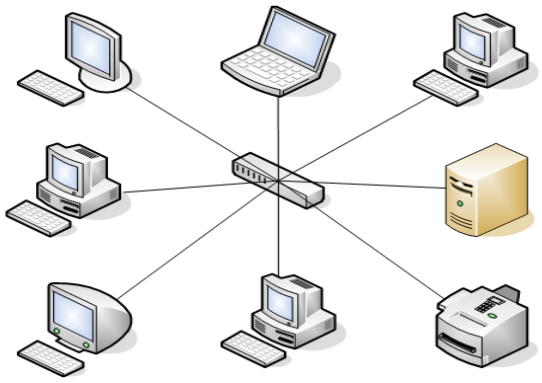


Figure 2: Star Topology

In general, there are two approaches that the central device to work. The first approach is for the central device to operate in a broadcast fashion where the transmission of a frame from one device to the central device is retransmitted on all the outgoing links. In this case, although the arrangement is physically a Star, it logically works as a Bus. In this case, the central device acts as a repeater where the transmission from any device is received by all other hosts, but only one host at a time successfully transmits. In the second approach, the central device acts as a switch and performs the switching or routing function where the incoming frame is buffered in the central device and then retransmitted on an outgoing link to the destination device.

Advantages:

- Easy to install and implement.
- Easy to troubleshoot and detect problems in the network.
- If one device fails, it does not affect the other devices in the network.
- Easily add or remove any devices without affecting the rest of the network.
- Centralized management and monitoring through the central device.

Disadvantages:

- If the central device is down, there will be a break down all the network which means a single point of failure.
- More cabling is needed since each individual device is connecting to the central device.
- Performance of the whole network depends on the performance of the central device.

3. Ring Topology:

Ring topology is set up in a circular fashion in which data travels around the ring in one direction and each device on the ring acts as a repeater to keep the signal strong as it travels, figure (3). When a device sends data, it must travel through each device on the ring until it reaches its destination. When the data frame circulates across all the devices, the destination device recognizes its address and copies the frame into a local buffer as it goes by. The frame continues to circulate until it returns to the source host, where it is removed. Because multiple devices share the ring, a medium access control protocol is needed to determine at what time each device may insert frames. The source can know whether it must transmit a new frame and whether the previous frame has been received properly by the destination or not through the behavior of the destination which changes a particular bit (bits) in the frame and when the receiver discovers that changed frame it knows if the right destination has received the frame or not.

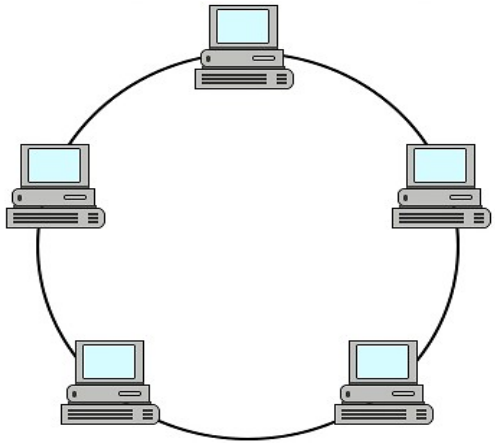


Figure 1: Ring Topology

Advantages:

- Fast network throughput.
- Less data collisions.
- High speed transfers

Disadvantage:

- Failure of a single device can break down the transmission of data on the network.
- Hard to manage.

4. Mesh Topology:

Mesh topology means that every device has a direct connection to every other device on the network, figure (4).

Mesh topology has two scenarios, called full mesh and partial mesh. In the full mesh topology, each device is connected directly to each of the others so that it does not need to use switching nor broadcasting. While in the partial mesh topology, some devices are connected to all the others, and some are connected only to those other nodes with which they exchange and share the data.

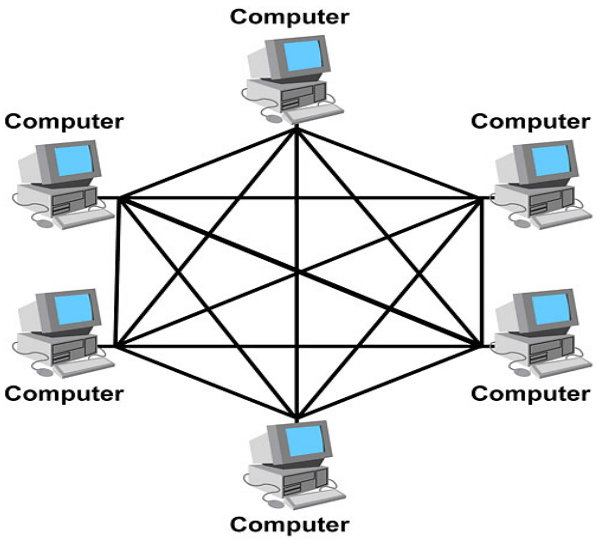


Figure 4: Mesh Topology

Advantages:

- If one device in the network fails, the rest of the devices can work normally without interruption.
- Adding more devices to the network does not affect the other devices.

Disadvantages:

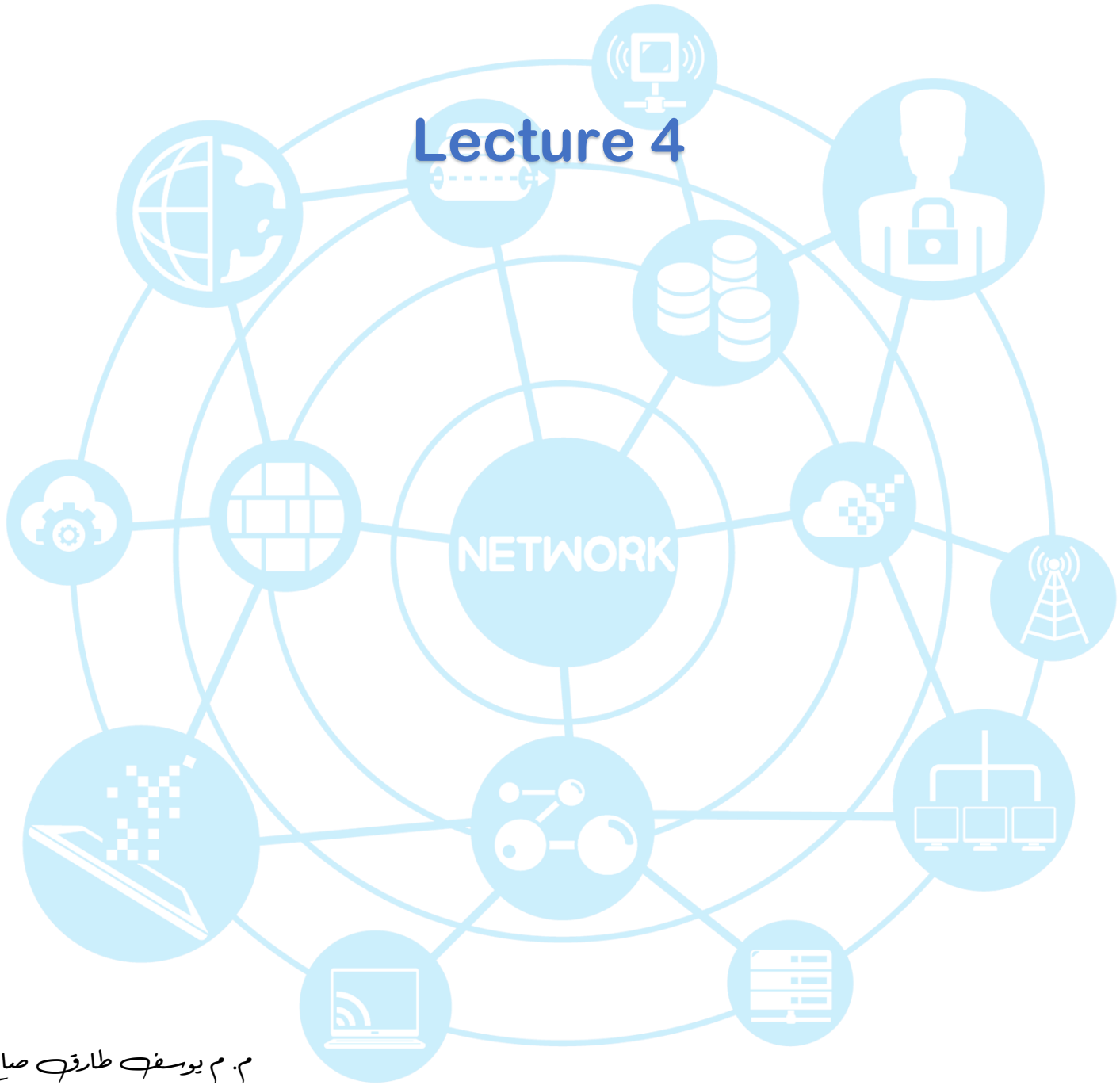
- High cost of implementation.
- Difficulty of implementation and maintenance.
- High cost due to the high density of needed cabling.
- Poor expandability.

Comparison Result:

Criteria	Bus	Star	Ring	Mesh
Installation	Easy	Easy	Difficult	Difficult
Cost	Inexpensive	Expensive	Moderate	Expensive
Reliability	Moderate	High	High	Very High
Privacy	Low	Moderate	Very Low	Very High
Robust	No	Yes	No	Yes
Flexibility	Yes	Yes	No	No
Expansion	Easy	Easy	Easy	Difficult
Troubleshooting And Maintainability	Difficult	Moderate	Difficult	Easy

OSI Model

Lecture 4



م.م يوسف طارق صالح

Table of Contents

Introduction:

A computer network defined as a group of computers or any other network devices (network nodes) such as phones, servers, or peripheral devices that could be located anywhere globally that are connected to each other to achieve transferring data, exchanging information, and sharing the network resources remotely.

As a result of the various types of network structure and the different operating systems around the world used in computers or any host that could be connected to a network, the need popped up to provide a global standard to be followed to make communication among those networks. One of those standards is the Operating System Interconnection (OSI) model which will be discussed in detail in this work. In 1984, OSI model was formally adopted by the International Standardization Organization (ISO).

The main aim of the OSI model is to standardize the way that different operating systems such as Windows, Linux, and Unix communicate with each other across the various structure of networks. That means providing more reliability to establish a connection among different types of networks, the simplicity to detect the faults, and more simplicity for the programmers to develop efficient applications for network purposes [3].

2. OSI Model:

2.1. OSI model Architecture:

Basically, the OSI model consists of seven layers which are Physical layer, Data-link layer, Network layer, Transport layer, Session layer, Presentation layer and Application layer as shown in figure (1). Starting from the sender, each layer serves a specific function or several tasks, receives data from the previous layer, adds its own functionalities, and then provides the new data to the next layer and vice versa, where the process can go back in a reverse path when the receiver gets the data. Also, a specific layer in the source node communicates with the corresponding layer in the destination node that is located anywhere as peer-to-peer communication [2].

Figure 1 : OSI Model Architecture

Furthermore, each layer consists of a package of protocols that achieve specific tasks according to that layer function.

Network Protocol refers to a set of rules that are established to control how is the communication among network devices performed without concerned about the differences in the OS that work on or their structure [2].

2.2. OSI model Functionality:

In general, the OSI model could be divided into two main parts, the lower layers, and the upper layers. In total, it consists of seven layers, starts with the Physical layer at the bottom and ends with the Application layer at the top.

The scenario of the OSI model is explained in term of sending data from node A to node B, in another word from the Application layer to the Physical layer of the source (sender), so all processes could take the reverse path when the data received by the destination (receiver) as shown in the figure (2).

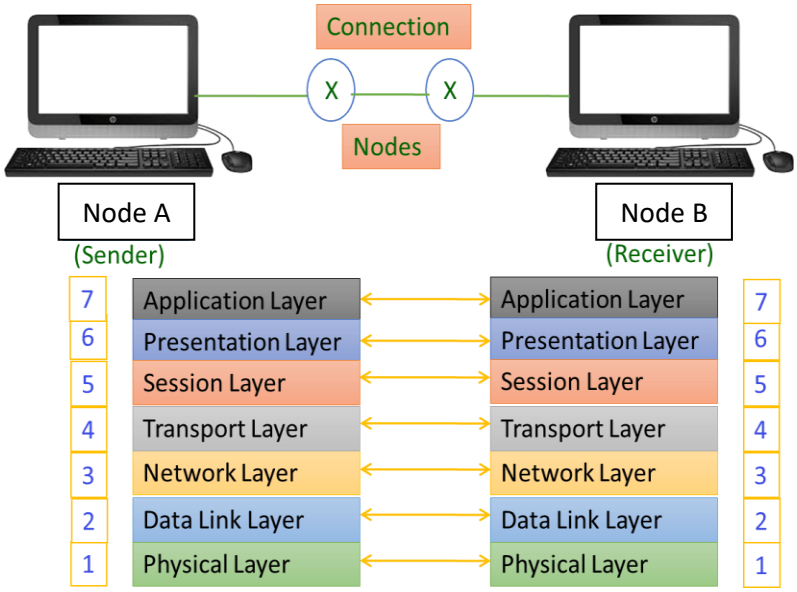


Figure 2 : The connection between two devices A and B

2.2.1 Upper Layers:

The OSI model is considered as a conceptual model which is used to help people know, understand, or simulate a subject the model represents, where in fact there is another model that is being used called the TCP model. The bottom two layers (Data Link and Physical) had merged in the Network Interface layer in the TCP/IP model, while the Network layer being called the Internet layer. Also, all the upper three layers had integrated as a single layer in the TCP/IP model called Application Layer. The responsibilities of those 3 layers are achieved by the network applications themselves such as web browsers or mail applications and so on as shown in figure (3).

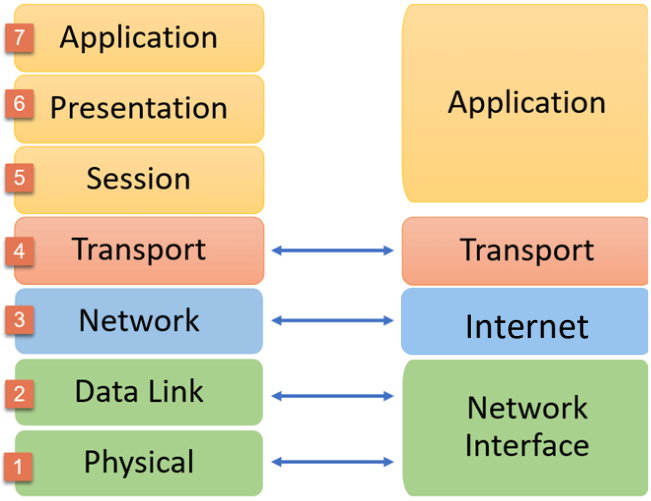


Figure 3: OSI Model and TCP Model

2.2.1.1 Application Layer:

It is the top layer in the OSI model, which is used by network applications such as web browsers, e-mails, conferences apps and so on.

- **Function:** Provides services for network applications with the help of protocols to perform user activities like web surfing and emails.
- **Protocols:** such as http, https, smtp, pop3, FTP, Telnet and DHCP [3][10].
- **Data Representation:** Data.

2.2.1.2 Presentation Layer:

Also, it is referred as syntax layer. It received data from the application layer in the form of numbers and characters.

- **Function:**
  - Translation:
    converts received data to machine understandable binary format such as ASCII to EBCDIC format.
  - Dara Compression:
    reduce the number of bits that are used to represent original data and it can be lossy or lossless. This can reduce the overall data size transmitted, which means faster transmission.
  - Data Encryption and Decryption:

- Protocols: such as Secure Socket Layer (SSL), JPEG, BMP, TIFF, WMV, AVI, ASCII, EBCDIC
- Data Representation: Data.

2.2.1.3 Session Layer:

enabling sending and receiving of data followed by termination of connections or sessions using the Application Programming Interfaces (APIs) such as NetBIOS.

- **Function:**
  - Session Management:
    Setting up and managing the connections. It allows different computers to communicate with each other and specify if the connection is a half-duplex or full duplex.
  - Authentication and Authorization:
    performs these tasks in a manner that a session or connection is established to the server.
  - Data Tracking:
    For example, the session layer Keeps track of which data packet belongs to which file during the downloading process.
- **Protocols:** such as Remote Procedure Call (RPC), Network File System (NFS), SQL.
- **Data Representation:** Data.

2.2.1.4 Transport Layer:

receives the data from the session layer to specify the type of protocol being used in the transmission process.

Transport layer provides two typed of services:

1- Connection Oriented service: in this type of connection the sender receives acknowledge from the receiver to ensure if the data are reliably transmitted.
Transmission Connection Protocol (TCP) is used with this type of connection.

The services that need for a reliable connection such as mailing, and file transfer use this type.

2- Connectionless service: in this type, the transmission of data is accomplished without acknowledge from the receiver [2][3].
User Datagram Protocol (UDP) is used with this type of connection. Where UDP is faster than TCP but less reliable due to there is no need for a feedback from the receiver device, so this type used for services online streaming movies, Voice over IP, gaming and DNS 3].

- **Function:**
  - Segmentation:

    Divides the received data into small chunks of data called segments [2].

  - Error Recovery:
    coordinates the connection between the source and destination and checks if there is any missed transmission of data by adding group of bits called checksum to the end of each segment. This technique called Automatic Repeat Request, so if there is any lost or corrupted data then will be sent again.
  - Flow Control:
    Control the amount of data being transmitted to be not exceed the capability of the transition media, for example in ethernet the segment should not be more than 1500 KB. Also, it controls the transmission rate of data between the sender and receiver to be in the range of the slower device.
  - Assignment of Port Number and Segment Sequence:
    By coordinating with the application layer, the port number are assigned to each segment for both the source and destination. The port number helps each segment to be directed to the correct application. As well the sequence number of each segment is being also added.
- **Protocols:** such as TCP, UDP.
- **Data Representation:** Segment.

2.2.2 Lower layers:

2.2.2.1 Network Layer: is responsible for data transmission between two devices that are in different networks.

- **Function:**
  - Routing:

    the process of determine the optimal path between the source and destination using some protocols such as Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Intermediate System- Intermediate System (IS-IS) [2][10].

- Logical Addressing:

  Adding the IP address to the header of both source and destination, so both of sender and receiver can be uniquely distinguished [2][10].

- **Protocols:** such as IP, IPS, OSPF, BGP and IS-IS [10].
- **Data Representation:** Packet.
- **Hardware:** Router.

2.2.2.2 Data Link Layer: receives packet form the Network layer. It is embedded as a software in the NIC.

Data Link Layer includes two sub layers [1]:

A) Logical Link Control (LLC) B) Media Access Control (MAC)

MAC address: is a unique number consisting of a group of digits in hexadecimal embedded in the Network Interface Card (NIC) by the manufacturer.

- **Function:**
  - responsible for encapsulating both the sender and receiver's MAC address to the received packets from the network layer after dividing them into frames according to the supported size from NIC and makes sure that it is transferred between two nodes is error-free by implementing Cyclic Redundancy Check (CRC), over the physical layer.
  - specifying the type of technology used in the network (such as Ethernet, wireless, or token ring) and grouping data according to that.
  - Also, it controls how data is placed and got off from the media. For example, on Ethernet to avoid the collision when multiple hosts send a message at the same time the Data Link layer keeps an eye on the media to hear when the media is free using the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol [7].

The MAC address of the receiver can be obtained by casting the source device for an ARP (Address Resolution Protocol) request on the transmission physical media as a query for other nodes in the network asking what is the host which has a certain IP and then gets the reply from the destination device with its MAC address [2].

- **Protocols:** MAC, ARP, High-level Data Link Control (HDLC), LAN drivers and access methods such as Ethernet and Token Ring, and the LAP-D protocol in ISDN networks.[3]
- **Data Representation:** Frame.
- **Hardware:** Switch and Bridge.

2.2.2.3 Physical Layer:

- **Function:** in charge of the actual physical connection among the nodes. where it conveys the stream of bits in the form of an electrical impulse, light, or radio signals depending on the used media from one node to the next other.
- **Protocols:** RS232, 100BaseTX, ISDN, COAX and Fiber
- **Data Representation:** Information in the form of bits.
- **Hardware:** such as Hub, NIC, Modem, Cables, Repeater and connectors.

After the data passed through all layers, the encapsulation process had done, and the final format of the data sent out from the physical layer will be as shown in figure (4).

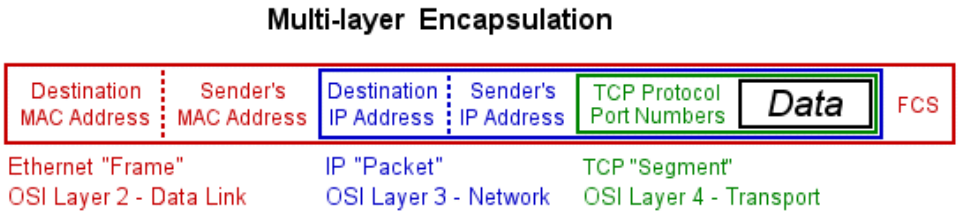


Figure (4): the final format of the data sent out from the physical layer.