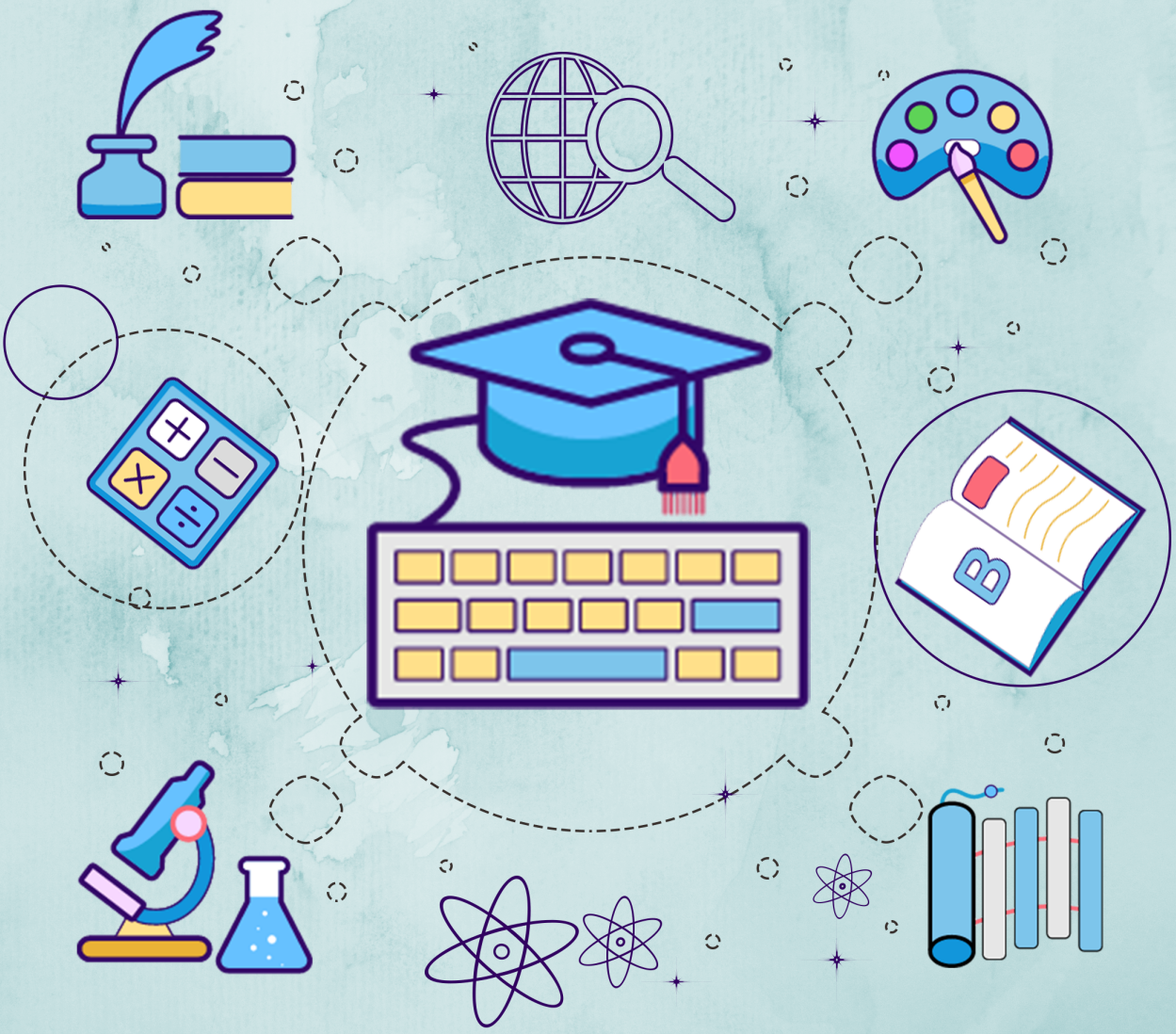
APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

KeralaNotes



SYLLABUS | STUDY MATERIALS | TEXTBOOK

PDF | SOLVED QUESTION PAPERS

www.keralanotes.com

KeralaNotes

KTU STUDY MATERIALS

COMPUTER NETWORKS

CST 303

Module 1

Related Link :

- KTU S5 STUDY MATERIALS
- KTU S5 NOTES
- KTU S5 SYLLABUS
- KTU S5 TEXTBOOK PDF
- KTU S5 PREVIOUS YEAR SOLVED QUESTION PAPER

COMPUTER NETWORKS

Module 1

Computer Network

- Set of devices(nodes) connected by a communication link(medium)
    - A node can be a computer, printer or any other device capable of sending/receiving data
    - A link can be a cable, air, optical fiber or any medium which can transport a signal carrying information
- Computer network is an Interconnected collection of computers
    - 2 computers are interconnected if they are able to exchange information
- Purpose : For sharing data & resources
    - *Communication* is the process of *exchanging information* between two persons or devices

Uses of Computer Networks

- **Business Applications**

  a) Resource sharing

  Ex: group of office workers sharing a common printer

  b)Information sharing

- **Home applications**

  1. Person-to-person communication. (email,instant messaging,group chat,video call)
  2. Access to remote information.(browsing,onlinenewspaper,online digital libraries)
  3. Interactive entertainment.(online games,live TV)
  4. E-commerce (home shopping,online payments)

- **Mobile users** (mobile with internet)

Advantages of Computer Networking

- It enhances communication and availability of information.
- It allows for more convenient resource sharing
- It makes file sharing easier
- It is highly flexible.
- Improved security
- Increased speed

Disadvantages of Computer Networking

- Privacy issues
- security difficulties
- Presence of computer viruses and malware
- Failure of server
- High cost of installation
- Proper & careful maintenance

Social Issues

Introduction of networking has introduced new social, ethical and political problems

- Newsgroups debate sensitive issues
- Network operator risk being sued for contents
- Right to free speech may be violated
- Anonymous message can be desirable

Network Topologies

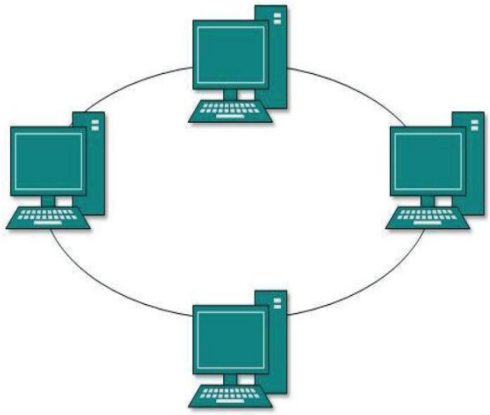
- Network Topology is the pattern used to arrange the nodes of network (describe the way computers are connected)
- Basic topologies: bus, ring, star, mesh, hybrid

1. Bus Topology

- Simplest
- designed in such a way that all the stations are connected through a single cable(known as a backbone cable)
- Advantages: low cost cable, moderate data speed, limited failure
- Disadvantages : reconfiguration is difficult, signal interference, extensive cabling

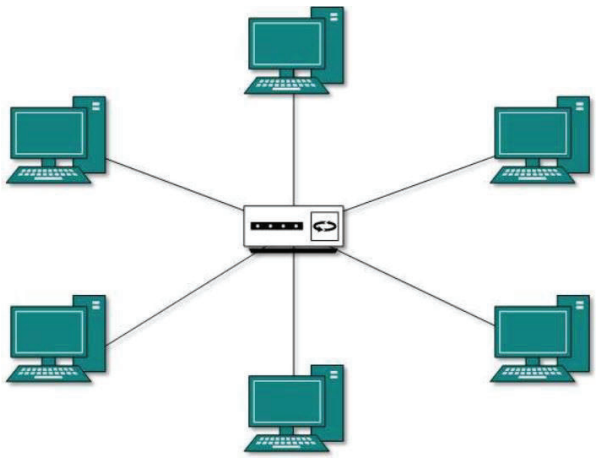
2. Ring Topology

- All computers are connected in a closed loop
- Each node connects to exactly two other nodes, creating a circular network structure.
- One broken device can disable entire network



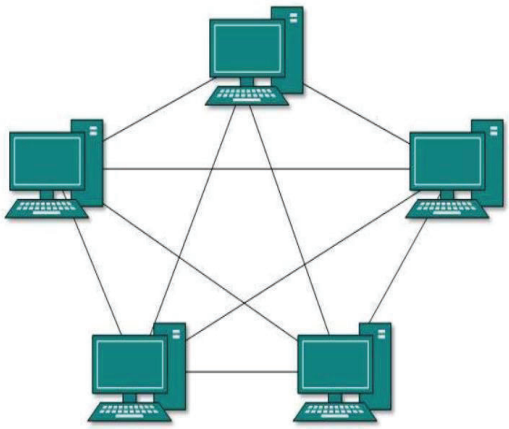
3. Star Topology

- All the devices are connected to a single hub
- This hub is the central node and all other nodes are connected to the central node
- Failure of central hub will make the entire network collapse
- Cost of installation is high



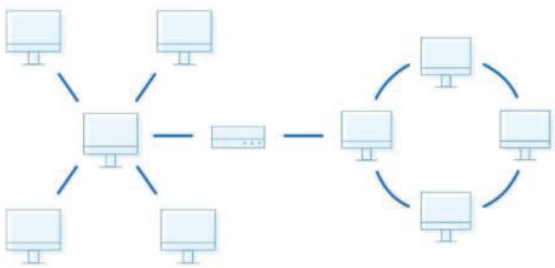
4. Mesh Topology

- Computers are inter-connected with each other
- There are multiple paths from one computer to another
- Internet is an example of mesh topology
- 2 types –fully connected and partially connected(certain computers are connected) mesh topology



5. Hybrid Topology

- Combination of various different topologies
- Two or more topologies are combined together
- Advantages: reliable, flexible, effective
- Disadvantages: complex design , costly infrastructure



Network hardware

❖ **Types of computer network (on the basis of area covered)**

1. Personal Area Network (PAN)
2. Local Area Network (LAN)
3. Metropolitan Area Network (MAN)
4. Wide Area Network (WAN)

1. Personal Area Network (PAN)

- A computer network that connect the devices within the range of a person
- smallest and most basic type of network
- Can be wired or wireless
- Cover small area

Ex:

- connection between a Bluetooth earpiece and a smartphone)
- connects a computer with its peripherals(keyboard, mouse,printer….)

2. Local Area Network (LAN)

- Interconnects computers within a limited area such as a residence,school,university campus or office building
- Its privately-owned networks
- Operates over a small physical area ie, within a single building or campus of up to a few kilometers in size.
- Easy to design and maintain
- WLAN: Wireless LAN –connect devices via Wi-fi to your home network

3. Metropolitan Area Network (MAN)

- A MAN, covers a city.
- geographical area covered by MAN is larger than LAN but Smaller than WAN
- The best-known example of a MAN is the cable television network available in many cities.
- Deliver fast and effective communication by using a high speed carrier eg: fiber optic cables

4. Wide Area Network (WAN)

- spans a large geographical area, often a country or continent
- Best example of WAN is internet
- Internet is considered as the largest WAN in the world
- communicate devices across the world

	LAN	MAN	WAN
	Local Area Network	**Metropolitan Area Network**	**Wide Area Network**
Coverage	Small geographical area	Covers cities or towns	Large geographical area
ownership	private	Private/public	Private/public
Design & maintenance	easy	difficult	difficult
cost	Low cost of set up	Moderate cost	high
Error rate in data transmission	Very low error rate	low error rate	Comparatively high error rate
Propagation delay	short	moderate	long

internetwork or internet

- A collection of interconnected networks is called an internetwork or internet.
- An internetwork is formed when distinct networks are interconnected
- Internet: not a single network, a network of networks
- Advantages:
    - Improved availability
    - Improved dataflow
    - Increased reach
    - Access to knowledge
- Disadvantages:
    - Theft of personal details
    - Virus threat

Transmission modes

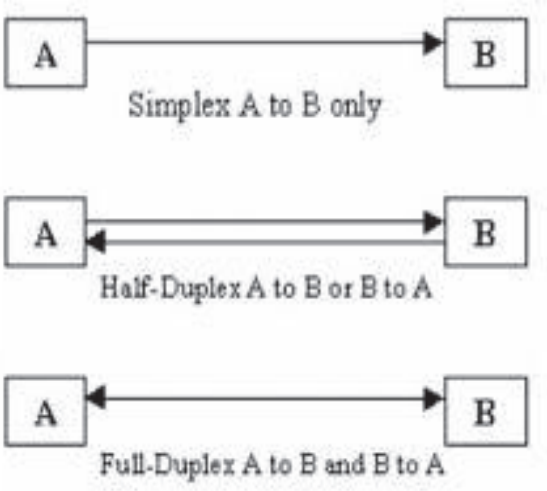
Communication between 2 devices can be

- ❑ **Simplex**
- ❑ **full-duplex**
- ❑ **half-duplex**

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. Ex: keyboard, monitor

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. Ex : walkie-talkies

In full-duplex mode, both stations can transmit and receive at same time ie, simultaneously. Ex : telephone network



Network Software

Protocol

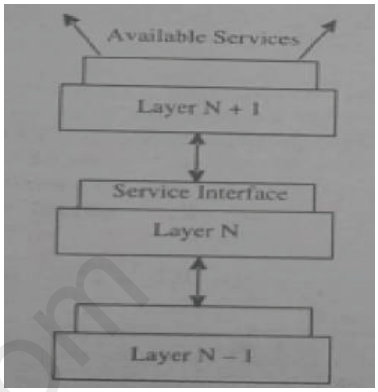
In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol.

- A **protocol** is a set of rules that govern data communications.
- A protocol defines what is communicated, how it is communicated, and when it is communicated.
- The key elements of a protocol are

1) **Syntax** (format or structure of data blocks)
2) **Semantics** (it refers to the meaning of each section of data bits. How are a specified pattern to be interpreted;and what action is to be taken based on that interpretation
3) **Timing** (when data should be sent ,how fast they can be sent)

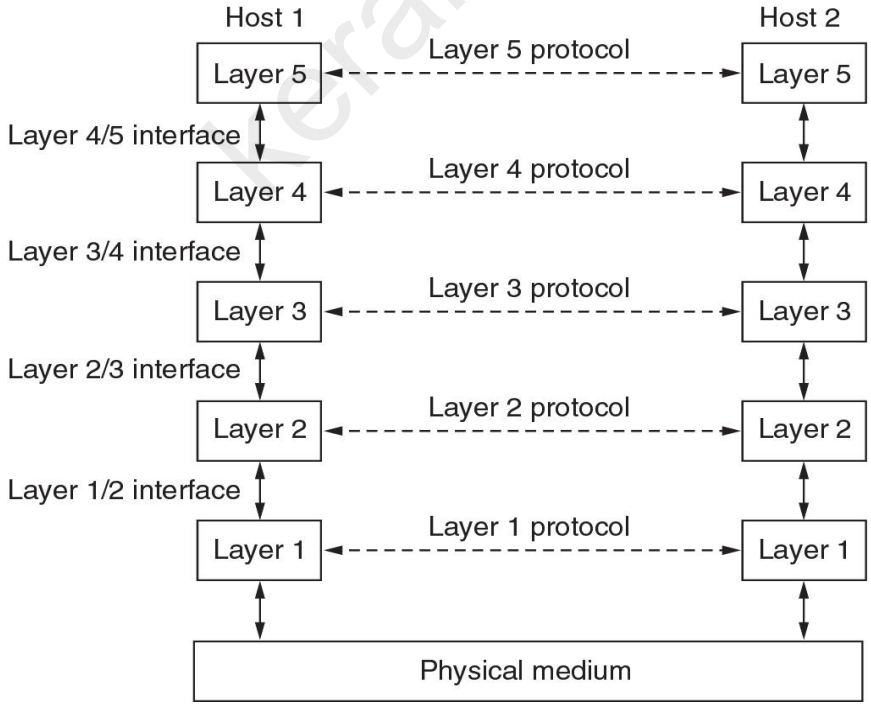
Protocol Hierarchies : - Layered architecture

- To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it.
- The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.
- The purpose of each layer is to offer certain services to the higher layers while shielding those layers from the details of how the offered services are actually implemented.
- each layer is offering certain services to the layer above it
- In a layer n architecture, layer n on one machine carries on a conversation with layer n on another machine, and the rules and conventions used in this conversation are collectively known as the layer n protocol.



- Basically, a protocol is an agreement between the communicating parties on how communication is to proceed.

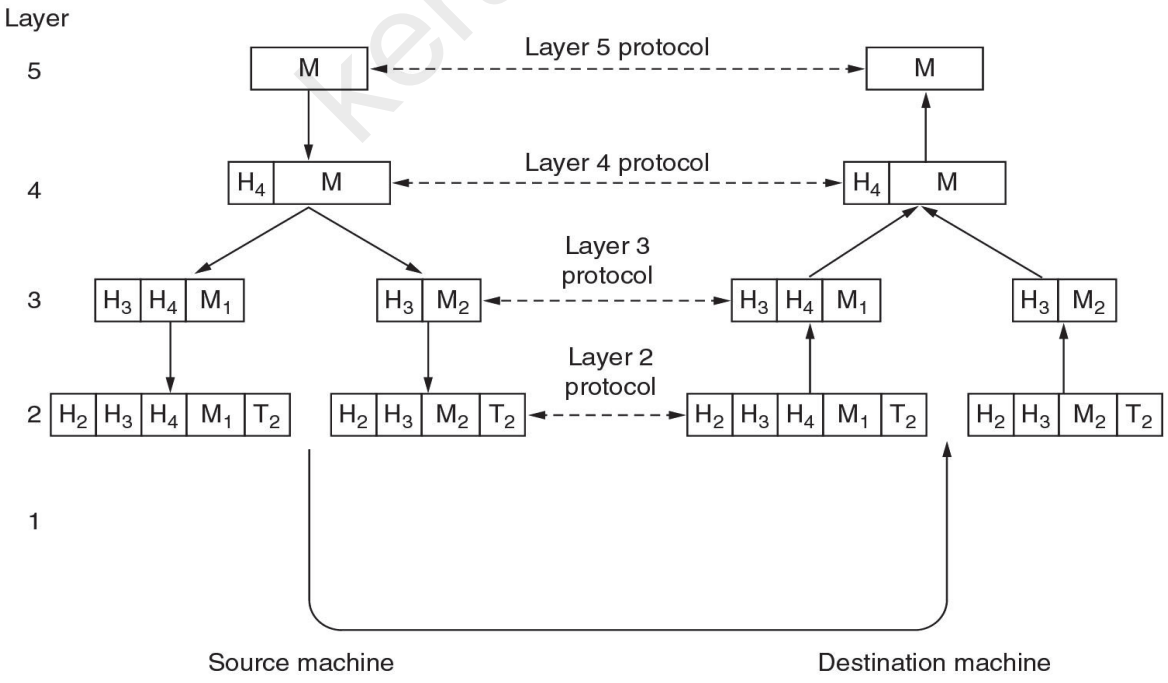
Lets take an example of the five layered architecture



A five-layer network is illustrated in Fig.

- In reality, no data are directly transferred from layer *n* on one machine to layer *n* on another machine. Instead, each layer passes data and control information to the layer immediately below it, until the lowest layer is reached. Ie, The data and information is passed by each layer to the lower layer.
- When the lower layer is reached it is passed to the physical medium
- Below layer 1 is the **physical medium** through which actual communication occurs.
- Between each pair of adjacent layers tis an **interface**. The interface defines which type of operations and services t the lower layer offers to the upper layer.
- Protocols are together called ***protocol stack*** or set of protocols And a set of layers and protocols is called network architecture.

Now consider a more technical example: how to provide communication to the top layer of the five-layer network in Fig.



- A message, *M*, is produced by an application process running in layer 5 and given to layer 4 for transmission. Layer 4 puts a header in front of the message to identify the message and passes the result to layer 3. The header includes control information such as addresses, to allow layer 4 on the destination machine to deliver the message.
- Consequently, layer 3 must break up the incoming messages into smaller units, packets, prepending a layer 3 header to each packet. In this example, *M* is split into two parts, M_1 and M_2, that will be transmitted separately. Layer 3 decides which of the outgoing lines to use and passes the packets to layer 2. Layer 2 adds to each piece not only a header but also a trailer, and gives the resulting unit to layer 1 for physical transmission.
- At the receiving machine the message moves upward, from layer to layer, with headers being stripped off as it progresses. None of the headers for layers below *n* are passed up to layer *n.*
- header & trailer includes control information, such as sequence numbers, sizes, times, and other control fields

Design Issues for the Layers

- Addressing
- Rules for data transfer
- Loss of sequencing
- Error Control
- Flow Control
- Inability to accept Long messages
- Routing

etc

1. **Addressing :** It is necessary to have a mechanism to identify senders and receivers. since there are multiple possible destinations, some form of addressing is required in order to specify the specific destination.
2. **Error Control:** Error detection and correction are important. Many error detecting and error correcting codes are available. Both sending and receiving ends must agree which one is being used. The Receiver should be able to tell the sender by some means , that it has received a correct message or a wrong message.
3. **Long messages (ability of receiving long messages.):** At several levels, another problem should be used, which is inability of all process to accept long messages. Hence , a mechanism needs to be developed to disassemble , transmit and then reassemble message
4. **Routing** : When there are multiple paths between source and destination, only one route must be chosen. This decision is made on the basis of several routing algorithms, which chooses optimized route to the destination.
5. **Loss of sequencing :** All the communication channels cannot preserve the order in which messages are sent on it. Therefore ,there is a possibility of Loss of sequencing. To avoid this, all the pieces should be numbered so that they can be put back together at the receiver in the appropriate sequence.

6. Rules for data transfer: In some data transfer take place in one direction and in some other it travel in both direction but not simultaneously. And there are situations were data transfer takes place simultaneously. Protocol determines how many logical channels are needed per connection

7. **Flow Control** : If there is a fast sender at one end sending data to a slow receiver, then there must be flow control mechanism to control the loss of data by slow receivers. There are several mechanisms used for flow control such as slow down the fast sender

8. A design issue concerns the **evolution of the network**. : Over time, networks grow larger and new designs emerge that need to be connected to the existing network.

9. Scalability : When network gets large, new problem arises. Thus scalability is important so that network can continue to work well when it gets large.

10. Confidentiality and Integrity: The last major design issue is to secure the network by defending it against different kinds of threats. One of the threats we have mentioned previously is that of eavesdropping on communications. Mechanisms that provide **confidentiality** defend against this threat, and they are used in multiple layers. Mechanisms for **authentication** prevent someone from impersonating someone else. Mechanisms for integrity prevent faulty changes to messages.

Connection-Oriented Versus Connectionless Service

Layers can offer two different types of service to the layers above them:

✓ connection-oriented

✓ connectionless.

1. Connection-oriented service

- This service follows a sequence of operations

i. Establish a connection

ii. Data transfer

iii. Terminate the connection

- To talk to someone, you pick up the phone, dial the number, talk, and then hang up. Similarly, to use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection. In some cases when a connection is established, the sender, receiver conduct a **negotiation** about the parameters to be used, such as maximum message size, quality of service required, and other issues. Typically, one side makes a proposal and the other side can accept it, reject it, or make a counter-proposal.
- Here Data arrive in the order they were sent
- reliable service

2. Connectionless service

- No connection Establishment
- Unreliable (meaning not acknowledged) connectionless service
- does not return an acknowledgement to the sender.
- Normally, when two messages are sent to the same destination, the first one sent will be the first one to arrive. However, it is possible that the first one sent can be delayed so that the second one arrives first.
- no guarantee.
- The order in which messages are sent and arrived can be different

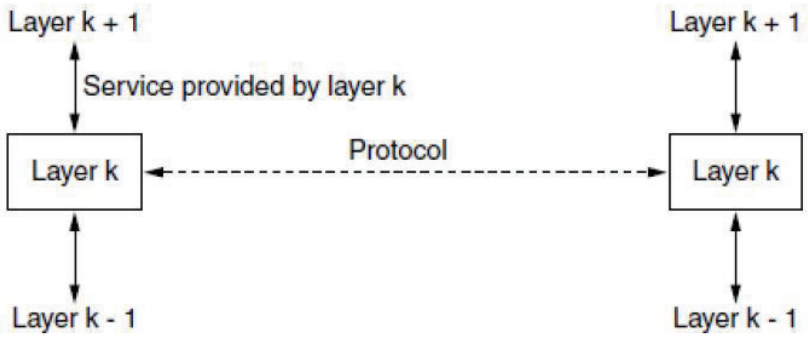
Service Primitives

- A service is formally specified by a set of primitives (operations)
- These primitives tell the service to perform some action or report on an action taken by a peer entity.
- The set of primitives available depends on the nature of the service being provided.
- The primitives for connection-oriented service are different from those of connectionless service
- primitives used for a request-reply interaction in a client-server environment =>

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection
ACCEPT	Accept an incoming connection from a peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

The Relationship of Services to Protocols

- Services and protocols are distinct concepts. This distinction is so important that we emphasize it again here. A *service* is a set of primitives (operations) that a layer provides to the layer above it. The service defines what operations the layer is prepared to perform on behalf of its users, but it says nothing at all about how these operations are implemented.
- A service relates to an interface between two layers, with the lower layer being the service provider and the upper layer being the service user. A *protocol*, in contrast, is a set of rules governing the format and meaning of the packets, or messages that are exchanged by the peer entities within a layer. Entities use protocols to implement their service definitions. They are free to change their protocols at will, provided they do not change the service visible to their users. In this way, the service and the protocol are completely decoupled. This is a key concept that any network designer should understand well. To repeat this crucial point, services relate to the interfaces between layers, as illustrated in Fig. In contrast, protocols relate to the packets sent between peer entities on different machines



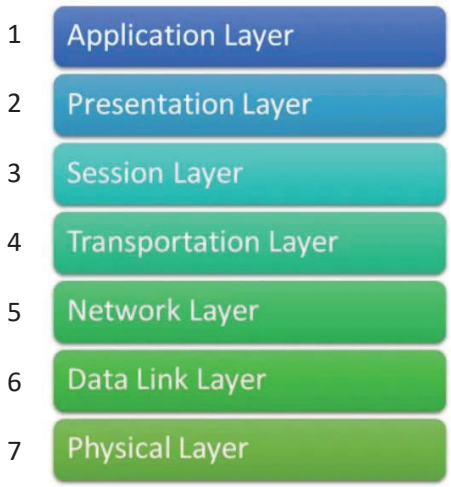
Reference Models (network architectures)

- **OSI Reference Model**
- **TCP/IP Reference Model**

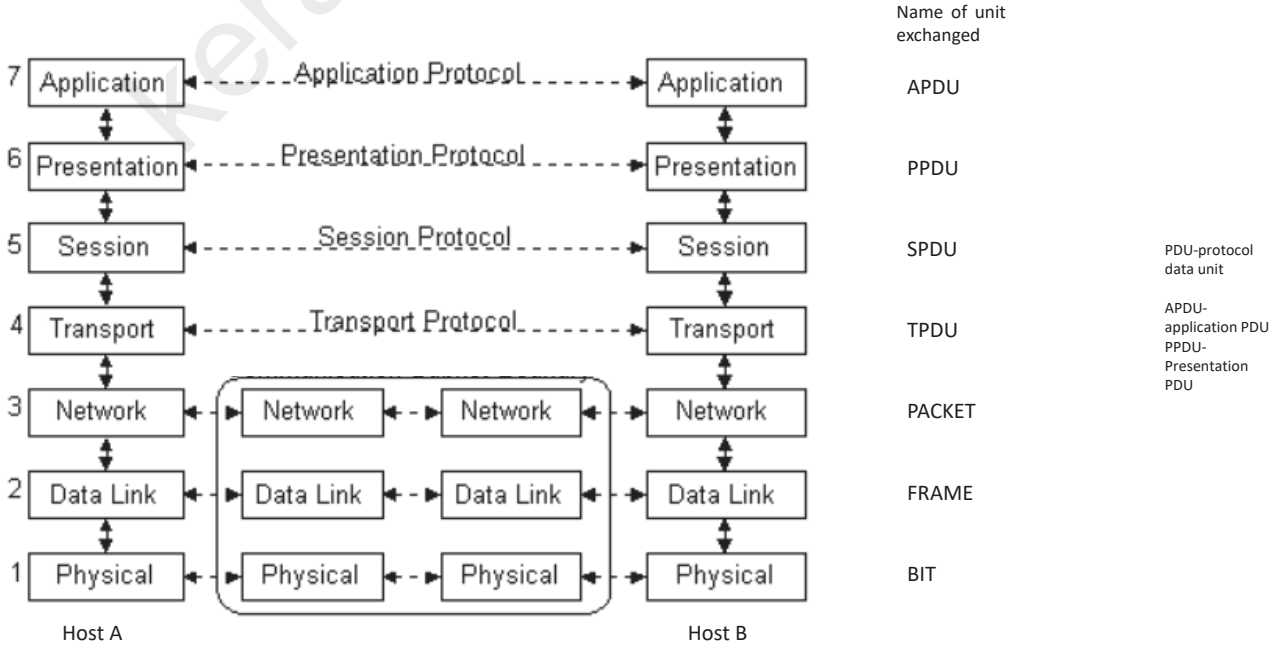
OSI Reference Model

- OSI stands for Open Systems Interconnection
- Designed by the International Standards Organization (ISO)
- The model is called the ISO-OSI (Open Systems Interconnection) Reference Model

  (Because it deals with connecting open systems—that is, systems that are open for communication with other systems.)
- It has seven layers :



- The OSI model is a Layered architecture



1. Physical Layer

- The physical layer handles the transmission of raw bits over a communication channel.
- Also concerned with
  - **Representation of bits:** The physical layer data consists of a stream of bits (sequence of Os or 1s). To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding (how Os and 1s are changed to signals).
  - **Data rate:** The transmission rate-the number of bits sent each second-is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.
  - **Synchronization of bits:** The sender and receiver must use the same bit rate also must be synchronized at the bit level.
  - **Line configuration:** The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices
  - **Physical topology:** The physical topology defines how devices are connected to make a network. (ie, mesh,ring,bus or a hybrid topology)
  - **Transmission mode**: The physical layer also defines the direction of transmission between two devices (simplex, half-duplex, or full-duplex)

2. Data Link Layer

- Data link layer is responsible for moving frames from one hop (node) to the next. (node-to-node delivery)
- 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.
  - **Flow control**: If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
  - **Error control**: The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames.
  - **Access control:** When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.
  - **Physical addressing**. If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one

3. Network Layer

- The network layer is responsible for the source-to-destination delivery of a packet
- At this layer, the unit of data exchanged among nodes is typically called a packet
- Network layer ensures that each packet gets from its point of origin to its final destination.
- Other responsibilities of the network layer includes routing and Logical addressing
- **Logical addressing:** The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
- **Routing** : When there are multiple paths between source and destination, only one route must be chosen

4. Transport Layer

- Here, the unit of data exchanged is TPDU
- The transport layer is responsible for process-to-process delivery of the entire message.
- Other responsibilities:
  - **Connection control:** The transport layer can be either connectionless or connection oriented. (A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.)
    - Protocols used :TCP-Transmission control protocol (connection oriented)
      UDP-user datagram protocol (connectionless)
  - **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 upon arriving at the destination and to identify and replace packets that were lost in transmission.
  - **Flow control**
  - **Error control**

5. Session Layer

- It establishes, maintains, and synchronizes the interaction among communicating systems.
- session layer is responsible for dialog control and synchronization.
- Specific responsibilities of the session layer includes:
  - Dialog control. The session layer allows two systems to enter into a dialog. It 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(inspect any packet), or synchronization points, to a stream of data.

6. Presentation Layer

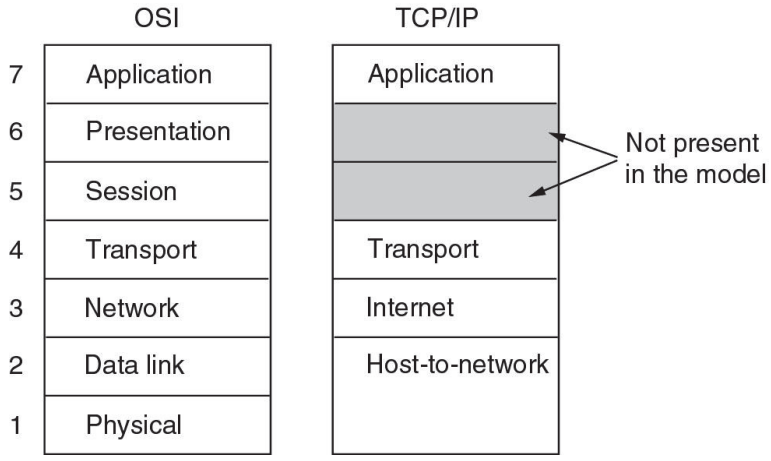
- presentation layer is concerned with the syntax and semantics of the information exchanged between two systems .
- Specific responsibilities of the presentation layer includes: the
  - **Translation** (exchanging information the form of character strings, numbers, and so on. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format)
  - **Encryption** : (ensure privacy) (sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form)
  - **compression** :Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video

6. Application Layer

- Provide services to users
- application layer 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, shared database management, and other types of distributed information services.
- Specific services provided:
  - **File transfer, access, and management**: This application allows a user to access files (to make changes or read data), to retrieve files , and to manage or control files.
  - **Mail services:** This application provides the basis for e-mail forwarding and storage
  - **Directory services**: This application provides distributed database sources and access for global information about various objects and services.
- Protocols used : FTP, SMTP, HTTP etc

TCP/IP Reference Model

- The TCP/IP protocol suite is a 4 layered suite of communication protocol
- It is named after the 2 main protocols –TCP and IP
- TCP stands for Transmission Control Protocol
- IP stands for Internet Protocol



- The 4 layers of TCP/Model are: **host-to-network, internet, transport, and application layer**

1. Host-to-Network Layer

- host-to-network layer is equivalent to the combination of the physical and data link layers
- The TCP/IP reference model does not really say much about what happens here, except to point out that the host has to connect to the network using some protocol so it can send IP packets to it. This protocol is not defined and varies from host to host and network to network.

2. Internet Layer

- Internet layer defines an official packet format and protocol called IP (Internet Protocol).
- The internet layer is equivalent to the network layer.
- The job of the internet layer is to deliver IP packets where they are supposed to go.
- Packet routing & avoiding congestion are the major issue here.
- For these reasons, it is reasonable to say that the TCP/IP internet layer is similar in functionality to the OSI network layer
- uses four supporting protocols:

  ARP - Address Resolution Protocol

  RARP -Reverse Address Resolution Protocol

  ICMP -Internet Control Message Protocol

  IGMP -Internet Group Message Protocol

3. Transport Layer

- UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process.
    - TCP (Transmission Control Protocol –it's a connection-oriented protocol . TCP is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data.
    - UDP (User Datagram Protocol) -Unreliable connectionless protocol
- A new transport layer protocol, SCTP, has been devised to meet the needs of some newer applications.
    - Stream Control Transmission Protocol (SCTP)-It is a transport layer protocol that combines the best features of UDP and TCP

4. Application Layer

- Provide services to users
- contains all the higher-level protocols like

    file transfer (FTP)

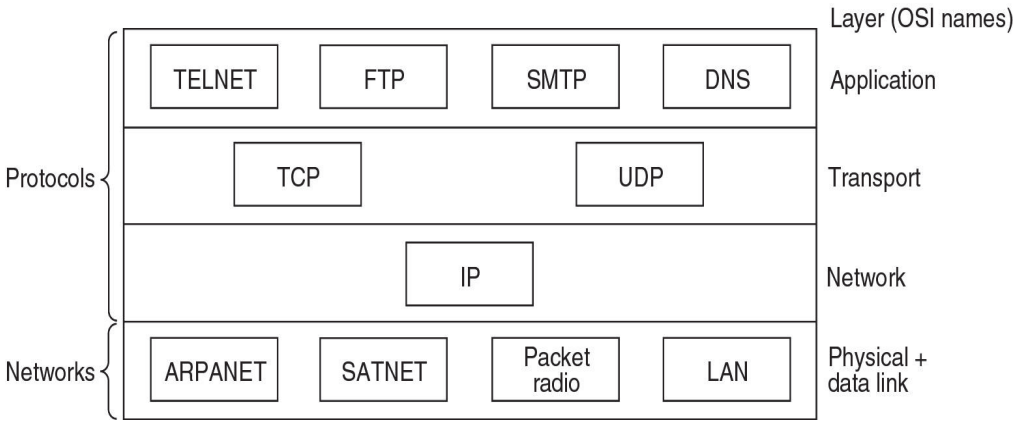
    electronic mail (SMTP-SMTP (Simple Mail Transfer Protocol)

    Domain Name System (DNS)

    Terminal network (TELNET)

    Hyper Text Transfer Protocol (HTTP) etc

=> Protocols and networks in the TCP/IP model

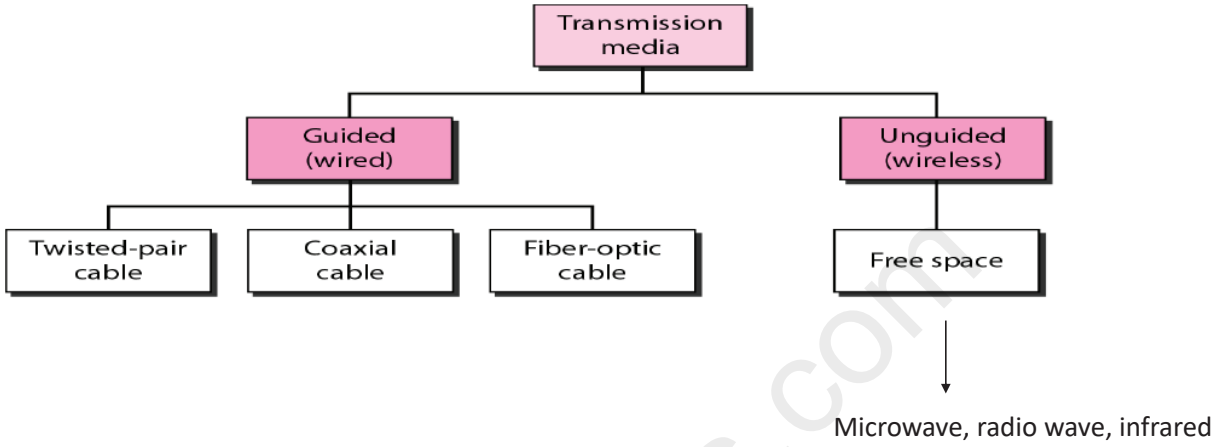


ARPANET - Advanced Research Projects Agency Network
SATNET – Sustainable Agriculture Trainers Network

OSI MODEL	TCP/IP MODEL
Contains 7 layers	Contains 4 layers
Considered a theoretical model	Considered more reliable
It distinguishes between service, interface and protocol	Does not clearly distinguish between service, interface and protocol
Model was developed before the development of protocols	Protocols were developed first & then the model was developed
Protocol independent standard	Protocol dependent standard
More complexity due to more number of layers	Less complexity due to less number of layers

Transmission Media

A transmission medium can be defined as anything that can carry information from a source to a destination.

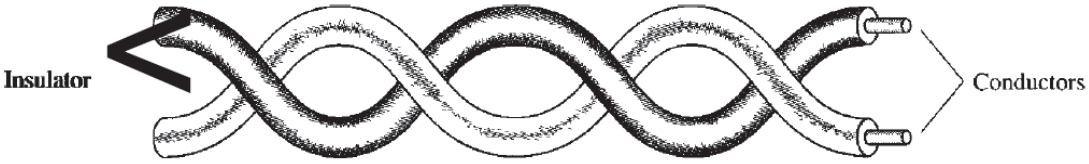


Guided media

- 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

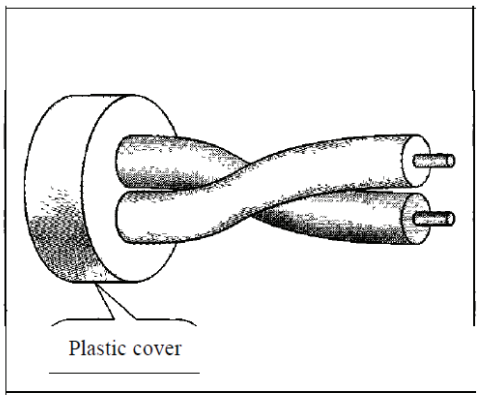
- A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together
- One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference



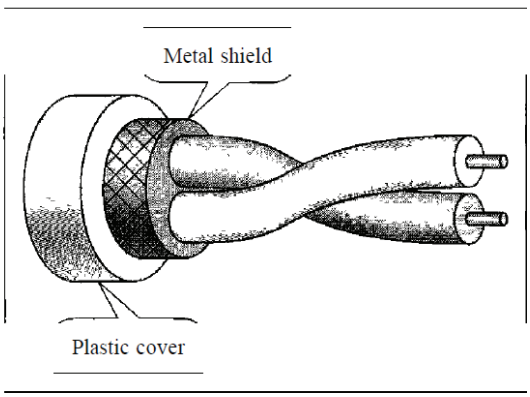
- *Why to twist the wires?*
  - ✓ Twisting of wires will reduce the effect of noise or external interference.
  - ✓ The number of twists per unit length will determine the quality of cable.
  - ✓ More twists means better quality

- 2 types: **a) Shielded Twisted-Pair Cable (STP)**
  b) Unshielded Twisted-Pair Cable (UTP)
- UTP:
  - The most common twisted-pair cable used in communications
  - Very cheap
  - Easy to install
  - Badly affected by the noise interference

- STP:
  - STP cable has a metal foil or braided mesh to cover each pair of insulating conductors. This is known as metal shield.It reduces the interference of the noise
  - metal casing improves the quality of cable by preventing the penetration of noise or crosstalk
  - it is bulkier
  - more expensive



a.UTP



b.STP

Applications :

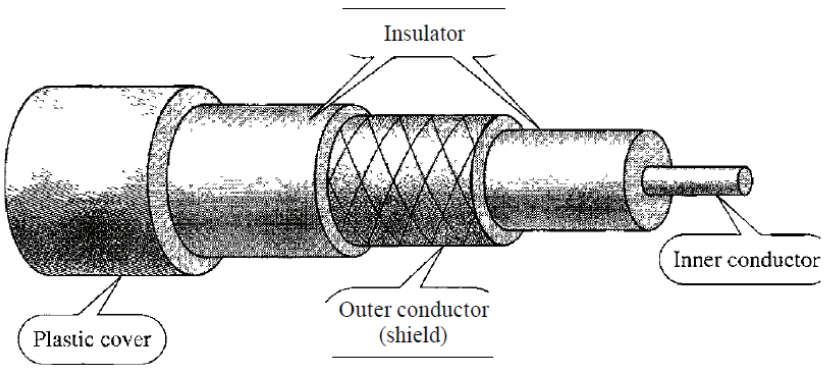
- In point to point and point to multipoint communications
- Telephone systems
- Local-area networks, such as l0Base-T and l00Base-T, also use twisted-pair cables.
- in telephone lines to provide voice and data channels.

……

In twisted pair , 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. This results in a difference at the receiver. By twisting the pairs, a balance is maintained. Twisting makes it probable that both wires are equally affected by external influences (noise or crosstalk). The number of twists per unit of length has some effect on the quality of the cable.

2. Coaxial Cable

- Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable.
- 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



Category	Impedance	Use
RG-59	75 Ω	Cable TV

- Coaxial cables are categorized by their radio government (RG) ratings
- To connect coaxial cable to devices, we need coaxial connectors (the BNC connector, the BNC T connector, and the BNC terminator.)
- Costlier than twisted-pair cable
- Excellent noise immunity
- Cheaper than optical fiber cables
- Large bandwidth and low losses

Applications :

- Analog telephone networks
- digital telephone networks
- Cable TV networks
- traditional Ethernet LAN
- Digital transmission

3. Optical fiber

- Optical fiber is a cable that accepts and transports signals in the form of light.
- A fiber-optic cable is made of glass or plastic
- It consist of an inner glass core surrounded by a glass cladding which has lower refractive index
- Optical fibers use reflection to guide light through a channel.
- Light is launched into the fiber using a light source such as light emitting diode(LED) Or laser
- A glass or plastic core is surrounded by a cladding of less dense glass or plastic.
- Its costlier than other 2 types

Advantages:

- Higher bandwidth
- Less signal attenuation
- Immunity to electromagnetic interference. (Electromagnetic noise cannot affect fiber-optic cables.)
- Resistance to corrosive materials (Glass is more resistant to corrosive materials than copper.)
- Light weight (Fiber-optic cables are much lighter than copper cables.)
- 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.)

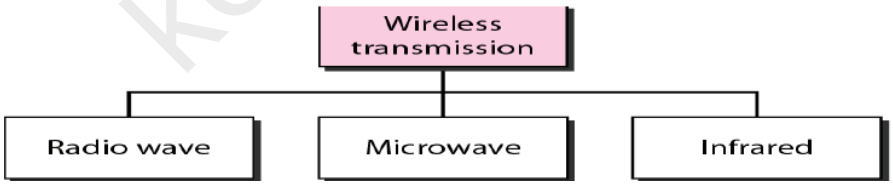
Disadvantages:

- Installation and maintenance. (Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.)
- Unidirectional light propagation. (Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.)
- Cost. (The cable and the interfaces are relatively more expensive than those of other guided media)

Applications:

- Fiber-optic cable is often found in backbone networks
- Telephone systems
- Some cable TV companies use a combination of optical fiber and coaxial cable,thus creating a hybrid network.
- Local-area networks (such as 100Base-FX network (Fast Ethernet) and 1000Base-X also use fiber-optic cable)

Unguided media



- Unguided media transport electromagnetic waves without using a physical conductor
- Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

1.Radio Waves

- Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves
- Radio waves 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.)
- 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.
- Radio waves, particularly those of low and medium frequencies, can penetrate walls.
- The radio wave band is relatively narrow, just under 1 GHz, compared to the microwave band. When this band is divided into sub-bands, the sub-bands are also narrow, leading to a low data rate for digital communications.
- Radio waves use omnidirectional antennas that send out signals in all directions

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, 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

Characteristics:

- 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.)
- Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside buildings.
- The microwave band is relatively wide, almost 299 GHz. Therefore wider subbands can be assigned, and a high data rate is possible
- Use of certain portions of the band requires permission from authorities

- 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

Applications

- cellular telephones
- satellite networks
- wireless LANs

3. Infrared

- Infrared waves having 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.
- 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

- Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

Performance indicators

1.Bandwidth

- One characteristic that measures network performance is bandwidth.
- It's the data carrying capacity of the network or transmission media
- It's the Max channel capacity to transmit data
- It's the Volume of data transmitted at a particular time
- The term can be used in two different contexts with two different measuring values:
  - bandwidth in hertz
  - bandwidth in bits per second.

✓ **bandwidth in hertz**, refers to the range of frequencies in a composite signal or the range of frequencies that a channel can pass.

For example, we can say the bandwidth of a subscriber telephone line is 4 kHz.

✓ **bandwidth in bits per second**, refers to the speed of bit transmission in a channel or link.ie, the number of bits per second that a channel, a link, or even a network can transmit.

For example, one can say the bandwidth of a Fast Ethernet network (or the links in this network) is a maximum of 100 Mbps. This means that this network can send 100 Mbps.

❑ an increase in bandwidth in hertz means an increase in bandwidth in bits per second. The relationship depends on whether we have baseband transmission or transmission with modulation

2. Throughput

- The throughput is a measure of how fast we can actually send data through a network.
- At first glance, bandwidth in bits per second and throughput seem the same, but they are different. The bandwidth is a potential measurement of a link; the throughput is an actual measurement of how fast we can send data.

3. Latency (Delay)

- The latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.
- latency is made of four components: propagation time, transmission time, queuing time and processing delay.
- Latency =propagation time +transmission time +queuing time + processing delay

Propagation Time

- Propagation time measures the time required for a bit to travel from the source to the destination.
- The propagation time is calculated by dividing the distance by the propagation speed.

$$\text{Propagation time} = \frac{\text{Distance}}{\text{Propagation speed}}$$

Transmission Time

- In data communications we don't send just 1 bit, we send a message. The first bit may take a time equal to the propagation time to reach its destination; the last bit also may take the same amount of time. However, there is a time between the first bit leaving the sender and the last bit arriving at the receiver. The first bit leaves earlier and arrives earlier; the last bit leaves later and arrives later. The time required for transmission of a message depends on the size of the message and the bandwidth of the channel.

$$\text{Transmission time} = \frac{\text{Message size}}{\text{Bandwidth}}$$

Queuing Time

- The third component in latency is the queuing time, the time needed for each intermediate or end device to hold the message before it can be processed.
- The queuing time is not a fixed factor; it changes with the load imposed on the network.
- When there is heavy traffic on the network, the queuing time increases. An intermediate device, such as a router, queues the arrived messages and processes them one by one. If there are many messages, each message will have to wait.

4.Bandwidth-Delay Product

- Bandwidth and delay are two performance metrics of a link. what is very important in data communications is the product of the two, the bandwidth-delay product.
- The bandwidth-delay product defines the number of bits that can fill the link.