Data Communication & Network Notes

ICT 5th Semester

by

Mukesh Singh
ICT 5th batch 2073

Sukuna Multiple Campus
Sundarharaincha-12, Morang.

Unit-1

Fundamentals of Digital Communications

1.1. Introduction to digital communications: Definitions of terms, Signal Propagation, Signal types (Sine Waves, Square waves), Signal Parameters (Amplitude, Frequency, Phase).

Introduction to digital communication:

Digital Communication is the process of devices communicating information digitally.

Digital communication is a mode of communication. In our increasingly connected world, one can hardly imagine his/her life without digital communication. It allows modern people to connect with each other more easily than ever before.

Signal

A signal is an electrical or electromagnetic current that is used for carrying data from one device or network to another.

Signal Propagation:

Signal propagation is the behaviour of radio wave as they travel, or are propagated, from one point to another, or into various parts of the atmosphere.

There are three basic types of propagation:

i) Ground-wave propagation.
ii) Sky-wave propagation
iii) line-of-sight propagation

Signal types (Sine waves, Square Waves)

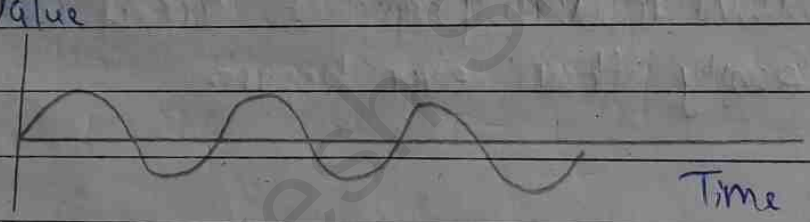
There are two types of signal.

i) Sine waves

The sine wave is the most fundamental form of a periodic analog signal.

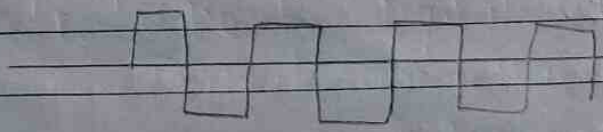
When we visualize it as a simple oscillating curve, its change over the course of cycle is smooth and consistent, a continuous, rolling flow.

Figure below shows a sine wave. Each cycle consists of a single arc above the time axis followed by a single arc below it.



ii) Square Wave

Square wave is a waveform that quickly rises to a particular level, remains constant for some period, then instantly drops to another level and stays there, and finally, rises to its original level to complete the wave cycle.



Signal Parameters (Amplitude, frequency, Phase)

i) Amplitude

Amplitude is the maximum absolute value of a periodically varying quantity.

for electric signals, peak amplitude is normally measured in volts.

ii) frequency

Frequency refers to the number of periods in 1 s.

Period refers to amount of time, in seconds, a signal needs to complete 1 cycle.

Period is inverse of frequency and vice versa.

i.e $F = 1/T$ and $T = 1/F$

Period is formally expressed in seconds.

Frequency is normally expressed in Hertz (Hz), which is cycle per second.

iii) Phase

The term phase describes the position of the wave form relative to time 0.

Phase is measured in degrees or radians.

12. Channel effects on transmission : Attenuation, Effects of limited bandwidth, Delay distortion, Noise

#i) Attenuation :
- Attenuation means a loss of energy.
- When a signal travels through a medium, it loses some of its energy in overcoming the resistance of the medium.

ii) Delay Distortion
- Distortion means that the signal changes its form or shape.
- Distortion can occur in composite signal made of different frequencies.
- Delay distortion is a guided transmission media phenomenon where network data signals are transmitted via a media at certain frequency and speed.
- This means that all the signals do not arrive at the same time, resulting in distortion of the signal.

iii) Noise
- The unwanted signal is called the noise.
- Practically, we cannot avoid the existence of unwanted signal transmitted by the transmitter.
- Noise is a random signal that exists in a communication system.

Types of noise:
i) Thermal noise
ii) Induced noise
iii) Crosstalk
iv) Impulse noise

1.3. Data rate limits in Channels : Nyquist's theorem, Shannon's theorem

Data rate limits is very important consideration in data communications ie how fast we can send data, in ~~bits~~ per second, over a channel.

i) Nyquist's theorem

1.4. Performance of Channel: Bandwidth, Throughput, Latency, Jitter, Bit Error Rate (BER)

Performance of channel refers to the measures of service quality of a network as seen by the customer. There are different ways to measure the performance of a network, as each network is different in nature and design.

i) Bandwidth:-

It is the amount of ~~tense~~ data that can be transmitted in fixed amount of time.

Bandwidth is usually expressed in bits per second (bps) or bytes per second.

For analog ~~signals~~. devices, the bandwidth is expressed in cycles per second, or Hertz (Hz)

ii) Throughput

- Throughput is the measure of how fast we can actually send data through a network.
- It is the rate of sucessful message delivery over a communication channel.
- It is usually measured in bits per second (bps), and sometimes in data packets per second (p/s or pps).

iii) Latency:

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

i.e Latency = propagation time + transmission time + queuing time + processing delay.

iv) Jitter:

Jitter or Network jitter, is the variance in time delay in milliseconds (ms) between data packets over a network.

It is a disruption in the normal sequence of sending data packets.

v) Bit Error Rate (BER):

- BER is the number of bit errors per unit time.
- BER is the percentage of bits that have errors relative to the total number of bits received in a transmission, ~~usually~~.
- It is usually expressed as ten to a negative power.

Unit-2

Physical Layer Characterization

2.1 Electromagnetic Spectrum for Communication and Type of Propagation:

Electromagnetic Spectrum

The electromagnetic spectrum is the range of frequencies (the spectrum) of electromagnetic radiation and their respective wavelengths and photon energies.

The different types of electromagnetic radiation shown in electromagnetic spectrum consists of radio waves, microwaves, infrared waves, visible light, ultraviolet radiation, X-rays and gamma rays.

Types of Propagation

Signal propagation is the behaviour of radio waves as they travel, or are propagated from one point to another, or into various parts of the atmosphere.

There are three types of propagation:

i) Ground wave propagation:

- Ground wave propagation is a method of radio wave propagation that uses the area between the surface of the earth and the ionosphere for transmission.
- Ground wave propagation is used for low frequency waves and is also known as surface waves.
- Frequencies up to about 2 MHz fall in this category of propagation.

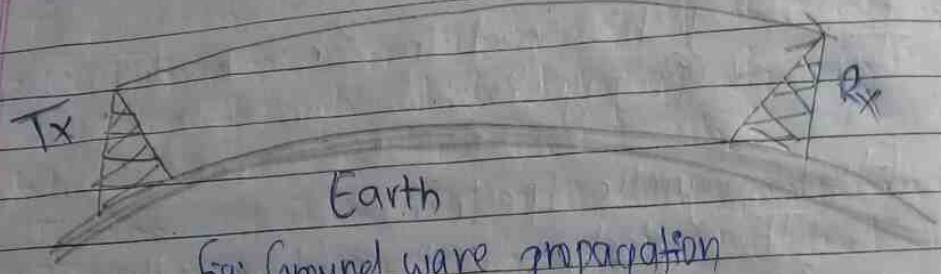


Fig: Ground wave propagation

ii) Skywave Propagation

- It refers to the propagation of radio waves reflected or refracted back toward Earth from the ionosphere (an electrically charged layer of upper atmosphere).
- It is used to cover the distances beyond the horizon.
- Frequencies between 2 MHz and 30 MHz falls in this category of propagation.

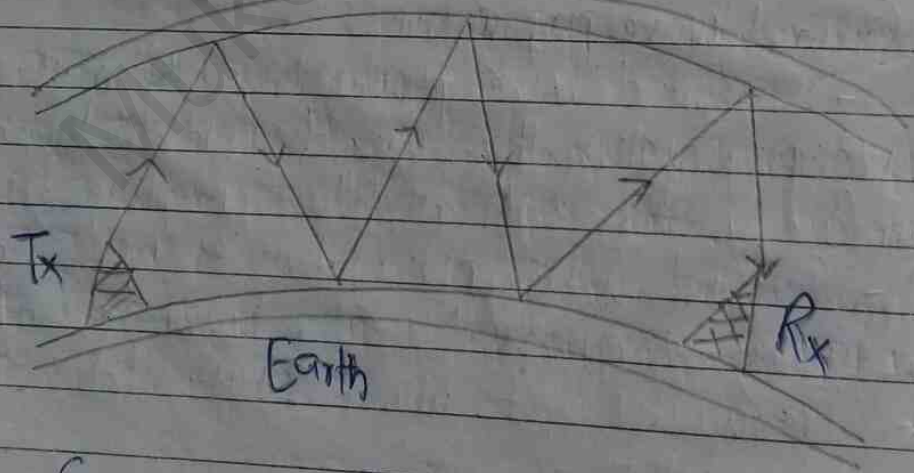


Fig: Skywave Propagation

(ii) Line of Sight Propagation

- It is a type of propagation that can transmit and receive data only where transmit and receive stations are in view of each other without any sort of an obstacle between them. Ex - fm radio, microwave and satellite transmission etc.
- Frequencies above 30 MHz falls in this category of propagation.

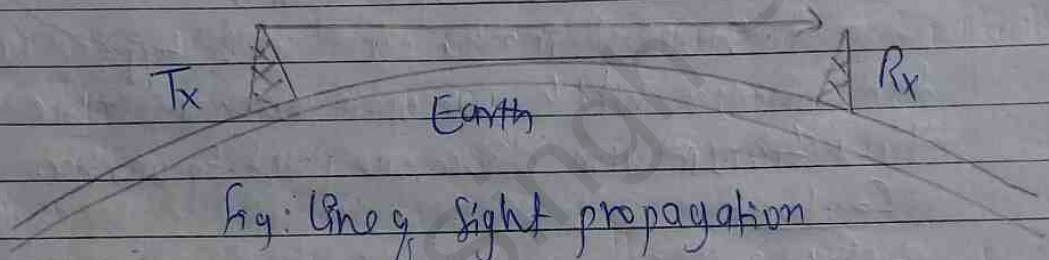


fig: Line of Sight propagation

2.2 Transmission Media:

Transmission media refers to the physical connection through which data are transmitted between sender and receiver devices.

Eg: Cables, light, radio waves, microwaves etc

Transmission media are ~~transmit~~ classified into two categories:

2.2 Guided Transmission Media : Twisted Pair Cables, Co-axial Cables, fibre Optic Cables

Guided media are such type of communication media which use open wire or cable line for data transmission from one point to another.

Features
- High speed
- Secure
- Used for comparatively shorter distances.

There are 3 major types of guided media:

i) Twisted Pair Cable

It is the least expensive and most widely used guided transmission medium.

It is made from a pair of copper wires twisted to each other and finally surrounded by outer insulating jacket.

One wire of pair for ~~sending~~ receiving signal and other for transmitting data.

The wires are twisted in ~~the~~ order to reduce

unwanted noise and interference from external sources.
- It is used for both analog and digital signals transmission.

It is available in two forms:
a) Unshielded Twisted Pair (UTP)
b) Shielded Twisted Pair (STP)

Advantages
- Less expensive
- Suitable for digital data transmission
- It has higher data transfer rate upto 4 bps.

Disadvantages
- Used for only short distance
- It emits electromagnetic interference.
- It is not suitable for video transmission.

ii) Coaxial Cables

They are such type of guided media which have wider bandwidth and noise immunity. They are widely used in long distance telephone lines, cable TV in our home.

It consists of two conductors. The inner copper conductor is surrounded by an insulator. The outer conductor is covered with a jacket or shield.

It is available in two forms:
a) Thinnet coaxial cable
b) Thicknet coaxial cable

Advantages:
- Transmission speed is higher than twisted pair cables.
- It is less affected by electromagnetic interference.
- It can support multiple channels.
- Inexpensive
- Easy to install and expand
- Better noise immunity

Disadvantages:
- Expensive than twisted pair cables.
- Not suitable for digital data transmission.

iii) Fibre Optic Cables.

Fibre optic cables are made up of plastic or glass fiber which gives high quality transmission of signals at very high speed.

It transmits signals in the form of light.

Advantages
- Suitable for long data transmission
- Can communicate with both analog or digital signals.
- Higher bandwidth i.e more than 1 gbps.
- Thinner and lighter in weight.

Disadvantages
- Not so flexible than other cables.
- High cost
- Fragile
- Difficult to install and maintain.

2.3. Unguided Transmission Media: Wireless Media (Terrestrial Microwaves, Satellite Communication, and Cellular System)

Transmission media which do not use any physical connection between two communicating devices are called Unbounded Media or Unguided Media.

Example: Infrared, Bluetooth, Wifi etc.

There are various types of unguided media:

i) Terrestrial Microwaves

High frequency electromagnetic wave (more than 1 GHz) is called microwave. Microwaves are unidirectional.

It cannot bend and pass obstacles like hill or building so it requires line-of-sight transmission.

Microwave is used in WAN or MAN Communication.

Advantages:
- Higher bandwidth
- Better quality data transmission

Disadvantages
- Can't bend and pass obstacles.
- Does not cover very large space.

ii) Satellite Communication

Satellite Communication are artificial satellites that relay receive signals from an earth station and then retransmits the signal to other earth stations.

Satellite communication is the use of satellite

technology in the field of communications.
The services provided by satellite communications are voice and video calling, internet, fax, television and radio ~~waves~~ channels.

Advantages
- Covers all geographical area of earth.
- It has higher bandwidth than radio or microwave.

Disadvantages
- Very expensive
- It has signals experience propagation delay

iii) Cellular System

Cellular system (cellular network or mobile network) is a communication network where the last link is wireless.

Cellular network is an underlying technology for mobile phones, personal communication systems and, wireless networking, etc. The technology is developed for mobile radio telephone to replace high power transmitter/receiver systems.

2.4. Physical Layer Interfaces : RS 232 / EIA 232 / USB

The physical layer is the first layer of the Open System Interconnection Model (OSI Model). The physical layer deals with bit-level transmission between different devices and supports electrical or mechanical interfaces connection to the physical medium for synchronized communication.

i) RS 232 / EIA 232

RS-232 is a standard communication protocol for linking computer and its peripheral devices to allow serial data exchange.

RS-232 interfaces are still used - particularly in industrial machines, networking equipment and scientific instruments where short-range, point-to-point, low-speed wired data connection is adequate.

ii) USB

USB stands for Universal Serial Bus.

USB is a plug and play interface that allows a computer to communicate with peripheral and other devices.

It connects peripheral devices such as digital camera, mouse, keyboard, printers, scanners, media devices, external hard drives and flash drives.

Unit-3

Data Transmission Mechanisms

3.1. Communication Mode: Simplex, Half-duplex, Full-duplex

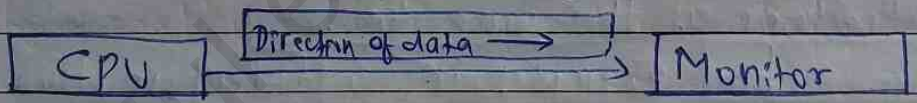
Communication mode refers to the mechanism of transferring of data between two devices connected over a network. These modes direct the flow of information.

There are three types of Communication modes:

i) Simplex Mode

Simplex refers to one-way communications where one party is the transmitter and the other is the receiver. In this type of communication, data can be sent only in one direction. i.e. Communication is unidirectional. We cannot send message back to the sender.

Examples of simplex mode are: Loudspeakers, radio, television broadcasting, keyboard & monitor etc.

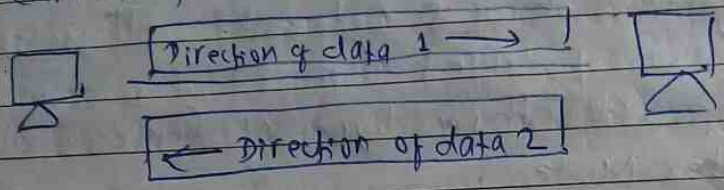


ii) Half-duplex mode:

The communication between sender and receiver occurs in both directions in a half duplex mode, but one at a time. The sender and receiver both can send and receive information but, only one is allowed to send at a time. Half duplex is still considered a one-way road, in which a vehicle travelling in the opposite direction of the traffic has

to wait till the road is empty.

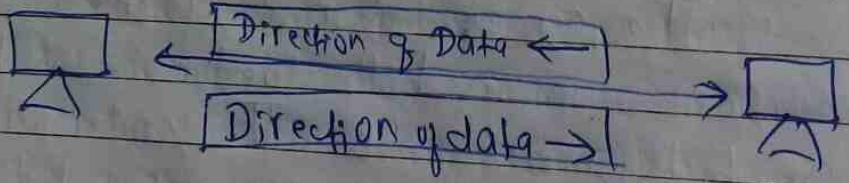
Example of half duplex is walkie-talkie in which the speaker at the both end can speak but they have to speak one by one. Both cannot speak simultaneously.



(iii) Full duplex mode

In a full duplex communication mode, the communication between sender and receiver can occur simultaneously. The sender and receiver can both transmit and receive at the same time. The full duplex transmission mode is like a two-way road in which traffic can flow in both directions at the same time.

For example, in a telephone, two people communicate, and both are free to speak and listen at the same time.



3. ~~Transmission modes: Serial transmission, parallel~~

	Simplex	Half Duplex	Full Duplex
1.	Communication is undirectional.	Communication is two directional, one at a time.	Communication is two directional, simultaneously.
2.	Sender can only send data.	Sender can send and receive data, but one at a time.	Sender can send and receive data simultaneously.
3.	Least performing mode of transmission.	Better than simplex.	Most performing mode of transmission.
4.	Eg: Radio, television, keyboard & monitor.	Eg: Walkie-talkie.	Eg: Telephone

3.2 Transmission mode: Serial transmission, Parallel transmission (Data Transmission)

Data transmission refers to the movement of data in form of bits between two or more digital devices. OR

It is the process of transferring data between two or more digital devices.

This transfer of data takes place via some form of transmission media (for example co-axial cable, fiber optics etc.)

There are two methods of data transmission shown below:

1. Serial Transmission

In serial transmission, data is sent bit by bit from one computer to another in bi-direction.

In serial data transmission, bits are sent sequentially (one after the other) down the same channel (wire). Using the single wire reduces the cost but slows down the speed of transmission. Sending data sequentially is perfect for transmitting

over longer distance as there are no synchronization issues.

Example: transmission to another computer or external devices, medium to long distances, USB etc.

Serial transmission are of two types:

i) Asynchronous

ii) Synchronous

2. Parallel Transmission

In parallel data transmission, multiple bits are sent simultaneously down the different ~~wires~~ channels (wires) within the same cable.

It is expensive but it is a fast way to transmit data as it uses many input/output lines for transferring the data.

Serial Transmission	Parallel Transmission
1 Data flows in bi-direction, bit by bit.	1 Multiple lines are used to send data i.e. 8 bits or 1 byte at a time.
2 Bits are sent sequentially down the same channel (wire).	2 Bits are sent simultaneously down the different channels (wires).
3. It is cheaper/economical.	3. It is expensive.
4. It is used for long distance communication.	4 It is used for shorter distance.
5 Only one bit is transfered at 1 clock pulse.	5 8 bits or 1 byte are transfered at 1 clock pulse.
6 Speed is slower.	6 Speed is faster.
7. It is full duplex.	7. It is half duplex.
8. Less noise and error.	8 More noise and error.
9. Eg: Computer to Computer communication.	9. Eg: Computer to printer Communication.

3.3. Synchronization: Asynchronous transmission, Synchronous transmission

Bit synchronization is a function that is required to determine when the beginning and the end of the data transmission occur.
There are two types of Synchronizations in Serial data transmission:

1) Asynchronous transmission

In asynchronous transmission, data flows ~~only~~ in half duplex mode, 1 byte or 1 character at a time.

Asynchronous transmission sends only one character at a time where a character is either a letter of the alphabet or number or control character i.e. it sends one byte of data at a time.

Bit synchronisation is made possible between two devices using start bit and stop bit.

It is simple, fast, economical and does not require a 2-way communication.

Letters, emails, forums, televisions and radios are some examples of Asynchronous transmission.

2) Synchronous Transmission

In synchronous transmission, data flows in full duplex mode in the form of blocks or frames.

It does not use start and stop bits.

Chat rooms, video conferencing, telephonic conversations are some examples of synchronous transmission.

Asynchronous transmission	Synchronous transmission
1. Sends 1 byte or character at a time.	1. Sends data in the form of blocks or frames.
2 Data flows in half duplex mode.	2 Data flows in full duplex mode.
3. It is ~~faster~~ slower.	3. It is ~~slower~~ faster.
4 It is cheaper.	4 It is expensive
5. It is simple & economic.	5 It is complex & expensive.
6 It has random time interval.	6 It has constant time interval.
7. It uses start & stop bits.	7. It does not use start & stop bits.
8. Examples: Letters, emails, forums etc	8 Examples: Chat rooms, video conferencing, telephone conversation etc

Modulation is a technique that changes the characteristics of the carrier frequency in accordance to the input signal [1,2].

3.4. Modulation techniques: Types of Analog Modulation (Amplitude Modulation, frequency modulation, and Phase Modulation), Digital Modulation (Amplitude shift keying (ASK), frequency shift keying (FSK), Phase shift keying (PSK), Quadrature Amplitude Modulation (QAM)]

Modulation is the process of converting data into radio waves by adding information to an electronic or optical carrier signal.

There are two main types of modulation:

A. Analog Modulation
B. Digital Modulation

A. Analog Modulation

In analog modulation, the modulation is applied continuously in response to the analog information signal. In this modulation, a continuously varying sine wave is used as a carrier wave that modulates the message signal or data signal.

The types of analog modulation are:

1. Amplitude Modulation (AM)

In amplitude modulation, the amplitude of the carrier wave is varied in proportional to the message signal, and the other factors like frequency and phase remain constant.

This type of modulation requires greater bandwidth, more power.

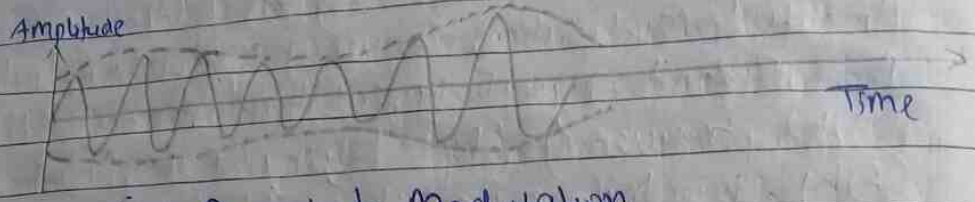


fig: Amplitude Modulation

2 Frequency Modulation (FM)

Frequency modulation is the process of varying the frequency of the carrier signal linearly with the message signal keeping phase and amplitude as constant.

The efficiency and bandwidths depend on modulation index and maximum frequency.

It is widely used in FM radio broadcasting, direct satellite broadcasting, telemetry, radar, etc.

Advantage- Increased immunity to noise.

Disadvantage- Requires larger bandwidth

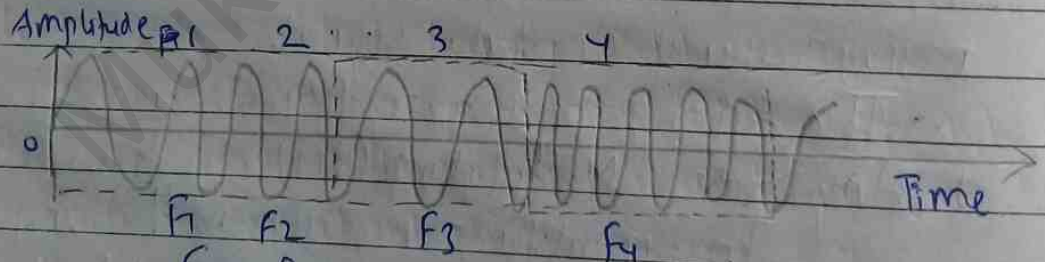


fig: frequency modulation

3. Phase Modulation (PM)

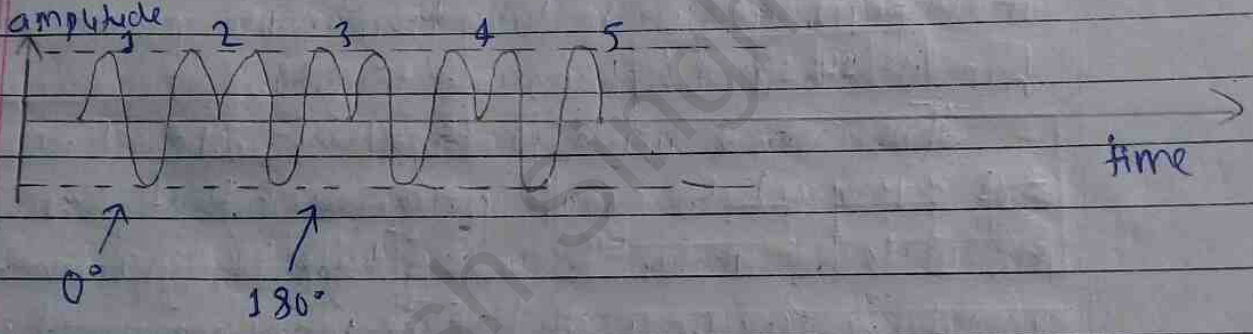
Phase modulation is the process of varying the phase of the carrier signal linearly with the message signal keeping amplitude and frequency as constant.

It is similar to FM. and also comes under FM.

It is widely used in data communication systems, for transmitting radio waves, Wifi, satellite television etc.

Advantage: Increased immunity to noise

Disadvantage: More complex hardware at receiver



B. Digital Modulation

Digital modulation refers to the process of transferring digital low frequency baseband signal like, digital bitstream from computers over a higher frequency carrier signal such as a radio frequency band.

For a better quality and efficient communication digital modulation technique is used.

The main advantages of digital modulation over analog modulation include transmissible power, available bandwidth and high noise immunity.

The carrier wave is keyed or switched on and off (1 or 0) to create pulse such that signal is modulated. Similar to analog, here the parameters like amplitude, frequency and phase variation of the carrier wave decides the types of digital modulation.

Digital modulation is of following types:

1. Amplitude Shift keying (ASK)

ASK is a type of modulation in which the amplitude of the carrier signal is varied to create two signal elements keeping both frequency and phase constant.

ASK is normally implemented using only two levels (i.e ON/OFF or 1/0).

As the information is an on-off signal. the output is also an on-off signal. where the carrier is present when information is 1 and carrier is

absent when information is 0. Thus, this modulation scheme is known as on-off keying (OOK) or amplitude shift keying.

Applications:
- Used in our infrared remote controls.
- Used in fibre optical transmitter and receiver.

2. Frequency Shift Keying (FSK)

FSK is the digital modulation technique in which the frequency of carrier signal is varied to represent data whereas keeping both amplitude and phase constant for all signal elements.

Application:
- Many modems used FSK in telemetry systems.

3. Phase Shift Key (PSK)

PSK is the digital modulation technique in which the phase of carrier signal is varied to represent two or more different signal elements, keeping both amplitude and frequency constant.

The phase of carrier signal is changed by varying the sine and cosine inputs at a particular time.

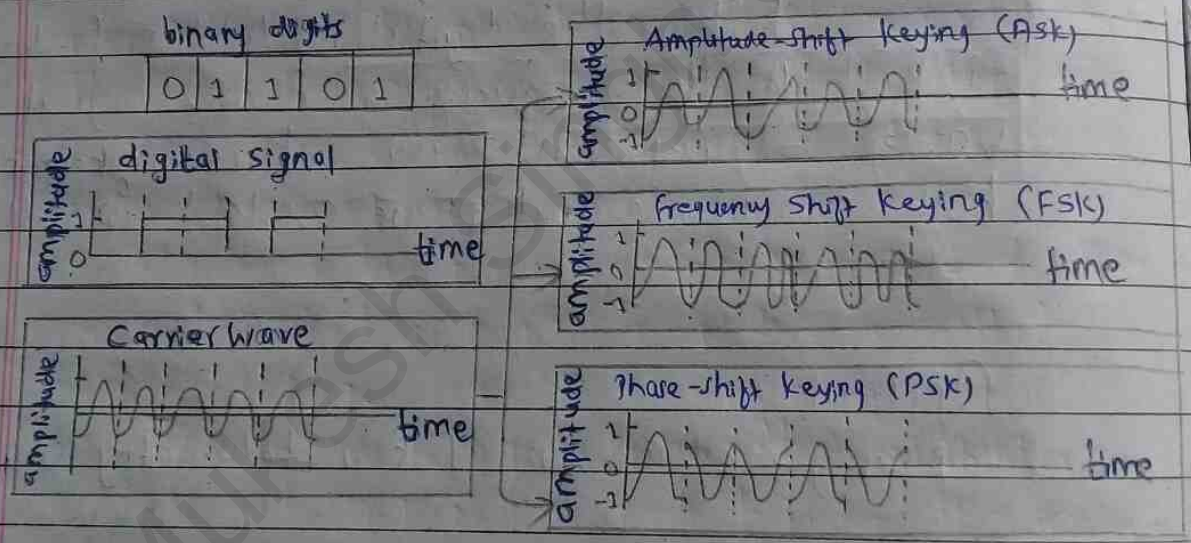
Application:
- Wireless LANs

- Used in ADSL Broadband modem
- Used in satellite communication
- Used in bluetooth communication
- Used in our mobile phones.

PSK is of two types:

i) Binary Phase Shift Key (BPSK)

ii) Quadrature Phase Shift Key (QPSK)



Good

Quadrature Amplitude Modulation (QAM)

QAM is a modulation scheme used for both digital and analog signals. QAM doubles the effective bandwidth by combining two amplitude modulated signals into a single channel.

In a QAM signal, there are two carriers, each having the same frequency but different in phase by 90 degrees. One signal is called the "I" signal, and the other is called the "Q" signal. Mathematically, one of the signals can be represented by sine wave, and the other by a cosine wave.

It is used in everything from cellular phones to Wi-Fi and almost every other form of high speed data communication.

3.5. Introduction to Packet Switching: Circuit Switching vs Packet Switching, Connection Oriented Services (Virtual Circuits), Connectionless Services (Datagrams), X.25, Frame Relay and ATM.

The mechanism for exchange of information between different computer networks and network segments is called switching.

The process of transferring data blocks from one node to another node is called data switching.

There are three types of switching techniques:

1. Circuit Switching:

When two nodes communicate with each other over a dedicated communication path, it is called circuit switching.

It is a switching technique that establishes a dedicated communication path between the sending and receiving devices. A telephone network uses circuit switching, where a dedicated path is set between the caller and the called party for the duration of a telephone call.

A complete end-to-end path must exist before the communication takes place.

To transfer the data, circuit must be established so that the data transfer can take place.

Circuit switching involves three steps:

- Circuit establishment

- Data transfer
- Circuit termination (circuit disconnect)

Advantages
- The communication channel is dedicated
- It has fixed bandwidth

Disadvantages
- It takes long time to establish a connection approx 10 seconds.
- It is more expensive than other switching techniques.

2.

2. Message Switching

In message switching, there is not necessary to establish a dedicated path between the sending and receiving devices.

So, many callers can use the same channel at the same time.

In this, each message is routed independently through the network. Each message is treated as an independent blocks.

Each and every switching node receives a message, stores the entire message and then transmits / forwards it to the next node. Thus, message switching is also called store and forward switching.

Message switching is slow because of store and forward technique.

Message switching is not recommended for real time applications like voice and video, streaming media.

Examples of message switching techniques are: e-mail, telegram, computer file transfer etc.

Advantages

- Traffic congestion can be reduced.
- Supports data of unlimited size

Disadvantages

- Every switch needs enough storage.
- Very slow because of store & forward technique.

3. Packet Switching

Packet switching is a method of transferring the data to a network in form of packets.

It is a technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.

The message splits into smaller pieces known as packets and are given a unique number to identify their order at the receiving end.

Each switching node receives the message, stores it shortly and then transmits it to the next node until it reaches the destination.

If any packet is missing or corrupted, then the message will be sent to resend the message.

If the correct order of the packet is reached, then the acknowledgement message will be sent.

Generally, the length of packet is from 128 bytes to 4096 bytes.

Advantages

- Efficient technique
- Reliable
- Faults tolerant
- Minimal transmission latency

Disadvantages

- Unordered delivery of packets
- Complexity at each node
- It is not suitable for large messages (bursty data)

There are two approaches of packet switching:

i.) Connection-Oriented Packet Switching (Virtual Circuits):

In virtual circuit approach, a fixed (logical) path through the network from the sender to the receiver is established before any packets are sent. In other words, a pre-planned route is established before the messages are sent.

Call request and call accept packets are used to establish the connection between sender and receiver.

In this case, the path is fixed or unchanged for the duration of a logical connection.

ii) Connectionless Service (Datagrams)

In datagram approach, each packet is treated as independent entity. and may follow a different path through the network.

Packets may be re-ordered, dropped or delivered in wrong sequence.

The packets are reassembled at the receiving end in correct order.

	Datagram Circuit Approach	Virtual Circuit Approach
1.	Node takes routing decisions to forward the packets.	Node does not take any routing decision.
2.	Route is established for each packet.	Route is established for entire conversation.
3.	Congestion cannot occur as all packets travel in different directions.	Congestion can occur when the node is busy, and does not allow other packets to pass through.
4.	It is more flexible.	It is not very flexible.
5.	Packet transmission delay.	Call setup delay as well as packet transmission delay.

Circuit Switching	Packet Switching
1. Connection oriented.	1. Connectionless.
2 Dedicated transmission path.	2 No dedicated transmission path.
3 A uniform path is followed throughout the session.	3. There is no uniform path that is followed end to end throughout the session.
4. Fixed bandwidth.	4. Dynamic use of bandwidth.
5. It is not a store and forward technique.	5. It is a store and forward technique.
6. Initially designed for voice communication.	6 Initially designed for data transmission.
7. It is implemented at physical layer.	7. It is implemented at Network layer.
8. Congestion can occur during Connection establishment time.	8. Congestion can occur during data transfer phase.

X.25

~~X.25 is a packet-switching protocol for wide area network (WAN) communication~~

X.25 is an ITU-T (International Telecommunication Union) standard protocol suite for packet-switched communication over a wide area network (WAN).
X.25 was originally defined by the International Telegraph and Telephone Consultative Committee (CCITT, now ITU-T) in 1976.

It was developed to provide reliable data communication on public data networks.

It uses packed switching and virtual circuits, and provides a data rate upto 64 Kbps.

It provides very robust error checking features, which makes it a good choice for older networks.

Presently, it is used for networks for ATMs and credit card verification.

It allows multiple logical channels to use the same physical line.

X.25 has three protocol layers:

i) Physical layer (level 1)

Concerned with electrical or signalling. It lays out the physical, electrical and functional characteristics that interfaces between the computer terminal and link to the packet switched node. X.21 physical ~~layer~~ is implementer is commonly used for the linking.

ii) Data link layer:
It composes the link access procedures for exchanging data over the link.

iii) The Network layer (Packet Layer)
X.25 defines a protocol for an access to packet data subnetwork.

Characterising X.25

~~Frame Relay~~
- Multiple logical channels can be set on a single physical line.
- Terminals of different communications speeds can communicate.
- The procedure for transmission controls can be changed.

Frame Relay
Frame relay is a digital packet-switching network protocol technology designed to connect local area networks (LANs) and transfer data across wide area networks (WANs).
It is a service that provided with a variety of speeds from 56 Kbps upto to 25 Mbps.
It is considered to be a broadband ISDN service.
It supports variable size data packets.
It has only two layers:
a) Physical layer b) Data link layer

Advantages of frame relay:
- Higher data rates
- It allows transfer of bursty data.
- It has lower overheads.

ATM:

ATM stands for Asynchronous transfer mode.
- It is a switching technique that uses time division multiplexing (TDM) for data communication.
- It is a high-speed networking standard designed to support voice, video and data communications, and to improve utilization and quality of service (QoS) on high-traffic networks.
- It encodes data into small fixed-sized cells so that they are suitable for TDM and transmits them over a physical medium.
- The size of ATM cell is 53 bytes: 5 byte header and 48 byte payload.
- ATM networks are scalable both in size and speed.
- An ATM header can have two cell formats:
  a) User-network Interface (UNI)
  b) Network-network Interface (NNI)

- ATM has 3 layers:
  a) Physical layer
  b) ATM layer
  c) ATM Adaptation Layer (AAL)

Four data bit rates are available for ATM services:

i) Constant Bit Rate (CBR)
ii) Variable Bit Rate (VBR)
iii) Available Bit Rate (ABR)
iv) Unspecified Bit Rate (UBR)

3.6. Multiplexing : frequency division Multiplexing (FDM), Time Division Multiplexing (TDM), Wave Division Multiplexing (WDM)

Multiplexing is a method by which multiple analog or digital signals are combined into one signal over a shared medium. Multiplexing divides the high capacity medium into low capacity ~~medium~~ logical medium which is then shared by different streams.

Multiplexing is done by a device called multiplexer (MUX) that combines n input lines to generate one output line (i.e. many to one). So, multiplexer (MUX) has several inputs and one output.

At the receiving end, a device called demultiplexer (DEMUX) is used that separates signal into its component signals. So, DEMUX has one input and several outputs.

Advantages

- More than one signal can be sent over a single medium.
- The bandwidth of a medium can be utilized effectively.

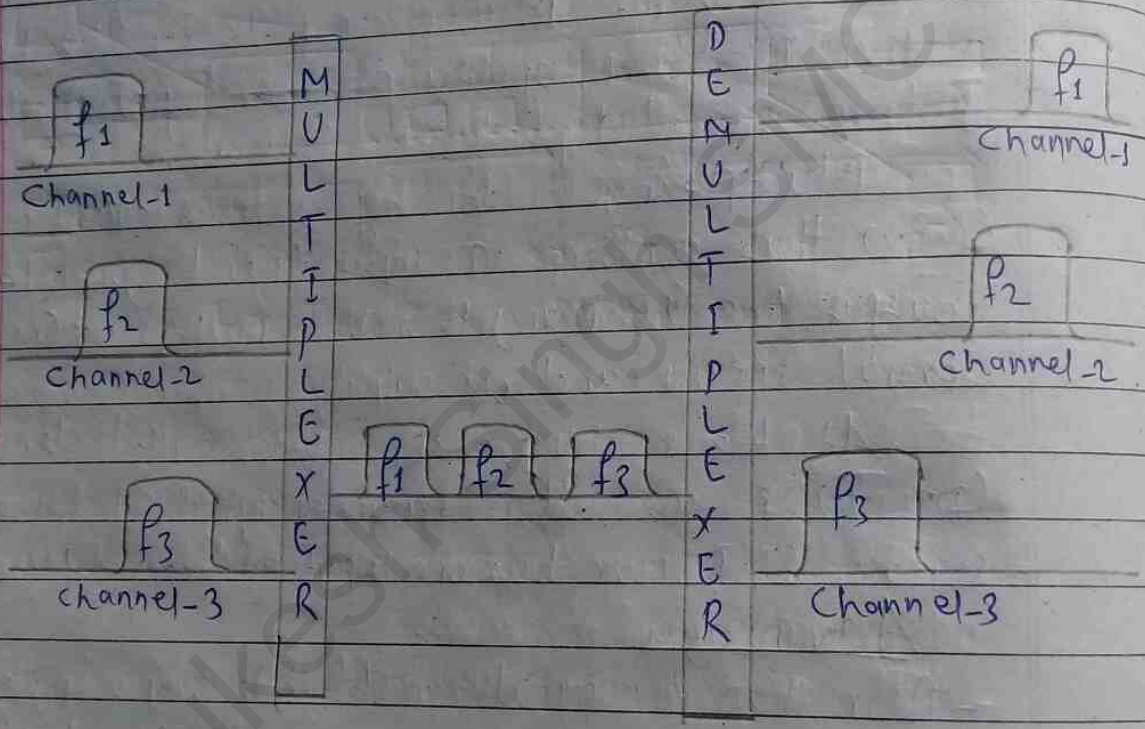
Multiplexing techniques can be classified as:

1. Frequency Division Multiplexing (FDM)

When the carrier is frequency, FDM is used. FDM is an analog technology in which the available bandwidth of a single transmission medium is sub-divided into several frequency channels and allocates one user to each channel.

Each user can use the channel frequency

independently and has exclusive access of it. All channels are divided in such a way that they do not overlap with each other. Channels are separated by guard bands. Guard band is a frequency which is not used by either channel.



Advantages of FDM:
- FDM is used for analog signals.
- Very simple & easy modulation
- A large number of signals can be sent simultaneously.
- Does not require any synchronization between sender and receiver.

Disadvantages of FDM
- Problem of crosstalk.
- A large number of modulators are required.
- It requires high bandwidth channel.

Application of FDM:
- Commonly used in TV networks.
- It is used in FM & AM radio broadcasting.
- First generation cellular telephone also uses FDM.

2. Time Division Multiplexing:
- TDM is applied primarily on digital signals but can be applied on analog signals as well.
- In TDM, the channel is not divided on the basis of frequency but on the basis of time.
- Total time available in the channel is divided between several users.
- Each user can transmit data within a particular time interval called time slot / time slice.
- The data rate capacity of the transmission medium should be greater than the data rate required by sending or receiving device.
- The data is not transmitted simultaneously rather the data is transmitted one by one.
- The signal is transmitted in the form of frames.

There are two types of TDM:

i) Synchronous TDM - time slots are fixed.

ii) Asynchronous TDM - time slots are not fixed

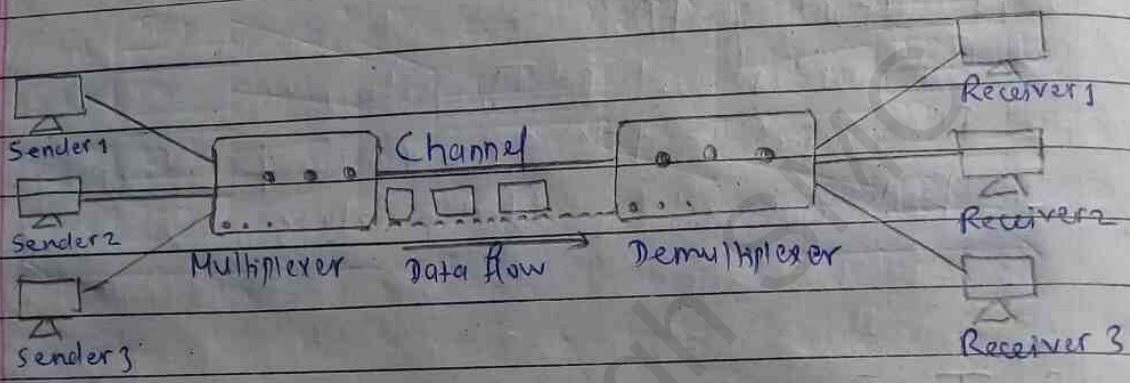


Fig: Time Division Multiplexing

Advantages of TDM:
- Full available channel bandwidth can be utilized for each channel.
- TDM circuitry is not very complex.
- The problem of crosstalk is not severe.
- Intermodulation distortion is absent.

Disadvantages of TDM
- Synchronization is needed for proper operation.
- Slow narrowband fading.

Applications
- Used in digital audio mixing system.
- Used in Public Switched Telephone Network (PSTN)
- Used in cellular Radio.

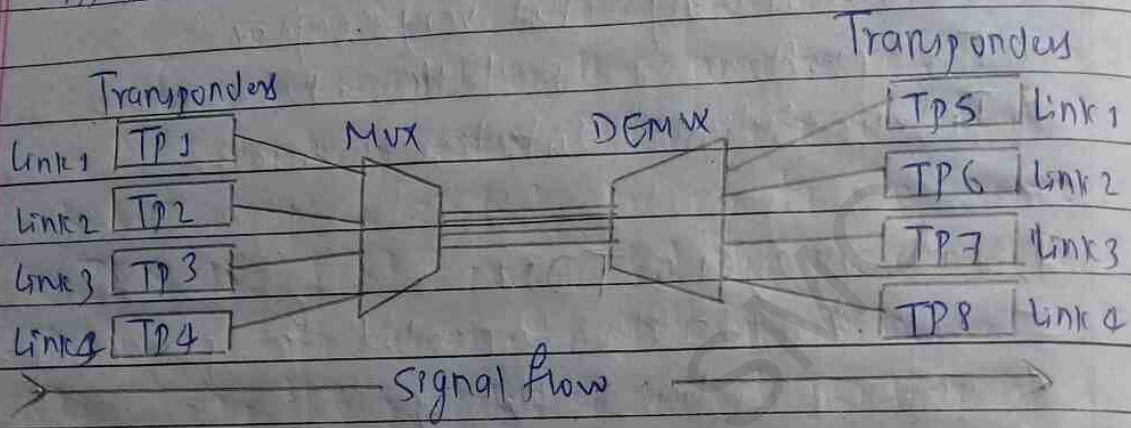
3. Wave Division Multiplexing (WDM):

WDM is a technology which multiplexes a number of optical carrier signals onto a single optical fiber by using different wavelengths (i.e. colors) of laser light. WDM allows communication in both the directions in the fiber cable.
- It is an analog multiplexing technique.
- Optical signals from different sources are combined to form a wider band of light with the help of multiplexer.
- At the receiving end, demultiplexer separates the signals to transmit them to their respective destinations.
- Multiplexing and demultiplexing can be done using a prism.

WDM is divided into two categories:

i) Course WDM

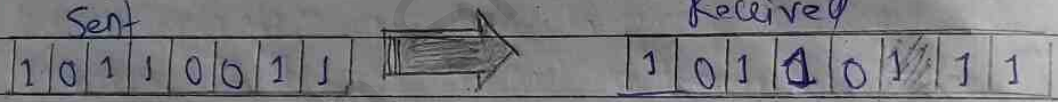
ii) Dense WDM



3.7. Error control methods: Feedback error recovery (ARQ) (Eg: Based on parity check), Forward error Correction (FEC) (Eg: CRC).

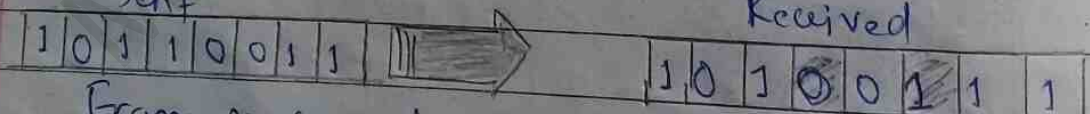
Error control is the process of detecting and correcting ~~error~~ data frames that have been corrupted or lost during transmission.
It is the technique of detecting and correcting blocks of data during communication.
It checks the reliability of characters at both at the bit level and packet level.
Types of Errors:

i) Single Bit error:



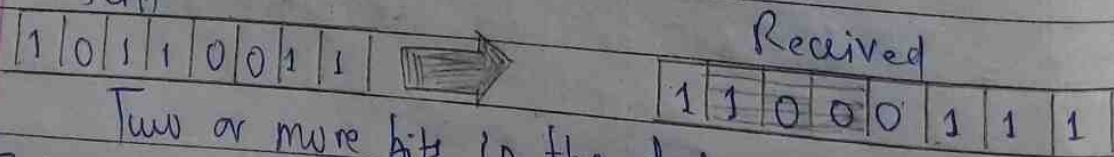
Only one bit bit of data unit was changed from 1 to 0 and 0 to 1, which is corrupt.

ii) Multiple bits error



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

iii) Burst error



Two or more bits in the data unit were changed. Frame contains more than 1 consecutive bits corrupted.

There are two ~~types~~ ways of error control mechanisms. They are:

A. Error detection B. Error Correction

1. ~~Forward Error Control~~

A. Error Detection:

It is the process of detecting the error during the transmission between the sender and the receiver.

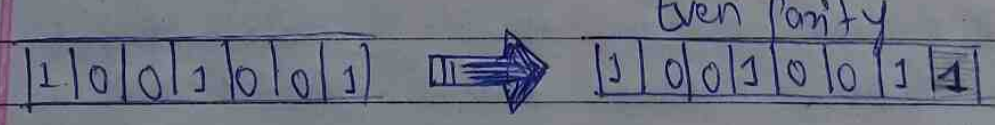
~~A~~ Types of error detection:

i) Parity Checking

Parity adds a single bit that indicates whether the number of 1 bits in the preceeding data is even or odd. If a single bit is changed in transmission, the message will change parity and error can be detected.

In other words, one extra bit is sent along with the original bits to make number of 1s either even in case of even parity or odd in case of odd parity.

For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even. If number of 1s is odd, to make it even a bit with value 1 is added.



ii) Cyclic Redundancy Check

CRC is a very efficient redundancy checking technique. The technique is based on the binary division of the data ~~being~~ bits being sent. The divisor is generated using polynomials.

The sender performs a division operation on the bits being sent and calculates the remainder. Before ~~the~~ sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a codeword. The sender transmits data bits as codewords.

~~At the~~

At the other end, the receiver performs division operation on codewords using the same CRC division. If the remainder contains all zero the data bits are accepted, otherwise it is considered as there some data corruption occured in transit.

B) Error Correction

This type of error control allows a receiver to reconstruct the original information when it has been corrupted during data transmission.

Error correction codes are used to detect and correct errors when data is transmitted from the sender to the receiver.

Error correction ensures that corrected and error free messages are obtained at the receiver side.

Two ways of error correction:

i) Feedback (Backward) error correction:

Once the error is discovered in the received data, the receiver requests the sender to retransmit the entire data unit.

ii) Forward error correction:

In this case, the receiver uses the error-correcting codes which automatically corrects the errors.

ARQ

Automatic Repeat Request (ARQ), also called Automatic Repeat Query, is an error-control protocol or method for data transmission that uses acknowledgements and timeouts to achieve reliable data transmission over an unreliable service.

OR, ARQ is an error-control method/protocol that automatically initiates a call to retransmit any data packet or frame after receiving incorrect data.

Unit - 4

Network Architectures

~~4.1 Computer Network~~

4.1. Introduction to Computer Network

A network is a set of devices (nodes) connected by communication links. Simply, it is interconnection of nodes.

Networking is the process of interconnecting two or more peoples or objects in a network.

Computer Network

A Computer network is a set of computers connected together for the purpose of sharing resources.

OR Computer network is the interconnection of two or more network devices with the help of transmission media and set of protocols (rules).

Advantages

- Sharing resources
- Faster and Cheaper Communication
- Centralized Control
- Backup and recovery
- Remote and Mobile Access

Disadvantages

- Expensive
- Security problem
- Needs technical person

Application of Computer Network:
- Business Applications
- Home Applications
- Mobile User
- Social issues

4.2 Network Topologies : Bus, Star, Ring

A network topology is a description of how network is laid out or arranged.

Network topology refers to the physical structure of a network that deals with how ~~networks are~~ computers are interconnected by using cabling system.

The most common network topologies are explained below:

1. Bus Topology:

Bus topology is a network type in which every computer and network devices are connected to a single continuous cable called "bus" or backbone. When it has exactly two end point, then it is called linear Bus Topology. A bus must be terminated on both sides to prevent signal bounce. It transmits data only in one direction.

It is based on client server network architecture.

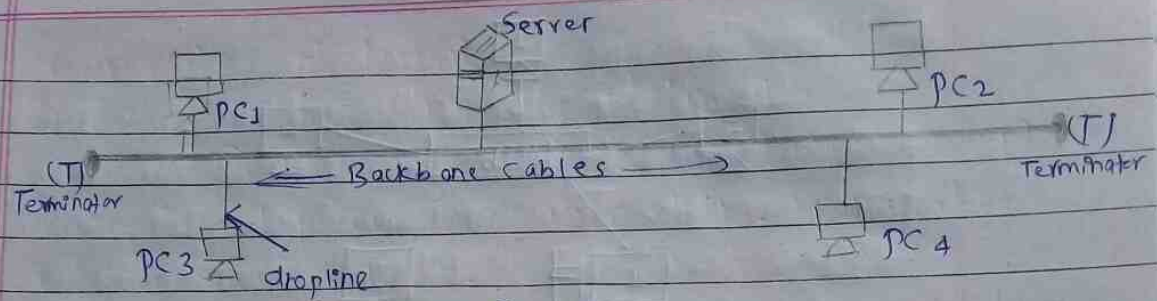


Fig: Bus Topology

Advantages
- Easy to setup and extend the network.
- Cost effective (inexpensive)
- Less amount of cable is required.
- Failure of one node(pc) does not affect others.

Disadvantages
- If main cable fails then whole network fails.
- Difficult to find and troubleshoot error.
- Limited cable length and number of nodes.
- High maintenance cost.

2 Star Topology:

It is a type of topology, in which all nodes or computers are connected with a central component or device called Hub or Switch or Server.

Every node has its own dedicated connection to the hub. Hub acts as repeater. It increases the strength of data flow. It uses twisted pair cable, Optical or Coaxial Cable. It is based on client server architecture.

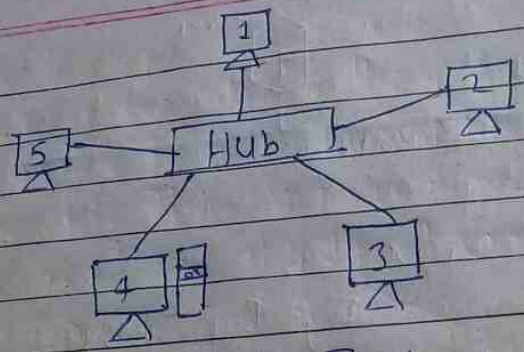


Fig: Star Topology.

Advantages
- Simple, reliable and easy to setup.
- It is flexible to add or remove computers/nodes in the network.
- Easy to find fault and troubleshoot.
- failure of one node does not affect others.

Disadvantages
- Requires large amount of cables.
- If hub fails then whole network fails.
- Expensive topology.

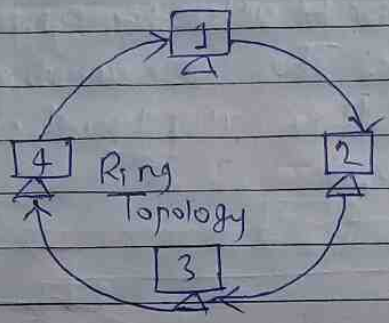
3. Ring Topology:

A ring topology is such type of network topology in which all nodes are connected to each other in a circular, loop or ring.

Each node/computer is connected directly to two other devices, one on either side of it.

It is based on par to peer network architecture. There is no server and communication takes place

only in one direction i.e either clockwise or anticlockwise.



Advantages

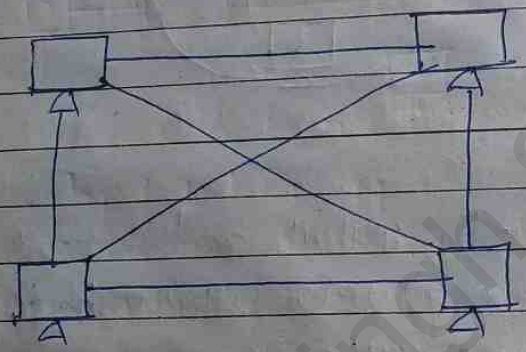
- Cheap to install and expand.
- Less chance of data collision. because of unidirectional data transmission.
- Each computer has equal access as there is no server.
- Better performance than bus topology.

Disadvantage

- Difficult for adding or removing new nodes.
- No suitable for large size network.
- Failure of one computer disturbs the whole network.
- Difficult to find errors.

1. Mesh Topology

Every computer in the network has point to point connection to all other computers by using multi port connector. The communication is done in both directions. It is also based on peer to peer architecture.



Advantages

- Fastest and robust type of topology.
- Failure of any node does not affect the entire network.
- Less data traffic due to multiple paths.
- Provides security and privacy.

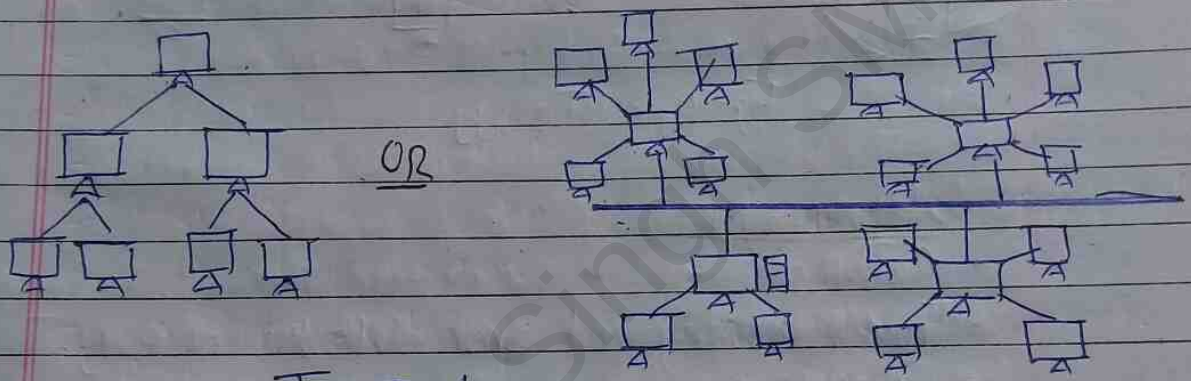
Disadvantages

- Complex and most expensive topology.
- Difficult to find error.
- Maximum amount of cables is required.

5. Tree Topology:

Tree topology is the extension of bus topology or star topology.

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should have at least three levels of hierarchy.



Tree Topology

Advantages

- Number of nodes can be added easily.
- Easier to find and detect error.

Disadvantages

- Failure of root node will cause failure of entire network.
- Expensive
- High data traffic.

6. Hybrid Topology

If two or more topologies are combined together then it is called hybrid topology.

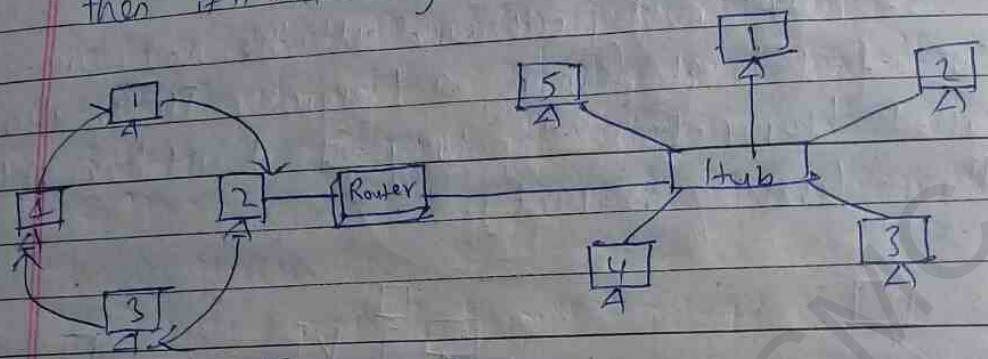


Fig: Hybrid Topology

Advantages

- Reliable
- Trouble shooting and error detection is easy.
- Flexible

Disadvantages

- Complex in design.
- Expensive

4.3. Types of Networks: Local area network, Wide area network, Personal area network

On the basis of geographical area that means how much area it covers, Computer networks are classified into following categories:

1. Local Area Network (LAN):

A computer network that is spread in a small local area is known as LAN. The network of computers within a room, building or campus is Local Area Network. A LAN is privately own small sized network.

Computers in LAN are usually connected with cables. The type of LAN where wireless media are used is called Wireless LAN or WLAN.

Features

- LAN is owned privately by a single organization.
- It covers very small area (upto 3 km)
- It has high data transmission rate usually 1 to 100 Mbps.
- Highly secured.
- Simpler and cheaper than other networking system.

2. Metropolitan Area Network (MAN).

A computer network that is bigger than LAN and smaller than WAN, is metropolitan area network. The network of computers within a ~~room~~ city or ~~neig~~ in between neighbouring cities is MAN. There may be larger numbers of LAN in a MAN. Eg: Cable Television.

Features of MAN:
- It can be either public or privately owned network.
- It covers larger area than MAN. Upto 100 km.
- It is slower than LAN. (Upto 10 Mbps)
- It is less secured and higher error rate than LAN.
- It is more expensive than LAN.
- It can connect 100's of LAN and 1000's of individual computers.
- It uses mesh or hybrid topologies.

3. Wide Area Network (WAN):
The network of computers within a country or continents is known as Wide Area Network. The WAN links computers of our country with computers of other countries like India, China America and Japan. The WAN covers very large geographical area i.e the whole world. The Internet is an example of WAN.

Features of WAN
- It is basically a public network.
- It covers very large area i.e whole world.
- It has low speed data transfer rate i.e 64 kbps to 10 mbps.
- It is less secured and has highest error rate.
- It is most expensive type of network.
- It can connect unlimited LANs and MANs.

4. Personal Area Network (PAN)

A PAN is a computer network organized around an individual person within a single building. This could be inside a small office or residence. A typical PAN would include one or more computers, telephones, peripheral devices etc.

If multiple individuals use the same network within a residence, the network is sometimes referred to as a home area network or HAN.

It covers very small area i.e 10 metres or 30 feet.

This type of network allows us to:

- Send a document to printer in the office.
- Upload a photo from our cellphone to desktop computer.
- Watch movies from an online streaming service on your TV.

5

9.9. Layered Network Model : OSI model, TCP/IP model

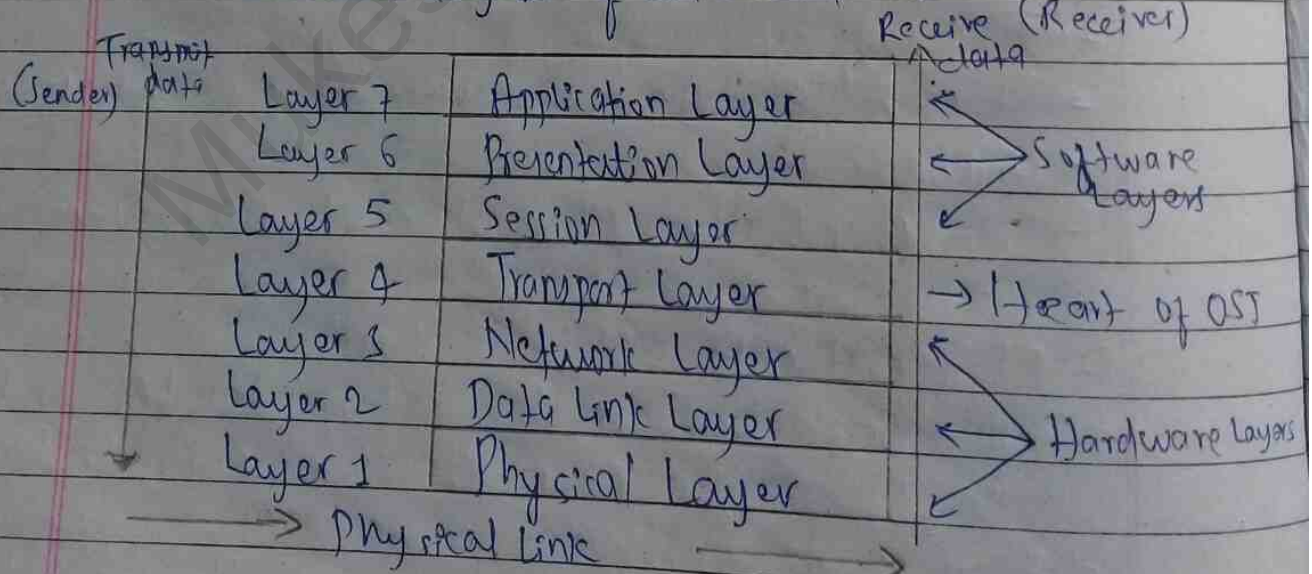
OSI model

OSI stands for Open System Interconnection. It has been developed by ISO in 1974.

Defn- An OSI reference model is a set of network ~~is~~ ISO certified model that entirely describes how information is transmitted from an application of one computer to another application of other computer.

The layers are divided into 3 groups: upper layer, middle layer and lower layer. The physical, data link and network layers belong to lower layer. Transport layer belongs to middle layer and the session, presentation & application layer belongs to upper layer.

The seven layers of OSI model are:



1. Physical Layer → It is the lowest layer of OSI model. It is responsible for actual physical connection between the devices. It is responsible for transmitting raw bits from one node to another over communication channel. This layer defines hardware, cabling wiring, power output, pulse rate etc.

2. Data Link Layer → It is responsible for moving frames from one node to another node. It also helps to detect errors that may occur in the physical layer.

3. Network Layer:→ It is responsible for delivery of packets from source host to destination host. It provides different facilities such as logical addressing, routing, switching etc.

4. Transport Layer → It is responsible for delivery of message from one application to another application. It divides the messages into blocks and transports them. It provides different facilities such as segmentation, connection control, flow control, error control etc.

5. Session Layer → This layer maintains sessions between hosts. It establishes, manages and terminates connection between applications. For example, once user/password authentication is done, the remote hosts maintains this session for a while and does not ask

for authenbication in that timespan.

6. Presentation Layer → It is also called translation layer or syntax layer. It is concerned with syntax and semantics of the information transmitted. It works to transform data into the form that the application layer can accept. It includes data connection and code translation (eg. ASCII to EBCDIC).

7. Application Layer → It is the uppermost layer. It allows application to access network services. It is completely user-oriented layer. Some of its functions are file transfer, accessing remote file, database, e-mail etc.

TCP/IP Model

TCP/IP stands for Transmission Control Protocol / Internet Protocol. This model was developed by the US Defense Advanced Research Project Agency (DARPA) for its packet switched network ARPANET in 1970s.

TCP/IP is a suite of communication protocol used to interconnect devices on the Internet. TCP/IP dictates how information should be packaged, sent and received as well as how to get to its destination.

This model has four layers:

Application Layer
Transport Layer
Internet Layer
Network Access Layer or Link Layer

1. Network Access Layer / Link Layer:

This layer corresponds to the combination of Data link layer and Physical Layer of the OSI ~~Layers of~~ model. This layer provides the mechanism of sending and receiving actual data.

2 Internet Layer → Internet Protocol (IP) works on this layer. to describe how packets are to be delivered. It defines the protocols which are responsible for logical transmission of data over the entire network.

3. Transport Layer → This layer utilizes UDP (User Datagram Protocol) and TCP to ensure the proper transmission of data. This layer defines how data should flow between hosts. It ensures data delivered between hosts in order and is responsible for end-to-end delivery.
Eg- Error control, flow control etc.

4. Application Layer → This layer contains the logic needed to support the various user applications. This layer defines the protocols which enables the user to interact with the network. for example: FTP, HTTP.
Presentation and Session Layer of OSI model are also incorporated in Application layer of TCP/IP model.

TCP/IP	OSI
1 TCP/IP refers to Transmission Control Protocol/Internet Protocol.	1. OSI refers to Open Systems Interconnection.
2 TCP/IP has 4 layers.	2 OSI has 7 layers.
3. TCP/IP is more reliable.	3. OSI is less reliable.
4 TCP/IP does not have strict boundaries.	4 OSI has strict boundaries.
5 It follows horizontal approach.	5 It follows a vertical approach.
6. Uses both session & presentation layer in the application layer itself.	6 Uses different session and presentation ~~and~~ layers.
7. TCP/IP developed protocols then model.	7. OSI developed model then protocols.

Unit-5

Internet Protocols

5.1. Introduction: History of Internet Protocols, Internet protocol stack, IP Addressing and Routing (Version 4), Subnetting: Fixed and Variable length, Unicast routing algorithms

History of Internet Protocols

The Internet, also known as Net, is a interconnection of millions of computers across the world by means of cables, telephone lines or wireless communication media. It is the largest network of computers in the world.

A protocol is a set of rules that manages the data communication.

The Internet Protocol (IP) is the method or protocol by which the data is sent from one computer to another on the Internet. Each computer ~~has~~ on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

History

Historically, IP was the connectionless datagram service in the original Transmission Control Program introduced by Vint Cerf and Bob Kahn in 1970, which was complemented by a connection-oriented service that became the basis for the Transmission Control Protocol (TCP). The Internet Protocol suite is therefore often reffered to as TCP/IP.

The first major version of IP, Internet Protocol

Version 4 (IPv4) is the dominant protocol of the Internet. Its successor, Internet Protocol Version 6 (IPv6), has been growing in adoption, reaching almost 25% of all Internet traffic as of October, 2018.

Internet Protocols Stack

Internet Protocol Stack is a set of network protocol layers that work together to allow software or hardware to perform a function.

The Internet Protocol stack consists of 5 layers: the physical layer, data link, network, transport and application layers.

	Stack	PDUs
Layer 5	Application Layer	message
Layer 4	Transport Layer	Segment
Layer 3	Network Layer	datagram
Layer 2	Data link Layer	frame
Layer 1	Physical Layer	1-PDU

Fig: The Protocol Stack & Protocol Data Units.

1. Physical Layer → Transfer the individual bits from one node to another the next node is with in the frame

2. Data Link Layer → Move the packets/frames from one node to the next node. Point-to-Point Protocol (PPP) used in data link layer.

3. Network Layer → Move packets between any two hosts in the network. IP protocol is used in network layer.

4. Transport Layer → Transfer the content/message between two endpoints mainly. TCP and UDP protocols are used in this layer.

5. Application Layer → It allows applications to access network services. It is used to send data over multiple end systems. HTTP, SMTP, and FTP protocols are used in this layer.

IP Addressing and Routing (Version 4)

IP Address

An Internet Protocol address (IP Address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.

OR, It is a logical address that should be unique for each device attached to a particular network.

The purpose of IP address is to allow communication between networks.

IP addresses are binary numbers but they are usually stored in text files and displayed in human readable notations, such as 172.16.254.1 (for IPv4) and 2001:db8:0:567:8:1 (for IPv6).

There are 5 classes of IP address with only first 3 being used commercially.
→ Class A: 1 to 127 (first octet)
→ Class B: 128 to 191 (first octet)
→ Class C: 192 to 223 (first octet)
→ Class D: used for multicasting 224-239
→ Class E: used for experimental purposes. 240-255

IP Routing:

IP routing is the process of sending/transporting data or packets from source to destination on a determined path across two or more networks. The process is usually done by routers.

1. IPv4:

IPv4 is a connectionless protocol used for packet switched networks such as Ethernet. As its name implies, it is the fourth version of the Internet Protocol. IPv4 was the first version of IP. It was deployed for production in the ARPANET in 1983. Today, it is most widely used IP version. It is used to identify devices on a network using an addressing system.

The IPv4 uses 32-bit address scheme allowing to store 2^{32} addresses which is more than 4 billion addresses. Till data, it is considered the primary Internet Protocol and carries 94% of Internet traffic.

Features
- Connectionless Protocol
- Requires less memory, and ease of remembering addresses.
- Already supported protocol by millions of devices.
- Offers wider libraries and Conferences.

2# IPv6

It is the enhanced and the most recent (newest) version of the Internet Protocol and is considered the successor to IPv4. Internet Engineer Task Force (IETF) initiated it in early 1994. The design and development of that suite is now called IPv6.

IPv6 is better than IPv4 in terms of complexity and efficiency. It was aimed to resolve issues which are associated with IPv4. It was developed in hexadecimal format and contains 8 octets to provide large scalibility. With 128-bit address space, it allows 340 undecillion unique address space. Its main aim is to provide online users with a more diverse range of IP addresses. IPv6 is also called ~~IPng~~ Internet Protocol Next Generation (IPng).

Features
- Hierarchical addressing and routing infrastructure
- Stateful and stateless configuration
- Support for quality of service (QoS)
-

IPv4	IPv6
1. IPv4 is a 32-bit IP Address.	1. IPv6 is 128-bit IP Address
2. It is a numeric address.	2. It is an alphanumeric address.
3. Its binary bits are separated by a dot (.).	3. Its binary bits are separated by colon (:).
4. It has a decimal format.	4. It has a hexadecimal format.
5. Number of header fields is 12	5. Number of header fields is 8.
6. Length of header field is 20.	6. Length of header field is 40.
7. Has checksum fields.	7. Does not have checksum fields.
8. Fragmentation is done by sending and forwarding routers.	8. Fragmentation is done by the sender.
9. Example: 172.244.233.165	9. Example 2001:0db8:0000:0000:00

Subnetting

Subnetting is the practice of dividing a network into two or more smaller networks. It increases routing efficiency, enhances the security of the network and reduce the size of the broadcast domain.

Subnetting allows an organization to add sub-networks without the need to acquire a new network number via the ISP.

Each IP address consists of a subnet mask. All classes types such as Class A, class B and class C include the ~~default~~ subnet mask known as default subnet mask. The default subnet mask is as follows:

- Class A : 255.0.0.0
- Class B : 255.255.0.0
- Class C : 255.255.255.0

The subnetting process allows the administrator to divide a single class ~~into~~ A, class B, or class C network into smaller portions.

Benefits

- Reduces network traffic
- Network Security

1. Fixed-length Subnet Mask (FLSM):

A FLSM is a sequence of numbers of unchanging length that streamlines packet routing within the subnets of a proprietary network.

- All subnets are equal.
- All subnets have equal number of hosts.
- All subnets use same subnet mask.
- It is easy in configuration and administration.
- It is also known as classful subnetting.
- It wastes lots of IP addresses.

2 Variable-length subnet Mask (VLSM):

Instead of forcing us to use a fixed size for all segments, it allows us to choose the individual size for each segment in VLSM.

- All subnets are may not be equal.
- Reduces the IP wastage.
- We can choose size of subnet according to requirement.

Routing algorithm:

A routing algorithm is a set of step-by-step operations used to direct Internet traffic efficiently. When a packet of data leaves its source, there are many different paths it can take to its destination. The routing algorithm is used to determine mathematically the best path to take.

Unicast routing algorithms:

Unicast means the transmission from a single sender to a single receiver. It is a point to point communication between sender and receiver. There are various unicast protocols such as TCP, HTTP, etc.

Routing unicast data over the internet is called unicast routing. It is the simplest form of routing because the destination is already known. Hence the router just has to look up the routing table and forward the packet to next hop.

5.2 Transport Layer Protocols : TCP and UDP

The transport layer is the fourth layer of the OSI reference model. The transport layer is essentially responsible for delivering data to the appropriate application on the host computer. It receives requests from the application layer protocols and passes them down to the Internet/Network layer.

The transport layer is represented by two protocols:

1. TCP
2. UDP

1. TCP

- TCP stands for Transmission Control Protocol.
- It provides full transport layer services to applications.
- It is a connection-oriented reliable protocol. It means the connection is established between both the ends of the transmission.
- For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

Advantages/Features of TCP protocol:

- Stream data transfer
- Reliability
- Flow Control
- Multiplexing
- Logical Connections
- Full duplex

2 UDP:

- UDP stands for User Datagram Protocol.
- UDP is a simple protocol and it provides nonrequenced transport functionality.
- UDP is a connectionless protocol.
- This type of protocol is used when reliability and security are less important than speed and size.
- UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
- The packet produced by the UDP protocol is known as a user datagram.

Disadvantages of UDP Protocol:

- Provides only the basic functions for end-to-end delivery & transmission.
- Does not provide any sequencing or reordering functions.

TCP	UDP
1. TCP establishes a virtual circuit before transmitting the data.	1. UDP transmits the data directly to the destination computer without verifying whether the receiver is ready to receive or not.
2. It is a connection oriented protocol.	2. It is a connectionless protocol.
3. Speed is slow.	3. Speed is high.
4. It is a reliable protocol.	4. It is unreliable protocol.
5. Header size is 20 bytes.	5. Header size is 8 bytes.
6. It waits for the acknowledgement of data and has the ability to resend the lost packets.	6. It neither takes the acknowledgement, nor it retransmits the damaged frame.

5.3. IP Support Protocols: ARP, DHCP and ICMP

The Internet protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries.

IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers.

Following are the types of IP protocols:

1. ARP Protocol
   - ARP stands for Address Resolution Protocol.
   - ARP is a network layer protocol which is used to find the physical address from the IP address.
   - The two terms are mainly associated with the ARP protocol:

• ARP request → When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.

• ARP reply → Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and send back its physical address in the form of ARP reply. The recipient adds the physical address to both to its cache memory and to the datagram header.

2 DHCP Protocol

- DHCP stands for Dynamic Host Configuration Protocol.
- DHCP is a network management protocol used to dynamically assign an IP address to any device or node on a network so that they can communicate using IP.
- There is no requirement for any user configuration to connect to a DHCP based network.
- DHCP can be implemented on local networks as well as large enterprise networks.
- DHCP manages the provision of all the nodes or devices added or dropped from the network.
- It is based on client - server protocol.
- It sends a request to DHCP server whenever a client/node, which is configured to work with DHCP, connects to a network.

The server acknowledges by providing an IP address to the client/node.

3. ICMP Protocol

- ICMP stands for Internet Control Menage Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router to router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that datagram is undeliverable.

- The core responsibility of ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- An ICMP protocol mainly uses two terms:

• ICMP Test - ICMP test is used to test whether the destination is reachable or not.

• ICMP Reply → ICMP reply is used to check whether the destination device is responding or not.

5.4 Application Layer Protocols : Domain Name System (DNS), Email - SMTP, POP, IMAP, FTP, HTTP, RTP and VOIP.

The Application layer is present at the top of the OSI model. It is the layer through which users interact. It provides services to the user.

An Application layer protocol defines how application processes (clients and servers), running on different end systems, pass message to each other.

Application layer protocols can be broadly divided into two categories:
- Protocols which are used by users. for eg: email
- Protocols which help and support protocols used by users. for eg: DNS.

1. Domain Name System (DNS)

DNS is the way that internet domain names are located and translated into internet protocol (IP) addresses.

Or, DNS is a hierarchical and decentralized naming system for computers, services, or other resources connected to the internet or a private network.

- DNS works on Client Server model.
- It is used to locate a resource easily over a network.

Email:

2 SMTP
- SMTP stands for Simple Mail Transfer Protocol.
- It deals with electronic mail service.
- It is used to transfer electronic mail from one user to another using TCP connections.
- When a mail server sends mail (to other mail servers), it acts as an SMTP client.
- When a mail server receives mail (from other mail server), it acts as an SMTP server.

3. POP
- POP stands for Post Office Protocol (or POP3)
- POP is also called as POP3 protocol.
- POP is a simple mail retrieval protocol used by User Agents (client email software) to retrieve mails from the mail server.
- When a user connects to the mail server to retrieve his mail, the messages are downloaded from mail server to the users hard disk.

4. IMAP →
- IMAP stands for Internet Message Access Protocol.
- IMAP is an Internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection.
- IMAP support multiple logins.
- It allows ~~a user~~ end user to simultaneously connect to the email server with different devices.

5. FTP
- FTP stands for File Transfer Protocol.
- It's the most widely used protocol for file transfer over the network.
- It's used to transfer file from one host to another using TCP/IP communication.
- FTP works on client/server model.
- A client requests file from server and the server sends requested resource back to the client.
- FTP uses two connections between hosts:
  ① Data Connection for data transfer.
  ② Control Connection for control information (commands and responses).

6. HTTP

- HTTP stands for Hyperfext Transfar Protocol.
- It is a protocol used mainly to access data on the World wide Web.
- It works on client/server model.
- Hypertext is well organized documentation system which uses hyperlinks to link the pages in the text documents.
- HTTP protocol transfer data in the form of plain text, hyper text, audio, video and so on.
- HTTP utilizes TCP connections to send client requests and server replies.

7. RTP

- RTP stands for Real-time Transport Protocol
- RTP is a network protocol for delivering audio and video over IP networks.
- It is used in communication and entertainment systems that involves streaming media, such as telephony, video teleconference, television services etc.
-

8. VOIP

- VoIP stands for Voice Over Internet Protocol.
- It is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol networks, such as the Internet.

Unit-6

Local Area Networks

Ajanta
Page No.
Date

6.1 Introduction to LANs

A computer network that is spread in a small area is known as LAN. The network of computers within a room, building or campus is Local Area Network. A LAN is privately owned small sized network.

Computers in LANs are usually connected with cables. The type of LAN where wireless media are used is called wireless LAN or WLAN.

Features

- LAN is owned privately by single organization.
- It covers very small area (up to 3 km).
- It has high data transmission rate usually 1 to 100 Mbps.
- Highly secured.
- Simpler and cheaper than other networking system.

6.2 Conventional LAN Architectures: Access Protocols (CSMA/CD*, Token Passing), Interconnecting devices (Hubs, L2/L3 Switch)

Access Protocols:

Access Control Protocol is the technology used to authenticate a user logging into a computer or network.

Multiple access protocols are required to decrease collision and avoid crosstalk.

Some multiple access protocols are described below:

i) CSMA - Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium before transmitting data. If it is idle (busy) then it sends data, ~~before~~ otherwise it waits till the channel becomes idle. However, there is still chance of collision in CSMA due to propagation delay.

ii) CSMA/CD → Carrier Sense Multiple Access with Collision detection. Stations can terminate transmission of data if collision is detected.

iii) CSMA/CA → Carrier Sense Multiple Access with Collision Avoidance. The process of collision detection involves sender receiving acknowledgement signals. If there is only one signal (its own) then the data is successfully

sent but if there are two signals (its own and the one with which it has collided) then it means a collision has occured.

iv) Token Passing: (Token Ring)

Token passing is a channel access method where a signal called a token is passed between nodes to authorize that node to communicate.

The stations are connected logically to each other in the form ring and access of stations is governed by tokens.

A token is a special bit pattern or a small message, which circulate from one station to the next in the some predefined order.

Interconnecting Devices:

Interconnecting devices are physical devices which are required for communication and interaction between devices on a computer network.

Some interconnecting devices are:

i) Hub

A hub is the most basic networking device that connects multiple computers or other network devices together. A hub is basically a multiport repeater. It is used to connect multiple computers to a server in LAN. It is generally used in star topology.

There are three types of hub:

a) Active hub b) Passive hub c) Intelligent hub

ii) Switch

Switch is also a multiport network connecting device which helps to connect multiple computers to a server in a LAN. It is generally used in star topology. But it works on layer of two of OSI reference model. Hub work on half-duplex mode where as switch works on full-duplex mode. It's functionality is same as bridge so switch is also known as multiport bridge.

iii) Bridge

A bridge is a network connecting device, which interconnects two networks that use the same technology and protocol. It creates a single aggregate network from multiple communication networks. A bridge can segment a network into two networks in order to isolate network traffic problem. It works upto layer 2 of OSI reference model.

There are 3 types of bridges.

a) Local Bridge b) Remote Bridge
c) Wireless Bridge

iv) Repeater

Repeater is a networking device that amplifies or regenerates electric signals.

Repeater is a signal amplifier device ~~that~~ used to amplify weak signal into its original signals. Repeaters can regenerate the weak signals so that they can travel more cable length.

~~vi) Gateway~~

v) Router

Router is a networking device designed to receive, analyze and move incoming packets to another network. It is highly intelligent and protocol sensitive linking device used to connect two different LANs or WANs. It works upto layer 3 of OSI reference model.

vi) Gateway

A gateway is a network connecting device which connects two different network protocols together which may be LANs and WANs or two different LANs. It is much more complex and powerful than routers. It works upto layer 4 of OSI reference model.

vii) Modem

Modem stands for Modulator and Demodulator. It is an electronic device which translates data from digital to analog and vice-versa. Modulation is

the conversion of digital data into analog data and the reverse process is called demodulation. Modem is used to connect internet via telephone lines which uses analog signals whereas the computer uses digital signals.

viii) NIC

A network interface card (NIC) is an interface for connecting the computer to the network devices through communication media. It is also known as network adapter. It is basically a circuit board that is built inside the main board of computer. It works on layer 2 of OSI reference model.

ix)

6.3 IEEE 802 MAC layer standards : 802.3, 802.11, 802.15

In IEEE 802 LAN/MAN standards, the Medium Access Layer (MAC) sublayer is the layer that controls the hardware responsible for interaction with the wired, optical or wireless transmission medium. The MAC sublayer and the logical link control (LLC) sublayer together make up the data link layer.

i) IEEE 802.3 Ethernet

- 802.3 of IEEE is Ethernet based network.
- It is the standard for CSMA/CD (Carrier Sense Multiple Access with Collision Detection).
- This standard defines both the physical layer and MAC layer of the data link layer.
- The original 802.3 standard is 10 Mbps, 802.3u defined the 100 Mbps standard (Fast Ethernet), 802.3z/802.3ab defined 1000 Mbps (Gigabit Ethernet) and 802.3ae defined 10 Gigabit Ethernet.
- The most common topology for Ethernet is star topology.

ii) IEEE 802.11 Wireless Network Standards

- IEEE 802.11 refers to the set of standards that define communication for wireless LANs.
- The technology behind 802.11 is overseen by the IEEE branded to consumers as Wi-Fi.
- It has three popular standards 802.11a, 802.11b

802.11g and latest one is 802.11n.
- ~~802.11a is cable of transmission of up to 54 Mbps~~
- 802-11 a operates in 5GHz radio band and can achieve maximum of 54 Mbps.
- 802-11b operates in 2.4GHz band and supports upto 11 Mbps.
- 802.11g operates in 2.4, 3.6 and 5GHz bands and can achieve maximum of 20 Mbps.
- 802.11n operates in 2.4GHz and 5GHz bands. ~~and~~

- Wireless LANs primarily use CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance).

iii) ~~802.1~~ IEEE 802.15
- IEEE 802.15 is the IEEE working group for Wireless Personal Area Networks (WPANs).
- The working group is developing standards for short-range communications of devices within a personal operating space. A personal wireless network consists of mobile devices such as a handheld or pocket computer, PDA, mobile phone and wireless microphone.

IEEE 802.15 consists of following workgroups:
- 802.15.1 (Standardization Task Group)
  → Standardization of bluetooth.
- 802.15.2 (Recommended Practice)
  → Co-existence of WPAN and WLAN devices.

- 802.15.3 (High rate WPAN)
  - → High rate (> 20 Mbps) WPANs
- 802.15.4 (Low rate WPAN)
  - → Low-rate (upto 200 kbps) WPANs
    - → Standardization of ZigBee.

6.4. Switched Ethernet Variants: Fast Ethernet, Gigabit Ethernet ~~and~~, 10 Gb Ethernet

Ethernet is very common method of networking computers in LAN using copper cabling.

There are various switched ethernet variants:

1. Fast Ethernet:

The Fast Ethernet standard (IEEE 802.3u) has been established for Ethernet networks that need higher transmission speeds.

It is type of Ethernet network that can transfer data at the rate of 100 Mbps using a twisted-pair cable or fiber-optic cable.

Fast Ethernet is based on the proven CSMA/CD Media Access Control (MAC) protocol and uses existing 10Base T cabling.

There are ~~th~~ 3 types of fast Ethernet:

i) 100 BASE-Tx for use with level 5 UTP cable;

ii) 100 BASE-Fx for use with fiber-optic cable;

iii) 100 BASE-T4 which utilizes an extra two wires for use with level 3 UTP.

2. Gigabit Ethernet

The Gigabit Ethernet standard (IEEE 802.3 ab) was developed to meet the need for faster communication networks with applications such as multimedia and voice over IP (VoIP).

- It is a type of Ethernet network capable of transferring data at a rate of 1000 Mbps based on twisted-pair cable or fiber-optic cable.
- 48 bits used for addressing in Gigabit Ethernet.

3) 10 Gigabit Ethernet

The 10 Gigabit Ethernet standard (IEEE 802.3ae) is the fastest and most recent of the Ethernet standards.

It is type of Ethernet network capable of transferring data at a rate of 10 Gbps using twisted-pair or fiber-optic cable.

It is 10 times faster than Gigabit Ethernet.

6.5 Wireless LANs (802.11): Access methods (CSMA/CA), Frequency Bands (ISM), Operating Modes (adhoc, Managed), Variants (802.11 a/b/g/n), Wireless interconnection devices (Hub, Router).

Wireless local Area Network (WLAN) is a network that allows devices to connect and communicate wirelessly.

Most modern WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name.

Access methods (CSMA/CA) → Wireless LANs primarily use CSMA/CA (Carrier sense Multiple Access / Collision Avoidance) access methods for path sharing.

Frequency bands (ISM) →

The 802.11 standard provides several distinct radio frequency bands for use in Wi-Fi communications: 900 MHz, 2.4 GHz, 3.6 GHz, 4.9 GHz, 5 GHz, 5.9 GHz and 60 GHz bands.

Within these bands there are many channels designated with numbers so that they can be identified.

ISM bands:

ISM stands for Industrial, Scientific and Medical. These bands have been internationally

agreed and unlike most other bands, they can be used without the need for a transmitting license. This gives access to everyone to use them freely.

ISM bands are available globally, there are some differences and restrictions that can occur in some countries.

Some ISM bands are : 2.4 GHz band (2400 - 2500 MHz), 5 GHz band / 5.8 GHz band (5725 - 5875 MHz) etc.

Operating Modes (adhoc, managed):

The 802.11 standards defines two operating modes : infrastructure mode and adhoc mode.

In infrastructure mode, wireless clients are connected to an access point. This is generally the default mode for 802.11 b cards.

In adhoc mode, clients are connected to one another without any access point.

Variants (802.11 a/b/g/n)

There are several variants in 802-11 a family:

- 802.11 a → Operates in 5 GHz radio band and can achieve a maximum of 54 Mbps.
- 802.11 b → Operates in 2.4 GHz band and supports upto 11 Mbps.
- 802.11 g → Operates in 2.4, 3.6 and 5 GHz bands and can achieve maximum of 54 Mbps.

- 802.11 n → Operates in 2.4 GHz and 5 GHz bands and can achieve ~~upto~~ speed upto 100 Mbps.

6.6. Bluetooth (802.15) wireless personal area network

IEEE 802.15 is the IEEE working group for Wireless Personal Area Networks (WPANs). A personal wireless network consists of mobile devices such as Tablet, PDA, mobile phone and wireless microphone.

IEEE 802.15 consists of following task/work groups:

- IEEE 802.15.1 (Bluetooth)

Task group one is based on Bluetooth technology. It defines physical layer (PHY) and Media Access Control (MAC) specification for wireless connectivity with fixed, portable and moving devices within or entering personal operating space. Standards were issued in 2002 and 2005.

Unit-7

Practical Aspects of Networking

7.1. Structured cabling and specifications : Standards CAT 5, 5E, CAT 6 etc

Structured cabling is building or campus cabling infrastructure that consists of a number of standardized smaller elements called subsystems.

Structured cabling is the design and installation of a cabling system that will support multiple hardware uses and be suitable for todays needs and those of future.

CAT 5 (Category 5) cable

Category 5 cable, commonly referred to as Cat 5, is a twisted pair cable for computer networks.

It is a type of cable that is used extensively in Ethernet connections in local networks, as well as telephony and other data transmissions.

Category 5 cable employes a twisted pair design, rather than a coaxial or fiber-optic cable design.

- Cat 5 has a maximum length of 100 m.
- It provides performance of up to 100 MHz.
- CAT 5 cable contains four pairs of copper wire supporting fast Ethernet speeds (upto 100 Mbps).

CAT 5E (Category 5 enhanced) Cable

The EIA/TIA (Electronics Industries Association and Telecommunication Industry Association) published a newer category of 5 cable specification in 2001 called CAT 5E (or CAT 5 enhanced).

It is designed to support better Gigabit Ethernet speeds (up to 1000 Mbps) by using all four wire pairs.

CAT 6 (Category 6) Cable:

Category 6 cable, commonly referred to as Cat6, is a standardized twisted pair cable for Ethernet and other network physical layers that is backward compatible with the category 5/5e cable standards.

It is specifically used in Gigabit Ethernet based computer networks (speed up to 10 Gbps)

- It consists of four pairs copper wires.
- Provides bandwidth of 250 MHz and may be stretched up to 100 metres in length.
- Cat 6 is supported by Ethernet networks, including 10 Base T, 100 Base-Tx, 1000 Base-T and 10 GBase-T.

CAT 6a (Category 6 Augmented) Cable :

Cat 6a is the latest iteration of Gigabit Ethernet cabling.

The Cat 6a doubles data transmission from 250 to 500 MHz.

It decreases the chance of crosstalk interference and provides superior reliability and transmission speeds through greater lengths of cable.

It has data transfer rate of upto 10 Gbps (10 Gb Ethernet).

It is backward compatible with CAT 6 and CAT 5E.

CAT 5	CAT 5E
1. Frequency upto 100 MHz	1. Frequency upto 100 MHz.
2. Cheaper in cost than 5E	2. Expensive than CAT 5.
3. More chance of crosstalk / interference.	3. Less chance of crosstalk / interference.
4. Maximum cable length is 100 metres	4. Maximum cable length is 100 metres.
5. Speed upto 100 Mbps.	5. Speed upto 1000 Mbps.
6. Supports 100 BASE-T network	6. Supports 1000 BASE-T network.

CAT 6	CAT 6A
1. Cost is 20% higher than Cat 5e.	1 Cost is 20-35% higher than Cat 6.
2 Frequency upto 250 MHz.	2 Frequency upto 500 MHz.
3. Max cable length is 100 metres	3 Max cable length is 100 metres
4 Speed upto 1 Gbps. (10 Gbps upto 33-55 metres)	4 Speed upto 10Gbps over 100 metres.
5. Supports 1000BASE-TX network	5. Supports 10GBASE-T network

7.2 Network Security: Firewalls and NAT, VLANs, VPNs, Proxy Servers, Wireless Security

Network security is the process of taking preventive measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction or improper disclosure.

Network security is any activity designed to protect the usability, integrity and accessibility of computer networks and data using both software and hardware technologies.

Types of network security are as follows:

i) Firewalls:

A firewall is a network security system that manages and regulates the network traffic based on some protocols. A firewall establishes a barrier between a trusted internal (private) network and the Internet. Firewalls are commonly used in private networks or intranets to prevent unauthorized access from the internet. It acts as a gatekeeper, deciding what enters and exits the network. A firewall can be hardware, software or both.

ii) NAT

NAT stands for Network Address Translation. It is a router function that enables public and private network connections and allows single IP address communication. While there are many public

networks worldwide, there is a limited number of private networks. NAT was introduced as an effective, timely solution to heavy network volume traffic.

iii) VLANs:

A Virtual Local Area Network is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution. A VLAN allows several network to work virtually as one LAN.

VLANs are implemented to achieve scability, security, increase network efficiency, ease of network management, to remove latency in network.

iv) VPNs:

A Virtual Private Network (VPN) is a private network that is built over a public infrastructure.

Security mechanisms such as encryption, allow VPN users to securely access a network from different locations via a public telecommunications network, most frequently the Internet.

The key advantage of VPN is that it is less expensive than a private WAN buildout.

v) Proxy Servers:

A proxy server is a server (computer system or application) that acts as an intermediary for requests ~~~~ from clients seeking resources from other servers.

A proxy server verifies and forwards incoming client requests to other server for further communication

- A proxy server is located between a client and a server when it acts as an intermediary between the two, such as Web browser and a Web Server.

Main role of proxy server is to provide security.

Purposes

- To provide internal system security.
- To speed up resource access.
- To scan for viruses and malware.

ii) Wireless Security:

Wireless network security is the process of designing, implementing and ensuring security on a wireless computer network. It is a subset of network security that adds protection for a wireless computer network.

Wireless security primarily protects a wireless network from unauthorized and malicious access attempts. Cybercriminals are increasingly targeting mobile devices and apps. So, you need to control which devices can access your network.

7.3. User access technologies: Wired (xDSL, FTTH), Cellular wireless (GPRS, EDGE, HSPDA), Broadband wireless (802.16)

Wired

① xDSL:

xDSL refers to the sum total of digital subscriber line (DSL) technologies. Line length limitations on DSL signal transmissions from the telephone exchange speeds have resulted in the many types of DSLs.

Some examples of DSL technologies (xDSL) are:

- Digital subscriber line (DSL)
- Integrated Service Digital Network (ISDN)
- Asymmetric Digital subscriber line (ADSL)
- Gigabit Digital subscriber line (GDSL) etc

② FTTH

Fiber to the home (FTTH), also called "fiber to the Premises" (FTTP), is the delivery of a communication signal over optical fiber from the operator's switching point (central) all the way to a home or business to provide unprecedented high-speed internet access.

FTTH is a relatively new and fast growing method of providing vastly higher bandwidths to consumers and business, and thereby enabling more robust video internet

and voice services.

Cellular wireless

① GPRS:

General Packet Radio Service (GPRS) is a packet-based mobile data service ~~over standard on the~~ on the global system for mobile communication (GSM) of 2G and 3G cellular communication systems. It is a non-voice, high-speed and useful packet-switching technology intented for GSM networks.

② ~~EDGE~~ EDGE:

EDGE is also known as Enhanced GPRS or EGPRS. ~~EDGE stands~~

Enhanced Data rates for GSM Evolution (EDGE). OR Enhanced Data Rates for Global Evolution (EDGE). It a digital mobile phone technology that allows improved data transmission rates as a back-compatible extension of GSM.

EDGE can be used for any ~~dat~~ packet switched application such as Internet connection.

It is also considered as 3G network. It was developed in 2003 and originally implemented by Cingular.

It is 3 times faster than GPRS. It has average speed of 75 to 135 kbps. It can attain maximum of 473.6 kbps.

(iii) HSDPA:

High-Speed Downlink Packet Access is a packet-based mobile telephony protocol used in 3G UMTS radio networks to increase data capacity and speed up transfer rates.

It is an enhanced 3G mobile communications protocol in the High Speed Packet Access (HSPA) family. HSDPA is also known as 3.5G, 3G+ or Turbo 3G.

Current HSDPA deployments support downlink speeds of 1.8 Mbps, 3.6 Mbps, 7.2 Mbps and 14.4 Mbps

UMTS = Universal Mobile Telecommunication System
HSUPA = High-Speed Uplink Packet Access.

Broadband Wireless:

(2) ~~802.16~~

Wireless Broadband is a telecommunication technology that provides high-speed wireless Internet access or computer networking access over a wide area.

802.16

802.16 is a group of broadband wireless communication standards for Metropolitan area networks (MANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE).

It uses a ~~real~~ point-to-multipoint architec