MAR GREGORIOS COLLEGE
OF ARTS & SCIENCE

Block No.8, College Road, Mogappair West, Chennai – 37

Affiliated to the University of Madras
Approved by the Government of Tamil Nadu
An ISO 9001:2015 Certified Institution

DEPARTMENT OF

COMPUTER APPLICATION

SUBJECT NAME: DATA COMMUNICATION AND NETWORKING

SUBJECT CODE: SAZ6B

SEMESTER: VI

PREPARED BY: PROF. S.RANGANATHAN

Title of the Course/	**Paper-XVIII DATA COMMUNICATION AND NETWORKING**		
Core	**III Year & Sixth Semester**	Credit: 4	
Objective of the course	This course introduces the concepts of Networking		
Course outline	Unit-1: Introduction to Data Communication, Network, Protocols & standards and standards organizations - Line Configuration - Topology - Transmission mode - Classification of Network - OSI Model - Layers of OSI Model.		
	Unit-2: Parallel and Serial Transmission - DTE/DCE/such as EIA-449, EIA-530, EIA-202 and x.21 interface - Interface standards - Modems - Guided Media - Unguided Media - Performance - Types of Error - Error Detection - Error Corrections.		
	Unit-3: Multiplexing - Types of Multiplexing - Multiplexing Application - Telephone system - Project 802 - Ethernet - Token Bus - Token Ring - FDDI - IEEE 802.6 - SMDS - Circuit Switching - Packet Switching - Message switching - Connection Oriented and Connectionless services.		
	Unit-4: History of Analog and Digital Network - Access to ISDN - ISDN Layers - Broadband ISDN - X.25 Layers - Packet Layer Protocol - ATM - ATM Topology - ATM Protocol.		
	Unit-5 : Repeaters - Bridges - Routers - Gateway - Routing algorithms - TCP/IP Network, Transport and Application Layers of TCP/IP - World Wide Web.		

1. Recommended Texts

i. Behrouz and Forouzan,2001,Introduction to Data Communication and Networking, 2nd Edition,TMH.

2. Reference Books

i. Jean Walrand 1998,Communication Networks (A first Course),Second Edition, WCB/McGraw Hill.

ii. Behrouz and Forouzan,2006,Data Communication and Networking,3nd Edition, TMH.

Unit I

Introduction to Data Communication:

In Data Communications, *data* generally are defined as information that is stored in digital form. *Data communications* is the process of transferring digital information between two or more points. *Information* is defined as the knowledge or intelligence. Data communications can be summarized as the transmission, reception, and processing of digital information. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

Network:

Any group of computers connected together can be called a *data communications network*, and the process of sharing resources between computers over a data communications network is called *networking*. The most important considerations of a data communications network are *performance, transmission rate, reliability and security*.

Protocols & standards and standards organizations:

An association of organizations, governments, manufacturers and users form the standards organizations and are responsible for developing, coordinating and maintaining the standards. The intent is that all data communications equipment manufacturers and users comply with these standards. The primary standards organizations for data communication are:

1. International Standard Organization (ISO)

ISO is the international organization for standardization on a wide range of subjects. It is comprised mainly of members from the standards committee of various governments throughout the world. It is even responsible for developing models which provides high level of system compatibility, quality enhancement, improved productivity and reduced costs. The ISO is also responsible for endorsing and coordinating the work of the other standards organizations.

2. International Telecommunications Union-Telecommunication Sector (ITU-T)

ITU-T is one of the four permanent parts of the International Telecommunications Union based in Geneva, Switzerland. It has developed three sets of specifications: the *V series* for modem interfacing and data transmission over telephone lines, the *X series* for data transmission over public digital networks, email and directory services; the *I and Q series* for Integrated Services Digital Network (ISDN) and its extension Broadband ISDN. ITU-T membership consists of government authorities and representatives from many countries and it is the present standards organization for the United Nations.

3. Institute of Electrical and Electronics Engineers (IEEE)
IEEE is an international professional organization founded in United States and is compromised of electronics, computer and communications engineers. It is currently the world's largest professional society with over 200,000 members. It develops communication and information processing standards with the underlying goal of advancing theory, creativity, and product quality in any field related to electrical engineering.

4. American National Standards Institute (ANSI)
ANSI is the official standards agency for the United States and is the U.S voting representative for the ISO. ANSI is a completely private, non-profit organization comprised of equipment manufacturers and users of data processing equipment and services. ANSI membership is comprised of people form professional societies, industry associations, governmental and regulatory bodies, and consumer goods.

5. Electronics Industry Association (EIA)
EIA is a non-profit U.S. trade association that establishes and recommends industrial standards. EIA activities include standards development, increasing public awareness, and lobbying and it is responsible for developing the RS (recommended standard) series of standards for data and communications.

6. Telecommunications Industry Association (TIA)
TIA is the leading trade association in the communications and information technology industry. It facilitates business development opportunities through market development, trade promotion, trade shows, and standards development. It represents manufacturers of communications and information technology products and also facilitates the convergence of new communications networks.

7. Internet Architecture Board (IAB)
IAB earlier known as Internet Activities Board is a committee created by ARPA (Advanced Research Projects Agency) so as to analyze the activities of ARPANET whose purpose is to accelerate the advancement of technologies useful for U.S military. IAB is a technical advisory group of the Internet Society and its responsibilities are:

I. Oversees the architecture protocols and procedures used by the Internet.

II. Manages the processes used to create Internet Standards and also serves as an appeal board for complaints regarding improper execution of standardization process.

III. Responsible for administration of the various Internet assigned numbers

IV. Acts as a representative for Internet Society interest in liaison relationships with other organizations.

V. Acts as a source of advice and guidance to the board of trustees and officers of Internet Society concerning various aspects of internet and its technologies.

Line Configuration:

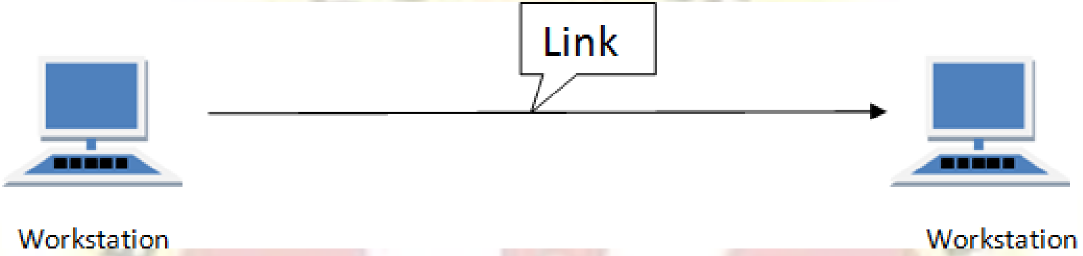
A network is two or more devices connected through a link. A link is a communication pathway that transfer data from one device to another. Devices can be a computer, printer or any other device that is capable to send and receive data. For visualization purpose, imagine any link as a line drawn between 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:

1. **Point-to-Point Connection**
2. **Multipoint Connection**

Point-to-Point Connection :

1. A point-to-point connection provides a dedicated link between two devices.
2. The entire capacity of the link is reserved for transmission between those two devices.
3. Most point-to-point connections use a actual length of wire or cable to connect the two end, but other options such as microwave or satellite links are also possible.
4. Point to point network topology is considered to be one of the easiest and most conventional network
topologies.
5. It is also the simplest to establish and understand.

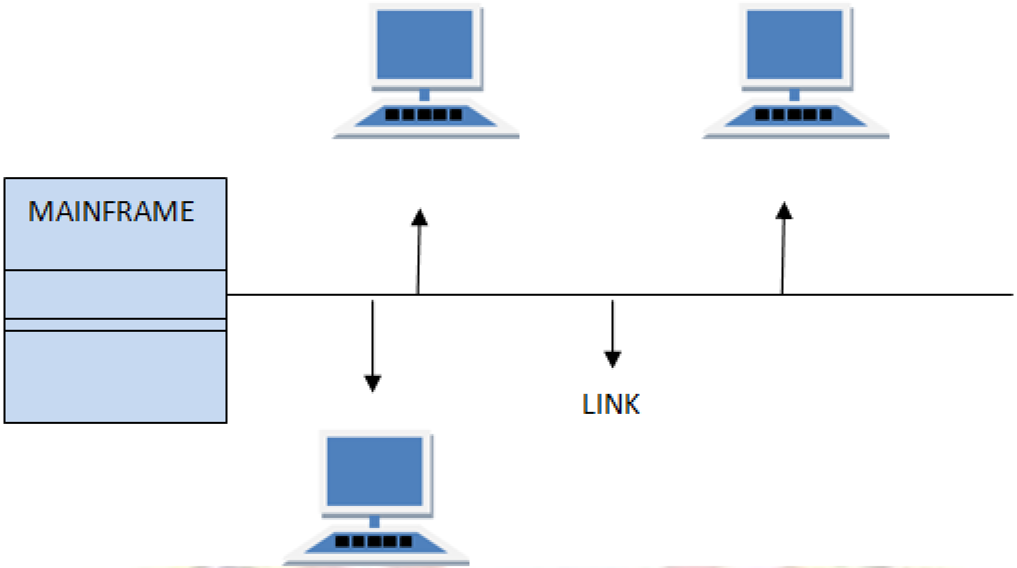


MultiPoint Connection

It is also called Multidrop configuration. In this connection two or more devices share a single link.

There are two kinds of Multipoint Connections :

- If the links are used simultaneously between many devices, then it is spatially shared line configuration.
- If user takes turns while using the link, then it is time shared (temporal) line configuration

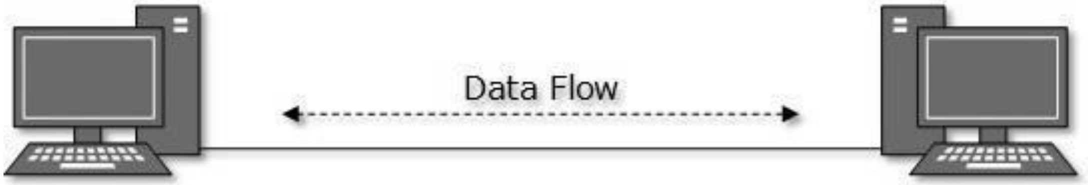


Topology:

A Network Topology is the arrangement with which computer systems or network devices are connected to each other. Topologies may define both physical and logical aspect of the network. Both logical and physical topologies could be same or different in a same network.

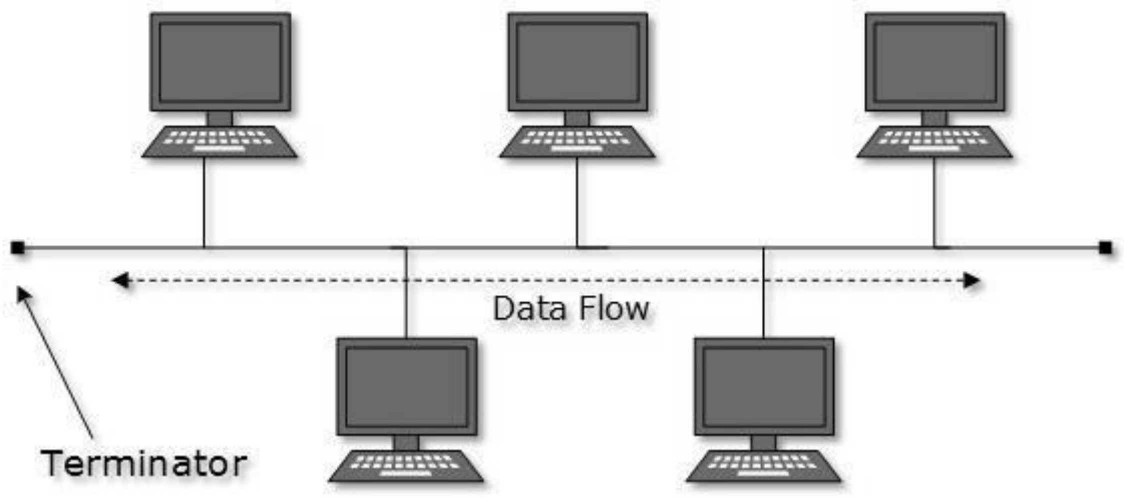
Point-to-Point

Point-to-point networks contains exactly two hosts such as computer, switches, routers, or servers connected back to back using a single piece of cable. Often, the receiving end of one host is connected to sending end of the other and vice versa.
If the hosts are connected point-to-point logically, then may have multiple intermediate devices. But the end hosts are unaware of underlying network and see each other as if they are connected directly.



Bus Topology

In case of Bus topology, all devices share single communication line or cable. Bus topology may have problem while multiple hosts sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue. It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning.



Both ends of the shared channel have line terminator. The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.

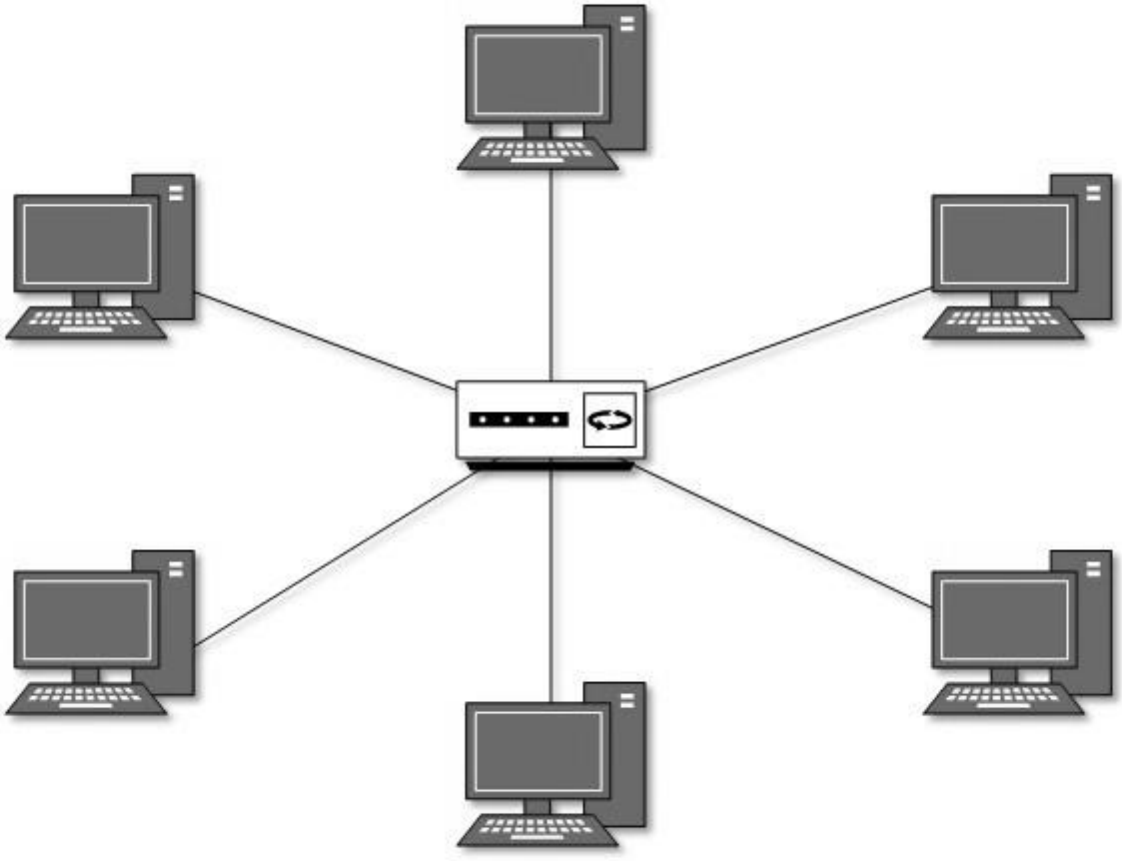
Star Topology

All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub. The hub device can be any of the following:

□ Layer-1 device such as hub or repeater

□ Layer-2 device such as switch or bridge

_ Layer-3 device such as router or gateway



As in Bus topology, hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails. Every communication between hosts takes place through only the hub. Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.

Ring Topology

In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host in the existing structure, the administrator may need only one more extra cable.

[

Failure of any host results in failure of the whole ring. Thus, every connection in the ring is a point of failure. There are methods which employ one more backup ring.

Mesh Topology

In this type of topology, a host is connected to one or multiple hosts. This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection with few hosts only.

Hosts in Mesh topology also work as relay for other hosts which do not have direct point-to-point links. Mesh technology comes into two types:

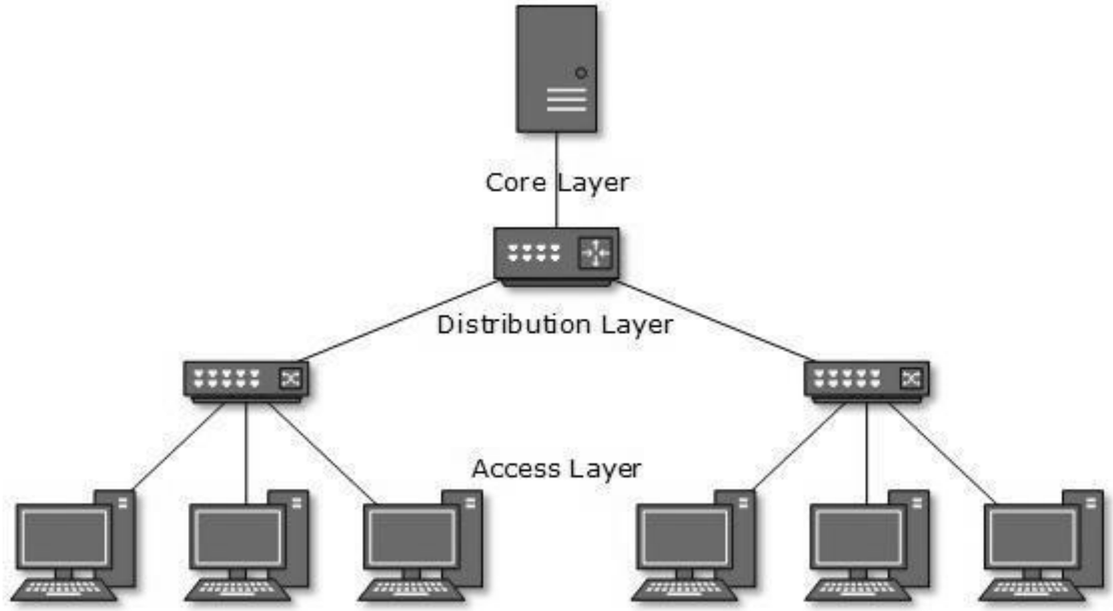
 Full Mesh: All hosts have a point-to-point connection to every other host in the network. Thus for every new host n(n-1)/2 connections are required. It provides the most reliable network structure among all network topologies.

 Partially Mesh: Not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrarily fashion. This topology exists where we need to provide reliability to some hosts out of all.

Tree Topology

Also known as Hierarchical Topology, this is the most common form of network topology in use presently. This topology imitates as extended Star topology and inherits properties of Bus topology.

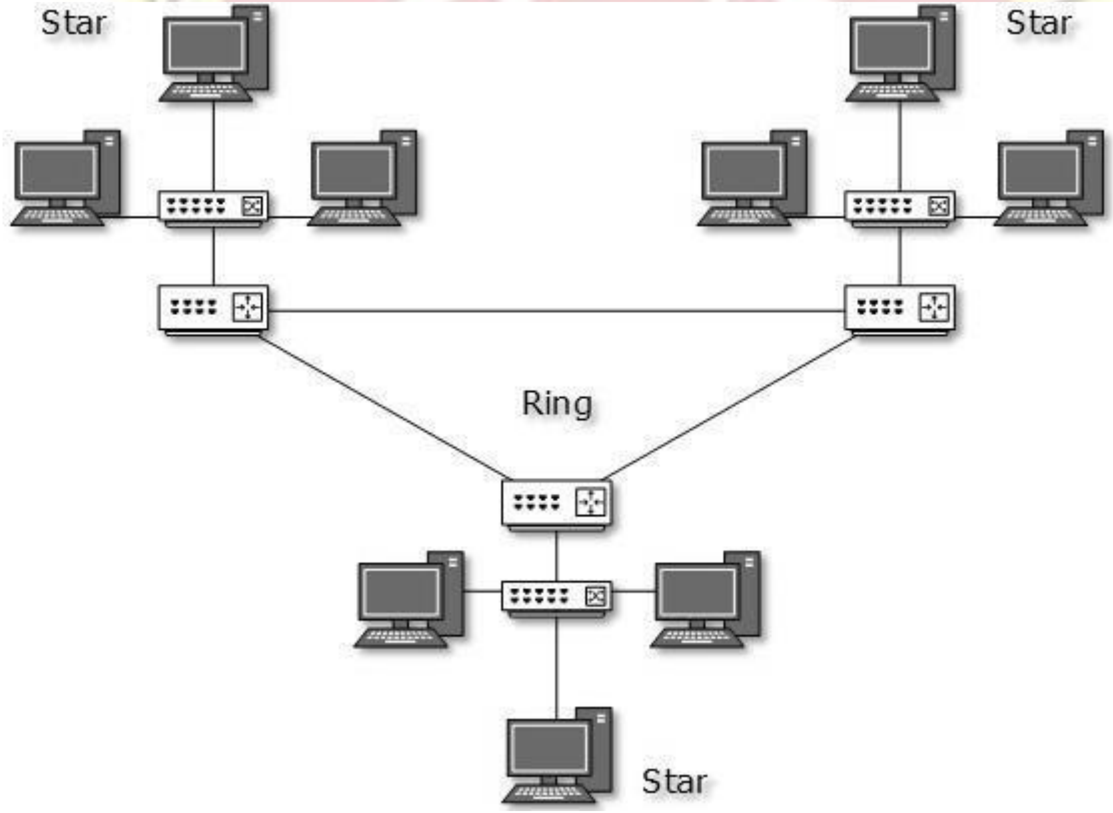
This topology divides the network into multiple levels/layers of network. Mainly in LANs, a network is bifurcated into three types of network devices. The lowermost is access-layer where computers are attached. The middle layer is known as distribution layer, which works as mediator between upper layer and lower layer. The highest layer is known as core layer, and is central point of the network, i.e. root of the tree from which all nodes fork.



All neighboring hosts have point-to-point connection between them. Similar to the Bus topology, if the root goes down, then the entire network suffers even though it is not the single point of failure. Every connection serves as point of failure, failing of which divides the network into unreachable segment.

Hybrid Topology

A network structure whose design contains more than one topology is said to be hybrid topology. Hybrid topology inherits merits and demerits of all the incorporating topologies.



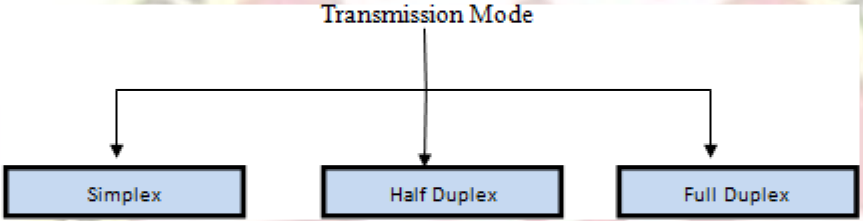
The above picture represents an arbitrarily hybrid topology. The combining topologies may contain attributes of Star, Ring, Bus, and Daisy-chain topologies. Most WANs are connected by means of Dual-

Ring topology and networks connected to them are mostly Star topology networks. Internet is the best example of largest Hybrid topology.

Transmission mode:

Transmission mode refers to the mechanism of transferring of data between two devices connected over a network. It is also called **Communication Mode**. These modes direct the direction of flow of information. There are three types of transmission modes. They are:

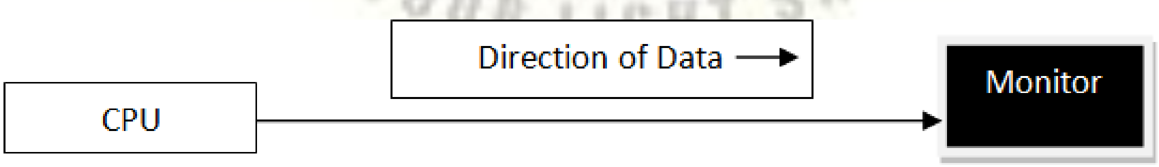
1. Simplex Mode
2. Half duplex Mode
3. Full duplex Mode



SIMPLEX Mode

In this type of transmission mode, data can be sent only in one direction i.e. communication is unidirectional. We cannot send a message back to the sender. Unidirectional communication is done in Simplex Systems where we just need to send a command/signal, and do not expect any response back.

Examples of simplex Mode are loudspeakers, television broadcasting, television and remote, keyboard and monitor etc.

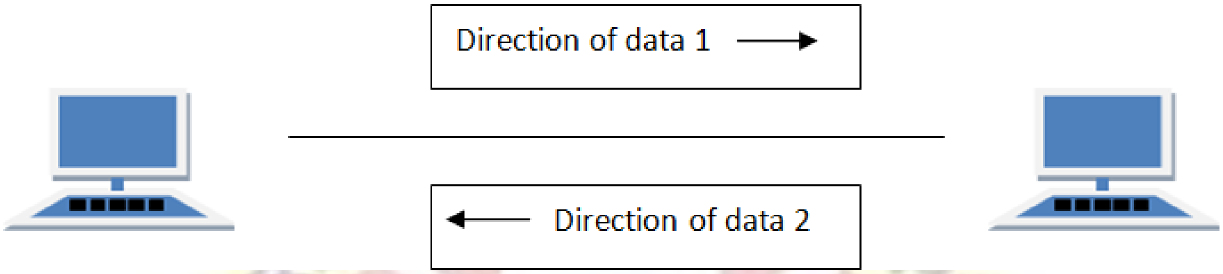


HALF DUPLEX Mode

Half-duplex data transmission means that data can be transmitted in both directions on a signal carrier, but not at the same time.

For example, on a local area network using a technology that has half-duplex transmission, one workstation can send data on the line and then immediately receive data on the line from the same direction in which data was just transmitted. Hence half-duplex transmission implies a bidirectional line (one that can carry data in both directions) but data can be sent in only one direction at a time.

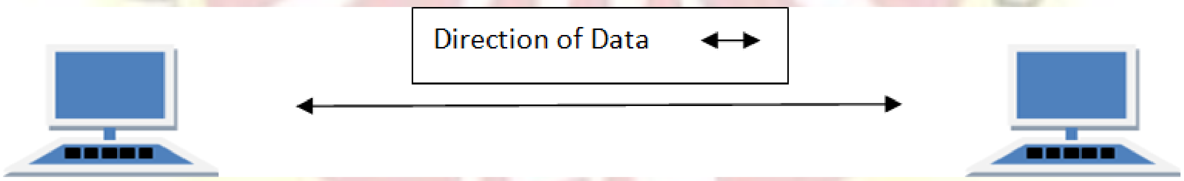
Example of half duplex is a walkie- talkie in which message is sent one at a time but messages are sent in both the directions.



FULL DUPLEX Mode

In full duplex system we can send data in both the directions as it is bidirectional at the same time in other words, data can be sent in both directions simultaneously.

Example of Full Duplex is a Telephone Network in which there is communication between two persons by a telephone line, using which both can talk and listen at the same time.



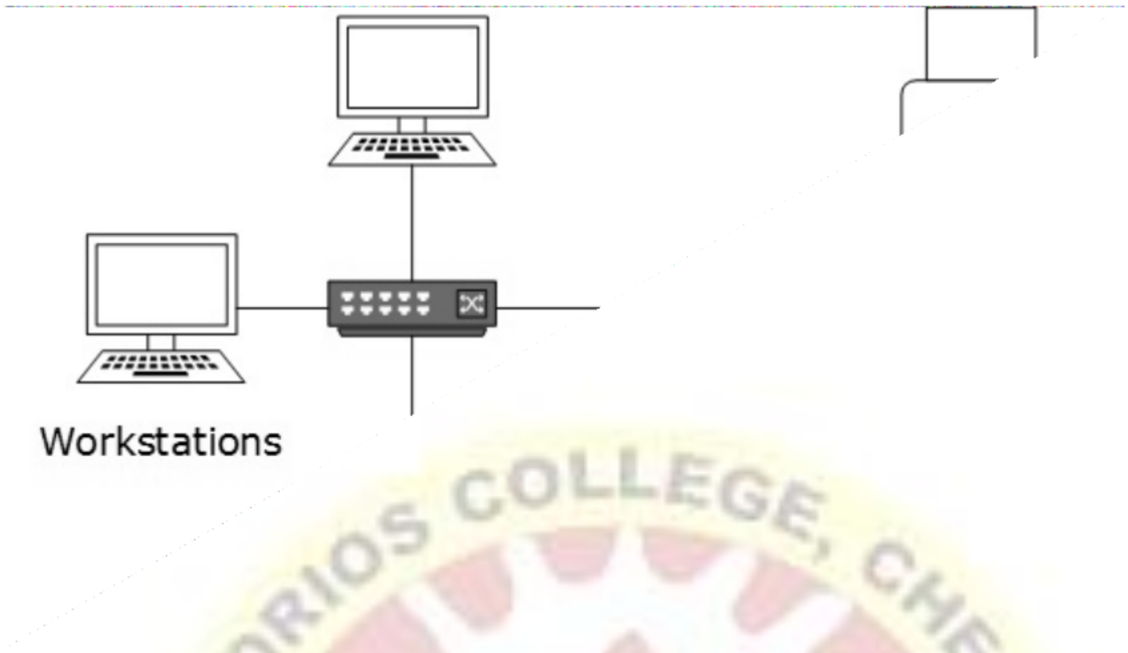
Classification of Network:

Generally, networks are distinguished based on their geographical span. A network can be as small as distance between your mobile phone and its Bluetooth headphone and as large as the internet itself, covering the whole geographical world.

Local Area Network

A computer network spanned inside a building and operated under single administrative system is generally termed as Local Area Network (LAN). Usually, LAN covers an organization offices, schools, colleges or universities. Number of systems connected in LAN may vary from as least as two to as much as 16 million.

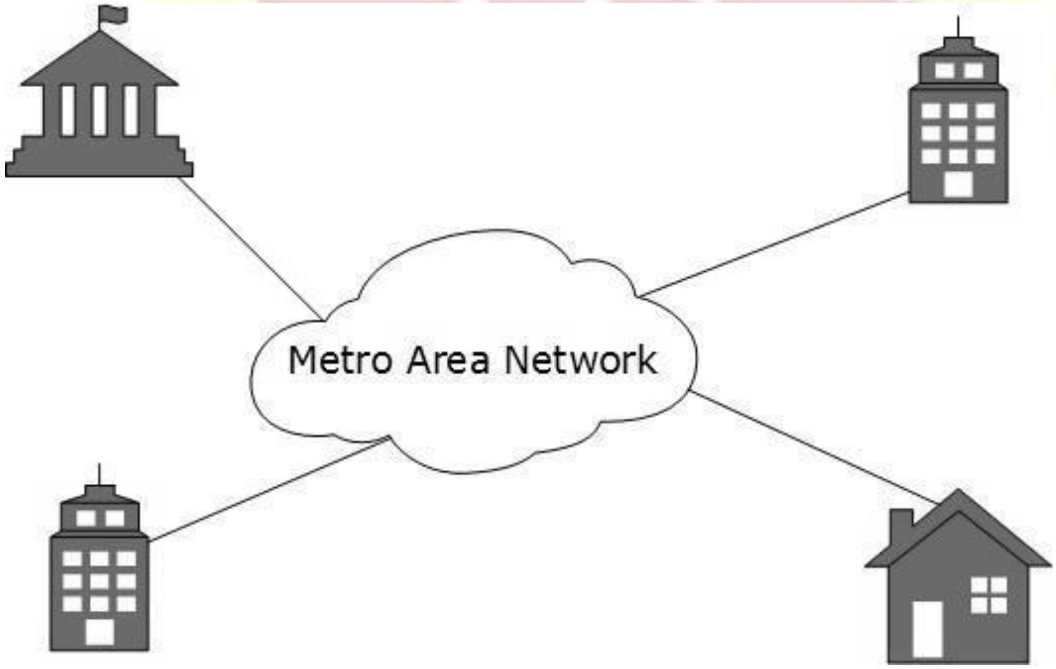
LAN provides a useful way of sharing the resources between end users. The resources such as printers, file servers, scanners, and internet are easily sharable among computers.



LANs are composed of inexpensive networking and routing equipment. It may contains local servers serving file storage and other locally shared applications. It mostly operates on private IP addresses and does not involve heavy routing. LAN works under its own local domain and controlled centrally.
LAN uses either Ethernet or Token-ring technology. Ethernet is most widely employed LAN technology and uses Star topology, while Token-ring is rarely seen.
LAN can be wired, wireless, or in both forms at once.

Metropolitan Area Network

The Metropolitan Area Network (MAN) generally expands throughout a city such as cable TV network. It can be in the form of Ethernet, Token-ring, ATM, or Fiber Distributed Data Interface (FDDI).
Metro Ethernet is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks. For example, MAN can help an organization to connect all of its offices in a city.



Backbone of MAN is high-capacity and high-speed fiber optics. MAN works in between Local Area Network and Wide Area Network. MAN provides uplink for LANs to WANs or internet.

Wide Area Network

As the name suggests, the Wide Area Network (WAN) covers a wide area which may span across provinces and even a whole country. Generally, telecommunication networks are Wide Area Network. These networks provide connectivity to MANs and LANs. Since they are equipped with very high speed backbone, WANs use very expensive network equipment.

WAN may use advanced technologies such as Asynchronous Transfer Mode (ATM), Frame Relay, and Synchronous Optical Network (SONET). WAN may be managed by multiple administration.

Internetwork

A network of networks is called an internetwork, or simply the internet. It is the largest network in existence on this planet. The internet hugely connects all WANs and it can have connection to LANs and Home networks. Internet uses TCP/IP protocol suite and uses IP as its addressing protocol. Present day, Internet is widely implemented using IPv4. Because of shortage of address spaces, it is gradually migrating from IPv4 to IPv6.

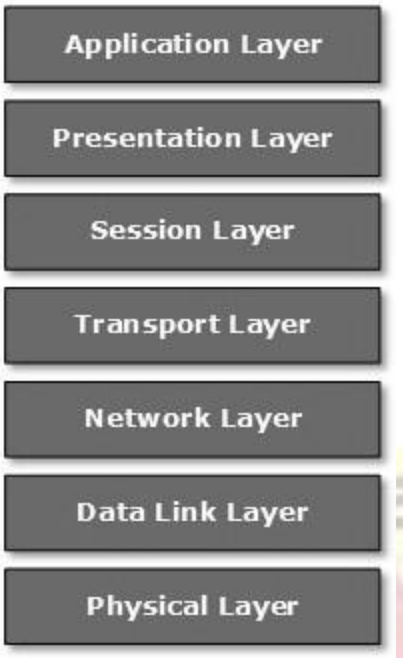
Internet enables its users to share and access enormous amount of information worldwide. It uses WWW, FTP, email services, audio, and video streaming etc. At huge level, internet works on Client-Server model.

Internet uses very high speed backbone of fiber optics. To inter-connect various continents, fibers are laid under sea known to us as submarine communication cable.

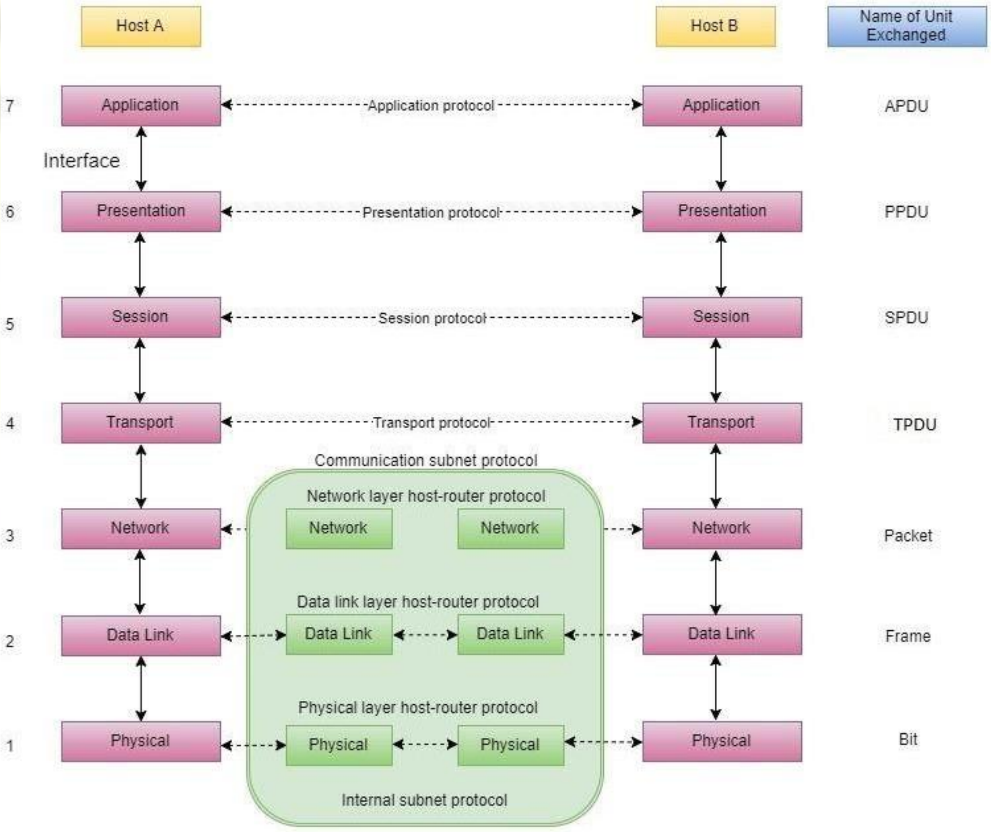
Internet is widely deployed on World Wide Web services using HTML linked pages and is accessible by client software known as Web Browsers. When a user requests a page using some web browser located on some Web Server anywhere in the world, the Web Server responds with the proper HTML page. The communication delay is very low.

OSI Model:

International standard organization (ISO) established a committee in 1977 to develop architecture for computer communication and the OSI model is the result of this effort. In 1984, the Open Systems Interconnection (OSI) reference model was approved as an international standard for communications architecture. The term "*open*" denotes the ability to connect any two systems which conform to the reference model and associated standards. The OSI model describes how information or data makes its way from applicationprogrammes (such as spreadsheets) through a network medium (such as wire) to another application programme located on another network. The OSI reference model divides the problem of moving information between computers over a network medium into **SEVEN** smaller and more manageable problems. The seven layers are:



Layers of OSI Model:



Feature of OSI Model

1. Big picture of communication over network is understandable through this OSI model.

2. We see how hardware and software work together.
3. We can understand new technologies as they are developed.
4. Troubleshooting is easier by separate networks.
5. Can be used to compare basic functional relationships on different networks.

Unit II

Parallel and Serial Transmission:

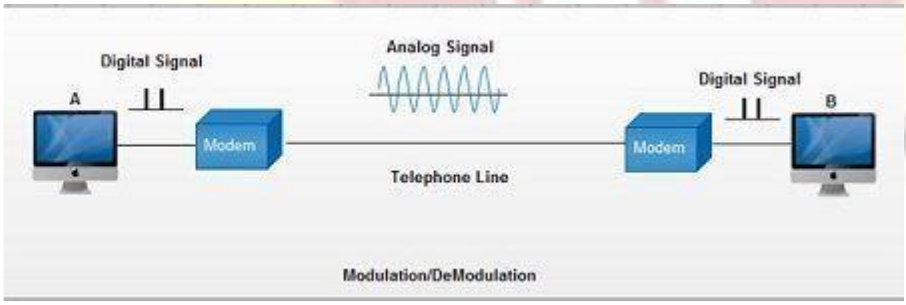
When data is sent or received using serial data transmission, the data bits are organized in a specific order, since they can only be sent one after another. The order of the data bits is important as it dictates how the transmission is organized when it is received. It is viewed as a reliable data transmission method because a data bit is only sent if the previous data bit has already been received.

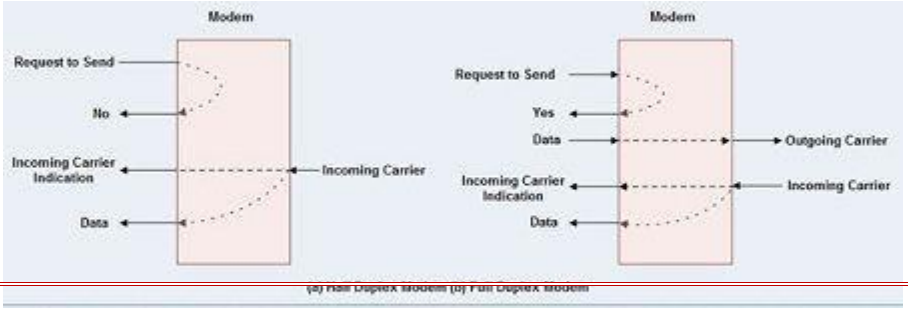
Modems:

Modem is abbreviation for Modulator – De-modulator. Modems are used for data transfer from one computer network to another computer network through telephone lines. The computer network works in digital mode, while analog technology is used for carrying massages across phone lines.

Modulator converts information from **digital mode to analog mode** at the transmitting end and de-modulator converts the same from **analog to digital at receiving end**. The process of converting analog signals of one computer network into digital signals of another computer network so they can be processed by a receiving computer is **referred to as digitizing.**

When an analog facility is used for data communication between two digital devices called Data Terminal Equipment (DTE), modems are used at each end. DTE can be a terminal or a computer.



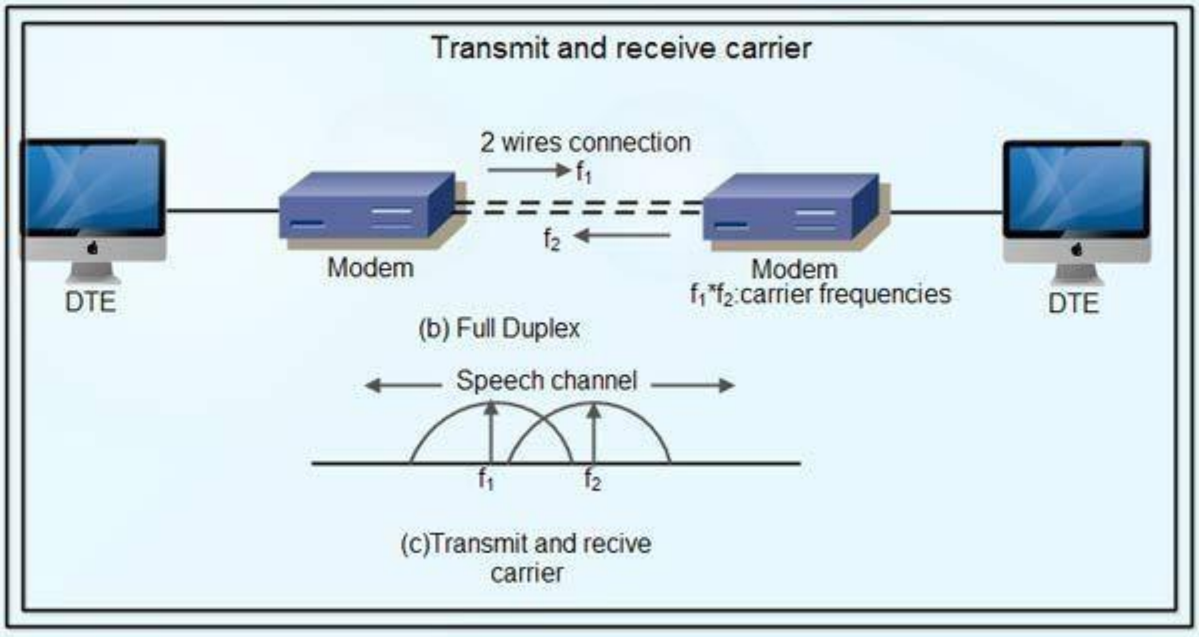


Full duplex

- A **full duplex modem** allows simultaneous transmission in both directions.
- Therefore, there are two carriers on the line, one outgoing and the other incoming. **Wire and 4-wire Modems**
- The line interface of the modem can have a 2-wire or a 4-wire connection to transmission medium. 4-wire Modem
- In a 4-wire connection, one pair of wires is used for the outgoing carrier and the other pair is used for incoming carrier.
- Full duplex and half duplex modes of data transmission are possible on a 4- wire connection.
- As the physical transmission path for each direction is separate, the same carrier frequency can be used for both the directions.

2-wire Modem

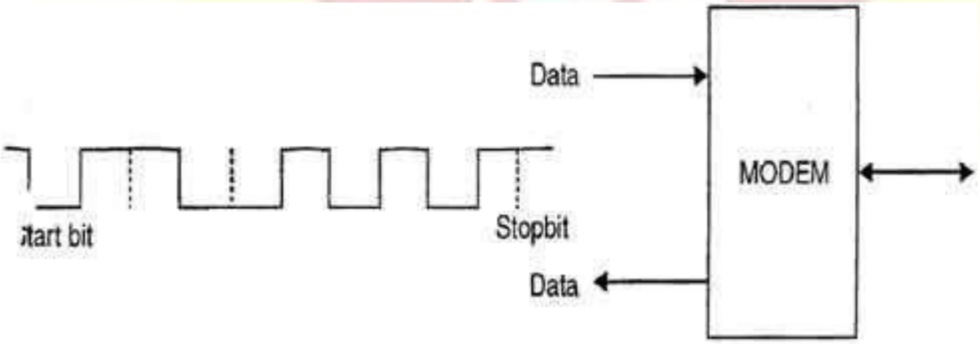
- 2-wire modems use the same pair of wires for outgoing and incoming carriers.
- A leased 2-wireconrlection is usually cheaper than a 4-wire connection as only one pair of wires is extended to the subscriber’s premises.
- The data connection established through telephone exchange is also a 2-wire connection.
- In 2-wire modems, half duplex mode of transmission that uses the same frequency for the incoming and outgoing carriers can be easily implemented.
- For full duplex mode of operation, it is necessary to have two transmission channels, one for transmit direction and the other for receive direction.
- This is achieved by frequency division multiplexing of two different carrier frequencies. These carriers are placed within the bandwidth of the speech channel.


Transmit and receive carrier
2 wires connection
f_1
f_2
DTE
Modem
Modem
f_1*f_2:carrier frequencies
DTE
(b) Full Duplex
Speech channel
f_1
f_2
(c)Transmit and recive carrier

Asynchronous

Modem

- Asynchronous modems can handle data bytes with start and stop bits.
- There is no separate timing signal or clock between the modem and the DTE.
- The internal timing pulses are synchronized repeatedly to the leading edge of the start pulse



Asynchronous modem

Modulation techniques used for Modem:

The basic modulation techniques used by a modem to convert digital data to analog signals are :

- Amplitude shift keying (ASK).
- Frequency shift keying (FSK).
- Phase shift keying (PSK).
- Differential PSK (DPSK).

These techniques are known as the binary continuous wave (CW) modulation.

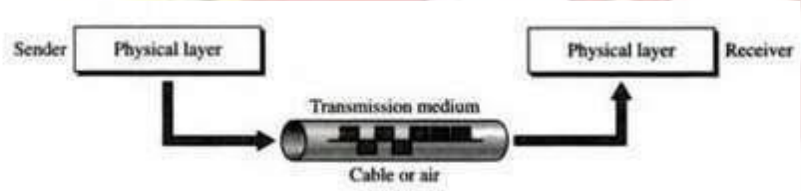
- Modems are always used in pairs. Any system whether simplex, half duplex or full duplex requires a modem at the transmitting as well as the receiving end.
- Thus a modem acts as the electronic bridge between two worlds – the world of purely digital signals and the established analog world.

Guided Media:

Transmission media is nothing but the physical layer or medium. The physical layer is to transport bits from one machine to another. Various physical media can be used for the actual transmission. Media are roughly grouped into TWO types.

✓ Guided media, such as copper wire and fiber optics

✓ Unguided media, such as terrestrial wireless, satellite, and lasers through the air.



Communication

1.7.1 Guided Media

There are five types in guided media

1) Magnetic Media
2) Twisted Pairs
3) Coaxial Cable
4) Power Lines
5) Fiber Optics

1. Magnetic Media:

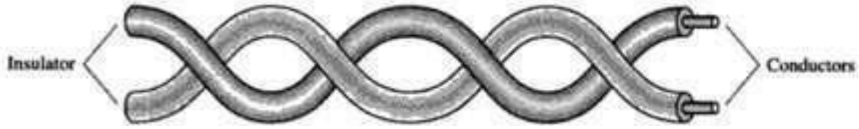
The most common ways to transport data from one computer to another is to write them onto magnetic tape or removable media. Physically transport the tape or disks to the destination machine, and read them back in again. A simple calculation will make this point clear.

An industry-standard Ultrium tape can hold 800 gigabytes. A box 60 × 60 × 60 cm can hold about 1000 of these tapes, for a total capacity of 800 terabytes, or 6400 terabits (6.4 petabits). A box of tapes can be delivered anywhere in the United States in 24 hours by Federal Express and other companies.

It is more cost effective, especially for applications in which high bandwidth or cost per bit transported. It has delay characteristics are poor.

2. Twisted Pairs

Its uses metallic (Copper) conductors that accept and transport signals in the form of electric current.



Twisted pair cable
A twisted pair consists of two insulated copper wires, typically about 1 mm thick. The wires are twisted together in a helical form. A twisted pair consists of two conductors(normally copper), each with its own plastic insulation, twisted together. One of these wires is used to carry signals to the receiver, and the other is used only as 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. This results in a difference at the receiver. Twisted Pair is of two types:

– **Unshielded Twisted Pair (UTP)**
– **Shielded Twisted Pair (STP)**

a). Unshielded Twisted Pair Cable

It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own colour

plastic insulator. Identification is the reason behind coloured plastic insulation. UTP cables consist of 2 or 4 pairs of twisted cable.

• Advantages of Unshielded Twisted Pair Cable

✓ Installation is easy
✓ Flexible
✓ Cheap
✓ It has high speed capacity,
✓ 100 meter limit
✓ Higher grades of UTP are used in LAN technologies like Ethernet.

• **Disadvantages of Unshielded Twisted Pair Cable**

✓ Bandwidth is low when compared with Coaxial Cable
✓ Provides less protection from interference.

b). Shielded Twisted Pair Cable

This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by metal casing

Advantages of Shielded Twisted Pair Cable

✓ Easy to install
✓ Performance is adequate
✓ Can be used for Analog or Digital transmission
✓ Increases the signalling rate
✓ Higher capacity than unshielded twisted pair

✓ Eliminates crosstalk

• **Disadvantages of Shielded Twisted Pair Cable**

✓ Difficult to manufacture

✓ Heavy

• **Applications of Shielded Twisted Pair Cable**

In telephone lines to provide voice and data channels. The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables.

Local Area Network, such as 10Base-T and 100Base-T, also use twisted-pair cables.

3. Coaxial Cable:

Another common transmission medium is the **coaxial cable.** Two kinds of coaxial cable are widely used. One kind, 50-ohm cable, is commonly used when it is intended for digital transmission from the start. The other kind, 75-ohm cable, is commonly used for analog transmission and cable television.

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

coaxial cable

The construction and shielding of the coaxial cable give it a good combination of high bandwidth and excellent noise immunity.

• **Advantagesof Coaxial Cable**

✓ Bandwidth is high

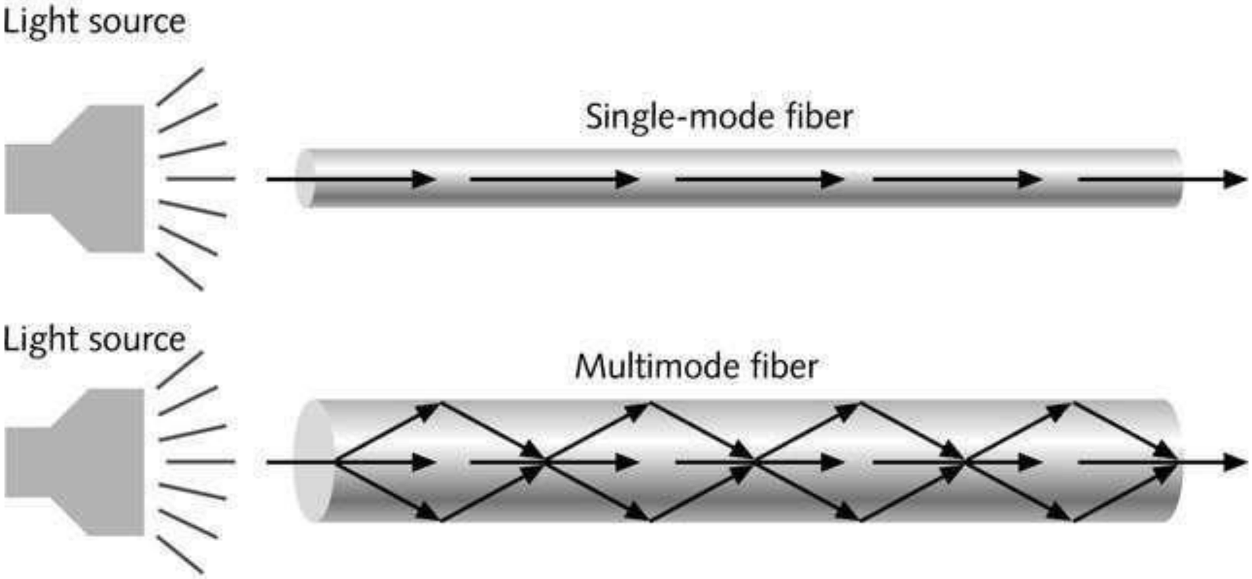
✓ Used in long distance telephone lines.

✓ Transmits digital signals at a very high rate of 10Mbps.

5. Fiber Optic Cable

A fibre-optic cable is made of glass or plastic and transmits signals in the form of light.

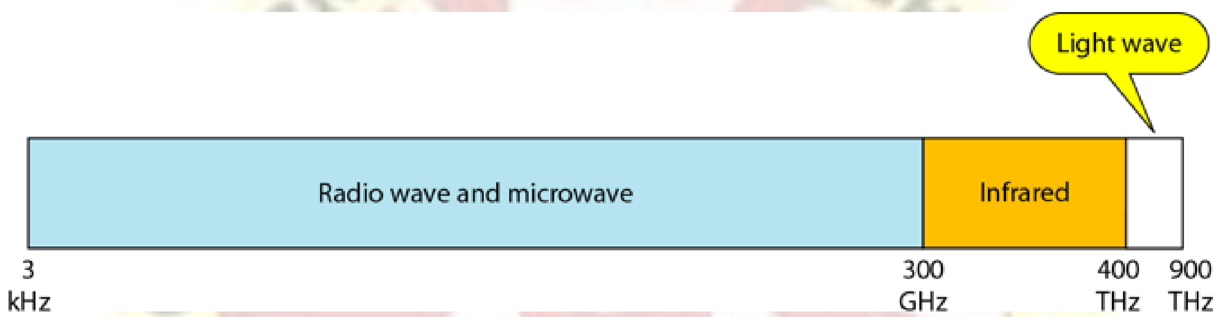
For better understanding we first need to explore several aspects of the **nature of light**. Light travels in a straight line as long as it is mobbing through a single uniform substance. If ray of light travelling through one substance suddenly enters another substance (of a different density), the ray changes direction. The below figure shows how a ray of light changes direction when going from a more dense to a less dense substance.

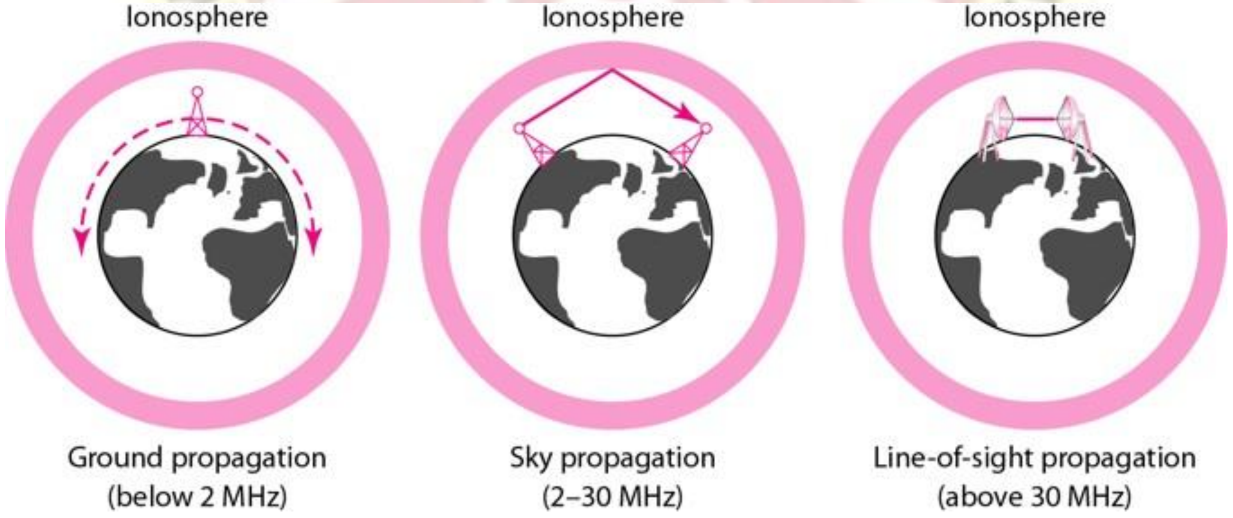


Unguided Media:

Unguided medium 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.

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




Ionosphere
Ionosphere
Ionosphere
Ground propagation (below 2 MHz)
Sky propagation (2–30 MHz)
Line-of-sight propagation (above 30 MHz)

Propagation Modes

- **Ground Propagation:** In this, 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.

- **Sky Propagation:** In this, 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.
- **Line-of-sight Propagation:** in this type, very high-frequency signals are transmitted in straight lines directly from antenna to antenna.

We can divide wireless transmission into three broad groups:

1. Radio waves
2. Micro waves
3. Infrared waves

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 send waves that can be received by any receiving antenna. The omnidirectional property has disadvantage, too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signal suing the same frequency or band.

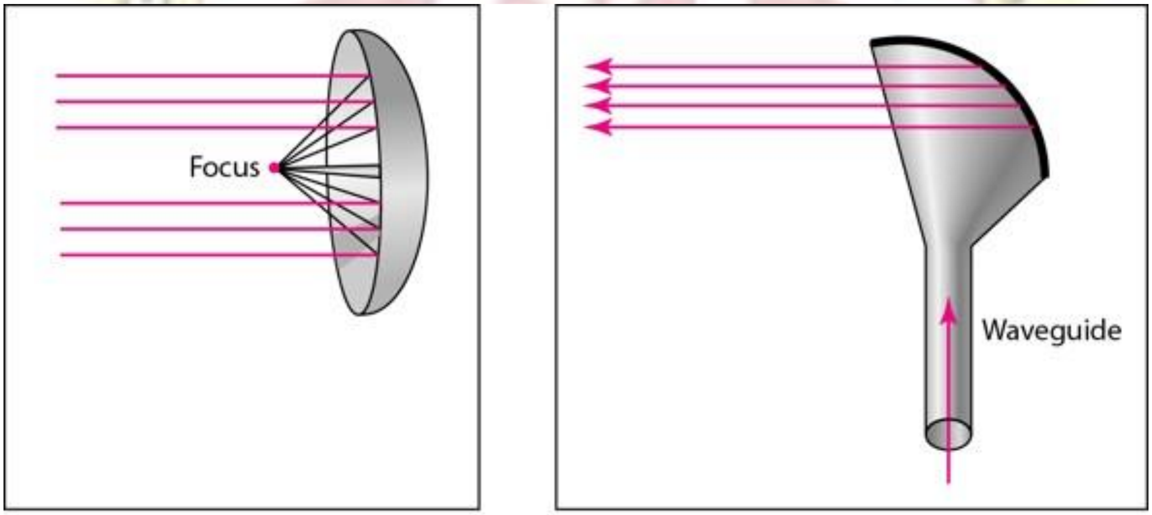
Radio waves, particularly with those of low and medium frequencies, can penetrate walls. This characteristic can be both an advantage and a disadvantage. It is an advantage because, an AM radio can receive signals inside a building. It is a disadvantage because we cannot isolate a communication to just inside or outside a building.

Micro Waves

Electromagnetic waves having frequencies between 1 and 300 GHz are called micro waves. Micro waves are unidirectional. When an antenna transmits microwaves, 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 microwaves propagation:

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

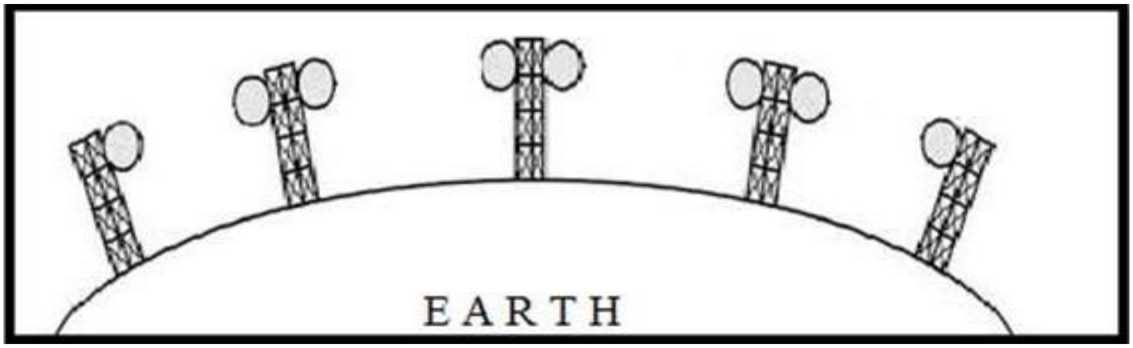


a. Dish antenna

b. Horn antenna

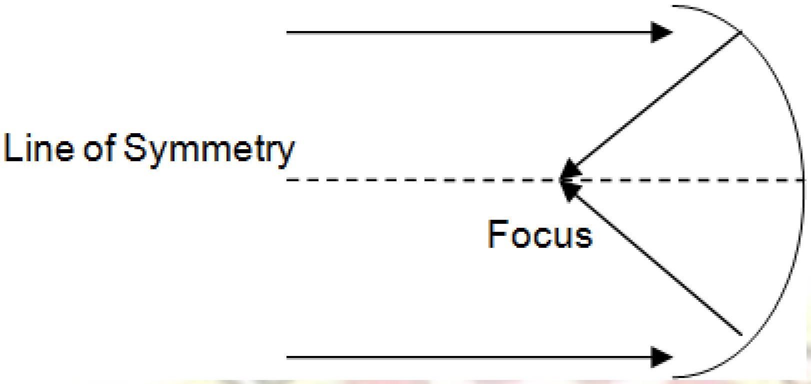
Terrestrial Microwave

For increasing the distance served by terrestrial microwave, repeaters can be installed with each antenna .The signal received by an antenna can be converted into transmittable form and relayed to next antenna as shown in below figure. It is an example of telephone systems all over the world


EARTH

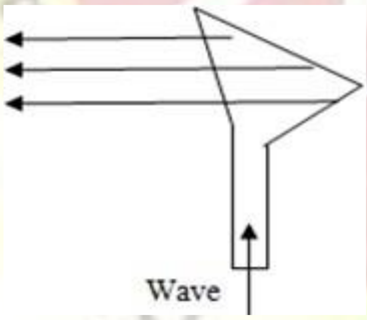
1. Parabolic Dish Antenna

In this every line parallel to the line of symmetry reflects off the curve at angles in a way that they intersect at a common point called focus. This antenna is based on geometry of parabola.



2. Horn Antenna

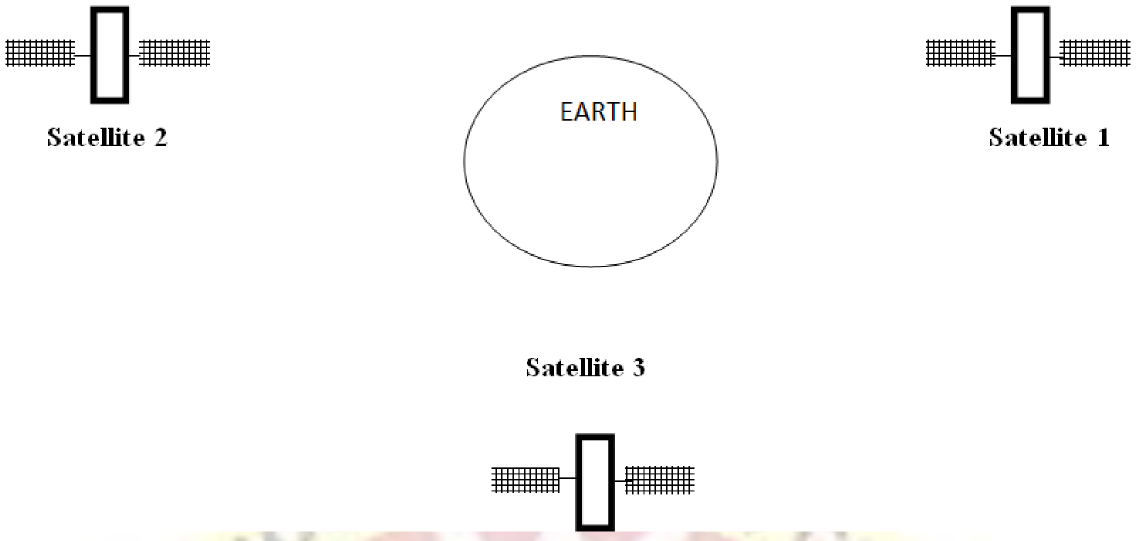
It is a like gigantic scoop. The outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by curved head.



Satellite Microwave

This is a microwave relay station which is placed in outer space. The satellites are launched either by rockets or space shuttles carry them.

These are positioned 36000 Km above the equator with an orbit speed that exactly matches the rotation speed of the earth. As the satellite is positioned in a geo-synchronous orbit, it is stationery relative to earth and always stays over the same point on the ground. This is usually done to allow ground stations to aim antenna at a fixed point in the sky.



Features of Satellite Microwave

- Bandwidth capacity depends on the frequency used.
- Satellite microwave deployment for orbiting satellite is difficult.

Advantages of Satellite Microwave

- Transmitting station can receive back its own transmission and check whether the satellite has transmitted information correctly.
- A single microwave relay station which is visible from any point.

Disadvantages of Satellite Microwave

- Satellite manufacturing cost is very high
- Cost of launching satellite is very expensive

Types of Error:

There are many reasons such as noise, cross-talk etc., which may help data to get corrupted during transmission. The upper layers work on some generalized view of network architecture and are not aware of actual hardware data processing. Hence, the upper layers expect error-free transmission between the systems. Most of the applications would not function expectedly if they receive erroneous data. Applications such as voice and video may not be that affected and with some errors they may still function well.

Data-link layer uses some error control mechanism to ensure that frames (data bit streams) are transmitted with certain level of accuracy. But to understand how errors is controlled, it is essential to know what types of errors may occur.

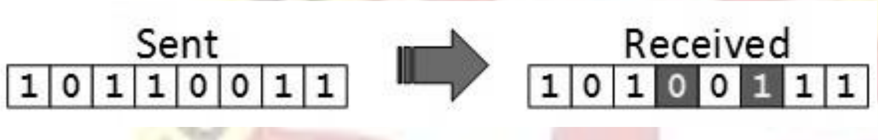
Types of Errors

There may be three types of errors:

Single bit error

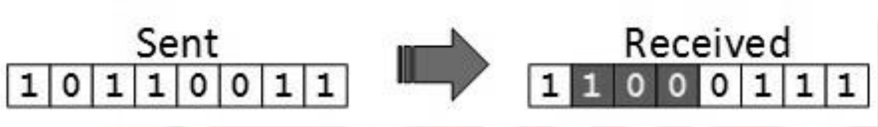
In a frame, there is only one bit, anywhere though, which is corrupt.

Multiple bits error



Frame is received with more than one bits in corrupted state.

Burst error



Frame contains more than1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

☐ Error detection

☐ Error correction

Error Detection

Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver end fails, the bits are considered corrupted.

Error Correction

In the digital world, error correction can be done in two ways:

Backward Error Correction

When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.

Forward Error Correction

When the receiver detects some error in the data received, it executes error- correcting code, which helps it to auto-recover and to correct some kinds of errors. The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive. For example, fiber optics. But in case of wireless transmission retransmitting may cost too much. In the latter case, ForwardError Correction is used.

To correct the error in data frame, the receiver must know exactly which bit in the frame is corrupted. To locate the bit in error, redundant bits are used as parity bits for error detection. Forexample, we take ASCII words (7 bits data), then there could be 8 kind of information we need: first seven bits to tell us which bit is in error and one more bit to tell that there is no error.

For m data bits, r redundant bits are used. r bits can provide 2r combinations of information. Inm+r bit codeword, there is possibility that the r bits themselves may get corrupted. So the number of r bits used must inform about m+r bit locations plus no-error information, i.e. m+r+1.

$2^r >= m+r+1$.

Unit III

Ethernet

Ethernet is a widely deployed LAN technology. This technology was invented by Bob Metcalfe and D.R. Boggs in the year 1970. It was standardized in IEEE 802.3 in 1980. Ethernet shares media. Network which uses shared media has high probability of data collision. Ethernet uses Carrier Sense Multi Access/Collision Detection (CSMA/CD) technology to detect collisions. On the occurrence of collision in Ethernet, all its hosts roll back, wait for some random amount of time, and then re-transmit the data. Ethernet connector is network interface card equipped with 48-bits MAC address. This helps other Ethernet devices to identify and communicate with remote devicesin Ethernet.

Traditional Ethernet uses 10BASE-T specifications. The number 10 depicts 10MBPS speed, BASE stands for baseband, and T stands for Thick Ethernet. 10BASE-T Ethernet provides transmission speed up to 10MBPS and uses coaxial cable or Cat-5twisted pair cable with RJ-5 connector. Ethernet follows Star topology with segmentlength up to 100 meters. All devices are connected to a hub/switch in a star fashion.

Ethernet Cabling

The name "Ethernet" refers to the cable (the ether). Four types of cabling are commonly Used.

- **10Base5** is called thick Ethernet. Connections use vampire taps. The first number,10, is the speed in Mbps. The word "Base" (or sometimes "BASE") to indicate baseband transmission and can support segments of up to 500 meters (for coaxial cable).
- **10Base2** is called thin Ethernet. Connections are done using T junctions. This is cheaper and easier to install. But it can run for only 185 meters per segment, eachof which can handle only 30 machines.

Detecting cable breaks, excessive length, bad taps, or loose connectors can be a major problem with both media. For this reason, techniques have been developed to track them o, it down. Basically, a pulse of known shape is injected into the cable. If the pulse hits an obstacle or the end of the cable, an echo will be generated and sent back. By carefully timing the interval between sending the pulse and receiving the echis possible to localize the origin of the echo.

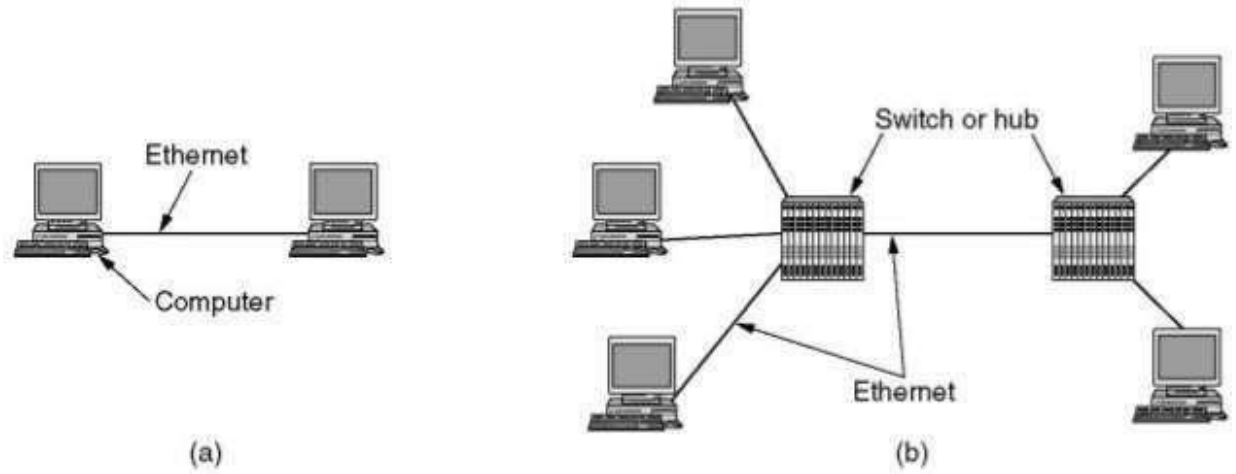
Fast-Ethernet

To encompass need of fast emerging software and hardware technologies, Ethernet extends itself as Fast-Ethernet. It can run on UTP, Optical Fiber, and wirelessly too. It can provide speed up to 100MBPS. This standard is named as 100BASE-T in IEEE 803.2 using Cat-5 twisted pair cable. It uses CSMA/CD technique for wired media sharing among the Ethernet hosts and CSMA/CA (CA stands for Collision Avoidance) technique for wireless Ethernet LAN.

Fast Ethernet on fiber is defined under 100BASE-FX standard which provides speed up to 100MBPS on fiber. Ethernet over fiber can be extended up to 100 meters in half-duplex mode and can reach maximum of 2000 meters in full-duplex over multimode fibers.

Giga-Ethernet

After being introduced in 1995, Fast-Ethernet retained its high speed status only for three years till Giga-Ethernet introduced. Giga-Ethernet provides speed up to 1000 mbits/seconds. IEEE802.3ab standardizes Giga-Ethernet over UTP using Cat-5, Cat-5e and Cat-6 cables. IEEE802.3ah defines Giga-Ethernet over Fiber.



Virtual LAN

LAN uses Ethernet which in turn works on shared media. Shared media in Ethernet create one single Broadcast domain and one single Collision domain. Introduction of switches to Ethernet has removed single collision domain issue and each device connected to switch works in its separate collision domain. But even Switches cannot divide a network into separate Broadcast domains.

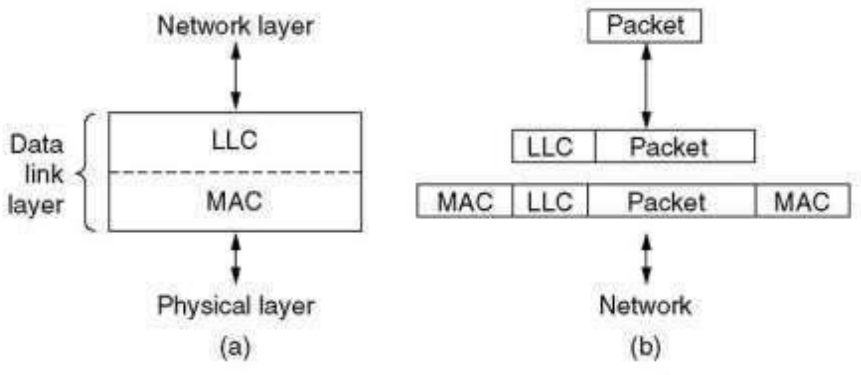
Virtual LAN is a solution to divide a single Broadcast domain into multiple Broadcast domains. Host in one VLAN cannot speak to a host in another. By default, all hosts are placed into the same VLAN.

In this diagram, different VLANs are depicted in different color codes. Hosts in one

VLAN, even if connected on the same Switch cannot see or speak to other hosts in different VLANs. VLAN is Layer-2 technology which works closely on Ethernet.

2.4.8. IEEE 802.2: Logical Link Control

It hides the differences between the various kinds of 802 networks by providing a single format and interface to the network layer. LLC forms the upper half of the data link layer, with the MAC sublayer below it, as shown in



Network layer passes the packet to LLC. LLC adds an LLC header containing sequence and acknowledgement numbers. The header is attached to the payload. At the receiver, the reverse process takes place.
LLC provides three service options: a) Unreliable datagram service b)Acknowledged datagram service c)Reliable connection-oriented service. The LLC header has three fields: destination and source access points, and a control field. The control field contains sequence and acknowledgement numbers.

Retrospective on Ethernet

✓ Ethernet is simple and flexible.

✓ Ethernet is reliable, cheap, and easy to maintain.

✓ Thin Ethernet and twisted-pair wiring are relatively inexpensive

✓ Ethernet is easy to maintain.

✓ There is no software to install (other than the drivers) and not much in the way of configuration tables to manage.

✓ Adding new hosts is as simple as just plugging them in.

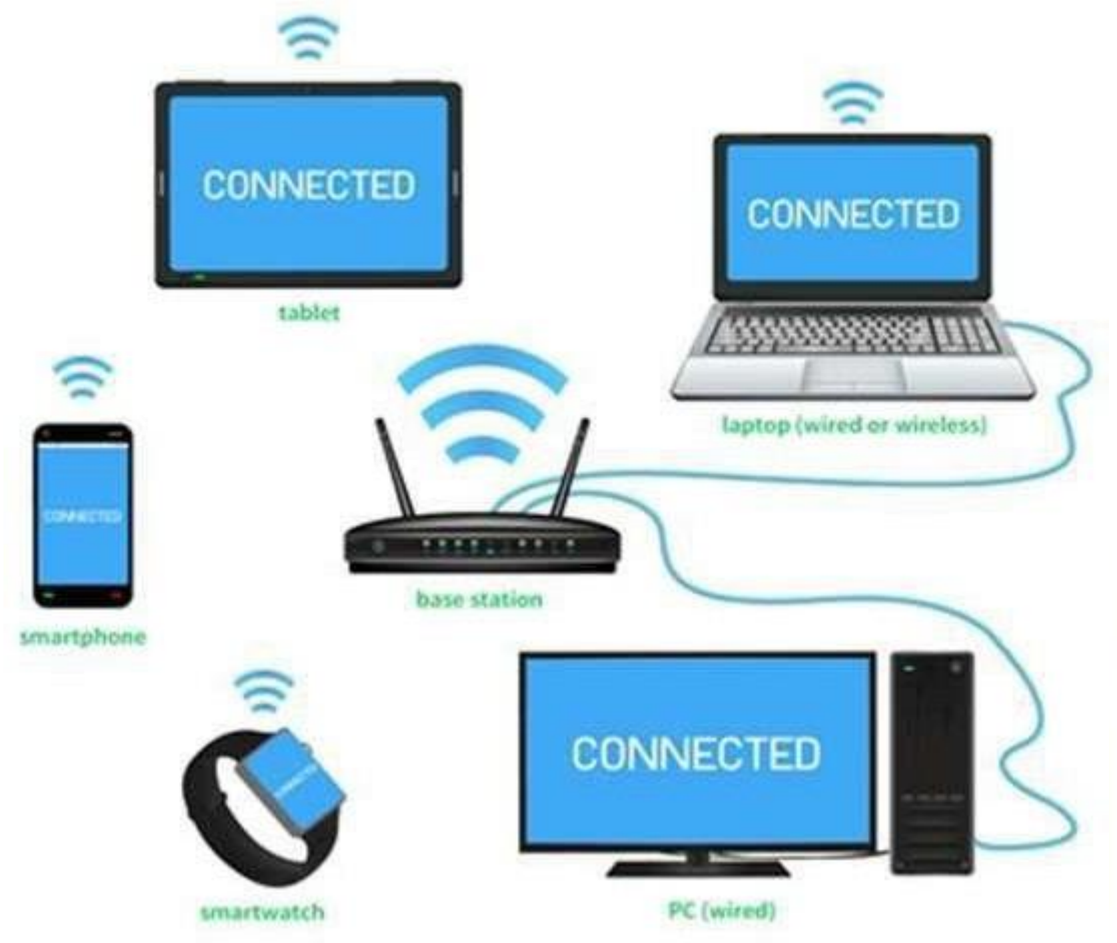
2.5. Wireless LAN

A wireless LAN (WLAN) is a wireless computer network that links two or more devices using wireless distribution method to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, office building etc. This gives users the ability to move around within the area and yet still be connected to the network (*Figure 2.27*). Most modern WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name. Wireless LANs have become popular for use in the home, due to their ease of installation and use. They are also popular in commercial properties that offer wireless access to their employees and customers.

• Advantages of Wireless LANs

✓ ***Flexibility***: Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.).

✓ ***Planning***: Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.



Robustness: Wireless networks can handle disasters, e.g., earthquakes, flood etc. whereas, networks requiring a wired infrastructure will usually break down completely in disasters.

✓ ***Cost***: The cost of installing and maintaining a wireless LAN is on average lower than the cost of installing and maintaining a traditional wired LAN, for two reasons.

✓ ***Ease of Use***: Wireless LAN is easy to use and the users need very little new information to take advantage of WLANs.

Disadvantages of wireless LANs

✓ ***Quality of Services***: Quality of wireless LAN is typically lower than wired networks. The main reason for this is the lower bandwidth due to limitations is radio transmission, higher error rates due to interference and higher delay/delay variation due to extensive error correction and detection mechanisms.

✓ ***Proprietary Solutions***: Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardization functionality plus many enhanced features. Most components today adhere to the basic standards IEEE 802.11a or 802.11b.

✓ ***Restrictions***: Several govt. and non-govt. institutions world-wide regulate the operation and restrict frequencies to minimize interference.

✓ ***Global operation***: Wireless LAN products are sold in all countries so, national and international frequency regulations have to be considered.

The 802.11 Physical Layer

Each of the five permitted transmission techniques makes it possible to send a MAC frame from one station to another.

1. Infrared

✓ uses diffused (i.e., not line of sight) transmission at 0.85 or 0.95 microns.

✓ Two capacities 1 Mbps (4-bit encoding produced 16-bit codeword) or 2 Mbps (2-bit encoding produced 4-bit codeword).

✓ Range is 10 to 20 meters and cannot penetrate walls.

✓ Does not work outdoors.

2. FHSS

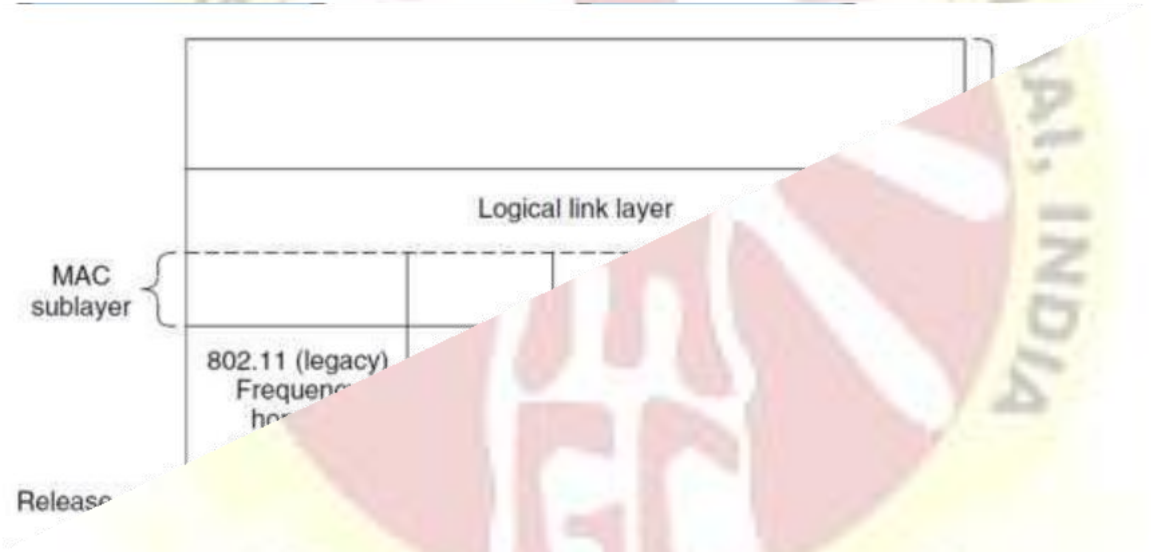
✓ The main issue is multipath fading.

✓ 79 non-overlapping channels, each 1 MHz wide at low end of 2.4 GHz ISM band.

✓ Same pseudo-random number generator used by all stations.

✓ Dwell time: min. time on channel before hopping (400msec).

✓ Its main disadvantage is its low bandwidth.



SMDS:

Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress. A communication system may include number of switches and nodes. At broad level, switching can be divided into two major categories:

☐ **Connectionless:** The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.

☐ **Connection Oriented:** Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. Data is then forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

Circuit Switching

When two nodes communicate with each other over a dedicated communication path, it is called circuit switching. There is a need of pre-specified route from which data travels and no other data is permitted. In circuit switching to transfer the data, circuit must be established so that the data transfer can take place.
Circuits can be permanent or temporary. Applications which use circuit switching may have to go through three phases:

☐ Establish a circuit

☐ Transfer the data

☐ Disconnect the circuit

Circuit switching was designed for voice applications. Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between caller and callee is established over the network.

Packet Switching:

Shortcomings of message switching gave birth to an idea of packet switching. The entire message is broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently.
It is easier for intermediate networking devices to store small size packets and they do not take much resources either on carrier path or in the internal memory of switches

Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded according to their priority to provide quality of service.

Message switching:

This technique was somewhere in middle of circuit switching and packet switching. In message switching, the whole message is treated as a data unit and is switching / transferred in its entirety.
A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop. If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.

This technique was considered substitute to circuit switching. As in circuit switching the whole path is blocked for two entities only. Message switching is replaced by packet switching. Message switching has the following drawbacks:

☐ Every switch in transit path needs enough storage to accommodate entire message.

☐ Because of store-and-forward technique and waits included until resources are available, message switching is very slow.

☐ Message switching was not a solution for streaming media and real-time applications.

Unit IV

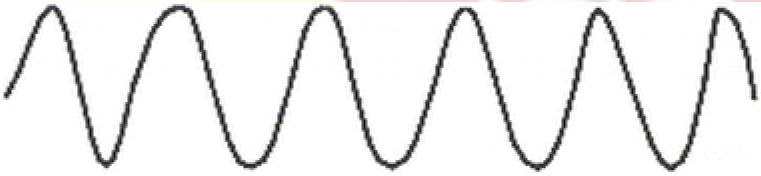
Analog Signals

An **analog** or **analogue signal** is any continuous signal for which the time varying feature (variable) of the signal is a representation of some other time varying quantity, i.e., analogous to another time varying signal. It differs from a digital signal in terms of small fluctuations in the signal which are meaningful. Analog is usually thought of in an electrical context; however, mechanical, pneumatic, hydraulic, and other systems may also convey analog signals.

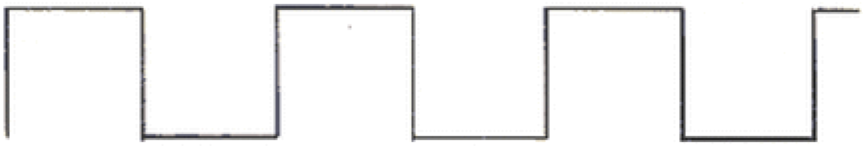
Digital Signals

A **digital signal** is a chemical signal that is a representation of a sequenceof discrete values (a quantified discrete-time signal), for example of arbitrary bit stream, or of a digitized (sampled and analog-to-digital converted) analog signal. The term digital signal can refer to

1. a continuous-time waveform signal used in any form of digital communication.
2. a pulse train signal that switches between a discrete number of voltage levels or levels of light intensity, also known as a a line coded signal, for example a signal found in digital electronics or in serial communications using digital baseband transmission in, or a pulse code modulation (PCM) representation of a digitized analog signal.

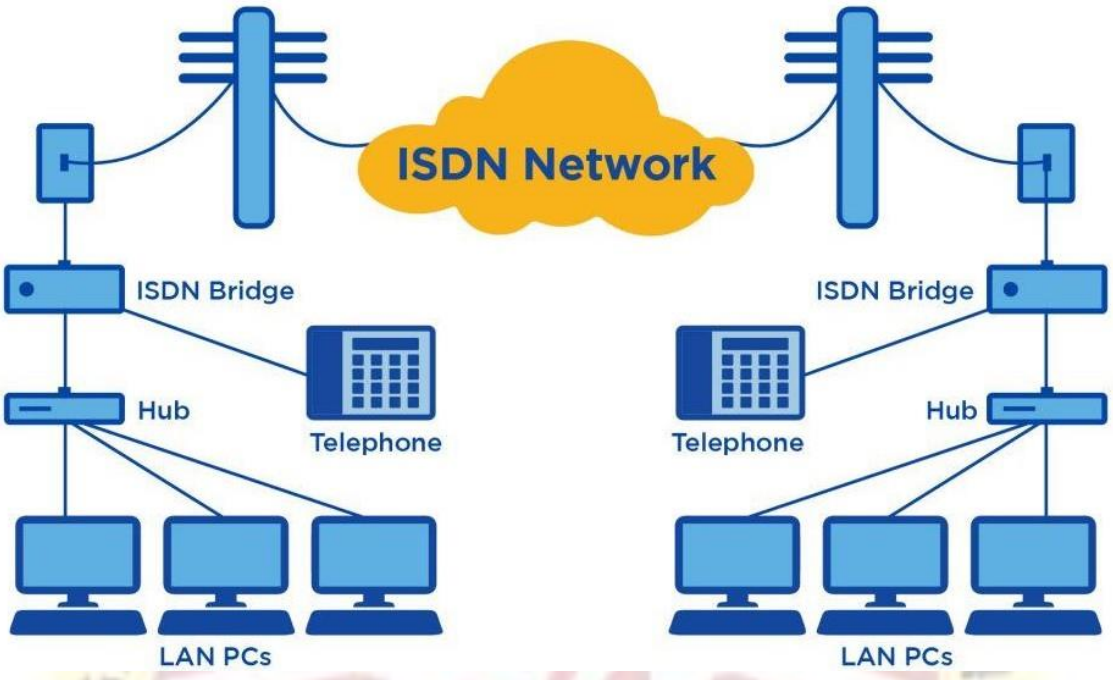


Analog Signal



Digital Signal

Access to ISDN:



Most people use ISDN for high-speed internet when options like DSL or cable modem connections are not available.

Setting up ISDN is something you'll want to work on with your Internet Service Provider (ISP). A lot of the steps can easily be done from your home.

Your ISDN will be plugged in through a traditional **POTS (Plain Old Telephone Service**) line that can access both phone numbers at once.

You'll have to make sure you have a working POTS line and assigned phone numbers to begin.

After that, you can follow the steps below to get your voice and data communications up and running.

ISDN setup

Setting up an ISDN connection involves using a serial port and plugging in the telephone company line.

The process of setting up ISDN involves:

- Loading the modem driver disk and programming the modem
- Pointing the modem toward the right phone numbers
- Setting your connection speeds for each line
- Directing your modem to dial your ISP (Internet Service Provider) — this phone number should be provided by your ISP
- If necessary, set your modem for BONDING (the ability to access higher speeds by allowing your modem to dial both phone numbers at once)

Broadband ISDN:

Functional Architecture off B-ISDN

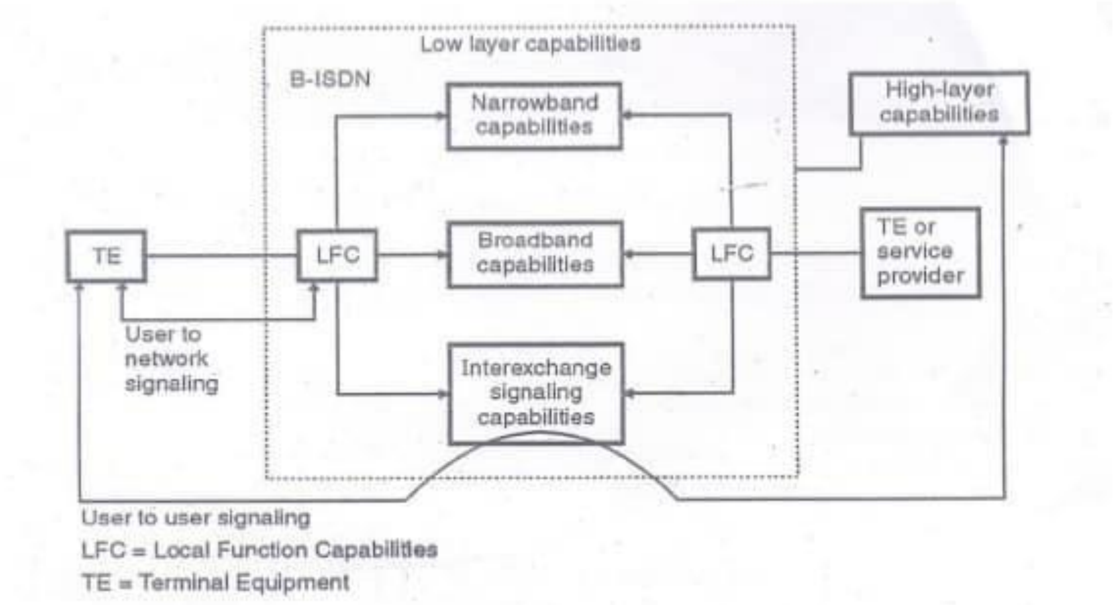


Figure: Functional architecture of B-ISDN

B-ISDN (Broadband ISDN) is the broadband transmission counterpart of Integrated Services Digital Network (ISDN). Broadband ISDN (B-ISDN) encompasses a set of International Telecommunication Union (ITU) standards and services designed to provide an integrated digital network for audio, video, and data transmission.

Instead of using the copper media used in ordinary ISDN, broadband ISDN uses fiber-optic and radio media. Broadband ISDN is designed to use the cell-switching transport technology of Asynchronous Transfer Mode (ATM) together with the underlying physical transport mechanisms of Synchronous Optical Network (SONET).

Before B-ISDN, the original ISDN attempted to substitute the analog telephone system with a digital system which was appropriate for both voice and non-voice traffic. Obtaining worldwide agreement on the basic rate interface standard was expected to lead to a large user demand for ISDN equipment, hence leading to mass production and inexpensive ISDN chips.

However, the standardization process took years while computer network technology moved rapidly. Once the ISDN standard was finally agreed upon and products were available, it was already obsolete.[citation needed] For home use the largest demand for new services was video and voice transfer, but the ISDN basic rate lacks the necessary channel capacity.

X.25

X.25 is a protocol suite defined by ITU-T for packet switched communications over WAN (Wide Area Network). It was originally designed for use in the 1970s and became very popular in 1980s. Presently, it is used for networks for ATMs and credit card verification. It allows multiple logical channels to use the same physical line. It also permits data exchange between terminals with different communication speeds.

X.25 has three protocol layers

- **Physical Layer:** It lays out the physical, electrical and functional characteristics that interface between the computer terminal and the link to the packet switched node. X.21 physical implementer is commonly used for the linking.
- **Data Link Layer:** It comprises the link access procedures for exchanging data over the link. Here, control information for transmission over the link is attached to the packets from the packet layer to form the LAPB frame (Link Access Procedure Balanced). This service ensures a bit-oriented, error-free, and ordered delivery of frames.
- **Packet Layer:** This layer defines the format of data packets and the procedures for control and transmission of the data packets. It provides external virtual circuit service. Virtual circuits may be of two types: virtual call and permanent virtual circuit. The virtual call is established dynamically when needed through call set up procedure, and the circuit is relinquished through call clearing procedure. Permanent virtual circuit, on the other hand, is fixed and network assigned.

Equipment used

- **X.21** implementer
- **DTE** − Data Terminal Equipmen
- **DCTE** − Data Circuit Terminating Equipment

Frame Relay

Frame Relay is a packet switched communication service from LANs (Local Area Network) to backbone networks and WANs. It operates at two layers: physical layer and data link layer. It supports all standard physical layer protocols. It is mostly implemented at the data link layer.

Frame Relay uses virtual circuits to connect a single router to multiple remote sites. In most cases, permanent virtual circuits are used, i.e. a fixed network-assigned circuit is used through which the user sees a continuous uninterrupted line. However, switched virtual circuits may also be used.

Frame relay is a fast packet technology based on X.25. Data is transmitted by encapsulating them in multiple sized frames. The protocol does not attempt to correct errors and so it is faster. Error correction is handled by the endpoints, which are responsible for retransmission of dropped frames

Packet Layer Protocol:

Packet Layer Protocol or **PLP** is the Network Layer protocol for the X.25 protocol suite. PLP manages the packet exchanges between DTE (data terminal) devices across VCs (virtual calls). PLP also can be used on ISDN using Link Access Procedures, D channel (LAPD).

There are 5 modes of PLP: call setup, data transfer, idle, call clearing, and restarting.

- *Call setup mode* is used to create VCs (virtual calls) between DTE devices. A PLP uses the 14-digit X.121 addressing scheme to set up the virtual call.
- *Data transfer mode* is used to send data between DTE devices across a virtual call. At this level PLP handles segmentation and reassembly, bit padding, error control and flow control.
- *Idle mode* is used when a virtual call is established but there is no data transfer happening.
- *Call clearing mode* is used to end sessions between DTE devices and to terminate VCs.
- *Restarting mode* is used to synchronize the transmission between a DTE device and its locally connected DCE (data communications) device.

There are 4 types of PLP packet fields:

- *General Format Identifier* (GFI): Identifies packet parameters (whether it is data or control information), what type of windowing is being used, and whether delivery confirmation is needed.
- *Logical Channel Identifier* (LCI): Identifies the virtual call across the local DTE/DCE interface.
- *Packet Type Identifier* (PTI): Identifies the PLP packet type (17 different types).
- *User Data*—Contains encapsulated upper-layer information when there is user data present, otherwise additional fields containing control information are added.

ATM Topology - ATM Protocol:

ATM and ATM Networks

ATM stands for Asynchronous Transfer Mode. It is a switching technique that uses time division multiplexing (TDM) for data communications.

ATM networks are connection oriented networks for cell relay that supports voice, video and data communications. It encodes data into small fixed - size cells so that they are suitable for TDM and transmits them over a physical medium.

The size of an ATM cell is 53 bytes: 5 byte header and 48 byte payload. There are two different cell formats - user-network interface (UNI) and network-network interface (NNI). The below image represents the Functional Reference Model of the Asynchronous Transfer Mode.

Benefits of ATM Networks are

- It provides the dynamic bandwidth that is particularly suited for bursty traffic.

- Since all data are encoded into identical cells, data transmission is simple, uniform and predictable.
- Uniform packet size ensures that mixed traffic is handled efficiently.
- Small sized header reduces packet overload, thus ensuring effective bandwidth usage.
- ATM networks are scalable both in size and speed.

ATM reference model comprises of three layers

- **Physical Layer −** This layer corresponds to physical layer of OSI model. At this layer, the cells are converted into bit streams and transmitted over the physical medium. This layer has two sub layers: PMD sub layer (Physical Medium Dependent) and TC (Transmission Convergence) sub layer.
- **ATM Layer −**This layer is comparable to data link layer of OSI model. It accepts the 48 byte segments from the upper layer, adds a 5 byte header to each segment and converts into 53 byte cells. This layer is responsible for routing of each cell, traffic management, multiplexing and switching.

Advantages of Wireless Networks

- It provides clutter-free desks due to the absence of wires and cables.
- It increases the mobility of network devices connected to the system since the devices need not be connected to each other.
- Accessing network devices from any location within the network coverage or Wi-Fi hotspot becomes convenient since laying out cables is not needed.
- Installation and setup of wireless networks are easier.
- New devices can be easily connected to the existing setup since they needn’t be wired to the present equipment. Also, the number of equipment that can be added or removed to the system can vary considerably since they are not limited by the cable capacity. This makes wireless networks very scalable.
- Wireless networks require very limited or no wires. Thus, it reduces the equipment and setup costs.

Unit V

Repeaters:

Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters.

Types of Repeaters

According to the types of signals that they regenerate, repeaters can be classified into two categories −

- **Analog Repeaters −** They can only amplify the analog signal.
- **Digital Repeaters −** They can reconstruct a distorted signal.

According to the types of networks that they connect, repeaters can be categorized into two types −

- **Wired Repeaters −** They are used in wired LANs.
- **Wireless Repeaters −** They are used in wireless LANs and cellular networks.

According to the domain of LANs they connect, repeaters can be divided into two categories −

- **Local Repeaters −** They connect LAN segments separated by small distance.
- **Remote Repeaters −** They connect LANs that are far from each other.

Advantages of Repeaters

- Repeaters are simple to install and can easily extend the length or the coverage area of networks.
- They are cost effective.
- Repeaters don’t require any processing overhead. The only time they need to be investigated is in case of degradation of performance.
- They can connect signals using different types of cables.

Disadvantages of Repeaters

- Repeaters cannot connect dissimilar networks.
- They cannot differentiate between actual signal and noise.
- They cannot reduce network traffic or congestion.
- Most networks have limitations upon the number of repeaters that can be deployed

Bridges:

A bridge is a network device that connects multiple LANs (local area networks) together to form a larger LAN. The process of aggregating networks is called network bridging. A bridge connects the different components so that they appear as parts of a single network. Bridges operate at the data link layer of the OSI model and hence also referred as Layer 2 switches.

Uses of Bridge

- Bridges connects two or more different LANs that has a similar protocol and provides communication between the devices (nodes) in them.
- By joining multiple LANs, bridges help in multiplying the network capacity of a single LAN.
- Since they operate at data link layer, they transmit data as data frames. On receiving a data frame, the bridge consults a database to decide whether to pass, transmit or discard the frame.
  - If the frame has a destination MAC (media access control) address in the same network, the bridge passes the frame to that node and then discards it.

  - If the frame has a destination MAC address in a connected network, it will forward the frame toward it.

- By deciding whether to forward or discard a frame, it prevents a single faulty node from bringing down the entire network.
- In cases where the destination MAC address is not available, bridges can broadcast data frames to each node. To discover new segments, they maintain the MAC address table.
- In order to provide full functional support, bridges ideally need to be transparent. No major hardware, software or architectural changes should be required for their installation.
- Bridges can switch any kind of packets, be it IP packets or AppleTalk packets, from the network layer above. This is because bridges do not examine the payload field of the data frame that arrives, but simply looks at the MAC address for switching.
- Bridges also connect virtual LANs (VLANs) to make a larger VLAN.
- A wireless bridge is used to connect wireless networks or networks having a wireless segment.

Routers:

Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.

Features of Routers

- A router is a layer 3 or network layer device.
- It connects different networks together and sends data packets from one network to another.
- A router can be used both in LANs (Local Area Networks) and WANs (Wide Area Networks).
- It transfers data in the form of IP packets. In order to transmit data, it uses IP address mentioned in the destination field of the IP packet.
- Routers have a routing table in it that is refreshed periodically according to the changes in the network. In order to transmit data packets, it consults the table and uses a routing protocol.
- In order to prepare or refresh the routing table, routers share information among each other.
- Routers provide protection against broadcast storms.
- Routers are more expensive than other networking devices like hubs,bridges and switches.
- Routers are manufactured by some popular companies like −

    - Cisco
    - D-Link
    - HP
    - 3Com

Routing Table

The functioning of a router depends largely upon the routing table stored in it. The routing table stores the available routes for all destinations. The router consults the routing table to determine the optimal route through which the data packets can be sent.

A routing table typically contains the following entities −

- IP addresses and subnet mask of the nodes in the network
- IP addresses of the routers in the network
- Interface information among the network devices and channels

Routing tables are of two types −

- **Static Routing Table −** Here, the routes are fed manually and are not refreshed automatically. It is suitable for small networks containing 2-3 routers.
- **Dynamic Routing Table −** Here, the router communicates with other routers using routing protocols to determine the available routes. It is suited for larger networks having large number of routers.

Types of Routers

A variety of routers are available depending upon their usages. The main types of routers are −

- **Wireless Router −** They provide WiFi connection WiFi devices like laptops, smartphones etc. They can also provide standard Ethernet routing. For indoor connections, the range is 150 feet while its 300 feet for outdoor connections.
- **Broadband Routers −** They are used to connect to the Internet through telephone and to use voice over Internet Protocol (VoIP) technology for providing high-speed Internet access. They are configured and provided by the Internet Service Provider (ISP).
- **Core Routers −** They can route data packets within a given network, but cannot route the packets between the networks. They helps to link all devices within a network thus forming the backbone of network. It is used by ISP and communication interfaces.
- **Edge Routers −** They are low-capacity routers placed at the periphery of the networks. They connect the internal network to the external networks, and are suitable for transferring data packets across networks. They use Border Gateway Protocol (BGP) for connectivity. There are two types of edge routers, subscriber edge routers and label edge routers.

Gateway:

A gateway is a network node that forms a passage between two networks operating with different transmission protocols. The most common type of gateways, the network gateway operates at layer 3, i.e. network layer of the OSI (open systems interconnection) model. However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model. It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway. Only the internal traffic between the nodes of a LAN does not pass through the gateway.

Features of Gateways

- Gateway is located at the boundary of a network and manages all data that inflows or outflows from that network.
- It forms a passage between two different networks operating with different transmission protocols.
- A gateway operates as a protocol converter, providing compatibility between the different protocols used in the two different networks.
- The feature that differentiates a gateway from other network devices is that it can operate at any layer of the OSI model.
- It also stores information about the routing paths of the communicating networks.
- When used in enterprise scenario, a gateway node may be supplemented as proxy server or firewall.
- A gateway is generally implemented as a node with multiple NICs (network interface cards) connected to different networks. However, it can also be configured using software.
- It uses packet switching technique to transmit data across the networks.

Types of Gateways

On basis of direction of data flow, gateways are broadly divided into two categories −

- **Unidirectional Gateways** − They allow data to flow in only one direction. Changes made in the source node are replicated in the destination node, but not vice versa. They can be used as archiving tools.
- **Bidirectional Gateways** − They allow data to flow in both directions. They can be used as synchronization tools.

On basis of functionalities, there can be a variety of gateways, the prominent among them are as follows −

- **Network Gateway** − This is the most common type of gateway that provides as interface between two dissimilar networks operating with different protocols. Whenever the term gateway is mentioned without specifying the type, it indicates a network gateway.
- **Cloud Storage Gateway** − It is a network node or server that translates storage

requests with different cloud storage service API calls, such as SOAP (Simple Object Access Protocol) or REST (REpresentational State Transfer).It facilitates integration of private cloud storage into applications without necessitating transfer of the applications into any public cloud, thus simplifying data communication.

- **Internet-To-Orbit Gateway (I2O)** − It connects devices on the Internet to satellites and spacecraft orbiting the earth. Two prominent I2O gateways are Project HERMES and Global Educational Network for Satellite Operations (GENSO)

[

Routing Algorithms

The main function of the network layer is routing packets from the source machine to the
destination machine. In most networks, packets will require multiple hops to make the journey.
The only notable exception is for broadcast networks, but even here routing is an issue if the
source and destination are not on the same network segment.

3.2.1 Routers

Before going to study about the routing algorithms, it is essential to study about router
and its functions.
A router can be hardware device with a software application. The router is connected to at least two networks and do the routing operations.
Mostly, router is located at the gateway and it routes packets as they travel from one
network to another network(s). the routers find the path/route to forward the packet to reach
the destination. It also find the alternate path, if the existing path is failed.
Routing = building maps and giving directions
Forwarding = moving packets between interfaces according to the "directions"

Routing Algorithms

The algorithms that choose the routes and the data structures that they use are a major area of network layer design.
Routing algorithm: It is that part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on.
If the network uses datagrams internally, this decision must be made anew for every arriving data packet since the best route may have changed since last time. If the network uses virtual circuits internally, routing decisions are made only when a new virtual circuit is being set up.
Session routing : Thereafter, data packets just follow the already established route. The latter case is sometimes called session routing because a route remains in force for an entire session (e.g., a login session at a terminal or a file transfer)
Forwarding: It is sometimes useful to make a distinction between routing, which is making the decision which routes to use, and forwarding, which is what happens

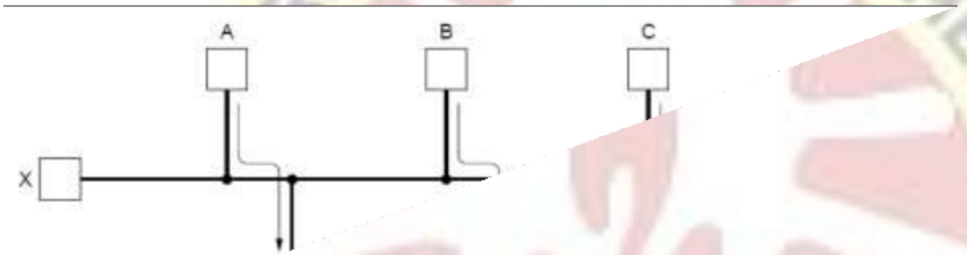
when a packet arrives.
One can think of a router as having two processes inside it. One of them handles each packet as it arrives, looking up the outgoing line to use for it in the routing tables

Properties of routing algorithms

Regardless of whether routes are chosen independently for each packet or only when new connections are established, certain properties are desirable in a routing algorithm:

✓ correctness,
✓ simplicity,
✓ robustness,
✓ stability,
✓ fairness,
✓ and optimality.

Fairness and optimality may sound obvious surely no reasonable person would oppose them, but as it turns out, they are often contradictory goals.



Types of Routing Algorithms

Routing algorithms can be grouped into two major classes:
1. Non Adaptive
2. Adaptive.

Nonadaptive algorithms do not base their routing decisions on any measurements or estimates of the current topology and traffic.

Static routing: The choice of the route to use to get from I to J (for all I and J) is computed in advance, offline, and downloaded to the routers when the network is booted.

Adaptive algorithms change their routing decisions to reflect changes in the topology, and sometimes changes in the traffic as well. These dynamic routing algorithms changes routes dynamically at run time in the following cases.

✓ Initially, get their information from locally, from adjacent routers, or from all routers.
✓ When the topology changes,
✓ When metric is used for optimization (e.g., distance, number of hops, or estimated transit time).

3.2.4 The Optimality Principle

It is necessary to find optimal routes without regard to network topology or traffic. The principal of optimality as follows;

✓ Find an optimal path has the property that whatever the initial conditions and control variables (choices) over some initial period.

✓ The control (or decision variables) chosen over the remaining period must be optimal for the remaining problem, with the state resulting from the early decisions taken to be the initial condition.

The optimality principle states that if router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same route.

Shortest Path Routing Algorithm

Shortest path algorithm works on graph of network, each node in graph represents router and each edge represents a communication link.

To choose route between given source and destination, this algorithm finds shortest path between them. Number of hopes, geographical distance, delay are some of the criteria on base of which, algorithm finds shortest path.

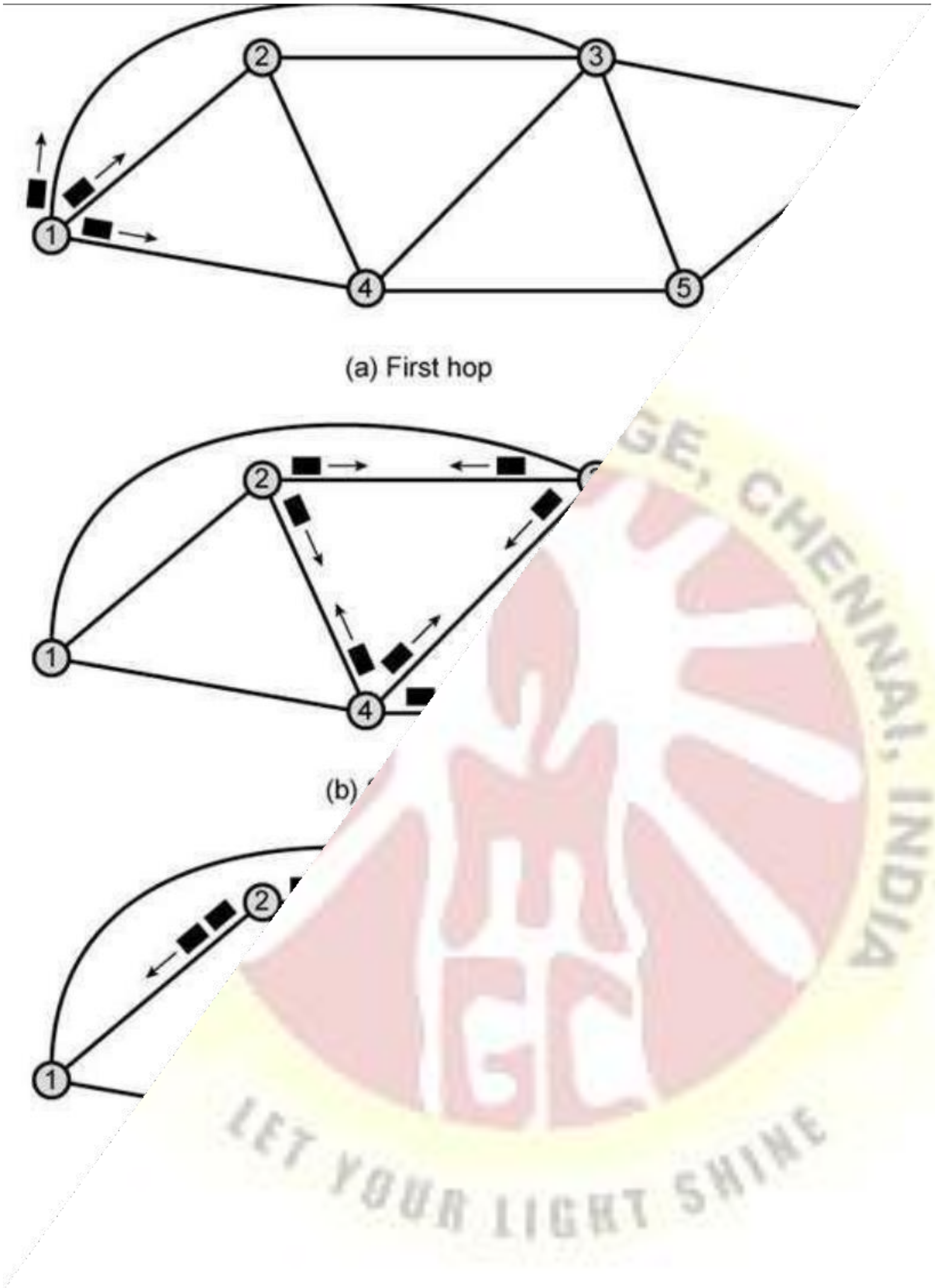
One way of measuring path length is the number of hops. Using this metric, the paths ABC and ABE in Figure 3.7 are equally long. Another metric is the geographic distance in kilometers. Many other metrics are also possible. For example, each arc could be labelled with the mean queuing and transmission delay for some standard test packet as determined by hourly test runs.

In the general case, the labels on the arcs could be computed as a function of the distance, bandwidth, average traffic, communication cost, mean queue length, measured delay, and other factors. By changing the weighting function, the algorithm would then compute the "shortest" path measured according to any one of a number of criteria or to a combination of criteria.

Flooding

Another static algorithm is flooding, in which every incoming packet is sent out on every outgoing line except the one it arrived on. Flooding obviously generates vast numbers of duplicate packets, in fact, an infinite number unless some measures are taken to damp the process.

One such measure is to have a hop counter contained in the header of each packet, which is decremented at each hop, with the packet being discarded when the counter reaches zero.



(a) First hop

(b)

Advantages

✓ Efficient and easy to implement.

✓ It does not require routers to know about spanning trees,

✓ Nor does it have the overhead of a destination list or bit map in each broadcast packet as does multidestination addressing.

✓ Nor does it require any special mechanism to stop the process, as flooding does.

TCP/IP Network:

Transmission Control Protocol (TCP)

TCP, like UDP, is a process-to-process (program-to-program) protocol. TCP, therefore, like UDP, uses port numbers. Unlike UDP, TCP is a connection oriented protocol; it creates a virtual connection between two TCPs to send data. In addition, TCP uses flow and error control mechanisms at the transport level. In brief, TCP is called a *connection-oriented, reliable* transport protocol. It adds connection-oriented and reliability features to the services of IP.

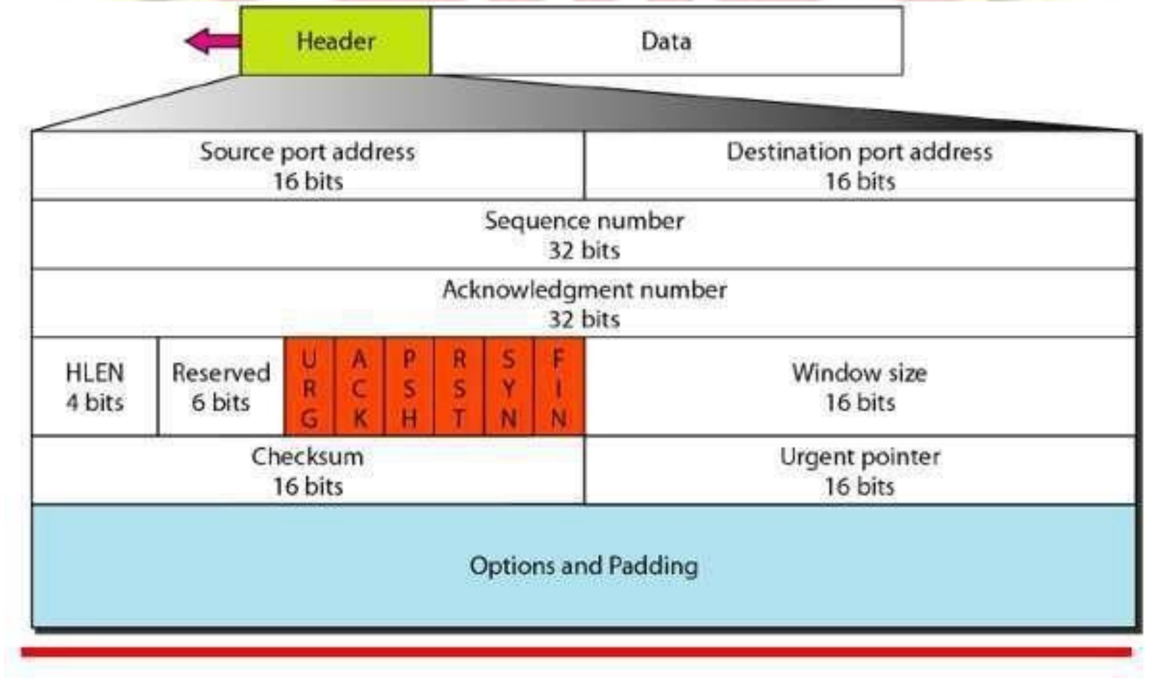
• **TCP Services**

The services offered by TCP to the processes at the application layer:

Process-to-Process Communication

Like UDP, TCP provides process-to-process communication using port numbers. Table *4-2* lists some well-known port numbers used by TCP.

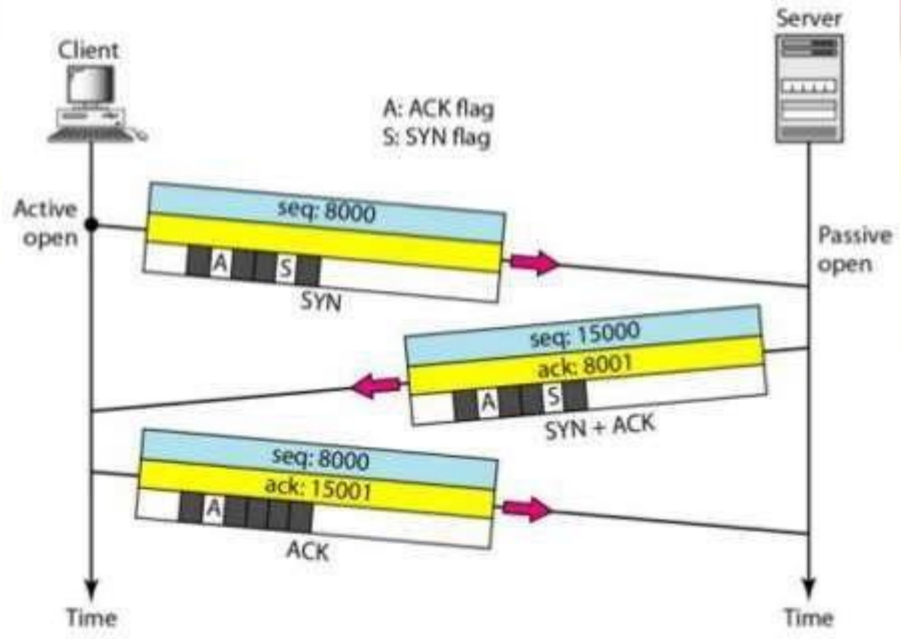
TCP, on the other hand, allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes. TCP creates an environment in which the two processes seem to be connected by an imaginary "tube" that carries their data across the Internet. This imaginary environment is depicted in Figure 4.13 *Stream delivery*. The sending process produces (writes to) the stream of bytes, and the receiving process consumes (reads from) them.



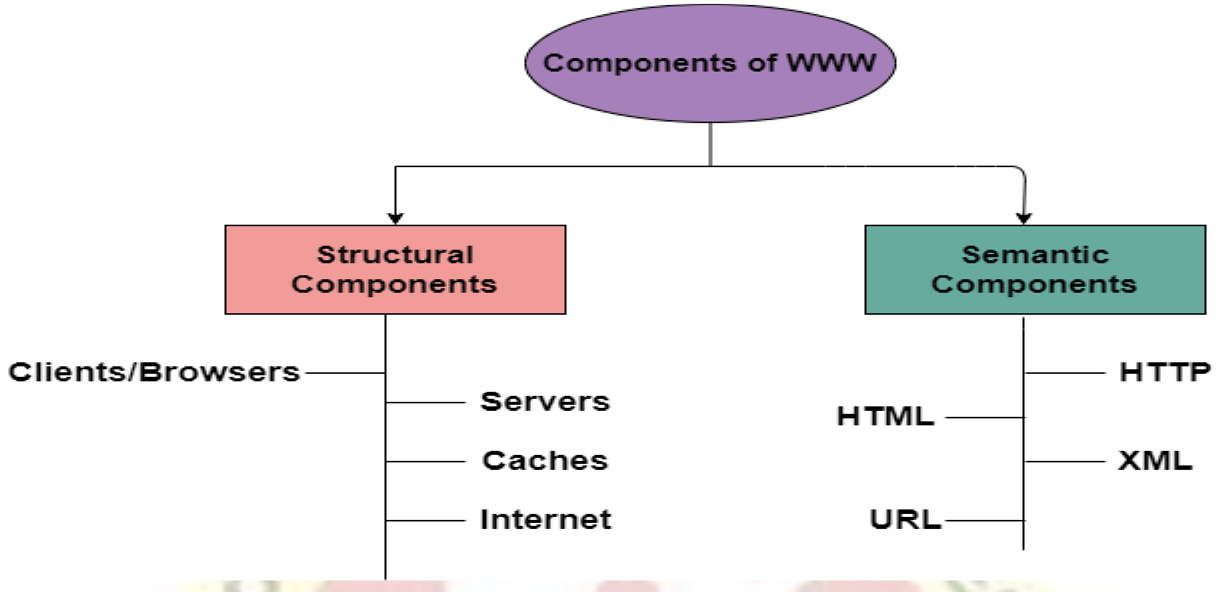
Sequence number. This 32-bit field defines the number assigned to the first byte of data contained in this segment. As we said before, TCP is a stream transport protocol. To ensure connectivity, each byte to be transmitted is numbered. The sequence number

tells the destination which byte in this sequence comprises the first byte in the segment. During connection establishment, each party uses a random number generator to create an initial sequence number (ISN), which is usually different in each direction.
Acknowledgment number. This 32-bit field defines the byte number that the receiver ofthe segment is expecting to receive from the other party. If the receiver of the segment has successfully received byte number *x* from the other party, it defines *x* + I as the acknowledgment number. Acknowledgment and data can be piggybacked together.
Header length. This 4-bit field indicates the number of 4-byte words in the TCP header.The length of the header can be between 20 and 60 bytes. Therefore, the value of this field can be between 5 (5 x 4 =20) and 15 (15 x 4 =60).
Reserved. This is a 6-bit field reserved for future use.

TCP Transmission
In TCP, connection-oriented transmission requires three phases: connection establishment, data transfer, and connection termination.
a. Connection Establishment
TCP transmits data in full-duplex mode. When two TCPs in two machines are connected, they are able to send segments to each other simultaneously. This implies that each party must initialize communication and get approval from the other party before any data are transferred.
Three-Way Handshaking The connection establishment in TCP is called three-way handshaking. In our example, an application program, called the client, wants to make a connection with another application program, called the server, using TCP as the transport layer protocol.
The process starts with the server. The server program tells its TCP that it is ready to accept a connection. This is called a request for a *passive open.* Although the server TCP is ready to accept any connection from any machine in the world, it cannot make the connection.



World Wide Web:



Internetworking

When two or more networks are connected it is called Internet. There will be a variety of different networks will always be around, for the following reasons.

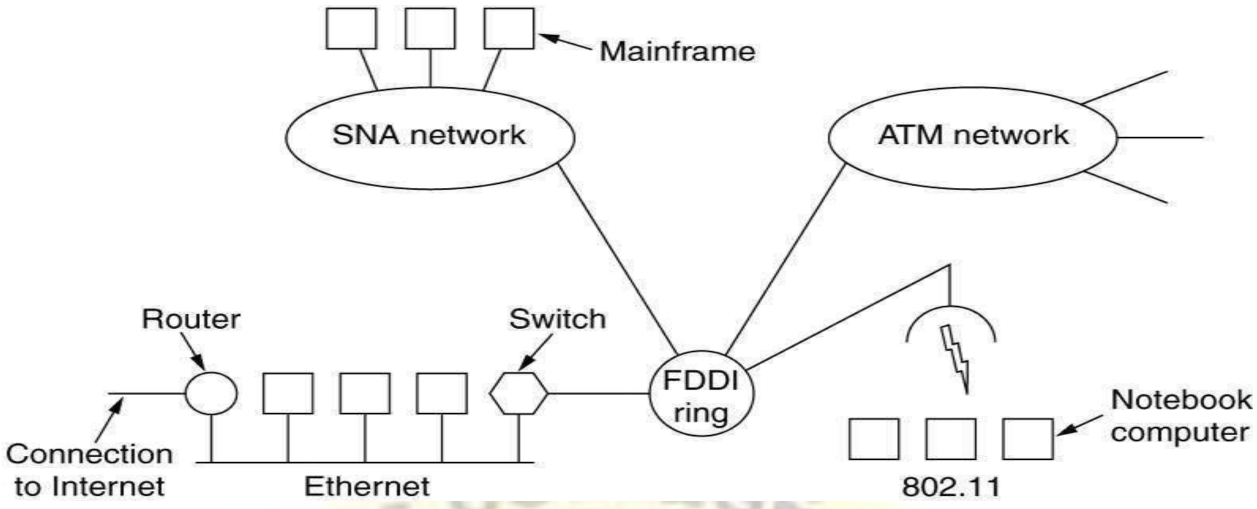
1. Different networks will use different technologies like personal computers run TCP/IP, mainframes run on IBM’s SNA

2. As computers and networks get cheaper, the place where decisions get made moves downwards in organizations.

3. As new hardware developments occur, new software will be created to fit the new hardware.

There are various types of network like LAN, MAN, WAN, ad hoc network, ATM etc. Different types of network varies from each other mainly due to protocol suite and technology used by network and various other parameters.

As an example of how different networks might be connected, consider the example of Figure 3.17. Here we see a corporate network with multiple locations tied together by a wide area ATM network. At one of the locations, an FDDI optical backbone is used to connect an Ethernet, an 802.11 wireless LAN, and the corporate data center's SNA mainframe network.



The purpose of interconnecting all these networks is to allow users on any of them to communicate with users don all the other ones to allow users on any of them to access data on any of them. Networks differ in many ways. In the network layer the following differences can occur.

✓ Some of the differences, such as different modulation techniques or frame formats, are in the physical and data link layers.

✓ The differing maximum packet sizes used by different networks can be a major nuisance.

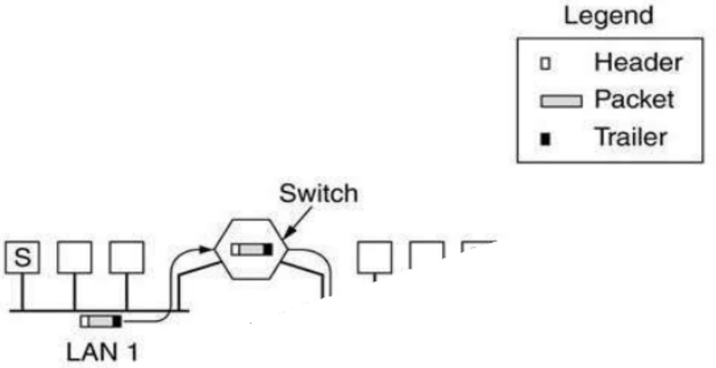
How networks can be connected?

Networks can inter connected by different devices. In the physical layer networks are connected by repeaters or hubs, which just move the bits from one network to an identical network.

At the Data Link layer bridges and switches are used. In network layer, routers are used to connect two network layers, the router may be able to translate between the packet formats. A router that can handle multiple protocols is called a ‘multi protocol’ router.

In the transport layer we find transport gateways, which can interface between two transport connections (allow packets to flow between a TCP network and an SNA network).

Finally, in the application layer, application gateways translate message semantics (gateways between Internet e-mail (RFC 822) and X.400 e-mail).


Legend
Header
Packet
Trailer
Switch
S
LAN 1