Data Communication and Computer Network

(Code : 22414)

SECOND YEAR DIPLOMA

Maharashtra State Board of Technical Education (MSBTE)

Semester IV – Computer Engineering Group (CO/CM/IF/CW)

Strictly as per new revised 'I' Scheme w.e.f. academic year 2018-2019

J. S. Katre

M.E. (Electronics and Telecommunication)

Formerly, Assistant Professor

Department of Electronics Engineering

Vishwakarma Institute of Technology (V.I.T.), Pune.

Maharashtra, India

TechKnowledge™ Publications

MDE28D Price ₹ 345/-

Data Communication and Computer Network (Code : 22414)

(Semester IV – Computer Engineering Group (CO/CM/IF/CW), MSBTE)

J. S. Katre

First Printed in India : January 2001
First Edition : January 2019 **(As per 'I' Scheme)**
Second Revised Edition : January 2020 **(TechKnowledge Publications)**
Third Revised Edition : February 2021
Fourth Revised Edition : March 2022
Fifth Revised Edition : January 2023

ISBN : 978-93-89503-99-9

Published by :

TechKnowledge Publications

Head Office : B/5, First floor, Maniratna Complex, Taware Colony, Aranyeshwar Corner, Pune - 411 009. Maharashtra State, India

Ph : 91-20-24221234, 91-20-24225678.

Email : info@techknowledgebooks.com,

Website : www.techknowledgebooks.com

[22414] (FID : MDE28) (Book Code : MDE28D)

We dedicate this Publication soulfully and wholeheartedly,

in loving memory of our beloved founder director,

Late Shri. Pradeepji Lalchandji Lunawat,

who will always be an inspiration, a positive force and strong support

behind us.

"My work is my prayer to God"

– Lt. Shri. Pradeepji L. Lunawat

Soulful Tribute and Gratitude for all Your

Sacrifices, Hardwork, and 40 years of Strong Vision...

Syllabus...

DCCN : Sem. IV (Computer Engineering Group (CO/CM/IF/CW), MSBTE)

Unit	Topics and Sub-topics
Unit - I : Fundamentals of Data Communication and Computer Network **Refer chapters 1 and 2**	1.1 Process of data communication and its components : Transmitter, Receiver, Medium, Message, Protocol. 1.2 Protocols, Standards, Standard organizations. Bandwidth, Data transmission rate, Baud rate and Bits per second. 1.3 Modes of communication (Simplex, Half duplex, Full duplex). 1.4 Analog signal and digital signal. Analog and digital transmission : Analog to digital, Digital to analog conversion. 1.5 Fundamentals of computer network, Definition and need of computer network, Applications, Network benefits. 1.6 Classification of network LAN, MAN, WAN. 1.7 Network architecture : Peer-to-Peer network, Client-server network.
Unit - II : Transmission Media and Switching **Refer chapters 3, 4 and 5**	2.1 Communication Media : Guided transmission media, Twisted pair cable, Co axial cable, Fiber optic cable. 2.2 Unguided transmission media, Radio waves, Microwaves, Infrared, Satellite. 2.3 Line of sight transmission, Point to point, Broadcast. 2.4 Multiplexing : Frequency Division Multiplexing, Time division multiplexing. 2.5 Switching : Circuit switched networks, Packet Switched networks.
Unit - III : Error Detection, Correction and Wireless Communication **Refer chapters 6 and 7**	3.1 Types of errors : Single bit error and burst error, Redundancy. 3.2 Error Detection : Longitudinal redundancy check (LRC), Vertical redundancy check (VRC), Cyclic redundancy check (CRC), Forward error correction. 3.3 IEEE standards : 802.1, 802.2, 802.3, 802.4, 805.5. 3.4 Wireless LANs : 802.11 Architecture, MAC sublayer, Addressing mechanism. 3.5 Bluetooth architecture : Piconet, Scatternet. 3.6 Mobile generations : 1G, 2G, 3G, 4G and 5G.

Unit	Topics and Sub-topics
Unit - IV : Network Topologies and Network Devices **Refer chapters 8 and 9**	4.1 Network topologies : Introduction, Definition, Selection criteria, Types of topology : 1. Bus 2. Ring 3. Star 4. Mesh 5. Tree 6. Hybrid. 4.2 Network connecting devices : Hub, Switch, Router, Bridge, Repeater, Gateway, Modem, Wireless infrastructure components.
Unit - V : Reference Models **Refer chapters 10, 11 and 12**	5.1 OSI reference model : Layered architecture, Peer-to-Peer Processes-Interfaces between layer, Protocols, Organization of the layers, Encapsulation layers of the OSI reference model (Functions and features of each layer and protocols used), Physical layer, Data-Link layer, Network layer, Transport layer, Session layer, Presentation layer, Application layer. 5.2 TCP/IP model : Layered architecture, Data link layer : Nodes and links, Services, Two categories of links, Two sublayers, Link layer addressing, Three types of addresses, Address resolution protocol (ARP), Network layer : Addresses : Address space, Classful and classless addressing, Dynamic host configuration protocol (DHCP), Network address resolution (NAT), Transport layer protocol : Transport layer services, Connectionless and connection oriented protocol. 5.3 Introduction, Addressing mechanism in the Internet IP addressing : IP address classes, Classless IP addressing, Subnetting, Supernetting, Masking. 5.4 IPv4 and IPv6. 5.5 OSI and TCP/IP network model.

□□□

Unit – I

Chapter 1 : Fundamentals of Data Communication 1-1 to 1-24

Syllabus : Process of data communication and its components : Transmitter, Receiver, Medium, Message, Protocol, Protocols, Standards, Standard organizations, Bandwidth, Data transmission rate, Baud rate and Bits per second. Modes of communication (Simplex, Half duplex, Full duplex). Analog signal and digital signal, Analog and digital transmission : Analog to digital, Digital to analog conversion.

Unit – I

Syllabus : Fundamentals of computer network, Definition and need of computer network, Applications, Network benefits-Classification of network LAN, MAN, WAN, Network architecture : Peer-to-Peer network, Client-server network.

Syllabus : Network topologies - Introduction, Definition, Selection criteria, Types of topology : 1. Bus 2. Ring 3. Star 4. Mesh 5. Tree 6. Hybrid.

Syllabus : Network connecting devices – Hub, Switch, Router, Bridge, Repeater, Gateway, Modem, Wireless infrastructure components.

Syllabus : OSI reference model : Layered architecture, Peer-to-Peer Processes-Interfaces between layer, Protocols, Organization of the layers, Encapsulation layers of the OSI reference model (Functions and features of each layer and protocols used) - Physical layer, Data-Link layer, Network layer, Transport layer, Session layer, Presentation layer, Application layer.

Syllabus : Layered architecture, Data link layer : Nodes and links, Services, Two categories of links, Two sublayers, Link layer addressing, Three types of addresses, Address resolution protocol (ARP), Network layer : Addresses : Address space, Classful and classless addressing, Dynamic host configuration protocol (DHCP), Network address resolution (NAT), Transport layer protocol : Transport layer services, Connectionless and connection oriented protocol.

Syllabus : Introduction, Addressing mechanism in the Internet IP addressing - IP address classes, Classless IP addressing, Subnetting, Supernetting, Masking, IPv4 and IPv6, Comparison of OSI and TCP/IP network models.

❑❑❑

Chapter 1

Fundamentals of Data Communication

Syllabus

Process of data communication and its components : Transmitter, Receiver, Medium, Message, Protocol, Protocols, Standards, Standard organizations. Bandwidth, Data transmission rate, Baud rate and Bits per second. Modes of communication (Simplex, Half duplex, Full duplex). Analog signal and digital signal, Analog and digital transmission : Analog to digital, Digital to analog conversion.

Chapter Contents

1.1 Data :

- Data is defined as information which is stored in the digital form. A single data unit is called as datum.
- Data communication is the process of exchanging the digital information between two points.

1.1.1 Type of Data :

- Data can correspond to alphabets, numeric or symbols and it consists of any one or the combination of the following : microprocessor OPcodes, control codes, user addresses, program data or data base information.
- At the source or destination the data is in digital form but during the transmission, it may be in the form of analog or digital signals.
- A data communication network can be simply consisting of two computers connected to each other a public telecommunication network.

(G-1429) **Fig. 1.1.1 : A simplest possible data communication network**

- Data communication system are used for interconnecting all types of digital computing equipments, internet etc.
- In this chapter we are going discuss data communication and networking.
- The aim of data communication and networking is to allow the exchange of data such as audio, text and video between any points in world.
- The transfer of data takes place over a computer network. A network is like a path or a road over which the data travels smoothly from sender to destination.

1.2 Introduction to Data Communication :

- In this chapter we are going discuss data communication and networking.
- The data communication and networking allows the exchange of data between any points in world. The data can be audio, text, video or of some other form.
- The transfer of data takes place over a computer network. A network provides path over which the data can travel to the desired destination.

1.2.1 Definition of Data Communication :

- Before exchanging information, creators and the users of data should agree upon how the information should be presented.
- An information that is presented in such a form is called as **data.**
- **Data communication** can be defined as the exchange of data between a source and destination over some kind of transmission medium, such as a co-axial cable, (wired communication) or air (wireless communication).

1.2.2 Characteristics of Data Communication System :

I-Scheme : W-19

- The three important characteristics of a data communication system are :

  1. Delivery 2. Accuracy 3. Timeliness

1. Delivery :

- A data communication system (DCS) must deliver data only to the user who is intended to use it and not to anyone else.

2. Accuracy :

- Due to noise the data may get altered or corrected when it is travelling over a communication medium. Errors will be introduced and the accuracy of the received data is adversely affected.
- The data communication system (DCS) must be designed in such a way that the delivered data is accurate and free from any errors.

3. Timeliness :

- The time delay is unacceptable for the audio and video data as it introduces errors in the reproduced sound or picture.
- So the DCS should deliver the data without any time delay.
- Such a data delivery is called as real-time transmission of data.

1.3 Components of Data Communication System :

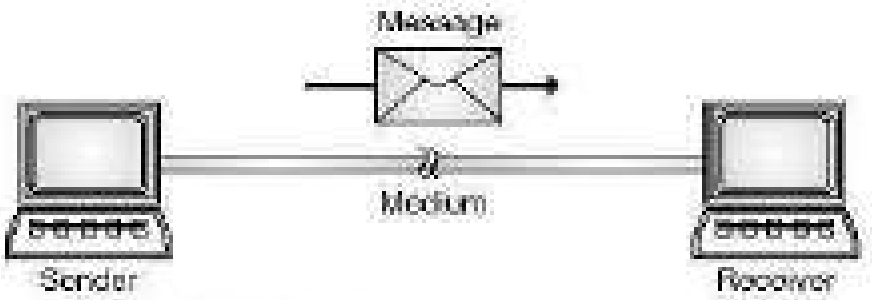
I-Scheme : W-19, S-22

Block diagram :

- If we specifically consider the communication between two computers then the data communication system is as shown in Fig. 1.3.1.

- It has the following five components.

1. Message
2. Sender
3. Medium
4. Receiver and
5. Protocol



(L-2) **Fig. 1.3.1 : Five components of a data communication system**

1. Message :

- Message is nothing but information or data which is to be sent from sender to the receiver.
- A message can be in the form of sound, text, number, pictures, video or combination of them.

2. Sender :

- Sender is a device such as a host, video camera, telephone, work station etc which sends the message over the medium.

3. Medium :

- The message originating from the sender needs a path over which it can travel to the receiver. Such a path is called as the medium or channel.
- The examples of transmission medium are coaxial cable, twisted pair wire, fiber optic cable, radio waves (used in terrestrical or satellite communication) etc.

4. Receiver :

- It is the device which receives the message and reproduces it. A receiver can be in the form of a workstation, telephone handset, a TV receiver, etc.

5. Protocol :

- Protocol is defined as the set of rules agreed by the sender and receiver.
- There can be different protocols defined for different functions. Protocols govern the exchange of data in true sense.
- A set of such rules is known as a "protocol" of the data communication system.
- Many different protocols are used in the modern data communication system.
- The interconnection of one station to many stations is called as networking.
- A network is any interconnection of two or more stations that wish to communicate.

1.4 Protocols and Standards :

- Protocol and standards are the two frequently used words in data communication.
- Let us define them first and then explain them.

1.4.1 Protocols : I-Scheme : S-22

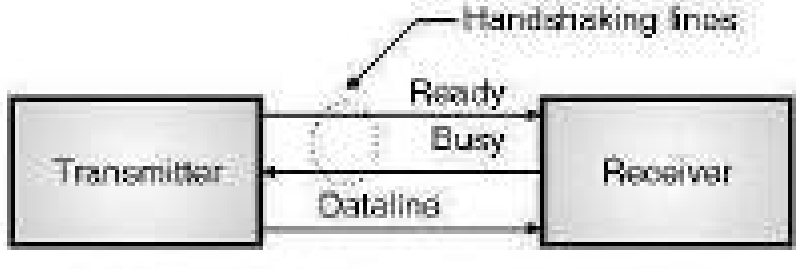
- For successful communication to occur, it is not enough for the "sender" to simply transmit the message and "assume" that the "receiver" will receive it properly.
- There are certain rules that must be followed to ensure proper communication.
- A successful communication of data can be ensured if sender and receiver agree upon certain rules and procedures in relation with the data.

Definition :

- A protocol is defined as the set of rules agreed upon by the sending and receiving computer systems, to facilitate a proper communication between them.
- Such rules and procedures are called as protocols. Different types of protocols are used in data communications.

Process of data communication :

- In data communications a message consists of more than one character. A group of characters forms a block.
- In order to send a message it is broken up into smaller blocks and each block is separately identified by transmitting one or more special characters before or after each block.
- Some of the characters at the beginning and end of each block are used for "handshaking" purpose.
- Fig. 1.4.1 demonstrates the basic handshaking process.



(G-47) **Fig. 1.4.1 : The handshaking process**

1. The transmitter starts by sending a "Ready" signal to the receiver to indicate to the receiver that it wants to send a character.
2. The receiver identifies this signal and communicates its status (busy or ready) on the "busy" line to the transmitter.
3. If the receiver is busy then it is indicated by the receiver by sending a character on the busy line.
4. The transmitter will wait if the receiver is busy and will send the data only when the receiver is not busy and the transmitter becomes ready.

1.4.2 Important Elements of a Protocol :

- Some of the important elements of a protocol are :

  1. Syntax 2. Semantics 3. Timing

1. Syntax :

- Generally the data is presented in a particular structure or format or order.
- The structure or format or order in which the data is presented is known as its syntax.

2. Semantics :

- A protocol defines the meaning of each section of data bits, or interprets a particular pattern of data bits.
- This is known as semantics of a protocol.
- It also tells us about what action is to be taken based on the interpretation.

3. Timing :

- The third element of a protocol is timing. It takes into consideration the instant of sending the data and the speed at which the data is to be sent.

1.4.3 Standards :

Definition :

- Data communication standards are defined as the guidelines to the product manufacturers and vendors to ensure national and international interconnectivity.

Need :

- Standards are needed for ensuring the interconnectivity and interoperability among various hardware and software components.
- Without standards, it is not possible to ensure connectivity and interoperability worldwide.

Classification :

- Data communication standards are classified into two categories.

  1. De facto standards
  2. De jure standards

1. De facto :

- The meaning of De facto is "by fact" or "by convention".
- These standards are established by the manufactures and adopted as standards due to their widespread use, but they are not approved by any standard organizations.

2. De jure :

- The meaning of this word is "by law" or "by regulation". So De jure standards are the standards which have the backing of law or which have been approved by standard organizations.

Advantages :

1. Many computers from all the world can connect together for communicating, because they are using the international standard.
2. Easier maintenance and installation because you get used on the standard.
3. Upgradation and adoptions of standard becomes easy.

Disadvantages :

1. Problems occur in standards, it takes time to solve as it involves all international regulating bodies.
2. All companies and manufactures must compulsorily follow standards to communicate.
3. The standards cannot be modified or customized as per the need by individuals.

1.4.4 Standard Organizations :

Need of standard organizations :

- The standard organizations are needed due to following reasons :

1. They create and maintain an open and competitive market for manufacturers.
2. They guarantee national and international interoperability of data and telecommunication technology and processes.
3. They provide guidelines to manufacturers. The data communication standards are developed through collective efforts of committees, forums and government regulatory agencies specially formed for creation of standards.

Standard creation committees :

– Some of the standard creation committees are :

1. Institute of Electrical and Electronics Engineers (IEEE).
2. Electronic Industries Association (EIA).
3. American National Standards Institute (ANSI).
4. International Telecommunication Union Telecommunication standards.
5. International Organization for Standardization (ISO).

Regulatory agencies :

– Federal Communications commission (FCC) is the government regulator body in U.S. for all communication technology.

Standard organizations for data communications :

– Some of the standard organizations for data communication are as follows :

1. Electronic Industries Association (EIA) :

– EIA is a U.S. organization. It forms and recommends the industrial standards.

– EIA has developed the RS (Recommended Standard) series of standards for data and telecommunications.

2. Institute of Electrical and Electronics Engineers (IEEE) :

– It is a professional organization of electronics, computer and communications engineers based in United States of America.

3. American National Standards Institute (ANSI) :

– ANSI is the official standard agency for United States.

4. Consultative Committee for International Telephony and Telegraphy (CCITT) or (ITU-T) :

– The CCITT is now a standard organization for the United Nations.

– Many government authorities and representatives are members of CCITT.

– CCITT develops the recommended sets of rules and standards for telephone and telegraph communications.

– On March 1993 the name of this Committee was changed to International Telecommunication Union-Telecommunication Standards Sector (ITU-T).

5. International Standard Organization (ISO) :

– ISO is one of the international organization for standardization. It creates sets of rules and standards for graphics, document exchange etc.

– ISO has a role of endorsing and co-ordinating the work of the other standard organizations.

6. Standards Council of Canada (SCC) :

– SCC is the official standards agency for Canada. It has similar responsibilities to those of ANSI.

1.5 Signals :

– In the long distance communications, the computer data cannot be transmitted as it is.

– We have to first convert it into electrical signals (wired communication) or electromagnetic signals (wireless communication).

– Both data and the signals which represent them can be of analog form or digital form.

1.5.1 Analog and Digital Data :

Analog data :

– The human voice is the best example of analog data. When a person speaks, an analog wave is created in air.

– We can convert it into an analog signal by means of a microphone.

Digital data :

– The data is stored in computer memory in the form of 0s and 1s is digital data.

1.5.2 Analog Signals :

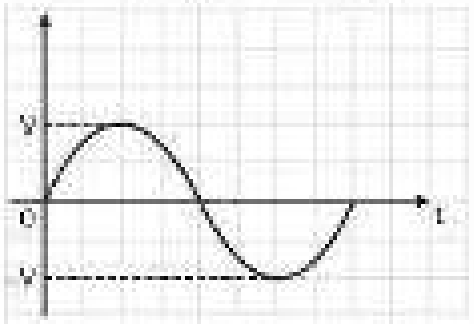
– These are the signals which can have infinite number of different magnitudes or values.

– They vary continuously with time. Sine wave, triangular wave etc. are the examples of analog signals.

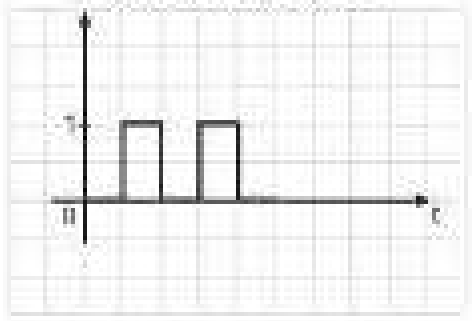
1.5.3 Digital Signals :

– A signal is called as a digital signal if it has only a finite number of predetermined distinct magnitudes.

– The digital signals are discrete time signals, i.e. they are not continuous with time as shown in Fig. 1.5.1.



(a) Analog signal



(b) Digital signal

(G-1426) Fig. 1.5.1

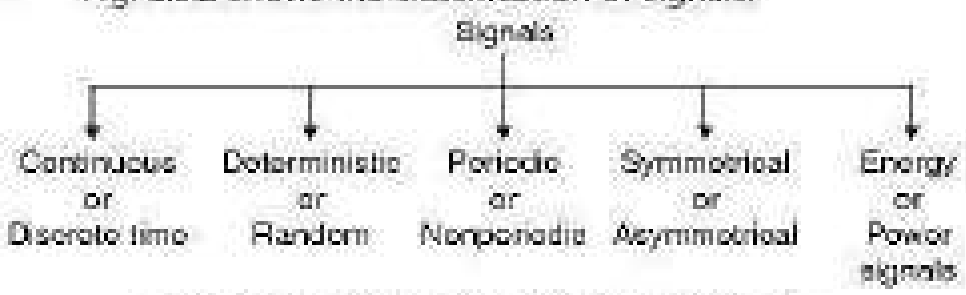
1.5.4 Comparison of Digital and Analog Signals :

I-Scheme : S-19

Sr. No.	Parameter	Analog signals	Digital signals
1.	Number of values	Infinite	Finite (2, 8, 16 etc.)
2.	Nature	Continuous	Discrete
3.	Sources	Signal generators, transducers etc.	Computers, A to D converters
4.	Examples	Sinewave, triangular wave	Binary signal

1.5.5 Classification of Signals :

- Fig. 1.5.2 shows the classification of signals.



(G-1250) Fig. 1.5.2 : Classification of signals

- Out of these we will concentrate only on periodic or non periodic signals.

1.5.6 Periodic and Non-periodic Signals :

Periodic signal :

- A signal which repeats itself after a fixed time period is called as a periodic signal. The periodicity of a signal can be defined mathematically as follows :

$$x(t) = x(t + T_0) \quad \text{: Condition of periodicity} \qquad ...(1.5.1)$$

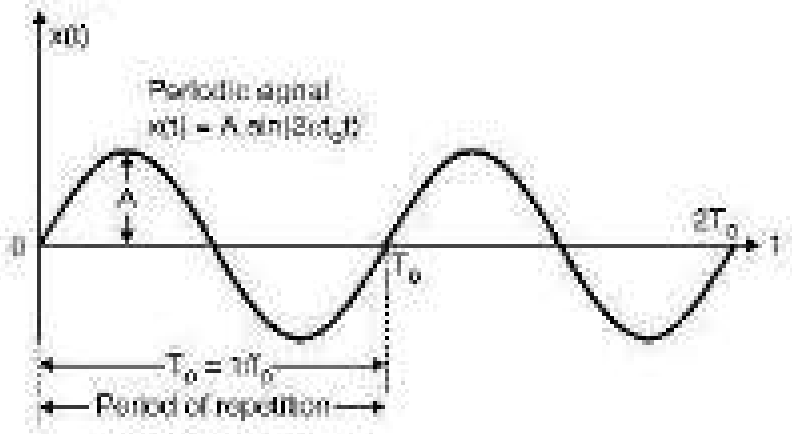
- Where T_0 is called as the period of signal x (t), in other words, signal x (t) repeats itself after a period of T_0 sec.
- Examples of periodic signals are sine wave, cosine wave, square wave etc. Fig. 1.5.3 shows a sine wave which is periodic because it repeats itself after a period T_0.

Non-periodic signal :

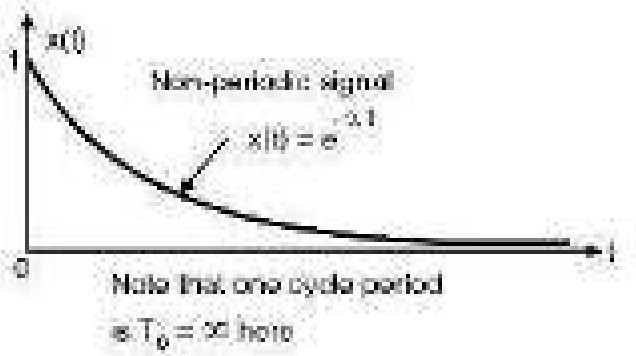
- A signal which does not repeat itself after a fixed time period or does not repeat at all is called as a non-periodic or aperiodic signal.
- The non-periodic signals do not satisfy the condition of periodicity stated in Equation (1.5.1).

$$\therefore \quad \text{For a non-periodic signal } x(t) \neq x(t + T_0) \qquad ...(1.5.2)$$

- Sometimes it is said that an aperiodic signal has a period $T_0 = \infty$. Fig. 1.5.3 shows a decaying exponential signal.
- This exponential signal is non-periodic but it is deterministic because we can mathematically express it as $x(t) = e^{-\alpha t}$.



(a)



(b)

(G-1251) Fig. 1.5.3 : Periodic and non-periodic signals

1.6 Composite Signal and Transmission Medium :

- The data is generally in the form of pulses and pulse is a composite signal which contains many frequencies.
- Note that the peculiar shape of a pulse is due to the sum of specific frequencies at specific amplitudes and phases.

– If there is any change in the amplitudes or phases of these frequency components, then the shape of the pulse will not remain the same.

1.6.1 Medium :

– The signal always travels over some medium from sender to destination.

– The medium can be a coaxial cable or optical fiber etc. A medium does not pass all frequencies equally due to its inadequate frequency spectrum.

– It may pass some frequencies and weaken or block the other frequencies.

– Hence when a composite signal is passed over such a transmission medium, at the receiving end we get a wave, having a different shape as shown in Fig. 1.6.1.

(G-82) **Fig. 1.6.1 : Signal distortion on a transmission medium**

– To avoid the signal distortion, the medium should pass all the frequencies present at the input without any change.

– But no medium is perfect and so some signal distortion is bound to take place.

1.7 Bandwidth of a Signal : I-Scheme : S-22

Definition :

– Bandwidth is defined as the portion of the electromagnetic spectrum occupied by a signal.

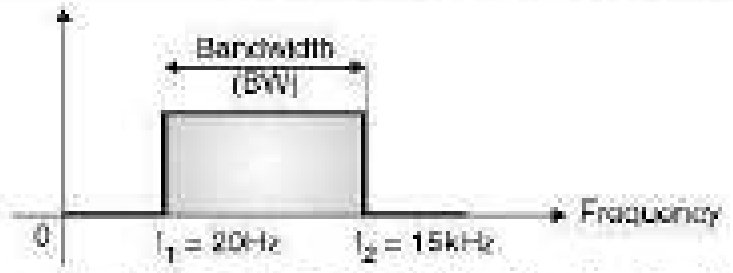
– We may also define the bandwidth as the frequency range over which an information signal is transmitted.

– Bandwidth is the difference between the upper and lower frequency limits of the signal.

– We already know different types of baseband signals such as voice signal, music signal, TV signal etc. Each of these signals will have its own frequency range. This frequency range of a signal is known as its bandwidth.

– For example the range of music signal is 20 Hz to 15 kHz. Therefore as shown in Fig. 1.7.1 the bandwidth is $(f_2 - f_1)$.

$$\therefore \quad BW = f_2 - f_1 = 15000 - 20 = 14980 \text{ Hz}.$$



(G-125S) **Fig. 1.7.1 : Bandwidth of music signal**

– The bandwidths of different signals are as listed in Table 1.7.1.

Table 1.7.1

Sr. No.	Type of the signal	Range of frequency in Hz	Bandwidth in Hz
1.	Voice signal (speech) for telephony	300 – 3400	3,100
2.	Music signal	20 – 15000	14,980
3.	TV signals (picture)	0 – 5 MHz	5 MHz
4.	Digital data	* 300 – 3400 (If it is using the telephone line for its transmission).	3,100

Note : Actually the required bandwidth in the data transmission depends on the rate at which the data is being transmitted. The BW increases with increase in the rate of data transmission.

1.7.1 Frequency Spectrum :

– Frequency spectrum is the representation of a signal in the frequency domain. It can be obtained by using either Fourier series or Fourier transform.

– It consists of the amplitude and phase spectrums of the signal. The frequency spectrum indicates the amplitude and phase of various frequency components present in the given signal.

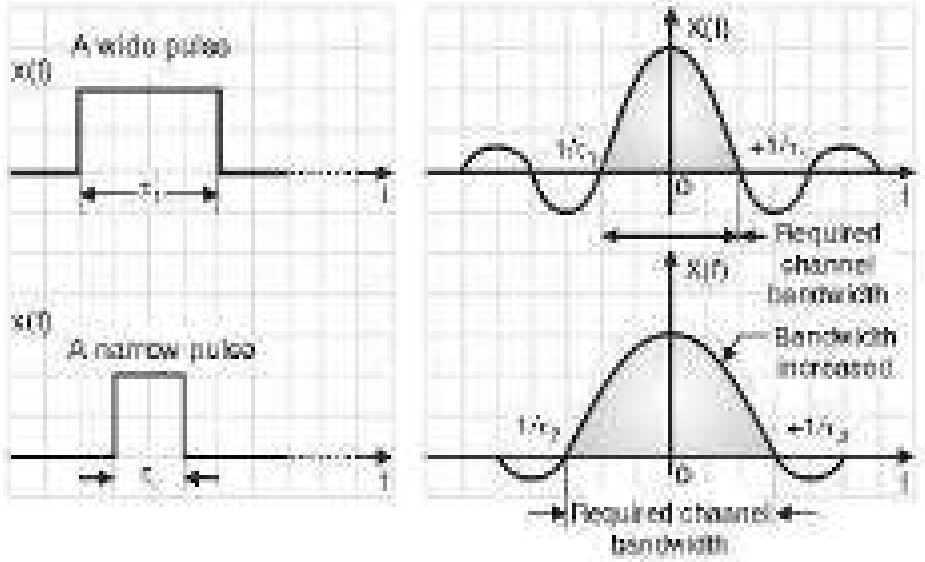
– The frequency spectrum enables us to analyze and synthesize a signal.

1.7.2 Effect of Pulse Width of Data on the BW :

– When data is to be transmitted, the bandwidth depends on the pulse width of data.

– As the width of the data pulses which are to be transmitted reduces (compression takes place in time domain), the bandwidth requirement increases (expansion takes place in the frequency domain), according to the time scaling property of Fourier transform.

– This is as shown in Fig. 1.7.2.



Compression in time domain = Expansion in frequency domain

(G-1255) **Fig. 1.7.2 : Effect of data pulse width on BW**

– Hence the signals having higher data rates need larger bandwidth.

1.7.3 Bandwidth of a Medium (Channel Bandwidth) :

– The range of frequencies that contain the information is called as the bandwidth. But the term channel bandwidth is used to describe the range of frequencies required to transmit the desired information.

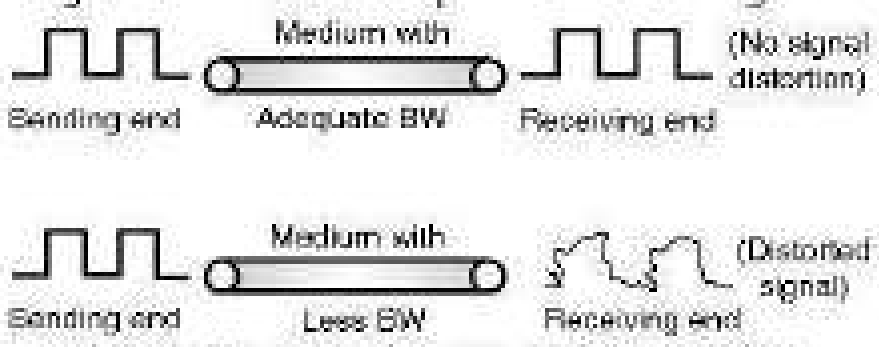
– For example the amplitude modulation (AM) systems needs a channel bandwidth of 10 kHz to transmit a signal of 5 kHz bandwidth.

– But the single sideband system (SSB) needs only 5 kHz channel bandwidth to transmit the same signal.

– All the efforts should be made to reduce the required channel bandwidth so that we can fit in more number of channels in the same available EM spectrum.

– Bandwidth of a medium (also called as channel bandwidth) is defined as the maximum frequency it can allow to pass through it without attenuating it and without distorting the shape of the signal.

– If the medium has less bandwidth than required, then signal distortion will take place as shown in Fig. 1.7.3.



(G-1256) **Fig. 1.7.3 : Importance of channel BW**

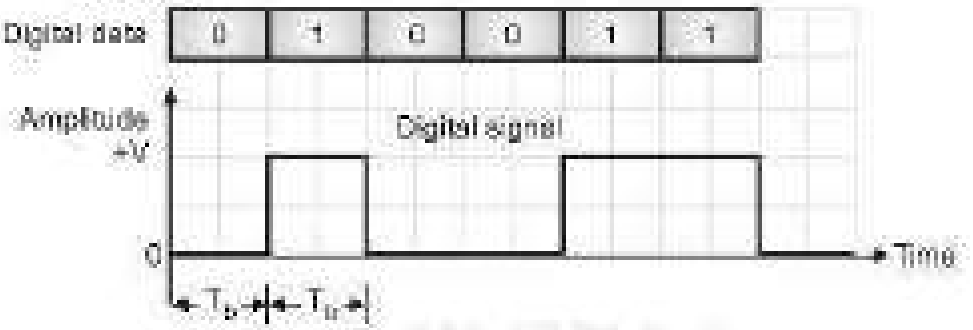
1.8 Digital Signals :

– The input data which is either analog or digital can also be represented by a digital signal.

Definition :

– A digital signal is a discrete time signal having finite number of amplitudes. For example see the digital signal shown in Fig. 1.8.1.

– A 0 is represented by zero volt and a 1 by some positive voltage.



(G-823) **Fig. 1.8.1 : Digital signal**

1.8.1 Bit Interval :

Definition :

– The bit interval is the time corresponding to one single bit (0 or 1).

– As shown in Fig. 1.8.2, time corresponding to a 0 or a 1 is T_b hence it is the bit interval or bit length.

1.8.2 Bit Rate :

I-Scheme : W-19, S-22

Definition :

– Bit rate is defined as the number of bits transmitted or sent in one second. It is expressed in bits per second (bps).

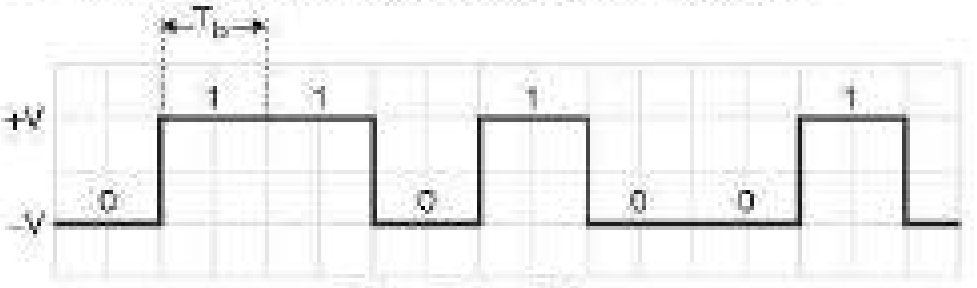
– Relation between bit rate and bit interval is as follows :

$$\text{Bit rate} = \frac{1}{\text{Bit interval}}$$

– Bit rate is also called as **signalling rate** and is defined as the number of bits which can be transmitted in a second.

– If the bit duration is "T_b" then bit rate will be $1/T_b$. Look at Fig. 1.8.2, you will see that the bit duration is necessarily equal to the pulse duration.

– In Fig. 1.8.2 the first pulse is of two bit duration.



(G-83) **Fig. 1.8.2 : A bit stream**

- Bit rate is also called as **signalling rate** and it should be as high as possible.
- However with increase in bit rate the bandwidth of transmission medium (channel bandwidth) must be increased, in order to ensure that the signal is received without any distortion.

1.8.3 Bauds (or Baud Rate) :

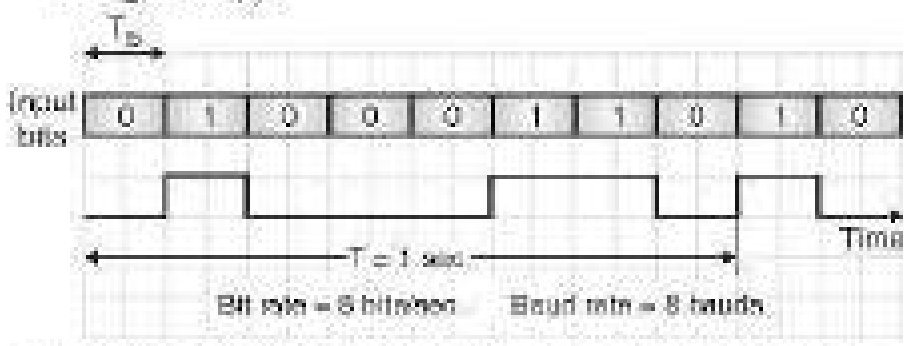
I-Scheme : W-19, S-22

Definition :

- **Baud** is defined as the unit of signalling speed or modulation rate or the rate of symbol transmission.
- It indicates the rate at which a signal level changes over a given period of time.

Baud rate of binary transmission :

- When binary bits are transmitted as an electrical signal with two levels "0" and "1" the bit rate and the modulation rate i.e. baud rate are same. This is as shown in Fig. 1.8.3(a).

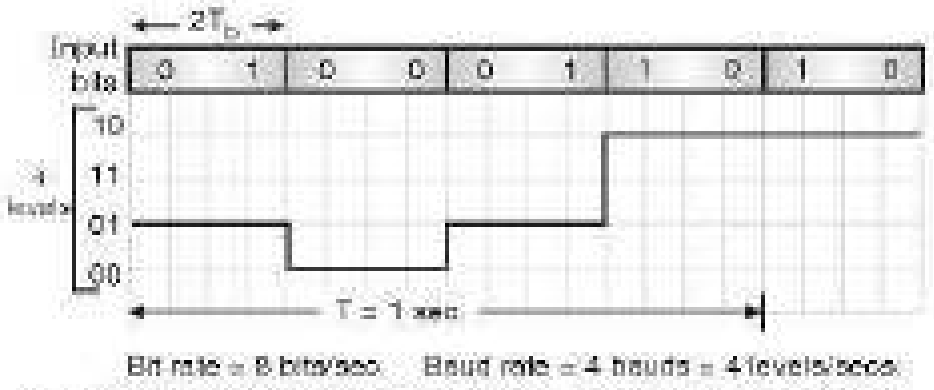


(G-84) **Fig. 1.8.3(a) : Baud rate for two level modulation**

- Thus for a two level signal (binary signal) the bit rate and bauds are equal.

Baud rate of M-ary transmission :

- Now consider Fig. 1.8.3(b) where four different levels are used to represent the data.



(G-85) **Fig. 1.8.3(b) : Baud rate for a four level modulation**

- Each level is being represented by a combination of two bits i.e. 00 or 01 etc. Thus each symbols consists of 2 bits.
- The bit rate is therefore not equal to the baud rate.
- The bit rate is 8 bits/sec. but baud rate is only 4 bauds as there are 4-levels per second, or four symbols transmitted per second.

1.9 The Data Transmission Rate and the Bandwidth :

- The digital signal changes its amplitude instantaneously. As mentioned earlier, an instantaneous change in amplitude corresponds to infinite number of frequencies. So a digital signal contains infinite frequency components.
- Hence a digital signal is actually a composite signal. That means the bandwidth of a digital signal is infinite.
- So as to preserve the shape of the digital signal the medium over which it is sent should also have an infinite bandwidth. But practically it does not happen that way.
- A practically available medium such as coaxial cable does not have an infinite bandwidth but it has a wide bandwidth.
- When a digital signals is transmitted over such a medium, some of the frequencies are blocked by the medium but still enough frequencies are passed.
- So the digital signal at the receiving end will have a decent shape with a small distortion.
- A medium having a narrow bandwidth is called as a bandlimited medium. The example of bandlimited medium is the telephone lines.
- We can send the digital signals over a bandlimited medium. The best example of this is the data transfer over telephone cables in internet.
- The most important question here is that what should be minimum bandwidth of the medium (B Hz) if we want to transmit a signal of n bps.
- The answer to this question is given by the Nyquist theorem and Shannon capacity theorem.

1.9.1 Relation between Required Bandwidth and Bit Rate :

- In computer communication we have to send as many bits as possible per second for fast data transfer.
- That means the bit rate should be as high as possible. But increase in bit rate has an undesired side effect.
- The signal bandwidth and the required bandwidth of the medium (channel bandwidth) increase with increase in bit rate.

- If we double the bit rate then the required channel bandwidth needs to be doubled.
- Thus bit rate and bandwidth are proportional to each other.

Relation between bit rate and BW :

- The general relation between required bandwidth (B) and bit rate (n) is as follows :

$$B \geq \frac{n}{2} \text{ or } n \leq 2B$$

- Thus over a medium having a bandwidth of 4 kHz we can send a digital signal with a bit rate upto 8 kbps.
- In practice the maximum bit rate can be more than 30 kbps using the traditional MODEMS.

1.10 Digital Versus Analog Bandwidth :

- If we are sending analog data over a medium, then the analog bandwidth of that medium should be considered. Analog bandwidth is expressed in Hz.
- But if the digital data is being sent over a medium, then we should consider its digital bandwidth.
- The digital bandwidth is expressed in bits per second (bps). The analog and digital bandwidths are different from each other.

1.10.1 Analog Bandwidth :

- It is defined as the range of frequencies that are allowed to pass by the medium without much reduction in amplitude. Analog bandwidth is measured in Hz.

1.10.2 Digital Bandwidth :

- It is defined as the maximum bit rate that a medium is able to pass or support. The digital bandwidth is expressed in bits per second (bps).
- Both analog and digital bandwidths should be as large as possible. Ideally they are infinite.

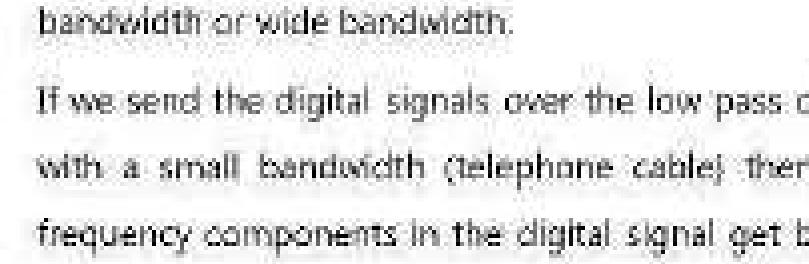
1.10.3 Types of Channels (Mediums) :

- There are two types of communication channels or mediums namely :

  1. Low pass channel 2. Bandpass channel

Low-pass channel :

- As shown in Fig. 1.10.1(a), a low pass channel is that channel whose bandwidth extends right from 0 Hz to f_1 Hz. That means it passes all the signal having frequencies in the range 0 to f_1.
- Since the frequency response is identical to that of a low pass filter, this channel is called as a low pass channel.



(a) Low pass channel

(I-775) **Fig. 1.10.1 : Types of channels**

1.11 Transmission of Digital Signals :

- The digital signals can be transmitted from one point to the other using one of the following two approaches :

  1. Baseband transmission.
  2. Bandpass transmission (with modulation).

1.11.1 Baseband Transmission :

- A baseband digital signal is the original signal without any modulation. In the modulation process the baseband digital signal is converted into analog signal.
- Baseband transmission is the transmission of baseband digital signal.
- A baseband signal occupies bandwidth from 0 to f_1 Hz.
- Hence baseband transmission requires the use of low pass channel. This low pass channel can have a narrow bandwidth or wide bandwidth.
- If we send the digital signals over the low pass channel with a small bandwidth (telephone cable) then same frequency components in the digital signal get blocked and the shape of the received signal will be badly distorted as shown in Fig. 1.11.1(b).

(a) Baseband transmission through a wideband channel

(b) Baseband transmission through a narrowband channel

(I-1101) **Fig. 1.11.1**

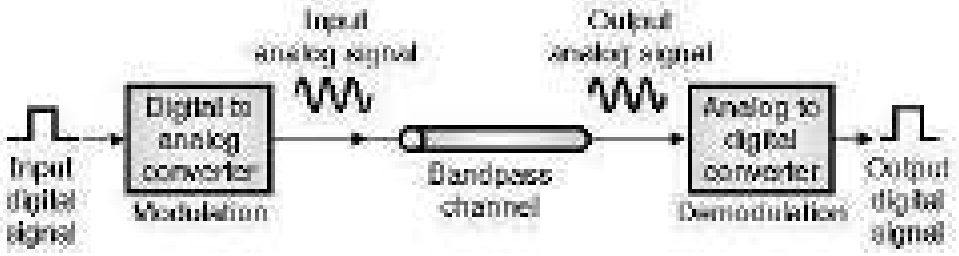
- A practically available medium such as coaxial cable does not have an infinite bandwidth but it has a wide bandwidth.
- When a digital signals is transmitted over such a medium, some of the frequencies are blocked by the medium but still enough frequencies are passed.
- So the digital signal at the receiving end will have a different shape with a small distortion as shown in Fig. 1.11.1(a).

Conclusion :

- Baseband transmission of digital signals over a low pass channel without waveform distortion is possible if and only if the channel has a wide or infinite bandwidth.

1.11.2 Broadband Transmission (with Modulation) :

- A baseband signal is passed through a D to A converter to obtain an equivalent analog signal.
- This is modulation and the modulated analog signal is called as a broadband signal.
- Transmission of a broadband signal is known as broadband transmission of digital signal. The spectrum of a broadband signal extends from f_1 to f_2 so it is a bandpass spectrum.
- We have to use a bandpass channel to carry this transmission. Fig. 1.11.2 shows the modulation process and broadband transmission.



(S-1302) **Fig. 1.11.2 : Broadband transmission of digital signal**

- Note that the output digital signal is distortion free.
- We can send the digital signals over a bandlimited medium. The best example of this is the data transfer over telephone cables in internet.
- The most important question here is that what should be minimum bandwidth of the medium (B Hz) if we want to transmit a signal of n bps.
- The answer to this question will be given when we study the Nyquist theorem and Shannon capacity.

1.12 Modes of Communication : Simplex, Half Duplex, Duplex : I-Scheme : S-19

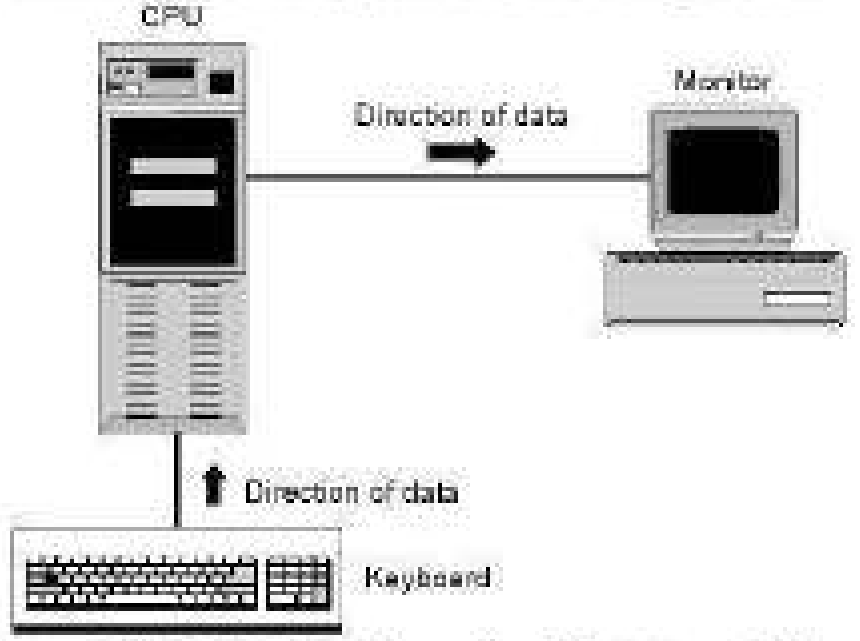
- Based on whether the given communication system communicates only in one direction only or in both the directions, the communication systems are classified as :
  1. Simplex systems.
  2. Half duplex systems.
  3. Full duplex systems.

1.12.1 Simplex Communication :

I-Scheme : S-19, W-19, S-22

Definition :

- A simplex communication is defined as the communication in only one direction.
- In these systems the information is communicated in only one direction. For example the radio or TV broadcasting systems can only transmit. They cannot receive.
- In data communication system the simplex communication takes place as shown in Fig. 1.12.1.



(S-53) **Fig. 1.12.1 : Simplex mode of data transmission**

- The communication from CPU to monitor or keyboard to CPU is unidirectional.
- Keyboard and traditional monitors are examples of simplex devices.

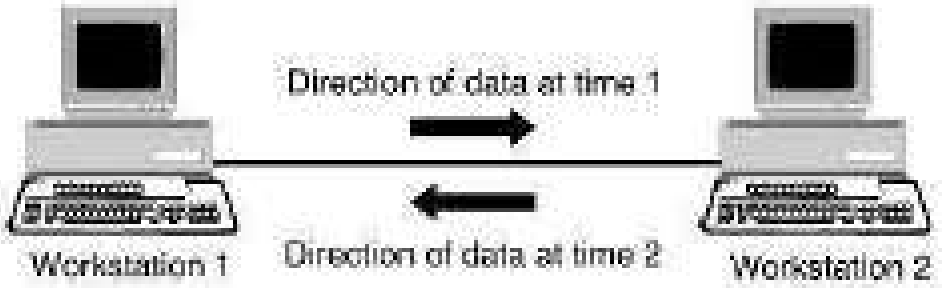
1.12.2 Half Duplex Communication :

I-Scheme : S-19, W-19, S-22

Definition :

- A half duplex communication is defined as the bidirectional communication which does not take place simultaneously.

- These systems are bi-directional, i.e. they can transmit as well as receive but not simultaneously.
- At a time these systems can either transmit or receive, for example a transreceiver or walky talky set. Thus the direction of communication will keep changing itself.
- A data communication system working in the half duplex mode is shown in Fig. 1.12.2.



(G-54) **Fig. 1.12.2 : Half duplex system**

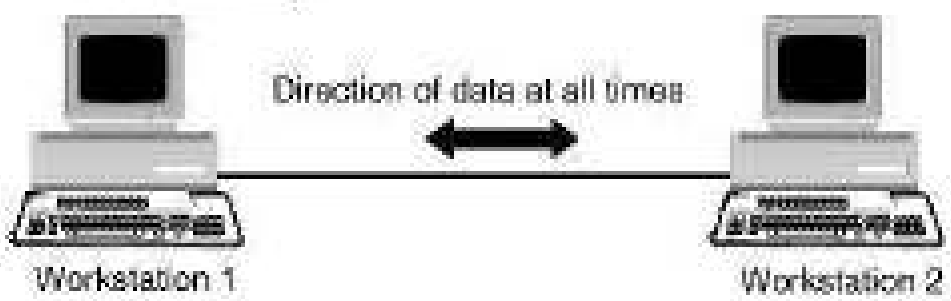
- Each station can transmit and receive, but not at the same time. When one device is ending the other one is receiving and vice versa.
- In half duplex transmission, the entire capacity of the channel is utilized by the transmitting (sending) system.

1.12.3 Full Duplex Communication :

I-Scheme : S-19, W-19, S-22

Definition :

- A duplex communication is defined as the type of communication in which a simultaneous flow of information takes place at any given time.
- These are truly bi-directional systems as they allow the communication to take place in both the directions simultaneously.
- These systems can transmit as well as receive simultaneously, for example the telephone systems.
- A full duplex data communication system is shown in Fig. 1.12.3. Each station can transmit and receive simultaneously.



(G-55) **Fig. 1.12.3 : Full duplex mode**

- In full duplex mode, signals going in either direction share the full capacity of link.
- The link may contain two physically separate transmission paths one for sending and another for receiving.
- Otherwise the capacity of channel is divided between signals travelling in both directions.

Comparison of communication modes :

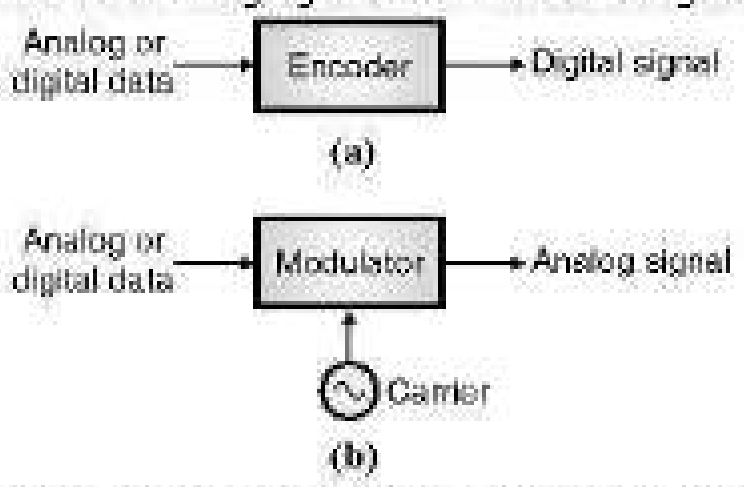
Sr. No.	Parameter	Simplex	Half duplex	Full duplex
1.	Communication takes place in	Only one direction at a time	In both directions but not simultaneously.	In both directions simultaneously.
2.	Example	Radio/TV broadcasting	Walky talky	Telephone

1.13 D to A or A to D Conversion :

- A computer network is designed to send information from one point to the other.
- It is necessary to convert this information to either digital signal or analog signal for transmission depending on the transmission medium and application.

1.13.1 Encoding and Modulation :

- It is possible to encode any type of data into any type of signal as shown in Fig. 1.13.1.
- Fig. 1.13.1(a) illustrates the concept of **digital signalling** in which the input data (analog or digital) is encoded into a digital signal.
- Fig. 1.13.1(b) illustrates the concept of **analog signalling** in which the analog / digital source is used for modulating a continuous time carrier signal to produce an analog signal called modulated signal.



(L-25) **Fig. 1.13.1 : Conversion from analog / digital data to analog / digital signal**

Encoding Types :

- There are four different possible transformations as follows :
  1. Digital data, digital signal.
  2. Analog data, digital signal.
  3. Digital data, analog signal.
  4. Analog data, analog signal.

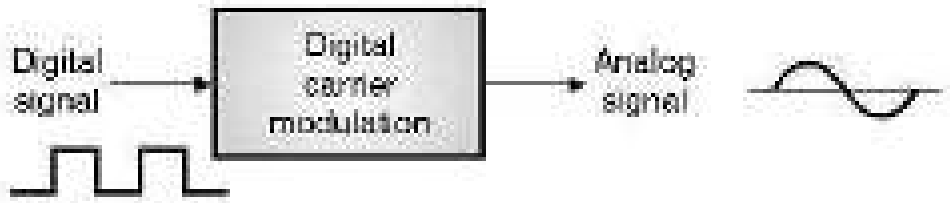
1.14 Digital to Analog Conversion :

- In the process of D to A conversion the digital data at the input is converted into an analog signals.
- These analog signals are transmitted over the transmission medium.
- The most familiar application of D to A conversion is for transmitting digital data through the public telephone network.
- The D to A conversion is done by the modems to convert the digital data from the computers into the analog signals that are sent on the telephone lines for the Internet.

(L-791) **Fig. 1.14.1 : Digital data to analog signal**

1.14.1 Need of Digital Carrier Wave Modulation :

- D to A conversion is also called as digital carrier wave modulation.
- PCM (Pulse Code Modulation) converts analog message signal into a digital signal.
- Now we will learn some techniques which convert the digital message signal into an analog signal and then transmits it.
- Such modulation schemes are called as digital carrier modulation schemes.
- This type of digital to analog conversion is essential when the digital message signal is to be sent over a bandlimited channel such as the telephone line.
- The best application of digital carrier modulation is MODEM.
- The modem will modulate the digital data signal from the DTE (computer) into an analog signal.
- This analog signal is then transmitted on the telephone lines.

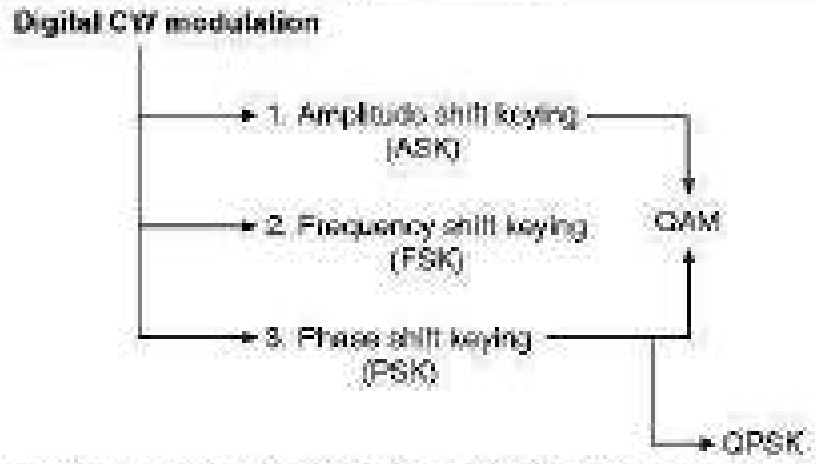


(L-62) **Fig. 1.14.2 : Digital carrier modulation**

- The question is why can't we send the digital signal as it is on the telephone lines ? Why should we modulate it ?
- Here is the answer for it. The digital data consists of binary 0s and 1s, therefore the waveform changes its value abruptly from high to low or low to high.
- In order to carry such a signal without any distortion being introduced, the communication medium needs to have a large bandwidth.
- Unfortunately the telephone lines do not have high bandwidth. Therefore we have to convert the digital signal first into an analog signal which needs lower bandwidth by means of the modulation process.

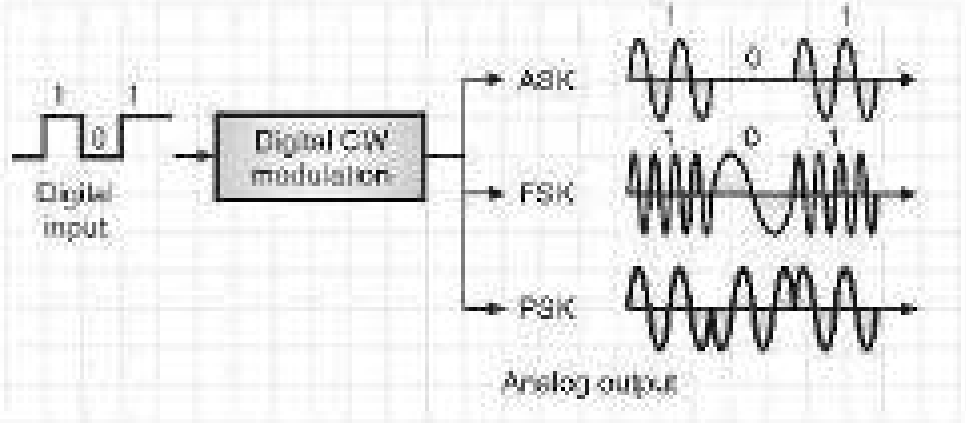
1.14.2 Types of Digital Carrier Modulation :

- There are three basic types of modulation techniques for the transmission of digital signals.
- These methods are based on the three characteristics of a sinusoidal signal; amplitude, frequency and phase. The corresponding modulation methods are then called as :
  1. Amplitude Shift Keying (ASK).
  2. Frequency Shift Keying (FSK).
  3. Phase Shift Keying (PSK).
  4. Quadrature Phase Shift Keying (QPSK) or 4-PSK.
  5. Quadrature Amplitude Modulation (QAM).
- QPSK is a multilevel modulation in which four phase shifts are used for representing four different symbols.
- At high bit rates, a combination of ASK and PSK is employed in order to minimize the errors in the received data.
- This method is known as "Quadrature Amplitude Modulation (QAM)". Let us discuss these methods one by one.
- Fig. 1.14.3 shows the classification of digital to analog modulation systems.



(L-62) **Fig. 1.14.3 : Classification of digital CW modulation**

– Digital CW modulation is demonstrated in Fig. 1.14.4.



(L-63) **Fig. 1.14.4 : Various digital CW modulation schemes**

1.15 Amplitude Shift Keying (ASK) :

Definition :

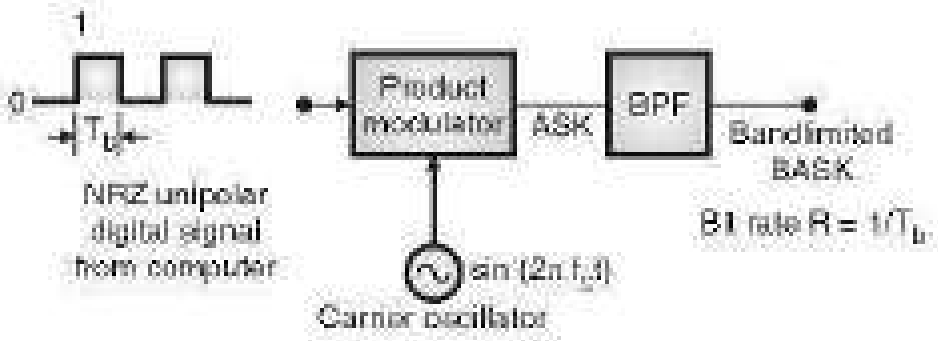
– ASK is the digital carrier modulation in which the amplitude of the sinusoidal carrier will take one of the two predetermined values in response to 0 or 1 value of digital input signal.

Generation and waveforms :

– Amplitude Shift Keying (ASK) is the simplest type of digital CW modulation. Here the carrier is a sinewave of frequency f_c. We can represent the carrier signal mathematically as follows :

$$e_c = \sin(2\pi f_c t) \quad \ldots(1.15.1)$$

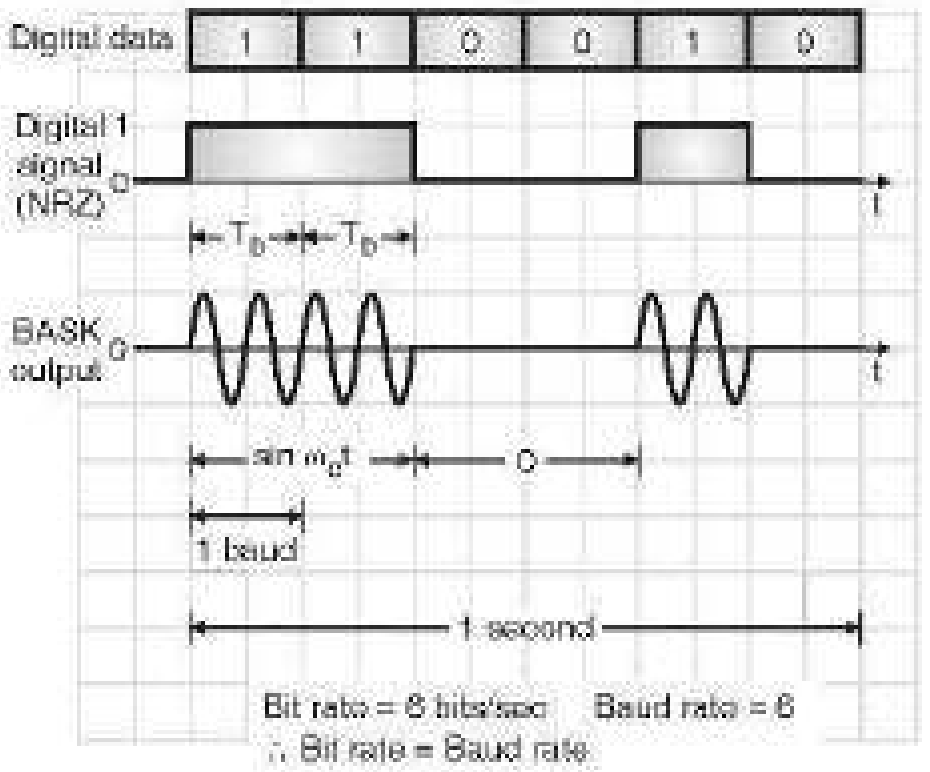
– The digital signal from the computer is a unipolar NRZ signal which acts as the modulating signal. The ASK modulator is nothing but a multiplier followed by a band pass filter as shown in Fig. 1.15.1(a).



(L-901(a)) **Fig. 1.15.1(a) : ASK modulator**

– Due to the multiplication, the ASK output will be present only when a binary "1" is to be transmitted.

– The ASK output corresponding to a binary "0" is zero as shown in Fig. 1.15.1(b).



(L-901(a)) **Fig. 1.15.1(b) : Waveforms of ASK**

– From the waveforms of Fig. 1.15.1(b) we can conclude that the carrier is transmitted when a binary 1 is to be sent and no carrier is transmitted when a binary 0 is to be sent.

– The ASK signal can be mathematically expressed as follows :

$$V_{ASK}(t) = d \sin(2\pi f_c t) \quad \ldots(1.15.2)$$

where d = Data bit which can take values 1 or 0.

$$\therefore \quad V_{ASK}(t) = \sin(2\pi f_c t) \quad \text{when } d = 1$$
$$\text{and} \quad V_{ASK}(t) = 0 \quad \text{when } d = 0 \quad \ldots(1.15.3)$$

1.15.1 Bandwidth of ASK :

– For ASK the baud is equal to the bit rate, and the bit rate is also equal to the minimum Nyquist bandwidth.

– We know that,

$$\text{Bandwidth } B = \frac{f_b}{\log_2 M}$$

$$\text{But} \quad \log_2 M = N$$

$$\therefore \quad B = \frac{f_b}{N}$$

– In ASK, M = 2 and N = 1

$$\therefore \quad B = f_b \text{ (Hz)}$$

1.15.2 Merits and Demerits of ASK :

– The advantage of using ASK is its simplicity. It is easy to generate and detect. However its disadvantage is that it is very sensitive to noise, therefore it finds limited application in data transmission.

– ASK system uses and amplitude modulated carrier to transport the digital information. It is a relatively low cost, low quality type of digital modulation.

Application :

– ASK is not used in many applications. One of its applications is very low speed telemetry circuits.

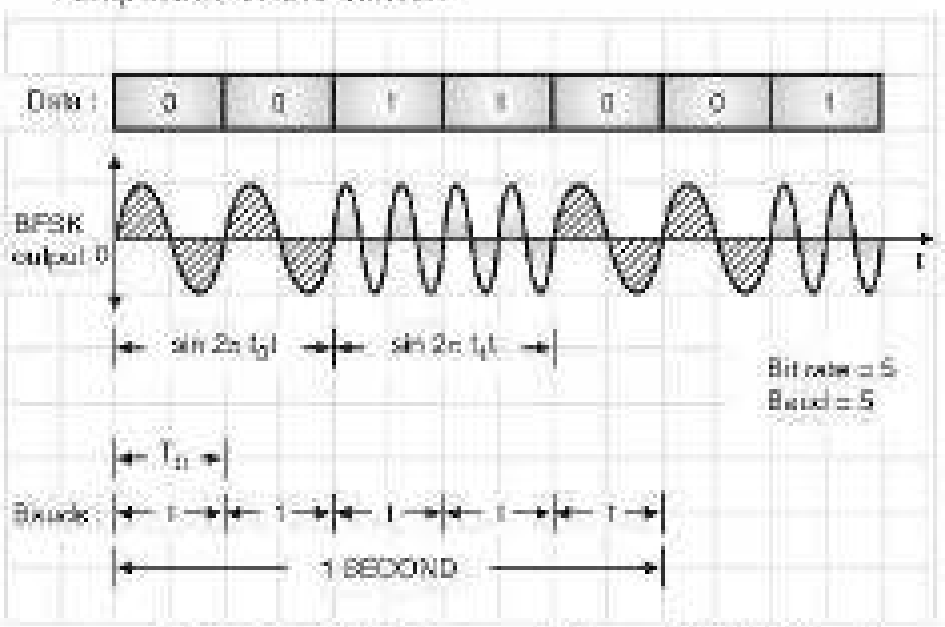
1.16 Frequency Shift Keying (FSK) :

Definition and waveforms :

– FSK is the type of digital modulation in which, the frequency of a sinusoidal carrier is shifted between two discrete values, in response to the value (0 or 1) of the digital input signal.

– One of these frequencies (f_1) represents a binary "1" and the other value (f_0) represents a binary "0".

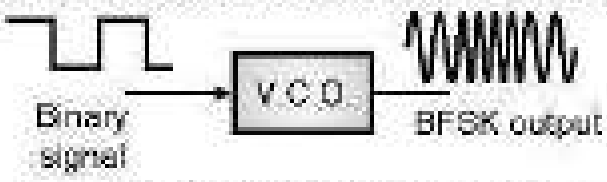
– The representation of digital data using FSK is as shown in Fig. 1.16.1(a). Note that there is no change in the amplitude of the carrier.



(L-902) **Fig. 1.16.1(a) : Representation of digital signal using FSK**

1.16.1 FSK Generation :

– Refer to the FSK generator shown in Fig. 1.16.1(b).



(L-785) **Fig. 1.16.1(b) : FSK generation**

– It is basically a Voltage Controlled Oscillator (VCO) which produce sinewaves at frequencies f_1 and f_0, respectively.

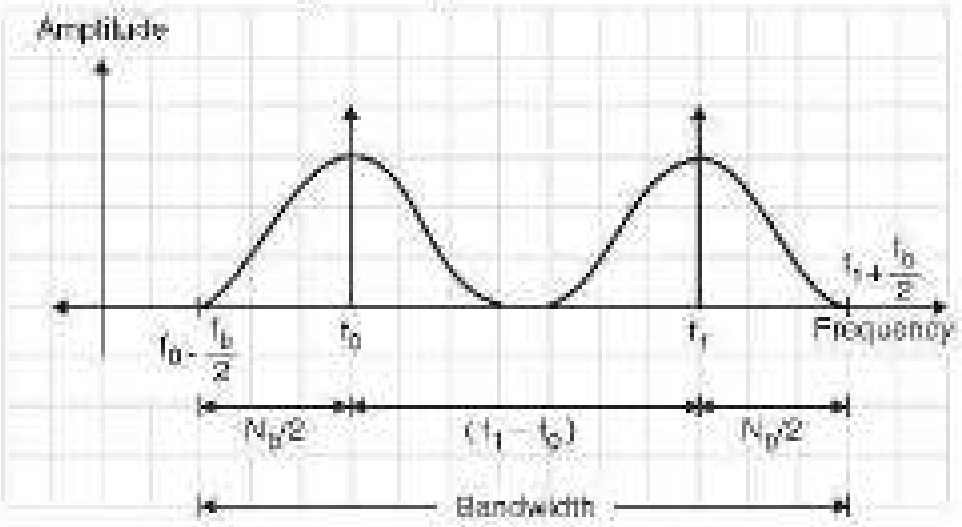
– Corresponding to binary 0 input, the VCO produces a sinewave of frequency f_0 whereas corresponding to binary 1 input, the VCO produces a sinewave of frequency f_1. ($f_1 > f_0$).

– Thus we obtain the Binary FSK (BFSK) signal at the output of VCO corresponding to the input digital data bits.

1.16.2 Bandwidth for FSK in Terms of Baud Rate :

– For FSK also bit rate is equal to baud rate. This is due to the fact that each data bit at the input is treated as a separate symbol.

– We can imagine the FSK spectrum to be a combination of two ASK spectrums centered at frequencies f_1 and f_0 as shown in Fig. 1.16.1(c).



(L-74) **Fig. 1.16.1(c) : Spectrum of FSK**

– From Fig. 1.16.1(c) the expression for bandwidth is given by,

$$BW = \frac{N_b}{2} + (f_1 - f_0) + \frac{N_b}{2}$$

$$= (f_1 - f_0) + N_b \quad ...(1.16.1)$$

Where N_b = Baud rate = Bit rate = f_b

– Minimum bandwidth will correspond to the situation in which $(f_1 - f_0) = N_b$.

$$\therefore \text{BW (min)} = N_b + N_b = 2\,N_b = 2f_b \quad ...(1.16.2)$$

1.16.3 Advantages of FSK :

1. FSK is relatively easy to implement.
2. It has better noise immunity than ASK. Therefore the probability of error free reception of data is high.

1.16.4 Disadvantages of FSK :

1. The major disadvantage is its high bandwidth requirement as discussed earlier.
2. Therefore FSK is extensively used in low speed modems having bit rates below 1200 bits/sec.
3. The FSK is not preferred for the high speed modems because with increase in speed, the bit rate increases.

4. This increases the channel bandwidth required to transmit the FSK signal.
5. As the telephone lines have a very low bandwidth, it is not possible to satisfy the bandwidth requirement of FSK at higher speed. Therefore FSK is preferred only for the low speed modems.

1.16.5 Applications of FSK :

- Binary FSK exhibits a poorer performer than the PSK or QAM systems. Therefore it is very rarely used for high performance digital radio systems.
- Hence generally BFSK is used in the low performance, low quality asynchronous data modems which are used for data communications over analog voice band telephone lines.

1.17 Phase Shift Keying (PSK) :

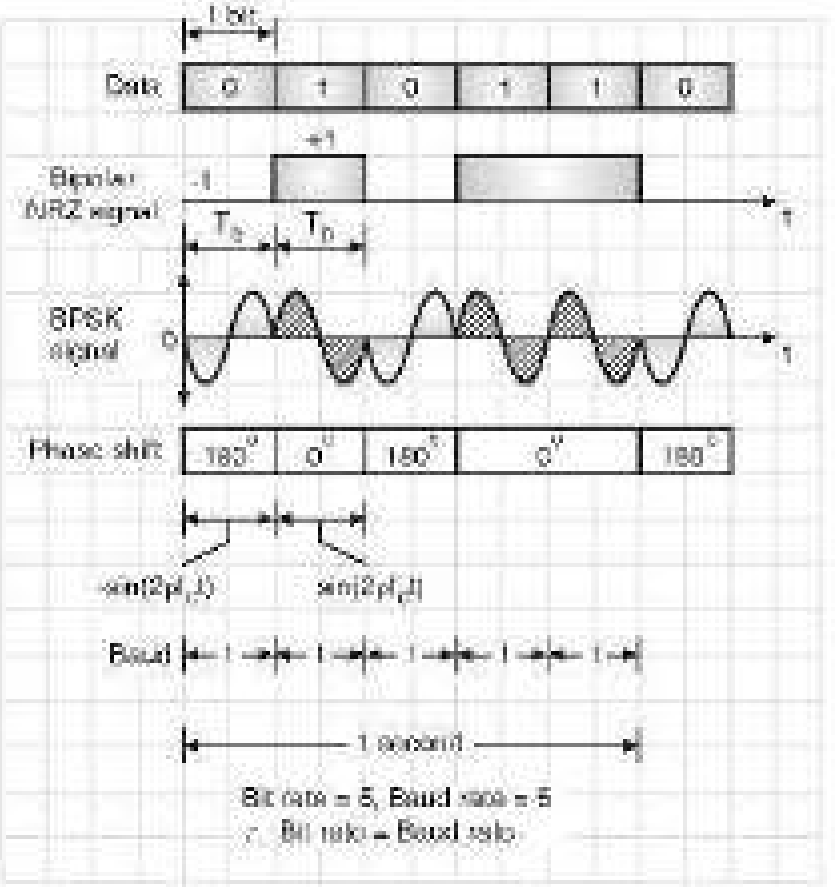
- PSK is another type of digital CW modulation. PSK is an M-ary digital modulation scheme which is similar to the phase modulation.
- However in PSK, the input is a binary digital signal and the number of output phases available is finite (2, 4, 8 etc).
- The input binary bits are grouped into groups of 1, 2, 3, 4 etc (N = 1, 2, 3, 4 ...) and the number of output phases could range from 1 to 12 or even more. The number of output phases is $M = 2^N$.

1.17.1 Binary Phase Shift Keying (BPSK) :

Definition and waveforms :

Definition :

- BPSK is a type of digital modulation in which the phase of a sinusoidal carrier is switched between two distinct values (0° and 180°) corresponding to the values of digital input (0 or 1).
- Phase Shift Keying (PSK) is the most efficient of the three modulation methods.
- Therefore it is used for high bit rates. In PSK, phase of the sinusoidal carrier is changed according to the data bit to be transmitted.
- Fig. 1.17.1(a) shows the simplest form of PSK called Binary PSK (BPSK). The carrier phase is changed between 0° and 180° by the bipolar digital signal. A bipolar NRZ signal is used to represent the digital data from the DTE.



(L-503) **Fig. 1.17.1(a) : Waveform of Binary PSK (BPSK)**

Mathematical Expression :

- The BPSK signal can be represented mathematically as :

$V_{BPSK}(t) = \sin(2\pi f_c t)$ when binary "0" is to be represented

and $V_{BPSK}(t) = -\sin(2\pi f_c t)$

$= \sin(2\pi f_c t + \pi)$ when binary "1" is to be represented.

- Combining the two conditions we can write

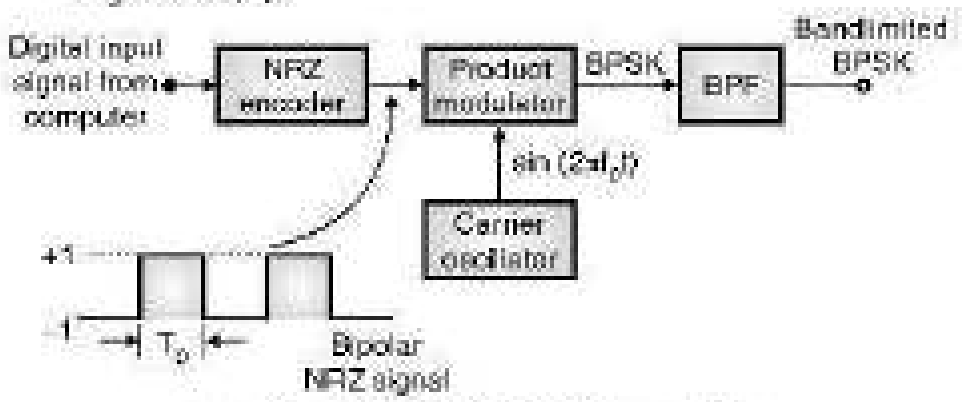
$$V_{BPSK}(t) = d \sin(2\pi f_c t) \quad \ldots(1.17.1)$$

where $d = \perp 1$

1.17.2 BPSK Generation :

Block diagram :

- The BPSK generation takes place as shown in Fig. 1.17.1(b).



(L-81) **Fig. 1.17.1(b) : BPSK generation**

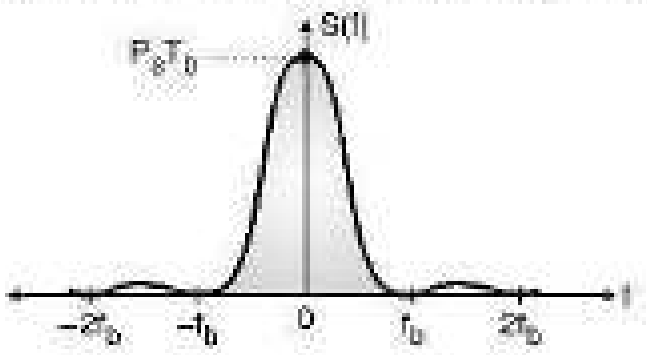
- The binary data signal (0s and 1s) is converted into a NRZ bipolar signal by an NRZ encoder, which is then applied to a multiplier (balanced modulator).

- The other input to the multiplier is the carrier signal ($2\pi f_c t$).
- The data bits 0s and 1s are converted into a bipolar NRZ signal "d" as shown in the following table.

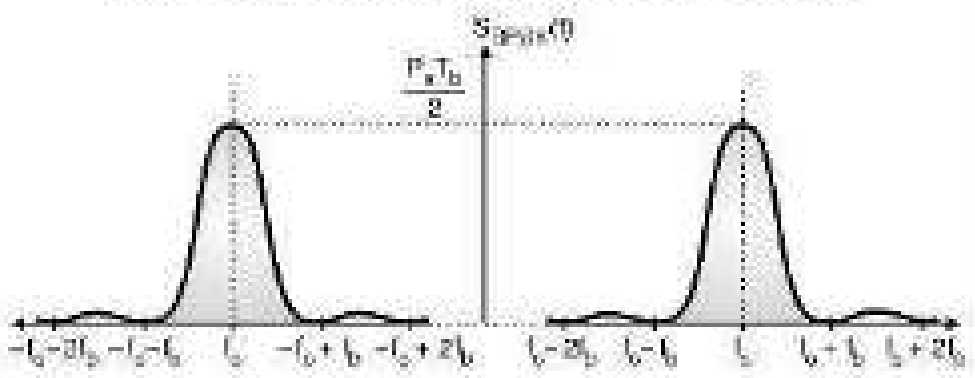
Digital signal	Bipolar NRZ signal	BPSK output
Binary 0	d = 1	$V_{BPSK}(t) = \sin(2\pi f_c t)$
Binary 1	d = – 1	$V_{BPSK}(t) = -\sin(2\pi f_c t)$

1.17.3 Spectrum of BPSK :

- The spectrum of BPSK is as shown in Fig. 1.17.2.



(a) Power spectral density of the NRZ data b(t)



(b) Spectrum of BPSK

(L-88) Fig. 1.17.2 : Spectrum of BPSK

1.17.4 Bandwidth of BPSK :

- From the frequency spectrum of BPSK signal, shown in Fig. 1.17.2(b), we can come to a conclusion that the bandwidth of a BPSK signal is given by,

$$BW = \text{Highest frequency} - \text{Lowest frequency in main lobe}$$

$$= (f_c + f_b) - (f_c - f_b)$$

$$\therefore BW = 2 f_b \quad \text{...(1.17.2)}$$

where $f_b = 1 / T_b$

- Thus the minimum bandwidth of BPSK signal is equal to twice the highest frequency contained in the baseband signal.

Baud rate :

- In BPSK also each digit (0 or 1) of the input digital data represents a symbol. Hence symbol rate is equal to bit rate.

$$\therefore \text{Baud rate } N_b = \text{Bit rate } f_b$$

$$\therefore BW = 2 N_b$$

1.17.5 Advantages of BPSK :

1. BPSK has a bandwidth which is lower than that of a BFSK signal.
2. BPSK has the best performance of all the systems in presence of noise. It gives the minimum possibility of error.
3. BPSK has a very good noise immunity.

1.17.6 Disadvantage of BPSK :

- The only disadvantage of BPSK is that generation and detection of BPSK is not easy. It is quite complicated.

1.17.7 Applications :

- Phase shift keying is the most efficient of the three modulation methods and it is used for high bit rates even higher than 1800 bits/sec.
- Due to low bandwidth requirement the BPSK modems are preferred over the FSK modems, at higher operating speeds.

1.17.8 Comparison of Binary Modulation Systems :

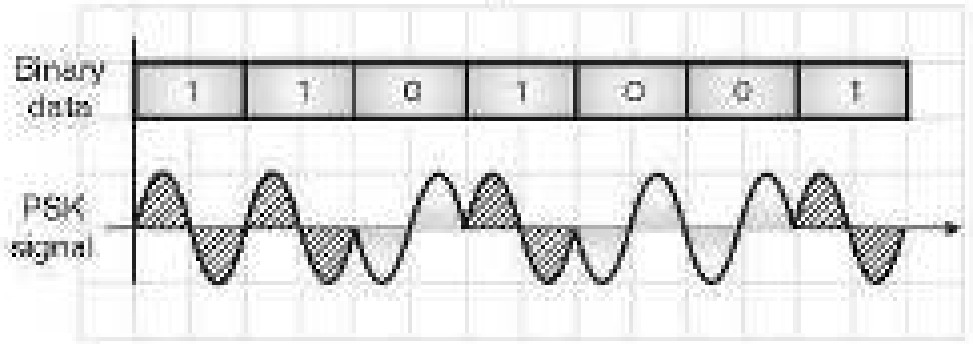
Sr. No.	Parameter	Binary ASK	Binary FSK	Binary PSK
1.	Variable characteristic.	Amplitude	Frequency	Phase
2.	Bandwidth (Hz)	f_b	$2f_b$	$2f_b$
3.	Noise immunity.	Low	High	High
4.	Error probability	High	Low	Low
5.	Performance in presence of noise.	Poor	Better than ASK	Better than FSK
6.	Complexity	Simple	Moderately complex	Very complex

Sr. No.	Parameter	Binary ASK	Binary FSK	Binary PSK
7.	Bit rate	Suitable upto 100 bits/sec.	Suitable upto about 1200 bits/sec.	Suitable for high bit rates.
8.	Detection method.	Envelope	Envelope	Coherent

Ex. 1.17.1 : Sketch the waveform of PSK for the binary sequence 1101001.

Soln. :

– Fig. P. 1.17.1 shows the required waveforms.



(L-904) **Fig. P. 1.17.1**

Ex. 1.17.2 : Find the baud and minimum bandwidth required to pass 10 kbps binary signal using ASK.

Soln. : For ASK,

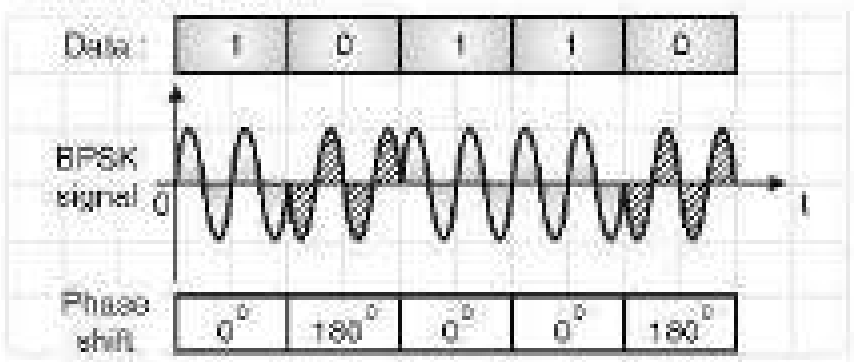
Baud = Bit rate = 10 kbps **...Ans.**

Minimum B.W. = f_b = 10 kHz **...Ans.**

Ex. 1.17.3 : Define PSK and draw the PSK waveform for the data 10110.

Soln. :

Refer Fig. P. 1.17.3.

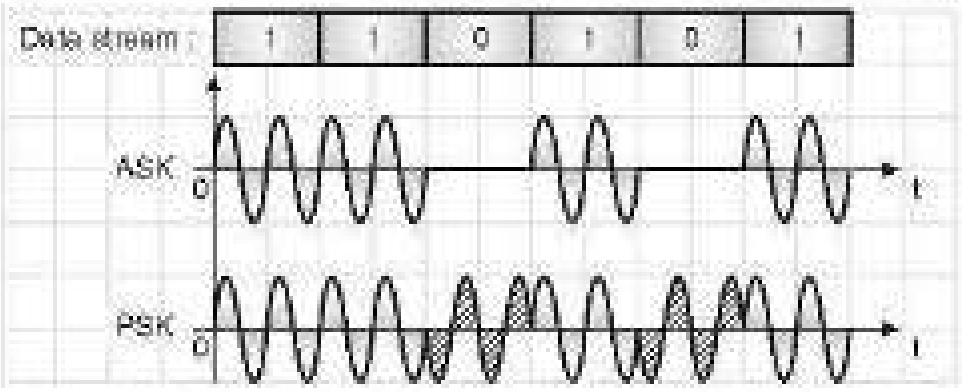


(L-905) **Fig. P. 1.17.3**

Ex. 1.17.4 : Draw ASK and PSK waveforms for a data stream 110101.

Soln. :

Refer Fig. P. 1.17.4.

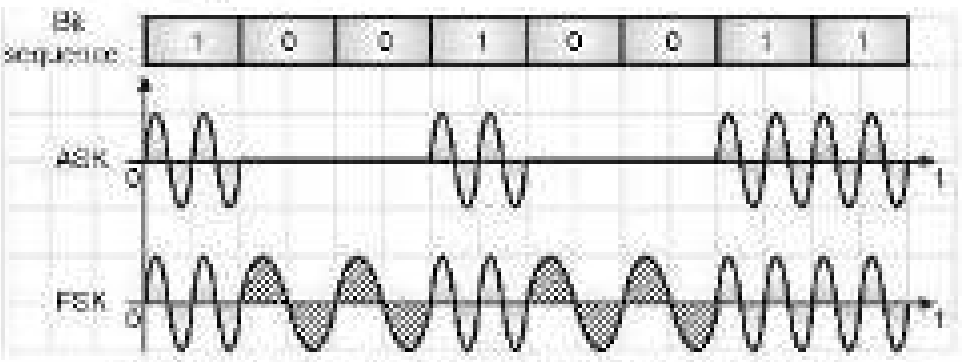


(L-906) **Fig. P. 1.17.4 : ASK and PSK waveforms**

Ex. 1.17.5 : Illustrate binary modulated waveforms of ASK and FSK for the bit sequence 10010011.

Soln. :

Refer Fig. P. 1.17.5.



(L-907) **Fig. P. 1.17.5 : ASK and FSK waveforms**

1.18 Analog to Digital Conversion :

– The process of converting the analog data to digital signal is known as digitisation.

– This process is essential in all the digital communication systems such as Pulse Code Modulation (PCM) or Delta Modulation (D.M).

– In order to carry out this transformation, one has to follow a sequence of operations such as sampling, quantization and encoding.

(L-218) **Fig. 1.18.1 : Transformation from Analog signal to digital signal**

1.19 Pulse Code Modulation (PCM) :

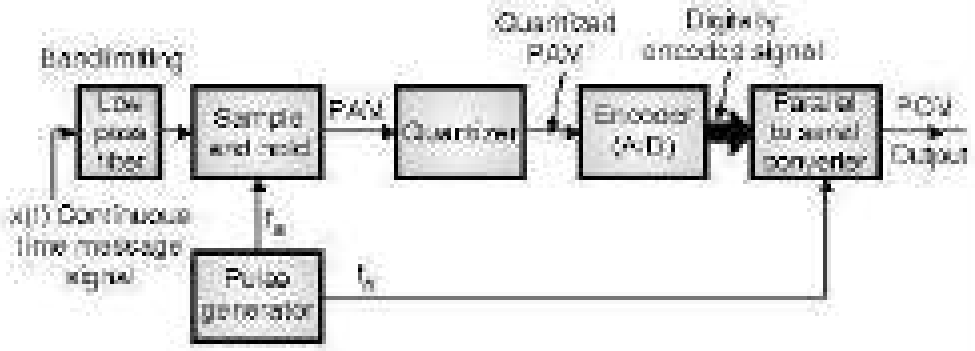
– PCM is a type of pulse modulation like PAM, PWM or PPM but there is an important difference between them. PAM, PWM or PPM are "analog" pulse modulation systems whereas PCM is a "digital" pulse modulation system.

– That means the PCM output is in the coded digital form. It is in the form of digital pulses of constant amplitude, width and position.

- The information is transmitted in the form of "code words". A PCM system consists of a PCM encoder (transmitter) and a PCM decoder (receiver).
- The essential operations in the PCM transmitter are sampling, quantizing and encoding.
- All these operations are usually performed in the same circuit called as analog-to-digital (A to D) converter.
- It should be understood that the PCM is not modulation in the conventional sense.
- Because in modulation, one of the characteristics of the carrier is varied in proportion with the amplitude of the modulating signal. Nothing of that sort happen in PCM.

1.19.1 PCM Transmitter (Encoder) :

- Block diagram of the PCM transmitter is as shown in Fig. 1.19.1.



(L-221) **Fig. 1.19.1 : PCM transmitter (Encoder)**

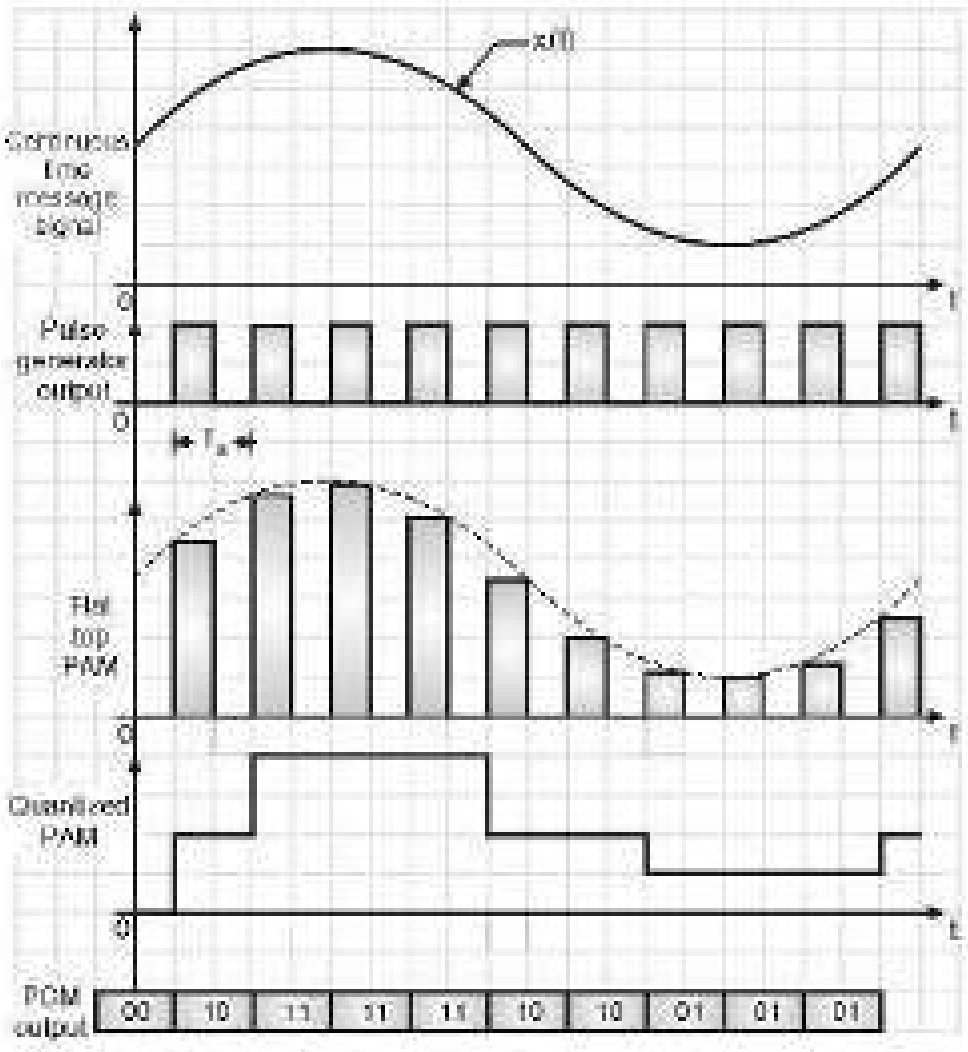
Operation of PCM transmitter :

Operation of the PCM transmitter is as follows :

- The analog signal x (t) is passed through a bandlimiting low pass filter, which has a cut-off frequency f_c = W Hz.
- This will ensure that x (t) will not have any frequency component higher than "W". This will eliminate the possibility of aliasing.
- The band limited analog signal is then applied to a sample and hold circuit where it is sampled at adequately high sampling rate.
- Output of sample and hold block is a flat topped PAM signal.
- These samples are then subjected to the operation called "Quantization" in the "Quantizer". Quantization process is the process of approximation.
- The quantization is used to reduce the effect of noise. The combined effect of sampling and quantization produces the quantized PAM at the quantizer output.
- The quantized PAM pulses are applied to an encoder which is basically an A to D converter.
- Each quantized level is converted into an N bit digital word by the A to D converter. The value of N can be 8, 16, 32, 64 etc.
- The encoder output is converted into a stream of pulses by the parallel to serial converter block. Thus at the PCM transmitter output we get a train of digital pulses.
- A pulse generator produces a train of rectangular pulses with each pulse of duration "τ" seconds.
- The frequency of this signal is "f_s" Hz. This signal acts as a sampling signal for the sample and hold block.
- The same signal acts as "clock" signal for the parallel to serial converter. The frequency "f_s" is adjusted to satisfy the Nyquist criteria.

Waveforms :

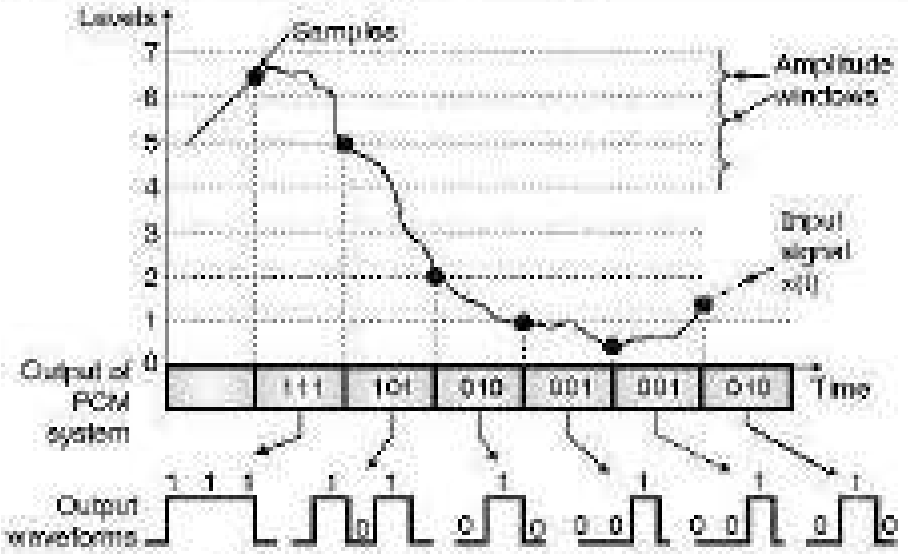
- The waveforms at various points in the PCM transmitter are as shown in Fig. 1.19.2.



(L-222) **Fig. 1.19.2 : Waveforms at different points in PCM transmitter**

1.19.2 Shape of the PCM Signal :

- Fig. 1.19.3 shows input to and output of a PCM system. It is important to understand that the output is in the form of binary codes.

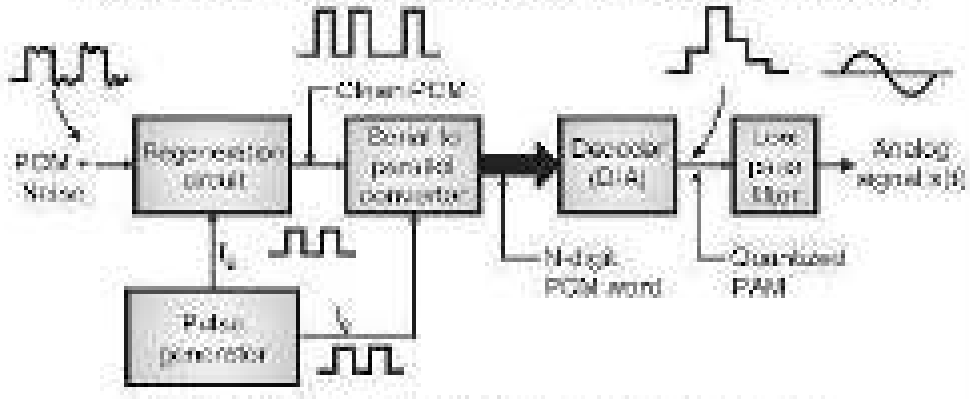


(L-223) **Fig. 1.19.3 : Input and output waveforms of a PCM system**

- Each transmitted binary code represents a particular amplitude of the input signal.
- Hence the "information" is contained in the "code" which is being transmitted.
- The range of input signal magnitudes is divided into 8 equal levels. Each level is denoted by a three bit digital word between 000 and 111.
- Input signal x (t) is sampled. If the sample is in the 5th - window of amplitude then a digital word 101 is transmitted.
- If the sample is in the 2nd - window then the transmitted word is 010 and so on.
- In this example we have converted the amplitudes into 3 bit codes, but in practice the number of bits per word can be as high as 8, 9 or 10.

1.19.3 PCM Receiver (Decoder) :

- Fig. 1.19.4 shows the block diagram of a PCM receiver.



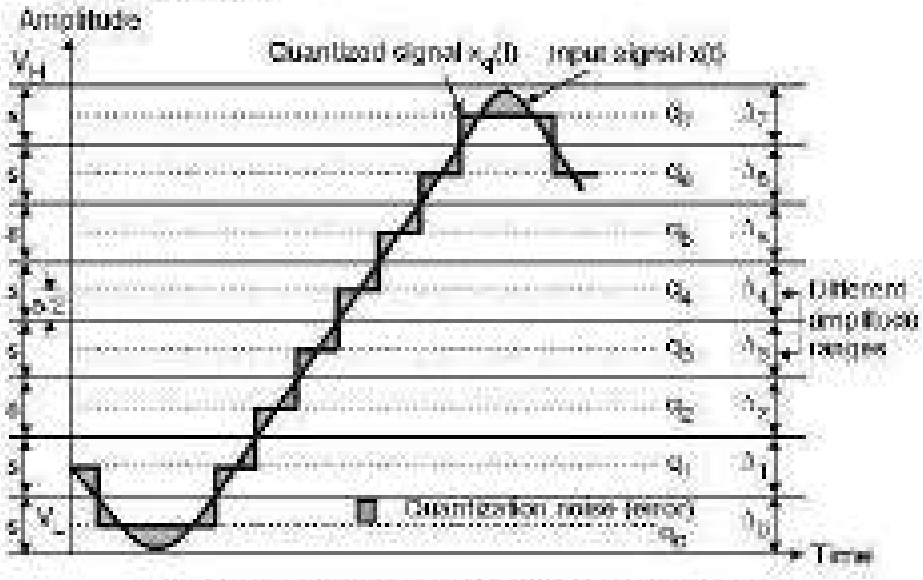
(L-224) **Fig. 1.19.4 : PCM receiver (Decoder)**

Operation of PCM receiver :

- A PCM signal contaminated with noise is available at the receiver input.
- The regeneration circuit at the receiver will separate the PCM pulses from noise and will reconstruct the original PCM signal.
- The pulse generator has to operate in synchronization with that at the transmitter.
- Thus at the regeneration circuit output we get a "clean" PCM signal.
- The reconstruction of PCM signal is possible due to the digital nature of PCM signal.
- The reconstructed PCM signal is then passed through a serial to parallel converter.
- Output of this block is then applied to a decoder.
- The decoder is a D to A converter which performs exactly the opposite operation of the encoder.
- The decoder output is the sequence of a quantized multilevel pulses. The quantized PAM signal is thus obtained, at the output of the decoder.
- This quantized PAM signal is passed through a low pass filter to recover the analog signal, x (t).
- The low pass filter is called as the reconstruction filter and its cut off frequency is equal to the message bandwidth W.

1.19.4 Quantization Process :

- Quantization is a process of approximation or rounding off. The sampled signal in PCM transmitted is applied to the quantizer block.
- Quantizer converts the sampled signal into an approximate quantized signal which consists of only a finite number of predecided voltage levels.
- Each sampled value at the input of the quantizer is approximated or rounded off to the nearest standard predecided voltage level.
- These standard levels are known as the "quantization levels". Refer to Fig. 1.19.5 to understand the process of quantization.



(L-225) **Fig. 1.19.5 : Process of quantization**

- The quantization process takes place as follows :
- The input signal x (t) is assumed to have a peak to peak swing of V_L to V_H volts. This entire voltage range has been divided into "Q" equal intervals each of size "s".

  "s" is called as the step size and its value is given as,

$$s = \frac{V_H - V_L}{Q} \quad \ldots(1.19.1)$$

- In Fig. 1.19.5, the value of Q = 8.
- At the center of these ranges, the quantization levels q_0, q_1,...q_7 are placed. Thus the number of quantization levels is Q = 8.
- The quantization levels are also called as decision thresholds.
- x_q (t) represents the quantized version of x (t). We obtain x_q (t) at the output of the quantizer.
- When x (t) is in the range Δ_0, then corresponding to any value of x (t), the quantizer output will be equal to "q_0".
- Similarly for all the values of x (t) in the range Δ_1, the quantizer output is constant equal to "q_1".
- Thus in each range from Δ_1 to Δ_8, the signal x (t) is rounded off to the nearest quantization level and the quantized signal is produced.
- The quantized signal x_q (t) is thus an approximation of x (t). The difference between them is called as **quantization error or quantization noise.**
- This error should be as small as possible.
- To minimize the quantization error we need to reduce the step size "s" by increasing the number of quantization levels Q.

Why is quantization required ?

- If we do not use the quantizer block in the PCM transmitter, then we will have to convert each and every sampled value into a unique digital word.
- This will need a large number of bits per word (N). This will increase the bit rate and hence the bandwidth requirement of the channel.
- To avoid this, if we use a quantizer with only 256 quantization levels then all the sampled values will be finally approximated into only 256 distinct voltage levels.
- So we need only 8 bits per word to represent each quantized sampled value.
- Thus the number of bits per word can be reduced. This will eventually reduce the bit rate and bandwidth requirement.

1.19.5 Quantization Error or Quantization Noise ∈ :

- The difference between the instantaneous values of the quantized signal and input signal is called as quantization error or quantization noise.

$$\epsilon = x_q(t) - x(t) \quad \ldots(1.19.2)$$

- The quantization error is shown by shaded portions of the waveform in Fig. 1.19.5.
- The maximum value of quantization error is $\pm s / 2$ where s is step size.
- Therefore to reduce the quantization error we have to reduce the step size by increasing the number of quantization levels i.e. Q.
- The mean square value of the quantization is given by,

$$\text{Mean square value of quantization error} = \frac{s^2}{12} \quad \ldots(1.19.3)$$

- The relation between the number of quantization levels Q and the number of bits per word (N) in the transmitted signal can be found as follows :
- Because each quantized level is to be converted into a unique N bit digital word, assuming a binary coded output signal,
- The number of quantization levels Q = Number of combinations of bits/word.

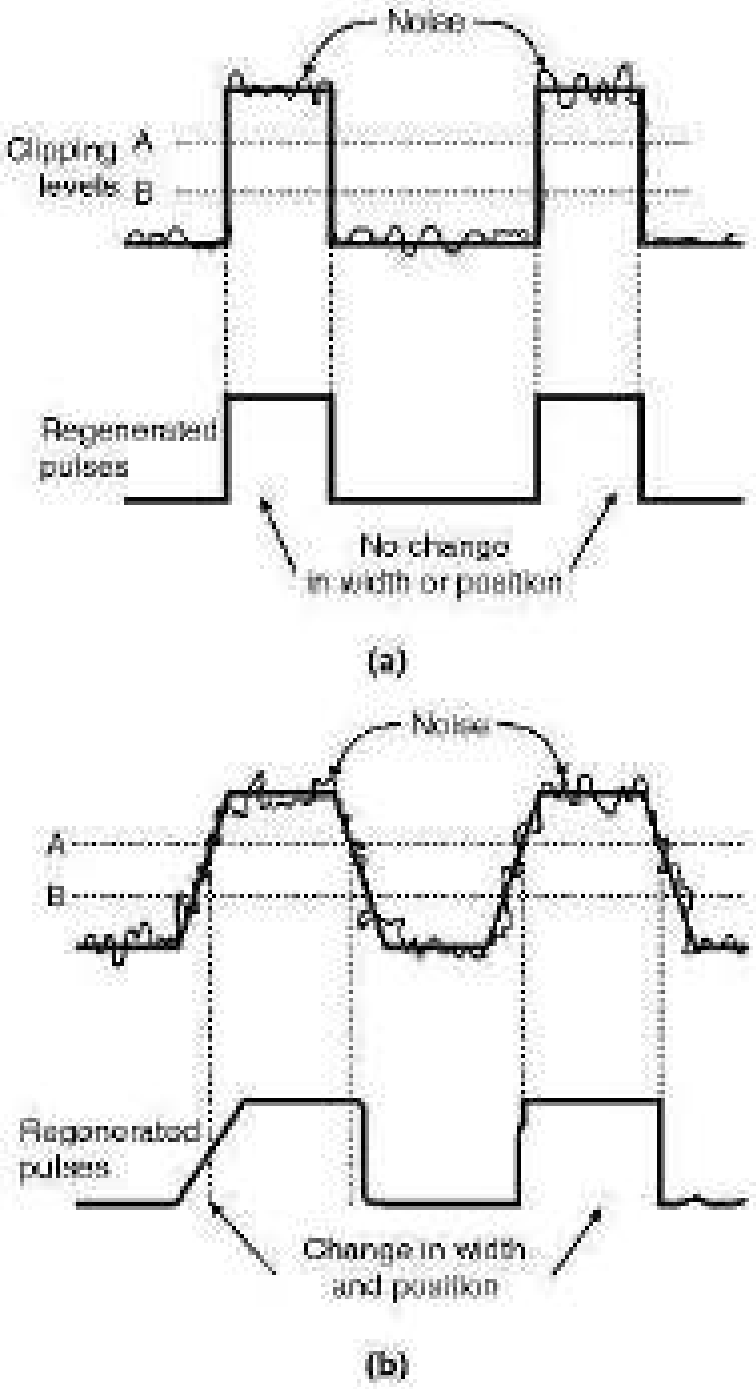
$$\therefore \quad Q = 2^N \quad \ldots(1.19.4)$$

- Thus if N = 4 i.e. 4 bits per word then the number of quantization levels will be 2^4 i.e. 16.

1.19.6 Effect of Noise on the PCM System :

- Look at the two Figs. 1.19.6(a) and 1.19.6(b) which illustrate the effect of noise on the transmitted pulses.
- Consider Fig. 1.19.6(a) first. Due to the noise superimposed on the pulses, only the PAM system will be affected.
- However the PWM, PFM and PCM systems will remain unaffected. The regeneration of the pulses is achieved by using a clipper circuit with reference levels A and B.

– Now consider Fig. 1.19.6(b). Here the sides of the transmitted pulse are not perfectly vertical. In practice the transmitted pulses usually have slightly sloping sides (edges).



(L-229) **Fig. 1.19.6 : Effect of noise on PCM**

– As the noise is superimposed on them, the width and the position of the regenerated pulses is changed.
– Now this is going to distort the information contents in the PWM and PPM signals.
– But PCM is still unaffected as it does not contain any information in the width or the position of the pulses.
– Thus PCM has much better noise immunity as compared to PAM, PWM and PPM systems.

1.20 Advantages, Disadvantages and Applications of PCM :

– The PCM is considered to be the best modulation scheme to transmit the voice and video signals.
– All the advantages of PCM are due to the fact that it uses coded pulses for the transmission of information.

1.20.1 Advantages of PCM :

1. Very high noise immunity (Noise does not affect the information content).
2. Due to digital nature of the signal, repeaters can be placed between the transmitter and the receivers. The repeaters actually regenerate the received PCM signal. This is not possible in analog systems. Repeaters further reduce the effect of noise.
3. It is possible to store the PCM signal due to its digital nature.
4. It is possible to use various coding techniques so that only the desired receiver can decode the received signal. This makes the communication secure.
5. The increased channel bandwidth requirement for PCM is balanced by the improved SNR. This is the due to the fact that PCM obeys an exponential law.
6. There is a **uniform format** used for the transmission of different types of base band signals. Hence it is easy to integrate all these signals together and send them on the common network.
7. It is easy to drop or reinsert the message sources in a PCM-TDM system.

1.20.2 Disadvantages of PCM :

1. The encoding, decoding and quantizing circuitry of PCM is complex.
2. PCM requires a large bandwidth as compared to the other systems.

1.20.3 Applications of PCM :

– Some of the applications of PCM are as follows :
  1. In telephony (with the advent of fibre optic cables).
  2. In the space communication, space craft transmits signals to earth. Here the transmitted power is very low (10 to 15W) and the distances are huge (a few million km). Still due to the high noise immunity, only PCM systems can be used in such applications.

Other A to D conversion systems :

– Some other A to D conversion systems are :
  1. Delta modulation (D.M.)
  2. Differential PCM (DPCM).
  3. Adaptive delta modulation (ADM).

Review Questions

Q. 1 What are the characteristics of data communication system ?

Q. 2 Which are the components of data communication system ?

Q. 3 State and explain the important elements of a protocol.

Q. 4 Define a protocol.

Q. 5 Define standards and state its types.

Q. 6 State and explain about various standard organizations.

Q. 7 Explain the concept of signal propagation.

Q. 8 Define a signal and state its types.

Q. 9 Define analog and digital signals.

Q. 10 Compare analog and digital signals.

Q. 11 Define medium and state its examples.

Q. 12 Define signal bandwidth and state its values for different types of signals.

Q. 13 Define the term "bandwidth of a medium" and state its importance.

Q. 14 Define the terms; amplitude, frequency and phase of a signal.

Q. 15 Define bit rate and baud rate.

Q. 16 Write a note on data transmission rate and bandwidth.

Q. 17 List the modes of data transmission.

Q. 18 Explain half duplex system and full duplex system.

Q. 19 What are the standard organizations for data communication ?

Q. 20 What is quantizing noise ?

Q. 21 State the applications of PCM signals.

Q. 22 What is quantization ?

Q. 23 What is quantization error ? What is its maximum value ?

Q. 24 How to reduce the quantization error ?

Q. 25 Draw and explain the block diagram for generation of PCM signal.

Q. 26 State the bandwidth requirement of ASK system.

Q. 27 What is the maximum B.W. of BPSK system ?

Q. 28 Draw the BPSK signal for the following binary signal.

1 0 1 1 1 0 1 0

Q. 29 State the expression for BFSK.

Q. 30 How is a message transmitted in BFSK ?

Q. 31 What is the BW of BFSK ?

Q. 32 State merits and demerits of BASK.

Q. 33 Compare ASK and FSK.

Q. 34 Draw the waveforms for FSK and PSK modulation.

Q. 35 What is ASK ? Draw its waveform ?

Q. 36 Draw the block diagram of binary PSK system and explain with signal space diagram.

Q. 37 Write an expression for the BFSK and explain the spectrum of BFSK.

Q. 38 Draw the BFSK waveform to represent the following bit stream : 00101110.

1.21 I-Scheme Questions and Answers :

Summer 2019 [Total Marks - 10]

Q. 1 Compare analog and digital signals.

(Section 1.5.4) **(4 Marks)**

Q. 2 Describe the process of data communication in various modes.

(Sections 1.12, 1.12.1, 1.12.2 and 1.12.3) **(6 Marks)**

Winter 2019 [Total Marks - 18]

Q. 3 Define bit rate and baud rate.

(Sections 1.8.2 and 1.8.3) **(2 Marks)**

Q. 4 List different characteristics of data communication system. (Any two) **(Section 1.2.2)** **(2 Marks)**

Q. 5 Differentiate between synchronous and asynchronous communication. (Any four points.) **(4 Marks)**

Ans. :

Comparison of synchronous and asynchronous communication :

Table 1 : Comparison of synchronous and asynchronous communication

Sr. No.	Parameter	Asynchronous transmission	Synchronous transmission
1.	Synchronization	Not needed	Needed
2.	Start and Stop bits	Used	Not used
3.	Gaps between data blocks	Present	Absent
4.	Speed	Low	High
5.	Application	Communication between a computer and keyboard.	Communication between two computers.

Q. 6 Draw and explain block diagram of communication system. **(Section 1.3)** **(4 Marks)**

Q. 7 Explain simplex, half duplex and full duplex modes in data communication.

(Sections 1.12.1, 1.12.2 and 1.12.3) **(6 Marks)**

Summer 2022 [Total Marks - 12]

Q. 8 Define :

i. Bit rate. **(Section 1.8.2)**

ii. Baud rate. **(Section 1.8.3)** **(2 Marks)**

Q. 9 Define following terms :

i. Protocol. **(Section 1.4.1)**

ii. Bandwidth. **(Section 1.7)** **(2 Marks)**

Q. 10 Describe modes of communication.

(Sections 1.12.1, 1.12.2 and 1.12.3) **(4 Marks)**

Q. 11 Describe the components of data communication with neat diagram. **(Section 1.3)** **(4 Marks)**

❑❑❑

Chapter 2

Fundamentals of Computer Network

Syllabus

Fundamentals of computer network, Definition and need of computer network, Applications, Network benefits-Classification of network LAN, MAN, WAN, Network architecture : Peer-to-Peer network, Client-server network.

Chapter Contents

2.1 A Network : S-12

MSBTE Questions

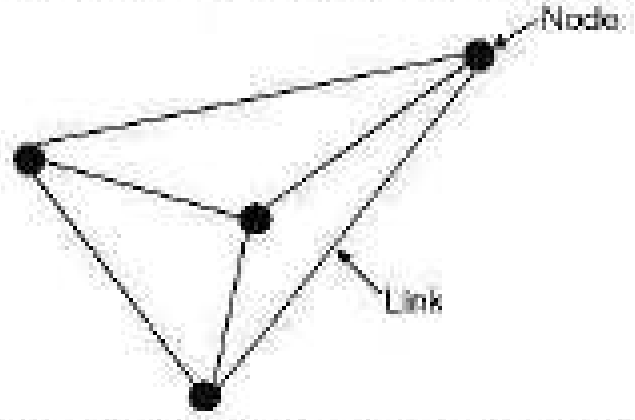
Q. 1 Define network. **(S-12, 2 Marks)**

Network :

- Network is a broad term similar to "system". Network is a communication system which supports many users.
- The interconnection of one station to many stations is called as networking.
- A network is any interconnection of two or more stations that wish to communicate.

Node :

- Each station in a communication network is called as a node. The nodes are connected in different way to each other to form a network.
- One of such networks is shown in Fig. 2.1.1.
- Many other forms of interconnections are possible. The most familiar network is the telephone system. It is the largest and most sophisticated network of all.



[G-13] **Fig. 2.1.1 : A simple communication network**

2.1.1 Computer Networks :

S-08, S-11, S-12, W-12, S-13, S-14, S-16, W-16, S-17, I-Scheme : S-19, S-22

MSBTE Questions

Q. 1 Define protocol. **(S-08, S-11, S-12, W-12, 2 Marks)**

Q. 2 Define computer network. **(W-12, 2 Marks)**

Q. 3 Define the term : Protocol. **(S-13, 1 Mark)**

Q. 4 Define 'Protocol' with reference to computer network. What is the function of IP ? **(S-14, 2 Marks)**

Q. 5 Define computer network. **(S-16, 2 Marks)**

Q. 6 Define : Protocol **(S-16, 1 Mark)**

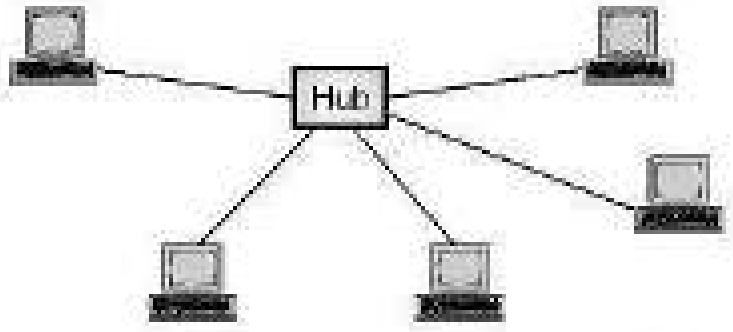
Q. 7 Define protocol. State the need for the same. **(W-16, 2 Marks)**

Q. 8 Define protocol. **(S-17, 2 Marks)**

- In contest with the computers we can say that a "computer network" is a system which allows communication among the computers connected in the network.
- During 20th century the most important technology has been the information gathering, its processing and distribution.
- The computers and communications have been merged together and their merger had a very deep impact on the manner in which computer systems are organized.
- In the old model a single computer used to serve all the computational needs of an organization. But now it is replaced by a new model in which a large number of separate but interconnected computers do the job.
- Such systems are called as **computer networks.**

Definition :

- A computer network is a group of computers and other computing hardware devices are linked together through communication channels to facilitate communication and resource sharing among wide range of users.
- Two computers are said to be interconnected if they exchange information. The connection between the separate computers can be done via a copper wire, fiber optics, microwaves or communication satellite.
- As shown in Fig. 2.1.2, each node in a computer network is a computer, or a connecting device such as a hub, or a switch etc.



(S-13)(S-19) **Fig. 2.1.2 : A computer network**

- The computers connected in a network share files, folders, applications and resources like scanners, web-cams, printers etc.
- The best example of a computer network is the Internet.
- In a computer network we need to make use of hardware and software.
- The **hardware** consists of connecting cables, connectors, network connecting devices and the **software** consists of protocols, programs etc.

- This enables the systematic exchange of information between the computers connected in the network.
- There are various ways of interconnecting the computers.

Protocol :

- For successful communication to occur, it is not enough for the "sender" to simply transmit the message and "assume" that the "receiver" will receive it properly.
- There are certain rules that must be followed to ensure proper communication.
- A set of such rules is known as a "protocol" of the computer communication system.

Definition :

- Protocol is defined as the set of rules agreed upon by the sending and receiving computer systems, to facilitate a proper communication between them.
- Many different protocols are used in the modern computer communication system.

Need :

- Protocols are needed to ensure proper communication among the computers connected in a computer network.

2.1.2 Need and Applications of Computer Network :

W-09, S-10, S-14, W-14, S-16, W-16, I-Scheme : S-19

MSBTE Questions

Q. 1 Explain the need of computer network. **(W-09, S-10, 4 Marks)**

Q. 2 List any two applications of computer network. **(S-14, 2 Marks)**

Q. 3 Enlist eight applications of computer network. **(W-14, 4 Marks)**

Q. 4 List two applications of computer network. **(S-16, 2 Marks)**

Q. 5 State the need of computer network. **(W-16, S-18, 2 Marks)**

- The computer networks are needed because of the following points :

1. For sharing the resources such as printers among all the users.
2. For sharing of expensive softwares and database.
3. To facilitate communication from one computer to the other.
4. To have exchange of data and information amongst the users, via the network.
5. For sharing of information over the geographically wide areas.
6. For connecting the computers between various buildings of an organization.
7. For educational purposes.

2.1.3 Components of a Computer Network :

S-14, W-14, S-15

MSBTE Questions

Q. 1 What are the various components of computer network ? **(S-14, 4 Marks)**

Q. 2 Enlist the components of computer network. **(W-14, 4 Marks)**

Q. 3 Enlist essential components required to design computer networks. **(S-15, 4 Marks)**

- Following are some of the important components of a computer network.

1. Two or more computers.
2. Cables (coaxial, twisted pair or fiber optic) as links between the computers.
3. A Network Interfacing Card (NIC) on each computer.
4. Switches or other suitable connecting device.
5. A software called network operating system.

2.2 Network Benefits : W-11

MSBTE Questions

Q. 1 Explain benefits of computer network. **(W-11, 4 Marks)**

- A network is supposed to provide its uses some unique capabilities, better than what the individual machines and their software can provide.
- The benefits provided by the network to the users can be divided into two categories as follows :

1. Sharing. 2. Connectivity.

2.2.1 Sharing Information : S-11, W-11

MSBTE Questions

Q. 1 State any four benefits of networking. **(S-11, 2 Marks)**

Q. 2 Explain benefits of computer network. **(W-11, 4 Marks)**

- Networking allows the users to access the data stored on other's computers.
- It is possible for every user to share his bit of information with the other users over the network.
- The information sharing can be in the form of exchange of data, chatting, sending E-mails, sharing video information, groups etc.
- It is also possible for the users to share the information about various products, movies, technical information, cooking, travel books on internet.
- Sharing of information via Internet has become very common now a days.
- The information which is to be shared or being shared should be shared centrally, it must be kept consistent and secured.
- The access to this stored information should be allowed only to the authorized users.
- Sharing of information eliminates the need of transferring files on CDs or pen drives etc.

2.2.2 Sharing Resources :

S-09, W-15, S-16, W-16

MSBTE Questions

Q. 1 What is meant by file sharing and printer sharing ? How this can be achieved ? **(S-09, W-15, 4 Marks)**

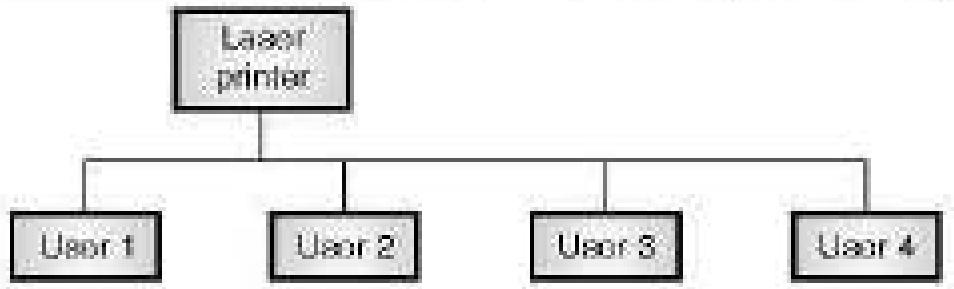
Q. 2 Explain which resources can be shared in computer networks. **(S-16, 4 Marks)**

Q. 3 Name any four resources that can be shared in a computer network. **(W-16, 4 Marks)**

- Networks can allow its users to share various types of resources. We can broadly categorize the shared resources as follows :
  1. Shared hardware resources.
  2. Shared software resources.

1. Sharing of hardware resources :

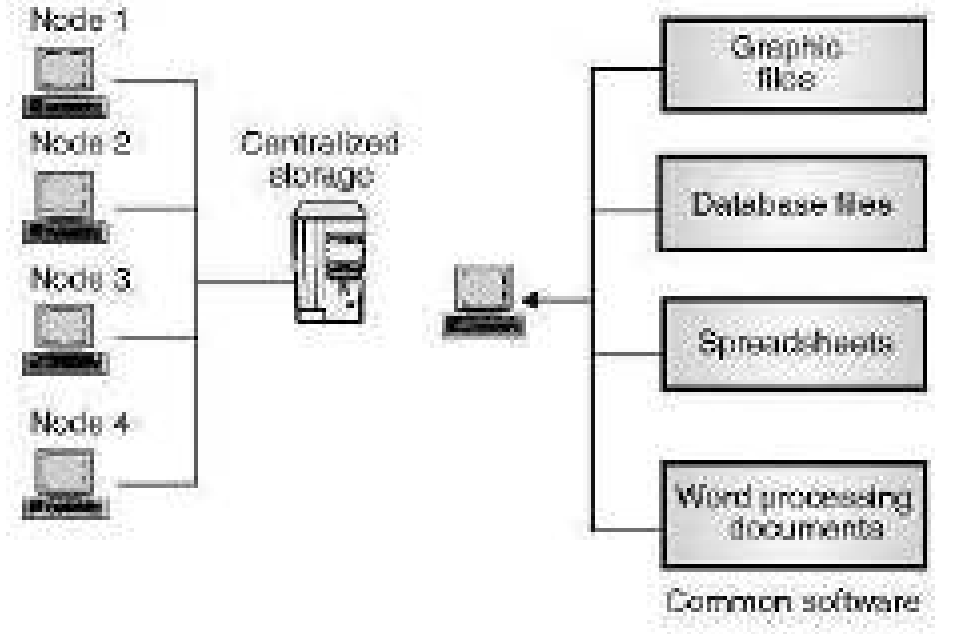
- A network allows its users to share the many hardware devices such as printers, modems, fax machines, CD ROM players etc.
- These resources are available to anyone on the network irrespective of the physical location of the resource and the user.
- This will save the expenses on duplication of such hardware resources Fig. 2.2.1 shows a laser printer being shared by many users.



(G-1398) **Fig. 2.2.1 : Sharing of hardware resources**

2. Sharing of software resources :

- With every computer, we need to install some basic software's on each computer's hard disk.
- So each computer on the network will have to purchase a separate copy of each software required to be used. This will increase the cost to be incurred.
- In addition, installing software on each computer is time consuming and difficult.
- This problem can be overcome by using the concept of software resource sharing.
- In a network, we can centrally install and configure only one copy of each software and share it among rest of the computers.
- This actually saves a lot of time and cost Fig. 2.2.2 shows the principle of software sharing.



(G-1399) **Fig. 2.2.2 : Sharing of software resources**

2.2.3 Facilitating Centralized Management :

S-11, S-14, W-16

MSBTE Questions

Q. 1 List any four network tools used for maintaining network. **(S-11, 2 Marks)**

Q. 2 Explain computer network facilities in terms of centralized network management. **(S-11, 4 Marks)**

Q. 3 Describe in brief backing up data. **(S-14, 2 Marks)**

Q. 4 State four benefits of network used for centralized management. **(W-16, 4 Marks)**

- The computer network facilitates centralized network management with respect to following :
  1. Management of software.
  2. Maintenance of network.
  3. Keeping the data backup.
  4. Central network security.
- All this is allowed by the **client – server** network.

Managing software :

- As discussed earlier, it is a very good idea to share the software resources, instead of installing a separate copy of software on each computer.
- It is possible to load all the important software on a single computer (server).
- All the other computers can make use of this centralized software as per their requirements.
- This reduces the expenses in buying the expensive software's for each individual computer. It also makes the virus checks easy.
- We can add new computers on the existing network without purchasing the software's again.
- Thus the network helps in maintaining a centralized software bank.

Maintenance of network :

- The second aspect in the centralized management is the maintenance of network.
- The centralized management allows quick and easy way to the routine maintenance of network.
- The client server networks are maintained centrally. It is an important but difficult job.
- A central administrator keeps track of the status of the network in respect of its speed, traffic, performance and security.
- Some of the network maintenance tools available to help the network maintenance are as follows :
  1. Protocol analyzer.
  2. Event viewer.
  3. Performance monitor.
  4. Network analyzer.
  5. Network management protocol.

Backing up data :

- In the process of data backup, data from computer system is copied from the disk to some other medium for keeping it safe.
- Taking backup periodically is important because it protects the data against any unpredictable, accidental loss of data due to system failure, computer viruses, or human error.
- But taking a backup of individual user's data separately is a time consuming and unorganized.
- Hence in a network, the users first save their important data on the central server and then the backup can be taken on the server data.
- This reduces the time and stores the backup data at a signal place only. This makes the data retrieval easy.
- We can have two or three sets of the entire backup data. This helps in the event of one or two sets getting corrupt. The duplication of backup data becomes easily possible due to centralized storage.
- The centralized backup procedures have become easy now a days due to the advanced technology.
- There are two basic network backup strategies :
  1. Isolated backup.
  2. Centralized backup.
- The operating systems will provide tools required for data backups. For example windows NT proves a tape backup program called as **backup.**
- A proper backup policy which is suitable for the given network should be selected. Some of the backup policies are as follows :
  1. Full backup.
  2. Replication.
  3. Incremental or partial backup.

2.2.4 Other Benefits of Computer Networks :

S-09, S-11, S-14, S-15, W-15, S-16, S-17

MSBTE Questions

Q. 1 List advantages of computer networks. **(S-09, W-15, 2 Marks)**

Q. 2 Give the advantages and disadvantages of computer networks. **(S-11, 4 Marks, S-15, 8 Marks)**

Q. 3 Describe four advantages of computer network. **(S-14, 4 Marks)**

Q. 4 Explain any four benefits of computer network. **(S-14, 4 Marks)**

Q. 5 State four benefits of computer networks. **(S-16, 4 Marks)**

Q. 6 List advantages of computer network. **(S-17, 2 Marks)**

- Following are some of the other advantages of computer networks.

1. **Increased speed :**

- Networks provide a very fast means for sharing and transfer of files.
- If the computer networks would not have been there, then we would have to copy the files on CDs or pen drive and send them to the other computers.

2. **Reduced cost :**

- Many popular versions of softwares usable for the entire network are now available at a considerably reduced costs as compared to individual licensed copies.
- In addition to this it is also possible to share a program on a network. It is also possible to upgrade the program.

3. **Improved security :**

- It is possible to protect the programs and files from illegal copying.
- By allotting password the access can be restricted to authorized users only.

4. **Centralized software managements :**

- Due to the use of computer networks, all the softwares can be loaded on one computer.
- All the other computers can make use of this centralized software.
- It is not necessary to waste time and energy in installing updates and tracking files on independent computers.

5. **Electronic-mail :**

- The computer network makes the hardware available which is necessary to install an e-mail system.
- The person to person communication is improved due to a presence of e-mail system.

6. **Flexible access :**

- It is possible for the authorized users to access their files from any computer connected on the network.
- This provides tremendous flexibility in accessing.

2.2.5 Disadvantages of Networks : S-11, S-15

MSBTE Questions

Q. 1 Give the advantages and disadvantages of computer networks. **(S-11, 4 Marks, S-15, 8 Marks)**

- Following are some of the disadvantages of computer networks.

1. **High cost of installation :**

- The initial cost of installation of a computer network is high.
- This is due to the cost of cables, network cards, computers, printers and various softwares that are required to be installed.
- The cost of services of technicians may also get added.

2. **Requires time for administration :**

- Computer networks need proper and careful administration and maintenance. This is a time consuming job.

3. **Failure of server :**

- If the file servers "goes down" then the entire network comes to a standstill.
- If this happens then the entire organization can lose its valuable time and access to the necessary programs and files.

4. **Cable faults :**

- The computers in a network are interconnected with the help of connecting cables. So cable faults can paralize a network.

2.3 Network Services :

- The computer networks are playing an important role in providing services to large organizations as well as to the individual common man.

2.3.1 Service Provided by the Network for Organizations :

- Many organizations have a large number of computers in operation.
- These computers may be within the same building, campus, city or different cities.

– Eventhough the computers are located in different locations, the organisations want to keep track of inventories, monitor productivity, do the ordering and billing etc.

– The computer networks are useful to the organisations in the following ways :

1. Resource sharing :

– It allows all programs, equipments and data available to anyone on the network irrespective of the physical location of the resource and the user.

2. High reliability due to alternative sources of data :

– It provides high reliability by having alternative sources of data.

– For e.g. all files could be replicated on more than one machines, so if one of them is unavailable due to hardware failure or any other reason, the other copies can be used.

– The aspect of high reliability is very important for military, banking, air traffic control, nuclear reactor safety and many other applications where continuous operations is a must even if there are hardware or software failures.

3. Cost :

– Computer networking is an important financial aspect for organisations because it saves money.

– Organisations can use separate personal computer one per user instead of using mainframe computer which are expensive.

– The organisations can use the workgroup model (peer to peer) in which all the PCs are networked together and each one can have the access to the other for communicating or sharing purpose.

– The organisation, if it wants security for its operation it can go in for the domain model in which there is a server and clients.

– All the clients can communicate and access data through the server.

4. Communication medium :

– A computer network provides a powerful communication medium among widely separated employees.

– Using network it is easy for two or more employees, who are separated by geographical locations to work on a report, document or R and D simultaneously i.e. on – line.

2.3.2 Services Provided by the Network to People : S-11

MSBTE Questions

Q. 1 Describe the services provided by the network to people. **(S-11, 4 Marks)**

– The computer networks offer the following services to an individual person :

1. Access to remote information.
2. Person to person communication.
3. E-commerce.
4. Interactive entertainment.

1. Access to remote information :

– Access to remote information involves interaction between a person and a remote database. Access to remote information comes in many forms like :

– Home shopping, paying telephone, electricity bills, e-banking, on line share market etc.

– Newspaper is on-line and is personalised, digital library consisting of books, magazines, scientific journals etc.

– World wide web which contains information about the arts, business, cooking, government, health, history, hobbies, recreation, science, sports etc.

2. Person to person communication :

– Person to person communication includes :

– Electronic-mail (e-mail).

– Real time e-mail i.e. video conferencing allows remote users to communicate with no delay by seeing and hearing each other. Video-conferencing is being used for remote school, getting medical opinion from distant specialists etc.

– Worldwide new groups in which one person posts a message and all other subscribers to the newsgroup can read it or give their feedbacks.

3. Interactive entertainment :

– Interactive entertainment includes :

– Multiperson real-time simulation games.

- Video on demand.
- Participation in live TV programmes likes quiz, contest, discussions etc.

2.4 Computer Network Criteria : S-11

MSBTE Questions

Q. 1 Which criteria should be followed while designing a computer network ? **(S-11, 4 Marks)**

- Network is a broad term similar to system. Network is a communication system which supports many users.
- In context with the computers we can say that, a "computer network" is a system which allows communication among the computers connected in the network.
- A network must be able to meet certain criteria. The most important of them are :

  1. Performance. 2. Reliability. 3. Security.

Performance :

- Performance can be measured in different ways. We can measure it in terms of transit time and response time.
- **Transit time** is defined as the time required for a message to travel from one device to the other.
- **Response time** : It is the time elapsed between the instant of enquiry and the instant of giving response.
- The other factors deciding the performance are as follows :

  1. Number of users.
  2. Type of transmission medium.
  3. The hardware used.
  4. The software used.

Reliability :

- The network reliability is important because it decides the frequency at which network failure takes place.
- It also decides the time taken by the network to recover and its robustness in the catastrophe.

Security :

- The network security refers to protection of data from the unauthorized user or access.
- It also includes the data protection against damage and recovering it in the events of data losses.

2.5 Network Scale :

- This is an alternative criterion for classification of networks.
- Fig. 2.5.1 gives the network classification based on their physical size. All these systems are multiprocessor systems.

Interprocessor distance	Processors are located in	Example of network
0.1 m	Same circuit board	Data flow machine
1 m	Same system	Multicomputer
10 m	Same room	LAN
100 m	Same building	LAN
1 km	Same campus	LAN
10 km	Same city	MAN
100 km	Same state	WAN
1,000 km	Same continent	WAN
10, 000 km	Same planet	Internet

Fig. 2.5.1 : Network classification according to scale

- Beyond the multicomputers are the true networks, in which the computers communicate by exchanging messages over long cables.
- Such networks are divided into following categories :

  1. Local area networks.
  2. Metropolitan area networks.
  3. Wide area networks.

Internetwork :

- The connection of two or more networks is called as an internetwork.
- The best example of internetwork is the Internet.

2.6 Network Classification by their Geography :

W-11, S-12, S-14, S-15, S-16, S-17, S-18, I-Scheme : S-19

MSBTE Questions

Q. 1 Explain classification of computer network. **(W-11, 4 Marks)**

Q. 2 Classify the networks. **(S-12, 2 Marks)**

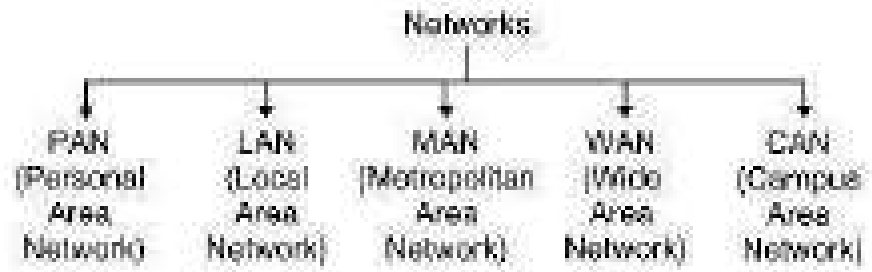
Q. 3 List any four types of computer network by considering geography. **(S-14, 2 Marks)**

Q. 4 Describe classification of computer networks. **(S-15, 4 Marks)**

Q. 5 Classify networks on the basis of their geography and define. **(S-16, S-18, 4 Marks)**

Q. 6 Explain classification of computer network by their geography. **(S-17, 4 Marks)**

- Computer network can be classified based on the geographical area they cover, i.e. the area over which the network is spread.
- Such a classification is shown in Fig. 2.6.1.



(G-1400) **Fig. 2.6.1 : Network categories**

- In this section, we will discuss the following categories of networks :

2.6.1 Local Area Networks (LAN) :

W-11, W-12, S-16, W-16, S-17, S-18

MSBTE Questions

Q. 1 Explain LAN with diagram. **(W-11, 4 Marks)**

Q. 2 Write any two characteristics of LAN. **(W-12, 2 Marks)**

Q. 3 Classify networks on the basis of their geography and define. **(S-16, S-18, 4 Marks)**

Q. 4 State four features of LAN and WAN. **(W-16, 4 Marks)**

Q. 5 List any two characteristics of LAN. **(S-17, 2 Marks)**

Definition :

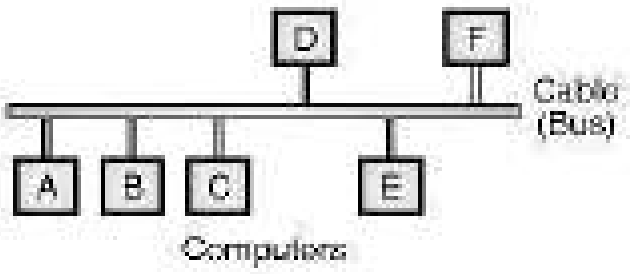
- The Local Area Network (LAN) is a network which is designed to operate over a small physical area such as an office, factory or a group of buildings. LANs are very widely used in a variety of applications.
- LANs are easy to design and troubleshoot. The personal computers and workstations in the offices are interconnected via LAN.
- The exchange of information and sharing of resources becomes easy because of LAN.
- In LAN all the machines are connected to a single cable. Different types of topologies such as Bus, Ring, Star, Tree etc. are used for LANs.
- LAN uses a layered architecture and they are capable of operating at hundreds of Mbits/sec.
- A Local Area Network (LAN) is usually a privately owned and links the devices in a single office, building or campus of upto a few kilometres in size as shown in Fig. 2.6.2.
- Depending on the needs of an organisation and the type of technology used, a LAN can be as simple as a few computers and a printer at home or it can contain many computers in a company and include voice, sound and video peripherals.
- LANs are widely used to allow resources to be shared between personal computers or workstations. The resources to be shared can be hardware like a printer or softwares or data.
- In a LAN one of the computer can become a server serving all the remaining computers called clients. Software can be stored on the server and it can be used by the remaining clients.
- LAN's are also distinguished from MAN's and WAN's based on the transmission media they use and topology. In general a given LAN will use only one type of transmission medium. The most common networking topologies used are bus, ring and star.
- The data rates for LAN can now range from 10 Mbps to 16 Gbps.

Important characteristics / Features of LAN :

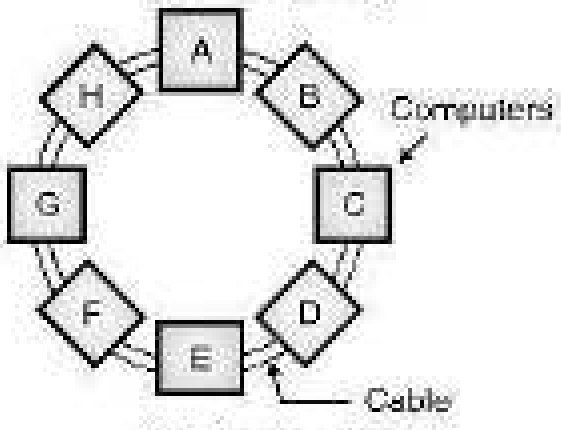
1. Very high degree of interconnection between the computers.
2. High rate of data transmission.
3. Physical connection of computers in a LAN is easy.
4. Every computer in the LAN can communicate with every other computer.
5. The medium used for data transmission is inexpensive.

LAN topologies :

- Network topology is defined as the pattern in which the network elements are connected to each other. Different network topologies are : Bus, ring, star etc.
- Various topologies are possible for the broadcast LANs such as bus topology or ring topology as shown in Fig. 2.6.2.



(a) Bus topology



(b) Ring topology

(G-32)**Fig. 2.6.2 : LAN topologies**

Advantages of LAN :

1. High reliability. Failure of individual computers does not affect the entire LAN.
2. It is possible to add a new computer easily.
3. The transmission of data is at a very high rate.
4. Sharing of peripheral devices such as printer is possible.

Applications of LAN :

1. File transfer and file access.
2. Personal computing.
3. Office automation.
4. Distributed computing.
5. Word and text processing.
6. Document distribution.
7. Remote access to database.
8. Electronic message handling.

2.6.2 Ethernet : S-13

MSBTE Questions

Q. 1 Define : Ethernet. **(S-13, 1 Mark)**

- Both Internet and ATM (Asynchronous Transfer Mode) were designed for wide area networking. But in many applications, a large number of computers are to be connected to each other.
- For this the Local Area Network (LAN) was introduced. The most popular LAN is called Ethernet.
- The IEEE 802.3 standard is popularly called as Ethernet. It is a bus based broadcast network with decentralized control.
- It can operate at 10 Mbps or 100 Mbps or even above 1 Gbps.
- Computers on an Ethernet can transmit whenever they want to do so. If two or more machines transmit simultaneously, then their packets collide.
- Then the transmitting computers just wait for an arbitrary time and retransmit their signal.
- There are various technologies available in the LAN market but the most popular one of them is **Ethernet.**

Definition :

- Ethernet is a way of connecting computers together in a LAN. It is the most widely used method of linking computers together in LAN.
- The basic idea behind its design is to facilitate multiple computers to access it and send data anytime.
- Traditional Ethernet was created in 1976 and has a data rate of 10 Mbps.

2.6.3 Metropolitan Area Network (MAN) :

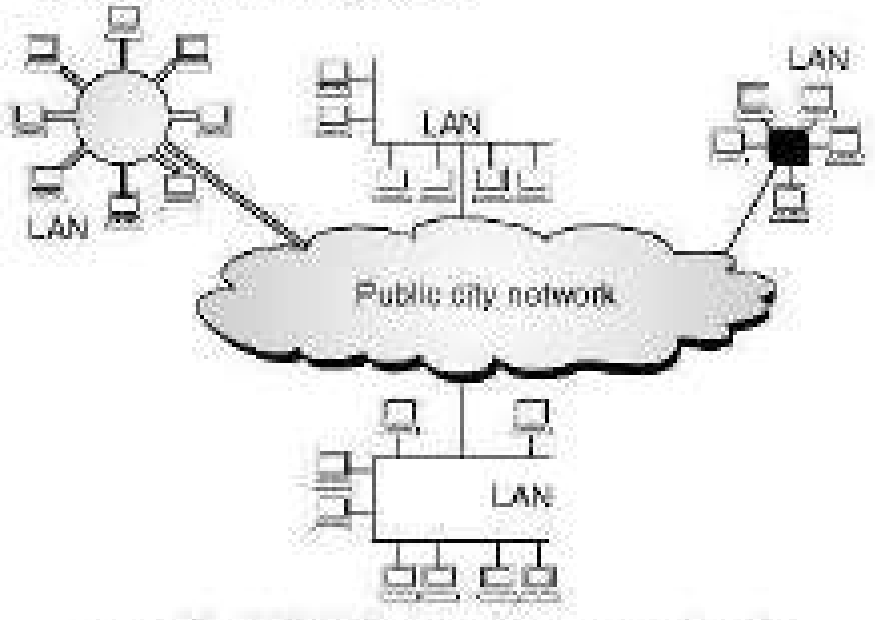
W-04, S-08, S-12, S-16, S-18

MSBTE Questions

Q. 1 Describe the situation where MAN is useful for an organization. Give one example. **(W-04, S-08, S-12, 4 Marks)**

Q. 2 Classify networks on the basis of their geography and define. **(S-16, S-18, 4 Marks)**

- A MAN is basically a bigger version of a LAN and normally uses similar technology.
- It is designed to extend over a larger area such as an entire city.
- The MAN can be in the form of a single network such as a cable network or it can be a combination of multiple LANs as shown in Fig. 2.6.3.



(G-33) **Fig. 2.6.3 : Metropolitan area network**

- A MAN may be wholly owned and operated by a private company or it may be a service provided by a public company, such as a local telephone company (telco).

Definition :

- A MAN is a network that interconnects users with the computer resources in a geographical area larger than that covered by a LAN and smaller than that covered by a wide area network (WAN).

2.6.4 Wide Area Network (WAN) :

S-11, S-16, W-16, S-17, S-18

MSBTE Questions

Q. 1 Draw and explain Wide Area Network. **(S-11, 4 Marks)**

Q. 2 Classify networks on the basis of their geography and define. **(S-16, S-18, 4 Marks)**

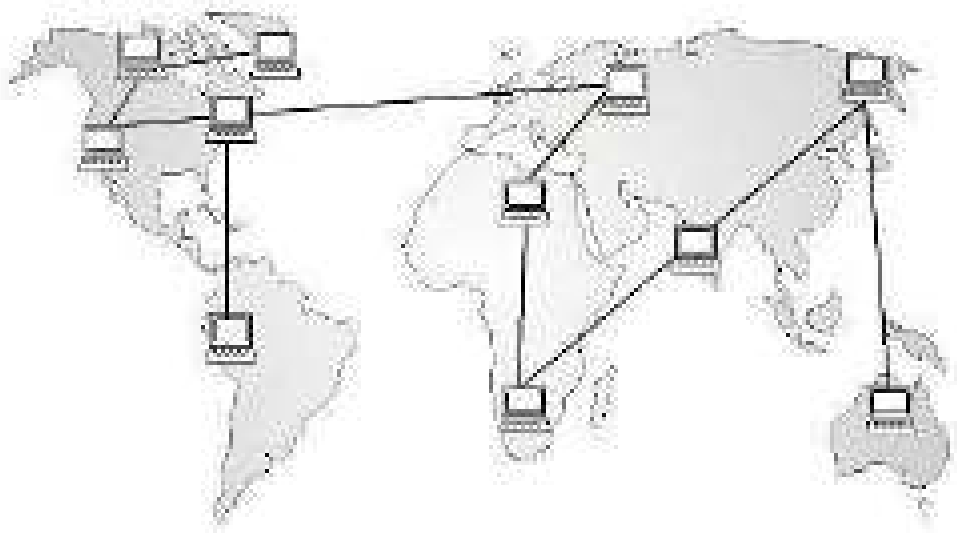
Q. 3 State four features of LAN and WAN. **(W-16, 4 Marks)**

Q. 4 Draw and explain wide area network. **(S-17, 4 Marks)**

- When a network spans a large distance or when the computers to be connected to each other are at widely separated locations a local area network cannot be used.
- For such situations a Wide Area Network (WAN) must be installed.
- The communication between different users of "WAN" is established using leased telephone lines or satellite links and similar channels.
- It is cheaper and more efficient to use the phone network for the links.

Definition :

- A WAN is a telecommunications network or computer network that extends over a large geographical distance/place.
- Wide area networks are generally established with leased telecommunication circuits.
- Most wide area networks are used for transferring large blocks of data between its users.
- As the data is from existing records or files, the exact time taken for this data transfer is not a critical parameter.
- An example of WAN is an airline reservation system. Terminals are located all over the country through which the reservations can be made.
- It is important to note here that all the terminals use the same centralized common data provided by the central reservation computer.
- Because of the large distances involved in the wide area networks, the propagation delays and variable signal travel times are major problems.
- Therefore most wide area networks are not used for time critical applications. As explained earlier they are more suitable for transfer of data from one user to the other which is not a time critical application. Wide area networks are basically packet switching networks.
- A WAN provides long distance transmission of data, voice image and video information over large geographical areas that may comprise a country, a continent or even the whole world as shown in Fig. 2.6.4.



(G-35) **Fig. 2.6.4 : Wide area network**

Characteristics / features of WAN :

- Following are some of the important characteristics of WAN :
  1. Remote data entry and access is possible.
  2. Communication facility is provided.
  3. Centralized information is created and used.
  4. WAN spans over a large distance.

2.6.5 PAN (Personal Area Network) :

S-16, S-18

MSBTE Questions

Q. 1 Classify networks on the basis of their geography and define. **(S-16, S-18, 4 Marks)**

- A Personal Area Network (PAN) is a computer network designed for and organized around an individual person.
- A PAN generally consists of a mobile computer such as a laptop, a cell phone and /or a personal digital assistant (PDA).
- PAN will allow the communication to take place among these devices.
- PAN can also be used for communication among personal devices themselves (intrapersonal communication) or for connecting to a higher level network and internet (This is called as an uplink).
- The PANs can be constructed using cables or it can be wireless.
- The wireless PANs typically use Bluetooth or sometimes use the infrared connections.
- The PANs generally cover a range upto 10 meters. PAN can be considered as a special type of local area network (LAN), which is designed for one person instead of a group.

2.6.6 CAN (Campus Area Network) :

S-16, S-18

MSBTE Questions

Q. 1 Classify networks on the basis of their geography and define. **(S-16, S-18, 4 Marks)**

- The Campus Area Network (CAN) is made up of an interconnection of LAN within a limited geographical area.
- The network equipments such as switches, routers and the transmission media i.e. optical fiber etc. are almost entirely owned by the campus owner (i.e. a company, university, government etc.)
- For example, a university CAN would connect different buildings in its campus, such as various departments, library, student hall to each other.
- CAN could also be thought of as a special case of WAN.

2.6.7 Comparison of LAN, WAN and MAN :

S-08, W-08, W-09, S-10, W-10, W-11, S-12, W-12, W-14, S-15, W-15, S-16

MSBTE Questions

Q. 1 Compare LAN and WAN on the basis of :

(a) Area (b) Ownership

(c) Speed (d) Error rate **(S-08, W-09, S-10, 4 Marks)**

Q. 2 Compare LAN with WAN with respect to :

1. Geographical area
2. Speed
3. Error correction
4. Bandwidth required **(W-08, 4 Marks)**

Q. 3 Compare LAN and WAN. **(W-10, S-16, 4 Marks)**

Q. 4 Compare MAN and WAN. **(W-11, 4 Marks)**

Q. 5 Differentiate LAN and WAN by considering following points :

1. Physical area 2. Installation cost
3. Bandwidth 4. Transmission media

(S-12, 4 Marks)

Q. 6 Distinguish between LAN and WAN. (4 points) **(W-12, 4 Marks)**

Q. 7 Compare LAN, MAN and WAN. (Any four points) **(W-14, 4 Marks)**

Q. 8 Compare LAN, MAN and WAN. **(S-15, 4 Marks)**

Q. 9 Differentiate LAN and WAN by considering following points :

1. Physical area 2. Installation cost
3. Bandwidth 4. Transmission media

(W-15, 4 Marks)

Sr. No.	Parameter	LAN	WAN	MAN
1.	Ownership of network	Private	Private or public	Private or public
2.	Geographical Area covered	Small	Very large (states or countries)	Moderate (city)
3.	Design and maintenance	Easy	Not easy	Not easy
4.	Communication medium	Coaxial cable	PSTN or satellite links	Coaxial cables, PSTN, optical fiber cables, wireless,
5.	Data rates (speed)	High	low	Moderate

Sr. No.	Parameter	LAN	WAN	MAN
6.	Mode of communication	Each station can transmit and receive	Each station cannot transmit	Each station can transmit or receive.
7.	Installation cost	Low	Moderate	High
8.	Principle	Operates on the principle of broadcasting	Switching	Both
9	Propagation delay	Short	Long	Moderate
10.	Bandwidth	Low	High	Moderate

2.7 Network Architecture : W-11, S-12

MSBTE Questions

Q. 1 Explain classification of computer network. **(W-11, 4 Marks)**

Q. 2 Classify the networks. **(S-12, 2 Marks)**

- The local area networks are classified into two types :
  1. Peer to peer networks.
  2. Client server networks.
- The relationship between each PC or device on the network with the others in terms of control will be dependent on the choice of network type.
- For these two types, the special software is required for controlling the flow of information between the users.
- The Network Operating System (NOS) is installed on each PC depending on the type of network.
- NOS monitors the data exchange, flow of files, and other information.
- The network operating systems are different for the peer to peer and client server networks.
- A peer-to-peer network is analogus to a company that uses decentralized management, where decision are made locally.
- A client-server network is similar to company that works on the principle of centralized management, where decisions are made in a central location.

2.8 Peer-to-Peer Networks :

S-03, S-05, W-10, W-11, S-14, W-16

MSBTE Questions

Q. 1 Draw peer to peer network configuration. Name network operating system used in this configuration. List any two situations under which peer to peer network is appropriate. **(S-03, 4 Marks)**

Q. 2 Draw peer to peer network configuration. Name network operating system used. Explain network security in peer to peer network. **(S-05, 4 Marks)**

Q. 3 It is proposed to design a network with all the machine having equal priority and without very strong security. Which network configuration would be appropriate in this situation ? State the reason. **(W-10, 4 Marks)**

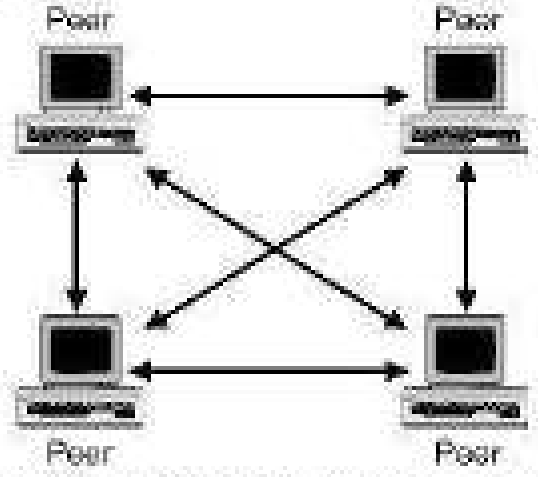
Q. 4 Draw and explain peer to peer network. **(W-11, 4 Marks)**

Q. 5 Describe the concept of peer-to-peer network. Where it is used ? **(S-14, 4 Marks)**

Q. 6 Describe the working of peer to peer network. **(W-16, 4 Marks)**

Structure :

- Fig. 2.8.1 shows the structure of the peer-to-peer network.



(S-10) Fig. 2.8.1 : Peer-to-peer network

- In this type of network, each computer is responsible for making its own resources available to other computers on the network.
- Each computer is responsible for setting up and maintaining its own security for its resources.
- Also each computer is responsible for accessing the required network resources from peer-to-peer relationships.

- Peer to peer network is useful for a small network containing less than 10 computers on a single LAN. Each computer maintains its own accounts and their security settings.
- In peer-to-peer network, every computer can function as both a client and server. **Windows 2000 comes** in both server and professional versions, but it's still a peer-to-peer operating system.
- Peer to peer networks do not have a central control system. There are no servers in peer networks.
- In this type of network users simply share disk space and resources, such as printers and faxes.
- Peer networks are organised into workgroups. Workgroups have very little security. There is no central login process.
- If the user has logged into one peer on the network he can use any resources on the network that are not controlled by a specific password.
- Access to individual resources can be controlled if the user who shared the resources installs a password to access it.
- Since there is no central security, the user will have to know individual password for each secured shared resource which he wants to access.
- Peer to peer networks are relatively simple. Each computer in the network can act as client as well as server as per requirement.
- This eliminates the need of expensive server.
- No additional software is necessary in order to set up the peer to peer network.

2.8.1 When to use Peer to Peer Networks ?

S-03, W-10, S-14, S-18

MSBTE Questions

Q. 1 Draw peer to peer network configuration. Name network operating system used in this configuration. List any two situations under which peer to peer network is appropriate. **(S-03, 4 Marks)**

Q. 2 It is proposed to design a network with all the machine having equal priority and without very strong security. Which network configuration would be appropriate in this situation ? State the reason. **(W-10, 4 Marks)**

Q. 3 Describe the concept of peer-to-peer network. Where it is used ? **(S-14, 4 Marks)**

Q. 4 Describe any four situations in which server based networks are more superior to peer to peer networks. **(S-18, 4 Marks)**

- The peer to peer networks are suitable for the following working conditions :
- If network security is not an important issue.
- If the number of users is less than 10 (small network).
- If all the users are situated in the same area.
- If the possibility of future expansion is less.

2.8.2 Features of Peer to Peer Networks :

1. It is useful for small networks with less than 10 computers.
2. Every computer can work as a client and server.
3. There is no central control system.
4. Operating system used is Windows 2000 and its subsequent versions.
5. No additional software is required to set up the peer to peer network.
6. It does not offer a high network security.

2.8.3 Advantages of Peer to Peer Networks :

W-03, S-04, W-04, S-06, W-06

MSBTE Questions

Q. 1 State any 4 advantages of peer to peer network over client / server network. **(W-03, 4 Marks)**

Q. 2 List two advantages of peer to peer network. **(S-04, W-04, S-06, W-06, 4 Marks)**

- Peer networks have many advantages, especially for small business houses that cannot afford to buy expensive server hardware and software.

1. **No extra investment in server hardware or software is required.**
2. **Use less expensive computer hardware :** In peer-to-peer network, the resources are distributed over many computers, so there is no need for higher-end-server computer.
3. **Easy to administer :** In peer-to-peer network each machine performs its own administration.
4. **No NOS required :** Peer-to-peer network does not require a Network Operating System (NOS).

5. **More built-in-redundancy :** If you have a small network, with 10-20 workstations and each one with some important data on it, and one fails you still have most of your shared resources available.

   Peer-to-peer network/achieve more redundancy because of smaller possibility of single point of failure.

6. Easy setup and lower cost for small networks.
7. Users can control resource sharing.
8. A user is not dependent on other computers for its operation.

2.8.4 Disadvantages of Peer to Peer Networks : S-04, W-04, S-06, W-06

MSBTE Questions

Q. 1 List two disadvantages of peer to peer network. **(S-04, W-04, S-06, W-06, 4 Marks)**

– There are several disadvantages of peer-to-peer network, particularly for larger networks as follows :

1. **Individual performance is affected :**

– If some workstations have frequently used resources on them, then the use of these resources by other computer might adversely affects the person using this particular workstation.

2. **Less security :**

A peer-to-peer network operates on the most common desktop operating systems like windows which are not very secure operating systems.

3. **Backup is difficult :**

– In peer-to-peer network there is no centralized server. Hence data is scattered over many workstations.

– So it is difficult to backup all data in an organized manner.

4. **Hard to maintain version control :**

– In peer-to-peer network, files are stored on number of different workstations.

– So it is difficult to manage different document versions or files.

5. As there is no centralized management it makes large peer networks hard to manage and final data easily.
6. Users are supposed to manage their own computers.
7. It is not possible to save important data in a centralized manner.
8. Additional load on computer because of resource sharing and absence of server.

2.9 Client / Server Network (Server Based Network) :

S-03, W-03, S-04, W-04, S-05, S-09, W-11, W-12, S-14, W-14, W-16, S-17, S-18

MSBTE Questions

Q. 1 Draw client server network configuration. Name network operating system used in this configuration. **(S-03, W-03, S-04, 4 Marks)**

Q. 2 Draw client server network configuration. Name network operating system used in this configuration. **(W-04, 2 Marks)**

Q. 3 Define :

1. Client 2. Server **(S-05, S-09, 2 Marks)**

Q. 4 Explain server based computer network. **(W-11, 4 Marks)**

Q. 5 With neat diagram, explain client server network along with its advantages and disadvantages. **(W-12, 8 Marks)**

Q. 6 For following situation which type of network architecture is appropriate ? **(W-12, 4 Marks)**

1. Number of user 10.
2. Data and resources need to be restricted.
3. Network administrator required.
4. Users with equal priority.

Q. 7 Define Server. Give the name of any two types of server. **(W-14, 2 Marks)**

Q. 8 Describe the working of server based networks. Where is it used ? **(W-16, 4 Marks)**

Q. 9 With neat diagram, explain client server network alongwith its advantages and disadvantages. **(S-17, 8 Marks)**

Q. 10 Describe the architecture of client-server network with its advantages and disadvantages. **(S-18, 4 Marks)**

– In client-server network relationships, certain computers act as server and other act as clients.

Definition of client :

– A **client** is a computer running a program that requests services from a server. The individual workstations in a network are clients.

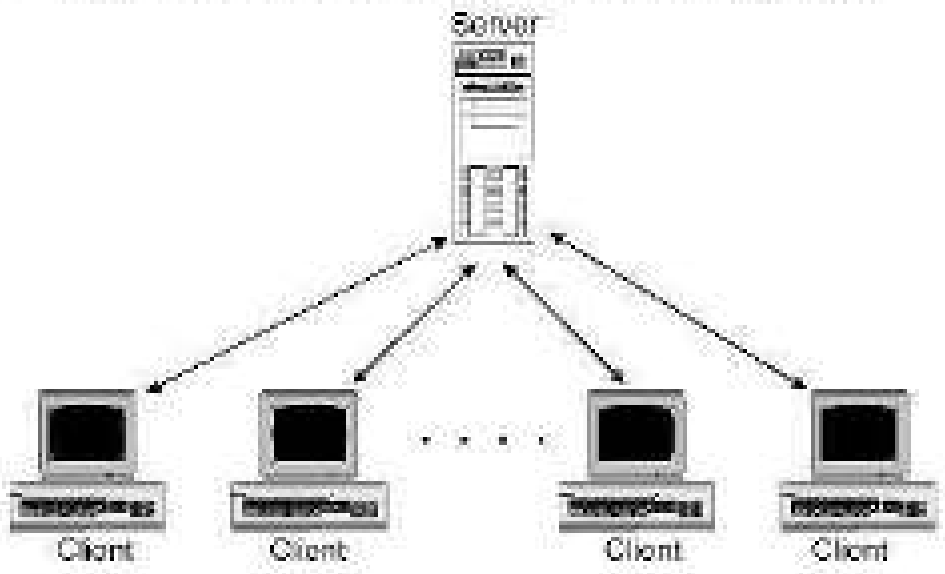
Definition of server :

– A **server** is simply a computer that makes the network resources available and provides service to other computers when they request for it.

- Local Area Networking (LAN) is based on the client-server network relationship.
- You can construct a client server network by using one or more powerful networked computers as a servers and the rest of as clients.
- Client-server network typically uses a directory service to store information about the network and its users.
- A client-server network is one in which all available network resources such as files, directories, applications and shared devices, are centrally managed, stored and then are accessed by client.

Network configuration :

- Fig. 2.9.1 shows client-server network configuration.



(G-41) **Fig. 2.9.1 : Client server network relationship**

- In the client server networks the servers provide security and administration of the entire network.
- In client-server networks the processing tasks are divided between clients and servers.
- Clients request services such as file storage and printing and servers deliver them.

Server :

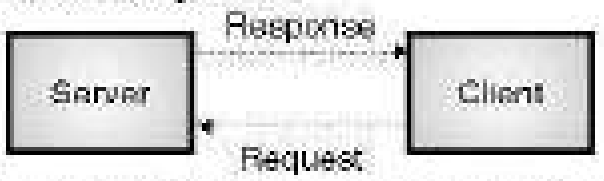
- The central computer which is more powerful than the clients and which allows the clients to access its softwares and database is called as the server.
- Server computers typically are more powerful than client computers or are optimised to function as servers.
- No user can access the resources of the servers until he has been authenticated (permitted) by the server to do so.

Operating system :

- We can use any common operating system such as Windows 7 for a client.
- But the server is loaded with a special operating system such as Microsoft Windows Server 2008.

2.9.1 Communication in Client-Server Configuration :

- Fig. 2.9.2 explains the principle of communication in the client server configuration.



(G-42) **Fig. 2.9.2 : Client/server communication**

- The client places a request on the server machine when he wants an access to the centralised resources.
- The server responds to this request and sends the signal accordingly to the client as shown in Fig. 2.9.2.
- The software run at the client computer is called as client program. This software configures that particular computer to act as a client.
- Similarly the software run on the server computer is called as server program. It configures that particular computer to act as a server.

2.9.2 Advantages of Client-server Network :

S-05, S-08, W-10, S-12, W-12, S-15, S-17, S-18

MSBTE Questions

Q. 1 State any four advantages of server-based network over peer to peer network. **(S-05, S-15, 4 Marks)**

Q. 2 State merits and demerits of client server network. **(S-08, W-10, S-12, 4 Marks)**

Q. 3 With neat diagram, explain client server network along with its advantages and disadvantages. **(W-12, 8 Marks)**

Q. 4 State merits and demerits of client server network. **(S-17, 4 Marks)**

Q. 5 With neat diagram, explain client server network alongwith its advantages and disadvantages. **(S-17, 8 Marks)**

Q. 6 Describe the architecture of client-server network with its advantages and disadvantages. **(S-18, 4 Marks)**

- The advantages of client-server network are as follows :

1. The network is secure :

- In client-server network's high security is because of several things :

(a) Shared resources are located in a centralized area and they are administered centrally.

(b) The servers are physically placed in secure location such as lockable separate server room.

(c) The operating system runs on client-server are designed to provide better security to network.

(d) Better security to network due to good administration.

2. **Better performance :**

– The dedicated server computers are more expensive than standard computer workstations, but they also offer considerably better performance.

3. **Centralized backup :**

– Backing up company's important data is much easier when it is located on a centralized server.

– Centralized backup is much faster too.

4. **Higher reliability :**

– In client server network centralized dedicated server provide more reliability. It has built-in redundancy.

5. Central file storage, which allows all users to work from the same of data.

6. Reduces cost because of sharing of hardware and software.

7. Increased speed due to dedicated server for sharing resources.

8. Single password allows access to all shared resources.

9. Central organisation which keeps data from getting lost among computers and easy manageability of large number of users.

10. The individual users don't have to manage or share resources.

2.9.3 Disadvantages of Client-server Networks : S-08, W-10, S-12, W-12, S-17, S-18

MSBTE Questions

Q. 1 State merits and demerits of client server network. **(S-08, W-10, S-12, 4 Marks)**

Q. 2 With neat diagram, explain client server network alongwith its advantages and disadvantages. **(W-12, 8 Marks)**

Q. 3 State merits and demerits of client server network. **(S-17, 4 Marks)**

Q. 4 With neat diagram, explain client server network alongwith its advantages and disadvantages. **(S-17, 8 Marks)**

Q. 5 Describe the architecture of client-server network with its advantages and disadvantages. **(S-18, 4 Marks)**

1. **Professional administration is required :** Client-server networks usually need professional administration. You can hire a network administrator or you can use a company which provides professional network administration services.

2. We have to use a high speed server computer with lots of memory and disk space.

3. It requires a special network operating system and a number of client licenses.

4. Expensive dedicated hardware needs to be used.

2.9.4 Applications of Client-server Configuration : W-16

MSBTE Questions

Q. 1 Describe the working of server based networks. Where is it used ? **(W-16, 4 Marks)**

– Some of the important applications are as follows :

1. E-mail clients.
2. Web browsers.
3. FTP (file transfer) clients.

2.9.5 Types of Servers :

S-11, W-14, S-15, W-16

MSBTE Questions

Q. 1 List any four types of servers. **(S-11, 2 Marks)**

Q. 2 Define server. Give the name of any two types of server. **(W-14, 2 Marks)**

Q. 3 List any four types of servers. Describe them in brief. **(S-15, 4 Marks)**

Q. 4 Name any two types of server. **(W-16, 2 Marks)**

– The commonly used servers are of following types :

1. File servers
2. Print servers
3. Application servers
4. Message servers
5. Database servers

– Windows NT server support all of these capabilities and can by itself serve in all of these capacities simultaneously on a small network.

– On large networks however a number of servers are required to increase the access speed.

File servers :

- Some of the important features of file servers are as follows :
- These servers provide the services such as storing, retrieving and moving the data.
- A user can read, write, exchange and manage the files with the help of file servers.
- A file can be stored in three different ways namely online, offline and nearline storage.

Print server :

- The print server controls and manages printing on the network.
- It also offers the fax service to the network users.
- A user can access fax and print services simultaneously.

Application servers :

- The expensive softwares can be shared by the users in a network with the help of application servers.
- The application servers also provide security and efficiency.

Message server :

- It is used to co-ordinate the interaction between users, documents and applications.
- The data can be in the form of audio, video, binary, text or graphics. The simple file server can not handle all these, so message server has to be used.
- It handles all the complex data types by using various types of communication methods.

Database server :

- It is a type of application server.
- It allows the users to access the centralised strong database.

2.9.6 Factors Influencing the Choice of Network : W-03, W-05, W-12, S-18

MSBTE Questions

Q. 1 List three factors that can influence the choice of whether to implement a peer to peer network or client server network. **(W-03, W-05, 4 Marks)**

Q. 2 State the reason for implementing a network **(W-12, S-18, 4 Marks)**

- The factors which influence the choice between the peer to peer or client server networks are as follows :
  1. Need of network security.
  2. Is the network administration needed ?
  3. Is the central storage of files essential ?
  4. How much important is cost effectiveness ?
  5. Is resource sharing necessary ?
  6. Will there be any future expansions of the network ?

2.9.7 Comparison between Peer-to-Peer Network and Client-Server Network :

S-03, W-03, S-04, W-08, S-09, S-12, S-13, W-14, S-16, S-17, S-18

MSBTE Questions

Q. 1 Compare peer-to-peer network with client/server network. **(S-03, W-03, S-04, W-08, 8 Marks)**

Q. 2 Differentiate between peer to peer networks and server based networks. **(S-09, 2 Marks)**

Q. 3 Compare peer to peer with client server network. **(S-12, S-13, S-18, 4 Marks)**

Q. 4 Compare client server and peer to peer network. **(S-13, S-17, 4 Marks)**

Q. 5 Compare server based network and peer-to-peer network. (Any four points.) **(W-14, 6 Marks)**

Q. 6 State the difference between server based network and peer to peer network. **(S-16, 4 Marks)**

Sr. No.	Peer-to-peer	Client-server
1.	It is much like company uses decentralized management.	It is much like company using centralized management.
2.	In this each machine has same power.	In this server has more power and client has less power.
3.	Uses less expensive computer hardware.	It has to use expensive hardware.
4.	Easy to setup and administer.	Complex to setup and require professional administrator.
5.	Less secure.	Very secure.
6.	Decentralized backup i.e. difficult to backup.	Centralized backup i.e. easy to backup.
7.	Network O.S. not required.	Network O.S. required.
8.	It has built-in redundancy.	Not built-in redundancy.
9.	It is suitable for small network.	It is suitable for large network.
10.	Poor performance.	Better performance.

2.10 Network Features :

S-09, W-09, S-12, S-13, W-14, S-18

MSBTE Questions

Q. 1 What are the features of a computer network ? (S-09, 2 Marks)

Q. 2 State various network features. (W-09, 1 Mark)

Q. 3 State the network features. (S-12, 2 Marks)

Q. 4 Explain network features. (S-13, 4 Marks)

Q. 5 Discuss any four network features. (W-14, 4 Marks)

Q. 6 State and explain network features. (S-18, 4 Marks)

- Now you can understand the types of things you can do with a network. The following are the features of network :
  1. File sharing.
  2. Printer sharing.
  3. Application services.
  4. E-mail.
  5. Remote access.
  6. Internet and intranet.
  7. Network security : Internal and external

2.10.1 File Sharing :

S-09, W-09, S-14, S-18

MSBTE Questions

Q. 1 What is meant by file sharing and printer sharing ? How this can be achieved ? (S-09, 4 Marks)

Q. 2 Explain any one network feature in detail. (W-09, 3 Marks)

Q. 3 Describe in brief file sharing. (S-14, 2 Marks)

Q. 4 State and explain network features. (S-18, 4 Marks)

- File sharing is the primary feature of network. Due to use of networks the sharing of files becomes easier.
- File sharing requires a shared directory or disk drive which many user can access over the network.
- When many users are accessing the same file on network, more than one person can make changes to a file at the same time. They might both making **conflicting** changes simultaneously.
- Hence most of software programs don't allow multiple changes to a single file at the same time.
- Network operating systems that perform file sharing also exercise and monitor the security of these shared files and what kind of access they have.
- For example : Some users might have permission to view only certain shared files, while other user have permission to edit or even delete certain shared files.

Advantages :

1. Easily share information on network.
2. User needs regular access of word processing files, spreadsheets so they access easily.

Disadvantages :

1. Conflicting problem arises if same file is simultaneously accessed by multiple users.
2. Less secure if permission to access is not set properly.

2.10.2 Printer Sharing :

S-09, W-11, S-18

MSBTE Questions

Q. 1 What is meant by file sharing and printer sharing ? How this can be achieved ? (S-09, 4 Marks)

Q. 2 Explain printer sharing. (W-11, 4 Marks)

Q. 3 State and explain network features. (S-18, 4 Marks)

- Printer sharing is beneficial to many users as they can share a costly and higher quality printers.
- Printer sharing can be done in several different ways on network. The most common way is to use **printer queues** on server.
- The printer queue contains the print jobs until any currently running print jobs are finished and then automatically send the waiting jobs to the printer. i.e. printer connected to server.
- Another way to share printer on a network is that each workstation accesses the printer directly. i.e. printer connected to the network just like network workstation.
- In the first method that uses printer queues always have a print server. That print server handles the job of sending each print job to the printer.

Advantages :

1. Reduce number of printer you need.
2. Share costly high quality color laser printers.

Disadvantages :

1. Reduce server performance if printer is connected to server.
2. Each user must wait its turn, if many users are request printer at once and the printer is directly connected to network.

2.10.3 Application Services :

- Just as you can share files on a network, you can also share applications on a network.
- For example you can have a shared copy of Microsoft office or some other application and keep it on the network server.
- When a particular workstation wants to run the program, it loads the files from the network into its own memory and run that program normally.
- Keeping applications centralized reduces the amount of storage space needed on each workstation.
- It is easier to administer the application in a centralized manner.
- Another application service you can have on the network is a shared installation.
- This enables you to use workstation without CD-ROM for installation. i.e. contents of CD-ROM copy to the server, then run the installation program for workstation from server.
- This makes installing application much faster and more convenient.

Advantages :

1. Reduces the amount of disk space needed on each workstation.
2. Centralized administration, so provide higher security and reliability.
3. Without CD-ROM we can install the software on workstation over network.
4. Installing application on workstation is much faster and more convenient.
5. This gives economical solution for more costly softwares.

Disadvantages :

1. It increases network traffic on network.
2. If server fail or crash, then workstation is useless on network.
3. Requires network license copy for application software or business software.

2.10.4 E-mail : S-09, S-12

MSBTE Questions

Q. 1 How E-mail service is provided and how an e-mail is sent ? **(S-09, S-12, 4 Marks)**

- E-mail is extremely valuable and important feature for communication within organization or outside the people in world.
- E-mail service can be used by user in two different ways :
  (a) File based.
  (b) Client server.
- File based e-mail system is the one that consists of a set of files kept in a shared location on a server.
- File based e-mail system requires **gateway server** for connecting or handling the e-mail interface between the two systems using gateway software that is part of the file-based e-mail system.
- A client-server e-mail system is the one where an e-mail server contains the messages and handles all incoming and outgoing mail.
- Client-server e-mail systems, are more secure and far more powerful than file based e-mail system.
- They offer additional features that enable you to use the e-mail system for different business processes.

Advantages :

1. Helpful for communication within a company or outside a company.
2. Faster communication.

Disadvantages :

1. Network becomes unreliable due to viruses.
2. Require more security.

2.10.5 Remote Access : W-08, W-15

MSBTE Questions

Q. 1 What do you mean by remote access ? **(W-08, 2 Marks, W-15, 4 Marks)**

- Another important feature of network is remote access to the network resources.
- Using this feature users can access their files and e-mail, when they are travelling or working on remote location.
- Remote access feature is implemented as per user need or business need. Some of the features are all follows :
  1. Setting up a simple remote access service connection on a windows 2000 server with using modem.
  2. Using a dedicated remote access system, which handles many modems.
  3. Using dial-up mechanism with modem for workstation on the network.
  4. Setting up a Virtual Private Network (VPN) connection to the Internet.
  5. Installing Windows Terminal Services on windows 2000 server.

Advantages :

1. User access their files and e-mail from remote location.
2. It enables users access to centralized application, stored private or shared files on LAN.

Disadvantages :

1. Require more security.
2. More hardware or complex hardware required.

Different types of remote access technologies :

- Following are different types of remote access technologies (connection types) as follows :
  1. Public Switched Telephone Networks (PSTN).
  2. Leased line.
  3. ISDN (Integrated Services Digital Network).
  4. Cable TV.
  5. DSL (Digital Subscriber Line).

2.11 Network Functions : S-11

MSBTE Questions

Q. 1 List any eight network functions. (S-11, 4 Marks)

- The basic function of a network is to transfer information between a source machine and a destination machine.
- The following is a list of functions that a network must carry out :
  1. Basic user service i.e. the primary services that are provided by the network to its users.
  2. Switching facility for connecting users.
  3. Transmission system for transmission of data on the medium.
  4. Routing in order to decide the path of the packets.
  5. Multiplexing for sharing multiple information channels.
  6. Information representation for determining the format of information handled by the network.
  7. Addressing for identifying the end system (Terminal).
- The essential network functions include all transmission, multiplexing, routing and switching in a network.
- The services that are provided to the user are built on the basic transfer capability of a network.
- There are three types of networks in existence which use three different types of switching techniques :
  1. Telegraph network which uses message switching for the transfer of text messages called telegrams.
  2. Telephone network which uses circuit switching for the transfer of voice messages.
  3. Internet operation is based on packet switching which provides the transfer of digital data.

Review Questions

Q. 1 Define the following terms :
1. Network
2. Protocol
3. Handshaking

Q. 2 Distinguish between computer network and distributed system.

Q. 3 State and explain the services provided by the network to organizations.

Q. 4 State and explain the services provided by the network to people.

Q. 5 What are the performance parameters of a network ?

Q. 6 State and explain the transmission technologies used in computer networks.

Q. 7 State the various types of networks.

Q. 8 Write a short note on LAN.

Q. 9 Write a short note on MAN.

Q. 10 Write a short note on WAN.

Q. 11 Compare LAN and WAN.

Q. 12 Write a note on : Peer to peer networks.

Q. 13 State the advantages and disadvantages of peer to peer network.

Q. 14 State merits and demerits of client server network.

Q. 15 Write a short note on : Client server network.

Q. 16 State the various functions carried out by a network.

Q. 17 Explain the human network.

Q. 18 What is family network ?

Q. 19 Explain different types of human networks.

Q. 20 What is the need of computer network ?

Q. 21 State various components of a computer network.

Q. 22 Explain the two models of network computing.

Q. 23 What is network plan ? What is its importance ?

Q. 24 State various benefits of computer networks.

Q. 25 Explain any two benefits in detail.

Q. 26 Explain the centralised management of software, maintenance, data backup.

Q. 27 Explain the disadvantages of networks.

Q. 28 State advantages of LAN.

Q. 29 State disadvantages of LAN.

Q. 30 Compare peer to peer and client server network.

Q. 31 State advantages of client –server networks.

Q. 32 Define client and server.

Q. 33 State different types of servers and explain.

Q. 34 What are the factors influencing the choice of network.

Q. 35 State different network features.

Q. 36 Explain file sharing and printer sharing.

Q. 37 Explain the application services.

Q. 38 Explain E – mail and Remote Access.

2.12 MSBTE Questions and Answers :

Q. 1 In an organization all the computers have large hard drives to store files and optical drives with removable cartridges. Someone who wants to print an image takes a cartridge with the image stored on it and takes printout on the computer connected to the printer. How would a network help this organization ? **(W-03, 4 Marks)**

Ans. :

– The networking can help this organization in two ways.

– One is in the field of data storage i.e. the important data can be stored centrally and can be shared by all the users.

– Secondly, the printer also can be shared by all the users.

– This will eliminate the need of separate printer for each computer and hence save money.

Q. 2 An organization situated within a small building, wants to setup a computer network for 7 users having equal priority. Suggest type of network to be used.

Justify your answer. **(S-04, 4 Marks)**

Ans. :

– Refer Section 2.8. It should be a peer-to-peer network.

Q. 3 Your company is having a difficult time keeping information consistence because not all users have the most current version of the project reports on their computers hard drives. Also, important information has been lost because one individual consistently failed to back up his hard drive.

How would you use a network to improve this situation ? **(W-04, 4 Marks)**

Ans. :

– This problem can be sorted out by storing the latest project report as well as the upgraded important information centrally and provide a network to allow all the users to access this information.

– If the job of updating is allotted to the most efficient person, then everyone will get the latest information.

Q. 4 State the reason for implementing a network.

Name three key resources often shared on a network. **(S-05, W-15, 4 Marks)**

Ans. :

– Please refer Section 2.1.2. Resources shared are printers, Database, expensive softwares.

Q. 5 In a small agency there are five PCs in the network. Cost is an issue and the company would prefer not to dedicate an individual's time to maintain a network. However, the agency is also concerned about keeping its data safe and the users are not sophisticated computer users. In what ways is a peer to peer network appropriate for the company ? In what ways it is inappropriate ? **(W-05, 4 Marks)**

Ans. :

– There are certain factors in favour of the peer to peer network and some are against the peer to peer network.

Favourable factors :

1. Small network size (only 5 computer).
2. Cost is an issue (Peer to peer costs less).
3. Users are not sophisticated computer users.

Factors against using peer to peer network :

1. Individuals time should not be wasted in network maintenance. But in P2P network there is no centralized maintenance.
2. Data should be kept safe. But P2P does not provide network security.

Q. 6 You are installing a small network for collection agency with 5 work stations. Company would prefer not to dedicate individual's time to maintain the network. The company is concerned about security of data but with low budget. In what way is a peer network appropriate and server based is appropriate for this company ? **(W-05, 4 Marks)**

Ans. :

– How P2P is appropriate is explained in Q. 5.

Factors favouring the server based network :

1. Individual's time should not be wasted in network maintenance. This requires centralized maintenance which is provided by the server based network.
2. Data should be kept safe. This is possible with the server based system, because first it provides network security and second, the important data can be stored on the server with a restricted access to it.

Q. 7 You are asked to replace micro computers and terminals in travel agency with 25 personal computers with Windows 98 installed on them. Justify the additional cost of server and why it will be better to make this server based network instead of peer to peer network. **(W-05, 4 Marks)**

Ans. :

– In the travel agency the important information such as the information about flight timings, availability of seats, present status of reservations, clients information, progress about any case has to be stored centrally on a server and should be shared by all the employees.

– Some information can be of secret nature and only a few employees should be allowed to access it.

– This point also is in favour of server based network.

– The number of computers is 25 which is too large for a P2P network.

– Thus server based network even though expensive will be more appropriate than the P2P network.

Q. 8 It is proposed to design a network with all the machine having equal priority and without very strong security. Which network configuration would be appropriate in this situation ? State the reason. **(W-10, 4 Marks)**

Ans. :

– Here, P2P will be appropriate. Refer Section 2.8.

Q. 9 Define LAN. Write any two disadvantages of LAN. **(W-14, 2 Marks)**

Ans. :

– Refer section 2.6.1 for definition of LAN.

Disadvantages of LAN :

1. Different types of LANs are not compatible to each other. So they cannot be connected directly.
2. With increase in number of nodes, the LAN wiring becomes complicated.

Q. 10 Define protocol. Give the name of any two protocols. **(W-14, 2 Marks)**

Ans. :

– Refer section 2.1.1 for protocol.

Types of protocol :

1. TCP 2. IP

Q. 11 Define the following : 1. Protocol 2. Peer. **(W-15, 2 Marks)**

Ans. :

1. **Protocol :** Refer section 2.1.1.
2. **Peer :** Peers are computer systems which are connected to each other via the Internet. Files can be shared directly between systems on the network without the need of a central server.

Q. 12 In a small agency, there are five PCs in the network. Cost is an issue and the company would prefer not to dedicate an individual's time to maintain a network. However the agency is also concerned about keeping its data safe and the users are not sophisticated computer users. In what ways is a peer to peer network appropriate for the company ? In what ways it is inappropriate ? **(W-15, 4 Marks)**

Ans. :

– There are certain factors in favour of the peer to peer network and some are against the peer to peer network.

Favourable factors :

1. Small network size (only 5 computer).
2. Cost is an issue (Peer to peer costs less).
3. Users are not sophisticated computer users.

Factors against using peer to peer network :

1. Individuals time should not be wasted in network maintenance. But in P2P network there is no centralized maintenance.
2. Data should be kept safe. But P2P does not provide network security.

Q. 13 For following situations, state which type of network architecture is appropriate : **(W-15, 4 Marks)**

1. Number of users 50.
2. Data and resources need to be restricted.
3. No network administrator required.
4. All users with equal priority.

Ans. :

1. **Number of users 50 :** Client-server network
2. **Data and resources need to be restricted :** Client-server network
3. **No network administrator required :** Peer to peer network
4. **All users with equal priority :** Peer to peer network

Q. 14 Draw a neat diagram and describe a wide area network. What are the three phases of communication in a WAN ? **(W-16, 4 Marks)**

Ans. :

– For wide area network refer section 2.6.4.

Three phases of communication in a WAN :

1. Circuit establishment.
2. Data transfer.
3. Circuit release.

2.13 I-Scheme Questions and Answers :

Summer 2019 [Total Marks - 08]

Q. 1 Define computer network and state it's types. **(Sections 2.1.1 and 2.6)** **(2 Marks)**

Q. 2 State various computer network applications. **(Section 2.1.2)** **(2 Marks)**

Q. 3 Classify the network based on geographical area and transmission technology. **(4 Marks)**

Ans. :

– Refer section 2.6 for network based on geographical area.

Classification based on transmission technology :

1. Broadcast networks.
2. Point to point networks.

Summer 2022 [Total Marks - 06]

Q. 4 Define computer network. **(Section 2.1.1)** **(2 Marks)**

Q. 5 Consider a network with 8 computer, which network architecture should be used peer to peer or client server ? Justify the answer. **(4 Marks)**

Ans. :

– Peer to peer architecture should be used due to the following reasons :

1. It is a small network with less than 10 computers.
2. Use of server would be costly.
3. All users are located in the same area.
4. P2P is easy to administer.
5. Easy setup and lower costs.

❑❑❑

Chapter 3

Communication Media

Syllabus

Communication media : Guided transmission media, Twisted pair cable, Coaxial cable, Fiber optic cable, Unguided transmission media : Radio waves, Microwaves, Infrared, Satellite, Line of sight transmission, Point to Point, Broadcast.

Chapter Contents

3.1 Communication (Transmission Media) :

W-05, W-15, S-16, I-Scheme : W-19

MSBTE Questions

Q. 1 Describe the word transmission media with respect to networks. **(W-05, 2 Marks)**

Q. 2 Define guided media. List the types of guided media. **(W-15, 2 Marks)**

Q. 3 Name the layer which is associated with the transmission media. **(W-15, 2 Marks)**

Q. 4 State the need of transmission media. **(S-16, 4 Marks)**

Definition :

- A transmission media is the medium over which information travels from the sender to receiver. In other words a communication channel is also called as a medium.
- Different media have different properties and used in different environments for different purposes.
- The **physical layer** of OSI model is associated with the transmission media.

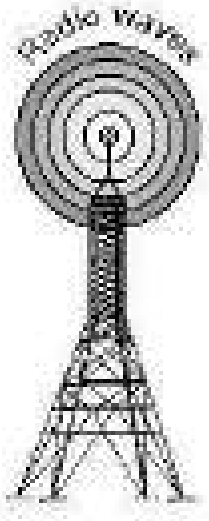
Types :

Media are roughly grouped into two classes :

1. Guided media 2. Unguided media

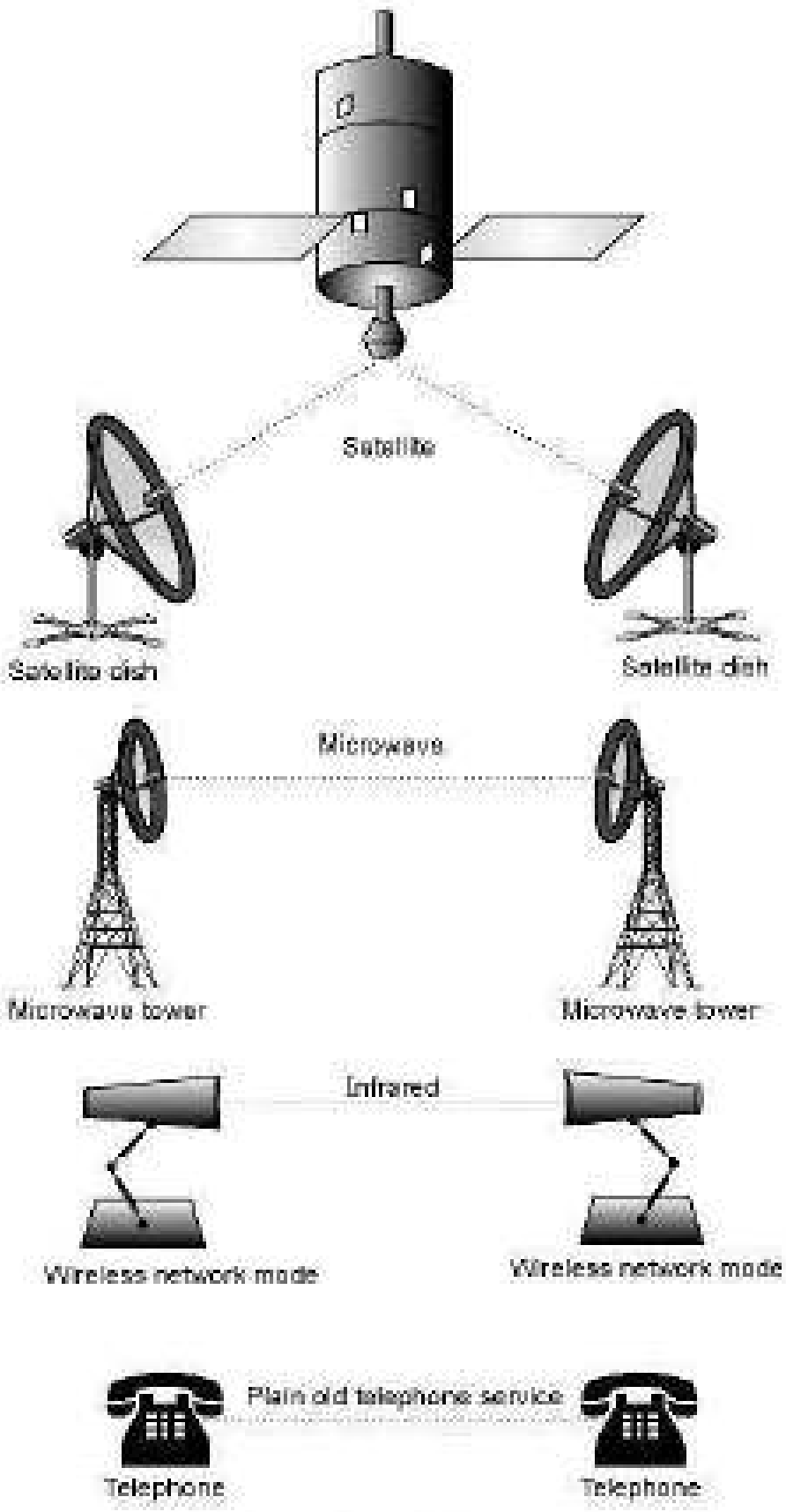
1. **Guided media :** Guided media is a communication medium which allows the data to get guided along it. For this the media need to have a point to point physical connection.
2. **Unguided media :** The wireless media is also called as an unguided media.

- The examples of guided media are copper wires and fiber-optics, whereas radio and lasers through the air are examples of unguided media as shown in Fig. 3.1.1.



Radio tower

(S-95) **Fig. 3.1.1**



(S-95) **Fig. 3.1.1 : Types of transmission media**

3.2 Criteria for the Selection of Transmission Media :

W-03, W-04, S-05, W-05, S-07, W-08, W-09, S-10, W-12, S-13, S-14, W-14, W-15, S-16, S-18

MSBTE Questions

Q. 1 Describe any six factors considered for cable selection. **(W-03, S-05, W-05, 4 Marks)**

Q. 2 State the criteria for selecting transmission media. **(W-04, W-08, W-09, W-15, S-18, 4 Marks, S-16, 2 Marks)**

Q. 3 Explain the factors to be considered while selecting a cable to establish a network. **(S-07, S-18, 4 Marks)**

Q. 4 Describe any four factors considered for cable selection. **(S-10, W-12, 4 Marks)**

Q. 5 State the factors to be considered for selecting transmission media. **(S-13, 4 Marks)**

Q. 6 Describe various factors to be considered while selecting transmission media. **(S-14, 4 Marks)**

Q. 7 State the factors to be considered for selecting transmission media. (Eight points). **(W-14, 4 Marks)**

- The important factors to be considered while selecting the transmission media are as follows :
  1. Type of medium (wired or wireless).
  2. Number of conductors.
  3. Flexibility.
  4. Durability or life span.
  5. Reliability of connection.
  6. Bandwidth.
  7. Effect of external interference.

3.3 Classification of Transmission Media :

W-03, S-04, S-05, W-05, S-07, S-12, W-15, S-16, S-17

MSBTE Questions

Q. 1 State three types of network cables. **(W-03, S-04, S-05, W-05, 4 Marks)**

Q. 2 Enlist any three types of transmission media commonly used. **(W-05, 4 Marks)**

Q. 3 List different types of cables used in network. **(S-07, 4 Marks)**

Q. 4 Which are the different transmission media ? **(S-12, 2 Marks)**

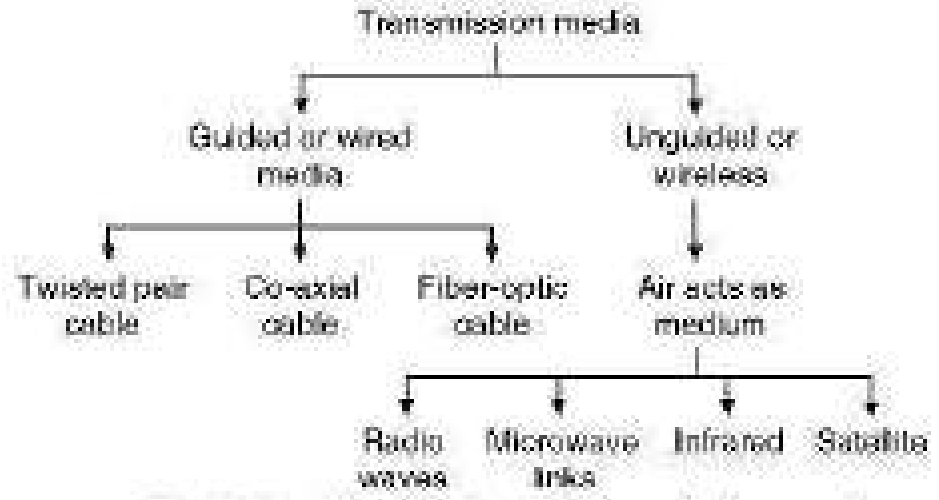
Q. 5 List the types of cables. Explain any one in detail. **(S-12, 4 Marks)**

Q. 6 Define guided media. List the types of guided media. **(W-15, 2 Marks)**

Q. 7 List types of cable. Draw and label the constructional sketch of co-axial cable. **(S-16, 4 Marks)**

Q. 8 What are different transmission media ? **(S-17, 2 Marks)**

- The classification of media is as follows :



(S-94) **Fig. 3.3.1 : Classification of transmission media**

3.3.1 Wired (Guided) Media :

- In this type of media, the signal energy is contained and guided within a solid media.
- The examples of wired media are copper pair wires, coaxial cables and fiber optic cables.
- The wired media is used for point to point communication.

3.3.2 Wireless (Unguided) Media :

- In the wireless media, the signal energy propagates in the form of unguided electromagnetic waves.
- The examples of wireless media are radio and infrared light.
- The Wireless media is used for radio broadcasting in all the directions.

3.3.3 Types of Wired Media : S-08, S-12

MSBTE Questions

Q. 1 List the types of cables. Explain any one in detail. **(S-08, S-12, 4 Marks)**

- The most commonly used wired media are :
  1. Co-axial cable
  2. Twisted pair cable
  3. Optical fiber cable.
- The selection of wired media depends on various factors such as cost, connectivity, bandwidth, performance in presence of noise, geographical coverage etc.

3.3.4 Twisted Pair Cables :

S-03, W-03, W-04, S-05, S-06, W-06, W-08, W-10, W-11, S-12, W-12, S-13, S-14, W-14, S-15, W-15, S-16, S-17, S-18, I-Scheme : S-22

MSBTE Questions

Q. 1 State physical and transmission characteristics of twisted pair cable along with its applications. **(S-03, 8 Marks, W-04, 4 Marks)**

Q. 2 State the types of twisted pair cable. Enlist three physical characteristics of STP. **(W-03, 4 Marks, W-04, 2 Marks)**

Q. 3 Draw a sketch of shielded twisted pair and describe any two characteristics. **(S-05, 4 Marks)**

Q. 4 Describe the characteristics of UTP cable. **(S-06, S-12, 4 Marks)**

Q. 5 Draw a neat sketch of a twisted pair cable. Give the transmission characteristics of a twisted pair cable. State its applications. **(W-06, 4 Marks)**

Q. 6 What is the effect of twisting of the wires in UTP cables ? **(W-08, 2 Marks)**

Q. 7 Draw and explain unshielded twisted pair cable. **(W-10, 4 Marks)**

Q. 8 Explain shielded twisted pair cable. **(W-10, 4 Marks)**

Q. 9 How cross cable is created ? Draw figure and explain. Give its use. **(W-11, 8 Marks)**

Q. 10 List the types of cables. Explain any one in detail. **(S-12, 4 Marks)**

Q. 11 Write any two features of STP **(W-12, 2 Marks)**

Q. 12 Why the network cable is twisted ? **(S-13, S-17, 2 Marks)**

Q. 13 Give two applications of twisted pair cable. **(S-14, 4 Marks)**

Q. 14 Give any four disadvantages of unshielded twisted pair cable. **(W-14, 2 Marks)**

Q. 15 How cross cable is created ? Draw figure and explain. Give its application. **(S-15, 8 Marks)**

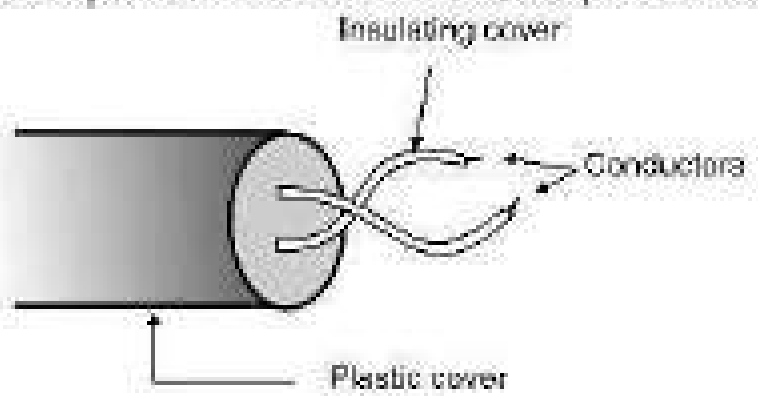
Q. 16 Explain twisted pair cable with neat sketch. **(W-15, S-18, 4 Marks)**

Q. 17 State characteristics of cables. **(S-16, 4 Marks)**

Q. 18 Draw a sketch of shielded twisted pair cable and describe any two characteristics. **(S-17, 4 Marks)**

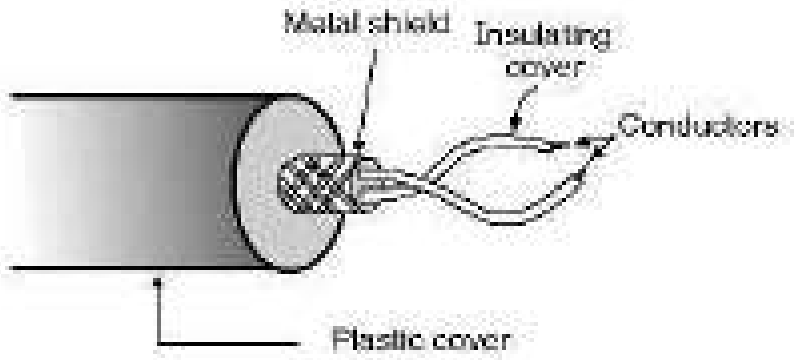
Construction :

- The construction of a twisted pair cable is as shown in Fig. 3.3.2. This is a very commonly used medium and it is cheaper than the co-axial cable, or optical fiber cable.



(a) UTP

Fig. 3.3.2



(b) STP

(G-98) **Fig. 3.3.2 : Construction of twisted pair cables**

Types of twisted pair cables :

- The two commonly used types of twisted pair cables are as follows :
  1. Unshielded Twisted Pair (UTP)
  2. Shielded Twisted Pair (STP)
- The construction of UTP and STP cables is shown in Fig. 3.3.2.

(G-97)

STP (Shielded Twisted Pair) :

Construction :

- STP cable as shown in Fig. 3.3.2(b) has a metal foil or braided mesh included in order to cover each pair of twisted insulating conductors.
- This is known as the metal shield, which is normally connected to ground so as to reduces the interference of the noise.
- But this makes the cable bulky and expensive.
- So practically UTP is more used than STP. The STP was developed by IBM and is used primarily for the IBM company only.
- Applications of the twisted pair cables are in point to point and point to multipoint communications, telephone systems etc.
- Twisted pairs can be used for either analog or digital transmission.
- The bandwidth supported by the wire depends on the thickness of the wire and the distance to be travelled by a signal on it.
- Twisted pairs support several megabits/sec for a few kilometres and are less costly.

Physical characteristics :

1. STP uses two insulated conducting wires twisted around each other.

2. These twisted conductors are shielded by a braided mesh.
3. It is a low cost guided medium.

Transmission characteristics :

1. The noise and electromagnetic interference is low due to shielding and twisting of wires.
2. It supports data rates upto several Mbps.
3. It can be used only for point to point communication.
4. It has a low to moderate bandwidth.

Features of STP :

- Low noise/electromagnetic interference.
- Low cost medium.
- Supports data rates upto few Mbps.
- Low or moderate bandwidth.

Application :

- STP is used only for IBM computers.

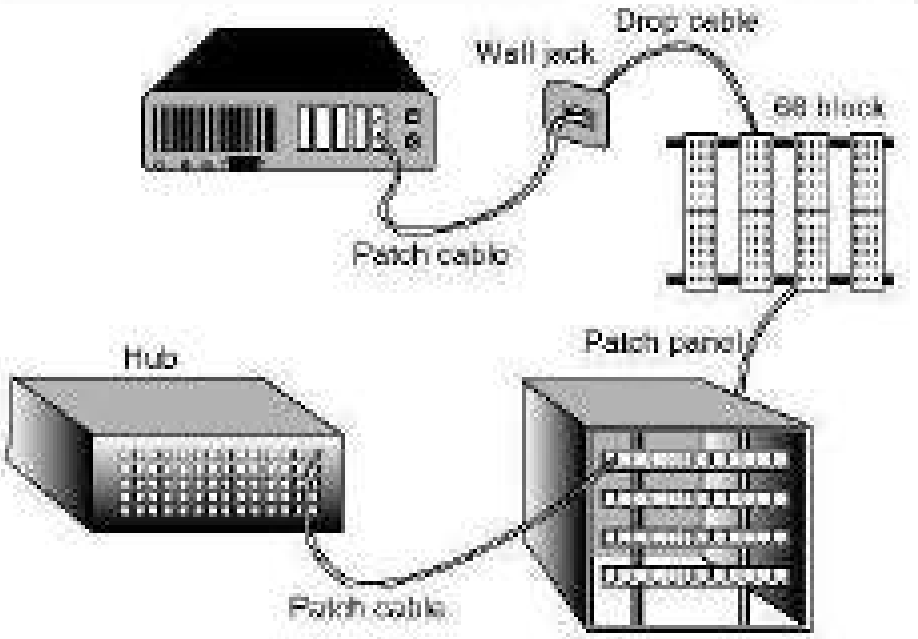
UTP (Unshielded Twisted Pair) :

Construction :

- A twisted pair consists of two insulated conductor twisted together in the shape of a spiral as shown in Fig. 3.3.2. It can be shielded or unshielded.
- The unshielded twisted pair cables are very cheap and easy to install. But they are badly affected by the electromagnetic noise interference.

Why to twist the wires ?

- Twisting of wires will reduce the effect of noise or external interference.
- The induced emf into the two wires due to interference tends to cancel each other due to twisting.
- Number of twists per unit length will determine the quality of cable. More twists means better quality.
- These cables ensure less crosstalk and a higher quality of signal over longer distances.
- Therefore these cables are popularly used for high speed computer communication.
- A connection diagram using the UTP is shown in Fig. 3.3.3.



(S-98) **Fig. 3.3.3 : A common UTP installation**

Characteristics of UTP :

1. The insulates wires are no shielded, but they are twisted around each other.
2. Noise and electromagnetic interference is high.
3. UTP is an economical guided medium.
4. Installation is easy.

Transmission characteristics :

1. Noise and electromagnetic interference is high.
2. It has a low to moderate bandwidth.
3. It can be used only for point to point communication.
4. Supports data rates upto several Mbps.

Disadvantages :

1. Moderate data rates.
2. Low or moderate bandwidth.
3. Noise and EM interference is high.

Applications of twisted pair cables :

- Some of the applications of twisted pair cables are as follows :

1. Local area networks for connecting computer to each other.
2. In the ISDN (Integrated Services Digital Network).
3. In the Digital Subscriber Line (DSL)
4. In the analog telephony (conventional telephone line) to carry voice and data signals.
5. In digital telephony system (T_1 system).

Note :

- A modular RJ-45 telephone connector is used to connect a four-pair cable.
- A modular RJ-11 telephone connector is used to connect a two pair cable.
- Shielded twisted pair (STP) cables were introduced by IBM corporation.

3.3.5 Comparison of Twisted Pair Cables :

S-03, W-09, S-10, S-11, W-11, S-12, W-12

MSBTE Questions

Q. 1 Distinguish between shielded twisted pair and unshielded twisted pair cables on the basis of cost, speed, attenuation and security. **(S-03, W-09, S-10, 4 Marks)**

Q. 2 Compare UTP and STP cables considering following points :
1. Bandwidth 2. EMI
3. Installation 4. Cost. **(S-11, 4 Marks)**

Q. 3 Compare STP and UTP transmission media. **(W-11, 4 Marks)**

Q. 4 Compare STP and UTP on any two points. **(S-12, 2 Marks)**

Q. 5 Compare between twisted pair cables UTP and STP with respect to following factors :
1. Bandwidth capacity
2. Node capacity or segment.
3. Attenuation
4. Cost. **(W-12, 4 Marks)**

Sr. No.	Parameters	UTP	STP
1.	Bandwidth	1 – 155 Mbps (typically 10 Mbps)	1 – 155 Mbps (typically 16 Mbps)
2.	Number of node connected per segment	2	2
3.	Attenuation	High	High
4.	Electromagnetic interference	Very high	Low
5.	Easy of installation	Easy	Fairly easy
6.	Cost	Lowest	Moderate
7.	Speed	Lower than STP	Higher than UTP
8.	Security	Low	Moderate

Ex. 3.3.1 : Which is the most practical medium to use when connecting computers that are fewer than 100 meters apart but located at different buildings ? Why ? Draw and explain the features of that transmission medium. **S-07, S-12, 4 Marks**

Soln. :

- Twisted pair cables are used for connecting computers that are fewer than 100 meters apart but located at different buildings.
- Refer section 3.3.4 for diagram and features of twisted pair cables.

3.3.6 Co-axial Cables :

S-03, S-04, S-05, S-09, W-09, S-10, W-12, S-13, S-14, W-14, S-15, S-16, W-16, S-17

MSBTE Questions

Q. 1 State any four benefits of co-axial cable. **(S-03, S-05, S-10, 4 Marks)**

Q. 2 Describe any six general characteristics of co-axial cable. **(S-04, 4 Marks)**

Q. 3 State advantages and disadvantages of coaxial cable and give applications. **(S-09, 4 Marks)**

Q. 4 Name the type of suitable cable to connect two computers in network. Explain the same cable. **(W-09, 4 Marks)**

Q. 5 Write any four characteristics of a co-axial cable. **(W-12, 4 Marks)**

Q. 6 Draw and explain co-axial cable. **(S-13, W-14, 4 Marks)**

Q. 7 Give two applications of co-axial cable. **(S-14, 4 Marks)**

Q. 8 Draw the constructional sketch of co-axial cable. Describe any three characteristics of co-axial cable. **(S-15, 4 Marks)**

Q. 9 State characteristics of cables. **(S-16, 4 Marks)**

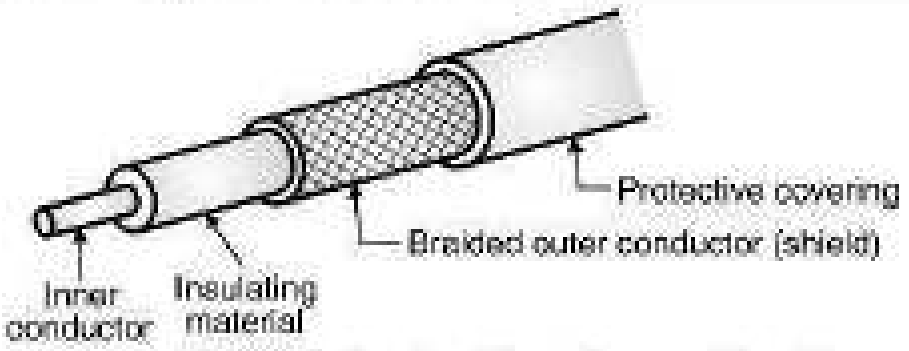
Q. 10 List types of cable. Draw and label the constructional sketch of co-axial cable. **(S-16, 4 Marks)**

Q. 11 Draw a neat sketch and describe the construction of co-axial cable. **(W-16, 4 Marks)**

Q. 12 State any two advantages of co-axial cable. **(S-17, 2 Marks)**

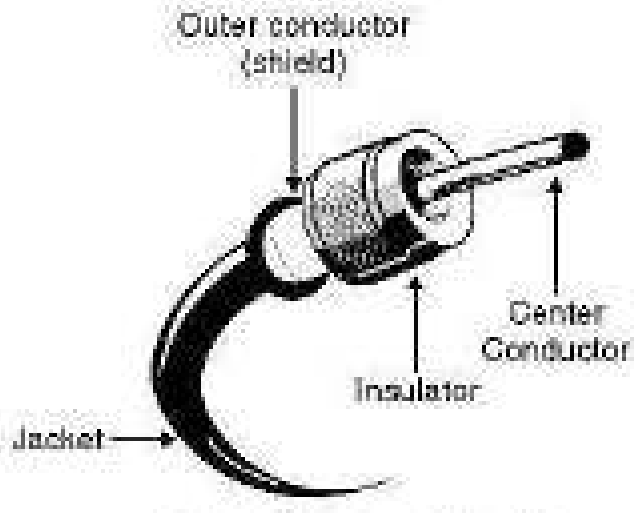
Construction :

- The construction of co-axial cable is as shown in Fig. 3.3.4. It consists of two concentric conductors namely an inner conductor and a braided outer conductor separated by a dielectric material.



(G-1001) **Fig. 3.3.4 : Construction of a co-axial cable**

- The external conductor is in the form of metallic braid and used for the purpose of shielding.
- The co-axial cable may contain one or more co-axial pairs.
- The construction of a co-axial cable with other accessories such as connector, jacket etc is shown in Fig. 3.3.5.



(G-1011) **Fig. 3.3.5 : Co-axial cable**

- The wire mesh (braided conductor) protects the inner conductor from Electromagnetic Interference (EMI). It is often called a shield.
- A tough plastic jacket forms the cover of the cable as shown in Fig. 3.3.5 providing insulation and protection.
- The co-axial cable was initially developed for analog telephone networks.
- A single co-axial cable would be used to carry more than 10,000 voice channels at a time.
- The digital transmission systems using the co-axial cable were developed in 1970s.
- These systems operated in the range of 8.5 Mb/s to 565 Mb/s.
- The most popular application of a co-axial cable is in the cable TV system.
- The existing co-axial cable system has a range from 54 MHz to 500 MHz.
- Other important application is cable modem, with the Cable Modem Termination System (CMTS).
- One more application is Ethernet LAN using the co-axial cable.
- The co-axial cable is used for its large bandwidth and high noise immunity.

Characteristics of a co-axial cable :

- The important characteristics of a co-axial cable are as follows :

1. Two types of cables having 75 Ω and 50 Ω impedance are available.
2. Due to the shield provided, this cable has excellent noise immunity.
3. It has a large bandwidth and low losses.
4. This cable is suitable for point to point or point to multipoint applications. Infact this is the most widely used medium for local area networks.
5. These cables are costlier than twisted pair cables but they are cheaper than the optical fiber cables.
6. It has a data rate of 10 Mbps which can be increased with the increase in diameter of the inner conductor.
7. The specified maximum number of nodes is upto 100.
8. The attenuation is less as compared to the twisted pair cable.
9. Co-axial cables are easy to install.
10. Co-axial cables are relatively inexpensive. (as compared to the optical fiber cable).

Applications of co-axial cables :

1. Analog telephone networks.
2. Digital telephone network.
3. Cable TV
4. Traditional Ethernet LANs
5. Digital transmission
6. Fast Ethernet

Advantages of co-axial cable :

1. Excellent noise immunity due to the shield
2. Larger bandwidth than twisted pair cables
3. Losses are small
4. Can be used for high data rates
5. Less attenuation
6. They are easy to install.

Disadvantages :

1. Costlier than the twisted pair cables.
2. BNC connectors are required to be used for connection.

3.4 Optical Fiber Cables :

W-03, W-11, S-13, W-14, S-16, W-16, S-17, I-Scheme : W-19

MSBTE Questions

Q. 1 With the help of neat diagram, describe functioning of an optical fiber cable. **(W-03, 2 Marks)**

Q. 2 Explain working of fiber optic cable. Give its advantage and disadvantage. **(W-11, 8 Marks)**

Q. 3 Draw the neat sketch of fiber optic cable. Give the transmission characteristics of fiber optic cable. State its applications. **(S-13, 8 Marks)**

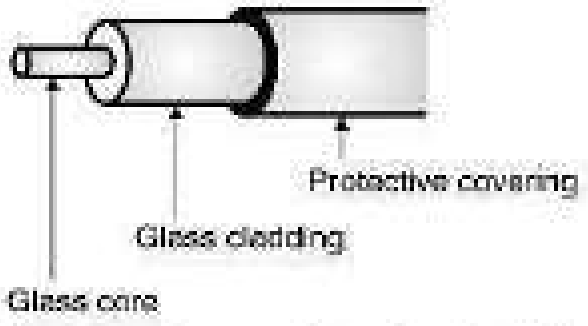
Q. 4 Draw and explain fiber optic cable. **(W-14, 4 Marks, S-16, 2 Marks)**

Q. 5 Draw a sketch indicating the construction of fibre optic cable. State four advantages over electrical cables. **(W-16, 4 Marks)**

Q. 6 With the help of neat diagram, describe working of fiber optic cable. **(S-17, 4 Marks)**

Construction :

- The construction of an optical fiber cable is as shown in Fig. 3.4.1.



(G-103) Fig. 3.4.1 : Construction of optical fiber cable

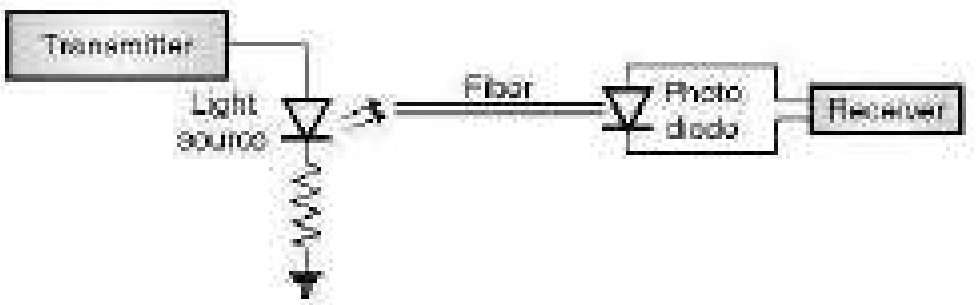
- It consists of an inner glass core surrounded by a glass cladding which has a lower refractive index and a protective covering.
- Digital signals are transmitted in the form of intensity - modulated light signal.
- Light is launched into the fiber at one end using a light source such as a Light Emitting Diode (LED) or laser.
- It is detected on the other side using a photo detector such as a phototransistor or photodiode.
- The optical fiber cables are costlier than the other two types but they have many advantages over the other two types.

3.4.1 Light Sources for Fiber : W-12

MSBTE Questions

Q. 1 Describe light sources for fiber. **(W-12, 4 Marks)**

- For data transmission to take place, the sending device that is the transmitter must be capable of inducing data bits 0 to 1 into the light source.
- At the receiver a photodiode is used to translate this light back into data bits as shown in Fig. 3.4.2.



(G-104) Fig. 3.4.2

- The two light sources which are used popularly are :
  1. LED (Light Emitting Diode)
  2. Injection Laser Diode (ILD)
- The LED is cheaper but has a disadvantage that it provides an unfocussed light which hits the core boundaries and gets diffused.
- So LED is preferred only for short distances.
- The laser diode can provide a very focused beam which can be used for a long distance communication.

3.4.2 Working of Fiber Optic Cable :

W-03, W-11, W-14, S-16, S-17, I-Scheme : W-19

MSBTE Questions

Q. 1 With the help of neat diagram, describe functioning of an optical fiber cable. **(W-03, 2 Marks)**

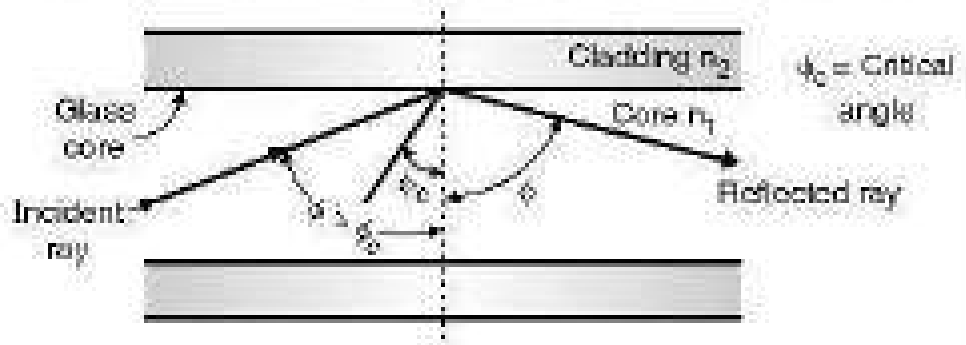
Q. 2 Explain working of fiber optic cable. Give its advantage and disadvantage. **(W-11, 8 Marks)**

Q. 3 Draw and explain fiber optic cable. **(W-14, 4 Marks, S-16, 2 Marks)**

Q. 4 With the help of neat diagram, describe working of fiber optic cable. **(S-17, 4 Marks)**

- The light enters into a glass fiber from one end, and gets reflected within the fiber. It follows a zigzag path along the length of the fiber as shown in Fig. 3.4.3(a).

(a) Light follows a zigzag path within the optical fiber



(b) Reflection at the interface of core and cladding

(G-105) Fig. 3.4.3

- Fig. 3.4.3(b) illustrates the principle of light travel through the optical fiber.
- When the light enters into a glass fiber from one end, most of it propagates along the length of the fiber and comes out from the far end.
- A small portion of the incident light escapes through the side walls of the fiber.
- The light which travels from one end to the other end of the glass fiber is said to have "guided" through the fiber.
- The light stays inside the fiber and does not escape through the walls because of the "total internal reflection" taking place inside the fiber.
- This total internal reflection can take place only if the following two conditions are satisfied.
  1. The glass fiber core must have a refractive index which is higher than the refractive index of the cladding around the core ($n_1 > n_2$).
  2. The angle of incidence of the light entering the fiber must be greater than the critical angle, "ϕ_c".

$$\sin \phi_c = \frac{n_2}{n_1}$$

- This is as shown in Fig. 3.4.3.

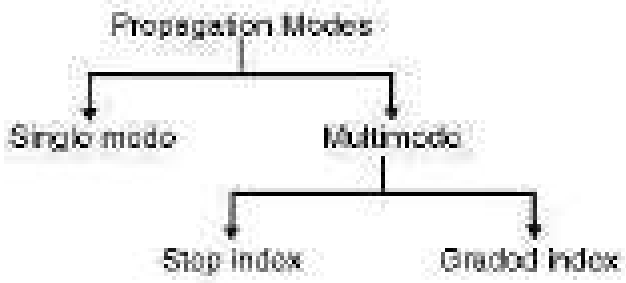
3.4.3 Modes of Propagation : W-14

MSBTE Questions

Q. 1 Explain different modes of fibre optic cable. **(W-14, 4 Marks)**

Definition :

- The number of paths followed by light rays inside the optical cable is called as modes.
- Fig. 3.4.4 shows different modes of operation of an optical fiber.
- There are two types namely single mode and multimodes fibers.



(G-108) Fig. 3.4.4 : Propagation modes in optical fibers

- In single mode fibers light follows a single path through the core whereas in multimode, the light takes more than one paths through the core.

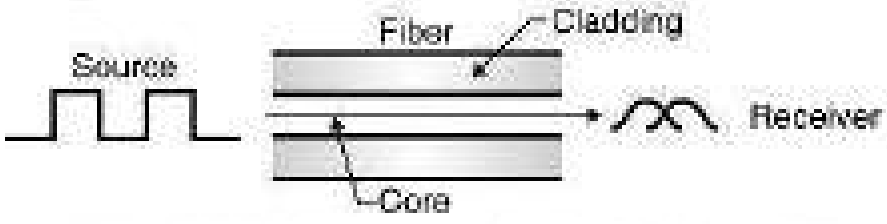
3.4.4 Single Mode Fibers : W-16

MSBTE Questions

Q. 1 With the help of neat diagram describe :
1. Single mode step index.
2. Single mode graded index.
3. Multimode step index.
4. Multimode graded index fiber.

(W-16, 8 Marks)

- These are called as single mode fibers because they support on one mode of propagation (TE, TM or TEM).
- The optical signal travelling inside this fiber has only one group velocity.
- Due to single mode travelling, the amount of dispersion is less than that introduced in multimode fibers.
- These fibers can have either step index or graded index profile.
- They are high quality fibers used for wideband long haul communication and they are fabricated from doped silica to reduce internal attenuation.
- The light travel in a single mode fiber is shown in Fig. 3.4.5.



(G-109) Fig. 3.4.5 : Light propagation in single mode fiber

- This beam travel's almost horizontally and follows only one path from source to destination as shown in Fig. 3.4.5.

- The critical angle of incident highly focused light beam is nearly equal to 90°.
- In the single mode fibers the delays are negligible and the signal reconstruction at the receiver is easier which results in almost no signal distortion.

3.4.5 Multimode Fibers : W-16

MSBTE Questions

Q. 1 With the help of neat diagram describe :

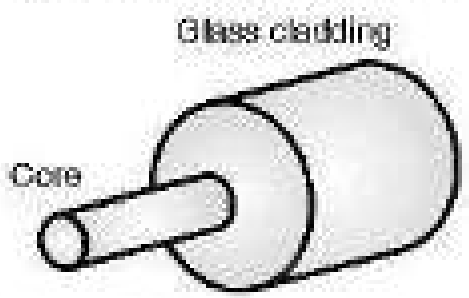
1. Single mode step index.
2. Single mode graded index.
3. Multimode step index.
4. Multimode graded index fiber.

(W-16, 8 Marks)

- These are called as multimode fibers because they support simultaneous propagation of many modes and the incident light follows different paths from the source to destination.
- Each mode has its own group velocity and each mode will follow its own path while travelling from the transmitter to receiver.
- Due to presence of more than one modes, the intermodal dispersion will exist.
- Multimode fibers can have the step index or graded index profile and they are fabricated using the multicomponent glasses or doped silica.

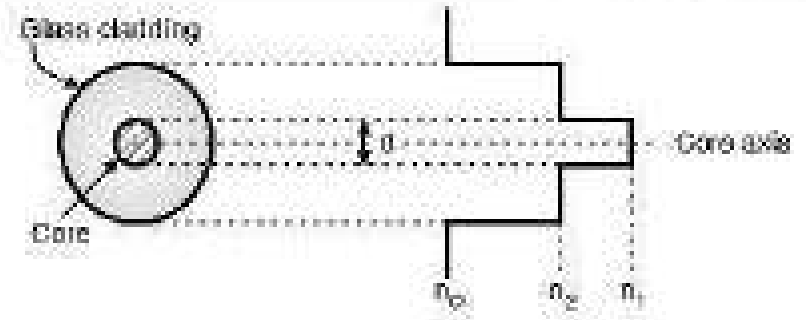
Step index fibers :

- The construction of an optical fiber with a core and glass cladding is as shown in Fig. 3.4.6(a).



(G-116) **Fig. 3.4.6(a) : Construction of a glass clad core type fiber**

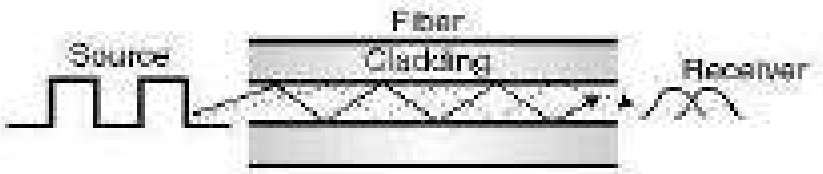
- The refractive index of the core is n_1 and that of the glass cladding is n_2, with $n_1 > n_2$.
- Therefore the index profile of glass clad core fiber is as shown in Fig. 3.4.6(c).



(b) Cross sectional view **(c) Index profile**

(G-110) **Fig. 3.4.6**

- Due to the sudden change in refractive index at the boundary of core and cladding, this fiber is called **step index** fiber.
- Fig. 3.4.7 illustrates the propagation of light over a step index fiber.

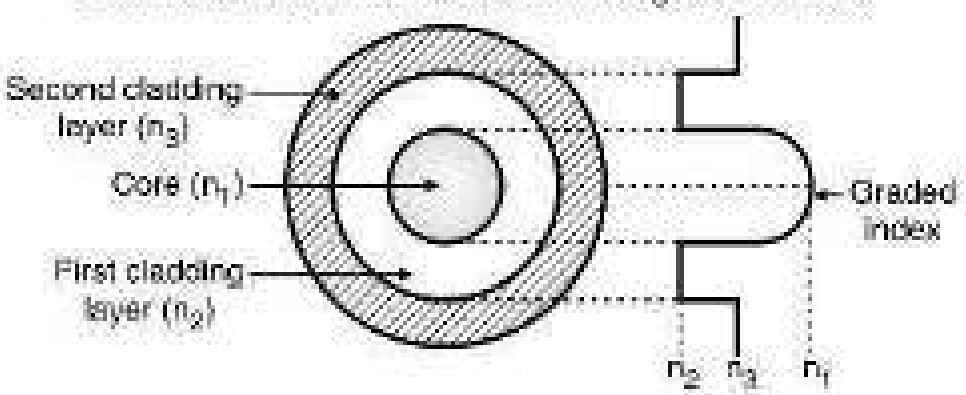


(G-111) **Fig. 3.4.7 : Light propagation in multimode step index fiber**

- Multiple beams will follow different zigzag paths as shown in Fig. 3.4.7.
- The number of reflections that a beam undergoes, depends on the angle of incidence of that beam.
- Hence, at the destination, all the beams do not reach simultaneously.
- This leads to diffusion of signal at the receiver.
- The step index multimode fibers are therefore not used for long distance communications.

Graded index fibers :

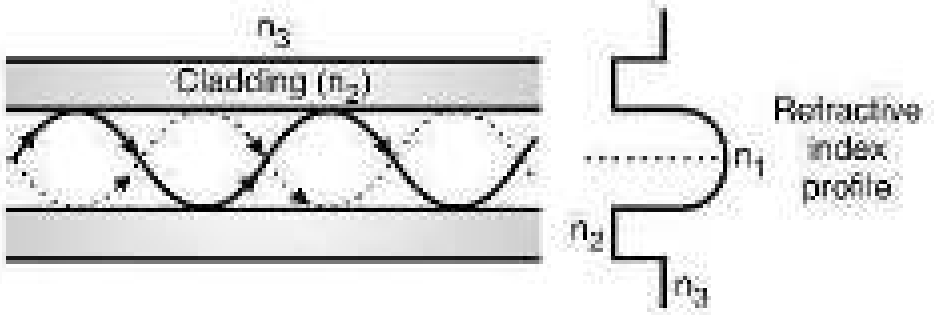
- As shown in Fig. 3.4.8, the refractive index of the fiber core does not remain constant throughout its bulk.



(G-112) **Fig. 3.4.8 : Refractive index profile of a graded index fiber**

- Instead it is maximum at the center of the core and reduces gradually towards the walls of the core.
- In order to get this type of index profile the material in the fiber core is modified.

- Due to the modification in the index profile, the light gets refracted inside the fiber core and does not travel in straight line as shown in Fig. 3.4.9.



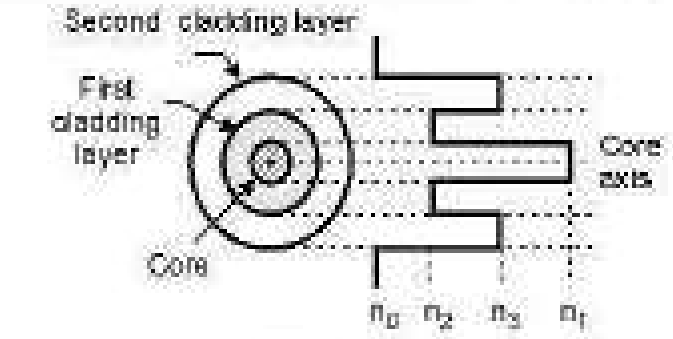
(G-113) **Fig. 3.4.9 : Propagation of light in a graded index fiber**

- Instead the light rays are curved towards the center of the core.
- These rays have been launched into the core within the acceptance cone.
- The acceptance cone of a graded index core is larger than that of the step index core.
- In graded index fibers as well different beams result in different curves or waveforms.
- Table 3.4.1 shows the comparison of step index and graded index fibers.

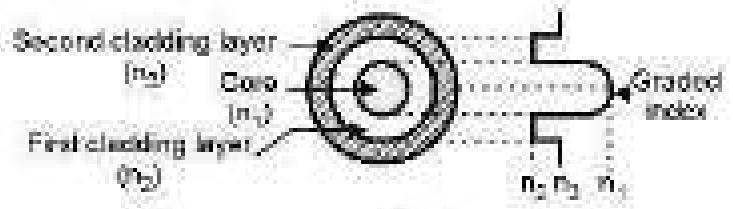
3.4.6 Comparison of Step Index and Graded Index Fibers :

Table 3.4.1 : Comparison of step index and graded index fibers

Sr. No.	Step index fibers	Graded index fibers
1.	The refractive index changes in steps or abruptly.	The refractive index changes gradually.
2.	The light rays travel in straight line through the step index fibers.	The light rays do not travel in straight line through the graded index fibers.
3.	Index profile : Refer Fig. A	Index profile : Refer Fig. B.
4.	The light rays travel in a straight line due to constant refractive index of the fiber throughout the bulk of the core.	The light rays do not travel in straight line due to the continuous refraction. This is due to the continuously changing refractive index throughout the core bulk.
5.	Acceptance cone of these fibers is smaller than that of the graded index fiber.	Acceptance cone of these fibers is larger than that of the step index fiber.



(G-114) **Fig. A**



(G-115) **Fig. B**

3.4.7 Comparison of Single Mode and Multimode Fibers :

Table 3.4.2 : Comparison of single mode and multimode fibers

Sr. No.	Single mode fibers	Multimode fibers
1.	These fibers support only one mode of propagation (TE or TM or TEM)	These fibers support the propagation of many modes.
2.	The travelling signal inside the fiber has only one group velocity.	The different modes have different group velocities and each mode will follow its own path between the transmitter and receiver.
3.	The amount of dispersion introduced is less than that introduced in the multimode fibers.	The intermodal dispersion exists due to different group velocities of various modes.
4.	These fibers can have either a step index or graded index profile.	These fibers can have either step index or graded index profile.
5.	These are high quality fiber for wideband long haul transmission and are fabricated from doped silica for reducing the attenuation.	These are fabricated using the multicomponent glasses or doped silica.

3.4.8 Characteristics of Optical Fiber Cables : W-03, W-09, S-13, W-15, S-18

MSBTE Questions

Q. 1 Describe any four physical characteristics of fiber optic cable. **(W-03, W-09, W-15, S-18, 4 Marks)**

Q. 2 Draw the neat sketch of fiber optic cable. Give the transmission characteristics of fiber optic cable. State its applications. **(S-13, 8 Marks)**

Physical characteristics :

1. Optical fibers are made from glass.
2. The information in the form of light travels over the optical fiber cables.
3. They are guided type media.
4. They are much expensive than the cables.
5. Installation is not easy.

Transmission characteristics :

1. Extremely large bandwidth (upto 2 Gbps).
2. High speed.
3. No effect of electromagnetic interference.
4. The number of nodes connected to this cable does not depend on the length.
5. They offer much lower attenuation. Hence a signal can travel very long distance without the need of any repeater or amplifier.
6. Three wavelength bands are used for fiber optic communication respectively 850 nanometer, 1300 nanometer, 1550 nanometer.
7. Fiber optic cable supports 75 nodes in an Ethernet network.
8. Single mode fiber optic cable are used to provide network links of several hundred kilometres in length.
9. Fiber optic cable does not leak signals so it is immune to evesdropping (tapping of signals).
10. Fiber optic cable does not require a ground, hence it is not affected by potential shifts in the electrical ground, nor does it produce sparks.

3.4.9 Advantages of Optical Fibers :

W-03, W-08, S-09, W-11, S-12, W-12, S-14, S-16, W-16, S-18

MSBTE Questions

Q. 1 State three advantages of optical fiber. **(W-03, S-18, 2 Marks)**

Q. 2 What are the advantages of fiber optic communication over the conventional means of communication ? **(W-08, 4 Marks)**

Q. 3 State the advantages of a optical fiber over copper cables. **(S-09, 1 Mark)**

Q. 4 Explain working of fiber optic cable. Give its advantage and disadvantage. **(W-11, 8 Marks)**

Q. 5 State two advantages of optical fiber. **(S-12, 2 Marks)**

Q. 6 Explain advantages of fiber optic cable. **(W-12, 4 Marks)**

Q. 7 List any two advantages of optical fiber cable. **(S-14, 2 Marks)**

Q. 8 State eight advantages of fiber optic cable over other cables. **(S-16, 8 Marks)**

Q. 9 Draw a sketch indicating the construction of fibre optic cable. State four advantages over electrical cables. **(W-16, 4 Marks)**

– Some of the advantages of fiber optic communication over the conventional means of communication are as follows :

1. Small size and light weight :

– The size (diameter) of the optical fibers is very small (it is comparable to the diameter of human hair).

– Therefore a large number of optical fibers can fit into a cable of small diameter.

2. Easy availability and low cost :

– The material used for the manufacturing of optical fibers is "silica glass".

– This material is easily available. So the optical fibers cost lower than the cables with metallic conductors.

3. No electrical or electromagnetic interference :

– Since the transmission takes place in the form of light rays the signal is not affected due to any electrical or electromagnetic interference.

4. Large bandwidth :

– As the light rays have a very high frequency in the GHz range, the bandwidth of the optical fiber is extremely large.

– This allows transmission of more number of channels.

– Therefore the information carrying capacity of an optical fiber is much higher than that of a co-axial cable.

5. Intermediate amplifier are not required as the transmission losses in the fiber are low.
6. Ground loops are absent.
7. These cables are not affected by the drastic environmental conditions. Because of all these advantages the optical fiber cable is replacing the conventional metallic conductor cable rapidly in many areas.

8. No cross-talk inside the optical fiber cable.
9. Signals at higher data rates can be sent.

3.4.10 Disadvantages of Optical Fiber :

W-03, W-11

MSBTE Questions

Q. 1 State three disadvantages of optical fiber. **(W-03, 2 Marks)**

Q. 2 Explain working of fiber optic cable. Give its advantage and disadvantage. **(W-11, 8 Marks)**

– Some of the disadvantages of optical communication system are :

1. Sophisticated plants are required for manufacturing optical fibers.
2. The initial cost incurred is high.
3. Joining the optical fibers to each other is a difficult job.

3.4.11 Applications :

S-04, S-13, S-15

MSBTE Questions

Q. 1 State applications of optical fiber cables. **(S-04, 4 Marks)**

Q. 2 Draw the neat sketch of fiber optic cable. Give the transmission characteristics of fiber optic cable. State its applications. **(S-13, 8 Marks)**

Q. 3 State two applications of optical fibre cable. **(S-15, 2 Marks)**

1. Optical fiber transmission systems are widely used in the backbone of networks.
2. Optical fibers are now used in the telephone systems.
3. In the Local Area Networks (LANs).

3.4.12 Comparison of Wired Media :

W-09, W-10, S-11, W-11

MSBTE Questions

Q. 1 Compare twisted pair with co-axial cable. **(W-09, 4 Marks)**

Q. 2 Compare twisted pair cable and coaxial cable with respect to :

1. Cost 2. Bandwidth
3. Attenuation 4. EMI **(W-10, 4 Marks)**

Q. 3 Compare co-axial cable and optical fibre cable with eight points. **(S-11, 4 Marks)**

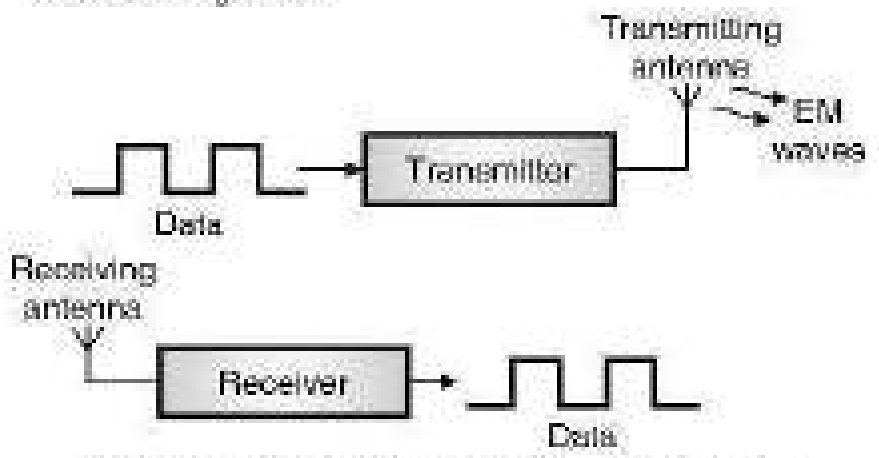
Q. 4 Compare fiber optic cable and STP with atleast four points. **(W-11, 4 Marks)**

Sr. No.	Twisted pair cable	Co-axial cable	Optical fiber
1.	Transmission of signals takes place in the electrical form over the metallic conducting wires.	Transmission of signals takes place in the electrical form over the inner conductor of the cable.	Signal transmission takes place in an optical form over a glass fiber.
2.	Noise immunity is low. Therefore more distortion.	Higher noise immunity than the twisted pair cable due to the presence of shielding conductor.	Highest noise immunity as the light rays are unaffected by the electrical noise.
3.	Affected due to external magnetic field.	Less affected due to external magnetic field.	Not affected by the external magnetic field.
4.	Short circuit between the two conductors is possible.	Short circuit between the two conductors is possible.	Short circuit is not possible.
5.	Cheapest	Moderately expensive	Expensive
6.	Can support low data rates.	Moderately high data rates	Very high data rates.
7.	Power loss due to conduction and radiation.	Power loss due to conduction	Power loss due to absorption, scattering, dispersion and bending.
8.	Low bandwidth	Moderately high bandwidth	Very high bandwidth
9.	Node capacity per segment is 2	Node capacity per segment is 30 to 100	Node capacity per segment is 2.
10.	Attenuation is very high	Attenuation is low	Attenuation is very low.
11.	Installation is easy	Installation is fairly easy	Installation is difficult.
12.	Electromegnetic interference (EMI) can take place	EMI is reduced due to shielding	EMI is not present.

3.5 Unguided (Wireless) Transmission Media :

Concept :

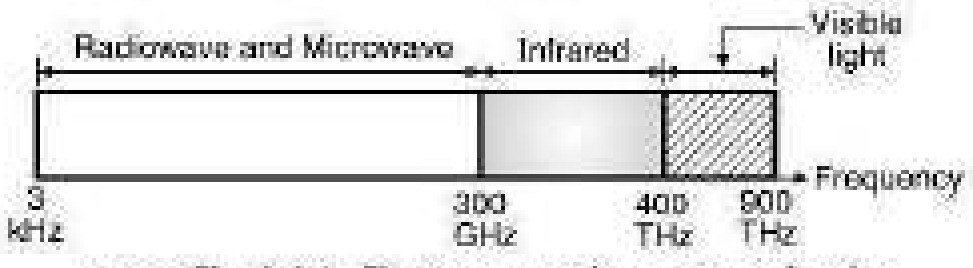
- As already defined, an unguided media (also called as wireless media) does not use a conductor or wire as a communication channel.
- Instead it uses the air or vacuum as medium to carry the information from transmitter to receiver.
- A transmitter first converts the data signal into electromagnetic waves and transmits them using a suitable antenna.
- The receiver receives them using a receiving antenna and converts the EM waves into data signal again, as shown in Fig. 3.5.1.



(G-117) **Fig. 3.5.1 : Concept of unguided media**

3.6 Electromagnetic Spectrum :

- We can use EM waves of different frequencies for different communication applications.
- The electromagnetic spectrum used for wireless communication is shown in Fig. 3.6.1. the signal from sender to receiver travels in the form of electromagnetic radiation through air.



(G-118) **Fig. 3.6.1 : Electromagnetic spectrum for the wireless communication**

3.6.1 Propagation Methods :

- The signals can travel from the transmitter to receiver in many different ways. The three most important methods are :

1. Ground wave propagation
2. Sky propagation.
3. Space propagation or line of sight propagation.

3.6.2 Communication Bands :

S-11, W-11, S-17

MSBTE Questions

- **Q. 1** Enlist any four communication bands for unguided media with their frequency range. **(S-11, 2 Marks)**
- **Q. 2** What is communication band ? **(W-11, 4 Marks)**
- **Q. 3** Enlist any four communication bands for unguided media with their frequency range. **(S-17, 4 Marks)**

- The electromagnetic spectrum is divided into several subbands.
- Table 3.6.1 gives various frequency bands, corresponding type of propagation and application.

Table 3.6.1 : Segments of the electromagnetic spectrum

Sr. No.	Name	Frequency	Wavelength
1.	Extremely Low Frequency (ELF)	30-300 Hz	10^7 to 10^6 m
2.	Voice Frequencies (VF)	300-3000 Hz	10^6 to 10^5 m
3.	Very Low Frequencies (VLF)	3-30 kHz	10^5 to 10^4 m
4.	Low Frequencies (LF)	30-300 kHz	10^4 to 10^3 m
5.	Medium Frequencies (MF)	300 kHz – 3 MHz	10^3 to 10^2 m
6.	High Frequencies (HF)	3-30 MHz	10^2 to 10 m
7.	Very High Frequencies (VHF)	30-300 MHz	10 to 1 m
8.	Ultra High Frequencies (UHF)	300 MHz-3GHz	1 to 10^{-1} m
9.	Super High Frequencies (SHF)	3-30 GHz	10^{-1} to 10^{-2} m
10.	Extremely High Frequencies (EHF)	30-300 GHz	10^{-2} to 10^{-3} m
11.	Infrared	–	0.7 to 10 μm
12.	Visible light	–	0.4 μm to 0.8 μm

3.6.3 Infrared Signals :

- The EM signals having frequencies above 300 GHz are not referred as radio waves.
- The signal occupying the range between 0.1 mm and 700 nanometers (nm) that is 300 GHz to 400. THz are called infrared signals.
- These are used in various special types of communications. Some of them are as follows :
  1. In astronomy to detect stars and other heavenly bodies.
  2. In the guided weapon systems.
  3. TV remote control.
  4. Wireless keyboards and mouse.

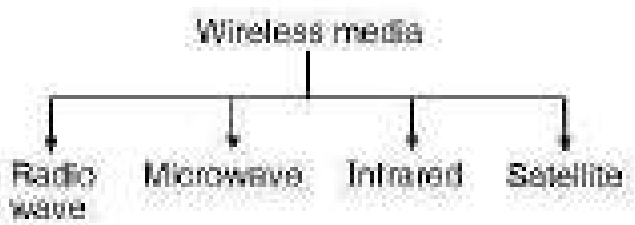
3.6.4 Visible Light :

- Light is a special type of electromagnetic radiation. It has wavelength in the range of 0.4 to 0.8 µm. and its frequency range is 400 THz to 900 THz.
- Light is used for various kinds of communications.
- Light waves can be modulated and transmitted through the glass fibers in the optical fiber communication system.
- Light signals can also be transmitted through free space. Laser is a type of light, which can be easily modulated with voice, video and data information.

3.7 Types of Wireless Media :

I-Scheme : S-19

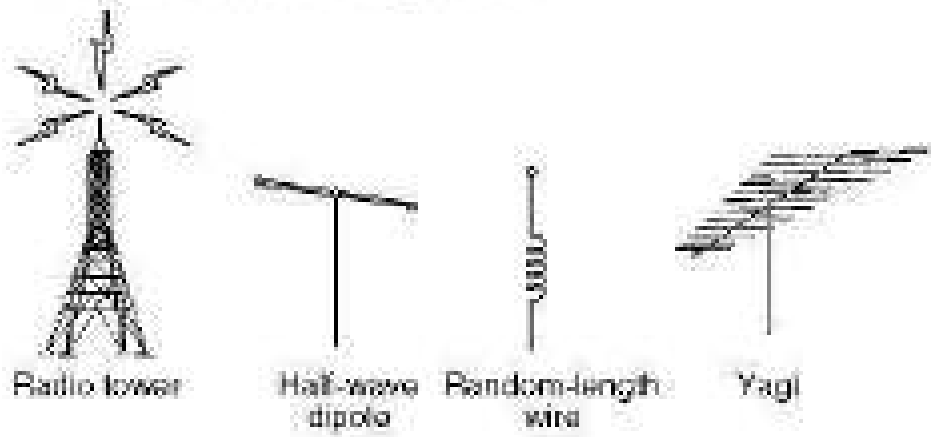
- The wireless media is not in the form of an electrical or optical conductor. In most cases the earths atmosphere is used as the physical path to carry data from sender to receiver.
- Wireless media is used when it is not possible to use media due to distance or obstructions make cable media difficult. There are four main types :
  1. Radiowave 2. Microwave
  3. Infrared. 4. Satellite.



(G-119) **Fig. 3.7.1 : Classification of wireless media**

3.7.1 Radio Wave Transmission Systems :

- Radio waves have frequencies between 10 kHz and 1 gigahertz. The range of electromagnetic spectrum between 10 kHz and 1 GHz is called Radio Frequency (RF).
- Radio waves include the following types :
  1. Short wave used in AM radio.
  2. Very High Frequency (VHF) used in FM radio and TV.
  3. Ultra High Frequency (UHF) used in TV.
- The radio frequency bands are regulated and require a license from the regulatory body.
- Unregulated frequency bands are also present which operate at less than 1 watt transmitted power.
- Radio waves can broadcast omnidirectionally or directionally.
- Various types of antennas are used to broadcast these signals as shown in Fig. 3.7.2.



(G-120) **Fig. 3.7.2 : Various types of antennas**

- The power of the RF signal is determined by the antenna and transceiver.
- Each range has characteristics that affect its use in computer network.
- For computer network applications, radio waves fall into three categories :
  1. Low power, single frequency.
  2. High power, single frequency.
  3. Spread - spectrum.

Characteristics of the three types of radio waves :

- The characteristics of the three types of radio wave are given in Table 3.7.1.

Table 3.7.1

Sr. No.	Factors	Low power single frequency	High power single frequency	Spread spectrum
1.	Frequency range	All radio frequencies	All radio frequencies	All radio frequencies (typically 902 to 928 MHz.)
2.	Bandwidth capacity	1 - 10 Mbps	1 - 10 Mbps	2 - 6 Mbps
3.	Attenuation	High	Low	High
4.	EMI	Poor	Poor	Fair
5.	Installation	Simple	High	Moderate
6.	Cost	Low	Higher	Moderate

- The various areas of applications and the corresponding distances involved are given in Table 3.7.2.

Table 3.7.2

Sr. No.	System	Distance
1.	Paging	Tens of kilometres
2.	Cordless telephone	Tens of meters
3.	Cellular phone	Few hundred km
4.	Wireless LAN	100 m

Applications :

- Some of the important applications of radio transmission systems are :
  1. Cellular communication
  2. Wireless LAN
  3. Point to point and point to multipoint radio systems
  4. Satellite communication

3.7.2 Microwave Transmission System :

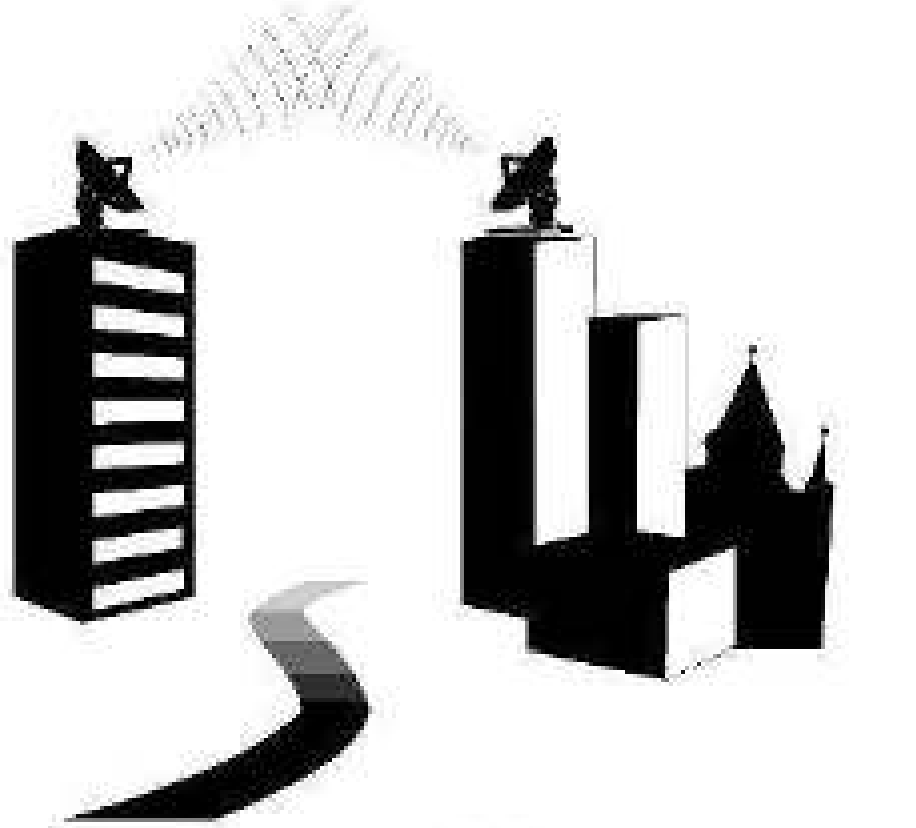
- It makes use of the lower gigahertz frequencies of the electromagnetic spectrum.
- These frequencies are higher than the RF and they produce better throughput and performance.
- There are two types of microwave data communication systems :
  1. Terrestrial 2. Satellite.

Microwaves :

- Microwaves are basically unidirectional electromagnetic waves with a frequency range from 1 to 300 GHz.
- Microwaves use **space wave** propagation. The space wave propagation is also called as **line of sight** communication.
- Due to large bandwidth available it is possible to allot wider subbands. Therefore high data rates can be easily supported using microwave communication.

3.7.3 Terrestrial Microwave Systems :

- These systems use directional parabolic antennas to transmit and receive signals in the lower gigahertz range as shown in Fig. 3.7.3.



(G-121) **Fig. 3.7.3 : Terrestrial microwave system**

- The signals are highly focussed and the physical path must be line of sight.
- Relay towers are used to extend the range. Smaller terrestrial microwave systems can be used even within a building.
- Microwave LANs operate at low power using small transmitters that communicate with omnidirectional hubs.
- Hubs can then be connected to form an entire network.

Characteristics of terrestrial microwave systems :

- Terrestrial microwave systems have the following characteristics :

1. The frequency range used is from 4 - 6 GHz and 21 to 23 GHz.

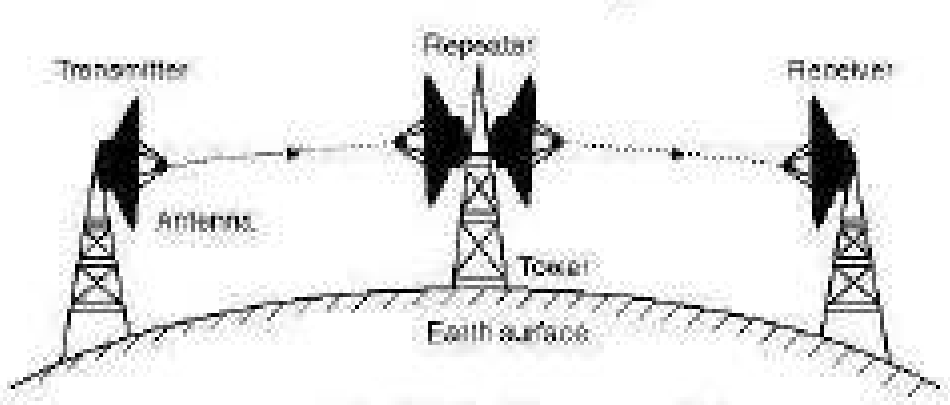
2. It supports a bandwidth from 1 to 10 mbps.
3. Attenuation is dependent on frequency, signal strength, antenna size and atmospheric conditions.
4. The signals are affected by problems such as EMI effect, jamming etc.
5. Line of sight requirements make installation difficult.
6. Short distance systems can be inexpensive but long distance systems are relatively expensive.

3.7.4 RF Link (Microwave Link) : S-11

MSBTE Questions

Q. 1 Explain Microwave (RF) Link with diagram. **(S-11, 4 Marks)**

- Long form of RF link is radio frequency link. This is actually a type of point to point wireless communication.
- The Radio Frequencies used for RF links are in microwave range therefore, RF links are also called as microwave links. This is shown in Fig. 3.7.4.



(S-12) **Fig. 3.7.4 : Microwave link**

- Although many wire communication systems use copper wires or optical fiber, some system prefer to use air as medium.
- This happens when infrared, lasers, microwaves and radio are used for the transmission of data, as they do not need any physical medium.
- For long distance communication, microwave radio transmission is successfully and popularly used as an alternative to co-axial cable.
- The signal transmission takes place in the form of electromagnetic waves which have wavelengths of few centimeters.
- Parabolic antennas can be mounted on the towers to send a beam of waves to another antenna, tens of kilometres away.
- The transmitting and receiving antennas are highly directional to enable a point to point communication.
- This system is widely used for both telephone and television transmission.
- The higher the tower which holds the antenna, the greater is the range. With a 100 metre high tower, the distances of 100 km can be easily covered.

Advantages of microwave link :

- Some of the important advantages are as follows :

1. Installation of towers and associated equipments is cheaper than laying down a cable of 100 km length.
2. Less maintenance as compared to cables.
3. Repeaters can be used. So effect of noise is reduced.
4. No adverse effects such as cable breakage etc.
5. Due to the use of highly directional antenna, these links do not make any interference with other communication systems.
6. Size of transmitter and receiver reduces due to the use of high frequency.

Disadvantages :

1. Signal strength at the receiving antenna reduces due to multipath reception.
2. The transmission will be affected by the thunderstorms, and other atmospheric phenomenons.

Applications of microwave transmission :

S-12, S-15, S-17

MSBTE Questions

Q. 1 State any two applications of microwave communication. **(S-12, S-15, S-17, 2 Marks)**

1. One-to-one communication.
2. In cellular phones.
3. In satellite networks.
4. In the wireless LANs.

3.8 Use of Infrared Light as Unguided Media :

- The electromagnetic waves having frequencies from 300 GHz to 400 THz (wave lengths from 1 mm to 770 nm) are known as infrared waves.
- IR waves uses line-of sight propagation (Space wave propagation).

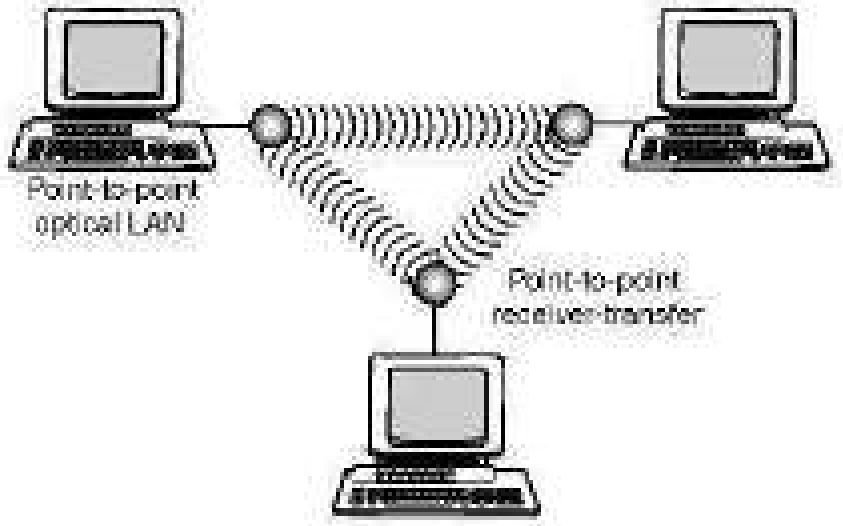
- Infrared light is a communication medium whose properties are significantly different from those of the radio frequencies.
- A very important property of the infrared light is that it cannot penetrate walls.
- That means it can be easily contained within a room.
- Due to this property, the infrared light can be used with a much reduced interference.
- Also the same frequency band can be used in the equipments located in the adjacent rooms as well.
- The wavelength of the infrared light ranges from 850 nm and 900 nm, where the receivers with good sensitivity are available.
- Another advantage of infrared communication is the very large bandwidth which is available for use but has not been exploited to its full extent.
- The major disadvantage is that the sun generates radiation in the infrared band.
- This can cause a lot of interference with the IR communication.
- The infrared band can be used in development of very high speed wireless LANs in future.

3.8.1 Standards of Infrared : W-14

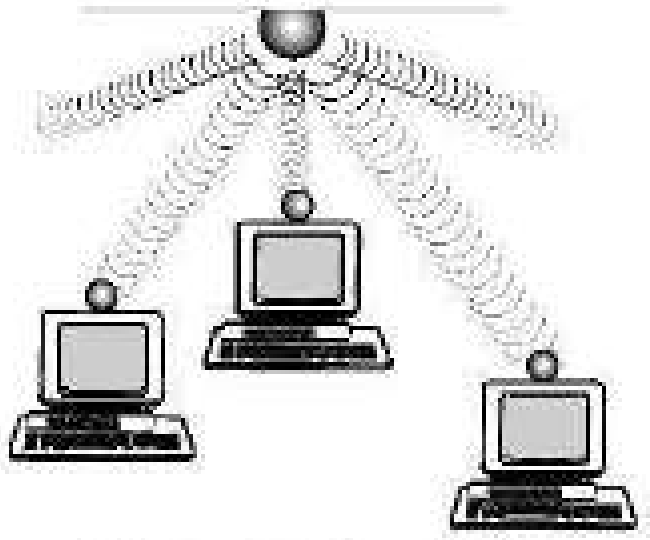
MSBTE Questions

Q. 1 Explain infrared communication. List any two disadvantages of infrared communication. **(W-14, 4 Marks)**

- A number of standards have been developed for an infrared data link (IRDA).
- The IRDA-C standard provides the standards for the bidirectional communications used in cordless devices such as mice, keyboards, joysticks and handheld computers.
- The IRDA-C standard operates at a bit rate of 75 kbits/sec and the distance range is upto 8 meters.
- Another standard called IRDA-D standard operates on the data rates from 115 kb/s to 4 Mb/s, with a distance range upto 1 metre.
- The IR data links can be designed as a wireless alternative to wired connection between computer and printer, or keyboard, mouse etc.
- One advantage of infrared is that an FCC license is not required to use it.
- The only disadvantage of infrared signals is that they cannot penetrate walls or other objects and they are diluted by strong light sources.



(a) Point-to-point infrared media in a network



(b) Broadcast infrared media

(G-125) **Fig. 3.8.1**

Advantages of infrared :

1. Very large bandwidth.
2. No electromagnetic interference.
3. It does not penetrate walls. Therefore there is no interference between the applications using IR, kept in different rooms.

Disadvantages :

1. It can be used only for short range applications.
2. The infrared transmission from the sun can interfere with the IR communication.
3. Poor performance
4. Low speed of operation.

Applications of Infrared :

1. Very high data rates can be supported, due to very high bandwidth (approximately 400 THz).
2. For communication between keyboard, mouse PCs and printers.

3.9 Satellite Communication :

I-Scheme : S-22

- Moon is a natural satellite of earth. However we are not interested in the natural satellites.
- In this section we will learn something about the artificial (man made) satellites.
- An artificial satellite orbits or revolves around the earth in exactly the same manner as electrons revolve around the nucleus of an atom.
- The paths in which satellites move are called as orbits. The orbits are of different types such as synchronous orbits, polar orbits and inclined orbits, out of which the synchronous or geostationary orbit is used by the geostationary satellites.
- The geostationary satellites take exactly 24 hours to complete one revolution around the earth, therefore they appear to be stationary.
- The satellites can be used for variety of purposes. Depending on the type of application, the satellites are classified into the following categories :
  1. Communication satellites.
  2. Remote sensing satellites.
  3. Weather satellites.
  4. Scientific satellites.

3.9.1 Principle of Satellite Communication :

S-03, W-08, W-11, W-12, S-13, W-14, S-15, W-15, S-17, I-Scheme : S-22

MSBTE Questions

Q. 1 With the help of diagram, explain satellite communication. **(S-03, S-13, 8 Marks)**

Q. 2 With the help of diagram, explain satellite communication. **(W-08, S-15, S-17, 4 Marks)**

Q. 3 Explain working of satellite communication with neat diagram. **(W-11, 4 Marks)**

Q. 4 With neat diagram, explain satellite communication system. **(W-12, 8 Marks)**

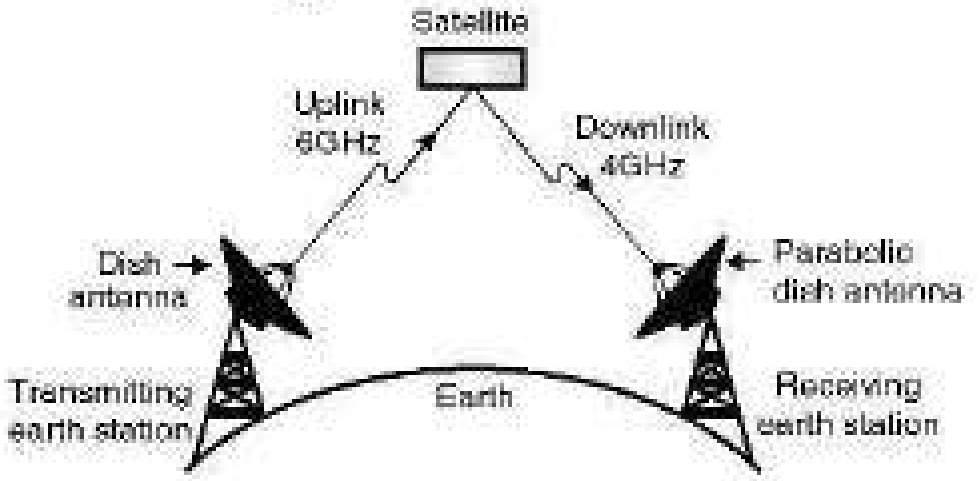
Q. 5 Explain satellite communication with neat diagram. **(W-14, 8 Marks)**

Q. 6 Explain satellite communication with the help of neat diagram. **(W-15, 4 Marks)**

- A geostationary communication satellite works basically as a relay station in space.
- It receives signal from one earth station, amplifies it, improves the signal quality and radiates the signal back to other earth stations.
- Such a relay system allows us to communicate with any corner of the world.

Block diagram and operation :

- The block diagram of a satellite communication system is shown in Fig. 3.9.1.



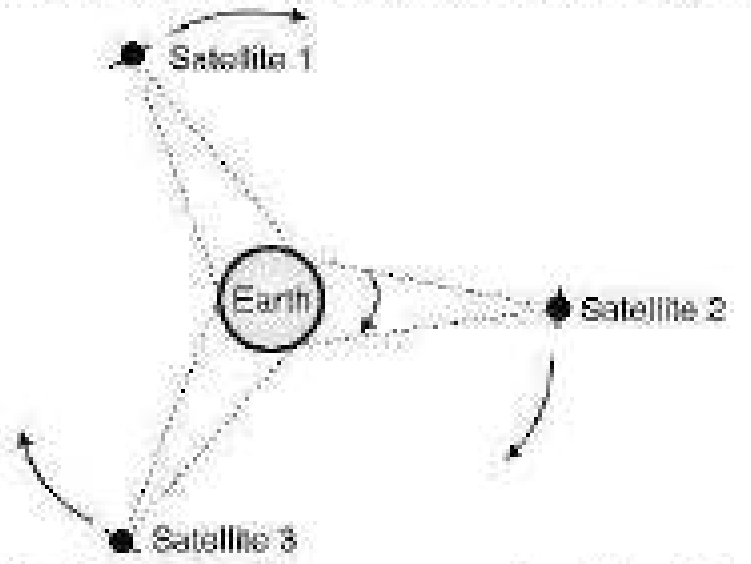
(C-414) **Fig. 3.9.1 : Basic operation of satellite communication system**

- An earth station transmits information signal to the satellite using a highly directional dish antenna.
- The satellite receives this signal, processes it and transmits it back at a reduced frequency.
- The receiving earth stations will receive this signal using parabolic dish antennas pointed towards the satellite.
- The signal which is being transmitted upwards to the satellite is called as the "up-link" and it is normally at a frequency of 6 GHz.
- The signal which is transmitted back to the receiving earth station is called as the "down link" and it is normally at a frequency of 4 GHz.
- Thus a satellite has to receive, process and transmit the signal.
- All these functions are performed by a unit called satellite transponder.
- A communication satellite generally has two sets of transponders, each set having 12 transponders making it a total of 24 transponders.
- Each transponder has a bandwidth of 36 MHz which is sufficient to handle at least one TV channel.
- The uplink signal received by a transponder is weak and downlink signal transmitted by the transponder is strong.
- Therefore to avoid interference between them, the uplink and downlink frequencies are selected to be of different values.

- The operation of satellite takes place at a very high signal frequencies in the **microwave range.**
- The typical band of signal frequencies used for the communication satellites are as follows :
  1. C band : 4/6 GHz
  2. Ku band : 11/14 GHz
  3. Ka band : 20/30 GHz
- The C band frequencies of 4/6 GHz indicate that the downlink frequency is 4 GHz while the Uplink frequency is 6 GHz.
- One of the advantages of operating at such a high frequency is reduction in the size of antennas and other components of the system.
- It is extremely important to maintain the position of the satellite with respect to earth.
- Therefore control routines such as station keeping and altitude control are executed from the control room in the earth stations.
- Multiple access methods such as FDMA (Frequency Division Multiple Access), TDMA (Time Division Multiple Access) and CDMA (Code Division Multiple Access) are used to allow the access of a satellite to the maximum number of earth stations.
- The power requirement of a satellite is satisfied by solar panels and a set of nickel cadmium batteries carried by the satellite itself.

3.9.2 Geostationary (GEO) Satellite :

- The satellites orbiting in the geostationary orbit are called geostationary satellites.
- They travel at the velocity of revolution of earth, hence complete one revolution around the earth in one day i.e. 24 hours.
- This is the reason why geostationary satellites appear to be stationary.
- The geostationary satellites are also called as GEO satellites. They are basically used for communication applications.
- These satellites are at about 36000 km above the earth's surface. There are certain advantages of such a high altitude such as :
- They are much above the inner radiation belt which poses problems to the solar cells of low altitude satellites.
- The solar cells get the solar radiation for almost 99% of the orbital period. Therefore energy storage is not necessary.
- The earth's magnetic field is weak at such heights. Therefore the adverse effects of magnetic field are absent.
- Large coverage area. A geostationary satellite is visible from about 42 % of the earth's surface area.
- Therefore three communication satellites can cover the entire surface area of the earth as shown in Fig. 3.9.2.



(G-815) **Fig. 3.9.2 : Complete coverage of earth's surface from three satellites**

- The geostationary satellites are mostly used as communication satellites.
- The earth stations which transmit and receive information from these satellites are relatively simple and low cost.

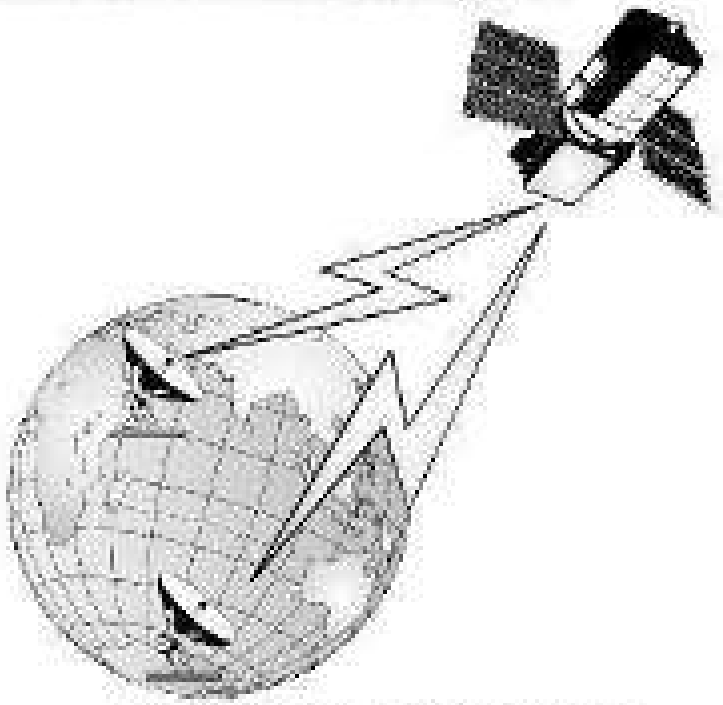
3.9.3 Types of Satellites :

- Satellites are divided in four major categories as follows :
  1. Communication satellite.
  2. Remote-sensing satellite.
  3. Weather satellite.
  4. Scientific satellite.

3.9.4 Satellite System for Data Communication :

- Satellite microwave systems transmits signals between directional parabolic installed at the earth station and satellites antennas.

- They use low gigahertz frequencies and line of sight communication.
- These systems use satellites which are in the geostationary orbit (36000 km above the earth).
- The satellites act as repeaters with receiving antenna, transponder and transmitting antenna.
- Satellite microwave systems can reach the most remote places on earth and communicate with mobile devices.
- This systems works in the following way : a LAN sends a signal through cable media to an antenna which beams the signal to the satellite.
- The satellite then transmits the signal back to another location on earth as shown in Fig. 3.9.3.



(S-818) **Fig. 3.9.3 : Satellite system**

- Satellite microwave systems experience delays between the transmission of a signal and its reception back to the earth (540 msec) due to the distance that the signal has to travel.

3.9.5 Characteristics of Satellite Microwave Systems : S-06, S-10

MSBTE Questions

Q. 1 Describe the characteristics of satellite microwave transmission. **(S-06, S-10, 4 Marks)**

- Satellite microwave systems have the following characteristics :

1. It uses frequency range between 11 to 14 GHz and 4 to 6 GHz. These geostationary satellites placed appropriately can cover the entire earth.
2. It supports a bandwidth and 1 to 10 Mbps.
3. Attenuation depends on frequency, power, antenna size and atmospheric condition.
4. The signals are affected by EMI effect, jamming and other reason.
5. The installation of satellites is extremely difficult and the alignment of earth station antennas must be perfectly aligned.
6. The cost of building and launching is very very expensive.

3.9.6 Comparison of Terrestrial Microwave and Satellite Microwave Transmission Systems :

Sr. No.	Factor	Terrestrial microwave system	Satellite microwave system
1.	Frequency range	Low gigahertz (typically between 4 to 6 or 21 to 23 GHz)	Low gigahertz (typically 11 to 14 GHz)
2.	Bandwidth capacity	About 1 to 10 mbps	About 1 to 10 mbps
3.	Node capacity	2 (sender and receiver)	2 (sender and receiver)
4.	Attenuation	Depends on frequency, signal strength, antenna size and atmospheric conditions	Depends on frequency, power, antenna size and atmospheric conditions
5.	EMI	Poor	Poor
6.	Installation	Moderately difficult	Very difficult
7.	Cost	High	Very high

Application of satellite communication : W-16

MSBTE Questions

Q. 1 State four applications of satellite communication. **(W-16, 2 Marks)**

1. For relay of TV channels.
2. For long distance telephony.
3. Satellite phones in military.
4. For the transmission and reception.
5. For the GPS systems.

Review Questions

Q. 1 Name the layer which is associated with the transmission media.

Q. 2 What is the difference between guided and unguided transmission media ?

Q. 3 State the types of guided media.

Q. 4 Explain the difference between UTP and STP.

Q. 5 What is the effect of twisting the wires in UTP cables ?

Q. 6 Give applications of co-axial cable.

Q. 7 What is the advantage of using shielding ?

Q. 8 Compare the guided transmission media.

Q. 9 State advantages of optical fiber cable.

Q. 10 State the three ways of wireless transmission.

Q. 11 State the applications of microwave communication.

Q. 12 Write a note on : Infrared transmission.

Q. 13 State applications of infrared transmission.

Q. 14 Compare twisted pair (UTP and STP).

Q. 15 Compare twisted pair, co-axial and fiber optic cable.

Q. 16 Which are the two types of microwave transmission systems ?

Q. 17 What are the characteristics of a terrestrial microwave system ?

Q. 18 Compare point to point and broadcast infrared transmission system.

Q. 19 What are the characteristics of a co-axial cable ?

Q. 20 Write note on radio wave transmission system.

Q. 21 Explain the classification of transmission media.

Q. 22 Write a note on microwave communication.

Q. 23 Compare the guided and unguided media.

Q. 24 State various communication bands and their applications.

Q. 25 Explain the basic principle of satellite communication.

Q. 26 What is a GEO satellite ?

Q. 27 State the types of satellites.

3.10 I-Scheme Questions and Answers :

Summer 2019 [Total Marks - 06]

Q. 1 List any four unguided transmission Media.

(Section 3.7) **(2 Marks)**

Q. 2 Draw structural diagram of fiber optic cable and write its functions. **(4 Marks)**

Ans. :

– Refer section 3.4 for structural diagram of fiber optic cable.

Functions of fiber optic cable :

1. Used in telephones and cable TV.
2. Used in computer networks and local area networks.

Winter 2019 [Total Marks - 10]

Q. 3 Define guided and unguided communication media.

(Section 3.1) **(2 Marks)**

Q. 4 Draw and explain fiber optic cable.

(Sections 3.4 and 3.4.2) **(4 Marks)**

Q. 5 State the two advantages and two disadvantages of unguided media **(4 Marks)**

Ans. :

Advantages of unguided media :

1. Used for long distance communication.
2. It provides high speed data transmission.
3. Many stations can receive signals from same sender station.

Disadvantages of unguided media :

1. The communication through unguided media is an insecure.
2. It is susceptible to whether effects like thunder, rain, storm etc.

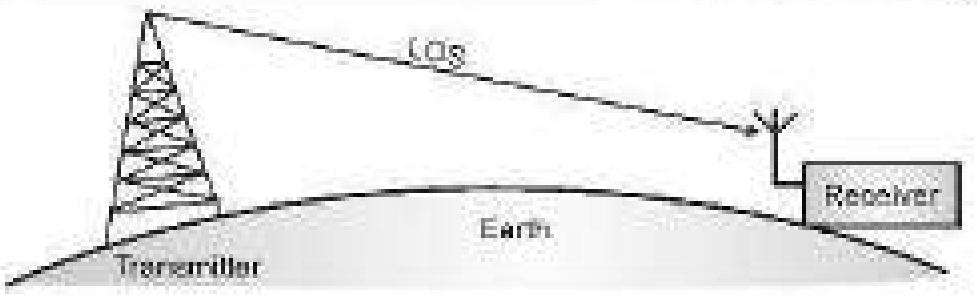
Summer 2022 [Total Marks - 12]

Q. 6 Draw a neat diagram of twisted pair cable and state its types. **(Section 3.3.4)** **(4 Marks)**

Q. 7 Describe line of sight transmission. **(4 Marks)**

Ans. :

- Line of sight is a type of communication where data is transmitted and received only if the transmitter and receiver are in view of each other without any obstacle between them.
- Fig. 1 illustrates the LOS communication. LOS is the direct path between two points.



(G-3213) **Fig. 1 : Line of sight communication**

- Example of LOS are as follows :
  1. FM radio.
  2. Microwave communication.
  3. Satellite communication.

Q. 8 Explain satellite communication.

(Sections 3.9 and 3.9.1) **(4 Marks)**

❑❑❑

Chapter 4

Multiplexing

Syllabus

Multiplexing : Frequency Division Multiplexing, Time division multiplexing.

Chapter Contents

4.1 Introduction to Multiplexing :

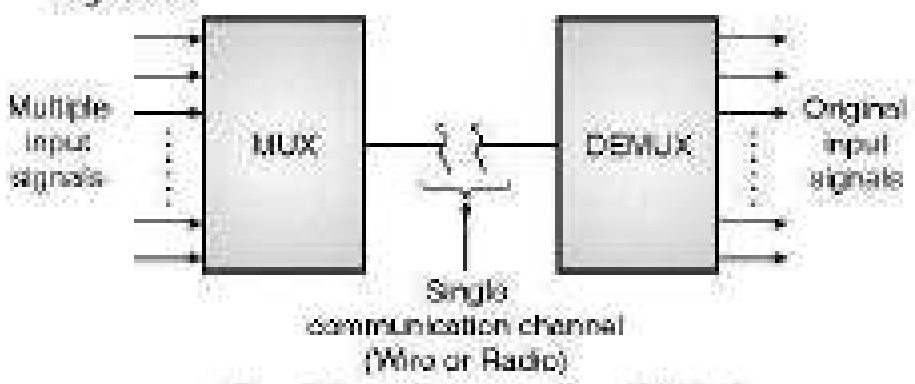
Definition :

- Multiplexing is the process of simultaneously transmitting two or more individual signals over a single communication channel.
- Due to multiplexing it is possible to increase the number of communication channels so that more information can be transmitted.
- The typical applications of multiplexing are in telemetry and telephony or in the satellite communication.

4.2 Concept of Multiplexing and Demultiplexing :

Multiplexing :

- The concept of a simple multiplexer is illustrated in Fig. 4.2.1.



(L-105) **Fig. 4.2.1 : Concept of multiplexing**

- The multiplexer receives a large number of different input signals.
- Multiplexer has only one output which is connected to the single communication channel.
- The multiplexer combines all input signals into a single composite signal and transmits it over the common communication medium.
- Sometimes the composite signal is used for modulating a carrier before transmission.

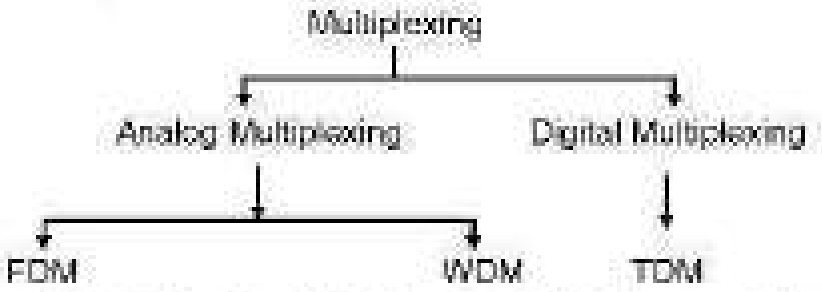
Demultiplexing :

- At the receiving end, of communication link, a demultiplexer is used to separate out the signals into their original form.
- The operation of demultiplexer is exactly opposite to that of a multiplexer. Demultiplexing is the process which is exactly opposite to that of multiplexing.

4.2.1 Types of Multiplexing :

I-Scheme : W-19, S-22

- There are three basic types of multiplexing.
- They are :
  1. Frequency division multiplexing (FDM).
  2. Time division multiplexing (TDM).
  3. Wavelength division multiplexing (WDM).
- The multiplexing techniques can be broadly classified into two categories namely analog and digital.
- Analog multiplexing can be either FDM or WDM and digital multiplexing is TDM.
- Fig. 4.2.2 shows the classification of multiplexing techniques.



(L-106) **Fig. 4.2.2 : Classification of multiplexing techniques**

- Generally the FDM and WDM systems are used to deal with the analog information whereas the TDM systems are used to handle the digital information.
- In FDM many signals are transmitted simultaneously where each signal occupies a different frequency slot within a common bandwidth.
- In TDM the signals are not transmitted at a time, instead they are transmitted in different time slots.

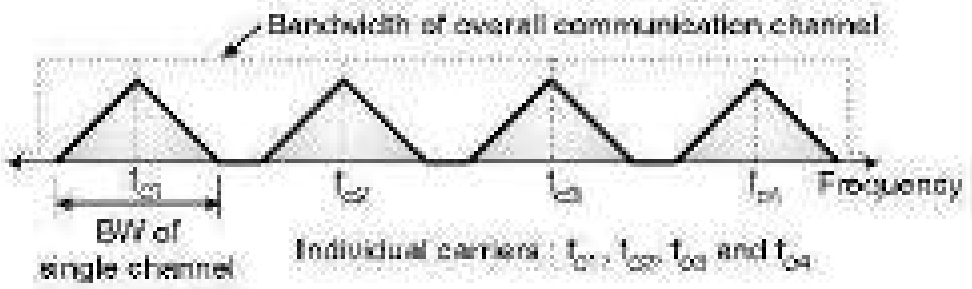
4.3 Frequency Division Multiplexing (FDM) :

I-Scheme : W-19, S-22

Definition :

- FDM is a type of multiplexing in which all the signals or channels to be multiplexed are transmitted at the same time with each channel occupying a distinct non overlapping frequency band.
- The operation of FDM is based on sharing the available bandwidth of a communication channel among the signals to be transmitted.
- That means many signals are transmitted simultaneously with each signal occupying a different frequency slot within the total available bandwidth.
- Each signal to be transmitted modulates a different carrier. The modulation can be AM, SSB, FM or PM.
- The modulated signals are then added together to form a composite signal which is transmitted over a single channel.

- The spectrum of composite FDM signal is shown in Fig. 4.3.1(a).



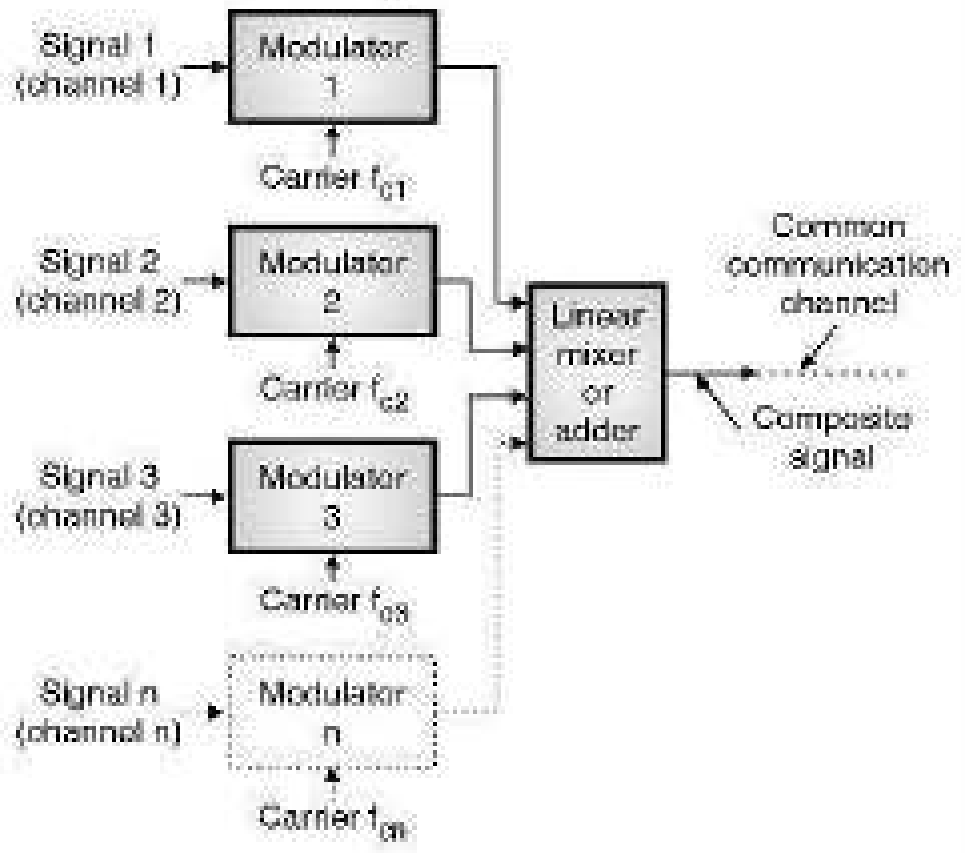
(I-107) **Fig. 4.3.1(a) : Spectrum of FDM signal**

- Generally the FDM systems are used for multiplexing the analog signals.

4.3.1 FDM Transmitter :

Block diagram :

- Fig. 4.3.1(b) shows the block diagram of an FDM transmitter. The signals which are to be multiplexed will each modulate a separate carrier.



(I-108) **Fig. 4.3.1(b) : The FDM transmitter**

- The type of modulation can be AM, SSB, FM or PM.
- The modulated signals are then added together to form a complex signal which is transmitted over a single channel.

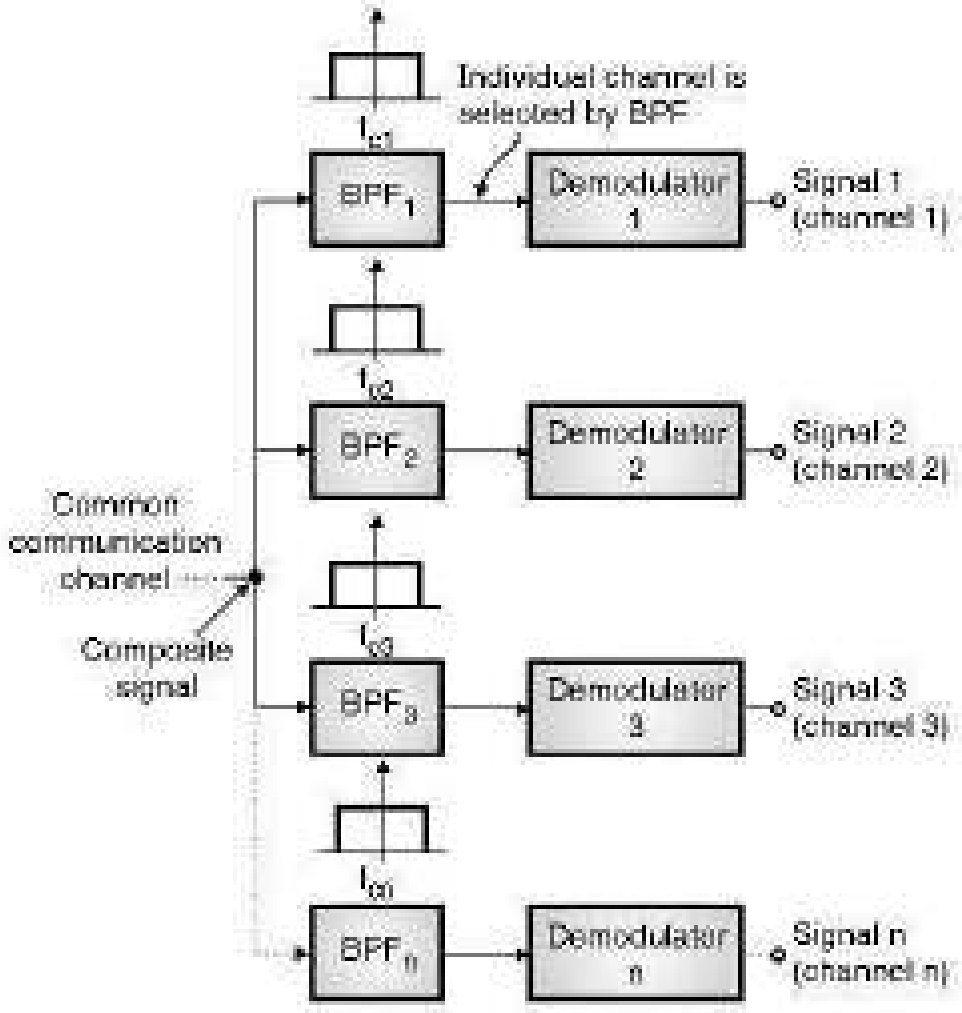
Operation of the FDM transmitter :

- Each signal modulates a separate carrier. The modulator outputs will contain the sidebands of the corresponding signals.
- The modulator outputs are added together in a linear mixer or adder.
- The linear mixer is different from the normal mixers. Here the sum and difference frequency components are not produced.
- But only the algebraic addition of the modulated outputs will take place.
- Different signals are thus added together in the time domain but they have their own separate identity in the frequency domain. This is as shown in the Fig. 4.3.1(a).
- The composite signal at the output of mixer is transmitted over the single communication channel as shown in Fig. 4.3.1(b).
- This signal can be used to modulate a radio transmitter if the FDM signal is to be transmitted through air.

4.3.2 FDM Receiver :

Block diagram and operation :

- The block diagram of an FDM receiver is as shown in Fig. 4.3.1(c). The composite signal is applied to a group of band pass filters (BPF).

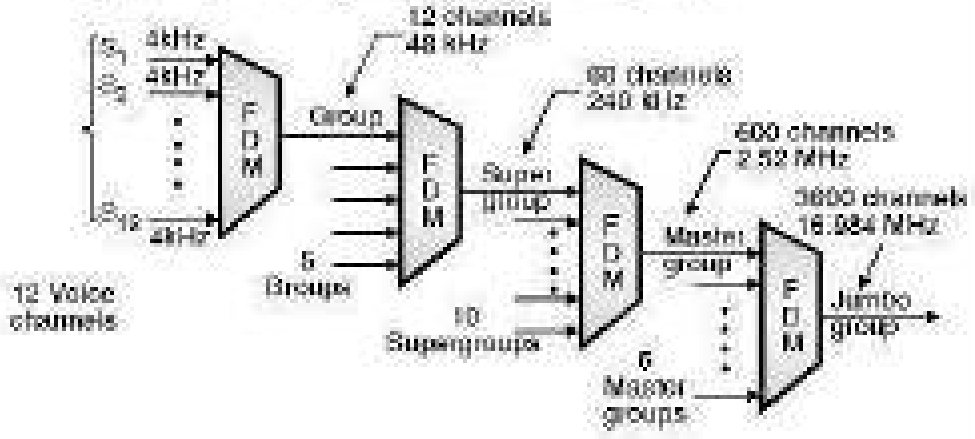


(I-109) **Fig. 4.3.1(c) : FDM receiver**

- Each BPF has a center frequency corresponding to one of the carriers used in the transmitter i.e. f_{c1}, f_{c2}, ... f_{cn} etc.
- The BPFs have an adequate bandwidth to pass all the channel information without any distortion.
- Each filter will pass through only its channel and reject all the other channels.
- Thus all the multiplexed channels are separated out.
- The channel demodulator then removes the carrier and recovers the original signal back.

4.3.3 FDM Hierarchy :

- To maximize the efficiency of their infrastructure, the telephone companies have used multiplexing technique for lower bandwidth lines.
- In this way it is possible to combine many switched or leased lines into fewer but bigger channels.
- One of such hierarchical system is used by AT and T. It is as shown in Fig. 4.3.2 and is made up of groups, super groups, master groups and jumbo groups.



(L-110) **Fig. 4.3.2 : FDM hierarchy**

- The levels of multiplexing is also called as multiplexing hierarchy.
- The different levels of multiplexing which is also called multiplexing hierarchy is as follows :

Level (1) : Basic group [12 voice channels multiplexed together].

↓

Level (2) : Super group [Upto 5 basic groups multiplexed together i.e. upto 60 voice channels].

↓

Level (3) : Master group [Upto 10 super groups multiplexed together i.e. upto 600 voice channels].

↓

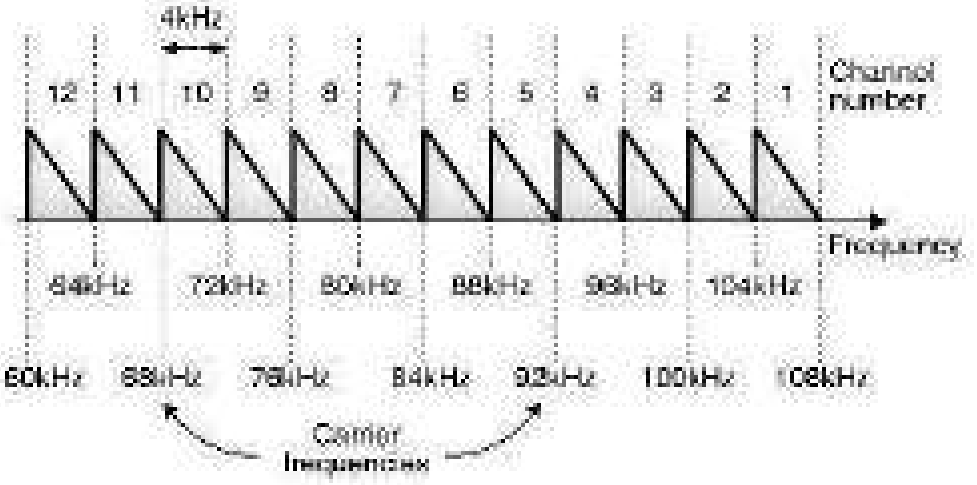
Level (4) : Jumbo group [Upto 6 master groups multiplexed together i.e. upto 3600 voice channels].

(E-1861)

- This hierarchy is used by AT and T and shown in Fig. 4.3.2.

Basic Group [12 voice channels] :

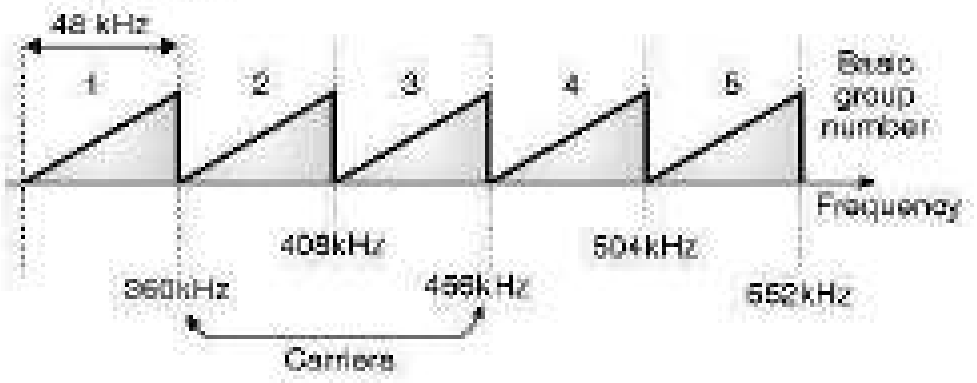
- The frequency plan for the typical basic group is as shown in Fig. 4.3.3.
- Here the 12 voice channels such as telephone channels modulate the carrier frequencies in the range of 60 to 108 kHz range.
- The carrier frequencies are spaced at 4 kHz from each other.
- SSB modulation technique is used to save the bandwidth. Each voice channel is applied to a balanced modulator along with a carrier.
- The output of a balanced modulator consists of the upper and lower sidebands.
- Frequency plans of groups of FDM are nothing but the frequency spectrums.
- The frequency plan for the basic group of FDM is shown in Fig. 4.3.3.



(L-111) **Fig. 4.3.3 : Frequency plan for the basic group of FDM**

Super group :

- The frequency plan for a super group is as shown in Fig. 4.3.4. A super group consists of at the most 60 voice channels.



(L-112) **Fig. 4.3.4 : Frequency plan for a super group of FDM**

4.4 Advantages, Disadvantages and Applications of FDM :

4.4.1 Advantages of FDM :

1. A large number of signals (channels) can be transmitted simultaneously.
2. FDM does not need synchronization between its transmitter and receiver for proper operation.
3. Demodulation of FDM is easy.
4. Due to slow narrow band fading only a single channel gets affected.

4.4.2 Disadvantages of FDM :

1. The communication channel must have a very large bandwidth.
2. Intermodulation distortion takes place.
3. Large number of modulators and filters are required.
4. FDM suffers from the problem of crosstalk.
5. All the FDM channels get affected due to wideband fading.

4.4.3 Applications of FDM :

- Some of the important applications of FDM are :

1. Telephone systems.
2. AM (amplitude modulation) and FM (frequency modulation) radio broadcasting.
3. TV broadcasting
4. First generation of cellular phones used FDM.

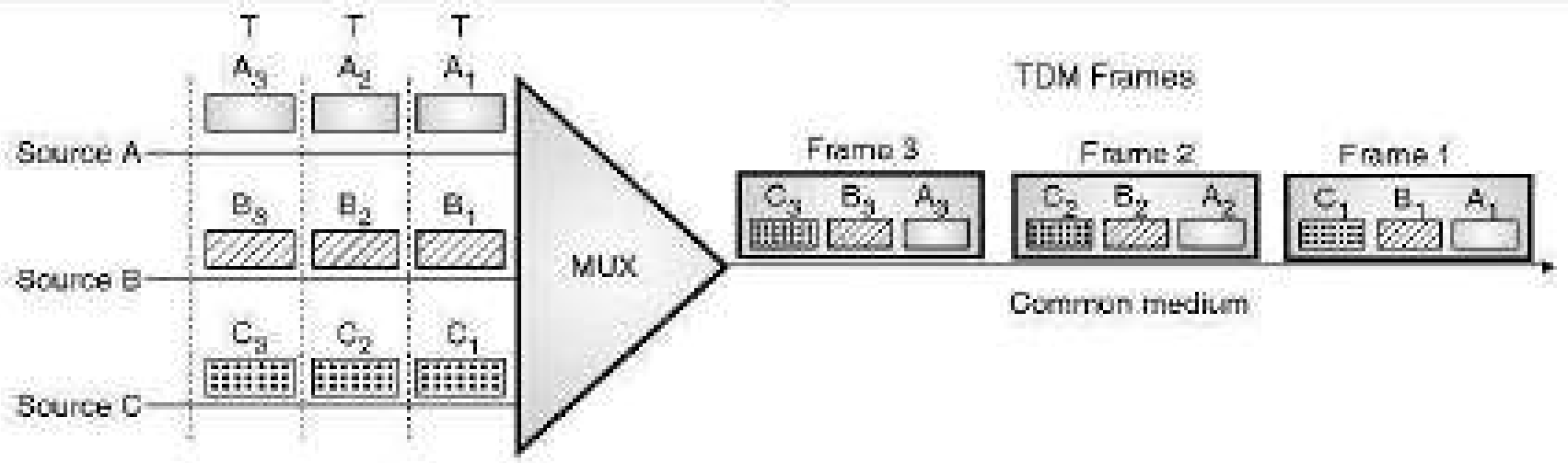
4.5 Synchronous Time Division Multiplexing : I-Scheme : W-19

Definition :

- TDM is defined as the type of multiplexing in which, the signals to be multiplexed are sent in a sequential manner (one by one) but all of them occupy the same frequency band.
- TDM is a digital multiplexing process.
- In TDM all the signals to be transmitted are not transmitted simultaneously. Instead, they are transmitted one-by-one.
- Thus each signal will be transmitted for a very short time. One cycle or frame is said to be complete when all the signals are transmitted once on the transmission channel. The TDM principle is illustrated in Fig. 4.5.1.

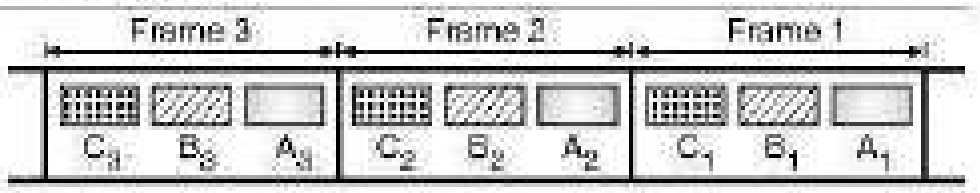
(I-122) **Fig. 4.5.1 : Principle of TDM**

- As shown in the Fig. 4.5.1 one transmission of each channel completes one cycle of operation called as a "Frame".
- The TDM system can be used to multiplex analog or digital signals, however it is more suitable for the digital signal multiplexing.
- The concept of TDM will be more clear if you refer to Fig. 4.5.2.



(I-123) **Fig. 4.5.2 : TDM system**

- The data flow of each source (A, B or C) is divided into units (say A_1, A_2 or B_1, C_1 etc.)
- Then one unit from each source is taken and combined to form one frame. The size of each unit such as A_1, B_1 etc. can be 1 bit or several bits.
- Fig. 4.5.3 shows the frames of TDM signal. For 3 inputs being multiplexed, a frame of TDM will consist of 3 units i.e. one unit from each source.
- Similarly for n number of inputs, each TDM frame will consist of n units.



(I-124) **Fig. 4.5.3 : TDM frames**

- The TDM signal in the form of frames is transmitted on the common communication medium.

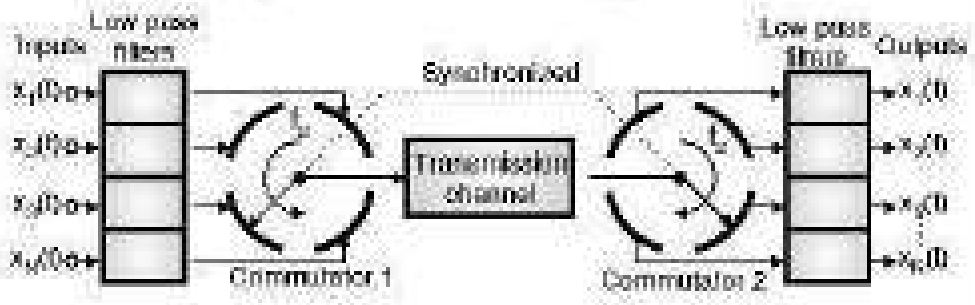
Data rate :

- For a TDM, the data rate of the multiplexed signal is always n times the data rate of individual sources, where n is the number of sources.

- So if three sources are being multiplexed, then the data rate of the TDM signal is three times higher than the individual data rate.
- Naturally the duration of every unit (A_1 or B_1 etc.) in TDM signal is n times shorter than the unit duration before multiplexing.

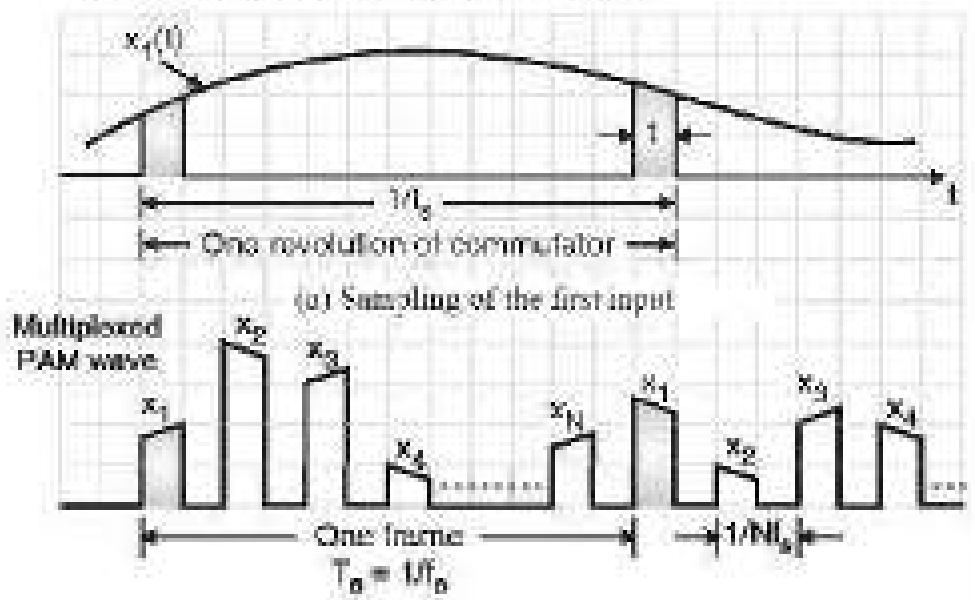
4.5.1 PAM - TDM System :

- The TDM system which is going to be discussed now, combines the concepts of PAM and TDM both.
- The TDM system is as shown in Fig. 4.5.4.



(L-125) **Fig. 4.5.4 : PAM/TDM system**

- The operation of the system is as follows :
- The multiplexer here is a single pole rotating switch or commutator.
- It can be a mechanical switch or an electronic switch. It rotates at f_s rotations per second.
- As the switch arm rotates, it is going to make contact with the position 1, 2, 3 or N for a short time. To these contacts are connected the N analog signals which are to be multiplexed.
- Thus the switch arm will connect these N input signals one by one to the communication channel.
- The waveform of a TDM signal which is being transmitted is as shown in Fig. 4.5.5.



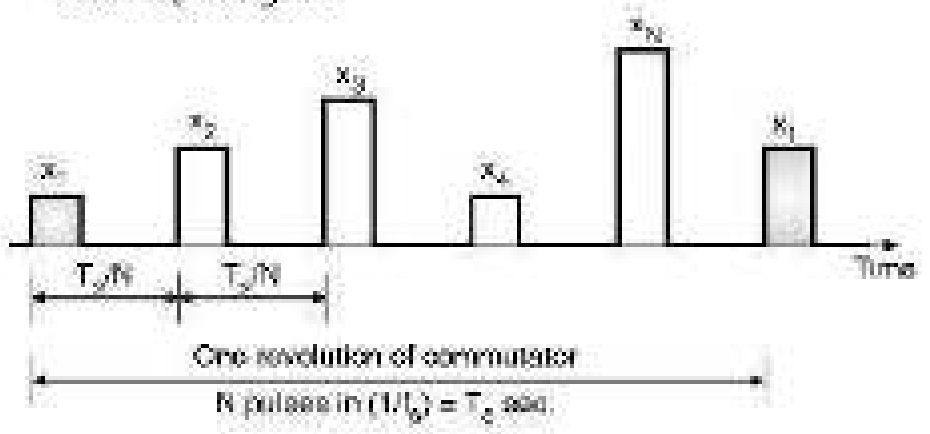
(b) Multiplexed PAM signal, transmitted on the transmission channel

(L-126) **Fig. 4.5.5**

- It shows that the rotary switch samples each channel during each of its rotations. Each rotation corresponds to one frame.
- Hence 1 frame is completed in T_s seconds where $T_s = 1/f_s$.
- At the receiver, there is one more rotating switch or commutator used for demultiplexing.
- It is important to note that this switch must rotate at the same speed as that of the commutator 1 at the transmitter and its position must be synchronized with commutator 1 in order to ensure proper demultiplexing.
- The same principle of multiplexing can be used for multiplexing more number of signals.

4.5.2 Signaling Rate (r) :

- The signaling rate of a TDM system is defined as the number of pulses transmitted per second.
- It is denoted by "r". Let us now derive the expression for the signaling rate of the PAM-TDM system.
- Let W = Maximum frequency of all the input signals x_1 to x_N.
- Therefore as per Nyquist criteria, the sampling frequency $f_s \geq 2$ W. Therefore the speed of rotation of the commentators is f_s rotations per second with $f_s \geq 2$ W.
- As shown in Fig. 4.5.6, one revolution of commutators corresponding to one frame contains one sample from each input signal.



(L-129) **Fig. 4.5.6 : Calculation of number of pulses per second for PAM-TDM system**

$$\therefore \quad 1 \text{ Revolution} \Rightarrow 1 \text{ frame} \Rightarrow N \text{ pulses} \qquad ...(4.5.1)$$

- 1 frame period is $(1/f_s)$ i.e. T_s seconds. Therefore in "T_s" seconds "N" number of pulses are transmitted. Hence the pulse to pulse spacing within the frame is given by,

$$\text{Pulse to pulse spacing} = \frac{T_s}{N} = \frac{1}{Nf_s} \quad ...(4.5.2)$$

- As the period of one pulse (ON + OFF) is $(1/Nf_s)$ seconds, the number of pulses per second is given by,

  Number of pulses per second = Nf_s

- This is nothing but the signaling rate.
- $\therefore$ Signaling rate of a TDM system = $r = Nf_s$ pulses/second. But as $f_s \geq 2W$.

Signaling rate of a TDM system = $r \geq 2NW$ pulses/second ...(4.5.3)

- A TDM system is supposed to have its signaling rate as high as possible.
- It is evident from the expressions above that the signaling rate can be increased by increasing the sampling rate f_s and/or the number of input signals N.

4.5.3 Transmission Bandwidth of a TDM Channel :

- The minimum transmission bandwidth of a PAM-TDM channel is given by,

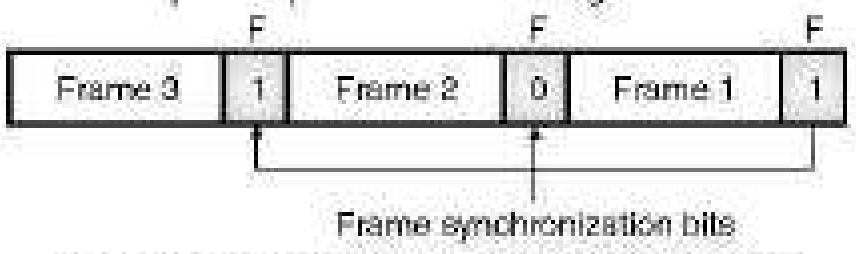
$$B_T = \frac{1}{2} \text{ signaling rate}$$

$\therefore$ Minimum transmission bandwidth $B_T \geq \frac{1}{2} \times 2\,NW$

$\therefore$ Minimum transmission bandwidth $B_T = NW$ ...(4.5.4)

4.5.4 Frame Synchronization :

- The implementation of TDM is not as simple as that of FDM because in TDM, the synchronization of multiplexer and demultiplexer is essential.
- If the synchronization is not there then the bit that belongs to one channel may be received by some other channel.
- Therefore one or more synchronization bits are generally added to the beginning of each frame.
- They are known as the framing bits.
- These bits are called frame synchronizing bits or simply framing bits.
- The framing bits will follow a pattern frame to frame. For example the pattern shown in Fig. 4.5.7 is 101.



(L-131) **Fig. 4.5.7 : Frame synchronization in TDM**

- The framing bit pattern will allow the demux to synchronize itself to the mux.

4.5.5 Advantages of TDM : I-Scheme : S-19

1. Full available channel bandwidth can be utilized for each channel.
2. Intermodulation distortion is absent.
3. TDM circuitry is not very complex.
4. The problem of crosstalk is not severe.

4.5.6 Disadvantages of TDM :

1. Synchronization is essential for proper operation.
2. Due to slow narrowband fading, all the TDM channels may get wiped out.

4.5.7 Applications of TDM :

1. Multiplexing of digital signals.
2. Digital telephony.
3. Satellite communications.
4. Fiber optic communication.
5. Wireless communication applications.

4.6 Comparison of FDM and TDM Systems : S-14, W-16, I-Scheme : S-19

MSBTE Questions

Q. 1 Compare FDM versus TDM. **(S-14, 4 Marks)**

Q. 2 Compare FDM and TDM. **(W-16, 4 Marks)**

Sr. No.	FDM	TDM
1.	The signals which are to be multiplexed are added in the time domain. But they occupy different slots in the frequency domain.	The signals which are to be multiplexed can occupy the entire bandwidth but they are isolated in the time domain.

Sr. No.	FDM	TDM
2.	FDM is usually preferred for the analog signals.	TDM is preferred for the digital signals.
3.	Synchronization is not required.	Synchronization is required.
4.	The FDM requires a complex circuitry at the transmitter and receiver.	TDM circuitry is not very complex.
5.	FDM suffers from the problem of crosstalk due to imperfect band pass filters.	In TDM the problem of crosstalk is not severe.
6.	Due to wideband fading in the transmission medium, all the FDM channels are affected.	Due to fading only a few TDM channels will be affected.
7.	Due to slow narrowband fading taking place in the transmission channel only a single channel may be affected in FDM.	Due to slow narrowband fading all the TDM channels may get wiped out.

4.7 Statistical (Asynchronous) TDM :

S-15

MSBTE Questions

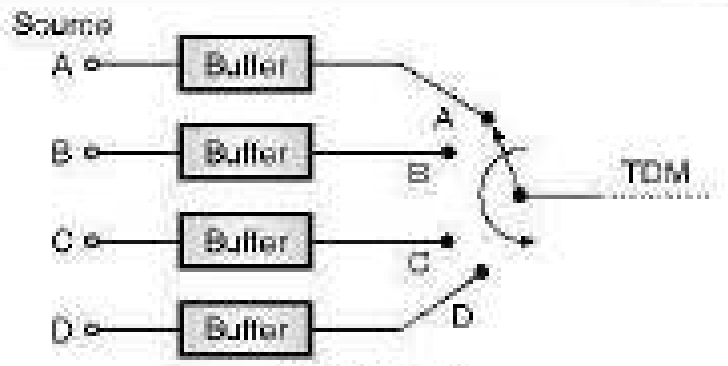
Q. 1 Explain the concept of Asynchronous TDM. **(S-15, 4 Marks)**

Concept :

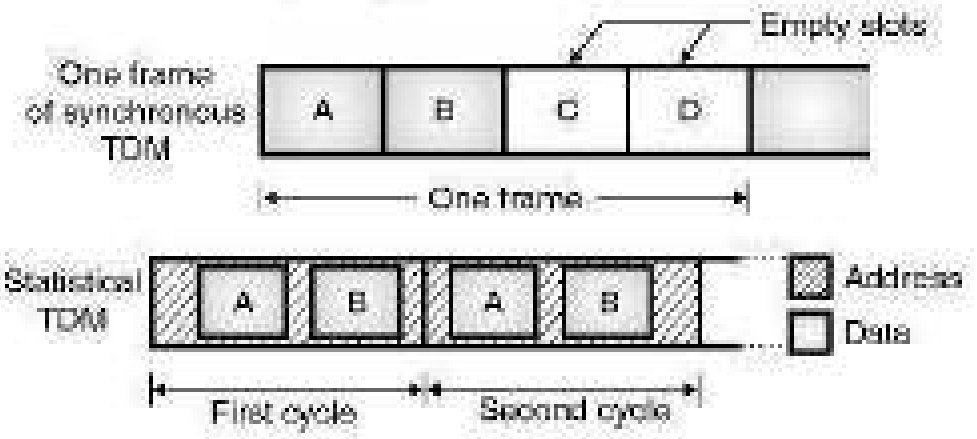
- The TDM system that we have discussed earlier is known as the synchronous TDM.
- This system has a major drawback. In synchronous TDM, many of the time slots in a frame are wasted due to absence of data on some of the time slots.
- Therefore an alternative system called as statistical TDM or asynchronous TDM or intelligent TDM is used.

Block diagram :

- The block diagram of the statistical TDM system is as shown in Fig. 4.7.1(a) and its frame format is as shown in Fig. 4.7.1(b).



(L-138) **(a) Block diagram**



(b) Frame format

(L-139) **Fig. 4.7.1 : Statistical TDM**

Operating principle :

- In statistical TDM, the time slots are not permanently assigned to all the available users (like synchronous TDM).
- Instead, the time slots are allocated dynamically on demand only to those channels holding data for transfer.
- Each TDM channel is called as an I/O line. Thus the statistical TDM has many I/O lines and one high speed multiplexed line.
- Each I/O line has a buffer associated with it. As shown in Fig. 4.7.1, there are N number of I/O lines.
- Out of these only K channels are transmitted which hold data for transfer.
- The remaining (N – K) channels are not considered for transmission.
- In statistical TDM, the multiplexer will "scan" the input buffers of all the channels, sequentially.
- During the scan time, it collects the data until a frame is filled. As soon as a frame is filled, it is transmitted.
- The data is transferred on the transmission medium. The received frame is then distributed among the output buffers by the output multiplexer.

4.7.1 Data Rate of Statistical TDM :

- In statistical TDM system, all the channels are not transmitted in every frame.
- Hence the data rate on the multiplexed line will be less than the sum of the data rates of all the sources.
- Thus a statistical multiplexer can use a transmission medium of lower data rate to support the same number of sources as the synchronous multiplexer.
- That means if we have a synchronous and statistical TDM with equal data rates, then the statistical TDM will support more number of sources.

4.7.2 Slot Size :

- The slot carries both data and address, the ratio of the data size to address size should be reasonable to ensure high efficiency.
- In statistical TDM, the data block contains many bits while address bits are very few.

4.7.3 No Synchronization Bit :

- The statistical TDM frames need not be synchronized. So it is not necessary to use the synchronizing bit.

4.7.4 Bandwidth :

- In statistical TDM, the capacity of multiplexed link is generally less than the sum of capacities of individual channels.
- Therefore the bandwidth requirement of the multiplexed link is less than that for the synchronous TDM.

Improvement in efficiency :

1. The throughput efficiency can be improved by allowing the multiple data sources to be packaged in a single frame.
2. When many sources are packaged in a single frame, it is necessary to specify the length of data for each source. Therefore the statistical TDM subframe consists of a sequence of data fields. Each data field is labelled with an address and a length.

4.7.5 Comparison of FDM, Synchronous TDM and Statistical TDM :

Table 4.7.1 : Comparison of data multiplexer techniques

Sr. No.	Parameter	FDM	Synchronous TDM	Statistical TDM
1.	Line utilization efficiency	Poor	Good	Very good
2.	Flexibility	Poor	Good	Very good
3.	Channel capacity	Poor	Good	Excellent
4.	Error control	Not possible	Not possible	Possible
5.	Multidrop capacity	Very good	Difficult to achieve	Possible
6.	Transmission delay	Does not exist	Low	Random
7.	Cost	High	Low	Moderate

Review Questions

Q. 1 With the help of block schematic, explain the principle of FDM.

Q. 2 Compare FDM and TDM methods of multiplexing ?

Q. 3 Illustrate working of FDM used for 96 channels of telephone.

Q. 4 With the help of block diagram explain the FDM system for telephone communication.

Q. 5 Explain the principles of Time Division Multiplexing.

Q. 6 What is statistical TDM ?

Q. 7 What is the difference between synchronous and statistical TDM ?

Q. 8 What are the advantages of statistical TDM ?

Q. 9 Why is it necessary to use time division multiplexing while transmitting PAM signals ?

Q. 10 Why is synchronization needed in TDM system ?

Q. 11 Describe how transmission distortion of a TDM signal can cause cross-talk between two adjacent channels.

Q. 12 Describe the multiplexing hierarchy for an FDM system.

Q. 13 State advantages and disadvantages of TDM system.

4.8 I-Scheme Questions and Answers :

Summer 2019 [Total Marks - 08]

Q. 1 What advantages does TDM have over FDM in a circuit switched network. **(Section 4.5.5)** **(4 Marks)**

Q. 2 Differentiate between FDM and TDM.

(Section 4.6) **(4 Marks)**

Winter 2019 [Total Marks - 04]

Q. 3 Describe multiplexing techniques.

(Sections 4.2.1, 4.3 and 4.5) **(4 Marks)**

Summer 2022 [Total Marks - 08]

Q. 4 List types of multiplexing. **(Section 4.2.1)** **(2 Marks)**

Q. 5 Explain multiplexing techniques.

(Section 4.3) **(6 Marks)**

❑❑❑

Chapter 5

Switching

Syllabus

Circuit switched networks, Packet switched networks.

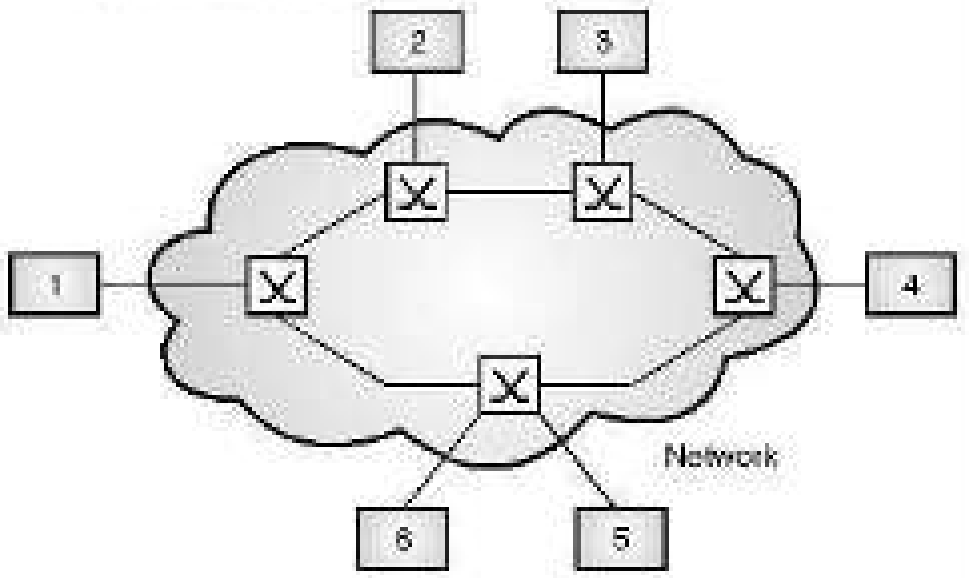
Chapter Contents

5.1 Introduction to Switching :

- A network consists of many switching devices. In order to connect multiple devices, one solution could be to have a point to point connection between each pair of devices. But this increases the number of connections.
- The other solution could be to have a central device and connect every device to each other via the central device (Star topology).
- Both these methods are wasteful and impractical for very large networks. The other topologies also cannot be used.
- Hence a better solution is **switching.** A switched network is made of a series of interconnected nodes called switches.

Definition of a switch :

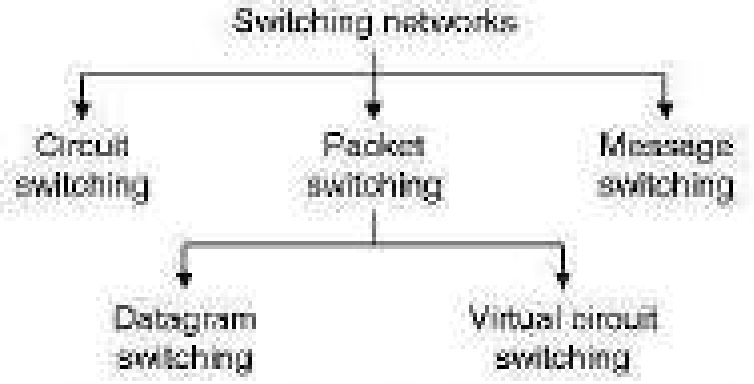
- Switch is a device that creates temporary connections between two or more devices. Fig. 5.1.1 shows a switched network.



(L-616) **Fig. 5.1.1 : Switched network**

5.2 Switching Methods :

- The three basic methods of switching are :
  1. Circuit switching.
  2. Packet switching.
  3. Message switching.
- Out of these, the circuit and packet switching are commonly used today but the message switching has been phased out in general communication but is still used in the networking applications.
- Fig. 5.2.1 shows the classification of switching methods.



(L-617) **Fig. 5.2.1 : Classification of switching methods**

5.3 Circuit Switching Networks :

I-Scheme : W-19

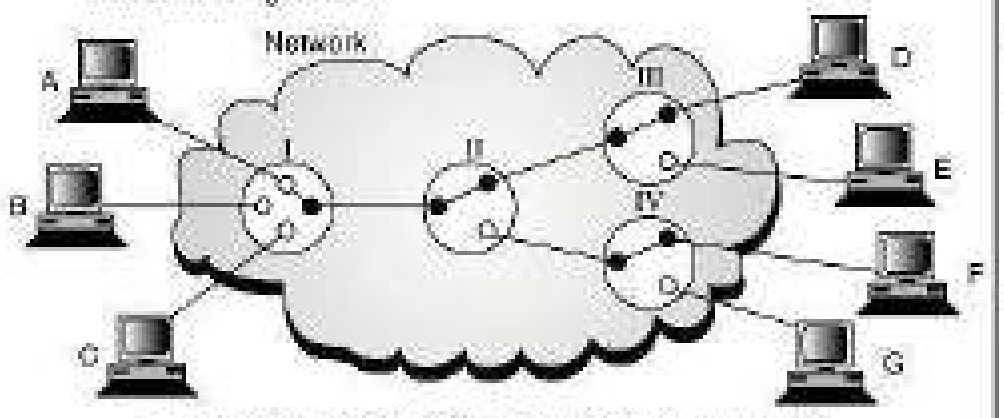
Concept :

- Circuit switching is a method of implementing a telecommunications network in which two network nodes establish a dedicated communication channel (Circuit) before the nodes communicate with each other.

Example :

- The simplest and the oldest telephone network is a circuit switched network.
- In a telephone network, when a call is made, from one telephone to the other, the switches within the telephone exchanges creates a continuous circuit (wired) between the two telephones as long as the call lasts.
- Circuit switching is used in public telephone networks. It was developed to handle voice traffic but it can also handle digital data.
- However circuit switching cannot handle digital data efficiently.
- Using the circuit switching, a dedicated path is established between two stations for communication.
- The telephone network provides telephone service which involves the two way, real-time transmission of voice signals across a network.
- The telephone networks are connection oriented because they require the setting up of a connection before the actual transfer of information can take place.
- It is also possible to use circuit switching for communication between computers.
- In circuit switching the routing decision is made when the path is set up across the network. After the link has been set between the sender and receiver, the information is forwarded continuously over the link.

- After the link has been set up no additional address information about the receiver or destination machine is required.
- In circuit switching a dedicated path is established between the sender and the receiver which is maintained for the entire duration of conversation, as shown in Fig. 5.3.1.



(L-618) **Fig. 5.3.1 : Circuit-switched network**

- If circuit switching is used in computer networks the sending machine has to first establishes a link with the receiving machine.
- After the link is established the data is transmitted from the sender to the receiver. After the data flow stops, the link is released (opened).

Block diagram :

- In Fig. 5.3.1, I, II, III and IV are called as the switching nodes. They are used to connect one user to the other.
- The circuit switched networks operate in three phases :
  1. Set up phase.
  2. Data transfer phase.
  3. Tear down phase.
- The circuit switching corresponds to the physical layer.
- Before starting communication in the setup phase the resources are reserved during communication. Some of these resources are channels, switch buffers, input/output ports etc.
- Data transferred between two stations is not in the packet form instead the data gets transferred continuously.
- No addressing is involved during the data transfer as the dedicated connection is established between the sender and receiver.
- The switches route the data on the basis of the allotted frequency band (FDM) or allotted time slot (TDM).

5.3.1 Three Phases :

- Communication via circuit switching takes place over three phases of operation as follows.
  1. Circuit establishment
  2. Data transfer
  3. Circuit disconnect (tear down)

1. Circuit establishment :

- In a circuit switching network, before any signal is transmitted, it is necessary to establish an end-to-end (station to station) link.
- For example, in Fig. 5.3.1, if the communication is to be between A and D, then the path from A to node I to node II to node III and D has to be established first.
- The node to node links are usually multiplexed. They either use FDM or TDM.

2. Data transfer :

- The information can now be transferred from A to D through the network.
- The data can be analog or digital depending on the nature of network.
- Generally all the internal connections are duplex.

3. Circuit disconnect (tear down phase) :

- After some time the connection between two users is terminated usually by the action of one or two stations.
- Circuit switching is inefficient in most of the applications.
- The entire channel capacity is dedicated for the duration of connection, even if the data is not being transferred.
- Once the circuit is established, the network is effectively transparent to the users with no delays involved.

5.3.2 Efficiency :

- In circuit switching the resources such as bandwidth are used as long as a connection is alive.
- Due to the allocation of resources during the entire duration of the connection, the efficiency of circuit switched networks is lower than the other two types of switching.

5.3.3 Delay :

- Eventhough the efficiency is low, the delay in this type of networks is very small.

5.3.4 Features :

– Some of the important feature of circuit switched networks are as follows :

1. Two nodes are connected to each other over a dedicated communication channel (circuit).
2. Switches are used to make or break the dedicated circuit.
3. Information or data is transferred continuously.
4. Circuit switching is preferred for voice communication.
5. No addressing needed during the data transfer phase.
6. Efficiency is low.
7. Delays are small.

Applications :

1. The circuit switching is used in the telephone networks.
2. For internet.

5.3.5 Advantages : I-Scheme : S-19

1. The major advantage of circuit switching is that the dedicated transmission channel the computers establish provides a guaranteed data rate.
2. In circuit switching because of the dedicated path there is no delay in data flow.

5.3.6 Disadvantages :

1. The disadvantage of circuit switching is that, since the connection is dedicated it cannot be used to transmit any other data even if the channel is free.
2. Dedicated channels require more bandwidth.
3. It takes long time to establish connection.

5.4 Packet Switching : I-Scheme : W-19

Definition :

– Packet switching is a method of switching in which the data (to be sent) is transmitted over a digital network in the form of **packets.**

Packet :

– A packet is made of two parts : header and payload or data as shown in Fig. 5.4.1.

(L-913) **Fig. 5.4.1 : A packet**

– The networking hardware uses the header contents to direct the packet to its destination.

– Packet switching is extensively used for data communication in computer networks.

Principle :

– In packet switching, messages are broken up into packets. Each packets has a header with source, destination and intermediate node address information.

– The other part of the packet includes data load.

– Individual packets can take different routes to reach the destination. Independent routing of packets gives two advantages :

1. Bandwidth is reduced due to splitting data onto different routes in a busy circuit.
2. If a certain link in the network goes down during the transmission, the remaining packets can be sent through another route.

– The packets can arrive out of order at the receiver and have to be reassembled in proper sequence.

– In packet switching, the packet length is restricted to a certain maximum length.

– This length is short enough to allow the switching devices to store the packet data in memory.

– There are two methods of packet switching :

1. Datagram packet switching.
2. Virtual circuit packet switching.

5.4.1 Datagram Packet Switching :

Principle :

– In this method a message is divided into a stream of packets.

– Each packet has its individually included address and treated as an independent unit with its own control instructors.

– The switching devices would route each packet independently through the network.

– Each intermediate node will determine the packet's next route segment.

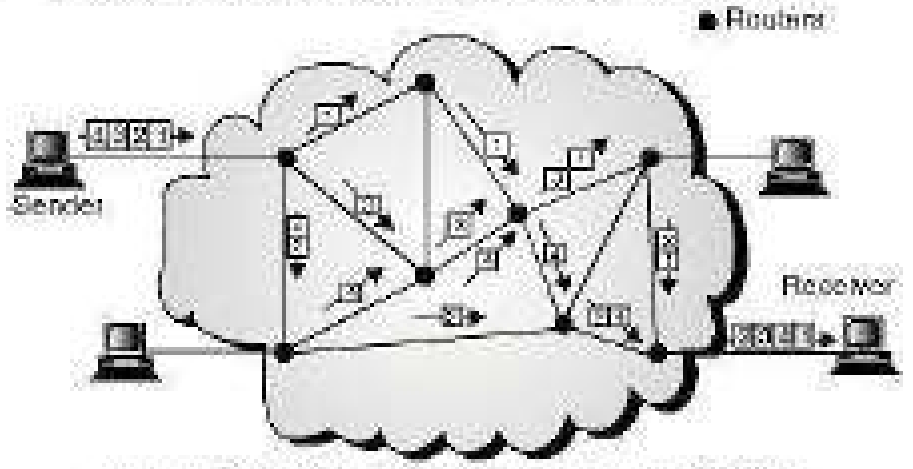
– Before transmission starts, the sequence of packets and their destinations are communicated by exchanging control information between the sending terminal, the network and the receiving terminal.

– In packet switching, the resources are not allocated for any packet so there is no reserved bandwidth and no scheduled processing time allotted for each packet.

- No dedicated connection is established between the sender and receiver.
- The resource allocation is on demand and on the first come first serve basis.
- When a switch receives a packet, it has to wait if there are any other packets being processed. This will increase the delay.
- The datagram packet switching generally corresponds to the network layer. The packet are called as **datagrams.**

Schematic diagram :

- Datagram packet switching is shown in Fig. 5.4.2.



(L-623) **Fig. 5.4.2 : Datagram packet switching**

- In this circuit, four packets are to be delivered from the sender to receiver. The switches in the datagram network are called as **routers.**
- All the four packets (datagrams) belong to the same message in this circuit however actually they can get originated from any computer.
- The four datagrams, as shown in Fig. 5.4.2 may travel different paths to reach the destination. Due to this the packets may arrive out of order at the destination.
- The delay associated with each packet will be different as a result of the different paths followed by them.
- The datagrams may get lost of dropped out due to lack of resources.
- The upper layer protocols are supposed to reorder the received datagrams or ask for the lost ones before passing them on the application.
- The datagram networks, are called as the **connectionless** networks.
- This is because the switch (packet switch) does not keep any information about the connection state.
- There are no connection set up or tear down processes in the packet switching networks.

5.4.2 Efficiency :

- As the resources are allocated only when the packets are to be transferred, the efficiency of datagram network is **higher** than that of the circuit switched network.

5.4.3 Delay :

- There are no set up or tear down phases in datagram circuit switching but each packet may have to wait at a switch before getting forwarded.
- All the packets in a message take different paths. Hence the delay associated with each packet is different.

5.4.4 Features of Packet Switching :

1. Message is broken into packets, and each packet follows its own path towards destination.
2. Needs less bandwidth.
3. If a link in the network is down, then the packets can be routed over an alternate route.
4. No dedicated connection is established between the sender and receiver.
5. The packets may arrive out of order at the destination and need to be arranged in sequence.
6. Efficiency is high.
7. Delay is longer than that in circuit switching.

5.4.5 Advantages of Packet Switching :

1. Greater line utilization efficiency, as a single node-to-node link can be dynamically shared by many packets over time.
2. A packet switching network can perform data-rate conversion.
3. When traffic become heavy on circuit switching network, some calls are blocked. On a packet switching network, packets are still accepted, but delivery delay increases.
4. Priorities can be used.
5. Each terminal in group sharing the same physical circuit may be connected to a totally different destination. This versatility is one of the major strengths of packet switching.
6. No single user or large data block can tie up circuit or node resources indefinitely, making it well suited for interactive traffic.

7. Data protection against corruption or loss, errors are corrected by retransmission.
8. Users can select different destinations for each virtual call, overcoming the inflexibility of point to point dedicated networks.
9. Simultaneous calls allow PC users to access multiple windows to different remote applications.
10. Since many users can share transmission resources efficiently, the cost of intermittent data communication is reduced.
11. New calls can be added and old ones disconnected without affecting other users.

5.4.6 Disadvantages of Packet Switching :

1. Delays are longer than those in circuit switching.
2. Header overhead reduces capacity to carry user data.
3. More processing is required at node.

5.4.7 Datagram Networks in Internet :

- The internet uses the datagram approach to switching at the Network layer.
- The routing of packets in Internet takes place on the basis of the universal addresses defined in the network layer.

5.5 Comparison of Circuit and Packet Switching :

I-Scheme : S-22

Parameter	Circuit switching	Packet switching
Application	Telephone network for bi-directional, real time transfer of voice signals.	Internet for datagram and reliable stream service between computers.
End terminal	Telephone, modem.	Computer
Information type	Analog voice or PCM digital voice	Binary information
Transmission system	Analog and digital data over different transmission media	Digital data over different transmission media.
Addressing scheme	Hierarchical numbering plan	Hierarchical address space
Routing scheme	Route selected during call setup.	Each packet is routed independently.
Multiplexing scheme	Circuit multiplexing.	Packet multiplexing shared media access networks.
Type of connection.	Dedicated channel (circuit) is established between the communicating parties.	No dedicated connection needed.
BW requirement	More	Less
Delay	Less	More
Efficiency	Less	More

Review Questions

Q. 1 Explain the term circuit switching. How is it different from the packet switching ?

Q. 2 Explain the three phases related to the communication via circuit switching.

Q. 3 Draw the neat diagram of circuit switching. Explain in brief.

Q. 4 Draw the neat diagram of packet switching. Explain in brief.

Q. 5 Compare between circuit switching and packet switching.

Q. 6 State the features of circuit switching.

Q. 7 State the advantages and drawbacks of packet switching.

Q. 8 What are the advantages and disadvantages of circuit switching ?

Q. 9 What is a packet ?

5.6 I-Scheme Questions and Answers :

Summer 2019 [Total Marks - 06]

Q. 1 Why is circuit switching preferred over packet switching in voice communication ? **(Section 5.3.5)** **(6 Marks)**

Winter 2019 [Total Marks - 04]

Q. 2 Explain circuit switching network with neat sketch. **(Section 5.3)** **(4 Marks)**

Q. 3 Describe the principles of packet switching and circuit switching techniques with neat diagram. **(Sections 5.3 and 5.4)** **(6 Marks)**

Summer 2022 [Total Marks - 04]

Q. 4 Compare packet switched and circuit switched network. **(Section 5.5)** **(4 Marks)**

❑❑❑

Chapter 6

Error Detection & Correction

Syllabus

Types of errors, Single bit error and burst error, Redundancy, Error Detection : Longitudinal redundancy check (LRC), Vertical redundancy check (VRC), Cyclic redundancy check (CRC), Forward error correction.

Chapter Contents

6.1 Errors and Their Effects :

W-14, S-16, W-17

MSBTE Questions

Q. 1 Define error. (S-16, 2 Marks)

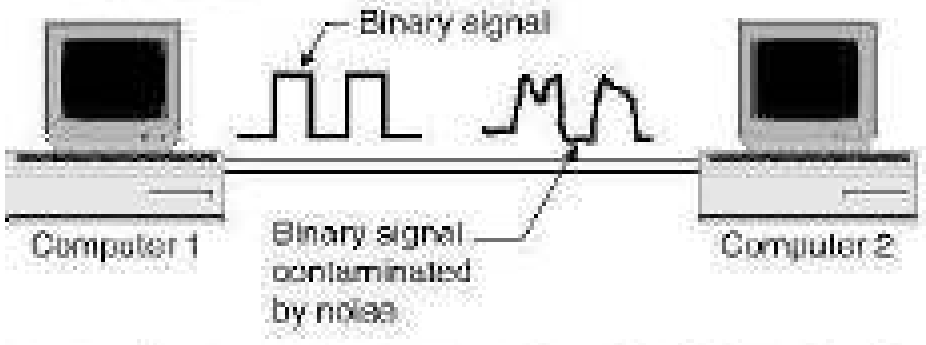
Q. 2 What is error ? Enlist different types of errors. (W-14, W-17, 2 Marks)

Definition of error :

- An error is defined as the measure of the difference between the observed or calculated value of a quantity and its true value.

Effects of errors :

- In the real time operating conditions, it is not possible to send a signal from source to destination without introducing any error.
- When transmission of digital signals takes place between two systems such as computers as shown in Fig. 6.1.1, the signal get contaminated due to the addition of "Noise" to it.



(L-302) **Fig. 6.1.1 : Noise contaminates the binary signal**

- The noise can introduce an error in the binary bits travelling from one system to the other.
- That means a 0 may change to 1 or a 1 may change to 0.
- These error can become a serious threat to the accuracy of the data. Therefore it is necessary to detect and correct the errors.

6.1.1 Need of Error Control Coding :

- In data communication, errors are introduced during the transmission of data from the transmitter to receiver due to noise or some other reasons.
- The reliability of data transmission will be severely affected due to these errors.
- In order to improve the reliability of data transmission, the designer will have to increase the signal power or reduce the noise spectral density N_o so as to maximize the ratio E_b / N_o.
- But practically there is a limitation on the maximum value of the ratio E_b / N_o. We cannot increase the ratio beyond this limit.
- **Hence for a fixed value of E_b / N_o, we have to use some kind of "coding" in order to improve the quality of the transmitted signal.**
- Another advantage of using coding is that we can reduce the required value of E_b / N_o if the error rate is predecided and remains fixed at that value.
- This will inturn reduce the required transmitted power and the size of antenna.

How to detect and correct errors ?

- For the detection and / or correction of these errors, one or more than one extra bits are added to the data bits at the time transmitting.
- These extra bits are called as parity bits. They allow the detection or sometimes correction of the errors.
- The data bits alongwith the parity bits form a code word.

6.1.2 Types of Errors :

W-09, S-10, W-10, W-11, S-13, W-14, W-15, W-16, W-17, I-Scheme : S-19, S-22

MSBTE Questions

Q. 1 Describe bit error and burst error with example. (W-09, 4 Marks)

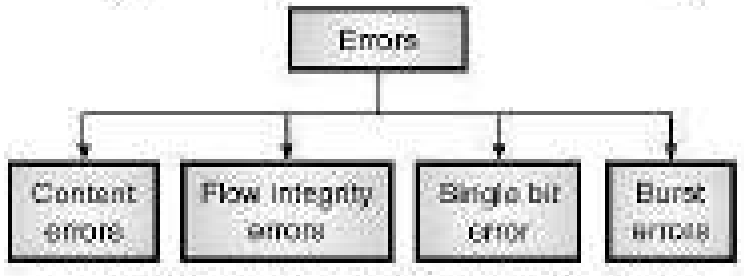
Q. 2 Explain different types of transmission errors. (S-10, S-13, W-15, W-16, 4 Marks)

Q. 3 Describe the term : Burst error. (W-10, 4 Marks)

Q. 4 Explain different types of error in data communication. (W-11, 4 Marks)

Q. 5 What is error ? Enlist different type of errors. (W-14, W-17, 2 Marks)

- Different types of errors have been listed in Fig. 6.1.2.



(L-911) **Fig. 6.1.2 : Classification of errors**

- The errors introduced in the data bits during their transmission can be categorised as :

1. Content errors.
2. Flow integrity errors.

1. Content error :

- The content errors are nothing but errors in the contents of a message e.g. a "0" may be received as "1" or vice versa.
- Such errors are introduced due to noise added into the data signal during its transmission.

2. Flow integrity error :

- Flow integrity errors means missing blocks of data. It is possible that a data block may be lost in the network possibly because it has been delivered to a wrong destination.
- Depending on the number of bits in error we can classify the errors into two types as :

  1. Single bit error 2. Burst errors.

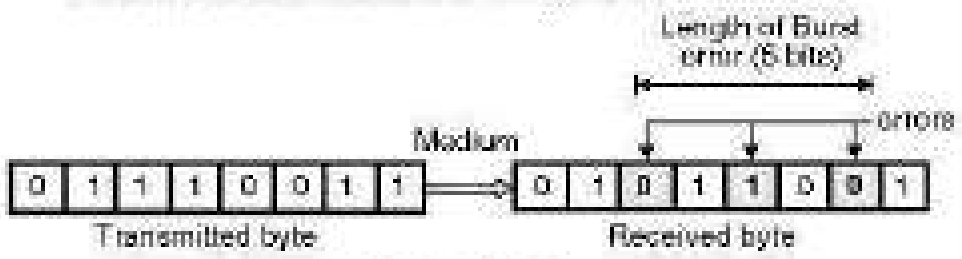
3. Single bit error :

- The term single bit error suggests that only one bit in the given data unit such as byte is in error.
- That means only one bit in a transmitted byte will change from 1 to 0 or 0 to 1, as shown in Fig. 6.1.3.

(G-188) **Fig. 6.1.3 : Single bit error**

4. Burst errors :

- If two or more bits from a data unit such as a byte change from 1 to 0 or from 0 to 1 then burst errors are said to have occurred.
- Refer Fig. 6.1.4 in which the shaded bits in the received byte have been the erroneous bits.
- These are 3 bits but the length of the burst is shown to be of 5 bits.
- The length of the burst error extends from the first erroneous bit to the last erroneous bit.
- Even though some of the bits in between have not been corrupted. The length of the burst error is shown to be 5 bits.
- Burst errors are illustrated in Fig. 6.1.4.



(G-189) **Fig. 6.1.4 : Burst errors**

Disadvantages of coding :

- Some of the disadvantages of the coding technique are :

1. An increased transmission bandwidth is required in order to transmit the encoded signal. This is due to the additional bits (redundancy) added by the encoder.
2. Use of coding make the system complex.

6.1.3 Redundancy :

Definition :

- Redundancy involves transmission of extra bits alongwith the data bits.
- These extra bits actually do not contain any data or information but they ensure the detection and correction of errors introduced during the data travel from sender to receiver.
- As these extra bits do not contain any information, they are known as **redundant bits.**
- The redundant bits are also known as **parity check** bits. They are produced from the data bits using some predecided rules.
- The data bits and redundant bits together form a code word as shown in Fig. 6.1.5.

(L-303) **Fig. 6.1.5 : Structure of a transmitted code word**

6.2 Detection Versus Correction :

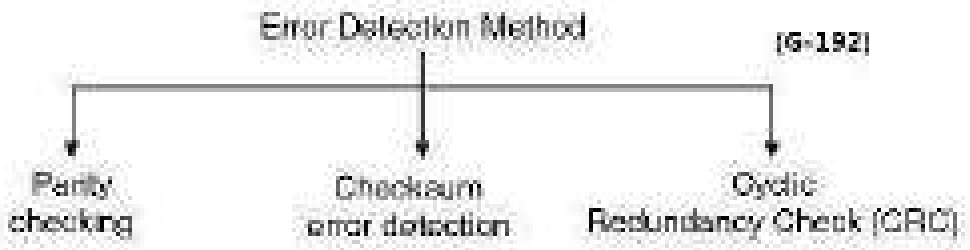
- Detection and correction of errors are the two most important aspects of error control in data communication.
- The correction of errors is more difficult as compared to their detection.
- The process of error detection is much easier because we have to simply find if error is present or absent in the received code word.
- In **error detection** we are even not interested in the number of errors.
- The only question to be answered is whether an error has occurred or not.
- In **error correction**, multiple processes are involved such as detecting the errors, knowing their number, the location of errors and then correcting the erroneous bits.

6.3 Error Detection :

- Error detection is a method or a process which is used by a receiver to find out whether an error is present in the received code word.
- Error detection does not involve correction of errors.
- A number of methods (techniques) are available now for the detection and correction of errors introduced in the transmitted signal.
- When a codeword is transmitted, one or more number of transmitted bits will be reversed (0 to 1 or vice versa) due to transmission impairments.

Error detection techniques :

- Some of the most important error detection methods are as follows :

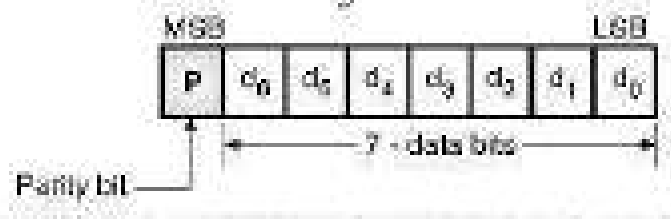


- Before thinking of correcting the errors introduced in the data bits it is necessary to first detect them.
- Some of the popular error detection methods are as follows :
  1. Parity checking.
  2. Checksum error detection.
  3. Cyclic Redundancy Check (CRC).

6.3.1 Parity Checking :

Definition of parity bit :

- A parity bit or a check bit is a bit added to a string of binary bits to ensure that the total number of 1-bit in the string including the parity bit is either even or add.
- The simplest technique for detecting errors is to add an extra bit known as **parity bit** to each word being transmitted.
- As shown in Fig. 6.3.1, generally the MSB of an 8-bit word is used as the parity bit and the remaining 7 bits are used as data or message bits.

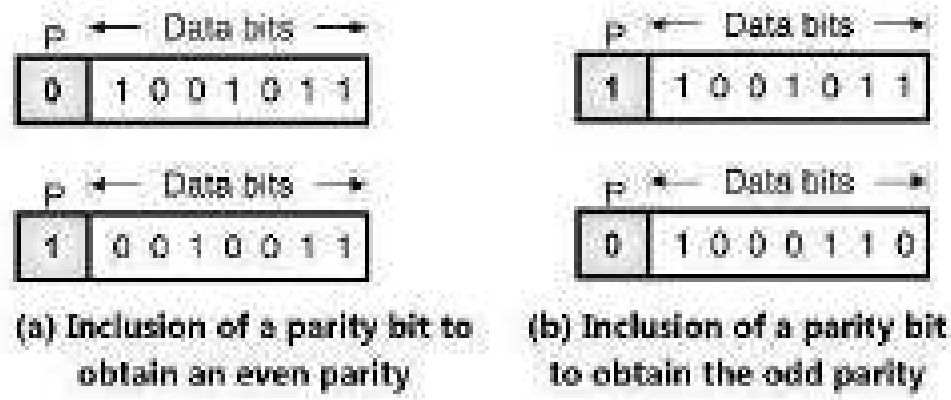


(L-309) **Fig. 6.3.1 : Format of a transmitted word with parity bit**

- The parity of the 8-bit transmitted word can be either even parity or odd parity.
- Even parity means the number of 1's in the given word including the parity bit should be even (2, 4, 6...).
- Odd parity means the number of 1's in the given word including the parity bit should be odd (1, 3, 5...).

Use of Parity Bit to Decide Parity :

- The parity bit can be set to 0 or 1 depending on the type of parity required.
- For odd parity this bit is set to 1 or 0 at the transmitter such that the number of "1 bits" in the entire word is odd.

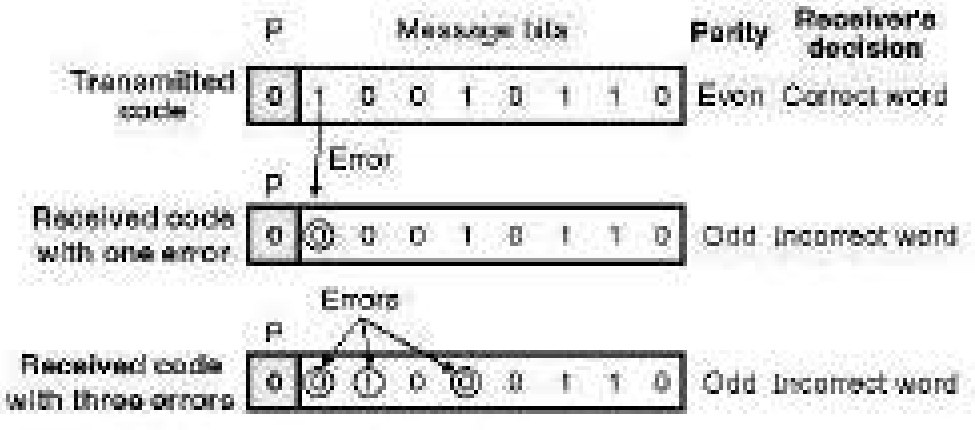


(a) Inclusion of a parity bit to obtain an even parity **(b) Inclusion of a parity bit to obtain the odd parity**

(L-310) **Fig. 6.3.2**

How does error detection take place ?

- The parity checking at the receiver can detect the presence of an error if the parity of the received signal is different from the expected parity.
- That means if it is known that the parity of the transmitted signal is always going to be "even" and if the received signal has an odd parity then the receiver can conclude that the received signal is not correct.
- This is as shown in Fig. 6.3.3.



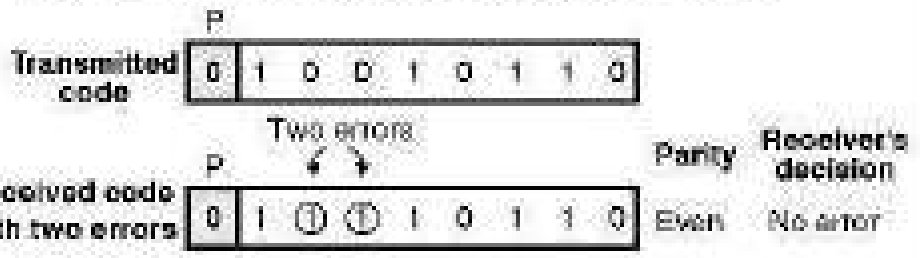
(L-311) **Fig. 6.3.3 : The receiver detects the presence of error if the number of errors is odd i.e. 1, 3, 5 ....**

- If a single error or an odd number of bits change due to errors introduced during transmission the parity of the code word will change.
- Parity of the received code word is checked at the receiver and if there is change in parity then it is understood that error is present in the received word. This is as shown in Fig. 6.3.3.

- If presence of error is detected then the receiver will ignore the received byte and request for the retransmission of the same byte to the transmitter.

When does parity checking fail to detect errors ?

- If the number of errors introduced in the transmitted code is two or any even number, then the parity of the received code word will not change.
- It will still remain even as shown in Fig. 6.3.4 and the receiver will fail to detect the presence of errors.



(L-312) **Fig. 6.3.4 : The receiver cannot detect the presence of error if the number of errors is even i.e. 2, 4, 6 ....**

Conclusions :

1. Double or any even number of errors in the received word will not change the parity. Therefore even number of errors will be unnoticed.
2. If one or odd number of errors occur then the parity of the received word will be different from the parity of transmitted signal. Thus error is noticed. However this error can neither be located nor be corrected.

Limitations of parity checking :

1. Thus the simple parity checking method has its limitations. It is not suitable for detection of multiple errors (two, four, six etc).
2. The other limitation of parity checking method is that it cannot reveal the location of erroneous bit. It cannot correct the error either.

6.3.2 Two Dimensional Parity Check (Block Parity) :

I-Scheme : S-22

Block of Data :

- When a large number of binary words are being transmitted or received in succession, the resulting collection of bits is considered as a **block of data,** with rows and columns as shown in Fig. 6.3.5.

LRC and VRC Bits :

- The parity bits are produced for each row and column of such block of data.

Characters		C	O	M	P	U	T	E	R	
7 bit ASCII codes (Message bits)	b_1	1	1	1	0	1	0	1	0	1
	b_2	1	1	0	0	0	0	0	1	1
	b_3	0	1	1	0	1	1	1	0	1
	b_4	0	1	1	0	0	0	0	0	0
	b_5	0	0	0	1	1	1	0	1	0
VRC bits (even parity)	b_6	0	0	0	0	0	0	0	0	0
	b_7	1	1	1	1	1	1	1	1	0
	→	1	1	0	0	0	1	1	1	1

These bits will make the parity of each column even

These bits will make the parity of each row even ← LRC bits (even parity)

(L-313) **Fig. 6.3.5 : Vertical and longitudinal parity check bits**

- The two sets of parity bits so generated are known as :
  1. Longitudinal Redundancy Check (LRC) bits.
  2. Vertical Redundancy Check (VRC) bits.
- The LRC bits indicate the parity of rows and VRC bits indicate the parity of columns as shown in Fig. 6.3.5.

The Vertical Redundancy Check (VRC) Bits :

- As shown in Fig. 6.3.5 the VRC bits are parity bits associated with the ASCII code of each character.
- Each VRC bit will make the parity of its corresponding column **"an even parity"**.
- For example consider column 1 corresponding to character "C". The ASCII code for the character C is, as follows :

Character	C	
b_1	1	
b_2	1	← Column - 1 of the data block
b_3	0	
b_4	0	
b_5	0	
b_6	0	
b_7	1	
VRC bit →	1	← VRC bit = 1 to make the parity of first column even

(S-1944)

- Therefore the 8^{th} bit which is a VRC bit is made "1" to make the parity even.
- Similarly the other VRC bits are found as shown in Fig. 6.3.5.

The Longitudinal Redundancy Check (LRC) Bits :

- The LRC bits are parity bits associated with the rows of the data block of Fig. 6.3.5. Each LRC bit will make the parity of the corresponding row, **an even parity.** For example, consider row 1 of Fig. 6.3.5.

(G-1945)

Row 1 : | b_1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | ← LRC bit to make parity even

How to locate the erroneous bit ?

- Even a single error in any bit will result in a noncorrect "LRC" in one of the rows and an incorrect VRC in one of the columns.
- The bit which is common to the row and column is the erroneous bit.
- However there is still a limitation on the Block parity code, which is that, multiple errors in rows and columns can be only detected but they cannot be corrected.
- This is because, it is not possible to locate the bits which are in error. This will be clear when you will solve the following example.

Ex. 6.3.1 : The following bit stream is encoded using VRC, LRC and even parity. Locate and correct the error if it is present.

1 1 0 0 0 0 1 1 1 1 1 1 0 0 1 1

1 0 1 1 0 0 1 0 0 0 0 1 0 1 0

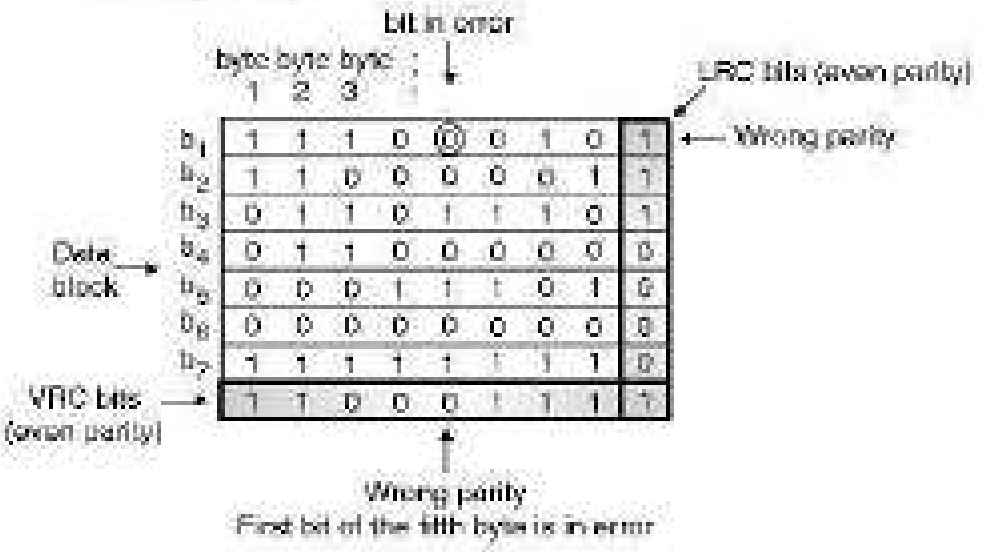
0 0 1 0 1 0 1 0 0 0 1 0 1 0 1 1

1 0 1 0 0 0 1 1 0 1 0 0 1 0 1 1

1 1 1 0 0 0 0 1 I-Schems : S-22

Soln. :

1. Fig. P. 6.3.1 shows the received data block alongwith the LRC and VRC bits.



(L-315(a)) **Fig. P. 6.3.1**

2. Note the parity bits corresponding to row 1 and column 5 indicate wrong parity. Therefore the fifth bit in the first row (encircled bit) is incorrect.
- Thus using VRC and LRC, it is possible to locate and correct the bits in error.

6.4 Cyclic Redundancy Check (CRC) :

Definition :

- CRC is an error detection code which is included in each transmitted codeword as showing Fig. 6.4.1 and used by the receiver to detect the errors in the received codeword.

(L-912) **Fig. 6.4.1 : Structure of transmitted codeword using CRC**

- This is a type of polynomial code in which a bit string is represented in the form of polynomials with coefficients of 0 and 1 only.
- Polynomial arithmetic uses a modulo-2 arithmetic i.e. addition and subtraction are identical to EXOR.
- For CRC code the sender and receiver should agree upon a generator polynomial G(x).
- A codeword can be generated for a given dataword (message) polynomial M(x) with the help of long division.
- This technique is more powerful than the parity check and checksum error detection.

Procedure of error detection :

- CRC works on the principle of binary division. A sequence of redundant bits called CRC or CRC remainder is appended at the end of the message.
- We will call this word as appended message word.
- The appended word thus obtained becomes exactly divisible by the generator word corresponding to G (x).
- The sender appends the CRC to the message word to form a codeword.
- At the receiver, this codeword is divided by the same generator word which corresponds to G (x).
- There is no error if the remainder of this division is zero. But a non-zero remainder indicates presence of errors in the received code word.
- Such an erroneous code word is then rejected.

6.4.1 Procedure to Obtain CRC :

- The redundancy bits used by CRC are derived by following the procedure given below :

1. Divide the data unit by a predetermined divisor.
2. Obtain the remainder. It is the CRC.

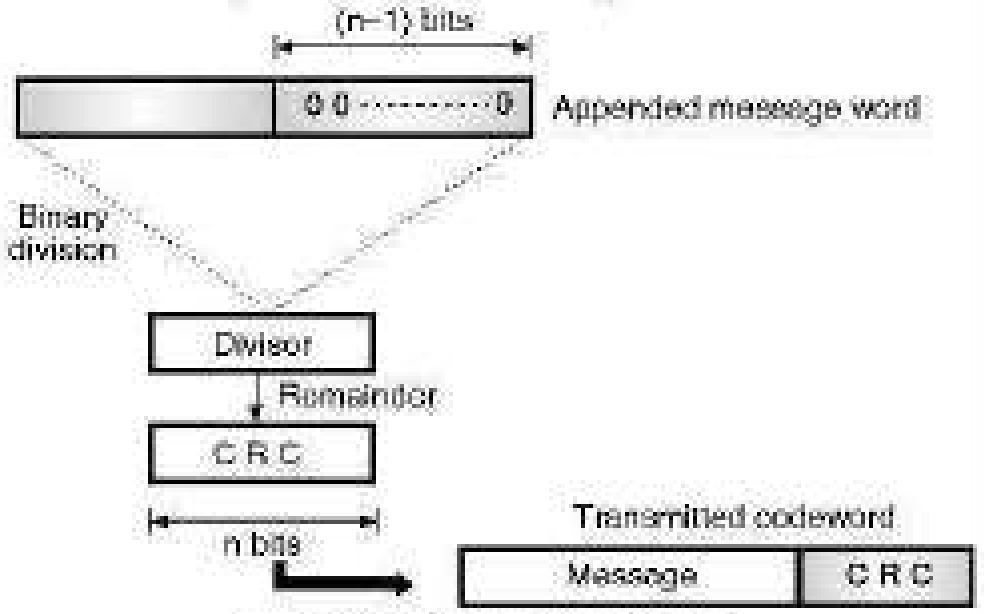
6.4.2 Requirements of CRC :

– A CRC will be valid if and only if it satisfies the following requirements :

1. The number of bits in CRC should be one less than the number of bits in the divisor.
2. After we append the CRC at the end of the data unit should result in the bit sequence which is exactly divisible by the divisor.

6.4.3 CRC Generator :

– The CRC generator is shown in Fig. 6.4.2.



(L-819) **Fig. 6.4.2 : CRC generator**

– The stepwise procedure in CRC generation is as follows :

Step 1 : Append a train of (n – 1) 0s to the message word where (n – 1) is 1 less than the number of bits in the predecided divisor (i.e. generator word) i.e. n. If the divisor is 5-bit long then we have to append 4-zeros to the message.

Step 2 : Divide the newly generated data unit in step 1 by the divisor (generator). This is a binary division.

Step 3 : The remainder obtained after the division in step 2 is the n bit CRC.

Step 4 : This CRC will replace the n 0s appended to the data unit in step 1, to get the codeword to be transmitted as shown in Fig. 6.4.2.

Ex. 6.4.1 : Generate the CRC code for the data word of 1 1 0 0 1 0 1 0 1. The divisor is 1 0 1 0 1.

Soln. :

Given : Data word : 1 1 0 0 1 0 1 0 1

Divisor : 1 0 1 0 1.

The number of data bits = m = 9

The number of bits in the divisor = n = 5

Dividend = Data word + (n – 1) zeros.

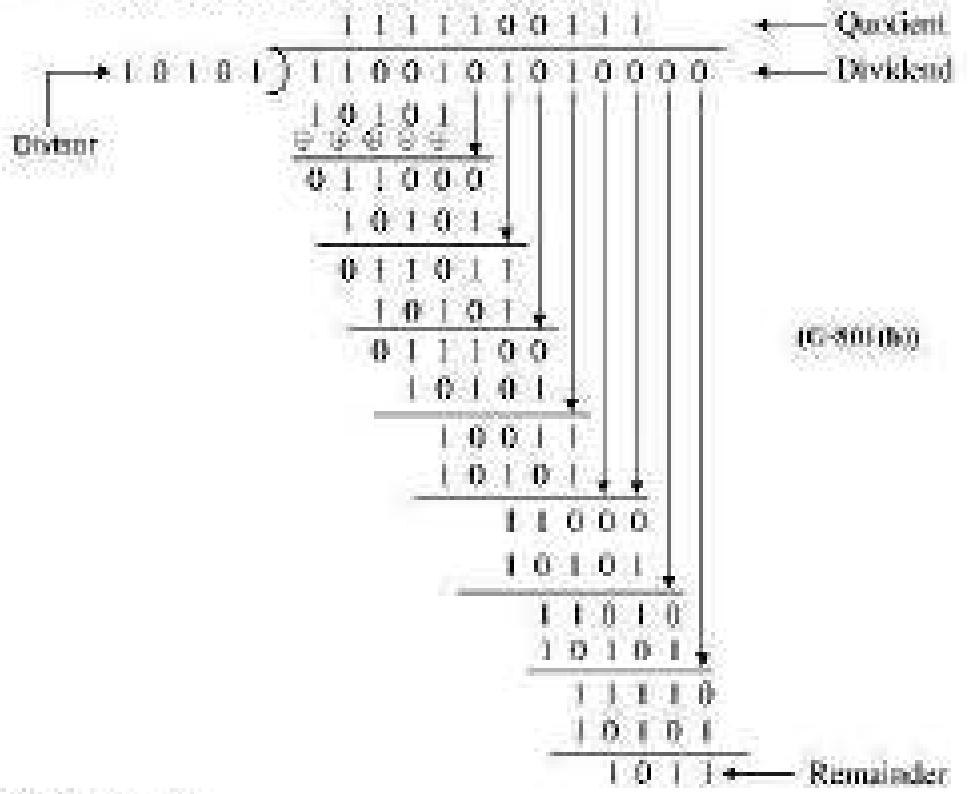
Dividend = 1 1 0 0 1 0 1 0 1 | 0 0 0 0

Data word — 4 additional zeros

(G-801(a))

Division :

– Carry out the division as follows :



(G-801(b))

Codeword :

– In CRC the required codeword is obtained by writing the data word followed by the remainder.

∴ 1 1 0 0 1 0 1 0 1 0 0 0 0 Dividend

\+ 1 0 1 1 Remainder

1 1 0 0 1 0 1 0 1 1 0 1 1 Codeword (G-2290)

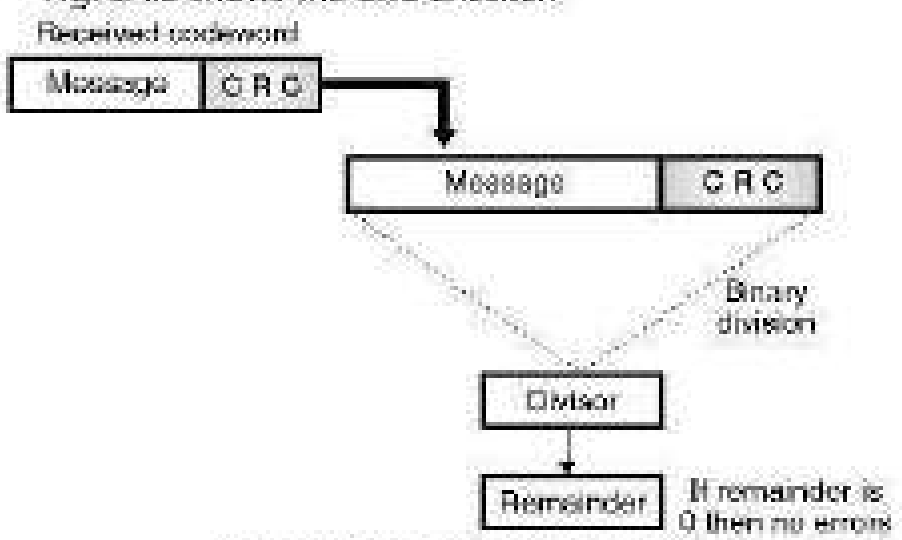
∴ Codeword = 1 1 0 0 1 0 1 0 1 | 1 0 1 1

Data word — Remainder or CRC

(G-1761)

6.4.4 CRC Checker and Detection of Error :

– Fig. 6.4.3 shows the CRC checker.



(L-820) **Fig. 6.4.3 : CRC checker**

- The codeword received at the receiver consists of message and CRC. (Fig. 6.4.3)
- The receiver treats it as one unit and divides it by the same (n) bit divisor (generator word) which was used at the transmitter.
- The remainder of this division is then checked.

Detection of error :

- If the remainder is zero, then the received codeword is error free and hence should be accepted.
- But a non-zero remainder indicates presence of errors hence the corresponding codeword should be rejected.

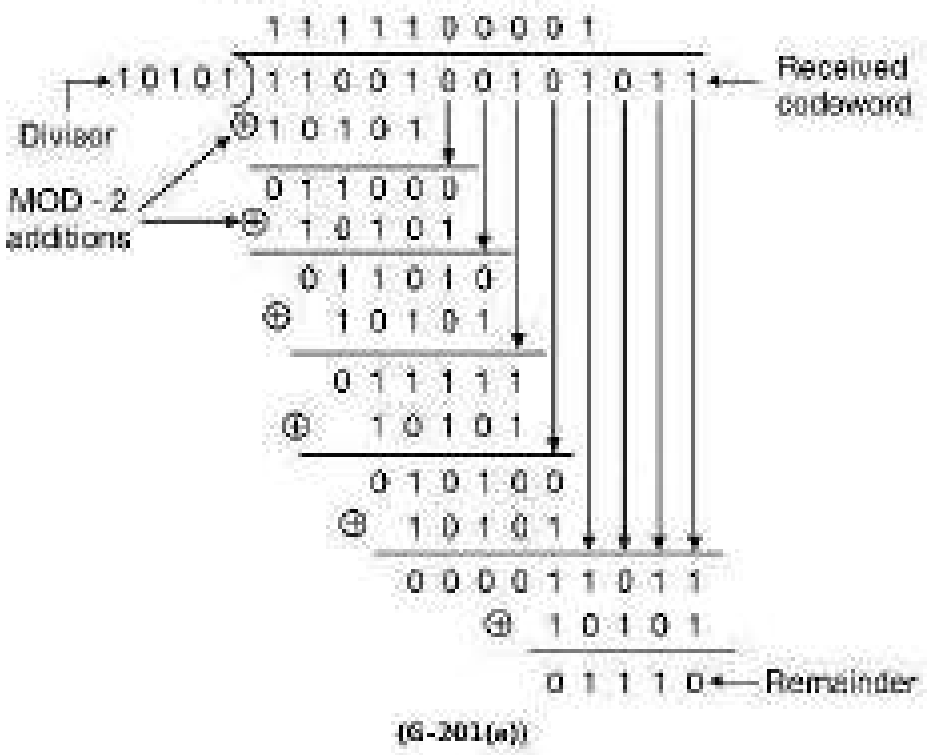
Ex. 6.4.2 : The codeword is received as 1100 1001 01011. Check whether there are errors in the received codeword, if the divisor is 10101. (The divisor corresponds to the generator polynomial).

Soln. :

- As we know the codeword is formed by adding the dividend and the remainder.
- This codeword will have an important property that it will be completely divisible by the divisor.
- Thus at the receiver we have to divide the received codeword by, the same divisor and check for the remainder.
- If there is no remainder then there are no errors.
- But if there is remainder after division, then there are errors in the received codeword.
- Let us use this technique and find if there are errors.

Data word : 1100 1001 01011

Divisor : 10101



(G-201(a))

Conclusion :

- The non zero remainder shows that there are errors in the received codeword.

Ex. 6.4.3 : Calculate CRC for the frame 110101011 and the generator polynomial = $x^4 + x + 1$ and write the transmitted frame.

Soln. :

- The generator polynomial actually acts as the divisor in the process of CRC generation.

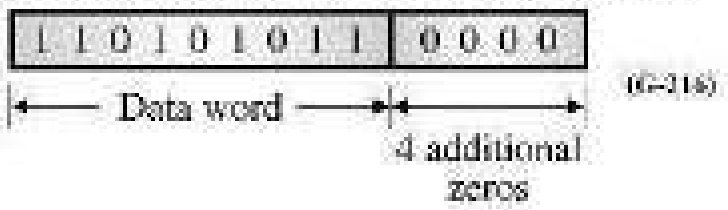
∴ Data word : 110101011

Divisor : $x^4 + 0x^3 + 0x^2 + x + 1 = 10011$

The number of data bits = m = 9

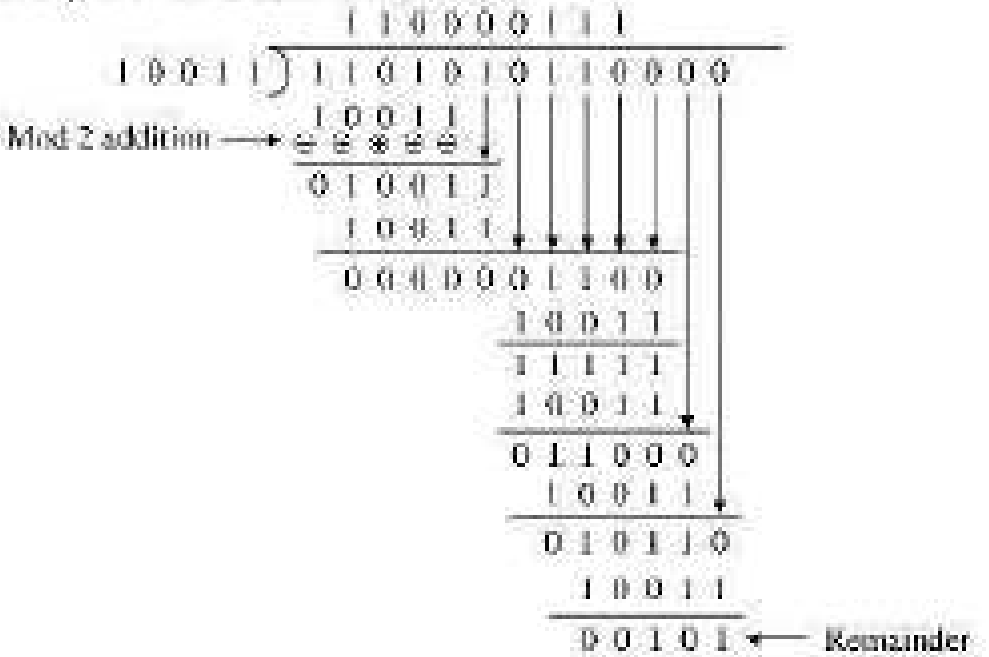
The number of bit in the divisor = N = 5

Dividend = Data word + (N – 1) number of zeros.



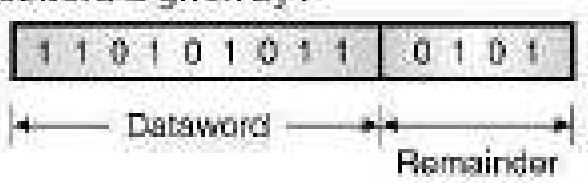
(G-218)

Carry out the division as follows :



(G-216(a))

Codeword : The codeword is given by :



(G-216(b))

Ex. 6.4.4 : What is the remainder obtained by dividing $x^7 + x^5 + 1$ by the generator polynomial $x^3 + 1$?

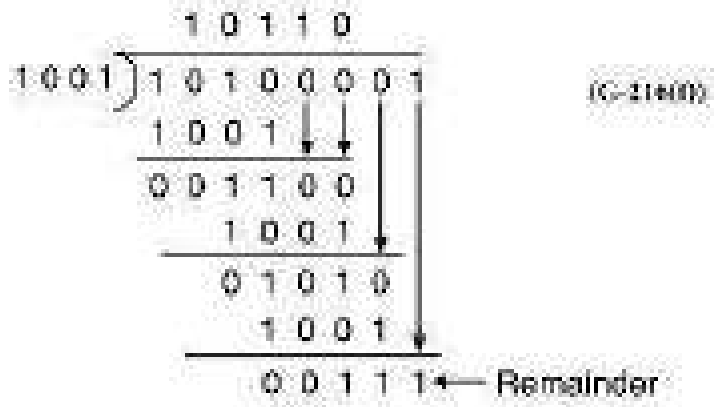
Soln. :

Given : Dividend : $x^7 + x^5 + 1 = x^7 + 0x^6 + x^5 + 0x^4 + 0x^3 + 0x^2 + 0x + 1$

$= 10100001$

Divisor : $x^3 + 1 = x^3 + 0x^2 + 0x + 1 = 1001$

The long division is as follows :



(G-2168)

The remainder is 00111 = $x^2 + x + 1$ in the polynomial form.

Ex. 6.4.5 : A bit stream 10011101 is transmitted using the standard CRC method. The generator polynomial is $x^3 + 1$. Show the actual bit string transmitted. Suppose the third bit from left is inverted during transmission. Show that this error is detected at the receiver's end.

Soln. :

Given : Data word (Bit string) : 1 0 0 1 1 1 0 1

Generator polynomial : $x^3 + 1 = x^3 + 0x^2 + 0x + 1$

= 1 0 0 1 = n

Obtain transmitted codeword :

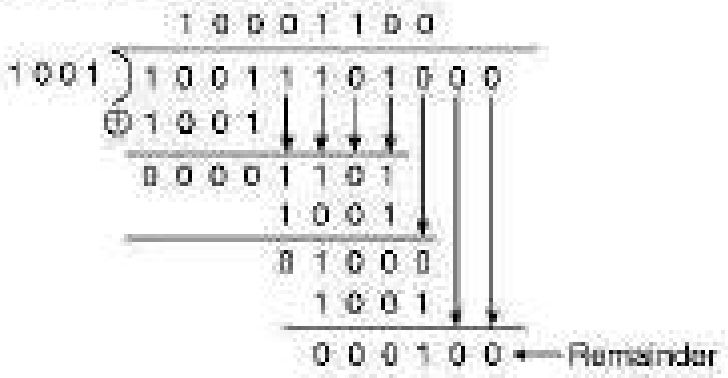
Step 1 : Obtain the dividend :

Dividend = Data word + 3 zeros.

The dividend is as follows :

(G-216(g))

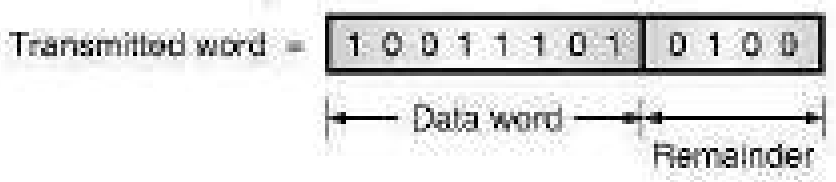
Step 2 : Carry out the division :



(G-216(h))

Step 3 : Obtain the actually transmitted bit stream :

– The transmitted word is obtained by writing the data word followed by the remainder as follows :



(G-216(i))

Error detection :

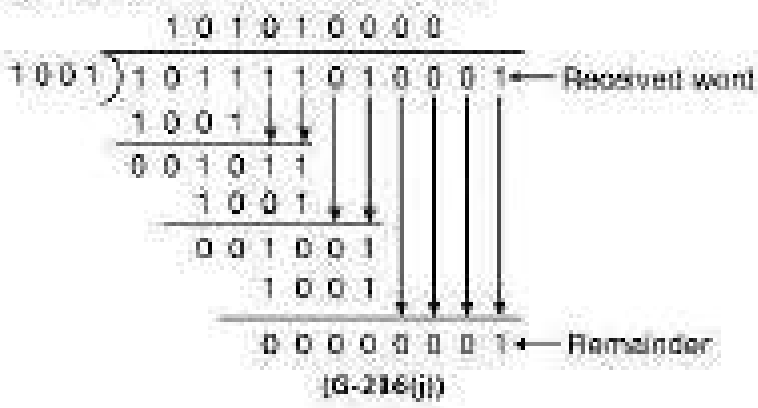
Step 4 : Write the erroneous received word :

The received word = 1 0 (1) 1 1 1 0 1 0 0 0 1

↑ Error

(G-1982)

– At the receiver, this word is divided by the same divider used at the transmitter i.e. 1001.



(G-216(j))

– A non zero remainder indicates that there is an error in the received codeword.

Ex. 6.4.6 : Generate the CRC code for message 1101010101. Given generator polynomial, $g(x) = x^4 + x^2 + 1$.

Soln. :

Message = 1101010101

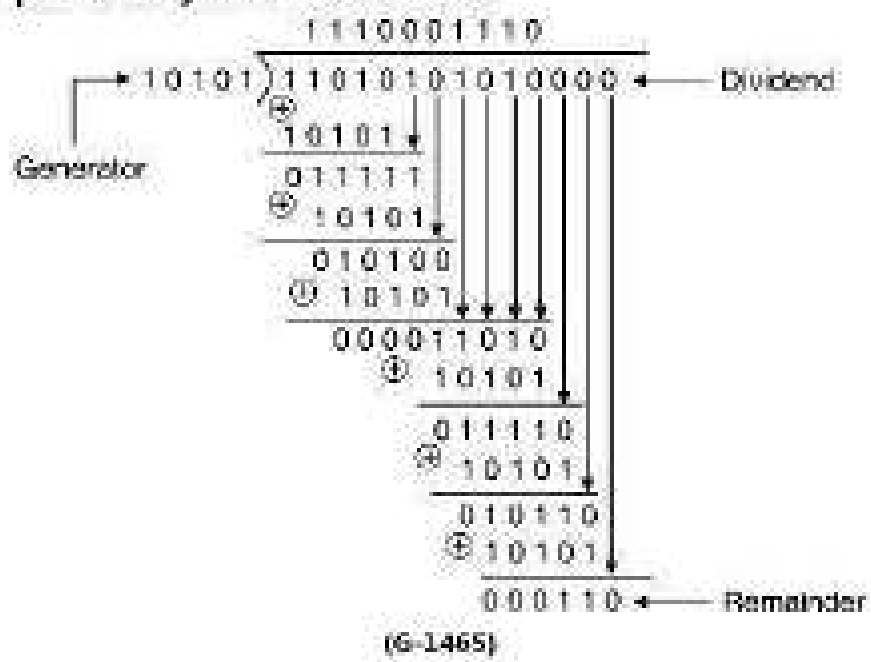
Generator = $x^4 + x^2 + 1 = x^4 + 0x^3 + x^2 + 0x + 1$

= 1 0 1 0 1

Step 1 : Obtain the dividend :

(G-1464)

Step 2 : Carry out the division :



(G-1465)

Step 3 : Transmitted code word :

(G-2319)

Dividend : 1 1 0 1 0 1 0 1 0 1 0 0 0 0

Remainder : + 0 1 1 0

Transmitted codeword : 1 1 0 1 0 1 0 1 0 1 0 1 1 0

6.5 Forward Error Correction (FEC) Versus Retransmission :

- The two most important techniques used for error correction are as follows :
  1. Forward Error Correction (FEC).
  2. Automatic request for retransmission (ARQ).

The ARQ technique :

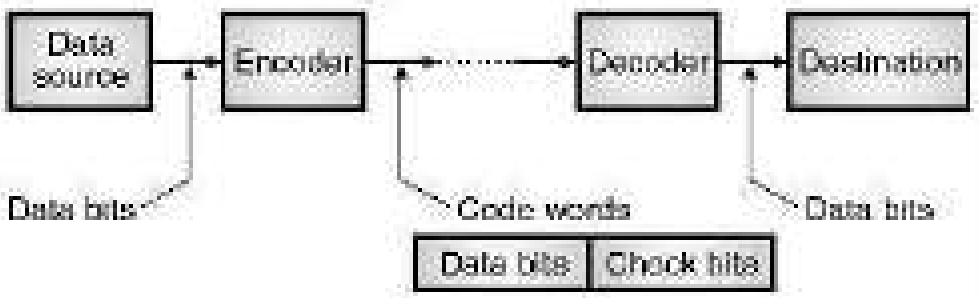
- In the ARQ system, the receiver can request for the retransmission of the complete or a part of message if it finds some error in the received message.
- This needs an additional channel called feedback channel to send the receiver's request for retransmission.

The FEC technique :

- In the FEC technique there is no such feedback path and request for retransmission. So error correction has to take place at the receiver.
- In this technique, the receiver tries to guess the transmitted message with the help of the redundant bits (parity bits or code bits).
- This technique is useful only when the number of errors is small.

6.5.1 Error Correction Techniques :

- In the error correction techniques, codes are generated at transmitter by adding a group of parity bits or check bits as shown in Fig. 6.5.1.

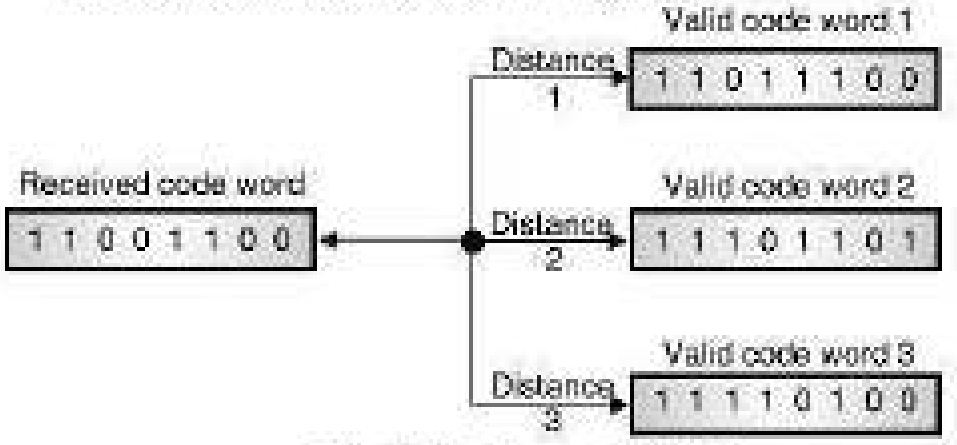


(L-306) **Fig. 6.5.1 : Error correction technique**

- The source generates the data (message) in the form of binary symbols.
- The encoder accepts these bits and adds the check (parity) bits to them to produce the code words.
- These code words are transmitted towards the receiver. The check bits are used by the decoder to detect and correct the errors.
- The encoder of Fig. 6.5.1, adds the check bits to the data bits, **according to a prescribed rule.**
- This rule will be dependent on the type of code being used.
- The decoder separates out the data and check bits. It uses the parity bits to detect and correct errors if they are present in the received code words.
- The data bits are then passed on to the destination.

6.5.2 FEC (Forward Error Correction) :

- In FEC the receiver searches for the most likely correct code word.
- When an error is detected, the distance between the received invalid code word and all the possible valid code word is obtained.
- The nearest valid code word (the one having minimum distance) is the most likely the correct version of the received code word as shown in Fig. 6.5.2.



(L-307) **Fig. 6.5.2 : Concept of FEC**

- In Fig. 6.5.2, the valid code word 1 has the minimum distance (1), hence it is the most likely correct code word.

6.5.3 Retransmission :

- In this technique, the receiver detects the presence of errors in the received code word and requests the sender to resend that code word (message) again.
- Retransmission is repeated until the received message is error free.

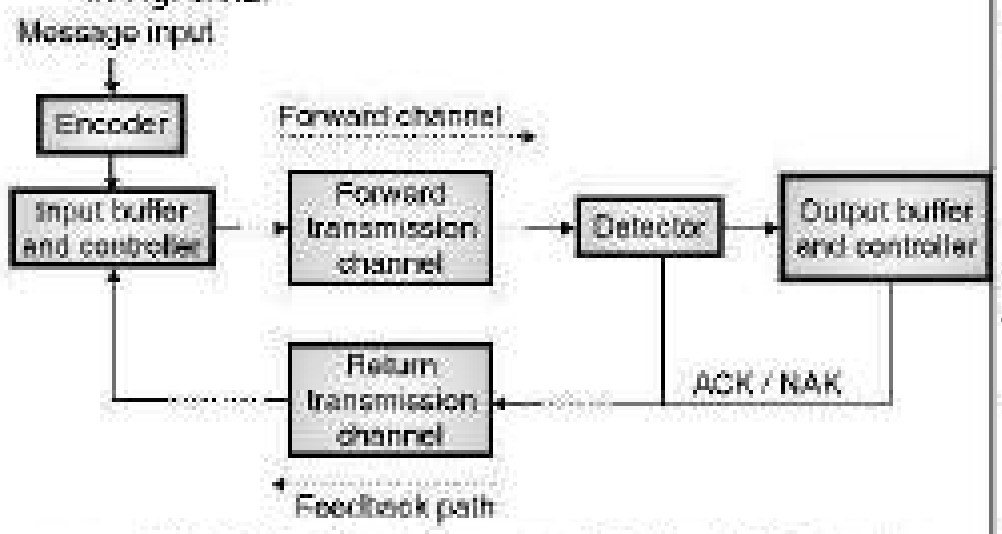
6.6 ARQ Technique (Retransmission) :

- There are two basic systems of error detection and correction.
- The first on being the Forward Error Correction (FEC) system and the second one is the automatic repeat request (ARQ) system.
- In the ARQ system of error control, when an error is detected, the receiver makes a request for the retransmission of that signal. Therefore a feedback channel is required for sending the request for retransmission.

- The ARQ systems differ from the FEC systems in three important aspects. They are as follows :
  1. In ARQ system less number of check bits (parity bits) are required to be sent. This will increase the (k/n) ratio for an (n, k) block code if transmitted using the ARQ system.
  2. A return transmission path and additional hardware in order to implement repeat transmission of codewords will be needed.
  3. The bit rate of forward transmission must make allowance for the backward repeat transmission.

Basic ARQ system :

- The block diagram of the basic ARQ system is as shown in Fig. 6.6.1.



(A-572) **Fig. 6.6.1 : Block diagram of the basic ARQ system**

Operation of ARQ system :

- The encoder produces codewords for each message signal at its input.
- Each codeword at the encoder output is stored temporarily and transmitted over the forward transmission channel.
- At the destination a decoder will decode the code words and search for errors.
- The decoder will send a "positive acknowledgment" (ACK) if no errors are detected and it will output a negative acknowledgment (NAK) if errors are detected, to the transmitter on the return transmission channel.
- On receiving a negative acknowledgment (NAK) signal via the return transmission path the "controller" will retransmit the appropriate word from the words stored by the input buffer.
- A particular word may be retransmitted only once or it may be retransmitted twice or more number of times.
- The output controller and buffer on the receiver side assemble the output bit stream from the code words accepted by the decoder.

Error probability on the return path :

- The bit rate of the return transmission which involves the return transmission of ACK/NAK signal is low as compared to the bit rate of the forward transmission.
- Therefore the error probability of the return transmission is negligibly small.

Types of ARQ system :

The three types of ARQ systems are :

1. Stop-and-wait ARQ system.
2. Go back n ARQ.
3. Selective repeat ARQ.

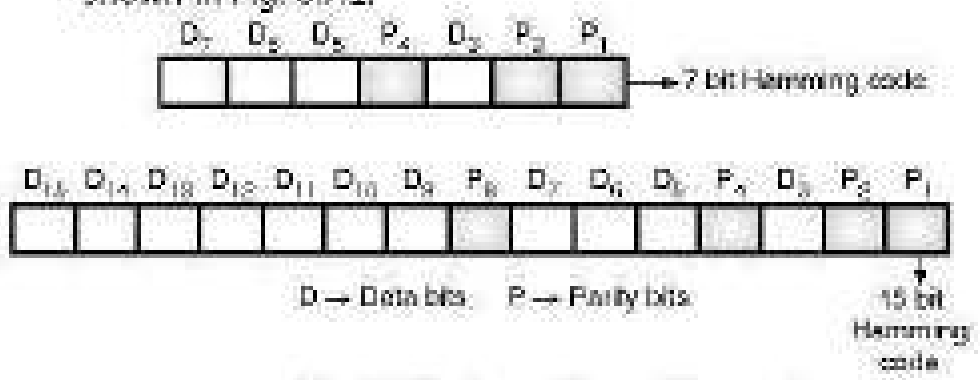
> **Note :** Error control in the data link layer is based on the principle of request for automatic retransmission (ARQ) of the missing, lost or damaged frames.

6.7 Hamming Codes :

- Now let us discuss the other category of codes i.e. the error correcting codes known as the Hamming codes.
- Hamming codes are a family of linear error correcting codes.
- They can detect upto two bit errors and correct one bit error without detection of uncorrected errors.

6.7.1 Hamming Code Structure :

- Hamming code is basically a linear block code named after its inventor. It is an error correcting code.
- The parity bits are inserted in between the data bits as shown in Fig. 6.7.1.



(G-1946) **Fig. 6.7.1 : Hamming code words**

- The 7-bit Hamming code is used commonly, but the concept can be extended to any number of bits.
- Note that the parity bits are inserted at each 2^n bit where n = 0, 1, 2, 3 .....

– Thus P_1 is at $2^0 = 1$, i.e. at first bit, P_2 is at $2^1 = 2$ P_4 is as 2^2 and P_8 is at 2^3 as shown in Fig. 6.7.1.

7-Bit Hamming Code :

1. A scientist named R.W. Hamming developed a coding system which was easy to implement. Assuming that four data bits are to be transmitted, he suggested a code word pattern shown in Fig. 6.7.2.

(6-1947) **Fig. 6.7.2 : Code word pattern for Hamming code**

2. The D bits in Fig. 6.7.2 are data bits, whereas P bits are parity bits. The parity bits P_1, P_2, P_4 are adjusted in a particular way as explained below.

Minimum number of parity bits :

– Table 6.7.1(a) gives a listing of minimum number of parity bits needed for various ranges of "m" information bits.

Table 6.7.1(a) : Number of parity bits to be used

Number of information bits	Number of parity bits
2 to 4	3
5 to 11	4
12 to 26	5
27 to 57	6
58 to 120	7

Deciding the values of parity bits :

– Table 6.7.1(b) indicates which bit positions are associated with each parity bit in order to establish required parity (even or odd) over the selected bits positions.

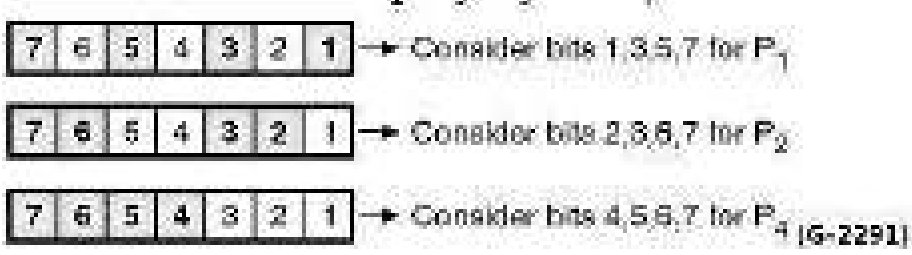
Table 6.7.1(b)

Parity Bit	Bits to be checked
P_1	1,3,5,7,9,11,13,15,.....
P_2	2,3,6,7,10,11,14,15, ...
P_4	4,5,6,7,12,13,14,15, ...
P_8	8,9,10,11,12,13,14,15, ...

6.7.2 Deciding the Parity Bits :

Selection of P_1 :

– P_1 is adjusted to 0 or 1 so as to establish even parity over bits 1, 3, 5 and 7 i.e. P_1, D_3, D_5 and D_7.



(6-2291)

Selection of P_2 :

– P_2 is adjusted to 0 or 1 so as to set even parity over bits 2, 3, 6 and 7 (P_2, D_3, D_6 and D_7).

Selection of P_4 :

– P_4 is adjusted to 0 or 1 so as to set even parity over bits 4, 5, 6 and 7 (P_4, D_5, D_6 and D_7).

Generation of a Hamming Code :

– Once we decide the values of the parity bits, we can generate a Hamming code word.

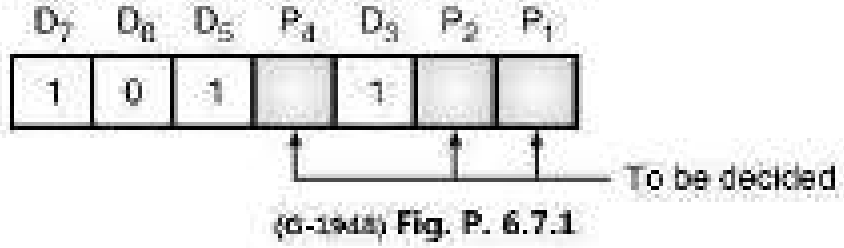
– The codeword generation will be clear by referring to the following example.

Ex. 6.7.1 : A bit word 1 0 1 1 is to be transmitted. Construct the even parity seven-bit Hamming code for this data.

Soln. :

Step 1 : The code word format :

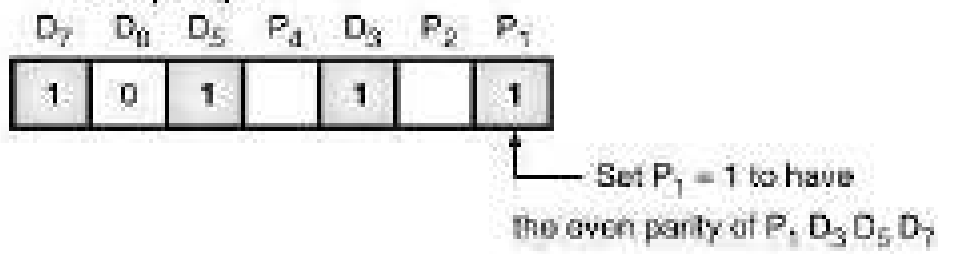
– The seven bit Hamming code format is shown in Fig. P. 6.7.1. Given bit word = 1 0 1 1



(6-1948) **Fig. P. 6.7.1**

Step 2 : Decide P_1 :

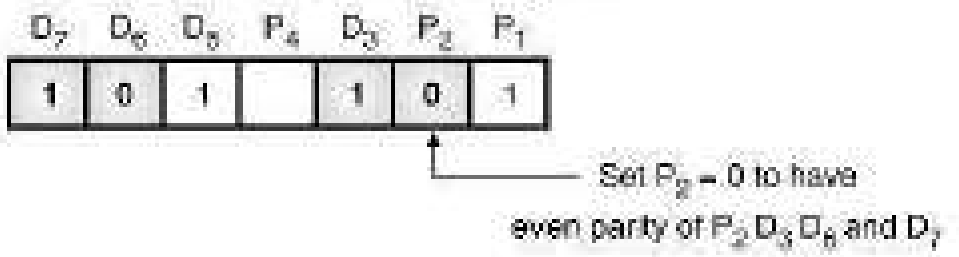
– P_1 sets the parity of bits P_1, D_3, D_5 and D_7. As D_7, D_6, D_3 = 1 1 1 we have to set P_1 = 1 in order to have the even parity.



(6-1949)

Step 3 : Decide P_2 :

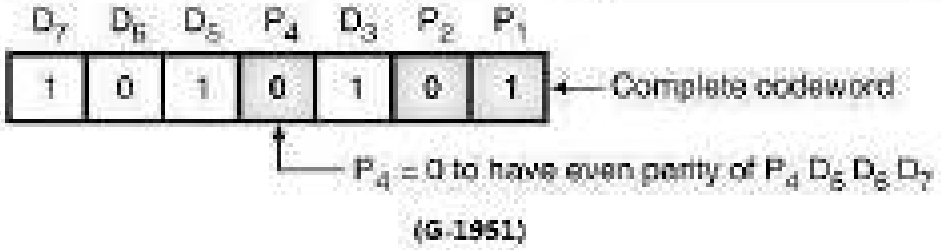
– P_2 is set to have the even parity of P_2, D_3, D_6 and D_7. But D_3, D_6, D_7 = 1 0 1 hence set P_2 = 0.



(6-1950)

Step 4 : Decide P_4 :

– P_4 is set to have the even parity of P_4, D_5, D_6 and D_7. But D_5, D_6, D_7 = 1 0 1, hence set P_4 = 0.



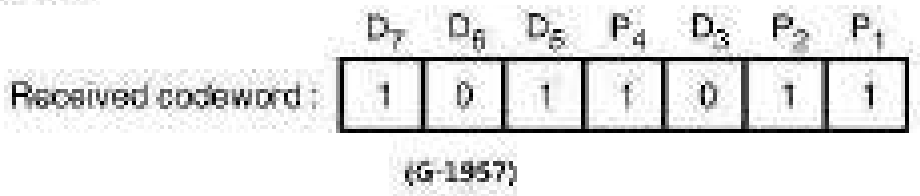
(G-1951)

6.7.3 Detection and Correction of Errors :

1. The Hamming coded data is now transmitted. At the receiver it is decoded to get the data back.
2. The bits (1, 3, 5,7) , (2, 3, 6,7) and (4, 5, 6,7) are checked for even parity.
3. If all the 4-bit groups mentioned above possess the even parity then the received code word is correct ie. it does not contain errors.
4. But if the parity is not even (i.e. it is odd) then error exists. Such an error can be located by forming a three bit number out of the three parity checks. This process becomes clear by solving the example given below.

Ex. 6.7.2 : If the 7-bit Hamming code word received by a receiver is 1 0 1 1 0 1 1. Assuming the even parity state whether the received code word is correct or wrong. If wrong, locate the bit in error.

Soln. :



(G-1957)

Step 1 : Analyze bits 4, 5, 6 and 7 :

$P_4\ D_5\ D_6\ D_7 = 1\ 1\ 0\ 1 \rightarrow$ Odd parity.

$\therefore$ Error exists here.

$\therefore$ Put $P_4 = 1$ in the 4's position of the error word.

Step 2 : Analyze bits 2, 3, 6 and 7 :

$\therefore\ P_2\ D_3\ D_6\ D_7 = 1\ 0\ 0\ 1$ Even parity so no error.

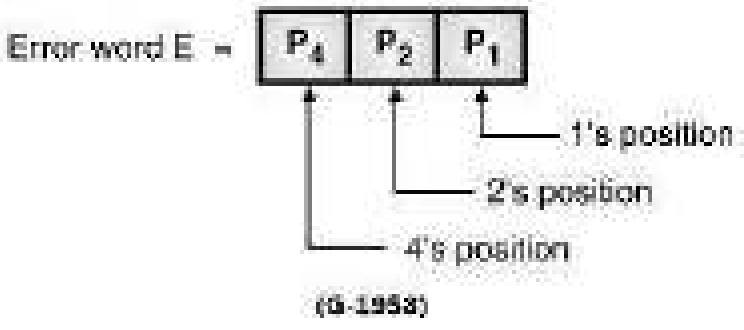
Hence put $P_2 = 0$ in the 2's position of the error word.

Step 3 : Check the bits 1, 3, 5, 7 :

$\therefore P_1\ D_3\ D_5\ D_7 = 1\ 0\ 1\ 1 \rightarrow$ Odd parity so error exists.

Hence put $P_1 = 1$ in the 1's position of the error word.

Step 4 : Write the error word :

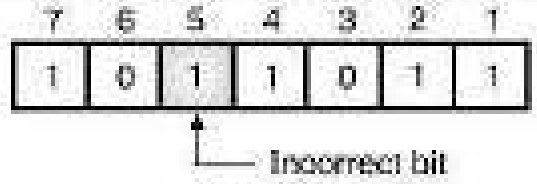


(G-1958)

– Substituting the values of P_4 , P_2 and P_1 obtained in steps 1, 2 and 3 we get

$E = (5)_{10}$ (G-1959)

Hence bit 5 of the transmitted code word is in error.



(G-1960)

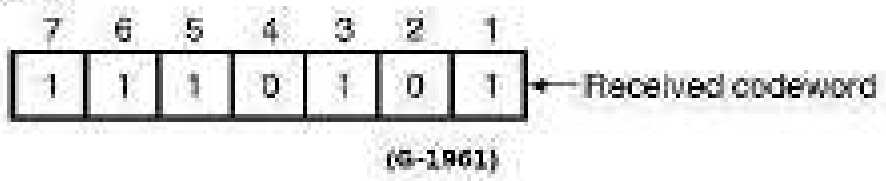
Step 5 : Correct the error :

– Invert the incorrect bit to obtain the correct code word as follows :

Correct code word = [1 0 0 1 0 1 1]

Ex. 6.7.3 : A seven bit even parity Hamming code is received as 1 1 1 0 1 0 1. What is the correct code ?

Soln. :



(G-1961)

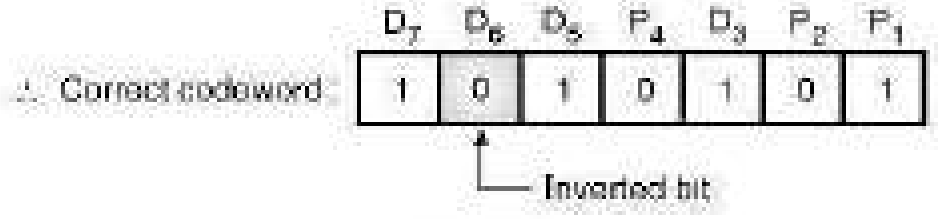
1. Check bits 4, 5, 6, 7 → Odd parity, hence error $\therefore P_4 = 1$
2. Check bits 2, 3, 6, 7 → Odd parity, hence error $\therefore P_2 = 1$
3. Check bits 1, 3, 5, 7 → Even parity, hence no error $\therefore P_1 = 0$

(G-1968)

$\therefore$ Error word E = 1 1 0 (P_4 P_2 P_1)

4. Decimal equivalent of E = 1 1 0 = $(6)_{10}$

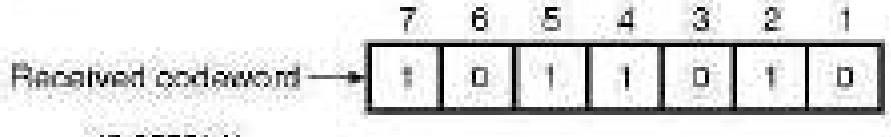
$\therefore$ 6th bit in the received codeword is incorrect. So invert it



(G-1962)

Ex. 6.7.4 : In a particular system the data received was 1 0 1 1 0 1 0. Using seven bit odd parity Hamming code, determine the correct code.

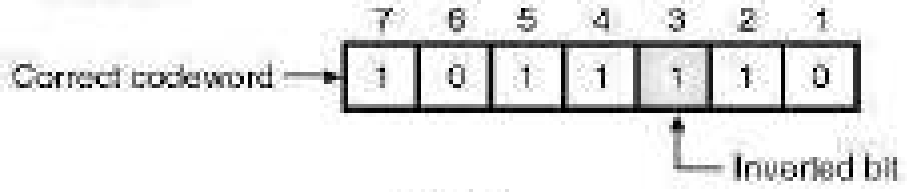
Soln. :



(G-1980(a))

1. Check bits 4, 5, 6,7 = 1101 odd parity, no error
   $\therefore P_4 = 0$
2. Check bits 2, 3, 6, 7 = 1001 even parity, so error
   $\therefore P_2 = 1$
3. Check bits 1, 3, 5, 7 = 0011 even parity, so error
   $\therefore P_1 = 1$

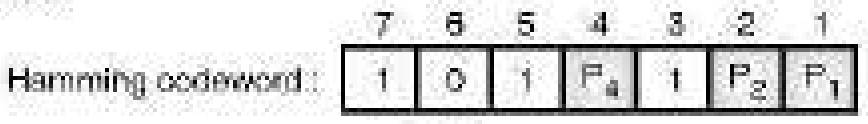
   $\therefore$ Error word E = 0 1 1
   P_4 P_2 P_1
4. Decimal equivalent of E = $(3)_{10}$. Hence the third bit is incorrect. So change it to get the correct code word as follows :



(G-1980)

Ex. 6.7.5 : Data bits 1 0 1 1 have to be transmitted. Construct the odd parity seven bit Hamming code for the given data.

Soln. :



(G-2311)

Check bits 1, 3, 5, 7 for P_1 :

3, 5, 7 = 1 1 1, odd parity. $\therefore P_1 = 0$

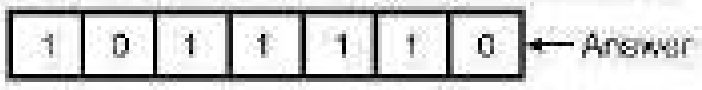
Check bits 2, 3, 6, 7 for deciding P_2

3, 6, 7 = 1 0 1, even parity. So select $P_2 = 1$.

Check bits 4, 5, 6, 7 for deciding P_4

5, 6, 7 = 1 0 1, even parity. So select $P_4 = 1$.

$\therefore$ Required code word with odd parity is as follows :



(G-2312)

Review Questions

Q. 1 How does the parity checking technique helps in detecting the presence of error ?

Q. 2 When does the parity check technique fail ?

Q. 3 Is it possible to correct errors using parity check ?

Q. 4 Write a note on : Checksum error detection.

Q. 5 Explain the VRC and LRC techniques.

Q. 6 Write a short note on : Cyclic Redundancy Check (CRC).

Q. 7 Write a short note on : Hamming codes.

Q. 8 What is the role of the parity bits in a code word ?

6.8 I-Scheme Questions and Answers :

Summer 2019 [Total Marks - 08]

Q. 1 State types of errors. **(Section 6.1.2)** **(2 Marks)**

Q. 2 A system uses CRC on a block of 8 bytes. How many redundant bits are sent per block ? What is the ratio of useful bits to the total bits ? **(6 Marks)**

Ans. :

- Refer Section 6.4 for CRC.
- Generally the number of bits allotted for the CRC field in an information transfer frame is 16 or two bytes.
- All the CRC bits are redundant bits. Hence the number of redundant bits sent per block of data is 16.
- Therefore the ratio of useful bits to redundant bits is (64/16) = 4.

Winter 2019 [Total Marks - 02]

Q. 3 Compare LRC and CRC. (any two points each)

(W-19, 2 Marks)

Ans. :

Comparison of LRC and CRC :

Sr. No.	Parameter	LRC	CRC
1.	Type of technique	Block parity check	Error detection technique
2.	Principle	One LRC bit is added to make the parity of each row of data even	CRC code is transmitted alongwith the message bits
3.	Effectiveness	Less than CRC	More than LRC

Summer 2022 [Total Marks - 06]

Q. 4 List different types of errors.
(Section 6.1.2) **(2 Marks)**

Q. 5 Explain LRC with example.
(Section 6.3.2 and Ex. 6.3.1) **(4 Marks)**

❑❑❑

Chapter 7

Wireless Communication

Syllabus

IEEE standards : 802.1, 802.2, 802.3, 802.4, 805.5, Wireless LANs : 802.11 Architecture, MAC sublayer, Addressing mechanism, Bluetooth architecture : Piconet, Scatternet Mobile generations : 1G, 2G, 3G, 4G and 5G.

Chapter Contents

7.1 Introduction to WLAN and WPAN :

- We all know wired Local Area Networks (LANs) very well. In order to get rid of the wiring associated with the interconnections of PCs in LANs, researchers have explored use of radio waves or infrared light as a replacement to the wires.
- This has resulted in the emergence of wireless LANs i.e. WLANs.
- WPAN is a Wireless Personal Area Network. It is one step down from WLANs. The WPANs cover smaller areas, use less power for transmission.
- WPANs are used for networking of portable and very small computers, cell phones, printers, speakers, microphones, etc.

7.1.1 IEEE Standards : I-Scheme : S-19, W-19

- The Institution of Electrical and Electronics Engineers (IEEE) has developed the layered architecture and other standards of LAN, under their project 802 set up in 1980. The IEEE 802 standards are as follows :

802.1	Architecture, Management and Internetworking
802.2	Logical Link Control (LLC)
802.3	Carrier Sense Multiple Access/Collision Detect (CSMA/CD)
802.4	Token Bus
802.5	Token Ring
802.6	Metropolitan Area Networks (MANs)
802.7	Bandpass Technical Advisory Group
802.8	Fibre Optic Technical Advisory Group
802.9	Integrated Data and Voice Network
802.10	Security Working Group
802.11	Wireless LAN Working Group
802.12	Demand Priority Working Group
802.13	Not Used
802.14	Cable Modem Working Group
802.15	Wireless Personal Area Networking Group
802.16	Broadband Wireless Access Study Group.

7.1.2 Wi-Fi : S-14

MSBTE Questions

Q. 1 Explain following wireless technologies used in computer communication : Wi-Fi. **(S-14, 4 Marks)**

- Wi-Fi is a popular technology which allows an electronic device to exchange data or to connect to the Internet using radio waves.
- We can define Wi-Fi as any Wireless Local Area Network (WLAN) product that are based on the IEEE 802.11 standards.
- The devices which can use Wi-Fi are personal computers, video game consoles, smart phones, some digital cameras, Tablet computers etc.
- Wireless communication is one of the fastest growing technologies.
- The wireless LANs are used in following applications :
  1. Office buildings.
  2. Colleges.
  3. Public areas.
- In this chapter we are going to discuss about two important wireless technologies for LANs :
  1. IEEE 802.11 wireless LAN. 2. Bluetooth

7.2 Architectural Comparison :

- In this section we will compare the architectures of wired and wireless LANs on the basis of the following points :
  1. Medium.
  2. Hosts.
  3. Isolated LANs.
  4. Connection to other networks.
  5. Moving between environments.

7.2.1 Medium :

- The wires (shielded or coaxial) are used to connect the hosts in a wired LAN. But the medium used by the wireless LANs is air.

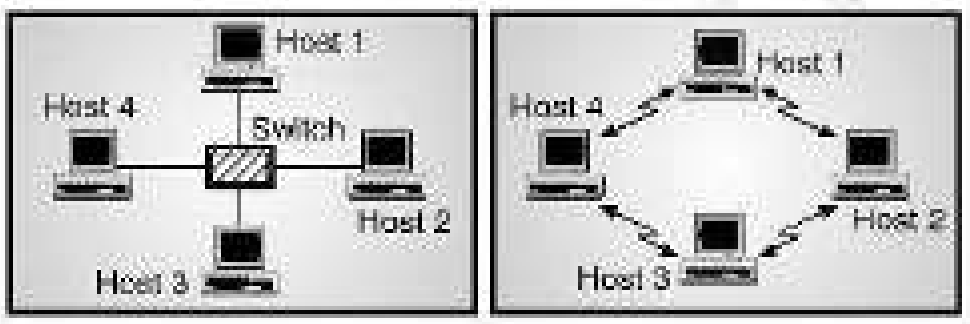
- In the wired LANs the type of communication is point to point and full duplex i.e. bidirectional.
- But in wireless LANs the signal is generally broadcast.
- The hosts in a WLAN share the same medium i.e. air (it is called as multiple access).
- In WLANs a point to point communication between the wireless hosts is extremely rare.

7.2.2 Hosts :

- A host in a wired LAN is always connected at a point to its network. Each host will have a fixed link layer address related to its network interface card (NIC).
- If the host moves from one point to the other in the Internet its link layer address remains the same but the network layer address will change.
- A host in a wireless LAN can move freely as it is not connected physically to the network at all.
- It can still use all the services provided by the network.
- In short the mobility issue in the wired and wireless LANs is entirely different.

7.2.3 Isolated LANs :

- The meaning of the word isolated is different for the wired LANs and wireless LANs.
- Refer Fig. 7.2.1(a) which shows an isolated wired LAN. As shown it consists of hosts which are interconnected via a link layer switch with connecting wires.
- A wireless isolated LAN is as shown in Fig. 7.2.1(b).



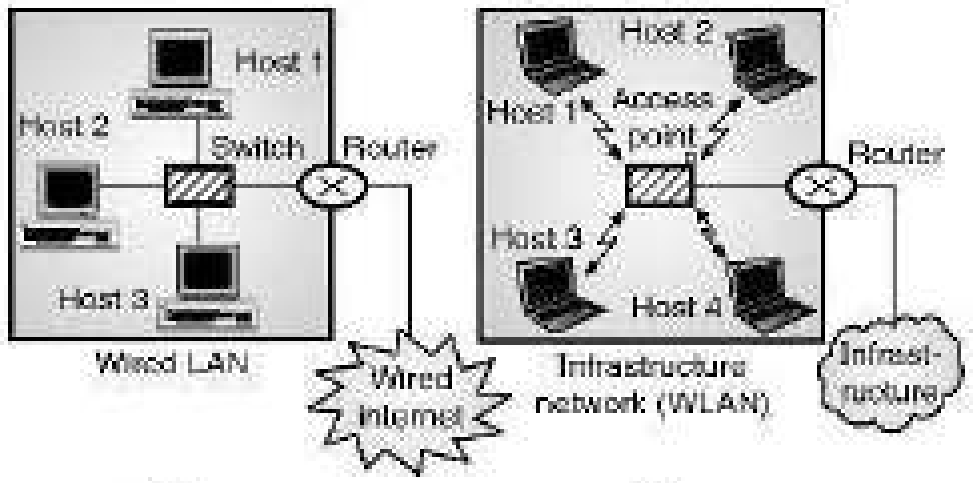
(a) Isolated wired LAN **(b) Ad hoc network**

(G-2096) Fig. 7.2.1

- It is also known as the **Ad hoc Network** in the terminology used for wireless LANs.
- Here a group of wireless hosts communicate with each other directly and freely without using any switch or wired links.

7.2.4 Connection to Other Networks :

- Refer Fig. 7.2.2(a), which shows the manner in which a wired LAN is connected to some other network such as the Internet through a **router.**
- It is possible to connect a wireless LAN either to a wired infrastructure network or a wireless infrastructure network, or to another wireless LAN.
- Fig. 7.2.2(b) shows the connection of a wireless LAN to a wired infrastructure network.



(a) **(b)**

(G-2097) Fig. 7.2.2 : Connection of wired LAN and wireless LAN to the other network

- Consider Fig. 7.2.2(b). In this case the wireless LAN is called as **infrastructure network.**
- It is connected to the wired infrastructure such as the Internet through a special device called as **Access Point (AP).**
- The communication between the wireless hosts and AP is wireless in nature whereas that between the AP and the wired infrastructure is a wired communication.

7.2.5 Moving between Environments :

- It is important to that both wired and wireless LANs operate only in the two lowest layers (physical and data link layers) of the TCP/IP protocol suite.
- Now suppose we want to replace a wired LAN connected to Internet via a router or a modem with a wireless LAN. Then we need to make the following changes :

1. Replace the network interfacing card (NIC) designed for wired environment by a NIC designed for the wireless environment.
2. Use an Access Point (AP) in place of the data link switch.

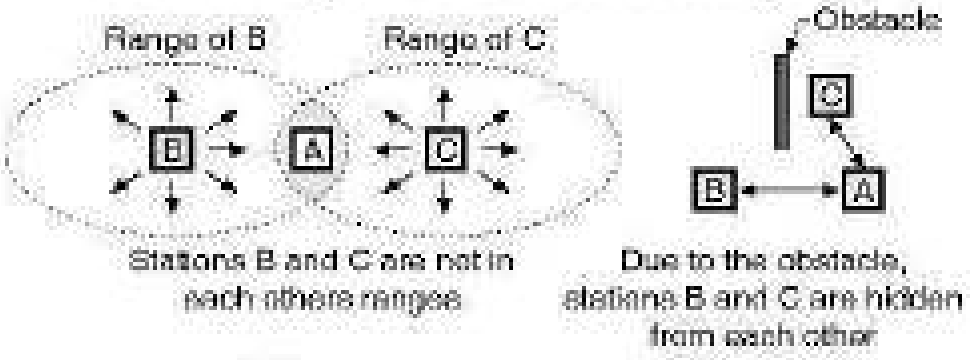
- When we change the NIC of each host, the link layer address will change for each host but there won't be any change in the network layer address i.e. the IP address of each host.
- In this way we can move from wired LAN to a wireless LAN.

7.3 Access Control in WLANs :

- Access control means how a wireless host in a wireless LAN can get access to the shared medium which is air.
- The access control is possibly the most important issue in a wireless LAN.
- In the standard Ethernet the CSMA/CD algorithm is used for access control.
- In this technique each host is a contender to share the medium so it sends its frame if the medium is found idle.
- In this mechanism, there is always a possibility of collision. If collision takes place, the CSMA/CD detects it and the frame is sent again.
- The collision detection is useful in two ways :
  1. In the event of collision, the sent frame is not received and hence it should be sent again.
  2. The absence of collision is a kind of acknowledgement that the frame was received.
- For the **wireless LANs** however, the CSMA/CD algorithm does not work properly.

Reasons for CSMA/CD not being suitable for WLANs :

- Following are the resons why CSMA/CD algorithm does not work for wireless LANs :
  1. For a successful detection of a collision, a host should work in the **duplex** mode. That means it should send the frame and receive the collision signal at the same time. But the wireless hosts cannot do this. They can either send or receive at one time, because being battery operated they do not have enough power to do so.
  2. Hidden station problem :
- The hidden station problem occurs when a station may not be aware that some other station is transmitting because of either range problem or some obstacle. In this situation collision may occur but may not be detected.
- The hidden station problem is illustrated in Fig. 7.3.1. Refer Fig. 7.3.1(a) which shows three wireless stations-A, B and C. The transmission ranges of stations-B and C have been shown by the two ovals on left and right respectively which shows that station-C is not in the range of B and B is not in the range of C.



(S-2018) **Fig. 7.3.1 : Hidden station problem**

- However station-A is in the range of both B and C. So A can hear signals transmitted by B and C.
- Refer Fig. 7.3.1(a) where station-B is transmitting to station-A.
- Now if station-C checks the medium to see if anyone is transmitting, it will not hear station-B because it is out of range. So station-C will come to a wrong conclusion that no one is transmitting and so it can start transmitting to station-A.
- If station-C starts transmitting, it will create a collision at station-A and will wipe out the frames from station-B.
- This problem in which a station is not able to detect an already transmitting other station which is too far away is called as the **hidden station problem.**
- In this example it is said that stations-B and C are hidden from each other with respect to station-A.
- Now consider Fig. 7.3.1(b) which shows the hidden station problem occurring due to an obstacle.

Note : Due to hidden station problem, the possibility of collision increases and the capacity network will reduce.

3. The third reason of not using the CSMA/CD for wireless networks is that the distance between the stations can be sometimes too large. Due to huge distance, the signal fading could occur and the station at one end could be prevented from hearing a collision at the other end.

Which Access Control Algorithm for Wireless LAN ?

- The Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is the access control algorithm used for the wireless networks because it overcomes all the problems of CSMA/CD.

7.4 IEEE 802.11 : I-Scheme : S-22

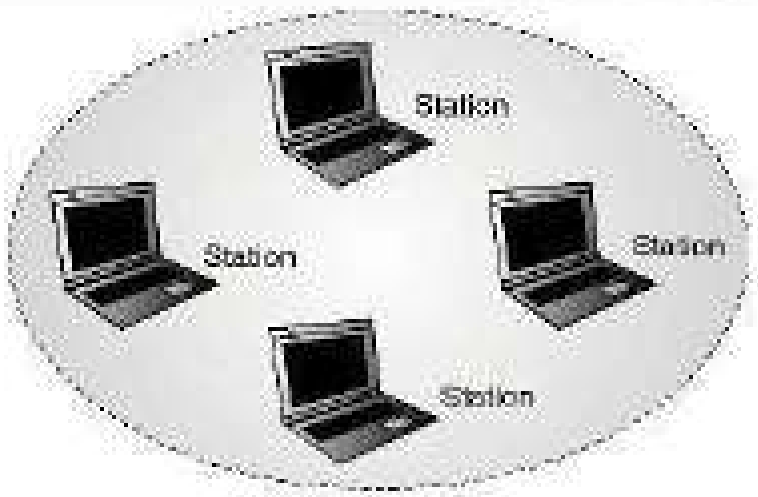
- The 802.11 is the specifications for the wireless LANs, defined by IEEE.
- This specification defines the physical and data link layers. It is some times called as **Wireless Ethernet.**
- Generally the term **Wi-Fi** (Wireless fidelity) is used as a synonym for wireless LAN.
- However in reality, Wi-Fi is a wireless LAN which is certified by the **Wi-Fi Alliance** a global industry association.

7.4.1 Architecture (Components of 802.11 Network) : I-Scheme : W-19, S-22

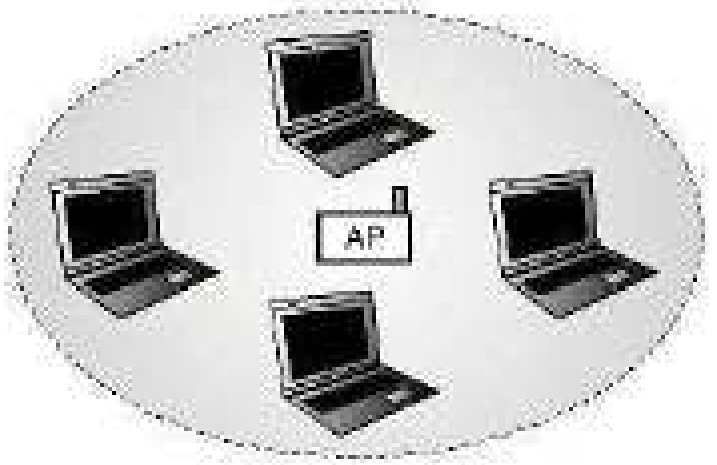
- IEEE 802.11 is the most popular WLAN standard. It defines the specifications for the physical and MAC layers.
- IEEE 802.11 defines two types of services :
  1. Basic Service Set (BSS).
  2. Extended Service Set (ESS).

7.4.2 Basic Service Set (BSS) : I-Scheme : W-19

- As per IEEE 802.11 the BSS has been defined as the basic building block of wireless LAN.
- A BSS consists of stationary or moving wireless stations and a central base station which is optional called as the Access Point (AP).
- Thus a BSS can be either without AP or with AP as shown in Figs. 7.4.1(a) and (b).
- The BSS without AP cannot send data to another BSS. So no data exchange can take place outside that BSS hence it is known as a stand alone network or **ad hoc BSS.** However all the stations inside a BSS can exchange data among themselves.



(a) BSS without AP



(b) BSS with an AP

(G-330) **Fig. 7.4.1 : Types of BSS**

- A BSS with AP is as shown in Fig. 7.4.1(b). It can however communicate with the other BSS via the access point AP.
- The BSS with AP is also called as **Infrastructure BSS.**

7.4.3 Extended Service Set (ESS) :

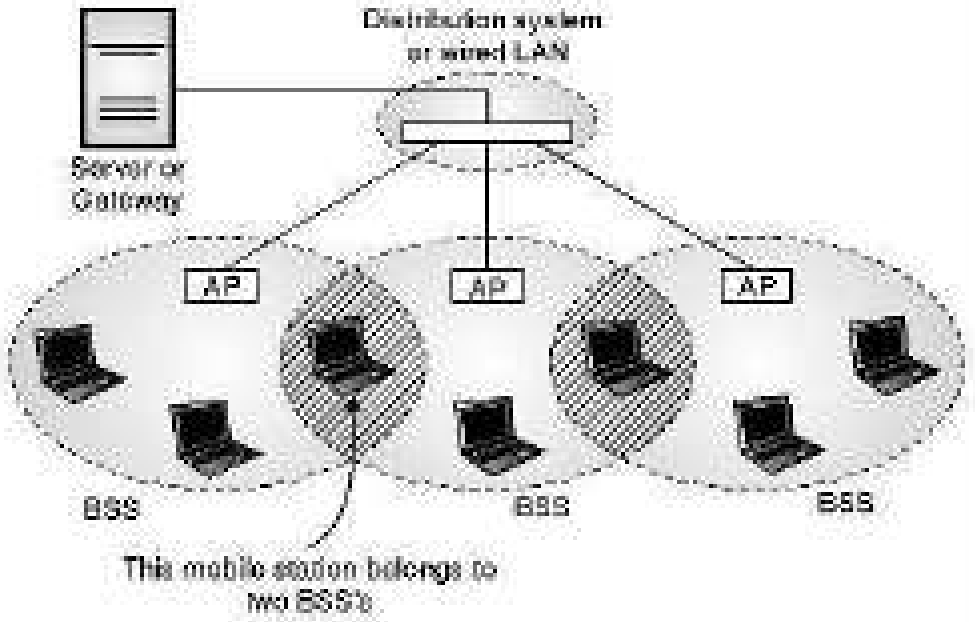
S-17, I-Scheme : W-19

MSBTE Questions

Q. 1 With neat diagram explain the ESS architecture of IEEE 802.11. **(S-17, 4 Marks)**

- An Extended Service Set (ESS) consists of multiple BSSs with APs.
- The BSSs in this system are connected to each other via a **distribution system** or a wired LAN as shown in Fig. 7.4.2.
- The APs are connected to each other via the distribution system as shown. The distribution system can be any type of LAN such as Ethernet.
- The ESS contains two types of stations :
  1. Mobile stations which can move and change location.
  2. Stationary of non-moving stations.

- Out of these, the non-moving stations are the APs which are a part of the wired LAN.
- Whereas the mobile stations are those contained in the BSS. Fig. 7.4.2 shows the structure of an ESS.



(G-381) **Fig. 7.4.2 : ESS (Extended Service Set)**

- The BSSs are connected to each other to form a network called **infrastructure network.**
- In such networks the stations close to each other can communicate without taking help of AP.
- But if two stations located in two different BSS wish to communicate with each other, than they have to do so through APs.
- This type of communication is very similar to that in the cellular communication.
- The BSS acts as a cell and AP as base station.
- As shown in Fig. 7.4.2 it is possible that a mobile station can belong to more than one BSSs simultaneously.

7.4.4 Types of Stations :

- Three types of stations are defined by IEEE 802.11 depending on their mobility in the wireless LAN as :
  1. No transition.
  2. BSS transition.
  3. ESS transition.

1. No transition mobility :

- It is defined as a station which is not-moving at all (stationary) or moving inside a BSS only.

2. BSS transition mobility :

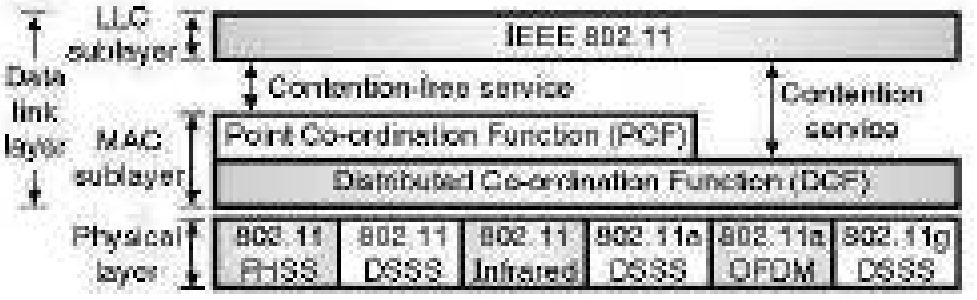
- A station having BSS transition mobility is the one which can move from one BSS to the other BSS but does not move outside one ESS.

3. ESS transition mobility :

- A station having ESS transition mobility is the one which can move from one ESS to any other ESS, But IEEE 802.11 does not guarantee a continuous communication when the station is moving.

7.5 MAC Sublayer :

- In IEEE 802.11, two MAC sublayers are defined. They are as follows :
  1. The Distributed Co-ordination Functions (DCF).
  2. Point Co-ordination Function (PCF).
- The relation between DCF, PDF, the LLC sublayer and the physical layer has been shown in Fig. 7.5.1.



(G-2099) **Fig. 7.5.1 : MAC layers in 802.11 standard**

- The physical layer implementations have been discussed later on in this chapter.
- For now we will focus on the MAC sublayer.

7.5.1 Distributed Co-ordination Function (DCF) :

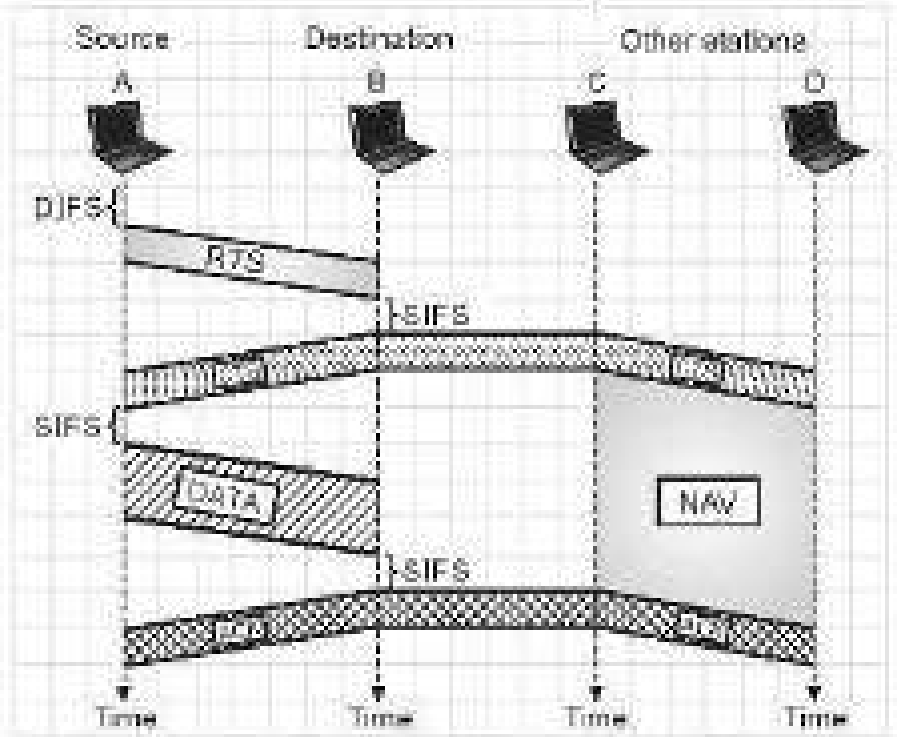
- IEEE has defined two protocols at the MAC sublayer. One of these two protocols is called as the distributed co-ordination function (DCF).
- The access method used by DCF is CSMA/CA.

7.5.2 Frame Exchange Time Line :

- The exchange of control and data frames with time has been shown Fig. 7.5.2.
- We assume that there are four wireless stations A, B, C and D present in a wireless LAN.

- A is a source and B is the destination. Therefore C and D are referred to as other stations.
- The sequence of control and data exchange is as follows :

1. The source station A senses the medium for its idleness before sending a frame. It does the media sensing by checking the energy level at the carrier frequency.
   (a) A persistence strategy is used with back of until the channel is found to be idle.
   (b) Once the channel is found to be idle, the source station A waits for a specific amount of time called as the Distributed Interframe Space (DIFS). After this waiting time the station A sends a control frame called as Request to Send (RTS) as shown in Fig. 7.5.2.



(G-2100) **Fig. 7.5.2 : CSMA/CA and NAV**

2. After receiving the RTS, the destination station B waits for a specific amount of time called the **Short Interframe Space (SIFS)** and then sends a control frame **Clear to Send** (CTS) back to the source station A. The CTS frame is an indication that the destination station is ready for receiving the data.
3. The source station receives the CTS frame, waits for a duration of SIFS and then sends the data to the destination station.
4. The destination station receives the data, waits for a duration of SIFS and sends the acknowledgement (ACK) frame to indicate that it has received the data frame.

- Note that in the CSMA/CA protocol, the acknowledgement (ACK) is needed because otherwise the source station does not have any means to know that the data has been received by the destination station.
- In CSMA/CD the ACK is not needed because the lack of collision itself is treated as an acknowledgement of data being received successfully.

7.5.3 Network Allocation Vector (NAV) :

- The question here is how do other stations restrain from sending their data when one channel is already transmitting ?
- In other words how is the **collision avoidance** is practically accomplished ? The answer to both these questions is a special feature called as **NAV.**
- The concept of NAV i.e. **Network Allocation Factor** is as follows :
- When station A sends an RTS frame (see Fig. 7.5.2), which consists of the time duration for which A needs to use the channel, the stations which are affected by this transmission create a **timer** called as **NAV.**
- The NAV will indicate the amount of time that must pass before these stations can check again, whether the cannel has again become idle.
- This happens everytime when a station sends its RTS frame, the other stations will initiate their NAV.
- During the NAV interval no other station will initiate its transmission.
- In this way the collision avoidance aspect of the CSMA / CA protocol is accomplished.
- The other stations check the channel for idleness only after the expiry of their NAV.

7.5.4 Collision During Handshaking :

- If the collision takes place when the RTS and CTS frames are in transition, then it is called as collision during handshaking.
- In such a situation, two or more stations try to send the RTS frame at the same time, which may collide with each other.

- But in CSMA/CA there is no mechanism to detect such collisions. So the collision of RTS frames also will go undetected.
- Then how will the sources know that a collision has taken place ?
- Well, a source will assume that the collision has taken place if it does not receive the **CTS** frame from the receiver in response to RTS.
- In such events, the sender applies the **back-off** strategy and tries after sometime.
- This is how the collision during handshaking is handled by CSMA/CA in the wireless environment.

7.5.5 Hidden Station Problem :

- Let see now, how CSMA/CA avoids the hidden station problem. Refer Fig. 7.5.2.
- Actually the RTS and CTS frames (handshake frames) are used to solve the hidden station problem.
- As shown in Fig. 7.5.2 the RTS message from A can reach B but not C (because C is out of range of A).
- In response to this, station B sends the CTS frame. Since both A and C are in the range of B, the CTS frame will reach stations A as well as C.
- Due to this CTS frame station C will understand that some hidden station (A in this case) is already using the channel.
- Therefore C will refrain from transmitting. This will avoid the possible collision.

7.6 Address Mechanism in WLANs :

- The address mechanism of IEEE 802.11 (wireless LAN) standard specifies four different cases on the basis of the values of **two flags** present in the **FC field** namely : **To DS** and **From DS.**
- Each of these two flags is a 1-bit flag. Hence each one can have a value of either 0 or 1.
- Therefore with two flags we will have four different situations (combinations).
- The four addresses i.e. address-1 to address-4 in the MAC frame will have their meanings dependent on the values of the above mentioned two flags, as shown in Table 7.6.1 given below.

Table 7.6.1 : Addresses in the MAC frame

Flags		Addresses			
To DS	From DS	Address-1	Address-2	Address-3	Address-4
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

- Note that the four address fields represent the following addresses.

1. **Address – 1 :**

- The contents of this field always correspond to the address of the next device which is to be visited by the frame.

2. **Address – 2 :**

- The contents of this field always correspond to the address of the last device which was visited by the frame.

3. **Address - 3 :**

- It is the address of the final destination station if it is not defined by address - 1 or the address of the original source station if it is not defined by the address - 2.

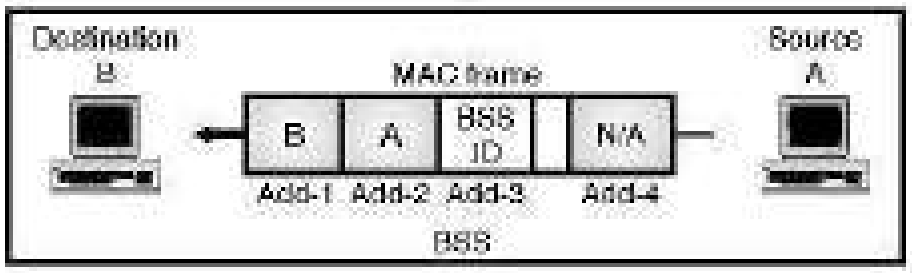
4. **Address - 4 :**

- It is the address of the original source when the distribution system is also wireless.
- Now let us discuss the four cases based on the values of the two flags one by one.

7.6.1 Case 1 : 00 :

- For this case the values of the two flags are : To DS = 0 and From DS = 0. Since the value of **To DS = 0**, it means that the frame is not going to a distribution system (DS). And because the value of **From DS = 0**, it means that the frame is not coming from a distribution system.
- The frame is moving from one station to the other in the same BSS but without passing through the distribution system.

– The addresses for this case are as shown in Fig. 7.6.1(a). The frame shown in this figure is the MAC frame.



(G-2151) **Fig. 7.6.1(a) : Case 1 : 00 Addresses**

– B is the destination and A is the source. Since Flags = 00, as per Table 7.6.1, the addresses are as follows :

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination	Source	BSS ID	N/A

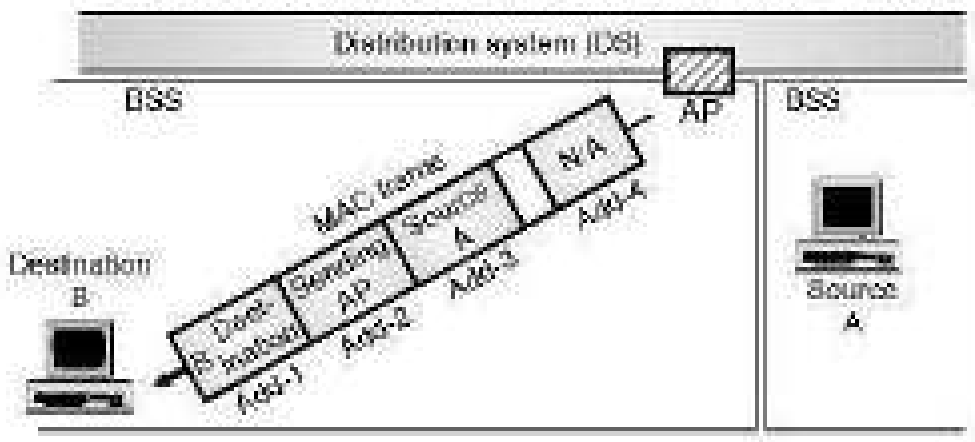
7.6.2 Case 2 : 01 :

– In this case the two flags have the following values :

– **To DS = 0** and **From DS = 1.** These values show that the frame is coming from a distribution system.

– That means it is coming from an AP and going to a station.

– Fig. 7.6.1(b) shows the addresses for this case. B is the destination station (address 1), the address-2 is the sending AP, address-3 contains the address of the original source A in the other BSS and address 4 is N/A.



(G-2152) **Fig. 7.6.1(b) : Case 2 : 01 Addresses**

– As per Table 7.6.1, the addresses are as follows :

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	1	Destination B	Sending AP	Source A	N/A

7.6.3 Case 3 : 10 :

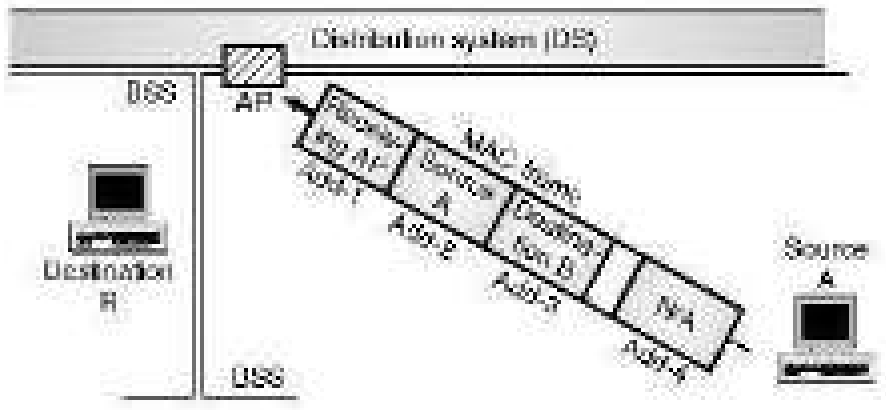
– The two flags have the following values :

– **To DS = 1** and **From DS = 0.** That means the frame is coming from a station (A) and going to the distribution system i.e. AP.

– Address - 3 contains the address of the final destination (B) of the frame in the other BSS.

– As per Table 7.6.1, the addresses are as follows and the addresses are as shown in Fig. 7.6.1(c).

To DS	From DS	Address 1	Address 2	Address 3	Address 4
1	0	Destination	Source	BSS ID	N/A



(G-2153) **Fig. 7.6.1(c) : Case 3 : 01 Addresses**

7.6.4 Case 4 : 11 :

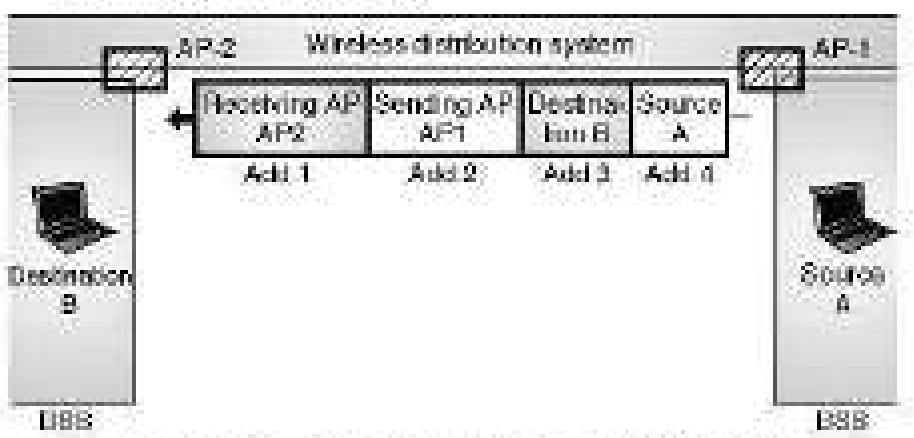
– The two flags have the following values.

– **To DS = 1** and **From DS = 1.** This means the frame is coming from an AP and going to another AP. The distribution system is wireless.

– In this we need to use four address as shown below.

To DS	From DS	Address 1	Address 2	Address 3	Address 4
1	1	Receiving AP	Sending AP	Destination B	Source A

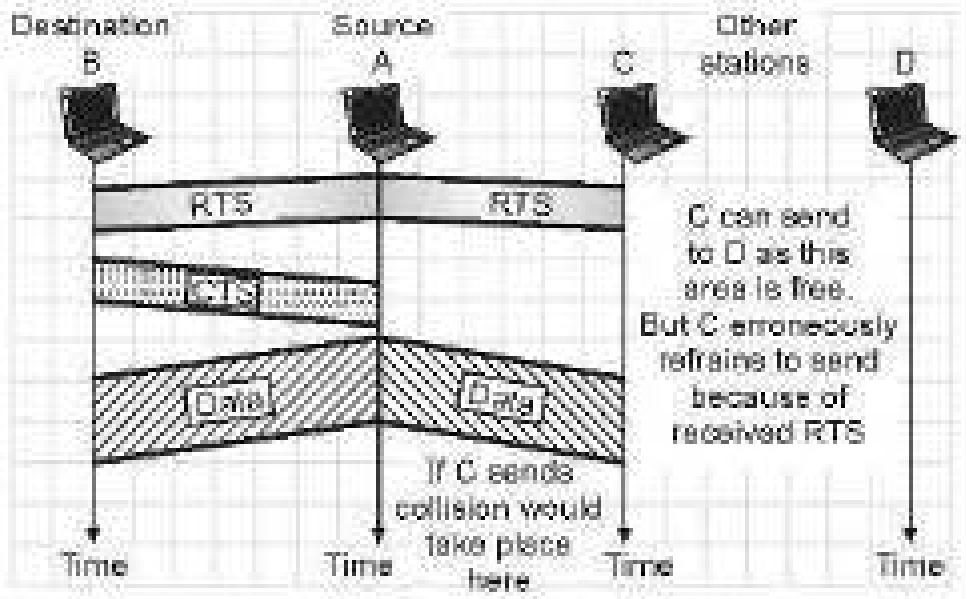
– As shown in Fig. 7.6.1(d) the source A and destination B are in two different BSS.



(G-2154) **Fig. 7.6.1(d) : Case 4 : 11 Addresses**

7.6.5 Exposed Station Problem :

- Earlier in this chapter the problem of hidden station and its remedy have been discussed.
- The **exposed station problem** is a similar problem.
- In this problem, a station refrains from using the common even when no other station is using it (i.e. the channel is actually free).
- In order to understand this concept clearly, refer Fig. 7.6.2 where A is the sending station and B is the destination. A is sending data to B.



(G-2155) **Fig. 7.6.2 : Exposed station problem**

- Station C wants to send its data to station D and it is possible to do so without interfering in the communication between A and B.
- As shown in Fig. 7.6.2, station C is in the range of station A. In otherwords C is exposed to A.
- So C listens to what A is transmitting and decides to refrain itself from sending its message to D.
- This causes wastage of channel capacity.
- The handshaking messages RTS and CTS are not helpful in solving the exposed station problem.
- In fact station C refrains itself when it hears the RTS message from station A.
- This happens because station C does not know that the communication between A and B does not affect the zone between C and D.

7.6.6 Advantages of WLAN :

1. WLAN is cheaper than wired LAN, because wires are not required.
2. WLAN can be laid down where it is difficult to run cables e.g. Historical buildings.
3. It is possible to form WLAN using laptops.
4. Any standard Wi-Fi device can work anywhere in the world.
5. WPA2 protocol used for Wi-Fi is secure protocol so WLANs are safe.

7.6.7 Limitations of WLAN :

1. Spectrum assignment and operational conditions are not same world wide.
2. Radiated power is limited to 100 mW. So the range will be limited.
3. Wi-Fi networks have a limited range typically 35 m or 120 ft indoor and 100 m or 300 ft outdoor.
4. There are data security risks. Wi-Fi networks are not protected thoroughly.
5. Wi-Fi connections can be easily disrupted.

7.7 Comparison of Wired and Wireless LANs : S-18

MSBTE Questions

Q. 1 Compare wire and wireless transmission. **(S-18, 4 Marks)**

Sr. No.	Parameter	Wired LAN	Wireless LAN
1.	IEEE standard	IEEE 802.3	IEEE 802.11
2.	Communication medium	Coaxial cables	Infrared or RF waves.
3.	Use of spread spectrum technique	Not used	Used.
4.	Access algorithm	CSMA/CD	CSMA/CA
5.	Efficiency	High	Low
6.	Noise problem	Low	High
7.	Addressing	Simpler	Complicated
8.	Range	Large	Short
9.	Mobility	Zero	Possible

7.8 Applications of Wireless LAN :

- Due to flexibility and possibility to configure in a variety of topologies, WLANs can be used in a number of varied applications. Some of them are as follows :
  1. For accessing the Internet, checking E-mails and receive/send instant messages when the user is moving.
  2. WLANs can set up networks in the locations affected by earthquakes or other disasters where no suitable infrastructure is available and wired networks have been destroyed.
  3. In places of historic importance, where wiring may not be permitted, the WLAN can be used easily and effectively.

7.9 Bluetooth : S-14, S-15

MSBTE Questions

Q. 1 Explain following wireless technologies used in computer communication : Bluetooth. **(S-14, 4 Marks)**

Q. 2 Explain in brief the functioning of Bluetooth. **(S-15, 4 Marks)**

What is Bluetooth ?

- Bluetooth is the name given to a new technology using short-range radio links, which could replace the cable(s) connecting portable and/or fixed electronic devices.
- Bluetooth replaces cables that connect one device to another with one universal radio link.
- Its key features are robustness, low complexity, low power and low cost.
- Designed to operate in noisy frequency environments, the Bluetooth radio uses a fast acknowledgement and frequency-hopping scheme to make the link more reliable.
- Bluetooth radio modules operate in the unlicensed ISM band at 2.4 GHz, and avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet.
- Compared with other systems in the same frequency band, the Bluetooth radio hops faster and uses shorter wavelengths.
- Thus Bluetooth is a wireless LAN technology which can connect devices such as telephones, computers, printers, cameras, etc. without using wires.
- A Bluetooth LAN is an Ad hoc network i.e. it does not use a base station. It is possible to connect the Bluetooth LAN to the Internet.
- This technology is implemented using the IEEE 802.15 standard.

7.9.1 Architecture :

- Bluetooth defines two types of networks :
  1. Piconets and 2. Scatternets.

7.9.2 Piconets :

S-15, S-16, W-16, I-Scheme : W-19, S-22

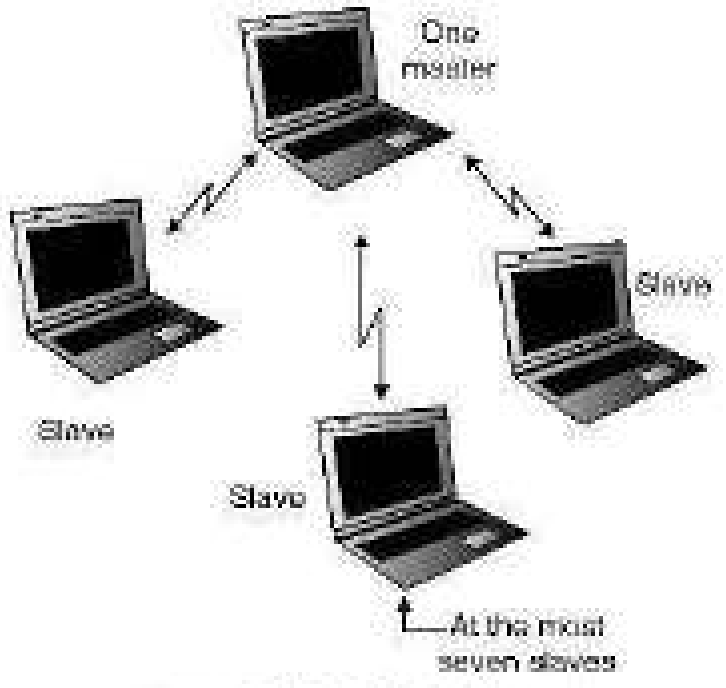
MSBTE Questions

Q. 1 Explain in brief the functioning of Bluetooth. **(S-15, 4 Marks)**

Q. 2 Draw the Bluetooth architecture and describe its working. **(S-16, 4 Marks)**

Q. 3 Describe the architecture of Bluetooth technology. **(W-16, 4 Marks)**

- The first type of a Bluetooth network is called as a **piconet** or a **small net.**
- It can have at the most eight stations. One of them is called as a **master** and all others are called as **slaves.**
- All the slave stations are synchronised in all aspects with the master.
- A piconet can have only one master station. Fig. 7.9.1 shows a piconet.



(G-3881) **Fig. 7.9.1 : A piconet**

- A master can also be called as a primary station and slaves are secondary station.
- The communication between a master and slaves can be one-to-one or one-to-many.
- Note that the communication takes place between the master and slaves but no direct communication takes place between the slaves.

7.9.3 Scatternet :

S-15, S-16, W-16, I-Scheme : W-19, S-22

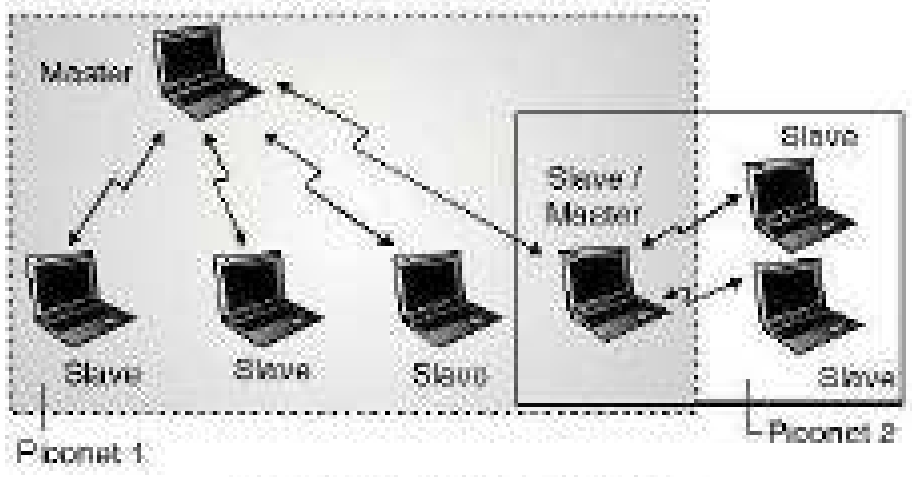
MSBTE Questions

Q. 1 Explain in brief the functioning of Bluetooth. **(S-15, 4 Marks)**

Q. 2 Draw the Bluetooth architecture and describe its working. **(S-16, 4 Marks)**

Q. 3 Describe the architecture of Bluetooth technology. **(W-16, 4 Marks)**

- A scatternet is obtained by combining piconets as shown in Fig. 7.9.2.



(G-389) **Fig. 7.9.2 : Scatternet**

- Fig. 7.9.2 shows a scatternet consisting of two piconets. A slave in the first piconet can act as a master in the second piconet.
- It will receive the messages from the master in the first piconet by acting as a slave and then delivers the message to the slaves in the second piconet as shown in Fig. 7.9.2.
- So the same device acts as a slave in the first piconet and as master in the second piconet.

7.9.4 Bluetooth Devices :

- Every Bluetooth device consists of a built in short range **radio transmitter.** The current data rate is 1 Mbps and the bandwidth is 2.4 GHz.
- So an interface between the IEEE 802.11 wireless LAN and Bluetooth LAN is possible.
- The Bluetooth specification standard defines a short-range (10-meter) radio link.
- The devices carrying Bluetooth-enabled chips can easily transfer data at a rate of about 1 Mbps (Megabits per second) within 10 meters (33 feet) of range through walls, clothing and luggage bags.
- The interaction between devices occurs by itself without direct human intervention whenever they are within each other's range.
- In this process, the software technology embedded in the Bluetooth transceiver chip triggers an automatic connection to deliver and accept the data flow.
- Since Bluetooth is of short range with limited speed and low-power technology.
- It is less attractive to corporate wireless local area networks that are generally powered with the 802.11 wireless LAN technologies.
- Each Bluetooth-enabled device contains a 1.5-inch square transceiver chip operating in the ISM (industrial, scientific, and medical) radio frequency band of 2.40 GHz to 2.48 GHz.
- This frequency is generally available worldwide for free without any licensing restrictions.
- The ISM band is divided into 79 channels with each carrying a bandwidth of 1 MHz.

7.9.5 Security Limitations in Bluetooth :

- Due to its wireless nature, experts express a security concern with Bluetooth.
- The issue can be addressed with three aspects: specific sequence of channel hopping known only to the sending and receiving devices, challenge-response authentication routine to verify the validity of the receiving unit, and the 128-bit key encryption standard for securing transmission between devices.

7.9.6 Bluetooth Advantages :

1. One can create a personal area network at home or on the road with Bluetooth-enabled devices such as keyboard, mouse, scanner, PDA, laptop, cell phone, etc.

2. This network can automatically help synchronize notes, calendar, address book and also print pictures, receive emails, access cell phones messages, etc. It can even help consumers pay bills with credit card through Bluetooth cash register if a Bluetooth PDA stores the card information.

7.9.7 Difference between Bluetooth and WLAN IEEE 802.11x :

Sr. No.	Bluetooth	IEEE 802.11x
1.	Bluetooth hop frequency is 1600 hops/second	IEEE 802.11x hop frequency is 2.5 hops/second
2.	Data transfer rate is 1 Mbps	Data transfer rate is 11 Mbps
3.	Transmission range is 10 m	Transmission range is 15-150 m indoor and 300 m outdoor
4.	Bluetooth uses lower transmission power	IEEE 802.11 uses more transmission power than Bluetooth
5.	It is used to connect devices that are in close proximity such as palm computing devices attached to smart phones, notebooks to printers.	It is a full LAN connectivity solution designed to provide full network service at Ethernet data rate.
6.	Bluetooth is being a standard for short time network.	IEEE 802.11 is a standard for LAN and is for longer time network.
7.	Bluetooth uses GFSK (Gaussian Frequency Shift Keying) modulation technique.	IEEE 802.11 uses CCK (Complementary Code Keying) modulation technique.

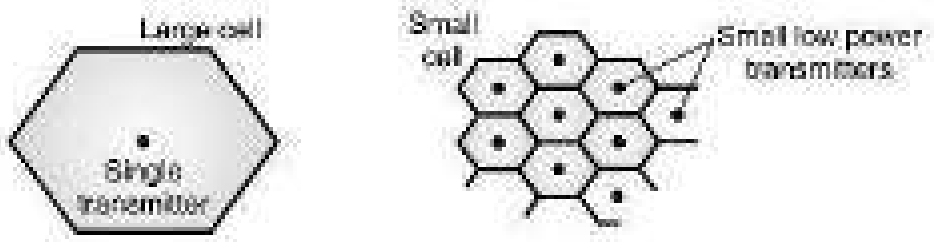
7.9.8 Applications of Bluetooth Technology :

- Some of its applications are as follows :
  1. Ad-hoc network of laptops for interactive conference.
  2. Transferring data, photographs from one cell phone to other cell phones or computers and vice versa.
  3. Connecting a digital camera wirelessly to a mobile phone.
  4. Three in one phone where the same phone functions as an intercom, a cordless phone and a mobile phone.
  5. Mouse, printer, keyboards etc can be connected to a computer without using wires.

7.10 The Mobile Telephone System :

- The aim of the early mobile radio system was to provide coverage to a large area with the help of a single high power transmitter having an antenna mounted on a tall tower.
- This approach had the following disadvantages :
  1. Frequency reuse was not possible.
  2. Proper spectrum allocation in proportion with increasing demand was not possible.
- Hence it became necessary to restructure to radio telephone system so as to achieve the following objectives :
  1. High capacity.
  2. To utilize the available radio spectrum effectively.
  3. Coverage of large areas.
- The major breakthrough in this field was the introduction of the **cellular concept.**
- The cellular concept offered the following advantages :
  1. Improved user capacity.
  2. No spectral congestion.
  3. No major technological changes.
  4. Efficient utilization of the available spectrum.
- In the **cellular systems,** a single high power transmitter is (large cell) is replaced by many low power transmitter (small cells) as shown in Fig. 7.10.1.

– Note that each small cell provides coverage to a small portion of the entire large service area (large cell).



(G-1562) **Fig. 7.10.1 : The cellular concept**

7.10.1 Basic Concept : S-10

MSBTE Questions

Q. 1 Explain basic principle of mobile communication. **(S-10, 4 Marks)**

– Cellular phone is wireless communication just like cordless phone.

– In cell phone distance is not restricted to within home but one can travel in the city or even outside the city without interruption in communication.

– The demand for cellular mobile phone is increasing at alarming level and is likely that wired communication will be replaced by wireless technology.

– In the cellular system city is divided into small areas called 'cells'. Each cell is around 10 square kilometre (depends upon power of base station).

– The cells are normally thought of hexagons. Because cell phones and base stations use low power transmitters, the same frequencies can be reused in non-adjacent cell.

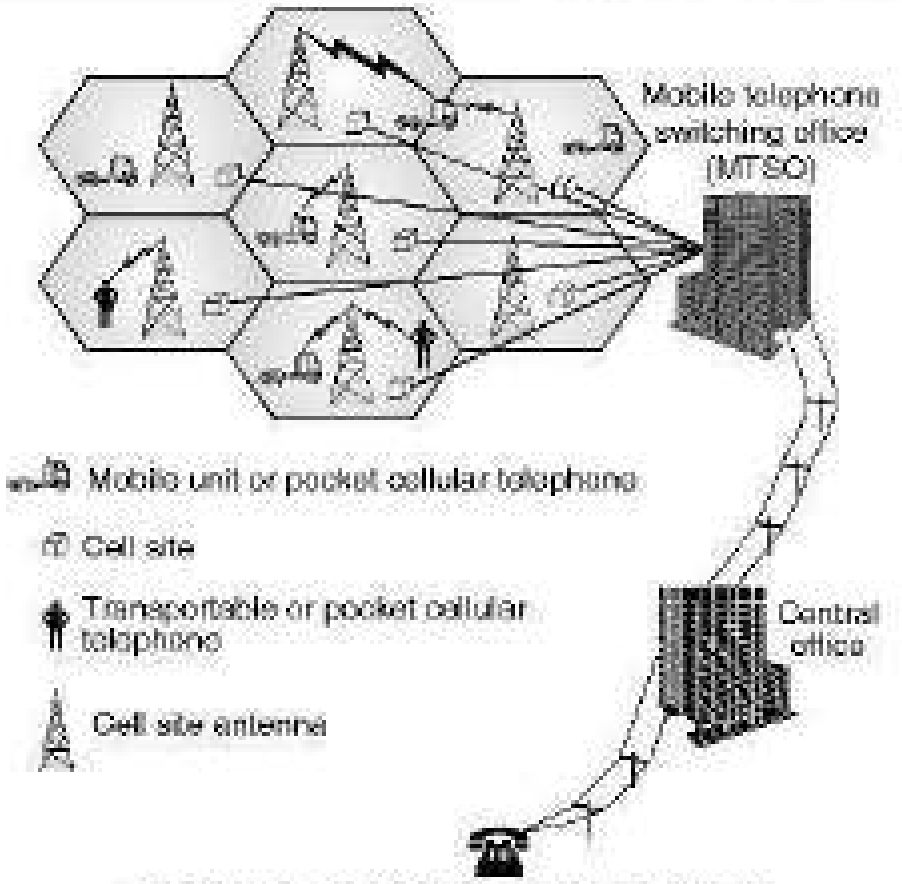
– Each cell is (The cellular network is as shown in Fig. 7.10.2) linked to central location called the Mobile Telephone Switching Office (MTSO).

– MTSO coordinates all mobile calls between an area which consists of several cell sites and the central office.

– Time and billing information for each mobile unit is accounted for by MTSO.

– At the cell site base station is provided to transmit, receive, and switch calls to and from any mobile unit within the call to the MTSO.

– A cell covers only few square kilometre area, thus reducing the power requirement necessary to communicate with cellular telephones.



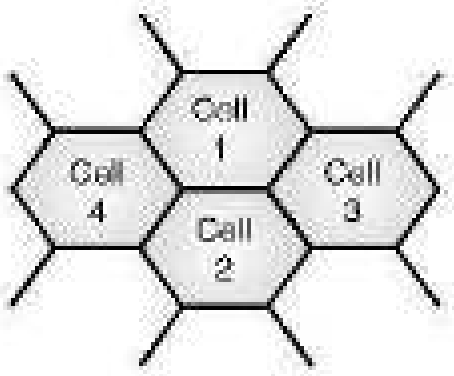
(G-1025) **Fig. 7.10.2 : The cellular network**

– In this manner heavily populated areas can be serviced by several stations, rather than one as used by conventional mobile techniques.

Cell :

– The basic geographic unit of a cellular communication system is called as a cell.

– Its shape is hexagonal as shown in Fig. 7.10.3(a). Cells have the base stations transmitting over small geographic areas.



(G-1026) **Fig. 7.10.3(a) : Cell**

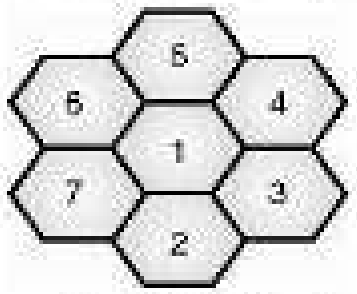
– The size of a cell is not fixed. Practically the shape of the cell may not be a perfect hexagone.

Cluster :

– A group of cells is called as a **cluster.**

– Fig. 7.10.3(b) shows the cluster of seven cells or a seven cell cluster (n = 7).

– The cluster size (n) is not fixed. It depends on the requirements of a particular area.



(S-1027) **Fig. 7.10.3(b) : Cluster**

7.10.2 Bands in Cellular Telephony :

S-09, W-10, S-15, W-16

MSBTE Questions

Q. 1 What is the frequency band used for cellular telephony ? How a mobile call is transmitted and received ? **(S-09, S-15, 4 Marks)**

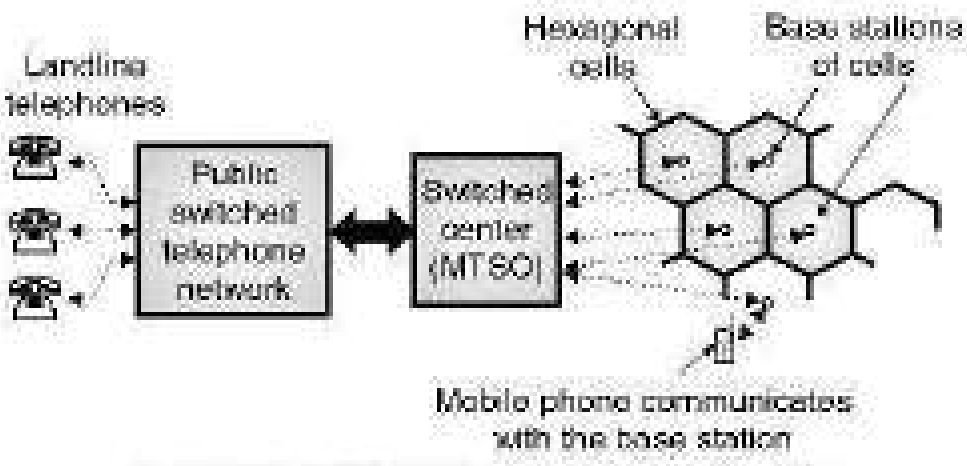
Q. 2 Explain the bands in cellular telephony. **(W-10, 4 Marks)**

Q. 3 State the frequency band used in cellular telephony for transmission and reception. **(W-16, 2 Marks)**

- For the first generation cell phones analog communication was used.
- Frequency Modulation (FM) was used for communication between the mobile phone and the cell office.
- Two frequency bands were allocated for this purpose. One for the communication initiated by the cell phone and the other for the land phone.
- For cellular communications, the FCC has apportioned 40 MHz of the frequency spectrum ranging from 825 to 845 MHz and 870 to 890 MHz.
- One of these bands is used for transmission and the other is used for reception.
- Full-duplex operation is possible by separating transmit and receive signals into separate frequency bands.
- Cellular phone units transmit in the lower band of frequencies i.e. 825 to 845 MHz, and receive in the higher band, 870 to 890 MHz.
- The base unit uses exactly opposite frequency bands at the cell sites.
- Within these two bands, 666 separate channels (333 channels per band) have been assigned for voice and control.
- Each channel occupies a bandwidth of 30 kHz.

7.10.3 Basic Structure of Mobile Phone System :

- In the communication systems discussed so far, the transmitter and the receiver both were stationary.
- In the **mobile communication** which we are going to discuss now, either the transmitter or the receiver or both are going to be movable.
- As the points between which the communication takes place are movable, the communication channel has to be air, that means it is a wireless communication.
- The structure of the mobile phone network alongwith the public switched telephone networks is shown in Fig. 7.10.4.



(S-1028) **Fig. 7.10.4 : Basic structure of mobile telephone network**

Description :

- The mobile telephone system has hexagonal shaped cells as shown in Fig. 7.10.4. Each cell has a base station situated at the center.
- The task of the base stations is to act as an interface between the mobile phone and the cellular radio system.
- The base stations of all the cells are connected to the switched center. Observe that this interface is a bi-directional one. That means the exchange of information between the switched center and the base stations is a two way.
- As shown in Fig. 7.10.4, the communication area of the mobile communication is divided into hexagonal cells. Therefore, the system is named as the cellular radio system.

- The switching center acts as the interface between the Public Switched Telephone Network (PSTN). In addition to that it performs the supervision and control operations in the mobile communication system.
- Due to this kind of a system layout, the communication can take place between two mobile subscribers or between a mobile subscriber and a landline telephone as well.
- If a mobile subscriber travels from one cell area to the other then it automatically gets connected to base station of that cell. Thus the service provided to a mobile subscriber is continuous without any break.

7.10.4 Functions of MTSO :

- The MTSO control all the cells and provides the interface between each cell and the main telephone office.
- As the mobile user from one cell to the next cell the system automatically switches from one cell to the next.
- The computer at MTSO causes transmission from the mobile user to be switched from the weaker cell to the stronger cell within a very short time.

7.10.5 Calls using Mobile Phones :

S-09, W-12, S-15

MSBTE Questions

Q. 1 What is the frequency band used for cellular telephony ? How a mobile call is transmitted and received ? **(S-09, S-15, 4 Marks)**

Q. 2 Explain two cases related to calls using mobile phones :

1. Call initiated by mobile phone
2. A land phone calls a mobile phone.

(W-12, 8 Marks)

Case 1 : Call initiated by a mobile phone :

- When we make a call from the mobile phone by entering the required 10 digit phone number the sequence of events take place as follows :

1. The phone itself scans the band and seeks a channel to set up the call.
2. It sends this number to the closest cell office.
3. The cell office sends this number to MTSO.
4. MTSO sends it to the CTO (central telephone office).
5. If the called person is available, then CTO informs this to MTSO.
6. MTSO will allocate an empty voice channel to the cell phone to establish the connection, and the conversation begins.

(G-1413)

Case 2 : A Land phone calls a mobile phone :

- When the call is initiated by a land phone, the sequence of events is as follows :

1. The telephone central office sends the number to MTSO.
2. The MTSO performs a look up to see the current location of mobile phone sending query signals to all the cells. This is called as paging.
3. The cell where the mobile phone is currently located responds to MTSO.
4. The MTSO then transmits the incoming call signal to that mobile phone.
5. When the mobile phone answers, the MTSO assigns a voice channel to the call and the conversation begins.

(G-1414)

7.10.6 Roaming : S-09, W-09, S-13, S-18

MSBTE Questions

Q. 1 Define : Roaming. **(S-09, 1 Mark)**

Q. 2 Describe the term with respect to cellular telephony : Roaming. **(W-09, S-13, 4 Marks)**

Q. 3 Define the term : Roaming. **(S-18, 2 Marks)**

- Normally the cellular phone is used only within the metropolitan area in which the cellular phone is registered.
- This may include several cities or countries. Frequently there is a need to operate a cellular phone outside the home area.

- This is called **roaming**. Roaming is possible anywhere throughout the country provided that cellular services are available and a prearranged agreement has been made between telephone companies and their users.
- A roam LED indicator on the cellular phone will light when the cellular phone travels outside the home area.
- With new cell coverage being implemented everyday, a cellular phone can be used in virtually every city and village.
- Hence calls can be placed anywhere in the world.

7.11 Essential Features of Cellular Concept :

- The cellular phone system uses the following important features :

  1. Frequency reuse. 2. Cell splitting.

7.11.1 Frequency Reuse :

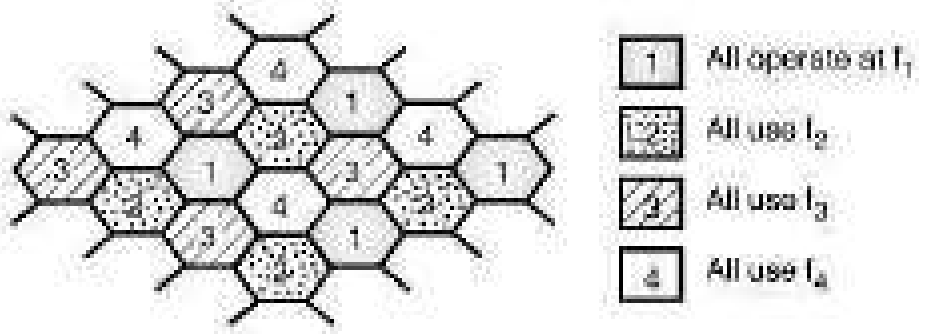
- In frequency reuse concept the radio channels use on the same frequency to cover different areas, that are physically separate from each other.
- In frequency reuse it is necessary to see that the co-channel interference is not objectionable.
- Frequency reuse is an important concept because in this a single transmitter of higher power need not be used to cover the entire area.
- Instead many transmitter of small output power operating at the same frequency can be used.
- This technique also reduces the minimum height of the transmitting antenna, because now each antenna has to cover a small area.
- Frequency reuse is a very important concept of the cellular mobile radio system.
- The users located in different geographical areas i.e. different cells can use the same frequency simultaneously.
- The advantages of frequency reuse is that it drastically increases the spectrum efficiency but the disadvantage is that if the system is not designed properly then **co-channel** interference may take place.

7.11.2 Frequency Reuse Schemes :

- We can use the concept of frequency reuse in either time domain or in the space domain.
- In the time domain the same frequency is used by different users in different time slots.
- This is called as Time Division Multiplexing (TDM).
- There are two categories of frequency reuse in the space domain as follows :

  1. Same frequency is assigned in two different geographic areas. (such as two different cities).
  2. To use the same frequency repeatedly in a same general area in one system. This scheme is popularly used in cellular systems.

- The second scheme is illustrated in Fig. 7.11.1. The total available frequency spectrum is divided into 4 cochannel cell groups in the system as shown in Fig. 7.11.1.



(C-1051) **Fig. 7.11.1 : Frequency reuse**

- The cells marked-1 will use the same frequency say f_1, the cells marked-2 will use same frequency f_2 and so on.

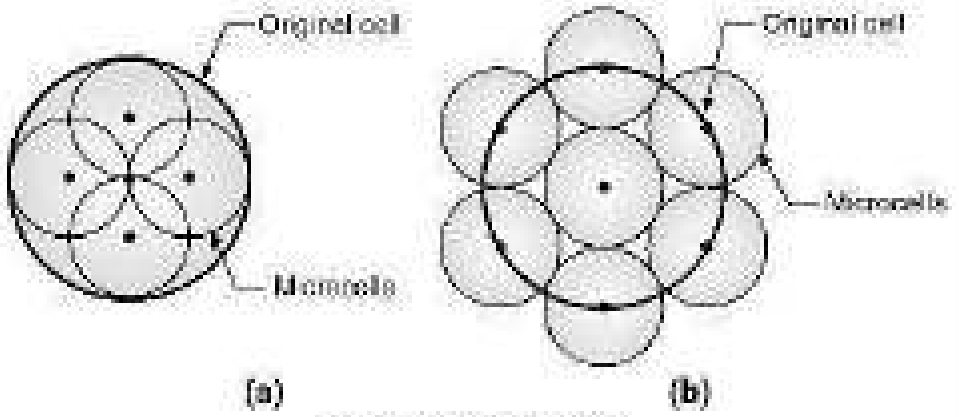
7.11.3 Cell Splitting :

- In order to improve the spectrum efficiency of a cellular mobile systems, we can take the following two steps :

  1. Implement the frequency reuse technique.
  2. Use the cell splitting technique.

- Every cell is supposed to handle a particular value of maximum traffic load.
- But sometimes the load is higher than this maximum permissible traffic which can be handled by a cell.
- Under such circumstances, a technique called cell splitting is used for handling the additional traffic.

- In cell splitting, the cell boundaries are revised in such a way that the local area which was earlier considered as a single cell can now be thought of equivalent to a number of smaller cells.
- These new cells which are smaller than the original cells are called as **microcells.**
- Thus in cell splitting the original cell is split into smaller cells. Generally the radius of a new cell is one half of the original radius as shown in Fig. 7.11.2.



(G-1032) **Fig. 7.11.2**

Splitting techniques :

- There are two splitting techniques :

  1. Permanent splitting. 2. Dynamic splitting.

- The transmitted power and antenna heights of the new base stations are reduced accordingly.
- The same set of frequencies is used again (frequency reuse) as per the new plan.

7.12 Hand Off Procedure :

S-14, S-16, W-16

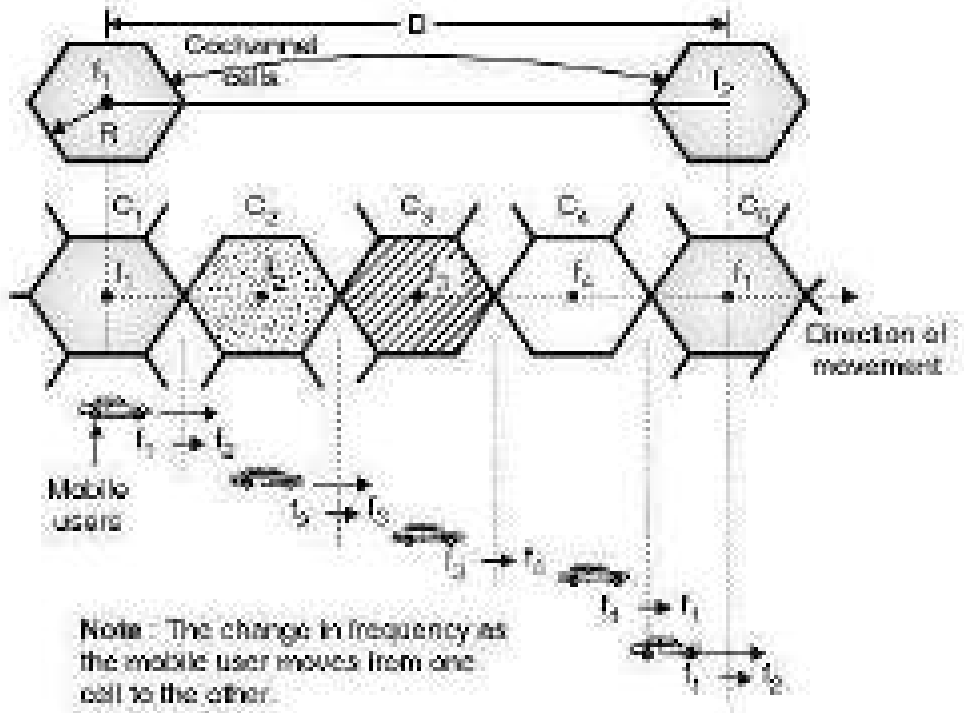
MSBTE Questions

Q. 1 Explain handoff procedure of cellular mobile phone. **(S-14, 4 Marks)**

Q. 2 Name the types of handoffs in mobile communication and describe handoff procedure with suitable diagram. **(S-16, 4 Marks)**

Q. 3 Explain Handoff procedure in mobile communication. **(W-16, 4 Marks)**

- Assume that there is a cell going on between two parties over a voice channel.
- When the mobile unit moves out of coverage area of a particular cell site, the reception becomes weak.
- Then the present cell site will request a hand off.
- The system will switch the call to a new cell site without interrupting the call.
- This procedure is called as the hand off procedure or handover procedure.
- The user can continue talking without even noticing that the hand off procedure has taken place.
- The advantage of hand off procedure is increase in the effectiveness of the mobile system.
- Refer Fig. 7.12.1 to understand the hand off procedure clearly.



(G-1033) **Fig. 7.12.1 : Hand off procedure**

- Fig. 7.12.1 shows two cochannel cells seperated by a distance D and using the frequency f_1.
- Other cells such as C_1, C_2, C_3, C_4, C_5 etc. exist in between the two cochannel using frequency f_1.
- The cells C_1, C_2, C_3 and C_4 use different frequencies f_2, f_3, f_4 and f_5 etc as shown in Fig. 7.12.1.
- Suppose a mobile unit initiates a call in cell C_1 and then moves to cell C_2.
- Then as it starts going away from C_1 the call is dropped and reinitiated in the frequency channel from f_1 and f_2 when the mobile unit (such as car) moves from C_1 to C_2.
- Similarly when the mobile unit moves from cell C_2 to C_3 the frequency is changed automatically from f_2 to f_3 as shown in Fig. 7.12.1.
- The process of changing the frequency is done automatically by the system and the user does not even notice it.

7.12.1 Different Types of Hand Offs :

S-10, S-13, S-15, S-16

MSBTE Questions

Q. 1 Describe the following terms with respect to cellular telephony : Soft hand off. **(S-10, S-13, 4 Marks)**

Q. 2 Describe the following terms with reference to cellular telephony :

1. Hard Hand Off 2. Soft Hand Off

(S-15, 4 Marks)

Q. 3 Name the types of handoffs in mobile communication and describe handoff procedure with suitable diagram. **(S-16, 4 Marks)**

– Following are various types of handoffs, supported by a Mobile Station (MS) :

1. Hard hand off.
2. Soft hand off.
3. Delayed hand off.
4. Forced hand off.
5. Queued hand off.

1. Hard hand off :

– The hand off is known as **hard handoff** if a Mobile Station (MS) transmits between two base stations having different frequency assignments.

2. Soft hand off :

– The hand off is known as soft handoff if the MS starts communication with a new base station without stopping the communication with the older base station.

– In soft handoff the frequencies assigned to the old and new base stations are identical and not different like that in the hard hand off.

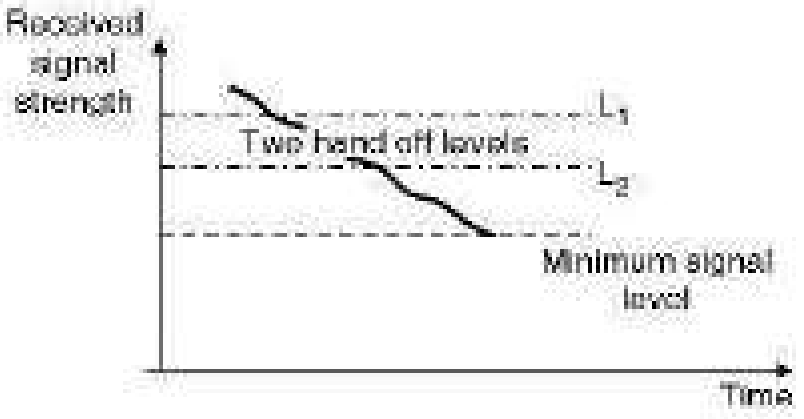
– If the handoff takes place between sectors within a cell then it is known as **softer hand off.**

3. Delayed hand off :

– In many situations, instead of one level, a two level handoff procedure is used, in order to boost the possibility of a successful handoff.

– A hand off can be **delayed** if none of the available cells could take the call.

– Fig. 7.12.2 shows a graph of signal strength with two handoff levels.



(G-1415) **Fig. 7.12.2 : A two level handoff scheme**

– When the signal level drops below the first handoff level, a hand off request is initiated.

– If due to some reason the mobile unit is in a hole (Place in a cell with low signal level) or neighbouring cell is busy then the handoff is requested after every 5 seconds. The L_1 corresponds to this type of request.

– But if the signal strength becomes lower and reaches the second handoff level (L_2) then the handoff will take place without any condition, immediately. Thus L_2 corresponds to the unconditional hand off.

– This process is called as **delayed hand off.**

Advantages :

1. It is possible to delay the handoff if neighbouring cells are busy.
2. Lower number of hand offs are required to be carried out.

   This will allow the processor to handle calls more efficiently.
3. It makes the handoff occur at the proper location and eliminates the possible interference in the system.

4. Forced handoff :

– A **forced handoff** is defined as the hand off which would normally occur but is prevented from happening or a handoff that should not occur but is forced to happen.

5. Queued handoff :

– In the queued handoff process, the MTSO arranges the handoff requests in a queue and does not reject them, if the new cell sites are busy.

- These handoff requests are then processed in a sequential manner.
- Queuing of handoffs is more effective than the two threshold handoff.
- Also, a queuing scheme is effective only when the handoff requests arrive at the MTSO in batches or bundles.

7.13 Various Generations of Mobile Phones :

I-Scheme : W-19

- The **first generation wireless networks** are based on analog technology and they are used only for analog voice services.
- The **second generation wireless systems (2G)** employ digital modulation and advanced call processing capabilities.
- Typical examples include Global System for Mobile (GSM), cordless telephone (CT2) etc.
- The **third generation wireless systems (3G)** are developed to provide universal access throughout the world.
- They have used broadband ISDN to provide access to information networks like internet, communications using Voice Over
- Internet Protocol (VoIP), voice-activated calls etc.
- The **fourth generation wireless systems (4G)** are currently under deployment but continue to evolve.
- The next generation cellular networks have been designed to support high speed data communications traffic in addition to the voice calls.
- The new technologies and standards are being implemented so that the wireless networks can replace the fiber optic or copper cables.
- The wireless networks are used as replacement for wires within offices, buildings, homes with the use of **Wireless Local Area Networks (WLANs).**
- The **Bluetooth** modem standard can connect several devices with invisible wireless connections within a person's personal workspace.
- It was conceived as a wireless alternative to RS232 cables.
- WLANs and Bluetooth use low power levels. They don't need a license for spectrum use.
- They are used for adhoc wireless communication of voice and data anywhere in the world.

7.14 First Generation : Analog Voice :

I-Scheme : S-22

- The first generation of cellular telephony was suitable only for voice communication using analog signals.
- Now cellular technology is in the fourth generation.
- One of the important first generation mobile system used in North America is AMPS.
- The first generation of wireless mobile system was implemented in 1980's. The modulation scheme used was frequency modulation (FM).
- Long form of AMPS is Advanced Mobile Phone System. It is one of the leading analog cellular system in North America.
- It makes use of FDMA (Frequency Division Multiple Access) to separate channels in a link.

Frequency bands :

- AMPS uses the ISM 800-MHz band for its operation. It uses two separate channels for forward i.e. base station to mobile station and for reverse i.e. from mobile station to base station communication.
- The frequency bands allotted for the forward and reverse communication are as follows :
- Reverse Communication : 824 MHz to 849 MHz.
- Forward Communication : 869 MHz to 894 MHz.
- Each band has been divided into 832 channels. But two providers are allowed to share an area.
- That each provider is allowed to use 416 channels in each cell.
- Out of 416, 21 channels are used for control and the remaining 395 channels for information.

Transmission :

- AMPS makes use of FSK and FM systems for modulation. FM stands for frequency modulation while FSK is frequency shift keying.
- FM is used for the modulation of voice signals whereas FSK is used for the control channels.
- The coverage area of first generation systems was 2100 square km.
- The other 1G technologies developed to provide only analog voice communication were Nordic Mobile Telephone (NMT) and Total Access Communication System (TACS).
- 1G technology was developed only for providing the voice communication but **paging networks** also are considered as 1G technology.
- Pager system provides only one way messaging.

7.14.1 Drawbacks of 1G System :

1. Poor voice quality.
2. No security.

7.14.2 Features of First Generation :

St. No.	Feature	Value / Description
1.	Generation	1G (1970 – 1984)
2.	Technology	Analog cellular
3.	Standard	AMPS
4.	Switching	Circuit switching
5.	Frequency band	824-894 MHz
6.	Modulation	FM
7.	Data speed	2.4 kbps
8.	Multiplexing	FDMA
9.	Core network	PSTN
10.	Service	Only voice or only message

7.15 Second Generation : Digital Voice :

I-Scheme : S-22

- The second generation of cellular telephony was developed in order to improve the quality of communication.
- The second generation was designed for digital voice.
- 2G networks began to emerge around 1980's but their actual implementation started by 1990's.
- The second generation mobile systems are digital systems and it has the following types of developments :
  1. IS-54 (TDMA) in 1991.
  2. IS-95 (CDMA) in 1993.
  3. IS-136 in 1996.
  4. GSM (TDMA).
- Out of these the GSM (Global system for mobile communications) is by far the most consistant 2G standard.
- 2.5G and 2.75G are the upgraded versions of 2G.

7.15.1 Services :

- The 2G family of systems provides the following services :
  1. Digital voice.
  2. Web.
  3. E-mails.
  4. Browsing.

7.15.2 Performance :

- Although 2G systems provided a huge improvement over 1G and increased the number of subscribers the standards were poor.
- 2G systems were unable to handle complex data and they could not use the available bandwidth efficiently.

7.15.3 Features of 2G Systems :

- Some of the important features of the 2G-mobile systems are as follows :

Sr. No.	Feature	Value / Description
1.	Generation	2G (1990)
2.	Technology	Digital Cellular Technology
3.	Standard	CDMA, TDMA and GSM

Sr. No.	Feature	Value / Description
4.	Switching	Circuit/packet switching
5.	Frequency band	850 - 1900 MHz (GSM)
6.	Data speed	9.6 kbps.
7.	Multiplexing	CDMA, TDMA
8.	Modulation	GMSK
9.	Core network	PSTN
10.	Services	Digital voice, Data and SMS facility
11.	Handoff	Horizontal

7.16 Third Generation : Digital Voice and Data :

I-Scheme : S-22

- The third generation of wireless mobile communication systems have been developed to meet the International Mobile Telecommunication - 2000 (IMT - 2000) specifications which are defined by International Telecommunications Union (ITU).
- The 3G systems have evolved due to the need for high speed, fast data transmission and better quality of service (QoS).
- The 3G systems were launched in 2001 and it provides the network for transporting rich **multimedia** contents.
- The 3G systems use circuit switching technology for voice calls/SMS facility, whereas they use the packet switching for the high speed data.
- The will known examples of 3G systems are :
  1. W-CDMA
  2. CDMA - 2000
  3. TD - SCDMA
- 3G systems are compatible with the other cellular standards like CDMA, GSM and TDMA.
- The frequency range used by the 3G standards is 2100 MHz and it has a bandwidth of 15-20 MHz.
- 3G standards facilitate the users to use high speed internet services, as well as video chatting.
- The international roaming has become possible due to 3G standard.
- Universal Mobile Telecommunications System (UMTS) was adopted by Europe which uses W-CDMA as its standard.
- UMTS is based on the GSM infrastructure. Hence UMTS is the most popular 3G technology.

7.16.1 Features of Third Generation :

- Some of the important features of 3G mobile systems are as follows :

Sr. No.	Feature	Value / Description
1.	Generation	3G (2001)
2.	Technology	Broadband/IP, FDD, TDD
3.	Standards	CDMA, W-CDMA, UMTS.
4.	Switching	Circuit/Packet switching
5.	Frequency band	1.6 GHz to 2.5 GHz
6.	Data speed	2 Mbps
7.	Multiplexing	CDMA
8.	Core network	Packet network
9.	Services	High speed data, voice, video
10.	Handoff	Horizontal

7.17 Fourth Generation (4G) :

I-Scheme : S-22

- The 4G wireless systems were designed to fulfill the requirements of International Mobile Telecommunications Advanced (IMT-A) using IP (Internet Protocol) for all the services.

7.17.1 Applications of 4G :

- The 4G is developed to support the QoS and data rate requirements of the advanced applications such as :
  1. Wireless broadband access.
  2. Multimedia Messaging Service (MMS).
  3. Video chat.
  4. Mobile TV.

5. HDTV
6. Digital Video Broadcasting (DVB).
7. Voice and data.
8. Other services which need large bandwidth.

- In 4G systems, an advanced radio interface is used with Orthogonal Frequency Division Multiplexing (OFDM), Multiple
- Input Multiple Output (MIMO) and the link adaptation technologies.
- 4G standards also includes **Long Term Evolution (LTE)** and IEEE 802.16 (Wi-Max).
- The 4G systems provide very high data rates as compared to 3G. But the major problem with 4G systems is security because of its IP address system.

7.17.2 Features of 4G Systems :

- The important features of 4G mobile systems are as follows :

Sr. No.	Feature	Value / Description
1.	Generation	4G (2010)
2.	Technology	IP-Broadband, Wi-Fi, MIMO
3.	Standard	Wi Max and LTE
4.	Switching	Packet switching
5.	Frequency band	2 GHz – 8 GHz
6.	Data speed	50 Mbps
7.	Multiplexing	MC-CDMA and OFDM
8.	Core network	Internet
9.	Service	Dynamic Information Access
10.	Handoff	Vertical

7.17.3 Comparison of Various Mobile System Generations :

Sr. No.	Feature	Generation			
		1G	2G	3G	4G
1.	Generation	First	Second	Third	Fourth
2.	Year of introduction	1970	1990	2001	2010
3.	Technology	Analog cellular	Digital cellular	Broadband, IP, FDD, TDD	IP-broadband Wi-Fi, MIMO
4.	Standard	AMPS	CDMA, TDMA, GSM	CDMA, UMTS, W-CDMA	Wi-Max and LTE
5.	Switching	Circuit	Circuit/packet	Circuit/Packet	Packet
6.	Frequency band	824-894 MHz	850-1900 MHz	1.6-2.5 GHz	2-8 GHz
7.	Data speed	2.4 kbps	9.6 kbps	2 Mbps	50 Mbps
8.	Multiplexing	FDMA	CDMA, TDMA	CDMA	MC-CDMA OFDM
9.	Core network	PSTN	PSTN	Packet Network	Internet
10.	Services	Only voice or only message	Digital voice, Data, SMS	High speed data, Voice, Video	Dynamic Information Access.

7.18 Next Generation Mobile Communication :

- Following are few possible new developments in the field of mobile phones :

1. Digital cellular telephone.
2. Integration of cell phone and satellite communication.
3. Integration of cell phone and PC.

- The combination of cell phone and satellite communication will enable the user to have same telephone number throughout the world.
- The numbers for mobile and land phone would be the same.
- The combination of mobile phone and PC is called as Mobile Personnel Communication.
- This will enable the users to use a small mobile PC and communicate multimedia information in all the possible forms that is data, voice, image or video.

7.18.1 Next Possible Generation (5G) :

- The 4G technology has now been deployed and the research for the next generation named as 5G has already begun.
- It is considered to be the next major phase of mobile telecommunication standard after 4G.
- The 5G standard will be made commercially available by 2020. This standard is way beyond just the faster data speeds or faster mobile devices.
- Instead 5G will provide an access to high and low speed data services. It will involve combination of existing and evolving systems.

Requirements for 5G networks :

- The next generation Mobile Networks Alliance defines the following requirements for 5G networks.
  1. Very high data rates of several tens of Gbps.
  2. Several hundreds of thousands of simultaneous connections.
  3. Enhanced spectral efficiency than 4G.
  4. Improved coverage.
  5. Improvement in signaling efficiency.
  6. Latency should be reduced significantly.
  7. The 5G network should be supported by the technologies such as LAS-CDMA (Large Area Synchronized CDMA), OFDM, MCCDMA, Smart antennas, World Wide Wireless Web (WWWW) and many more.

Services :

- The 5G systems will provide services like interactive multimedia, voice over IP, HD videos, Internet and other high quality services.
- 5G may also provide support for use of various types of sensors, Internet of things, Virtual Reality (VR) and Augmented Reality (AR).

Features of fifth generation :

Sr. No.	Feature	Value / Description
1.	Generation	5G (2020)
2.	Technology	WWWW, IPv6
3.	Standard	Yet to be finalized
4.	Switching	Packet
5.	Frequency	15 GHz
6.	Data speed	> 1 Gbps
7.	Multiplexing	MC-CDMA, LAS-CDMA, OFDM
8.	Core network	Internet
9.	Services	Interactive multimedia, Voice over IP, Virtual reality, Augmented reality, IOT etc.
10.	Handoff	Horizontal and vertical

Review Questions

Q. 1 Explain the basic configuration of wireless LAN.

Q. 2 Define BSS and ESS.

Q. 3 Explain different types of stations in ESS.

Q. 4 Write a short note on physical layer specifications of IEEE 802.11.

Q. 5 Explain IEEE 802.111 FHSS.

Q. 6 Explain the principle of IEEE 802.11 DSSS.

Q. 7 Write a short note on MAC layer specification for IEEE 802.11.

Q. 8 Define DCF and PCF.

Q. 9 Explain the architecture of wireless LAN 802.11 with suitable diagram.

Q. 10 Compare : Ethernet and Wireless networks.

Q. 11 What is Bluetooth ?

Q. 12 Explain the architecture of Bluetooth.

Q. 13 List the Bluetooth devices.

Q. 14 Explain the frame format of Bluetooth.

Q. 15 State the advantages and applications of Bluetooth.

Q. 16 Compare : Bluetooth and wireless LAN.

Q. 17 What is cellular communication ?

Q. 18 State the frequency bands used for mobile communication.

Q. 19 Explain the basic principle of mobile communication.

Q. 20 Explain the transmit, receive, hand off operations.

Q. 21 Explain the procedure followed to make calls using a mobile phone.

Q. 22 Name the cellular access technologies.

Q. 23 State functions of MTSO.

Q. 24 What are the new developments expected in the field of mobile communication ?

Q. 25 Explain the concept of mobile communication.

Q. 26 Define the following :

1. Cell.
2. Cluster.

Q. 27 What is frequency reuse ?

Q. 28 Explain the concept of handoff in mobile communication.

Q. 29 Explain about the first generation mobile communication systems.

Q. 30 State the features of 2G mobile systems.

Q. 31 State the following for 3G mobile systems :

(a) Standards.

(b) Frequency band.

(c) Multiplexing.

Q. 32 What are the applications of 4G mobile systems ?

Q. 33 State the important features of 4G.

Q. 34 Compare various generations of mobile systems.

Q. 35 What is VoLTE ? Explain its principle of operation.

Q. 36 How VoLTE is superior to the 2G/3G mobile systems for voice communication ?

Q. 37 What are the services offered by VoLTE ?

Q. 38 State the features of VoLTE.

Q. 39 Explain the requirements of the 5G system.

Q. 40 State the important features of the 5G system.

7.19 MSBTE Questions and Answers :

Q. 1 Define the term : AMPS. **(S-09, W-09, 1 Mark)**

Ans. :

AMPS :

– Many mobile radio standards have been developed for wireless systems throughout the world. Some of the important ones are AMPS, NAMPS, IS95 or GSM.

– All these mobile standards are developed in North America. The specification of the AMPS system are as follows :

Feature / Standard	Type	Introduced in the year	Multiple access method	Type of modulation	Frequency bands used	Channel bandwidth
AMPS	Cellular	1983	FDMA	FM	824-894 MHz	10 kHz

7.20 I-Scheme Questions and Answers :

Summer 2019 [Total Marks - 06]

Q. 1 List IEEE 802 X standards for networks. **(2 Marks)**

(Section 7.1.1)

Q. 2 Describe various IEEE standards for network topologies. **(Section 7.1.1)** **(4 Marks)**

Winter 2019 [Total Marks - 16]

Q. 3 Classify mobile generations.

(Section 7.13) **(2 Marks)**

Q. 4 Explain wireless LAN 802.11 architecture.

(Sections 7.4.1, 7.4.2 and 7.4.3) **(4 Marks)**

Q. 5 Explain various IEEE communication standards.

(Section 7.1.1) **(4 Marks)**

Q. 6 Describe Bluetooth architecture technologies.

(Sections 7.9.2 and 7.9.3) **(6 Marks)**

Summer 2022 [Total Marks - 12]

Q. 7 Explain 802.11 architecture.

(Sections 7.4 and 7.4.1) **(4 Marks)**

Q. 8 Explain Bluetooth architecture.

(Sections 7.9.2 and 7.9.3) **(4 Marks)**

Q. 9 Describe various mobile generations in detail.

(Sections 7.14, 7.15, 7.16 and 7.17) **(4 Marks)**

❑❑❑

Chapter 8

Network Topologies

Syllabus

Network topologies - Introduction, Definition, Selection criteria, Types of topology : 1. Bus 2. Ring 3. Star 4. Mesh 5. Tree 6. Hybrid

Chapter Contents

8.1 Introduction :

- Earlier we have discussed the basic concepts of Local Area Network (LAN).
- It is possible to connect the computer in many different ways in a LAN.
- The way of connecting the computers is called as the topology.
- So depending on the manner of connecting the computers we can have different network topologies.
- In this chapter we are going to discuss some of the important network topologies.

8.2 Network Topology Types :

8.2.1 Definition :

S-03, W-03, W-04, S-06, S-08, W-12, S-13, S-15, S-16

MSBTE Questions

Q. 1 Describe network topology. Draw star bus topology connecting three star networks, each star network consists of four computers. **(S-03, W-03, W-04, 4 Marks)**

Q. 2 Define network topology. **(S-06, 2 Marks)**

Q. 3 Define the term topology. Give names of any two topology. **(S-08, 2 Marks)**

Q. 4 Describe network topology. Explain mesh topology in detail with suitable diagram. **(W-12, 4 Marks)**

Q. 5 Define the term : Topology. **(S-13, 4 Marks)**

Q. 6 Define the term 'Topology'. List the names of any two network topologies. **(S-15, 2 Marks)**

Q. 7 Define network topology. List types of network topologies. **(S-16, 2 Marks)**

Definition :

- Topology is defined as the logical arrangement of the nodes (computers).
- The word physical network topology is used to explain the manner in which a network is connected.
- Devices or nodes in a network get connected to each other via communication links and all these links are related to each other in one way or the other.
- The geometric representation of such a relationship of links and nodes is known as the topology of that network.

8.2.2 Types :

S-08, W-09, W-10, W-11, S-15, W-15, S-16, S-17, I-Scheme : W-19

MSBTE Questions

Q. 1 Define the term topology. Give names of any two topology. **(S-08, 2 Marks)**

Q. 2 List types of network topology. **(W-09, 2 Marks)**

Q. 3 State any four topology. **(W-10, S-17, 2 Marks)**

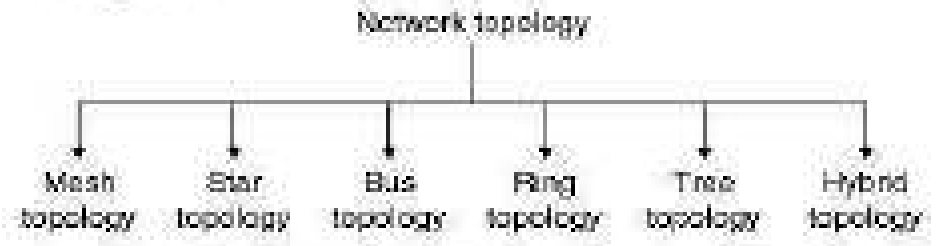
Q. 4 List down the topologies used in LAN. Explain star topology in detail. **(W-11, 8 Marks)**

Q. 5 Define the term 'Topology'. List the names of any two network topologies. **(S-15, 2 Marks)**

Q. 6 List types of network topology. Name one device used in star topology. **(W-15, 2 Marks)**

Q. 7 Define network topology. List types of network topologies. **(S-16, 2 Marks)**

- The six basic network topologies are as shown in Fig. 8.2.1.



(S-14(b)) **Fig. 8.2.1 : Classification of network topology**

- These topologies can be classified into two types :
  1. Peer to peer.
  2. Primary – secondary.
- Peer to peer is the relationship where the devices share the link equally. The examples are ring and mesh topologies.
- In Primary – secondary relationship, one device controls and the other devices have to transmit through it. For example star and tree topology.

Note : An important point to be kept in mind is that the topology refers to the logical arrangement of the nodes (computers) and not the physical appearance. So sometimes a network which physically looks like a STAR may have a Bus topology when examined logically.

Switching :

- Switching is a technique of connecting computers (nodes) to a central node called switch. A switch can then be used to connect these nodes to the other nodes.

- Without switching we would need to connect every computer in the world to every other computer using separate wires.
- Practically it will not be possible to do due to the number of wires required to be used and the associated unreliability.

8.2.3 Selection Criteria for Topologies :

W-14, S-16, W-16

MSBTE Questions

Q. 1 Give any four selection criteria for selecting network topology. **(W-14, 6 Marks)**

Q. 2 List and describe criteria for selection of network topology. **(S-16, 4 Marks)**

Q. 3 Give two criteria for selection of network topologies. **(W-16, 2 Marks)**

- Each network topology mentioned thus far has its own advantages and disadvantages.
- Hence the selection of a topology depends on the needs of the particular application.
- Following are some of the selection criteria for selecting a topology for an application :

1. Size of the network and number of devices (nodes) being connected.
2. Ease of configuration and installing.
3. The ease of adding a new device (user) in an existing network.
4. The ease of fault indication and rectification.
5. Number of physical links required to be used for connecting the devices.
6. Whether connecting devices such as repeaters, switches, hubs etc are required or not.
7. Costs involved.
8. Need of data security.
9. Need of network administration.

8.3 Bus Topology :

W-05, S-15, W-15, S-16, W-16, I-Scheme : S-22

MSBTE Questions

Q. 1 State whether bus is active or passive network justify. **(W-05, 4 Marks)**

Q. 2 State whether the bus is active or passive Network. Justify your answer. **(S-15, 2 Marks)**

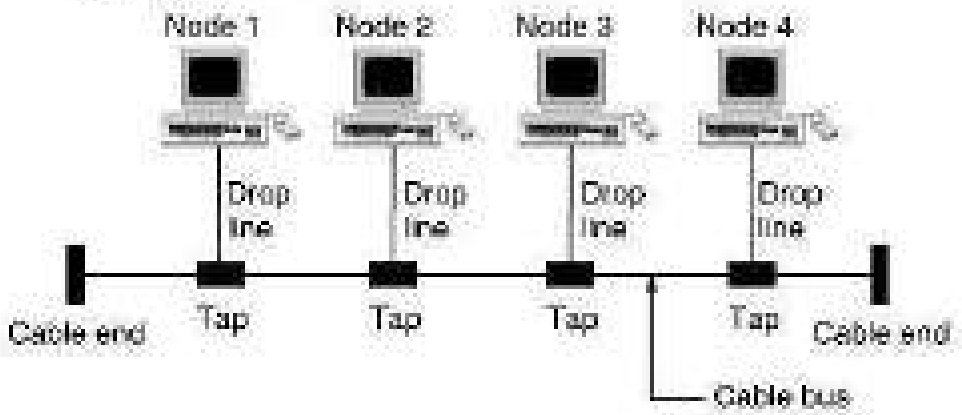
Q. 3 State any two advantages of bus topology. Explain whether adding more computers in bus topology affects performance of network. **(W-15, 4 Marks)**

Q. 4 Draw the sketch of bus topology and explain. **(S-16, 4 Marks)**

Q. 5 Draw a neat sketch of bus topology and describe its working. Give its advantages. **(W-16, 4 Marks)**

Definition :

- The bus topology is a network topology in which nodes are directly connected to the common linear or branched half duplex link called as bus.
- The bus topology is usually used when a network under consideration is small, simple or temporary as shown in Fig. 8.3.1.



(S-15)**Fig. 8.3.1 : Bus topology**

- On a typical bus network a simple cable is used without additional electronics to amplify the signal or pass it along from computer to computer. Therefore bus is a **passive topology.**
- This long cable called bus is used as backbone to all the nodes. The tap is connector that connects the node to the metallic core of the bus via a drop line.

Working :

- When one computer sends a signal on the cable, all the computers on the network receive the information.
- However only the one with the address that matches with the destination address stored in the message accepts the information while all the others reject the message.
- The speed of the bus topology is **slow** because only one computer can send a message at a time.
- A computer must wait until the bus is free before it can transmit.
- The bus topology requires a proper termination at both the ends of the cable in order to avoid reflections.

- Since the bus is a passive topology, the electrical signal from a transmitting computer is free to travel over the entire length of the cable.
- Without termination when the signal reaches the end of the cable, it returns back and travels back on the cable.
- The transmitted waves and reflected waves, if they are in phase add and if they are out of phase cancel.
- Thus addition and cancellation of wave results in a standing wave.
- The standing waves can distort the normal signals which are travelling along the cable.
- This can be avoided by terminating the bus on both ends in 50 Ω load.
- The terminators absorb the electrical energy and avoid reflections.
- As the signal travels across the bus, some of the energy is converted into heat. This will weaken the signal. This will limit the number of taps and the distance between them.
- Hence the bus topology cannot be used for very large networks that contain a number of computers.
- The bus topology is easy to install and uses less cable than the mesh, star or tree topology.
- Addition of a new node to the bus topology is difficult because this will change the number of taps and average distance between them.
- The number of taps and the distance between them is optimized so it is not supposed to be changed. Thus Bus topology is inflexible.
- It is very difficult to isolate a fault or faulty node. One more drawback is that even if a part of bus breaks down, the whole bus stops functioning.

8.3.1 Performance of Bus Topology :

W-04, W-15

MSBTE Questions

Q. 1 Explain whether adding more computers in Bus topology affects performance of network. **(W-04, 2 Marks)**

Q. 2 State any two advantages of bus topology. Explain whether adding more computers in bus topology affects performance of network. **(W-15, 4 Marks)**

- Adding more computers in bus topology affects performance of the network because :
  1. With increase in number of computers, the waiting time for each computer increases which makes the network traffic slow.
  2. The number of packet collisions increases which results in high amount of packet loss.

8.3.2 Characteristics of the Bus Topology :

- Following are some of the important characteristics of the bus topology :

1. This is a multipoint configuration. There are more than two devices connected to the medium and they are capable of transmitting on the medium. Hence the Medium Access Control (MAC) is essential for the bus topology.
2. The signal strength of the transmitted signal should be adequately high so as to meet the minimum signal strength requirements of the receiver.
3. Adequate signal to noise ratio (SNR) should be maintained for better quality reception.
4. The signal should not be too strong. This is necessary to avoid the overloading of transmitter and hence the possibility of signal distortion.
5. This is called as signal balancing which is not an easy task at all. Specially the signal balancing becomes increasingly difficult with increase in the number of stations.

8.3.3 Transmission Media for Bus LANs :

- We can use the following transmission media for the bus LANs :
  1. Twisted pair.
  2. Baseband co-axial cable.
  3. Broadband co axial cable.
  4. Optical fiber.

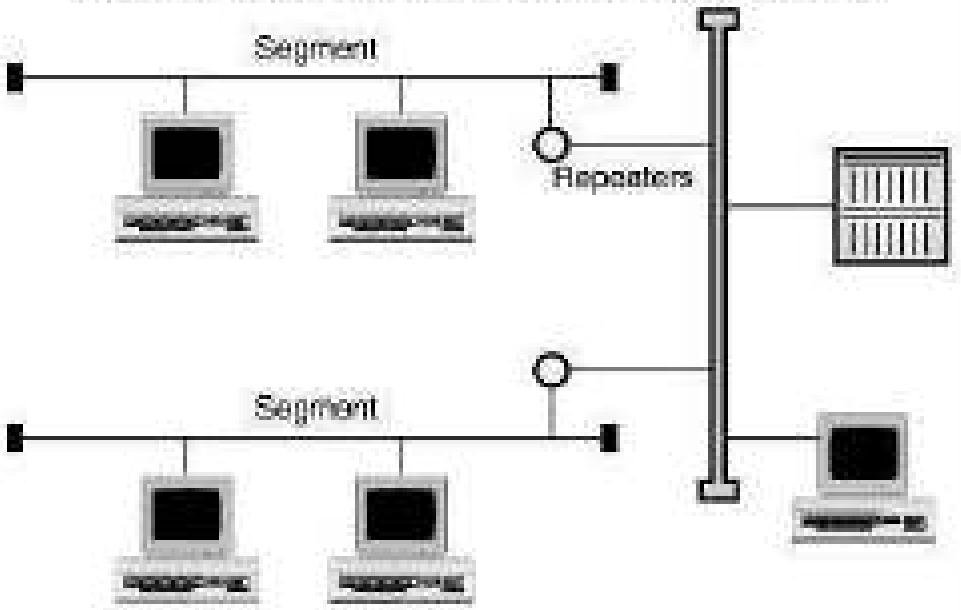
8.3.4 Repeaters : W-05

MSBTE Questions

Q. 1 Explain the use of repeater in bus topology. **(W-05, 2 Marks)**

- It is possible to extend the length of the network by using the repeaters.

- The bus repeaters are special type devices which can transmit and receive in both the directions.
- A repeater is connected between two segments of cables and it allows the signal to flow in both the directions.
- Fig. 8.3.2 shows a multiple segment baseband bus LAN using repeater to connect the segments to the bus.



(G-1353) **Fig. 8.3.2 : Multiple segment baseband bus LAN**

8.3.5 Use of BNC Barrel Connector : W-03

MSBTE Questions

Q. 1 Explain the use of BNC barrel connector in Bus topology. **(W-03, 2 Marks)**

- The coaxial cable is used as the transmission medium and to connect it to devices we need to use co-axial connectors.
- The most common type of connector used for a coaxial cable is Bayone-Neill-Concelman or BNC connector.
- The three types of BNC connectors are :
  1. BNC connector.
  2. BNC T connector.
  3. BNC terminator.
- The BNC connector is used to connect the end of the cable to a device such as TV set.
- The BNC T connector is used in Ethernet (LAN) networks, so as to branch out a cable for connection to a computer or other devices.
- Thus it is a T shaped connector. To the one leg of T an incoming cable is connected and to the remaining two legs we can connect the outgoing cables. This is branching.
- The BNC terminator is used at the end of cable to avoid reflection of the signal.

8.3.6 When to Use the Bus Topology ? W-09

MSBTE Questions

Q. 1 You need to link a small number of computers in a room into a training exercise. This will be a temporary network and low cost which network topology is appropriate for this situation ? Justify. **(W-09, 4 Marks)**

- The bus topology is preferred if :

1. The given network is small, simple or temporary.
2. Number of computers to be connected is small.
3. The cost involved are to be kept low.

8.3.7 Features :

1. It is an inexpensive topology.
2. Easy to install.
3. Preferred for small networks.
4. It needs to be properly terminated.
5. It slows down in the event of heavy traffic.
6. Medium Access control (MAC) is necessary.
7. Requires less cable length.
8. It is difficult to isolate faults on the network.
9. Entire network shuts down if there is a break in the main cable.

8.3.8 Advantages of Bus Topology :

W-03, W-04, S-10, S-13, W-15, W-16, S-18

MSBTE Questions

Q. 1 State any two advantages of bus topology. **(W-03, W-04, S-18, 2 Marks)**

Q. 2 State four advantages of bus topology. **(S-10, 4 Marks, S-13, 2 Marks)**

Q. 3 State any two advantages of bus topology. Explain whether adding more computers in bus topology affects performance of network. **(W-15, 4 Marks)**

Q. 4 Draw a neat sketch of bus topology and describe its working. Give its advantages. **(W-16, 4 Marks)**

1. The bus topology is easy to understand, install, and use for small networks.
2. The cabling cost is less as the bus topology requires a small length of cable to connect the computers.
3. The bus topology is easy to expand by joining two cables with a BNC barrel connector.
4. In the expansion of a bus topology repeaters can be used to boost the signal and increase the distance.

8.3.9 Disadvantages of Bus Topology :

S-05, W-14

MSBTE Questions

Q. 1 State any two disadvantages of bus topology. **(S-05, 2 Marks)**

Q. 2 List any two disadvantages of bus topology. **(W-14, 2 Marks)**

1. Heavy network traffic slows down the bus speed. In bus topology only one computer can transmit and other have to wait till their turn comes and there is no co-ordination between computers for reservation of transmitting time slot.
2. The BNC connectors used for expansion of the bus attenuates the signal considerably.
3. A cable break or loose BNC connector will cause reflections and bring down the whole network causing all network activity to stop.

Note : A bus network behaves erratically if it is not terminated or improperly terminated.

8.4 Ring Topology :

S-08, W-08, S-09, S-12, W-12, I-Scheme : S-19, S-22

MSBTE Questions

Q. 1 Under what circumstances ring topology is most suitable ? Name all devices used in establishing ring topology. **(S-08, S-12, 4 Marks)**

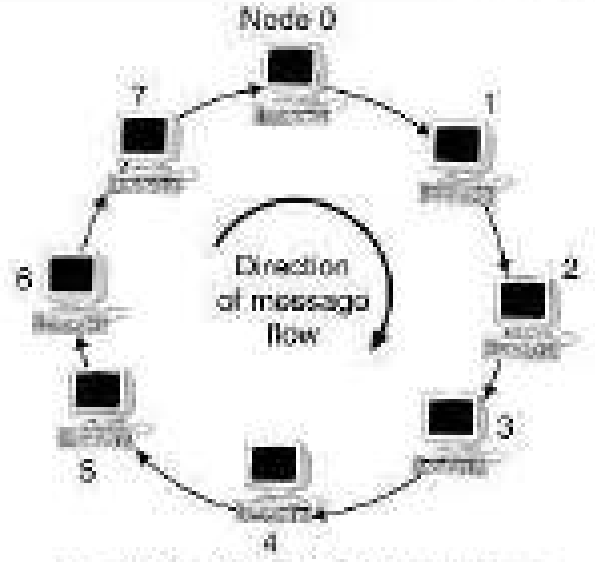
Q. 2 Explain the working of ring topology with neat sketch. **(W-08, 4 Marks)**

Q. 3 Discuss token passing for network systems. **(S-09, 8 Marks)**

Q. 4 State two disadvantages of ring. Whether ring network is active or passive network ? Justify your answer. **(W-12, 4 Marks)**

Definition :

- A ring topology is a network topology in which each node connects exactly to two other nodes, to form a single closed pathway for signal through each node.
- Data travels from node to node with each node having an access to every packet.
- In a ring topology, each computer is connected to the next computer, with the last one connected to the first as shown in Fig. 8.4.1.
- Rings are used in high performance networks where large bandwidth is necessary e.g. time sensitive features such as video and audio.



(G-16) **Fig. 8.4.1 : Ring topology**

- Every computer is connected to the next computer in the ring and each retransmits what it receives from the previous computer hence the ring is an active network.
- The messages flow around the ring in one direction. There is no termination because there is no end to the ring.

Token passing :

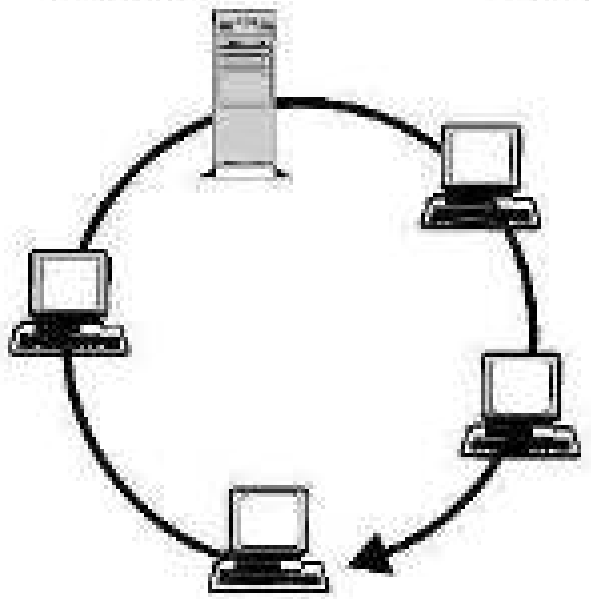
- Some ring networks do **token passing.** A short message called a **token** is passed around the ring until a computer wishes to send information to another computer.
- That computer modifies the token, adds an electronic address and data and sends it around the ring.
- Each computer one by one receives the token and the information and passes them to the next computer until either the electronic address matches the address of a computer or the token returns to its origin.
- The receiving computer returns a message to the sender to indicate that the message has been received.
- The sending computer then creates another token and places it on the network, so as to allow another computers to grab the token and begin their transmission.
- The token circulates until a station is ready to send and capture the token. Faster networks circulate several tokens at once.
- Some ring networks have two counter-rotating rings that help them recover from network faults.
- A ring is very easy to reconfigure and install and the signal keeps circulating over the ring all the time.
- A node which does not receive a signal for a long time indicates that it is faulty. This makes the fault detection easy.

- But if a node in a ring network fails, then the whole ring becomes inoperative.
- To overcome this problem, sometimes a ring topology with **dual rings** is used.
- Another disadvantage of ring is that the flow of information is only in one direction.
- So the ring topology is not used if a large number of nodes are to be connected in a network.

Active or passive ?

- Ring topology is an active topology, because each station has to recreate the packet.

Ex. 8.4.1 : Identify the topology shown in Fig. P. 8.4.1. Comment on whether this topology is active or passive. **S-05, 2 Marks**



(G-27) **Fig. P. 8.4.1**

Soln. : This is the ring topology. The ring topology is an active network.

8.4.1 Features of Ring Topology :

S-08, W-08, S-09, S-12, W-12

MSBTE Questions

Q. 1 State the features of ring topology. **(W-06, 4 Marks)**

- It is very easy to install and reconfigure.
- Better performance than bus, under heavy loads.
- Fault identification and isolation is easy.
- Ring is an active topology.
- Long delays.
- Failure of ever one node will affect the entire network.
- It is suitable for high performance, large, BW networks.
- Ring topology is defined by IEEE 802.5 standard.

8.4.2 Transmission Medium for Ring Topology :

- It is possible to use twisted pair, baseband co-axial cable and fibre optic cable for the link connecting the repeaters.
- The broadband co-axial cable cannot be easily used.

8.4.3 Problems Faced in the Ring Topology :

S-11, S-17

MSBTE Questions

Q. 1 Give the problems faced in ring topology. **(S-11, S-17, 2 Marks)**

1. If any link breaks or if any repeater fails then the entire network will be disabled.
2. To install a new repeater for supporting a new device, it is necessary to have the identification of two nearby, topologically adjacent repeaters.
3. It is necessary to take preventive measures to deal with the time jitter.
4. Due to the closed nature of the ring topology it is necessary to remove the circulating packets.

- These problems except for the fourth one can be rectified by refinements of the ring topology.

8.4.4 Advantages of Ring Topology :

1. Every computer gets an equal access to the token.
2. There are no standing waves produced.
3. It is very easy to reconfigure and install.
4. Ring performs better than a bus under heavy network load.
5. Point to point configuration makes it easy to identify and isolate faults.

8.4.5 Disadvantages of Ring Topology :

W-06, W-12

MSBTE Questions

Q. 1 State the drawbacks of ring topology. **(W-06, 4 Marks)**

Q. 2 State two disadvantages of ring. Whether ring network is active or passive network ? Justify your answer. **(W-12, 4 Marks)**

1. Failure of one computer on the ring can affect the whole network.
2. It is difficult to trouble shoot the ring topology.

3. Adding or removing the computers in an existing ring is difficult. It disturbs the network.
4. Communication delay is directly proportional to the number of nodes, connected in the network.
5. Bandwidth is shared on all links between devices.
6. Ring is more difficult to configure than star.

Note : Token ring networks are defined by the IEEE 802.5 standard. Fiber Distributed Data Interface (FDDI) is a fast fiber-optic network based on the ring topology.

8.5 Star Topology :

W-04, S-07, S-09, W-09, S-10, S-11, W-11, S-14, W-14, W-15, W-16, S-18, I-Scheme : S-19

MSBTE Questions

Q. 1 In which situation Star Network is most suitable ? Explain how message is transmitted from one computer to another in broadcast star network ? **(W-04, 4 Marks)**

Q. 2 Under what circumstances star topology is most suitable ? Name all devices used in establishing a star topology. **(S-07, 4 Marks)**

Q. 3 Draw neat sketches of star network topology and explain. **(S-09, 2 Marks)**

Q. 4 Name one device used in star topology. **(W-09, 2 Marks)**

Q. 5 State whether star is active or passive network. Justify. **(S-10, 4 Marks)**

Q. 6 State whether star is active or passive network. Justify. Also state the environment where it is more suitable. Draw a labelled diagram of a star network. **(S-11, 4 Marks)**

Q. 7 List down the topologies used in LAN. Explain star topology in detail. **(W-11, 8 Marks)**

Q. 8 In which circumstances star topology is preferred mostly ? Name the centralized device used in star topology. **(S-14, 2 Marks)**

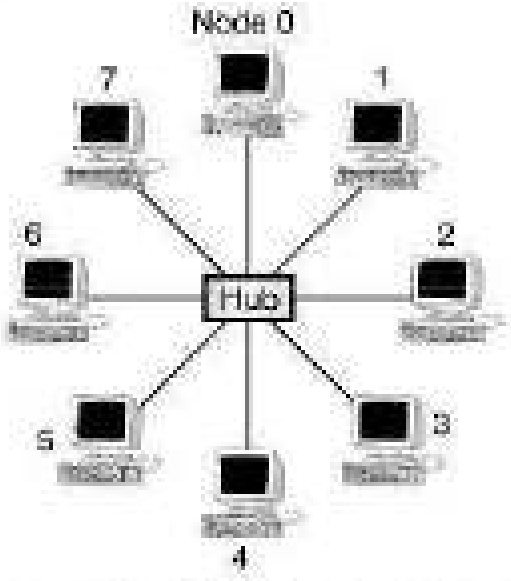
Q. 9 In star topology which device is preferable as a star device between switch and hub ? Justify your answer. **(W-14, 4 Marks)**

Q. 10 List types of network topology. Name one device used in star topology. **(W-15, 2 Marks)**

Q. 11 Draw a neat diagram and describe the working of star topology. **(W-16, S-18, 4 Marks)**

Definition :

- Star topology is a network topology, in which each individual piece of a network is connected to a central node called as a hub or switch.
- In a star topology all the computers (nodes) are connected via cables to a central location where they are all connected by a device called a hub as shown in Fig. 8.5.1.

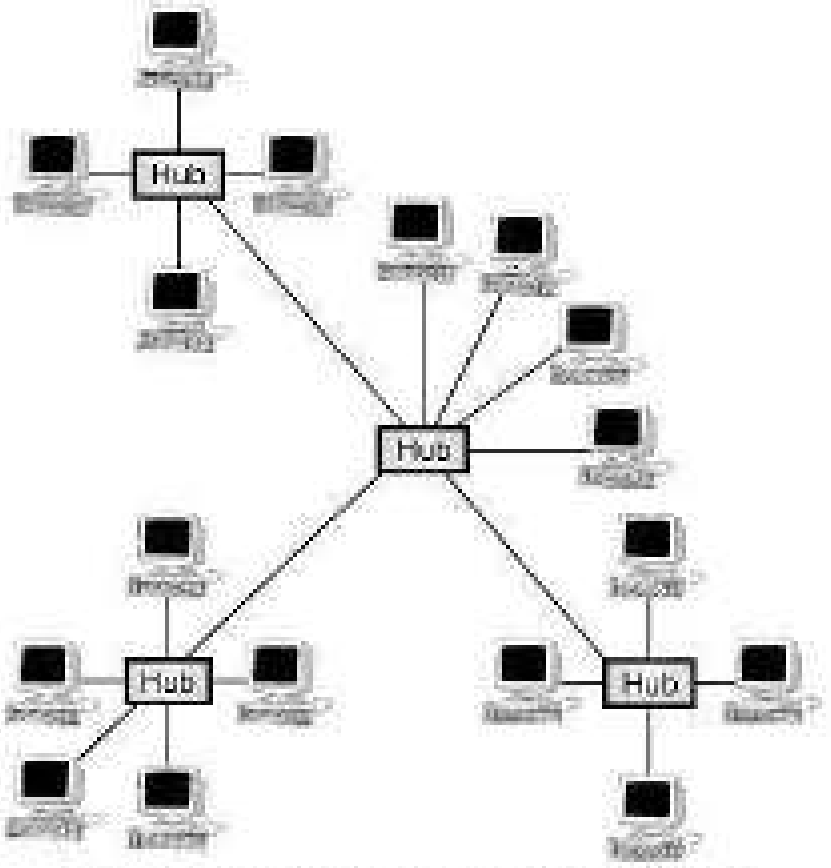


(S-18) Fig. 8.5.1 : Star topology

- There is no direct connections among the computers. All the connections are made via the central hub.
- Stars are used in concentrated networks, where the endpoints are directly reachable from a central location; when network expansion is expected and when the greater reliability of a star topology is needed.
- The telephone system also uses the star topology.
- Each computer on a star network communicates with a central hub. The hub then resends the message either to all the computers in a broadcast star network.
- It will resend the message only to the destination computer in a switched star network.
- The hub in a broadcast star network can be active or passive. An active hub generates the electrical signal and sends it to all the computers connected to it.
- This type of hub is usually called a multiport repeater. Active hubs require external power supply.
- A passive hub is a wiring panel or punch down block which acts as a connection point.
- It does not amplify or regenerate the signal. Passive hubs do not require electrical power supply.
- Several types of cables can be used to implement a star network. A hybrid hub can use different types of cable in the same star network.

Expansion of star :

- A star network can be expanded by placing another star hub as shown in Fig. 8.5.2.



(G-19) **Fig. 8.5.2 : Expansion of star topology**

- This arrangement allows several more computers or hubs to be connected to that hub. This creates a hybrid star network.
- Star topology is cheaper than mesh topology, as less number of links are required to be used.

Active or passive topology ?

- Star topology networks can be either active or passive depending on the following factors.
- If the central node performs processes like amplification or regeneration then it is an **active** topology. Other wise it is a **passive** topology.
- If the network actively controls the data transit, then it is **active** otherwise **passive.**
- If the network requires electrical power sources then it is **active** otherwise **passive.**

When is star topology suitable ?

- The star topology is preferred under the following circumstances :
  1. If the centralized network control is expected.
  2. If high reliability is more important than cost.
  3. If the network is to be expanded frequently.

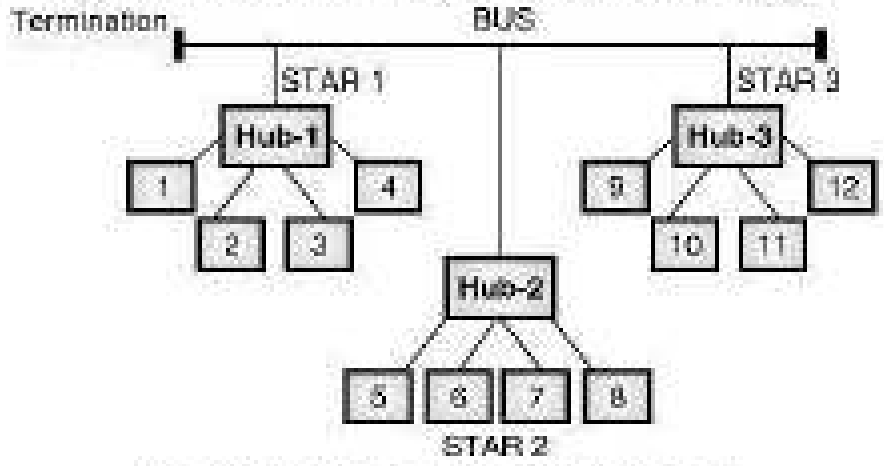
Devices used for star topology :

- The devices used for establishing a star topology network are : twisted pair cable, or optical fiber cable, a hub or switch, suitable connectors etc.

Ex. 8.5.1 : Draw the star bus topology connecting three star networks consisting of four computers.
S-03, W-03, 4 Marks

Soln. ;

- Fig. P. 8.5.1 shows the required star bus topology.

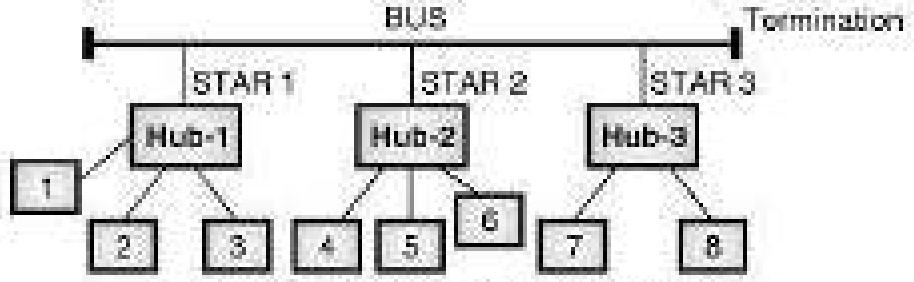


(G-25) **Fig. P. 8.5.1 : Star-bus topology**

Ex. 8.5.2 : Draw with neat-labelled sketch of star-bus topology connecting 3 star networks having 3 computers in 2 stars and 2 computers in one star.
S-07, W-08, 4 Marks

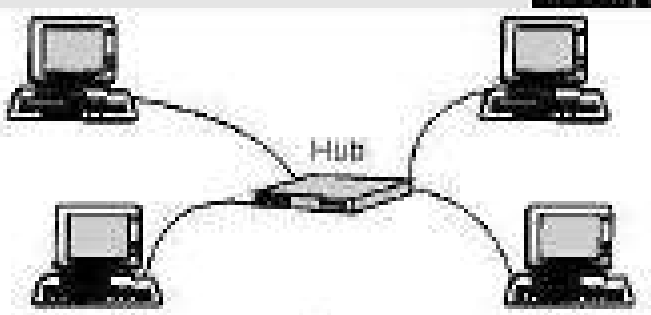
Soln. :

- Fig. P. 8.5.2 shows the required star-bus topology.



(G-28) **Fig. P. 8.5.2 : Star-bus network**

Ex. 8.5.3 : Identify topology in Fig. P. 8.5.3.
W-04, 4 Marks



(G-1389) **Fig. P. 8.5.3**

Soln. :

- Topology in Fig. P. 8.5.3 is star topology.

Ex. 8.5.4 : For the following situation state which type of network architecture is appropriate :
1. Data security is important.
2. No network administrator is required.
S-08, 2 Marks

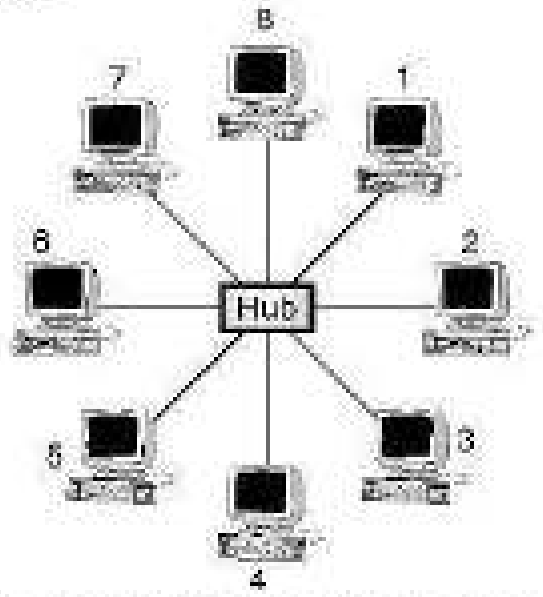
Soln. :

- For given situations star topology is appropriate.

Ex. 8.5.5 : A computer centre is connected in star topology with 8 computers : This set-up has to be converted into mesh topology. What are the requirements ? What are the advantages and disadvantages of the two systems ? Draw the sketches for both the topologies.
S-16, 4 Marks

Soln. :

– In a star topology all the computers (nodes) are connected via cables to a central location where they are all connected by a device called a hub as shown in Fig. P. 8.5.5.



(G-2371) **Fig. P. 8.5.5 : Star topology**

– There is no direct connections among the computers. All the connections are made via the central hub.

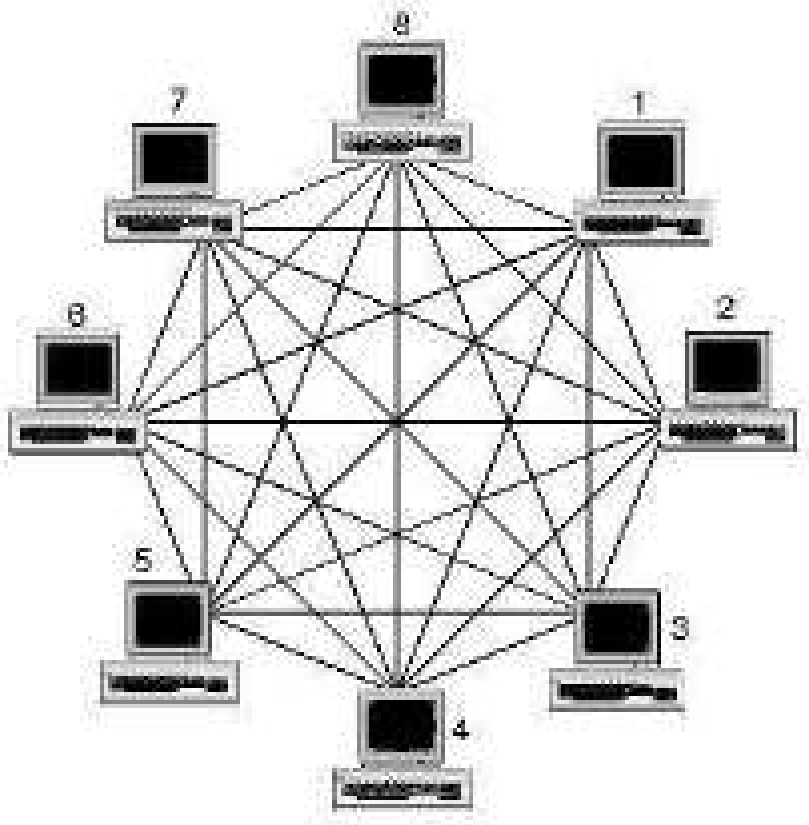
Requirements for conversion of star to mesh topology :

– In a mesh topology every device is physically connected to every other device with a point to point dedicated link.

– A fully connected mesh network therefore has n(n–1)/2 physical cables to connect n devices.

– To accommodate that many links every device on the network must have n–1 input/output ports.

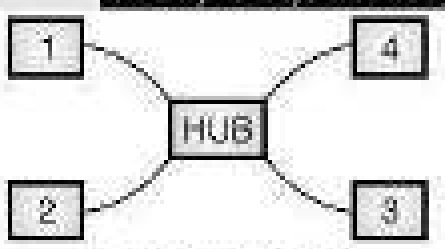
– Using this formula for a network of 8 computers, we will require 8 (8 – 1)/2 = 28 cables or links. Each device needs to be connected to 7 other devices.



(G-2372) **Fig. P. 8.5.5(a) : Mesh topology**

Ex. 8.5.6 : Identify the network topology shown in Fig. P. 8.5.6.

W-04, S-10, 2 Marks, S-13, 4 Marks



(G-26) **Fig. P. 8.5.6**

Soln. :

– The given network uses the star topology.

8.5.1 Hubs :

S-10, W-11, W-15

MSBTE Questions

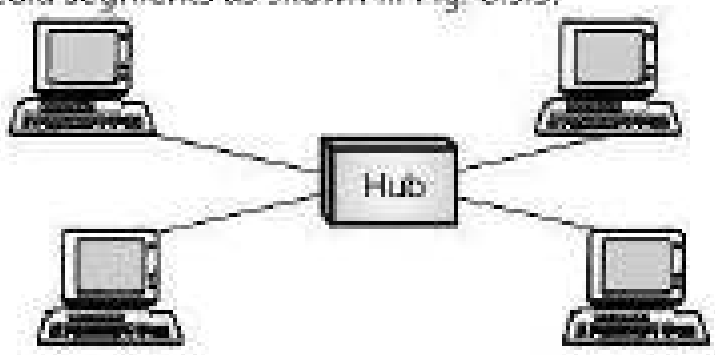
Q. 1 Describe the following term : Intelligent hub. **(S-10, 1 Mark)**

Q. 2 Write the working of Hub. **(W-11, 4 Marks)**

Q. 3 What is hub ? Give types of hub. **(W-15, 2 Marks)**

– All networks require a central location to connect various segments of media coming from various nodes.

– Such a central location is called as a hub. A hub organizes the cables and relays signals to the other media segments as shown in Fig. 8.5.3.



(G-350) **Fig. 8.5.3 : Hub**

– There are three main types of hubs :

1. Passive hubs
2. Active hubs
3. Intelligent hubs

1. Passive hubs :

– A passive hub simply combines the signals of a network segments. There is no signal processing or regeneration. It merely acts as a connector.

– A passive hub reduces the cabling distance by half because it does not boost the signals and infact absorbs some of the signal.

– With a passive hub, each computer receives the signals sent from all the other computers connected to the hub.

2. Active hubs :

– They are like passive hubs but have electronic components for regeneration and amplification of signals. By using active hubs the distance between devices can be increased. An active hub is equivalent to a multipoint repeater.

- The main drawback of active hub is that they amplify noise as well along with the signals. They are more expensive than passive hubs as well.

3. **Intelligent hubs :**

- In addition to signal regeneration, intelligent hubs perform some other intelligent functions such as network management and intelligent path selection.
- A switching hub chooses only the path of the device where the signal needs to go, rather than sending the signal along all paths.

8.5.2 Features of Star Topology :

- It needs to use a central location called hub. All connections are made through it.
- It improves the reliability of network.
- It needs less number of links than mesh topology.
- Expansion of network is very easy.
- It is an expensive topology because of the use of centralized hub.
- The entire network will be disrupted if the central hub malfunctions.

8.5.3 Advantages of Star Topology :

W-03, S-05, S-06, W-08, S-09, S-10, S-14

MSBTE Questions

Q. 1 State two advantages of star topology. **(W-03, S-05, 2 Marks)**

Q. 2 Describe the advantages of star topology. **(S-06, 2 Marks)**

Q. 3 Give the advantages of star topology. **(W-08, S-09, S-10, S-14, 2 Marks)**

1. It is easy to add new computers to a star network without disturbing the rest of the network.
2. The star network is easy to install and maintain.
3. The fault diagnosis is easy.
4. If a computer or link fails it does not bring down the whole star network.
5. Different types of cables can be used in the same network with a hub that can accommodate multiple cable types.

8.5.4 Disadvantages of Star Topology :

W-03, S-05, S-06, W-08, S-09

MSBTE Questions

Q. 1 State two disadvantages of star topology. **(W-03, S-05, W-08, 4 Marks)**

Q. 2 Describe disadvantages of star topology. **(S-06, 4 Marks)**

Q. 3 Give the disadvantages of star topology. **(W-08, S-09, 2 Marks)**

1. If the central hub fails, the whole network fails to operate.
2. Many star networks require a device at the central point to rebroadcast or switch the network traffic.
3. The cabling cost is more since cables must be pulled from all computers to the central hub.

Note : Ethernet 10 base T is a popular network based on the star topology. Intelligent hubs with microprocessor that implement features in addition to repeating network. Signals provide for centralized monitoring and management of the network. It is the most flexible and the easiest to diagnose when there is a network fault.

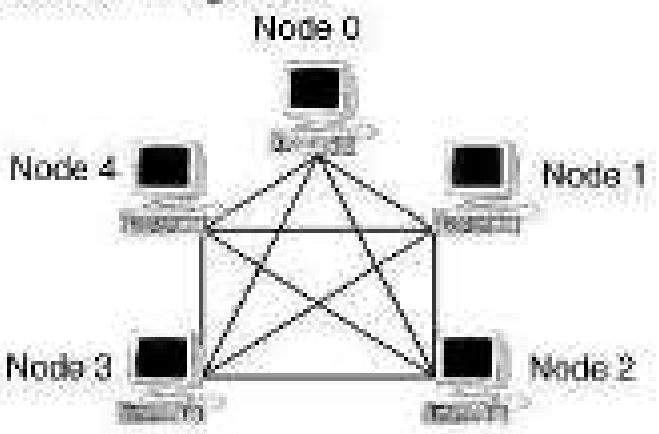
8.6 Mesh Topology : W-09, W-12

MSBTE Questions

Q. 1 The mesh topology is preferably used for very small network statement is true or false with your justification. **(W-09, 4 Marks)**

Q. 2 Describe network topology. Explain mesh topology in detail with suitable diagram. **(W-12, 4 Marks)**

- In a mesh topology every device is physically connected to every other device with a point to point dedicated link as shown in Fig. 8.6.1.



(G-21) **Fig. 8.6.1 : Mesh topology**

- The term dedicated means that the link carries data only between two devices connected on it.
- The mesh topology is also called as **complete topology.**

- The mesh topology does not have the traffic congestion problem, because dedicated lines are being used to connect the nodes.
- These links are not being shared. So the special protocol called Media Access Control (MAC) protocol is not required to be used.
- This topology has an advantage of **data security** due to the use of dedicated links. It is robust.
- If one link fails, the rest of the network can continue to function. The fault diagnosis and isolation of fault also is easy.
- The only disadvantages of this topology are the cable length, the cost of the cable and the associated complexity.
- A fully connected mesh network therefore has n(n–1)/2 physical cables to connect n devices.
- To accommodate that many links every device on the network must have n–1 input/output ports.
- So too many cables are required to be used for the mesh topology.
- Using this formula for a network of 1000 nodes, we will require 1000 (1000 – 1)/2 = 499500 cables or links. So this topology is suitable only for small networks.

8.6.1 Features of Mesh Topology :

- Every node is connected to every other device in the network.
- Every connection is done via a dedicated link.
- It is called as the complete topology.
- Congestion never takes place in the networks connected in the mesh topology.
- There is no need to use MAC (Media Access Control).
- It has a very high reliability and security.
- Mesh topology needs a large number of dedicated links. Hence it is suitable only for small networks.
- Easy fault diagnosis and isolation.

8.6.2 Advantages : S-11, S-14

MSBTE Questions

Q. 1 State advantages and disadvantages of mesh topology. **(S-11, 4 Marks)**

Q. 2 Give two advantages of mesh topology. **(S-14, 2 Marks)**

1. The use of dedicated links guarantees that each connection can carry its own data reliably.
2. A mesh topology is robust because the failure of any one computer does not bring down the entire network.
3. It provides security and privacy because every message sent travels along a dedicated line.
4. Point to point links make fault diagnose easy.
5. MAC protocol need not be used due to the use of dedicated links.

8.6.3 Disadvantages : S-11

MSBTE Questions

Q. 1 State advantages and disadvantages of mesh topology. **(S-11, 4 Marks)**

1. Since every computer must be connected to every other computer installation and reconfiguration is difficult.
2. Cabling cost is more.
3. The hardware required to connect each link input/output and cable is expensive.
4. It is suitable only for smaller networks.

Note : Mesh topology is usually implemented as a backbone connecting the main computers of a hybrid network that can include several other topologies.

8.7 Tree Topology :

W-08, S-15, S-17, S-18, I-Scheme : S-22

MSBTE Questions

Q. 1 Explain tree topology with neat diagram. **(W-08, 4 Marks)**

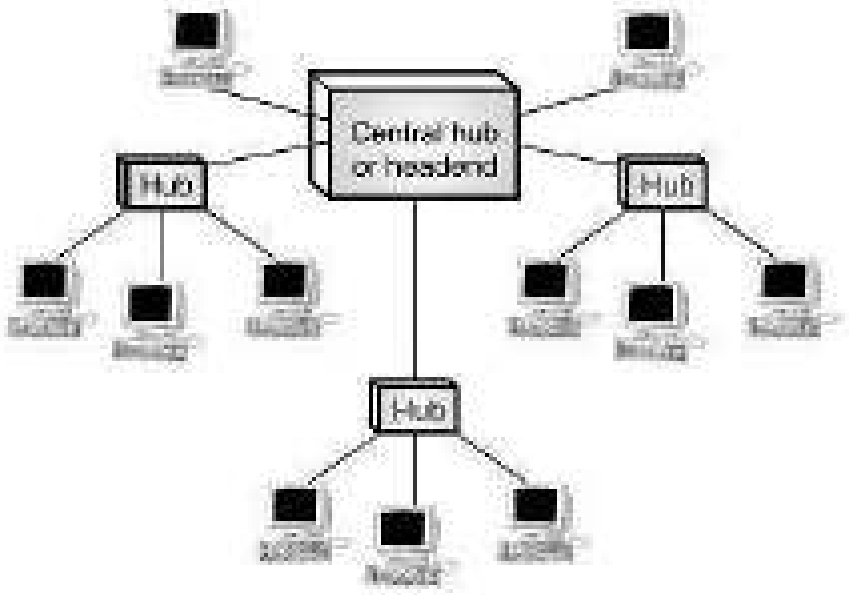
Q. 2 Describe Tree topology with neat diagram. State its advantages. (any two) **(S-15, 8 Marks)**

Q. 3 Explain tree topology with neat diagram. **(S-17, S-18, 4 Marks)**

Definition :

- Tree topology is a special type of structure in which many connected elements are arranged like the branches of a tree.
- A tree topology is a variation of a star. As in a star, nodes in a tree are connected to a central hub head end that controls the entire network.
- However, every computer is not plugged into the central hub.

– Most of them are connected to a secondary hub which in turn is connected to the central hub as shown in Fig. 8.7.1.



(S-22) **Fig. 8.7.1 : Tree topology**

– The central hub in the tree is an active hub which contains repeater.

– The repeater amplify the signal and increase the distance a signal can travel.

– The secondary hubs may be active or passive. A passive hub provides a simple physical connection between the attached devices.

– In this topology, there can be only one connection between any two nodes. Therefore it is also called as a parent-child topology.

8.7.1 Advantages : S-15

MSBTE Questions

Q. 1 Describe Tree topology with neat diagram. State its advantages. (any two) **(S-15, 8 Marks)**

1. It allows more devices to be attached to a single hub and can therefore increase the distance that a signal can travel between devices.
2. It allows the network to isolate and attach priorities to the communications from different computers.

8.7.2 Disadvantages :

1. If the central hub fails the system breaks down.
2. The cabling cost is more.

Note : The advantages and disadvantages of a tree topology are generally the same as those of a star.

8.8 Logical Topology :

– Logical topology describes the manner in which the stations are logically connected to each other for the purpose of data unit exchange.

– Physical topology discussed earlier can be different from the logical topology, of the network.

– As an example consider the bus topology. The bus acts as a central controller. It receives data and forwards it to the various nodes.

– Thus the stations have a logical connection to the bus which acts as a centralized controller.

– Therefore the logical topology of a bus is star topology, eventhough the physical topology is bus.

8.9 Comparisons :

8.9.1 Comparison of Star, Bus and Ring Topologies : S-13, S-14

MSBTE Questions

Q. 1 Compare ring, bus and star topology. **(S-13, 8 Marks)**

Q. 2 Compare bus topology and ring topology (four points). **(S-14, 4 Marks)**

Sr. No.	Parameter	Bus topology	Ring topology	Star topology
1.	Configuration	Fig. 8.3.1	Fig. 8.4.1	Fig. 8.5.1
2.	Routing methodology	Only one node sends information at a time, others wait for their turn.	Information goes in one direction around the ring until it reaches the correct node.	All information passes through the control hub.
3.	Complexity	The simplest	Moderately simple	Very simple.
4.	Ease of expansion	To add a computer, we need to shut down the network	Same as bus topology	Very easy
5.	Reliability	Low	Low	High. Depends on the reliability of central hub.

Sr. No.	Parameter	Bus topology	Ring topology	Star topology
6.	Cost	Cheapest	More expensive	Most expensive.
7.	Security	No security	No security	It is possible to provide security.
8.	Delay	Long	Moderate	Lowest

8.9.2 Comparison of Bus and Star Topologies : S-05, S-10

MSBTE Questions

Q. 1 Compare Bus with Star topology on the basis of cable used and fault tolerance. **(S-05, S-10, 2 Marks)**

Sr. No.	Bus	Star
1.	Uses a cable as bus or backbone to connect all nodes.	Uses a central hub to connect the nodes to each other.
2.	Baseband or broadband coaxial cable is used.	Twisted pair, coaxial cables or optical fiber cables are used.
3.	If a part of bus fails, the whole network fails.	Failure of the central hub will make the entire network collapse.
4.	Adding an new node is difficult.	Adding and removing a node is relatively easy.
5.	Fault diagnosis is relatively difficult.	Fault diagnosis is easy.

8.9.3 Comparison of Tree and Mesh Topologies : S-08, S-12

MSBTE Questions

Q. 1 Compare tree topology and mesh topology. **(S-08, S-12, 4 Marks)**

Sr. No.	Parameter	Mesh topology	Tree topology
1.	Dedicated links for connections.	Used	Connections are done through hubs.
2.	Reliability.	Higher	Low.
3.	Fault diagnosis	Easy	Not so easy.
4.	Number of links	Large	Small
5.	Congestion	Does not take place	Can take place.
6.	Suitable for	Small networks	Large networks.

8.9.4 Comparison of Mesh and Star Topologies : W-16

MSBTE Questions

Q. 1 Compare mesh topology with star topology. **(W-16, 4 Marks)**

Sr. No.	Mesh topology	Star topology
1.	Every device in mesh topology has a dedicated point to point link to every other device.	Each device in star topology has a dedicated point to point link only to a central controller.
2.	More cabling and input ports are required.	Less cabling and input ports are required.
3.	More expensive.	Less expensive.
4.	Fault diagnosis is relatively difficult.	Fault diagnosis is easy.
5.	It provides more privacy and security.	It provides less privacy and security as compared to mesh topology.

8.10 Hybrid Topology : S-09, S-14, W-14

MSBTE Questions

Q. 1 Why hybrid topology is preferred ? **(S-09, 2 Marks)**

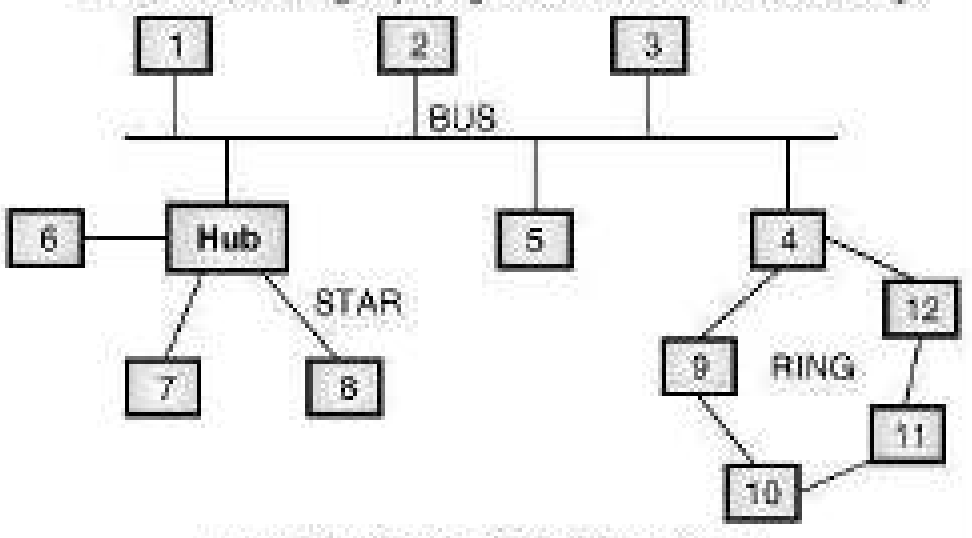
Q. 2 Describe with neat sketch "Hybrid topology". Give its applications. **(S-14, 4 Marks)**

Q. 3 Discuss hybrid topology with suitable diagram. **(W-14, 6 Marks)**

Definition :

- We have discussed various basic topologies such as bus, ring, mesh, star etc.

- Hybrid topology is the one which makes use of two or more basic topologies mentioned above, together.
- There are different ways in which a hybrid network is created. Fig. 8.10.1 shows the hybrid topology in which bus, star and ring topologies are used simultaneously.



(S-23) **Fig. 8.10.1 : Hybrid topology**

- In Fig. 8.10.1, the nodes 1, 2, 3, 4 and 5 are connected in the bus topology, node 6, 7 and 8 form a star and the nodes 4, 9, 10, 11, 12 are arranged in a ring topology.
- The practical networks generally make use of hybrid topology. Many complex networks can be reduced to some form of hybrid topology.
- The hybrid topology which is to be used for a particular application depends on the requirements of that application.

8.10.1 Advantages of Hybrid Topology :

1. High reliability.
2. Easy to detect fault.
3. It can be expanded very easily.
4. It can be used for both wired and wireless networks.
5. Low security risk.
6. Greater flexibility and speed.

8.10.2 Disadvantages :

1. It is difficult to design and manage.
2. Its design is expensive.
3. It needs to use the MAU (Multistation Access Unit).

8.10.3 Applications : S-14

MSBTE Questions

Q. 1 Describe with neat sketch "Hybrid topology". Give its applications. **(S-14, 4 Marks)**

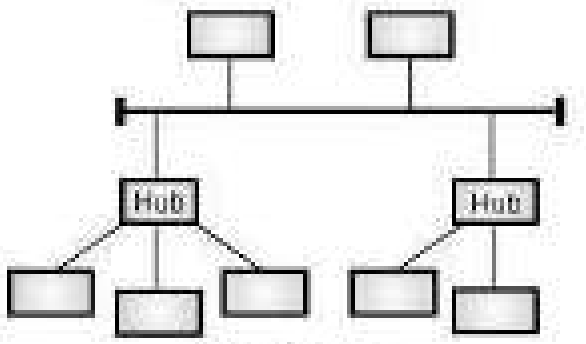
- Hybrid topology is often used in the wide area networks (WANs).

8.10.4 Comparison of Star Bus and Star Ring Topologies : S-06, S-18

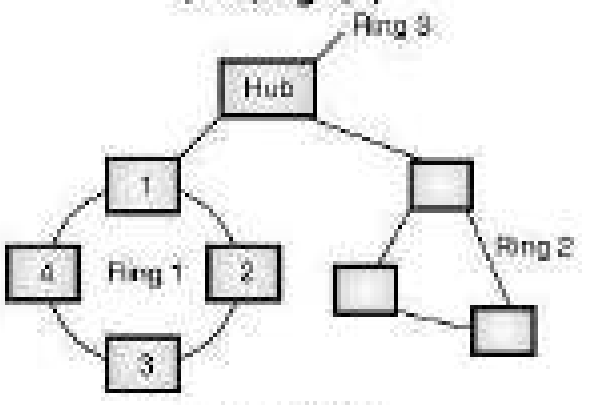
MSBTE Questions

Q. 1 Compare star-bus with star-ring topology. **(S-06, S-18, 4 Marks)**

Sr. No.	Parameter	Star Bus	Star Ring
1.	Topology	Hybrid. It is a combination of star and bus topologies.	Hybrid. It is a combination of star and ring topologies.
2.	Configuration	Fig. A	Fig. B
3.	Peculiarity	Many stars are connected to a bus.	Many rings are connected in star.
4.	Applications	Suitable for large networks.	Suitable for interconnection of many small networks.



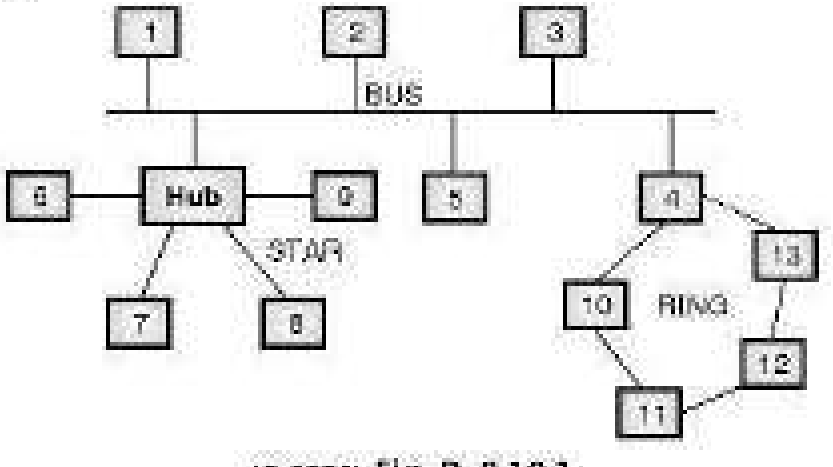
(G-24) **Fig. (A)**



(G-24) **Fig. (B)**

Ex. 8.10.1 : Draw a neat labeled sketch of hybrid topology connecting one star network of 4 computers, one ring network of 5 computers and one bus network of 5 computers. **S-11, 4 Marks**

Soln. :



(G-23) **Fig. P. 8.10.1**

Review Questions

Q. 1 Name the different network topology types.

Q. 2 Explain the basic concepts of bus topology with the help of suitable diagram.

Q. 3 State the important characteristics of bus topology.

Q. 4 Name the transmission media used for bus LANs.

Q. 5 Write a short note on repeaters in bus LAN.

Q. 6 State advantages and disadvantages of bus topology.

Q. 7 Write a note on : Ring topology.

Q. 8 What are the functions of a ring ?

Q. 9 Explain the following states in connection with the ring topology.

1. Listen state 2. Transmit state
3. Bypass state

Q. 10 What are the problems faced by the ring topology ?

Q. 11 State the advantages and disadvantages of ring topology.

Q. 12 Write a short note on star topology.

Q. 13 What is the difference between single level star topology and two level star topology.

Q. 14 State the advantages and disadvantages of star topology.

Q. 15 Write a short note on Mesh topology.

Q. 16 State advantages and disadvantages of mesh topology.

Q. 17 Write a short note on tree topology.

Q. 18 Compare Ring and Bus.

Q. 19 Compare Star and Ring.

8.11 MSBTE Questions and Answers :

Q. 1 State two advantages of Ring. Describe activity in Ring Network when no station is transmitting the packet. Whether collisions occur frequently in ring network ? **(S-03, 4 Marks)**

Ans. :

– For advantages of ring refer section 8.4.4.

– The ring network is in the listen state when the station is not transmitting. Collisions do occur frequently in the ring network due to the circulating packets.

Q. 2 Whether troubleshooting in Ring Network is easy or difficult ? Give two possible causes of failures in Ring network. State whether ring is a broadcast or point to point network. **(S-03, 4 Marks)**

Ans. :

– For troubleshooting in ring network refer section 8.4.3.

Ring is a point to point network.

Q. 3 You are considering networking topologies for a network for a telemarketing firm. Under what circumstances would a ring be less appropriate than star ? **(S-03, 4 Marks)**

Ans. :

– The circumstances under which a ring is less appropriate than star are as follows :

1. The communication from the firm to the customer and vice versa would not be efficient if a ring is used.
2. The ring topology would not be convenient because the number of customers would increase continuously.
3. Even if one node fails, the entire ring will fail.
4. The time taken for communication is more if the ring topology is used.

Q. 4 You are installing a new network for a company that is growing rapidly.

The current design calls for 40 computers, with expansion to 100 in the next six months. Because of the speed at which the network is expected to grow, you want to make sure that troubleshooting will be easy as possible. Considering these factors, which topologies should be used in the new network ? Justify your answer. **(W-03, W-04, 4 Marks)**

Ans. :

– For details refer section 8.5.

– Taking into consideration the future expansion and ease of troubleshooting, the star topology will be ideally suitable in the given environment.

Q. 5 State whether star is active or passive network ? Justify. Give two advantages of star topology. **(W-03, 4 Marks)**

Ans. :

– Please refer section 8.5.3 for advantages of star topology.

- The star is an active network because it uses hubs which can be of intelligent and passive types.
- The intelligent hubs need external power supply, electronic components for regeneration of signal as well as routing it to the required computer.

Q. 6 Describe network topology. Draw star topology. Name one device used in star topology. **(S-04, 4 Marks)**

Ans. :

- For network topology and star topology refer sections 8.2 and 8.5.
- Hub is used in star topology.

Q. 7 State whether Bus is active or passive Network. Justify compare bus with ring topology on the basis of cable used and fault tolerance. **(S-04, S-16, 4 Marks, S-17, 2 Marks)**

Ans. :

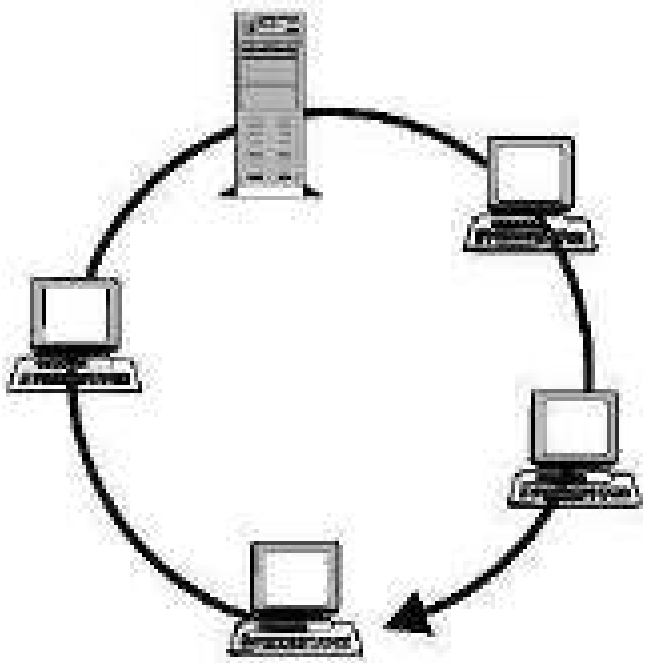
- Bus is passive network please refer sections 8.3 and 8.4.2.

Q. 8 State two advantages of Ring topology. Describe token. State whether ring topology is Broadcast or point to point network. **(S-04, W-15, 4 Marks)**

Ans. :

- Ring is point to point network. Refer section 8.4.4 for advantage and section 8.4 for token.

Q. 9 Describe Network topology. Identify topology shown in Fig. 1. Comment on whether this topology is active network or passive network justify. **(S-05, 4 Marks)**



(G-27) **Fig. 1**

Ans. :

- Please refer Ex. 8.4.1. The ring topology is active network. Refer Sections 8.2 and 8.4.

Q. 10 State two advantages of Ring topology. Describe token. State whether ring topology is Broadcast or point to point network. **(S-05, 4 Marks)**

Ans. :

- Ring is a point to point network. (Sections 8.4 and 8.4.4)

Q. 11 State two advantages of Ring. State whether addition of computers to existing ring network will slower the ring. Justify. **(W-05, 4 Marks)**

Ans. :

- For advantages of a ring, Please refer section 8.4.4.
- The addition of computers to the existing ring network will result in increased cable length. Since the ring is a unidirectional network, the time taken by a message to travel will increase due to increased number of computers. This will slow down the ring.

Q. 12 The mesh topology is preferably used for very small network. State this statement is true or false with your justification. **(S-07, 4 Marks)**

Ans. :

- True. Please refer section 8.6 for justification.

Q. 13 You are said to establish a network for your laboratory with atleast 10 computers and also centralized administration is necessary. Which type of network and Topology you will prefer in situation. Justify your answer. **(S-08, 4 Marks)**

Ans. :

- If the centralized administration is necessary, then the client-server type network will be the right choice.
- There are atleast 10 computers, the number can increase in future and centralized administration is necessary.
- So the star topology or star-bus topology can be used.

Q. 14 What are active and passive networks ? What is a ring network ? What are possible causes of failure of a ring network ? **(S-09, 4 Marks)**

Ans. :

- Refer sections 8.5 and 8.4.3 for active and passive networks and ring network.
- A network or topology which uses an active electronic device such as an amplifier to amplify the signal or to pass it along from one computer to the other is called as an **active network** or **active topology.**
- A network which does not use any such active electronic device is called as a **passive network.**

Q. 15 Which of the following network "topologies most gracefully used in high network load situation".

1. Star
2. Ring
3. Mesh
4. Bus

Justify your answer. **(S-10, 4 Marks)**

Ans. :

- The degradation with increase in the network load is most graceful for the star topology.
- The reason is that with increased load, there will be a large increase in the number of messages travelling on the network.
- There would be a large number of collisions, delays possible for the bus and ring topologies, mesh is not suitable for larger networks and so star is the correct answer.

Q. 16 You are installing a new network for a company that is growing rapidly. The current design for 40 computers with expansion to 100 in next six months. Because of the speed at which the network is expected to grow, you want to make sure that troubleshooting will be easy as possible. Which topology should be used in new network ? Justify your answer. **(W-10, 4 Marks)**

Ans. :

- For details refer section 8.5.
- Taking into consideration the future expansion and ease of troubleshooting, the star topology will be ideally suitable in the given environment.

Q. 17 Suppose you are going to implement a computer network in a small business mall. Which topology will you use ? Why ? **(S-14, 4 Marks)**

Ans. :

- In a small business mall, the computer network should be such that it should allow the centralized administration.
- Also number of end users (computers) can increase in future. So inclusion of new user should be easy.
- The trouble shooting also should not be difficult.
- Taking into account all these requirements, the client server type network will be the right choice. Also the star or star-bus topology should be used.

Q. 18 You are asked to establish a small network with minimum cost at least eight computer. Also it is necessary to use centralized database. Which type of network topology you will use ? Justify your answer. **(S-15, 8 Marks)**

Ans. :

- If the centralized database is necessary, then the client-server type network will be the right choice.
- There are atleast 8 computers, the number can increase in future and centralized database is necessary.
- So the star topology or star-bus topology can be used.

Q. 19 State any two advantages of ring topology, define token. State whether ring topology is broadcast or point to point network. **(S-15, 4 Marks)**

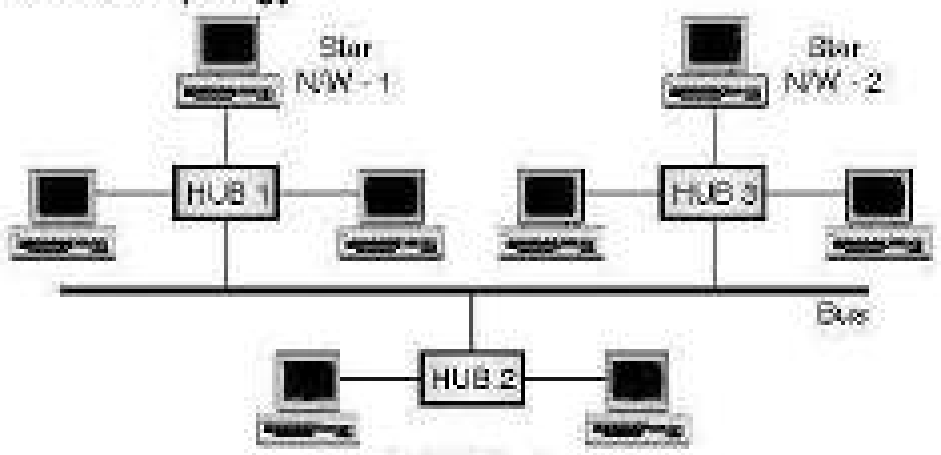
Ans. :

- Ring is point to point network.
- Refer section 8.4.4 for advantage of ring topology and section 8.4 for definition of token.

Q. 20 Draw with neat labeled sketch of star bus topology connecting three star networks having three computers in two stars and two computers in one star. **(W-15, 4 Marks)**

Ans. :

Star bus topology :



(S-1897) Fig. 2

Q. 21 You are said to establish a small network with minimum cost, at least ten computers and also necessary to use the centralized database. Which type of network and topology you will prefer in this situation ? Justify your answer. **(W-15, 4 Marks)**

Ans. :

- If the centralized database is necessary, then the client-server type network will be the right choice.
- There are atleast 10 computers, the number can increase in future and centralized database is necessary.
- So the star topology or star-bus topology can be used.

Q. 22 Name the topology which is combination of different topologies. Explain it with advantages.

(S-16, 4 Marks)

Ans. :

- Refer section 8.10. This has advantages of bus (refer section 8.3.8), star (refer section 8.5.3) and ring topologies (refer section 8.4.4).

Q. 23 Name the topology which combines two or more topologies. What are its advantages ? Draw a neat diagram of the same. **(W-16, 4 Marks)**

Ans. :

- Hybrid topology combines two or more topologies. Refer section 8.10 for a neat diagram of hybrid topology.

Advantages of hybrid topology :

1. Scalable
2. Reliable
3. Flexible
4. Effective.

8.12 I-Scheme Questions and Answers :

Summer 2019 [Total Marks - 12]

Q. 1 With suitable diagram describe :

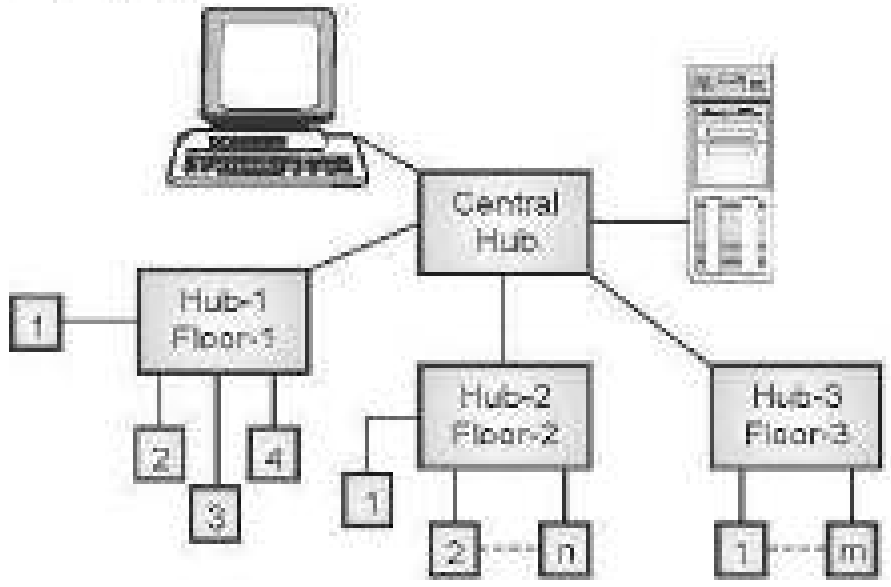
1. STAR topology. **(Section 8.5)**
2. RING topology. **(Section 8.4)** **(4 Marks)**

Q. 2 Draw and describe architecture for network using tree topology for an office in 3-storey's building.

(4 Marks)

Ans. :

- The required network using the tree topology is shown in Fig. 1.



(L-926) Fig. 1 : Required network using the tree topology

- The central hub is an active hub which contains repeaters.
- One secondary hub is used per floor. All the computers on each floor are connected to the secondary hub on that floor.
- The secondary hubs can be either active or passive. All of them are connected to the central hub as shown in Fig. 1.

Q. 3 Design suitable network layout for an organization with five department (ten users each). **(4 Marks)**

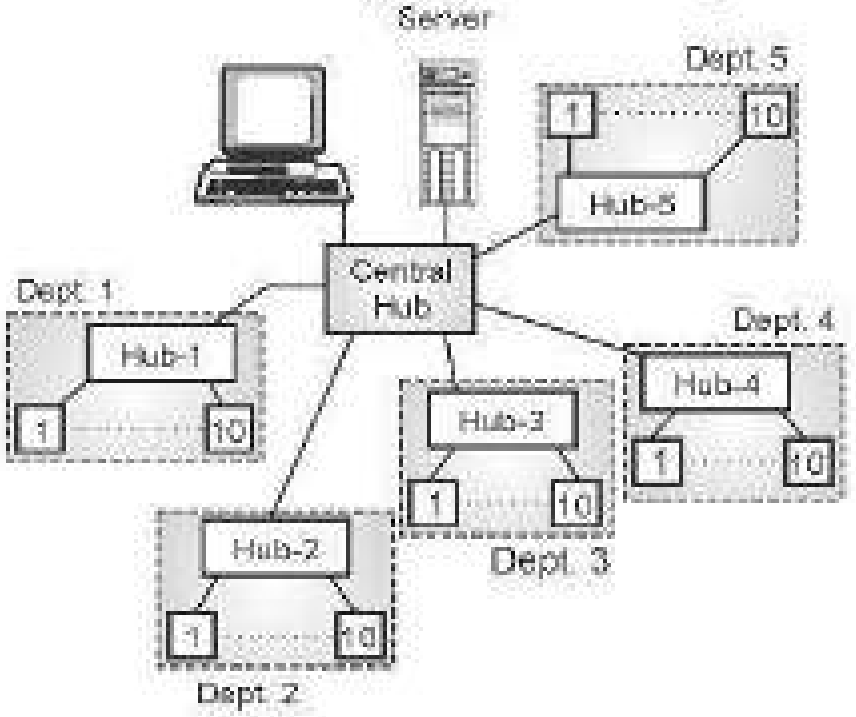
Ans. :

Given : 5 departments, 10 users per department.

- For an organization the network requirements would be as follows :

1. Centralized data base.
2. Future expansion.
3. Easy fault detection.

– These requirements can be fulfilled using a client-server network with a tree topology as shown in Fig. 2.



(L-927) **Fig. 2 : Layout of the required network**

Winter 2019 [Total Marks - 02]

Q. 4 State different types of network topologies. **(Section 8.2.2)** **(2 Marks)**

Summer 2022 [Total Marks - 06]

Q. 5 Explain the working of following topologies :

i. Bus. **(Section 8.3)**

ii. Ring. **(Sections 8.4)**

iii. Tree. **(Section 8.7)** **(6 Marks)**

❑❑❑

Chapter 9

Network Connecting Devices

Syllabus

Network connecting devices – Hub, Switch, Router, Bridge, Repeater, Gateway, Modem, Wireless infrastructure components.

Chapter Contents

9.1 Need of Network Control/Connecting Devices :

- Computers, LANs do not operate in an isolated manner. They are either connected to one another or to the Internet. For such connections, we need to use the connecting devices.
- Different layers of the Internet model correspond to different connecting devices.
- Without the connecting devices it would not be possible to communicate between two or more computers in a LAN or between LANs.

9.1.1 Types of Network Connecting Devices :

S-06, S-08, S-08, W-11, S-12, W-12, S-13, S-14, I-Scheme : S-22

MSBTE Questions

Q. 1 List different types of connectivity devices. **(S-06, 2 Marks)**

Q. 2 Enlist any four network connecting devices. **(S-08, 2 Marks)**

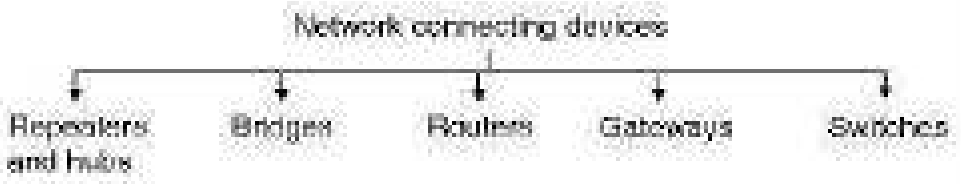
Q. 3 What are various network connecting devices ? **(S-09, 2 Marks)**

Q. 4 What are various network control devices ? **(W-11, W-12, S-13, 2 Marks)**

Q. 5 State and explain network control devices. (Any 4) **(S-12, 4 Marks)**

Q. 6 Give the names of various network connecting devices (Any two). **(S-14, 2 Marks)**

- Different types of network connecting devices are as shown in Fig. 9.1.1.



(G-348) **Fig. 9.1.1 : Network connecting devices**

- Out of these the repeaters, hubs and bridges are known as the **Networking Devices** because they connect the devices within a given network.
- Whereas the routers and gateways are known as the **Internetworking Devices.**
- These devices are used for connecting one network to other.
- We start our discussion from the connectors because they belong to the lowest portion i.e. the physical medium of the OSI reference model.
- After connectors, we will discuss the transceivers which connect a host to the medium.
- Then various connecting devices such as repeaters, hubs, bridges, routers and gateways are explained.

9.2 Transceivers : W-06, S-17

MSBTE Questions

Q. 1 What is a transceiver ? State the advantages and disadvantages of it. **(W-06, S-17, 4 Marks)**

- The word transceiver is a combination of transmitter and receiver. It performs three functions :
  1. Sends signals over the medium.
  2. Receives signals from the medium.
  3. Detects collisions.

Advantages and Disadvantages :

1. It combines the operations of transmission and reception.
2. It can detect collisions.
3. It can detect when the line is idle.
4. It can not regenerate a signal because it is not a repeater.
5. It does not have the filtering capability.

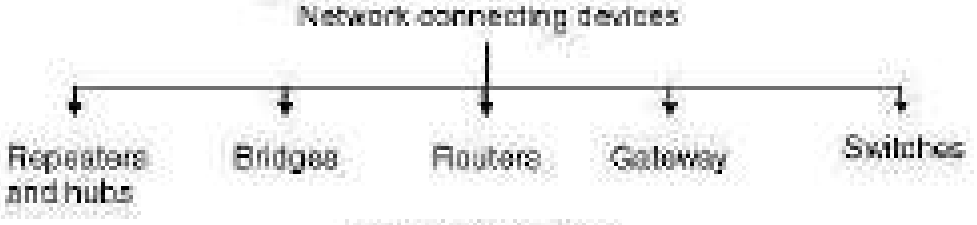
9.3 Role of Network Connecting Devices : W-14, S-16, S-18

MSBTE Questions

Q. 1 Write in brief any two role of network control devices in computer network **(W-14, 2 Marks)**

Q. 2 State the functions of : 1. Hub 2. Repeater 3. Bridge 4. Router. **(S-16, S-18, 4 Marks)**

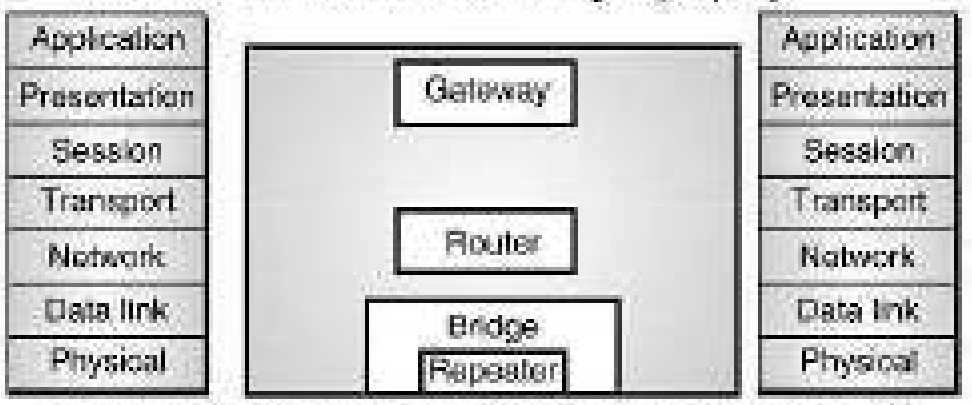
- Different types of network connecting devices are as shown in Fig. 9.3.1.



(G-348) **Fig. 9.3.1**

- The relation between OSI reference model and various connecting devices is shown in Fig. 9.3.2.
- Two or more devices are connected to each other for the purpose of sharing data or resources from a network.
- A LAN may be spread over a larger distance than its media can handle effectively.

- The number of stations also can be more than a number which can be handled and managed properly.



(S-05,15) **Fig. 9.3.2 : Connecting devices and OSI model**

- Such networks should be subdivided into smaller networks and these smaller subnetworks should be connected to each other through connecting devices.
- A device called a repeater is inserted into the network to increase the coverable distance or a device called a bridge can be inserted for traffic management.
- When two or more separate networks are connected for exchanging data or resources it creates an internetwork. Routers and gateways are used for internetworking.
- Each of these device type interacts with protocols at different layers of the OSI model.
- Repeaters act only upon the electrical components of a signal and are therefore active only at the physical layer.
- Bridges utilize addressing protocols and can affect the flow control of a single LAN. Bridges are most active at the data link layer.
- Routers provide links between two separate but same type LANs and are active at the network layer.
- Finally gateways provide translation services between incompatible LANs or applications and are active in all of the layers. Connecting devices and the OSI model is shown in Fig. 9.3.2.
- The following table summarizes the role of different networking devices.

Table 9.3.1 : Role of networking devices

Sr. No.	Name of the device	Role
1.	Repeater	Regenerates the original signal. Operates in the physical layer.
2.	Bridge	Bridges utilize the address protocol. They can carry out the traffic management. They are most active in the data link layer.
3.	Routers	Routers provide connections between two separate but compatible networks. It works in the network layer.
4.	Gateways	Gateways provide translation services between incompatible networks and works in all the layers.
5.	HUB	Connecting stations in a physical layer topology.
6.	Switch	Provides bridging functionality with great efficiency.

9.4 Repeaters :

S-05, W-05, W-06, W-10, S-12, S-13, S-15, I-Scheme : W-19

MSBTE Questions

Q. 1 Identify repeater device and state in which layer of OSI reference model it operates. List uses of it. **(S-05, 2 Marks)**

Q. 2 Describe repeater. State the situations under which repeater is necessary in network. **(W-05, W-10, 8 Marks, S-13, 4 Marks)**

Q. 3 What is a repeater ? State their advantages and disadvantages. **(W-06, 2 Marks)**

Q. 4 Identify the following devices operate in which layer of OSI reference model : Repeaters. **(W-10, 4 Marks)**

Q. 5 State and explain network control devices. (Any 4) **(S-12, 4 Marks)**

Q. 6 Describe the function of repeater. In which situation the repeater is used in the network ? **(S-15, 4 Marks)**

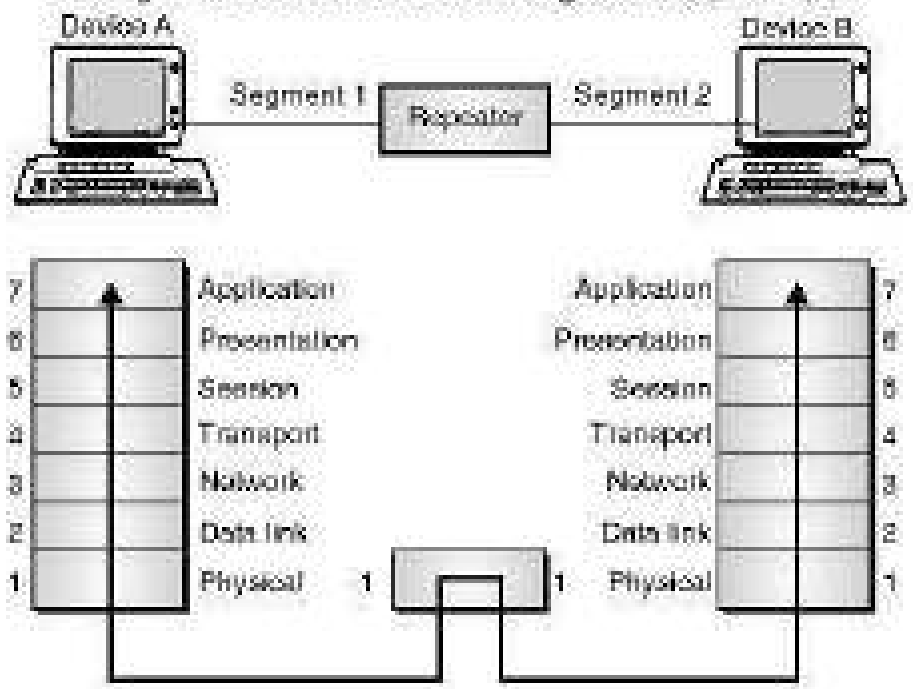
Definition :

- A repeater is a connecting device which can operate only in the physical layer of the OSI model.
- All transmission media weaken the electromagnetic waves that travel through them.
- Attenuation of signals limits the distance any medium can carry data. Devices that amplifies signals to ensure data transmission are called **repeaters.**

Function of a repeater :

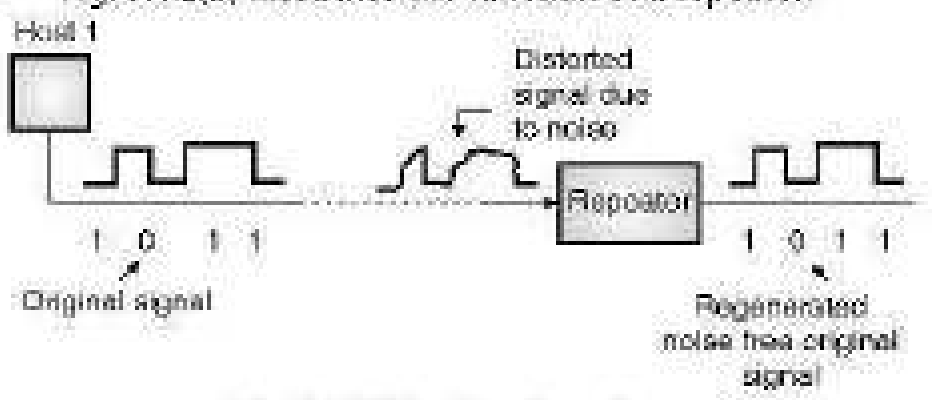
- A repeater receives a signal and before it gets attenuated or corrupted, regenerates the original signal.

- Thus we can use a repeater to extend the physical length of LAN as a shown in Fig. 9.4.1(a).
- Repeater is not an amplifier because amplifiers simply amplify the entire incoming signal along with noise.
- Signal – regenerating repeaters create an exact duplicate of incoming data by identifying it amidst the noise, reconstructing it and retransmitting only the desired information.
- The original signal is duplicated, boosted to its original strength and sent as shown in Figs. 9.4.1(a) and (b).



(G-351) **Fig. 9.4.1(a) : Repeater in OSI model**

- A repeater does not connect two LANs. It connects only two devices connected in the same LAN.
- It cannot connect two LANs of a different protocols.
- A repeater forwards every frame, it cannot filter out some frames and let the others pass through.
- A repeater should be placed at a precise point on the link. Such that the signal reaches it before the noise has induced an error in any of the transmitted bits.
- Fig. 9.4.1(b) illustrates the function of a repeater.



(G-352) **Fig. 9.4.1(b) : Function of a repeater**

- Repeaters operate at the physical layer of the OSI model and they deal with the actual physical signals.

9.4.1 Advantages : W-06

MSBTE Questions

Q. 1 State the advantages of repeater. **(W-06, 2 Marks)**

1. Repeaters can regenerate the desired information.
2. They can reduce the effect of noise.
3. They can extend the network.
4. It reduces the number of errors introduced due to noise.

9.4.2 Disadvantages : W-06

MSBTE Questions

Q. 1 State the disadvantages of repeater.
(W-06, 2 Marks)

1. A repeater cannot connect two LANs. It can only connect two devices connected in the same LAN.
2. It has no filtering capability.
3. Repeaters can operate only in the physical layer.
4. Repeaters must be placed at the precise point on the link so as to be effective.

9.5 Hubs :

S-06, W-06, S-09, W-09, W-10, S-12, W-12, S-13, S-14, S-16, W-16, S-18, I-Scheme : W-19, S-22

MSBTE Questions

Q. 1 Describe the types of hubs. **(S-06, S-18, 2 Marks)**

Q. 2 What are hubs ? How are they classified ?
(W-06, 4 Marks)

Q. 3 Define following terms :
(a) Active hub (b) Passive hub
(S-09, 2 Marks)

Q. 4 What is hub ? Give the types of hub.
(W-09, 2 Marks)

Q. 5 What are Hubs ? How are they classified.
(W-10, 4 Marks)

Q. 6 State and explain network control devices. (Any 4.)
(S-12, 4 Marks)

Q. 7 Explain :
1. Passive hubs 2. Active hubs
(W-12, 4 Marks)

Q. 8 What is hub ? Give the different types of hubs.
(S-13, 2 Marks)

Q. 9 List any two components which works at physical layer of OSI model. **(S-14, 2 Marks)**

Q. 10 Describe the role of following network devices used in computer network : Hub. **(S-14, 1 Mark)**

Q. 11 State the functions of : 1. Hub 2. Repeater 3. Bridge 4. Router. **(S-16, 4 Marks)**

Q. 12 State the function of : 1. Hub 2. Router
(W-16, 2 Marks)

Definition :

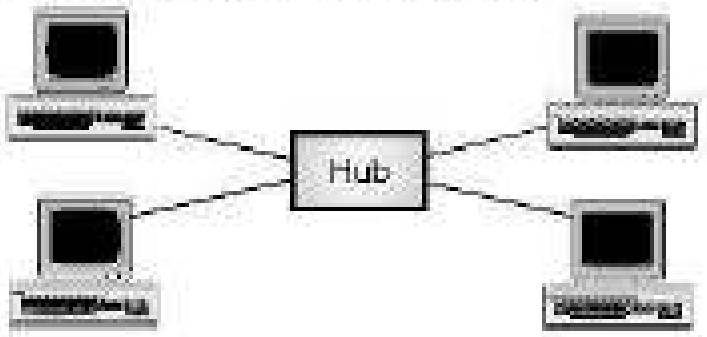
– The general meaning of the word hub is any connecting device. But its specific meaning is **multiport repeater.**

Function :

– It is normally used for connecting stations in a physical star topology.

– All networks require a central location to connect various segments of media coming from various nodes.

– Such a central location is called as a hub. A hub organises the cables and relays signals to the other media segments as shown in Fig. 9.5.1.



(G-350) **Fig. 9.5.1 : Hub**

Types :

– There are three main types of hubs :

1. Passive hubs
2. Active hubs
3. Intelligent hubs

1. Passive hubs :

– A passive hub simply combines the signals of a network segments. There is no signal processing or regeneration. It merely acts as a connector.

– A passive hub reduces the cabling distance by half because it does not boost the signals and in fact absorbs some of the signal.

– With a passive hub, each computer receives the signals sent from all the other computers connected to the hub.

2. Active hubs :

– They are like passive hubs but have electronic components for regeneration and amplification of signals.

– By using active hubs the distance between devices can be increased. An active hub is equivalent to a multipoint repeater.

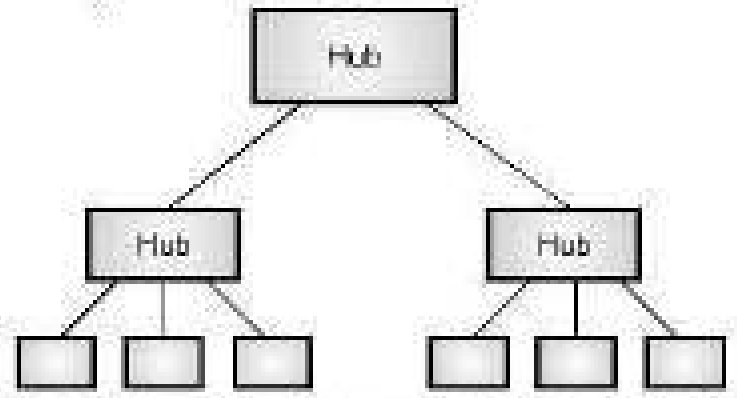
– The main drawback of active hubs is that they amplify noise as well along with the signals. They are more expensive than passive hubs as well.

3. Intelligent hubs :

– In addition to signal regeneration, intelligent hubs perform some other intelligent functions such as network management and intelligent path selection.

– A switching hub chooses only the port of the device where the signal needs to go, rather than sending the signal along all paths.

– Hubs can also be used to create multiple levels of hierarchy as shown in Fig. 9.5.2.



(G-353) **Fig. 9.5.2 : Hubs to create multiple levels of hierarchy**

9.6 Bridges :

S-05, W-10, W-11, S-12, S-14, I-Scheme : W-19, S-22

MSBTE Questions

Q. 1 Identify Bridges and state in which layer of OSI reference model they operate. List uses of it. **(S-05, 2 Marks)**

Q. 2 Identify the following devices operate in which layer of OSI reference model : Bridge. **(W-10, 4 Marks)**

Q. 3 Draw and explain the working of bridges. **(W-11, 4 Marks)**

Q. 4 State and explain network control devices. (Any 4) **(S-12, 4 Marks)**

Q. 5 List any two components which works at physical layer of OSI model. **(S-14, 2 Marks)**

Definition :

– Bridge is a computer network device, which creates a single aggregate network from multiple communication networks or network segments. This function is called as **network bridging.**

Function :

– A bridge can operate in the physical layer as well as in the data link layer of the OSI model.

– It can regenerate the signal that it receives and it can check the physical (MAC) addresses of source and destination mentioned in the header of a frame.

Types of Bridges :

– There are four types of bridges :

1. Simple bridges.
2. Multipoint bridges.

3. Transparent bridges.
4. Source routing bridges.

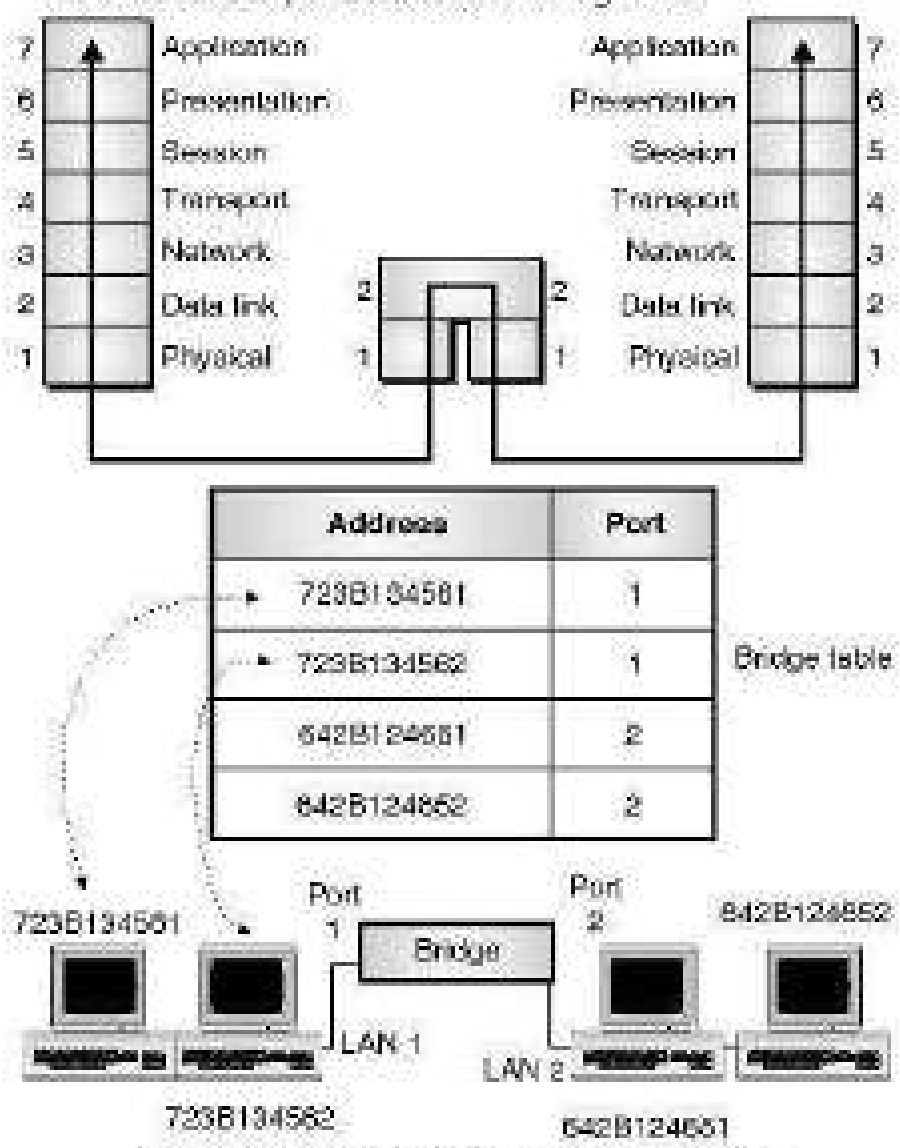
Configuration :

- Fig 9.6.1 shows the use of a bridge for connecting two local area networks to each other.

(G-2377) **Fig. 9.6.1 : Use of a bridge to connect two LANs**

Operation :

- The major difference between the bridge and repeater is that the bridge has a filtering capability.
- That means a bridge will check the destination address of a frame and make a decision about whether the frame should be forwarded or dropped.
- If the frame is to be forwarded, then the bridge should specify the port over which it should be forwarded.
- In order to achieve this a bridge has a table relating the addresses and ports as shown in Fig. 9.6.2.



(G-334) **Fig. 9.6.2 : Bridge and bridge table**

- If a frame for 723B134561 arrives at port 2 then the bridge goes through its table and understands that the frame is to be sent out on port 1 so it will do so.
- In Fig. 9.6.2 a two port bridge is shown but in reality a bridge has more than two ports.
- It is important to note that the bridges do not change the physical address contained in the frame.

Uses of Bridges :

1. A bridge joins two otherwise separate computer networks.
2. Bridges are used with LANs to extend their reach to cover larger physical area.
3. Bridges are used to inspect the incoming network traffic and determine whether to forward it or discard it.

9.7 Routers :

S-05, W-06, S-08, W-08, S-11, W-11, S-12, W-12, S-13, S-14, S-15, W-16, S-17, I-Scheme : W-19

MSBTE Questions

Q. 1 Identify routers and state in which layer of OSI reference model they operate. List uses of it. **(S-05, 8 Marks)**

Q. 2 What are routers ? Explain with neat diagram **(W-06, S-06, 8 Marks)**

Q. 3 What are the different types of routers ? Explain. **(W-08, S-13, 4 Marks)**

Q. 4 With the help of neat diagram, describe the working of Routers. Also enlist types of routers. **(S-11, 8 Marks)**

Q. 5 Explain working of router in detail. **(W-11, 8 Marks)**

Q. 6 What is router ? **(S-12, 2 Marks)**

Q. 7 State and explain routers with neat diagram. **(S-12, 4 Marks)**

Q. 8 What are routers ? With neat diagram explain operation of routers in OSI model. **(W-12, 8 Marks)**

Q. 9 Describe the role of following network devices used in computer network : Router. **(S-14, 1 Mark)**

Q. 10 With the help of neat sketch describe the working of Router. Describe in detail the operation of Router considering OSI model. **(S-15, 8 Marks)**

Q. 11 State the function of : 1. Hub 2. Router **(W-16, 2 Marks)**

Q. 12 With the help of neat diagram, describe the working of routers. Also enlist types of routers. **(S-17, 8 Marks)**

Definition :

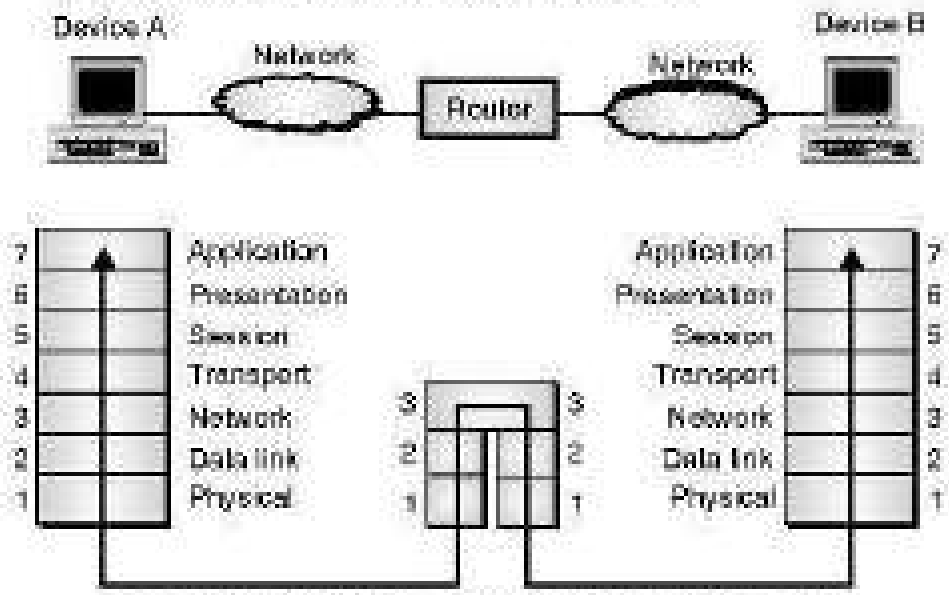
- Router is a networking device which forwards the data packets between computer networks.
- Routers perform the traffic directing function on the Internet.

Functions :

- The two important functions, performed by a router are :
  1. Determination of path (routing).
  2. Packet forwarding.

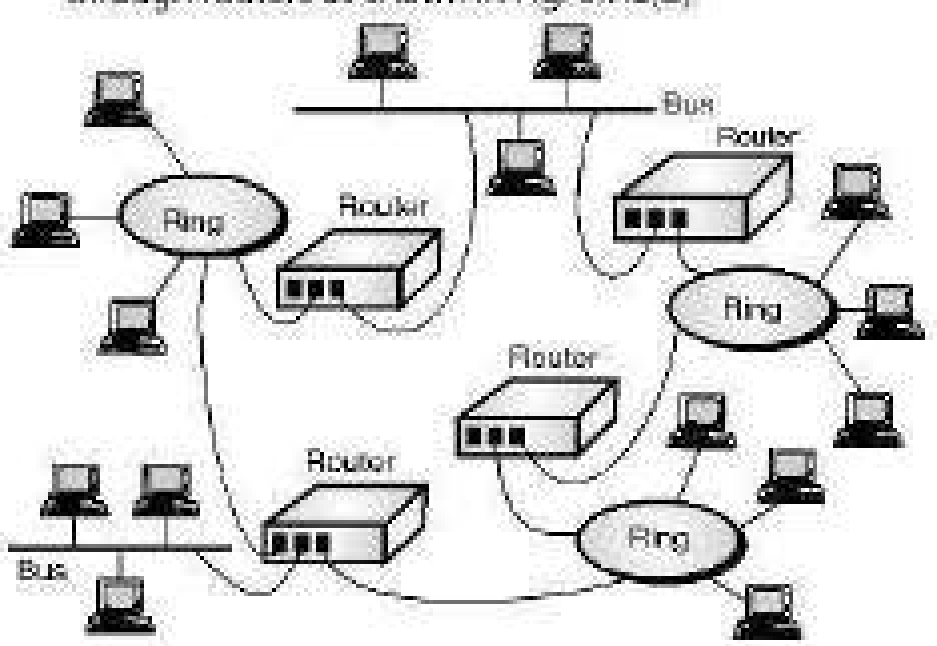
OSI layer :

- Routers work at the network layer of the OSI model.
- Routers are devices that connect two or more networks as shown in Figs. 9.7.1(a) and (b). They consist of a combination of hardware and software.



(G-364) **Fig. 9.7.1(a) : A router in the OSI model**

- The hardware can be in the form of a network server, a separate computer or a special device, as well as the physical interfaces to the various networks in the internetwork.
- Various types of networks can be interconnected through routers as shown in Fig. 9.7.1(b).



(G-365) **Fig. 9.7.1(b) : Routers in an internet**

- The software in a router are the operating system and the routing protocol. Management software can also be used.
- Routers use logical and physical addressing to connect two or more logically separate networks.
- The large network is organized into small network segments called as subnets and these subnets are interconnected via routers.
- Each of the subnet is given a logical address. This allows the networks to be separate but still access each other and exchange data.
- Data is grouped into packets, or blocks of data. Each packet has a physical device address as well as logical network address.
- The network address allows routers to calculate the optimal path to a workstation or computer.
- Route discovery is the process of finding the possible routes through the internetwork and then building routing tables to store that information.
- The two methods of route discovery are :
  1. Distance vector routing 2. Link state routing.

Types of routers :

- Following are different types of routers :

1. Wired routers.
2. Wireless routers.
3. Core and edge routers.
4. Virtual routers.
5. Broadband routers.

9.8 Gateways :

W-03, S-05, W-06, S-08, W-10, S-12, S-14, W-14, W-15, W-16, S-17, I-Scheme : W-19

MSBTE Questions

Q. 1 Describe gateways. State the situation under which gateways are necessary in the network. **(W-03, 2 Marks, W-10, 4 Marks, W-15, 8 Marks)**

Q. 2 Identify gateways and state in which layer of OSI reference model they operate. List uses of it. **(S-05, 8 Marks)**

Q. 3 What is a gateway ? Explain and state its operation. **(W-06, 8 Marks)**

Q. 4 State the situation under which gateways are necessary in the network. Give one example. **(S-08, S-12, W-14, 4 Marks)**

Q. 5 Identify the following devices operate in which layer of OSI reference model : Gateway. **(W-10, 4 Marks)**

Q. 6 Describe the role of following network devices used in computer network : Gateway. **(S-14, 1 Mark)**

Q. 7 What are the situations under which gateways are used in networks ? **(W-16, 4 Marks)**

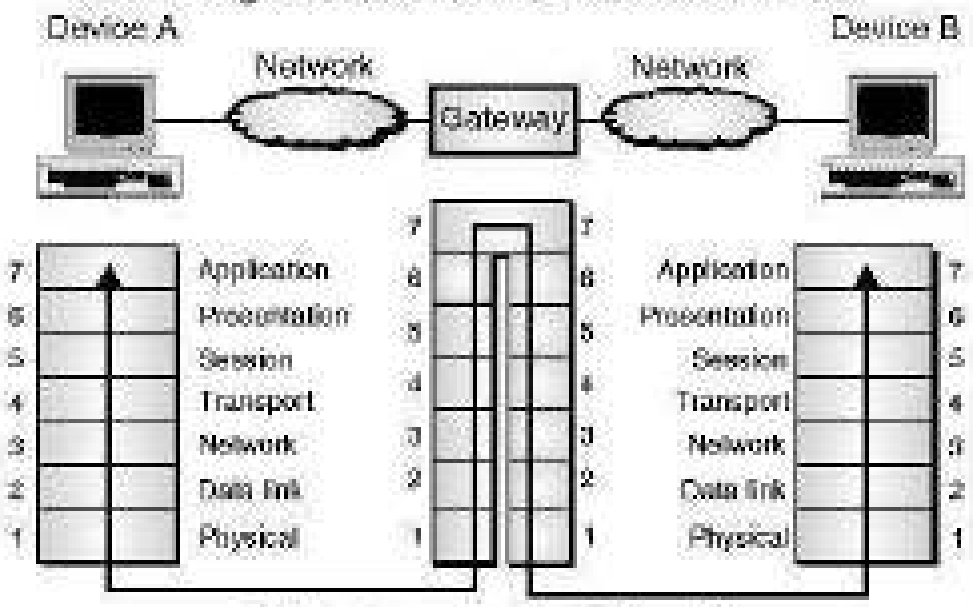
Q. 8 With neat diagram explain gateways. **(S-17, 4 Marks)**

Definition :

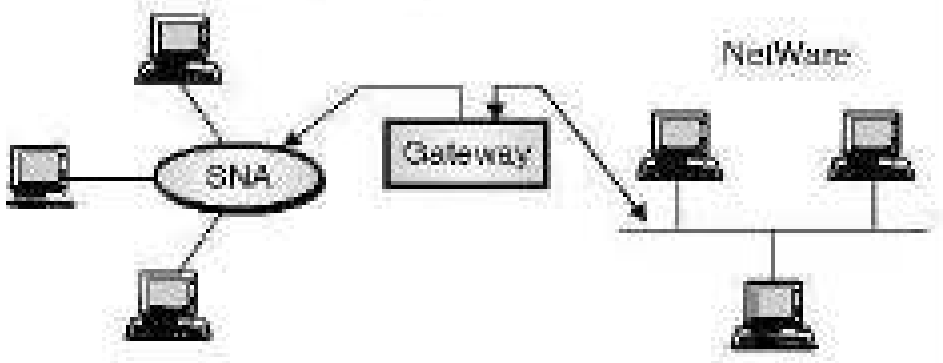
- Gateway is a network connecting device that connects two dissimilar networks together.

Diagram :

- Fig. 9.8.1(b) shows the diagram showing a gateway connecting two dissimilar networks SNA and LAN.



(a) A gateway in the OSI model



(b) A gateway

(S-366) **Fig. 9.8.1**

When to use a gateway ?

- When the networks that must be connected are using completely different protocols from each other, a powerful and intelligent device called a **gateway** is used.

Functions of a gateway :

- A gateway is a device that can interpret and translate different protocols that are used on two distinct networks as shown in Figs. 9.8.1(a) and (b).
- Gateways comprise of software, dedicated hardware or a combination of both.
- Gateway operate through all the seven layers of the OSI model and all five layers of the internet model.
- A gateway can actually convert data so that it works with an application on a computer on the other side of the gateway.
- For e.g. a gateway can receive e-mail message in one format and convert them into another format.
- Gateways can connect systems with different communication protocols, languages and architecture. For e.g. IBM networks using Systems Network Architecture (SNA) can be connected to LANs using a gateway.

Note : Gateways are slow because they need to perform intensive conversions.

9.9 Switches :

S-05, W-10, S-14. I-Scheme : W-19, S-22

MSBTE Questions

Q. 1 Identify switches and state in which layer of OSI reference model they operate. List uses of it. **(S-05, 2 Marks)**

Q. 2 Identify the following devices operate in which layer of OSI reference model : Switch. **(W-10, 4 Marks)**

Q. 3 Describe the role of following network devices used in computer network : Switch. **(S-14, 1 Mark)**

Definition :

- A switch is a networking device which connects devices together on a computer network by using packet switching to receive, process and forward data to the destination.

Which layer of OSI model ?

- Switches generally operate at the data link layer of the OSI model but some switches can work at the network layer too.

Role of a switch :

- A switch is a device which provides bridging functionality with greater efficiency.
- A switch acts as a multiport bridge to connect devices or segments in a LAN.
- The switch has a buffer for each link to which it is connected.

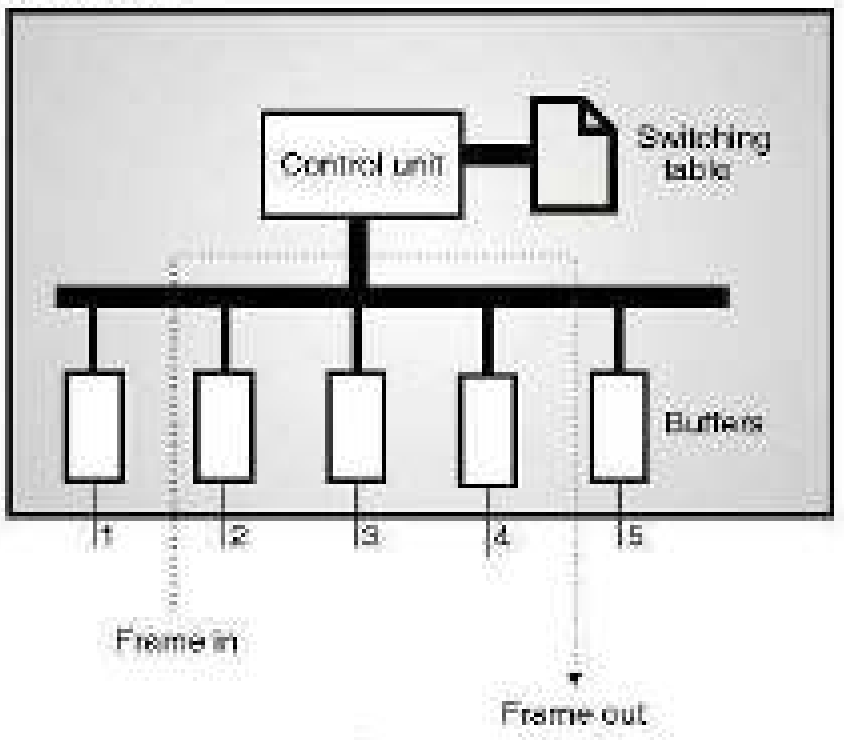
- When it receives a packet, it stores the packet in the buffer of the receiving link and checks the address to find the outgoing link.
- If the outgoing link is free, the switch sends the frame to that particular link.

Types of switches :

Switches are of two types :

1. Store - and - forward switch.
2. Cut - through switch.

- A store - and - forward switch stores the frame in the input buffer until the whole packet has arrived.
- A cut-through switch, forwards the packet to the output buffer as soon as the destination address is received.
- Concept of a switch is shown in Fig. 9.9.1. As shown in the Fig. 9.9.1 a frame arrives at port 2 and is stored in the buffer.



(G-367) **Fig. 9.9.1 : Switch**

- The CPU and the control unit, using the information in the frame consult the switching table to find the output port. The frame is then sent to port 5 for transmission.

Note : Routing switches use the network layer destination address to find the output link to which the packet should be forwarded.

9.9.1 Comparison of Hub and Switch :

W-08, W-09, S-10, S-11, S-13

MSBTE Questions

Q. 1 What is the main difference between hub and switch ? **(W-08, 2 Marks)**

Q. 2 Compare Hub and Switch. **(W-09, S-13, 2 Marks)**

Q. 3 Write difference between Hub and Switches. **(S-10, 2 Marks)**

Q. 4 Compare Hub and Switch with any four points. **(S-11, 4 Marks)**

Sr. No.	Hub	Switch
1.	It is a broadcast device.	It is a point to point device.
2.	It operates at physical layer.	It operates at datalink layer.
3.	It is not an intelligent device.	It is an intelligent device.
4.	It simply broadcasts the incoming packet.	It uses switching table to find the correct destination.
5.	It cannot be used as a repeater.	It can be used as a repeater.
6.	Not a sophisticated device.	It is a sophisticated device.
7.	Not very costly.	Costly.

9.9.2 Comparison of Router and Bridge :

S-09

MSBTE Questions

Q. 1 Give the use of Routers and Bridges in computer networks. Give the difference between a router and a bridge. **(S-09, 2 Marks)**

Sr. No.	Parameter	Router	Bridge
1.	Layer in OSI model.	Network layer	Physical or data link.
2.	Operation.	Connect two or more network.	Regeneration, check MAC address.
3.	Types.	Distance vector, Link state	Transparent, Routing.
4.	Principle of working.	Uses hardware and software.	Uses tables relating the addresses and ports.
5.	Used for	Connecting networks	Connecting computers.

9.9.3 Comparison of Bridge, Switch and Hub :

S-17

MSBTE Questions

Q. 1 Compare Hub, Switch and Bridge. **(S-17, 4 Marks)**

Sr. No.	Parameter	Hub	Switch	Bridge
1.	Type of device	Broadcast	Point to point	Both
2.	Layer of operation	Physical	Data link	Physical and data link
3.	Intelligence	Not intelligent	Intelligent	Highly intelligent
4.	Duties	Simply broadcast the incoming packet	Uses switching table to find correct destination	Filtering, forwarding and blocking of frames
5.	Sophistication	Low	High	Very high
6.	Cost	Low cost	Expensive	Very expensive

9.9.4 Comparison of Bridges, Routers and Switches :

Table 9.9.1 : Comparison of bridges, routers and switches

Sr. No.	Parameter	Router	Bridge	Switch
1.	Layer in OSI model	Network layer	Physical or data link	Data link and network layer
2.	Type of device	Point to point	Point to point or broad cast	Point to point
3	Operation	It connects two or more networks	It regenerates, checks MAC address	It provides bridging operation with greater accuracy
4.	Types	Distance vector, link state	Transparent, Routing	Two layer, three layer.
5.	Intelligence	Highly intelligent	Highly intelligent	Highly intelligent
6.	Used for	Connecting networks	Filtering forwarding and blocking frames.	Uses switching table to find correct destination.

9.10 Modems : S-10, W-10, S-13

MSBTE Questions

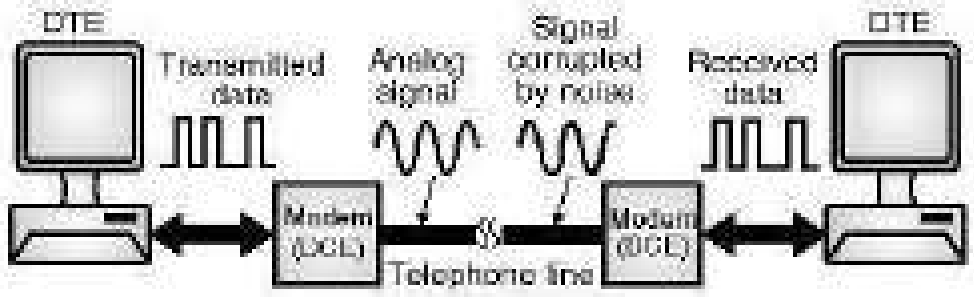
Q. 1 Describe modem. **(S-10, 1 Mark)**

Q. 2 What is modem ? **(W-10, 1 Mark)**

Q. 3 Explain the operation of a modem. **(S-13, 4 Marks)**

What is a MODEM ?

- A MODEM, is a hardware device which converts data in such a way that it is can be transmitted and received from computer to computer over telephone lines as shown in Fig. 9.10.1.



(G-148) **Fig. 9.10.1 : The role of MODEM**

- Modem is a very familiar word to everyone of us. It is used for connecting a computer to a telephone line. It is a combination of modulator and demodulator.
- The telephone lines are designed to carry analog signals and their bandwidth also is limited so they cannot be used for digital data transmission..
- A modem converts the digital data from computers to analog signals and puts it on the telephone lines on the sender side.
- If used on the receiver side the modem will convert the analog signals received on the telephone line to digital data.
- It is a bi-directional device which converts the analog signals on the telephone lines into digital data when it is used for data reception.
- Modem is a combination of two words Modulator and Demodulator.

9.10.1 Role of Modem :

W-05, S-11, S-15, S-16, S-18

MSBTE Questions

Q. 1 In which situation MODEM is useful in networks ? **(W-05, 4 Marks)**

Q. 2 Describe role of modem in transmission. **(S-11, 4 Marks)**

Q. 3 In which situation MODEMS are useful in network ? **(S-15, 4 Marks)**

Q. 4 What is role of modems in networking ? Explain types of modems. **(S-16, 4 Marks)**

Q. 5 Describe role of modem in Networking. **(S-18, 4 Marks)**

- The term 'MODEM' is derived from the words MOdulator and DEModulator. A modem contains a modulator as well as a demodulator.
- The normal digital signal cannot be put directly on the telephone lines.
- This is due to the fact that the bandwidth of the telephone lines is not sufficient to transfer the digital data without distortion.
- Therefore the digital data is first converted to a signal which is compatible to the telephone lines.
- This conversion is done by a special communications box called "MODEM".
- It is the box that makes a digital data signal compatible with any nondigital system and medium besides the phone system.
- An example is a modem which makes the data bits compatible with a microwave radio system.
- The role of MODEM can be better understood by referring to Fig. 9.10.1.
- The modem is a DCE (Data Communication Equipment) which is designed to operate with the DTE (Data Terminal Equipment). DTE is nothing else but computers.
- The principle of modem operation is based on using sine waves of various frequencies, phases or amplitudes to represent the binary data.
- Thus the binary data is converted into corresponding analog signals using modem on the sending side.
- On the receiving side, the modem converts these analog signals to corresponding digital data.

9.10.2 Functions of Modem :

W-08, W-10, S-12, W-12

MSBTE Questions

Q. 1 State function of MODEM. **(W-08, 2 Marks)**

Q. 2 State any two functions of modem. **(W-10, 2 Marks)**

Q. 3 State and explain functions of modem. **(S-12, 4 Marks)**

Q. 4 Write any four functions performed by modem at transmitting end. **(W-12, 4 Marks)**

- The functions to be performed by a modem depends on whether it is at the transmitting end or at the receiving end.

Functions to be performed at the transmitting end :

- Take the data from the RS-232 interface.
- Convert the data (0s and 1s) into appropriate analog signals (modulation process).
- Perform the line control and signalling to the other end of phone line.
- Send dialing signals if this modem is designed to dial without the presence of the user.
- Have protection against line overload and other problems.

Functions of receiving modem :

- Receive the analog signals and demodulate them into 1s and 0s.
- Put the demodulated signal into RS-232 format and connect to RS-232 interface.
- Perform line control and signalling.
- Have protection against line overload and other problems.
- Recover data with minimum number of errors from the received signal corrupted by noise.

9.11 Null Modem :

S-07, S-16

MSBTE Questions

Q. 1 Draw and describe the function of Null modem. **(S-07, 4 Marks)**

Q. 2 What is role of modems in networking ? Explain types of modems. **(S-16, 4 Marks)**

- If an observer stands between the DTE and DCE to observe the RS 232 interface, it is seen that a signal which comes out of a particular pin of DTE port goes toward DCE on the same pin.
- That means in any pair of corresponding pins of the DTE and DCE ports, one is the output pin and the other is the input pin.
- Hence in order to use RS 232 to interconnect any two devices, it is necessary that a DTE thinks that it is connected to a DCE, irrespective of whether the other devices is a DCE or not.
- Thus we can connect a computer and a terminal directly using RS 232 interface if one of them has a DCE port and the other has a DTE port as shown in Fig. 9.11.1(a).

(a) DTE - DCE interconnection

(b) DTE - DCE direct interconnection

(c) DTE - DCE interconnection using a Null modem

(G-1062) Fig. 9.11.1 : Use of a Null Modem

- However if both the devices that are to be interconnected have only the DTE ports, then one of the device has to "look like" a DCE. (see Fig. 9.11.1(b)).
- A null modem does this job as shown in Fig. 9.11.1(c). It converts a DTE port to DCE port and vice versa.
- Thus we can connect two DTEs using a Null Modem.

9.12 Wireless Infrastructure Components :

I-Scheme : W-19

- Following are the important wireless infrastructure components used for the wireless LANs.
  1. Radio NICs.
  2. Access points.
  3. Routers.
  4. Repeaters.
  5. Antennas.
  6. User devices.

9.12.1 Radio NICs :

I-Scheme : W-19

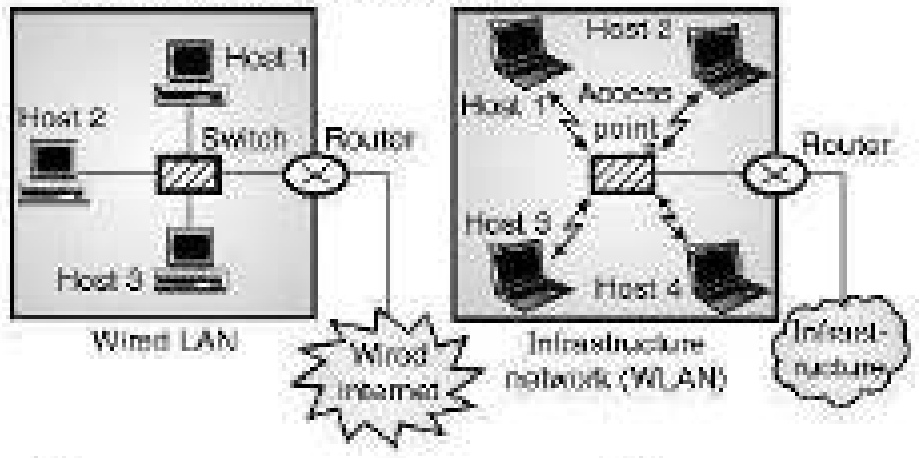
- NIC means network interfacing card. Radio NIC is a very important part of wireless LAN.
- Radio NIC operates inside the computer and provides wireless connectivity.
- Radio NIC is also called as the radio card and implements the 802.11 wireless LAN standard.
- Radio NICs generally implement one particular physical layer i.e. 802.11 a or 802.11 b/g.

9.12.2 Access Point (A.P.) :

I-Scheme : W-19

Definition :

- In computer networking an Access Point (A.P.) is a device that allows a Wi-Fi device to connect to a wired network.
- Refer Fig. 9.12.1(a), which shows the manner in which a wired LAN is connected to some other network such as the Internet through a **router.**
- It is possible to connect a wireless LAN either to a wired infrastructure network or a wireless infrastructure network, or to another wireless LAN.
- Fig. 9.12.1(b) shows the connection of a wireless LAN to a wired infrastructure network.



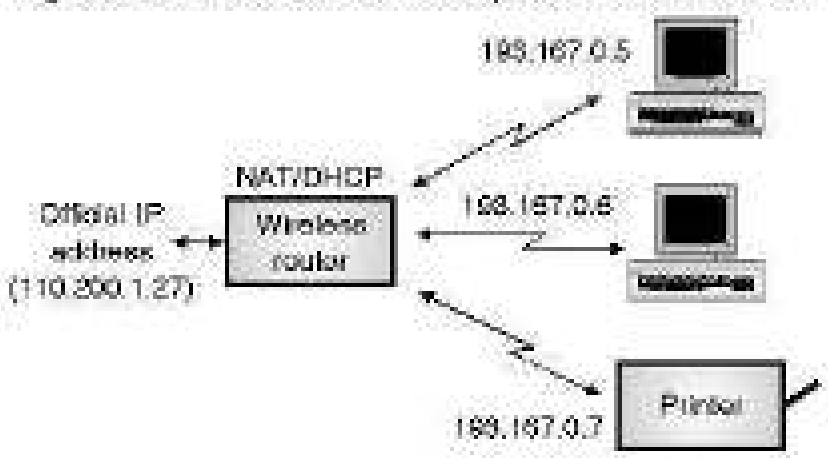
(a) **(b)**

(G-2097) Fig. 9.12.1 : Connection of wired LAN and wireless LAN to the other network

- Consider Fig. 9.12.1(b). In this case the wireless LAN is called as **infrastructure network.**
- It is connected to the wired infrastructure such as the Internet through a special device called as **Access Point (AP).**
- The communication between the wireless hosts and AP is wireless in nature whereas that between the AP and the wired infrastructure is a wired communication.
- An access point contains a radio card which communicates with the individual user devices as well as the wired NIC.
- Access Point (A.P.) is a station that transmits and receives data. Each A.P. can serve multiple users within a specified network area.
- As a user moves beyond this area, it is automatically handed over to the next A.P.
- A small WLAN may require only one A.P but their number increases with the increase in the size of the wireless network.
- Generally the adjacent APs use different frequencies to communicate with their clients to avoid interference, between the nearby wireless networks.
- Access points can have major security issues. If an A.P. is connected to a wired network, then anybody within the range of that A.P. can get connected to the network.
- Therefore every wireless A.P. must be protected with a password.

9.12.3 Wireless Routers : I-Scheme : W-19

- A router transfers packets between networks.
- The function of a wireless router is same as that of the router used in the wired networks.
- A wireless LAN router consists of a multiport Ethernet router alongwith a built in Access Point (A.P.).
- A typical wireless LAN router includes four Ethernet parts, an 802.11 Access Point and sometimes a parallel port so that it an be a print server.
- Routers implement the Network Address Translation (NAT) protocol that enables multiple network devices to share a single IP address provided by an Internet Service Provider (ISP).
- Fig. 9.12.2 illustrates the concept of wireless router.

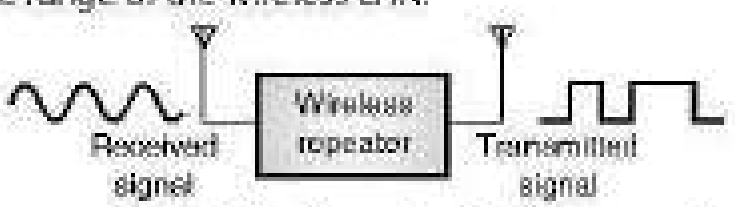


(G-2396) **Fig. 9.12.2 : Concept of a wireless router**

- In home and small office setup, the ISP provides a single IP address through DHCP to the wireless router and it then provides IP addresses through DHCP to clients on the local network.
- However wireless routers are not preferred in larger implementations such as hospitals. Instead Access Points are preferred.

9.12.4 Wireless Repeaters : I-Scheme : W-19

- APs play an important role in providing coverage in most wireless LANs. But wireless repeaters are used for extending the range of a wireless LAN, instead of adding more APs (that are expensive).
- Fig. 9.12.3 illustrates the concept of a wireless repeater. It simply regenerates the network signal and extends the range of the wireless LAN.



(G-2397) **Fig. 9.12.3 : Concept of wireless repeater**

- It does not use wires but receives the radio signals from an AP, end users, or other repeaters, regenerates the signal and retransmits it.
- We can overcome the signal impairment caused by RF attenuation, with the help of repeaters.

Demerit :

- As a repeater retransmits every received frame, the effective traffic on the network is doubled.
- This problem will further increase due to the use of multiple repeaters and therefore degrades the performance of a WLAN.
- Hence repeaters should be used carefully.

9.12.5 Antennas : I-Scheme : W-19

- Most of the wireless LAN antennas are omnidirectional and have low gain.
- Standard antennas are used in all the Access Points (APs), repeaters and wireless routers.
- Sometimes we need to use directional antennas for covering a long narrow area.
- Sometimes antennas are integrated within a radio card or Access Point.

Review Questions

Q. 1 Explain transceivers.

Q. 2 Give the classification of network connecting devices.

Q. 3 With the help of a diagram show the relation between connecting devices and OSI model.

Q. 4 Which layer does a repeater belong to ? Explain the operation of a repeater.

Q. 5 How does signal regeneration take place at the repeater ?

Q. 6 What is hub ? Explain different types of hubs.

Q. 7 Compare hub and switch.

Q. 8 What is a bridge ? Which layer of OSI does it operate in ?

Q. 9 What is filtering in bridge ?

Q. 10 State the types of bridges and explain the operation of a bridge.

Q. 11 Explain routers.

Q. 12 Write a note on gateways.

Q. 13 State the types of switches.

Q. 14 Explain the need and operation of switches.

Q. 15 Compare router and bridge.

Q. 16 What are modems ? What is the role of modem ?

Q. 17 Name different modulation techniques used in modem.

Q. 18 Explain the operation of modem.

9.13 MSBTE Questions and Answers :

Q. 1 Give two applications of :

1. Modems 2. Routers. **(W-16, 4 Marks)**

Ans. :

Applications of modems :

1. In broadband connectivity.
2. Modem is used to connect computer to communicate with wired or wireless devices.
3. In remote management.

Applications of routers :

1. To connect multiple LANs.
2. To connect same or different networks.
3. Used to connect WAN (Internet) to LAN.

9.14 I-Scheme Questions and Answers :

Summer 2019 [Total Marks - 02]

Q. 1 Compare router and repeater. **(2 Marks)**

Ans. :

Comparison of router and repeater :

Sr. No.	Parameter	Repeater	Router
1.	Layer in OSI model	Physical layer	Network layer
2.	Function	To regenerate the received signal	To connect two or more networks
3.	Types	-	Distance vector, Link state
4.	Principle of working	To identify data amidst noise and to reconstruct & retransmit it	Uses hardware & software

Winter 2019 [Total Marks - 10]

Q. 2 Describe different connecting devices used in computer network.
(Sections 9.4, 9.5, 9.6, 9.7, 9.8 and 9.9) **(4 Marks)**

Q. 3 Describe wireless infrastructure components in detail.
(Sections 9.12, 9.12.1, 9.12.2, 9.12.3, 9.12.4 and 9.12.5) **(6 Marks)**

Summer 2022 [Total Marks - 08]

Q. 4 List different types of network connecting devices.
(Section 9.1.1) **(2 Marks)**

Q. 5 Explain the working of hub, switch and bridge.
(Sections 9.5, 9.6 and 9.9) **(6 Marks)**

❑❑❑

Chapter 10

OSI Reference Model

Syllabus

OSI reference model : Layered architecture, Peer-to-Peer Processes-Interfaces between layer, Protocols, Organization of the layers, Encapsulation layers of the OSI reference model (Functions and features of each layer and protocols used) - Physical layer, Data-Link layer, Network layer, Transport layer, Session layer, Presentation layer, Application layer.

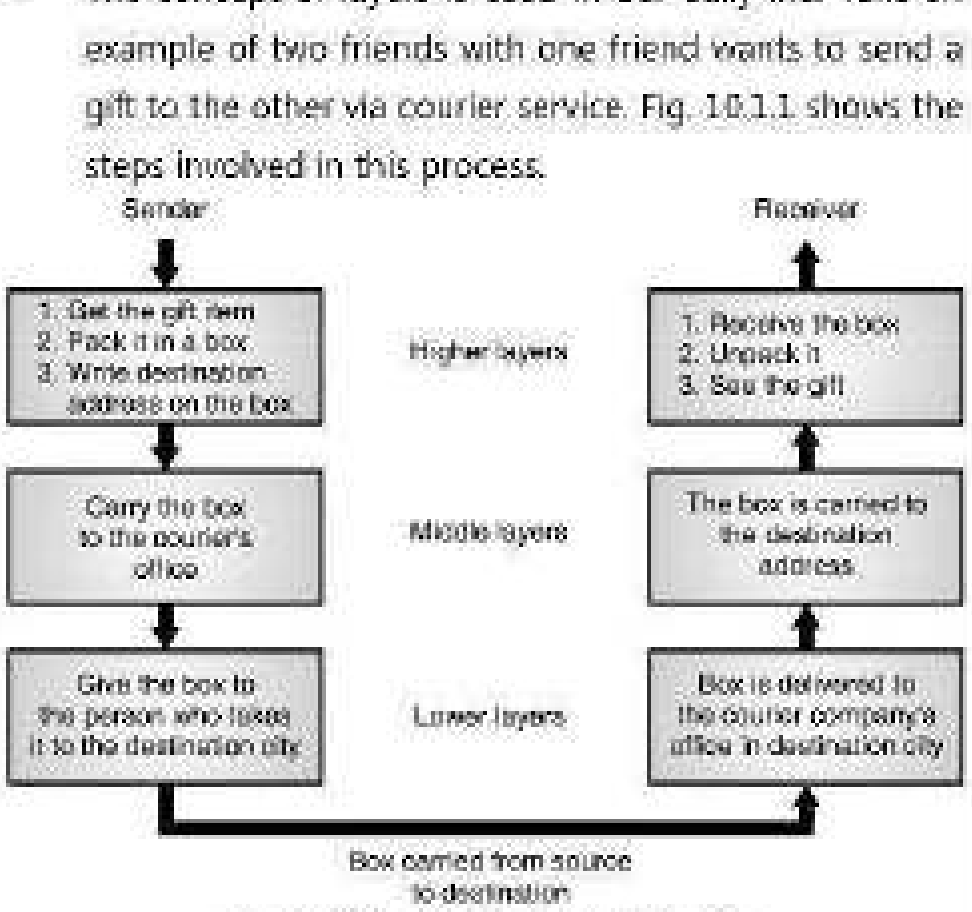
Chapter Contents

10.1 Introduction :

- A network is a combination of hardware and software that sends data from one computer to the other.
- The hardware is defined as the part of network which contains the physical equipment to carry signals from one point of network to the other.
- The software is defined as the other part of the network. Which consists of the instruction sets and program which makes it possible to carry out the expected services from the networks.
- Any task that is to be performed by a computer network can be divided into several smaller tasks each performed by a separate software package.
- Each software package uses services of another software package to carry out the task assigned to it.
- We can think of this process as a stack of layers as described in the subsection below.

10.1.1 Layered Tasks :

- The concept of layers is used in our daily life. Take an example of two friends with one friend wants to send a gift to the other via courier service. Fig. 10.1.1 shows the steps involved in this process.



(G-1546) **Fig. 10.1.1 : Layered tasks**

- In Fig. 10.1.1, we have three important persons involved namely the sender, the receiver and the carrier who carries the gift box, from one city to the other.

Hierarchy of tasks :

- The point to be noted is that in order to complete a task in day to day life small actions are being done in a hierarchical way or layered manner.

1. At the sender :

The tasks of higher layers :

1. Get the gift item.
2. Pack it in a box.
3. Write the destination address on the box.

Middle layer :

- Carry the addressed box to the office of a courier company.

Lower layer :

- Give the box to a person who will take it to the destination city.

2. At the receiver :

Tasks of lower layers :

- The box is delivered to the courier company office in the destination city.

Middle layers :

- The box is carrier by another person to the destination address and the box is delivered.

Upper layers :

1. Receive the box 2. Unpack it 3. See the gift.

Hierarchy and layered task :

- This discussion demonstrates that the important tasks are carried out by the higher layers whereas the simpler tasks are carried out by the middle and lower layers.
- In the network protocols as well the layered architecture is used.

Services :

- Referring to Fig. 10.1.1 for the sending end we can observe how each layer makes use of the services of the layer immediately below it.
- The third layer uses services of the second layer. The second layer uses services of the first layer and so on.
- The OSI model dominated the networking literature before 1990. But this model was never implemented fully.
- Instead the TCP/IP protocol suite became the more successful commercial architecture. It is used for the Internet as well. It is used by many other protocols being used Practically.
- In this chapter we are going to discuss the OSI model.

10.1.2 Network Architecture :

- A set of layers and protocols is called as network architecture.
- Protocol stack is defined as a list of protocols used for a certain system, one protocol per layer.

10.2 Reference Models :

- After discussing about the layered networks, now we will discuss two work architectures or reference models.
- The two most important reference models are :
  1. The OSI reference model.
  2. The TCP/IP reference model.
- The International Standards Organisation (ISO) covers all aspects of network communication in the Open Systems Interconnection (OSI) model.
- An OSI model is a layered framework for the design of network systems that allows for communication across all types of computer systems.
- The purpose of each layer is to offer certain services to the higher layers.
- Layer n on one machine (source) will communicate with layer n on another machine (destination).
- The rules and conventions used in this communication are collectively known as the layer n protocol.
- Basically a protocol is an agreement between the two communicating machines about how the communication link should be established, maintained and released.

10.3 OSI Model :

S-06, S-08, W-09, W-11, S-12, S-14, W-14, S-15, S-17, I-Scheme : W-19, S-22

MSBTE Questions

Q. 1 Describe OSI model with suitable diagram. **(S-06, S-14, 4 Marks, W-09, 8 Marks)**

Q. 2 Explain OSI reference model with its layered structure. **(S-08, 8 Marks, S-12, S-17, 4 Marks)**

Q. 3 What is OSI reference model ? Explain working of only data link layer in detail. **(W-11, 8 Marks)**

Q. 4 Explain the function of each layer of OSI reference model with neat diagram. **(W-14, 4 Marks)**

Q. 5 In brief describe OSI model with suitable diagram. **(S-15, 4 Marks)**

- The users of a computer network are located over a wide physical range i.e. all over the world.
- Therefore to ensure that nationwide and worldwide data communication systems can be developed and are compatible to each other, an international group of standards has been developed.
- These standards will fit into a framework which has been developed by the "International Organization of Standardization (ISO)".
- This framework is called as "Model for open system interconnection (OSI)" and it is normally referred to as "OSI reference model".

10.3.1 Layered Architecture :

S-06, W-08, S-08, S-09, W-09, S-10, W-11, S-12, S-13, S-14, W-14, S-15, S-16, W-16, S-17, I-Scheme : S-19, W-19, S-22

MSBTE Questions

Q. 1 Describe OSI model with suitable diagram. **(S-06, S-14, 4 Marks, W-09, 8 Marks)**

Q. 2 Draw neat diagram of OSI reference model. **(W-06, S-10, 4 Marks)**

Q. 3 Define : Peer **(S-08, 2 Marks)**

Q. 4 Explain OSI reference model with its layered structure. **(S-06, 8 Marks, S-12, S-17, 4 Marks)**

Q. 5 Draw the OSI reference model and state the role of each layer. **(S-09, 4 Marks)**

Q. 6 What is OSI reference model **(W-11, 4 Marks)**

Q. 7 Describe the seven layers of OSI model. **(S-13, 4 Marks)**

Q. 8 Why layered architecture is used in OSI reference model ? Discuss. **(W-14, 4 Marks)**

Q. 9 Explain the function of each layer of OSI reference model with neat diagram. **(W-14, 4 Marks)**

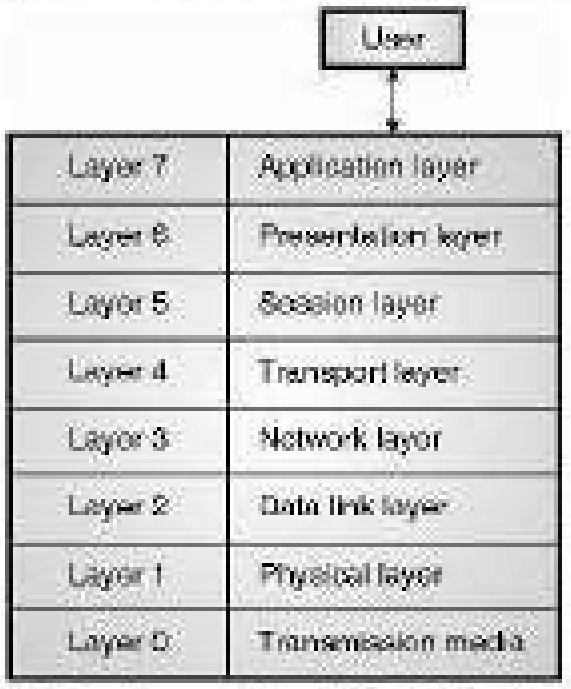
Q. 10 In brief describe OSI model with suitable diagram. **(S-15, 4 Marks)**

Q. 11 What do you mean by layered architecture ? **(S-16, 4 Marks)**

Q. 12 Draw and explain the functions of various layer of OSI reference model. **(S-16, 8 Marks)**

Q. 13 Draw a neat diagram showing the layers of OSI model and state the function of each layer. **(W-16, 8 Marks)**

- Fig. 10.3.1 shows the seven layer architecture of ISO OSI reference model. It defines seven levels or layers in a complete communication system.



(O-59) **Fig. 10.3.1 : A seven layer ISO-OSI reference model**

- The lowest layer is physical layer and highest one is called as the application layer.
- Each computer on a network uses a series of protocols to perform the functions assigned to each layer.
- These layers collectively form the protocol stack or networking stack.
- At the top of the stack we have the application and at the bottom is the physical medium which actually connects the computers to form a network.

Who developed the OSI model ?

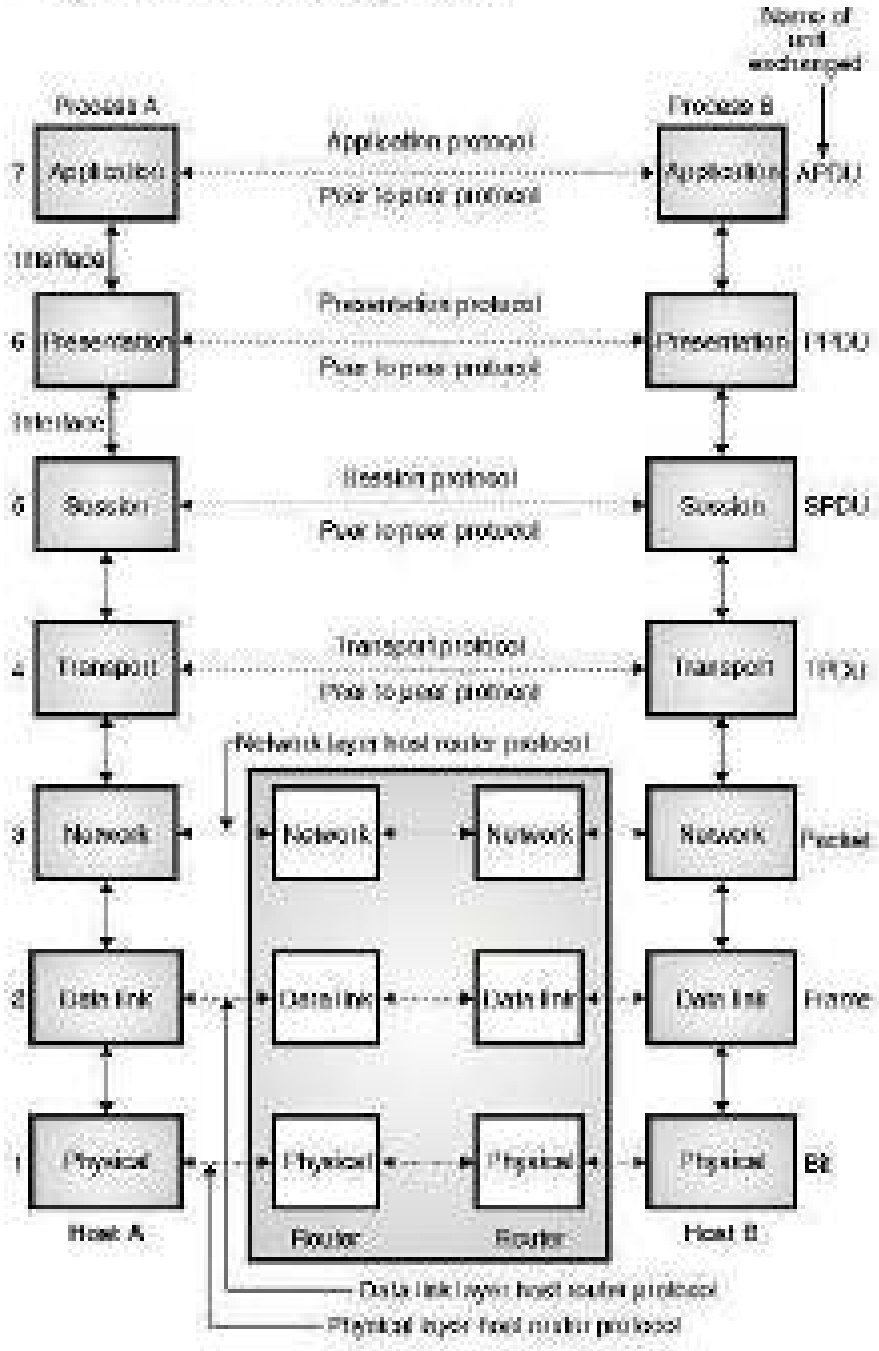
- The OSI model was developed in two different and completely independent projects by the International Organization for Standardization (ISO) and the Consultative Committee for International Telephone and Telegraphy (CCITT) which is now known as ITU-T.
- Both these organizations developed their own seven layer models. Then in 1983 the two projects were combined together.

OSI protocol suite :

- The OSI model was originally developed as a model for creating a 7 layer protocol suite. But this seven layer protocol suite never came into existence.
- In fact none of the protocol suites existing today exactly match the seven layer structure of the OSI model.
- But still the OSI reference model is so simple yet powerful that it is being used as a teaching, reference and communications tool.
- The reason why real protocol stacks differ from the OSI model is that many protocols used today were developed before the OSI model was developed.
- The TCP/IP protocols which are used extensively in practice have their own layered model. The TCP/IP reference model is discussed later on.
- Fig. 10.3.2 shows a more detailed OSI model with two hosts A and B communicating with each other.

Interface :

- An interface defines the operations and services offered by lower layer to the upper layer.
- There is an interface between each pair of adjacent layers as shown in Fig. 10.3.2.



(G-66) **Fig. 10.3.2 : The interaction between layers in the OSI model**

Peer :

- The active elements present in each layer are known as **entities.**
- The entities can be hardware entities or software entities.
- The entities comprising the corresponding layers on different machines are called as **peers.**
- The communication actually takes place between the peers using the protocol.

- The dotted lines in Fig. 10.3.2 show the virtual communication and physical communication is shown by solid lines.
- Within a single machine, each layer uses the services of the layer just below it.
- However between two machines A and B of Fig. 10.3.2 layer x on machine A will communicate with layer x on machine B.
- This communication is based on some mutually agreed rules called **protocols.**
- The processes on each machine which communicate at a given layer are called as **peer-to-peer processes.**

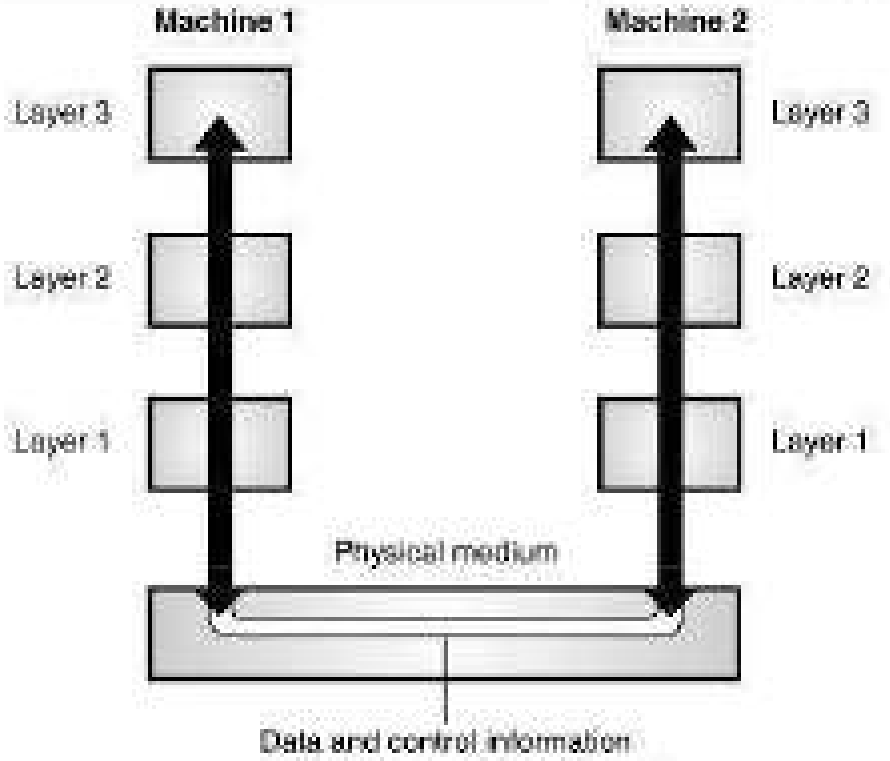
10.3.2 Peer to Peer Processes :

I-Scheme : S-22

- All the applications need not use all the seven layers shown in Fig. 10.3.1.
- The lower three layers are enough for most of the applications.
- Each layer is built from electronic circuits and/or software and has a separate existence from the remaining layers.
- Each layer is supposed to handle message or data from the layers which are immediately above or below it.
- This is done by following the protocol rules. Thus each layer takes data from the adjacent layer, handles it according to these rules and then passes the processed data to the next layer on the other side.

Interlayer communication :

- Networking is defined as the process of sending and receiving messages.
- The protocol stack illustrated by the OSI model defines the basic components needed to transmit the messages to their destinations.
- Just as the way we package a letter by placing it in an envelope and write an address on it, the networking protocols also package the data generated by an application, puts an address on it and sends to the destination computer.
- In order to get an idea of interlayer communication, let us take a simple example first. Consider a three layer model of Fig. 10.3.3.



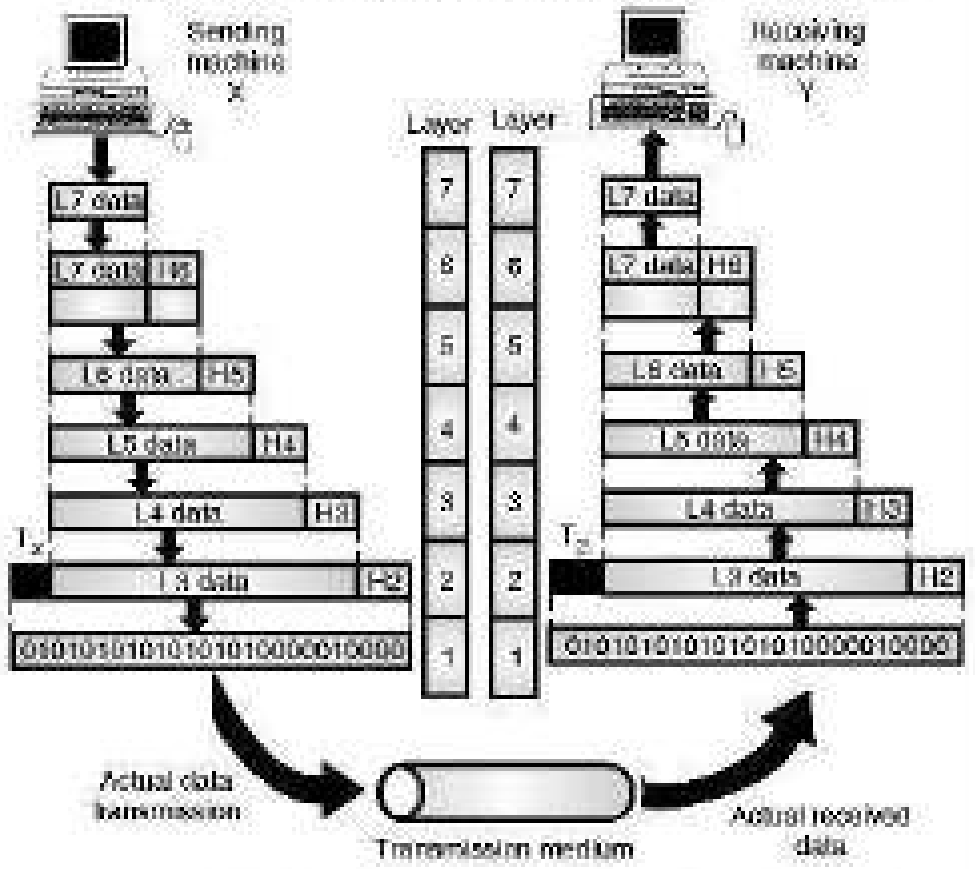
(S-50) **Fig. 10.3.3 : Data transfer**

- We want the data to get transferred from layer-3 of machine-A to layer 3 of machine-B.
- But the data does not get transferred directly from layer 3 of one machine to layer 3 of the other machine. Instead the data transfer takes place as explained below.
- The data and control information is passed on from the topmost layer to the lower layers until the lowest layer (layer 1) is reached.
- Below layer 1 lies the physical medium such as coaxial cable, through which the actual communication takes place.
- This is shown in Fig. 10.3.3. This is called as the actual communication between the layers.

10.3.3 Organization of the Layers :

- The seven layers in the OSI model can be considered to belong to three subgroups as follows :
  1. Subgroup 1 : Physical, data link and network-network support layers. (layers 1, 2 and 3)
  2. Subgroup 2 : Session, Presentation and application-user support layers. (layers 5, 6 and 7)
  3. Subgroup 3 : Transport layer linking of subgroups 1 and 2.
- The first subgroup consists of layers 1, 2 and 3 i.e. the physical, data link and network layers.
- They are important for the physical aspects of moving data from one computer to the other.
- The second subgroup is made up of the upper three layers (5, 6 and 7) i.e. session, presentation and application layers.

- This is called as the user support layers. They allow the interaction between unrelated software systems.
- The third subgroup consists of only the fourth layer i.e. the transport layer. It links the subgroups 1 and 2.
- The upper layers are implemented using software only whereas the lower layers are a combination of hardware and software
- The physical layer is implemented by only hardware.



(G-61) **Fig. 10.3.4 : An exchange using the OSI model**

10.3.4 Exchange of Information using the OSI Model :

- At the physical layer, communication is direct i.e. machine X sends a stream of bits to machine Y.
- At higher layers, each layer in the sending machine adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it as shown in Fig. 10.3.4.
- The information added by each layer is in the form of headers or trailers.
- Headers are added to the message at the layers 6, 5, 4, 3, and 2. A trailer is added at layer 2.
- At layer 1 the entire package is converted to a form that can be transferred to the receiving machine.
- At the receiving machine, the message is unwrapped layer by layer with each process receiving and removing the data meant for it.

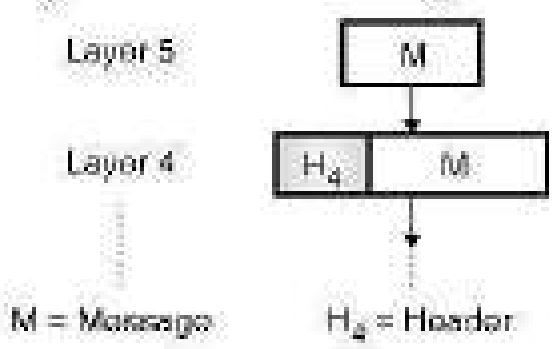
10.4 Data Encapsulation :

S-11, W-11, W-14, S-16, S-17

MSBTE Questions

Q. 1	Define : Data Encapsulation.	**(S-11, 2 Marks)**
Q. 2	Describe data encapsulation.	**(W-11, 4 Marks)**
Q. 3	Explain encapsulation with example.	**(W-14, 4 Marks)**
Q. 4	Define : Encapsulation.	**(S-16, 1 Mark)**
Q. 5	Describe data encapsulation in OSI model.	**(S-17, 4 Marks)**

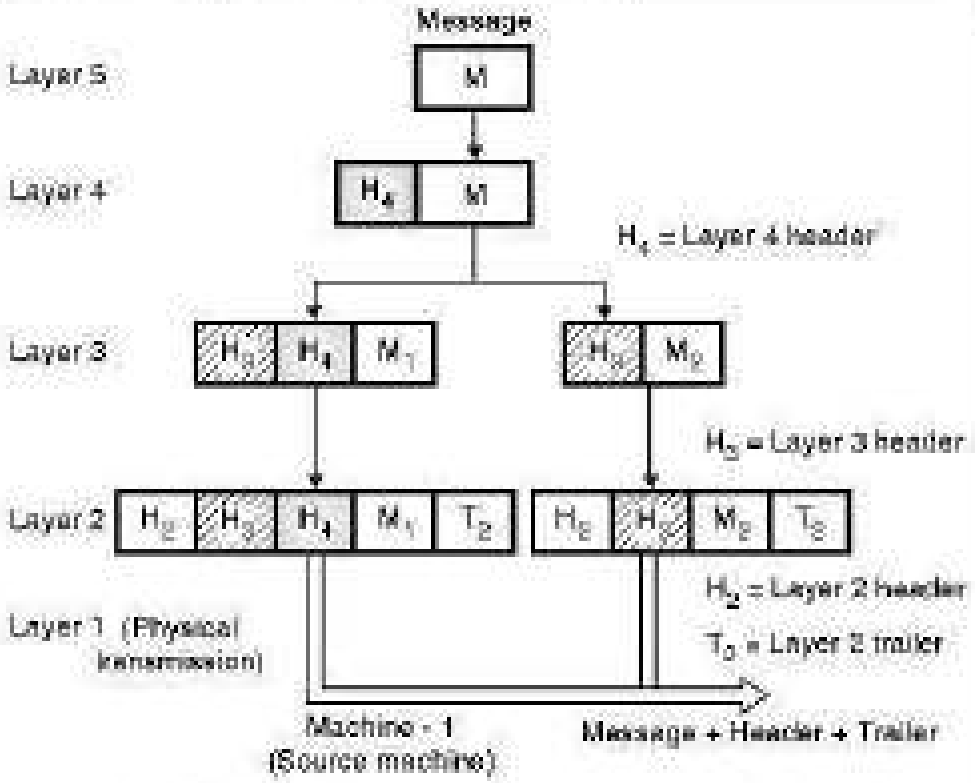
- Each layer in the layered architecture provides a service to the layers which are directly above and below it.
- That means layer 4 will provide services to layers 3 and 5.
- As discussed just now, the outgoing information will travel down through the layers to the lowest layer (network medium).
- While moving down on the source machine, the data unit acquires all the control information which is required to reach the destination machine.
- This control information is in the form of headers (and in one case a footer) which surrounds the data received from the layer above as shown in Fig. 10.4.1.



(G-1401) **Fig. 10.4.1 : Data encapsulation**

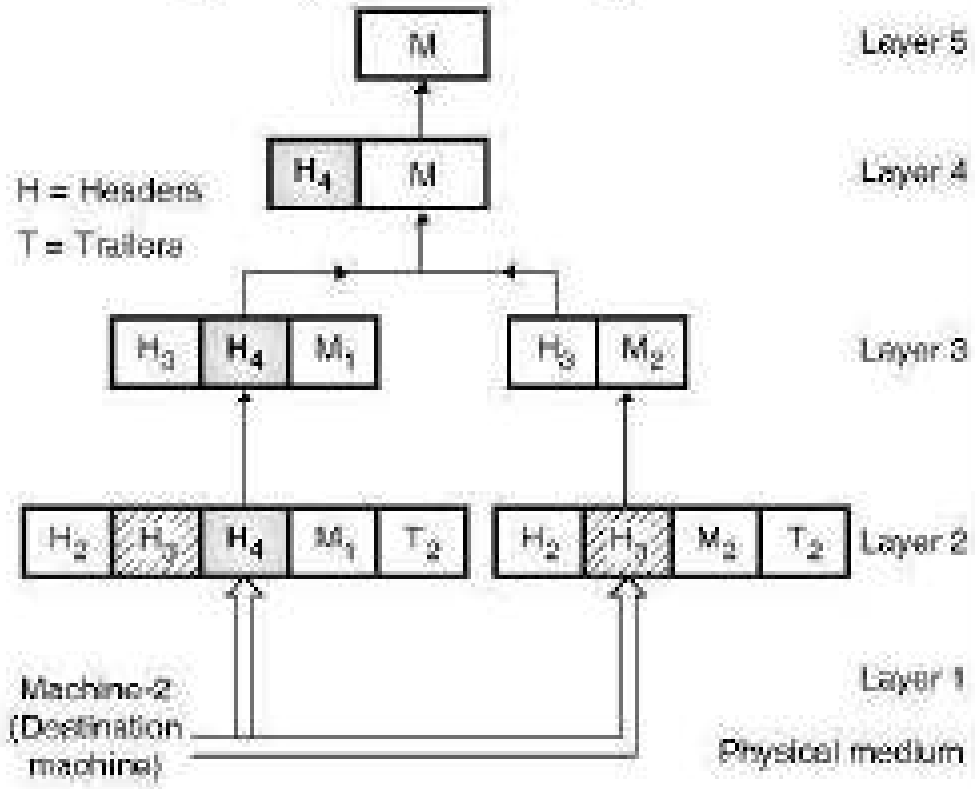
Definition of data encapsulation :

- This process of adding the headers and footers to the data is called as **Data Encapsulation** and it is demonstrated in Fig. 10.4.1.
- The headers and footers (or trailers) contain the control information in the individual fields. This control information is used to make the message packet reach the destination.
- Thus header and footer form the envelope which carries the message to the desired destination.
- This sequence of operation taking place at machine 1 is shown in Fig. 10.4.2.



(e-51) **Fig. 10.4.2 : Data encapsulation at the sending machine**

– The control information placed in headers is used at the destination machine (machine 2) to convey the message to layer 5 as shown in Fig. 10.4.3.



(e-52) **Fig. 10.4.3 : Reverse process at the destination machine**

10.4.1 A Simple Example of Data Encapsulation :

– Let us take an example of a 5 layer stack and understand the process of data encapsulation.

– Consider two machines with a 5-layer protocol stack. The 5th layer of sending machine wants to send a message "M" to the 5th layer of the destination machine.

– Then the sequence of data encapsulation takes place at the sending machine (Machine - 1) as follows :

– Refer Fig. 10.4.2 and go through the steps given below to understand the data encapsulation.

Step 1 : A messages M is produced by layer 5 of machine 1 and given to layer 4 for transmission.

Step 2 : Layer 4 adds a header H_4 in front of the message so as to identify the message and passes the (header + message) to layer 3.

A header includes the control information and it allow a layer 4 in machine 2 to deliver the messages in right order.

Step 3 : Layer 3 breaks up the incoming messages into small units, packets and appends a layer 3 adder to each packet M_1 and M_2 as shown in Fig. 10.4.2 and passes these packets to layer 2.

Step 4 : Layer 2 adds header as well as trailer (footer) to each packet obtained from layer 3 and hands over the resultant unit to layer 1 for physical transmission.

10.5 Interfaces and Services :

– The basic function of each layer in the layered structure is to provide service to the layer above it.

– Now we will discuss exactly what service does it provide. But before that, let us define some important terms.

10.5.1 Entities and Peer Entities : W-12

MSBTE Questions

Q. 1 Describe the terms : Entities and peer entities. **(W-12, 4 Marks)**

– An entity is defined as the active element in each layer. An entity can be either a software entity or a hardware entity.

– The example of software entity is a process and that of a hardware entity is an intelligent I/O chip.

– Entities in the same layer but on different machines are called as **peer entities.**

10.5.2 Service Provider and Service User :

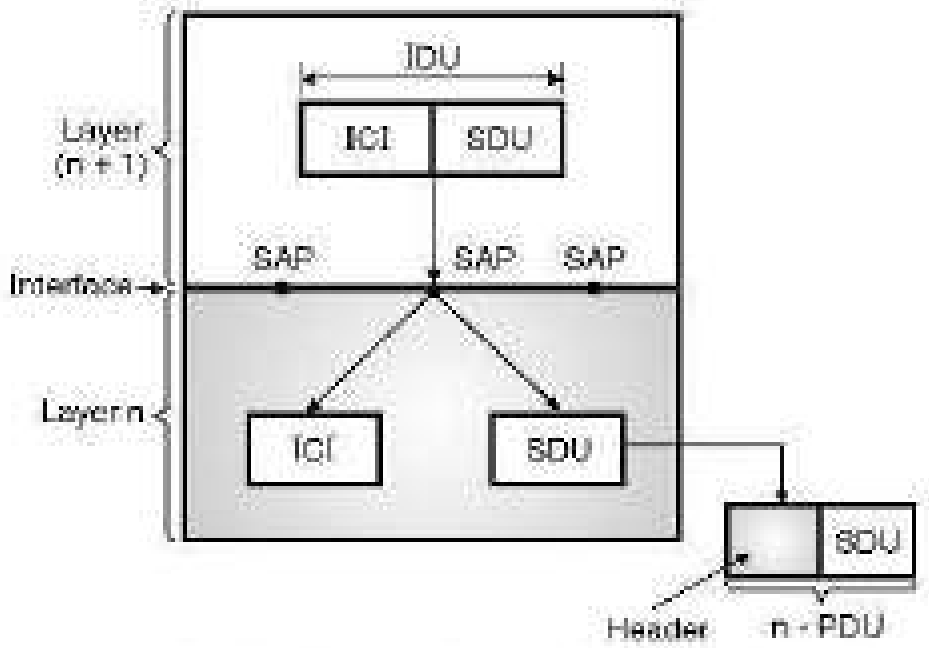
– The entities at layer n implement services for the layer (n + 1) which is above the n^{th} layer.

– So layer n which provides service is called as service provider and layer (n + 1) which takes this service is called as service user.

10.5.3 Service Access Points (SAPs) :

– Refer Fig. 10.5.1 to understand the definition of SAPs.

– The long form of SAP is service access point. They are available at the interface of n and n + 1 layer as shown in Fig. 10.5.1.



(G-56) **Fig. 10.5.1 : Relation between layers at an interface**

– Services are available at SAPs. That means the layer n SAPs are those places at the interface where layer (n + 1) can access the services being offered.

– Each SAP has a unique address for its identification.

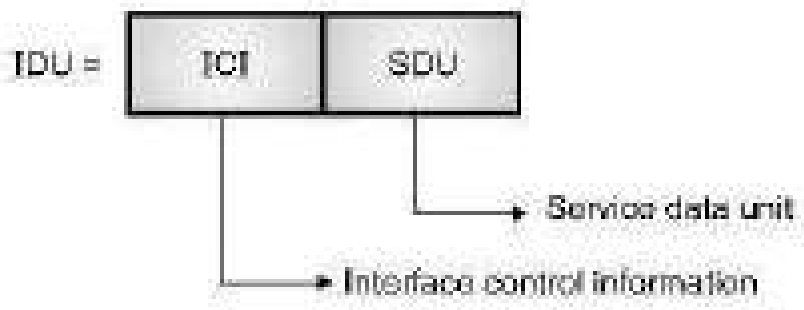
10.5.4 Interface Data Unit (IDU) : S-11

MSBTE Questions

Q. 1 Explain : Interface Data Unit (IDU). **(S-11, 2 Marks)**

– For successful exchange of information between two layers, a set of rules about the interface should be present.

– As shown in Fig. 10.5.2, the layer (n + 1) entity passes an IDU (interface data unit) to the layer n entity through the SAP.



(G-57) **Fig. 10.5.2 : IDU**

– An IDU consists of two parts namely SDU (service data unit) and ICI (interface control information).

10.5.5 Service Data Unit (SDU) :

– SDU is a part of IDU. The SDU is the information passed across the network to the peer entity and then upto layer (n + 1).

– ICI contains the control information which is necessary to help the lower layer (n) to do the necessary job.

10.5.6 Protocol Data Unit (PDU) :

W-05, S-11, W-12

MSBTE Questions

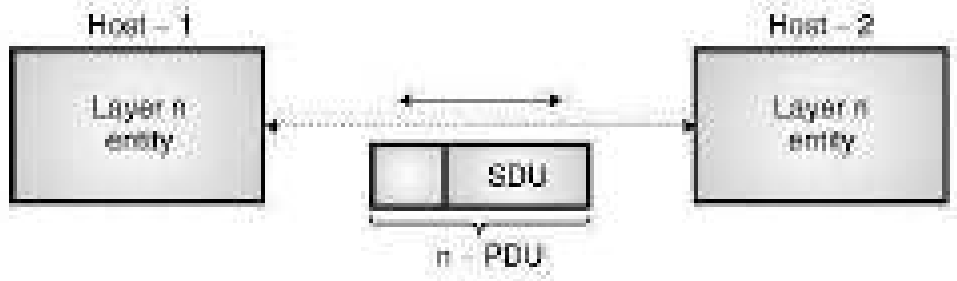
Q. 1 Describe : Protocol Data Unit (PDU). **(W-05, 2 Marks)**

Q. 2 Explain : Protocol Data Unit (PDU). **(S-11, W-12, 4 Marks)**

– In order to transfer the SDU, the layer n entity has to divide it into many smaller pieces.

– Each piece is given a header and sent as a separate PDU (Protocol Data Unit) such as a packet.

– The PDU headers are used by the peer entities to carry out their peer protocol.



(G-58) **Fig. 10.5.3 : Layer n entities exchange n-PDUs in their layer n protocol**

– Some PDUs contain data while other PDUs contain the control information. The PDU headers will identify or differentiate between different types of PDUs.

– They also provide sequence numbers and counts.

10.5.7 Connection Oriented and Connectionless Services :

S-13, S-15, W-15

MSBTE Questions

Q. 1 Explain connection oriented and connectionless services. **(S-13, S-15, 4 Marks)**

Q. 2 Define connection oriented protocol. **(W-15, 2 Marks)**

– Any layer can offer two types of services to the layer above it.

1. Connection oriented service.
2. Connectionless service.

1. Connection oriented service :

– The connection oriented service is similar to the one provided in the telephone system.

– The service users of the connection oriented service undergo the following sequence of operation :

1. Establish a connection.
2. Use the connection.
3. Release the connection.

- The connection acts like a tube. The sender pushes bits from one end of the tube and the receiver takes them out from the other end.
- The order is generally preserved. That means the order in which the bits are sent is same as the order in which they are received.
- Sometimes after establishing a connection, the sender and receiver can discuss and negotiate about parameters to be used such as maximum message size, quality of service and some other issues.

2. Connectionless service :

- The connectionless service is similar to the postal service.
- Each message (analogus to a letter) carries the full address of the destination. Each message is routed independently from source to destination through the system.
- It is possible that the order in which the messages are sent and the order in which they are received may be different.

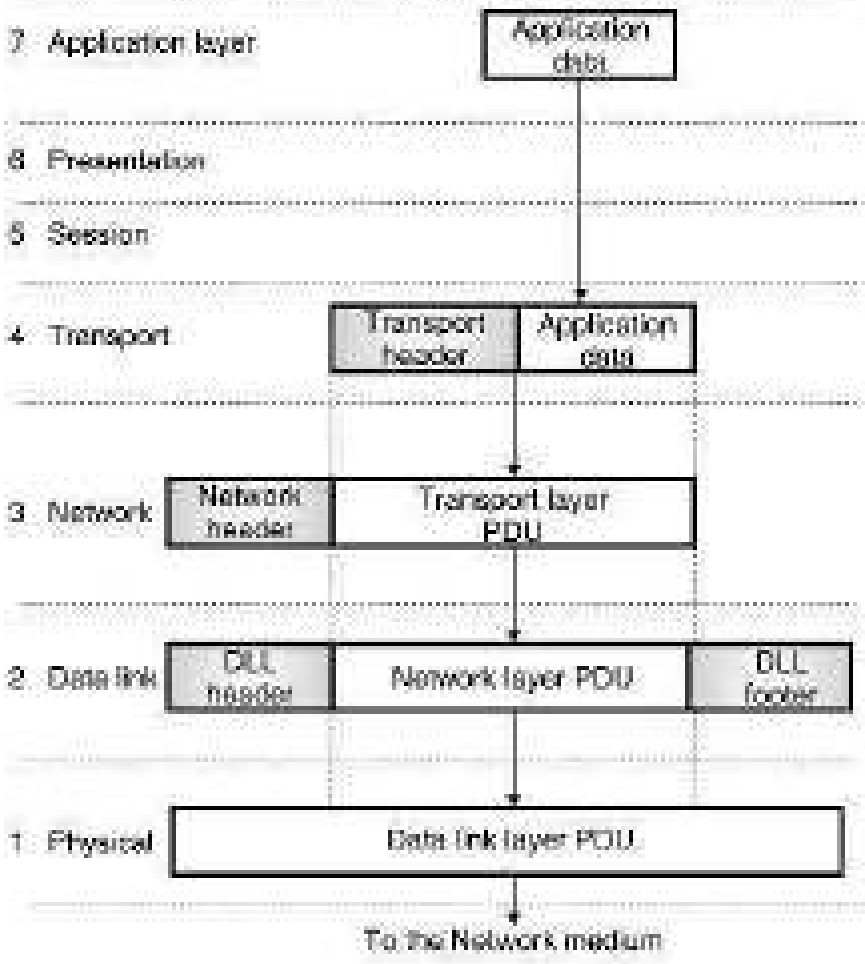
10.6 Data Encapsulation in OSI Model :

S-13, S-15

MSBTE Questions

Q. 1 Explain the data encapsulation in OSI model. **(S-13, S-15, 4 Marks)**

- We have already discussed the principle of data encapsulation. Now let us extend it and apply it to the seven layer OSI model.
- Refer Fig. 10.6.1 for the data encapsulation in OSI layer.
- An application-layer protocol which also includes the presentation and session layer functions will generate the message or data to be sent.
- This data is in a structure which is decided by the application layer protocol.
- This data is called **"application data"** is passed down to the transport layer as shown in Fig. 10.6.1.
- The transport layer protocol has its own PDU structure which includes a **transport header** and the **application data.**
- The transport layer PDU is then passed on to the network layer.
- The network layer protocol receives the transport layer PDU and encapsulates it within its own PDU by adding its own header as shown in Fig. 10.6.1.



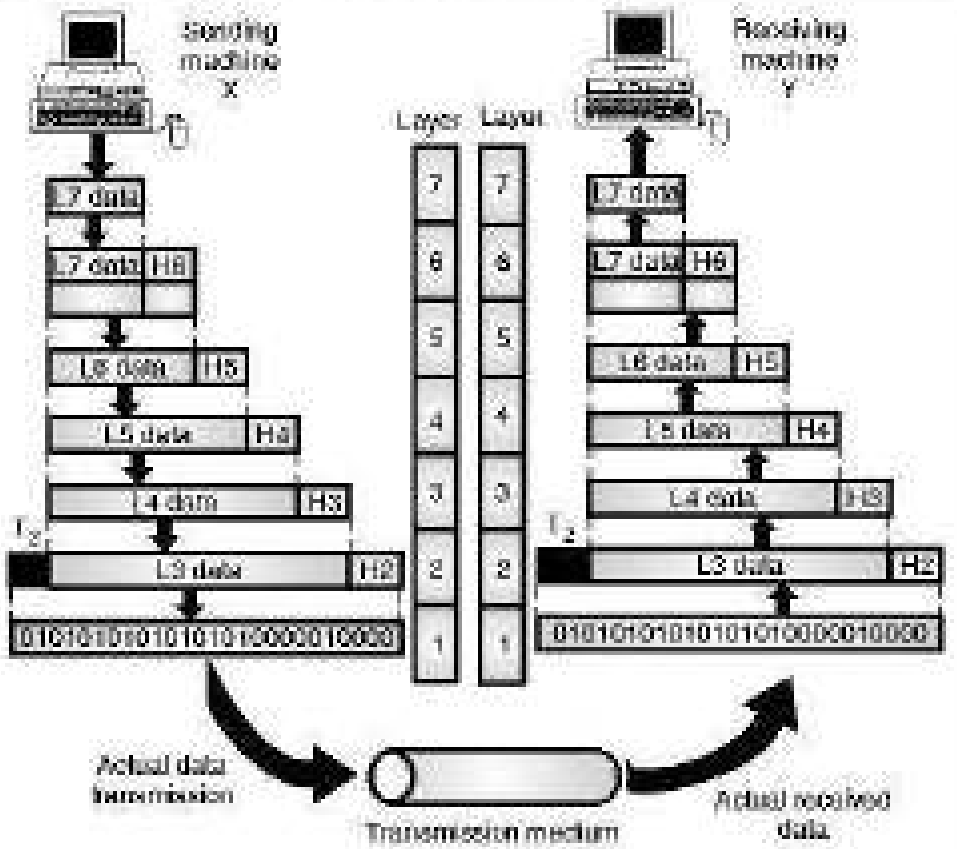
(G-1402) **Fig. 10.6.1 : Data encapsulation in OSI model**

- The network layer PDU is then passed over to the data link layer, where the DL header and footer are added to the network layer PDU, to form the data link layer PDU.
- The process of encapsulation is over at this point and the data link layer PDU is sent to the physical layer from where it is sent over a networking media such as a coaxial cable to the destination computer.
- The encapsulated packet by data link layer is called as frame.
- It has a format as shown in Fig. 10.6.2.

Data link layer header	Network layer header	Transport layer header	Application data	DL layer footer

(G-1517) **Fig. 10.6.2 : A complete encapsulated frame, ready for transmission**

- The encapsulation and de-encapsulation process is illustrated in Fig. 10.6.3.



(G-61) **Fig. 10.6.3 : Encapsulation and de-encapsulation**

10.7 Horizontal Communications :

S-08, W-10, S-11, S-12, W-12, S-14, W-14, W-15, S-17, S-18

MSBTE Questions

Q. 1 Explain horizontal communication and vertical communication.
(S-08, 2 Marks, W-10, S-12, W-14, W-15, 4 Marks)

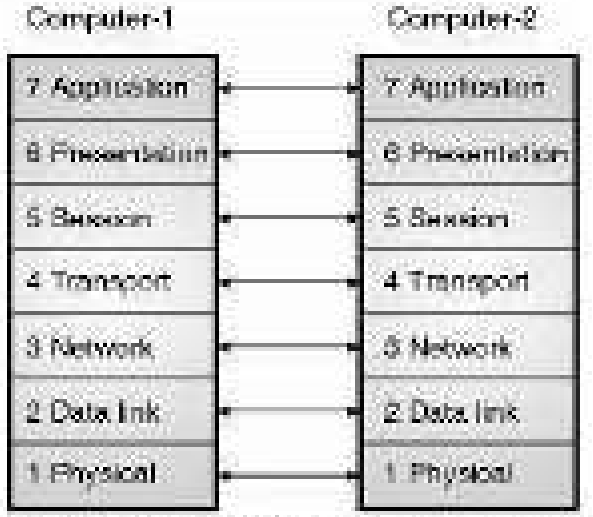
Q. 2 What is horizontal and vertical communication ?
(S-11, 4 Marks)

Q. 3 With neat diagram, explain horizontal communication. **(W-12, 4 Marks)**

Q. 4 Describe horizontal and vertical communication.
(S-14, 4 Marks)

Q. 5 Explain horizontal and vertical communication.
(S-17, S-18, 4 Marks)

- If we want two computers to communicate over a network, then the protocols used at each layer of the OSI model in the sending computer should be duplicated at the receiving end computer.
- When the encapsulated frame transmitted by the sender reaches the receiver, the process by which headers and footers are included at the source is repeated in reverse to get the message (application data).
- Note that the horizontal connections between the layers shown in Fig. 10.7.1 are logical connections.
- They are called virtual connections. There is no direct communication between them.



(G-1403) **Fig. 10.7.1 : Horizontal communication**

10.8 Vertical Communications :

S-08, W-09, W-10, S-11, W-11, S-12, S-14, W-14, W-15, S-17, S-18

MSBTE Questions

Q. 1 Explain horizontal communication and vertical communication.
(S-08, 2 Marks, W-10, S-12, W-14, W-15, 4 Marks)

Q. 2 Explain vertical communication in OSI reference model. **(W-09, 4 Marks)**

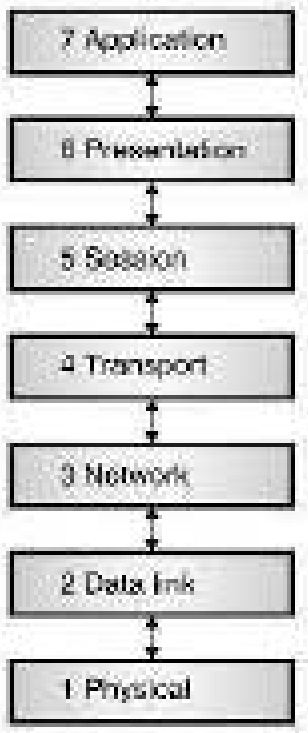
Q. 3 What is horizontal and vertical communication ?
(S-11, 4 Marks)

Q. 4 Explain vertical communication with example.
(W-11, 4 Marks)

Q. 5 Describe horizontal and vertical communication.
(S-14, 4 Marks)

Q. 6 Explain horizontal and vertical communication.
(S-17, S-18, 4 Marks)

- The headers used by the various protocols implement the specific functions carried out by those protocols.
- The header information communicates horizontally with the same protocol in the other system and it will enable each layer to communicate vertically with the layers above and below it as shown in Fig. 10.8.1.



(G-1404) **Fig. 10.8.1 : Vertical communication in OSI model**

- For example, the network layer will communicate with the data link layer and transport layer.
- This interlayer communication on the same machine is called as the **vertical communication.**
- When a system receives a packet and passes it up through various layers, the data link layer protocol header includes a field which specifies the name of network layer protocol to be used to process the packet.
- Similarly, the network layer protocol header will specify the name of transport layer protocol to be used to process the packet.
- Due to vertical communication, it becomes possible for a computer to support multiple protocols at each layer at the same time.

10.9 Encapsulation Terminology :

- Now let us see the terminology used for describing the PDUs generated by each layer.

1. Packet :

- Packet is the complete unit transmitted by sending the computer over the network medium.
- Sometimes packet is used as a generic term for the data unit at any stage in the process.

2. Frames :

- Most data link layer protocols are said to be working with frames.
- A frame includes header and footer around the data from the network layer.
- A frame is of variable size depending on the amount of data to be carried.
- The data link layer protocol which uses PDUs of uniform size such as ATM (Asynchronous Transfer Mode) uses **cells.**

3. Datagram :

- A transport layer data encapsulated by the network layer protocol such as IP (Internet Protocol) is called as a **datagram.**
- The PDUs of the user datagram protocol are also called as datagrams.

4. Fragments :

- While transmitting a datagram, sometimes it is split into small parts. Each part is called as fragment.

5. Segment and sequence :

- Transmission Control Protocol (TCP) is another example of transport layer protocol.
- The PDUs produced by the TCP are called as segments and the collection of segments is called as a sequence.

10.10 Functions of Various Layers in the OSI Model :

S-06, S-9, W-12, S-13, W-14, S-16, W-16,
I-Scheme : S-19, W-19

MSBTE Questions

Q. 1 Describe the functions of presentation layer. **(S-06, 4 Marks)**

Q. 2 Draw the OSI reference model and state the role of each layer. **(S-09, 4 Marks)**

Q. 3 Explain functions of following layers in OSI model :
1. Data link layer 2. Network layer
3. Transport layer 4. Session layer.
(W-12, 8 Marks)

Q. 4 Write the names of the layers that performs the following functions in OSI :
1. Data encryption 2. Error detection
3. File transfer 4. Data encoding
(S-13, W-14, 4 Marks)

Q. 5 Describe the seven layers of OSI model. **(S-13, 4 Marks)**

Q. 6 Explain the function of each layer of OSI reference model with neat diagram. **(W-14, 4 Marks)**

Q. 7 Draw and explain the functions of various layer of OSI reference model. **(S-16, 8 Marks)**

Q. 8 Draw a neat diagram showing the layers of OSI model and state the function of each layer. **(W-16, 8 Marks)**

Layer 1 : The physical layer :

Functions of the physical layer are as follows :

- To activate, maintain and deactivate the physical connection.
- To define voltages and data rates needed for transmission.
- To convert the digital data bits into electrical signal.
- To decide whether the transmission is simplex, half duplex or full duplex.
- A physical layer does not perform the following operations :

- It does not detect or correct errors.
- It does not decide the medium or modulation.
- The examples of the physical layer protocols are RS-232 or RS-449 standards.

Layer 2 : Data link layer :

- Functions of the data link layer are synchronization and error control for the information which is to be transmitted over the physical link.
- To enable the error detection, it adds error detection bits to the data which is to be transmitted.
- The encoded data is then passed to the physical layer.
- These error detection bits are used by the data link on layer on the other side to detect and correct the errors.
- At this level the outgoing messages are assembled into frames, and the system waits for the acknowledgements to be received after every frame transmitted.
- Correct operation of the data link layer ensures reliable transmission of each message. Examples of data link layer protocols are HDLC, SDLC and X.25 protocols.

Layer 3 : The network layer :

- The functions of network layer are as follows :
- To route the signals through various channels to the other end.
- To act as the network controller by deciding which route data should take.
- To divide the outgoing messages into packets and to assemble incoming packets into messages for the higher levels.
- In short the network layer acts as a network controller for routing data.

Layer 4 : Transport layer :

- As the name suggests this layer provides the transport services. The functions of the transport layer are as listed below :
- It decides if the data transmission should take place on parallel paths or single path.
- It does the functions such as multiplexing, splitting or segmenting on the data.
- Transport layer guarantees transmission of data from one end to the other.
- It breaks the data groups into smaller units so that they are handled more efficiently by the network layer.

Layer 5 : The session layer :

- This layer manages and synchronizes conversations between two different applications.
- This is the level at which the user will establish system to system connection.
- It controls logging on and off, user identification, billing and session management.
- In the transmission of data from one system to the other, at session layer streams of data are marked and resynchronized properly so that the ends of messages are not cut prematurely and data loss is avoided.

Layer 6 : The presentation layer :

- The presentation layer makes it sure that the information is delivered in such a form that the receiving system will understand and use it.
- The form and syntax (language) of the two communicating systems can be different e.g. one system is using the ASCII code for file transfer and the other one uses IBM's EBCDIC.
- Under such conditions the presentation layer provides the "translation" from ASCII to EBCDIC and vice versa.

Layer 7 : Application layer :

- Application layer is at the top of all. It provides different services such as manipulation of information in various ways, retransferring the files of information, distributing the results etc. to the user who is sitting above this layer.
- The functions such as LOGIN, or password checking are also performed by the application layer.
- Let us now go into the details of each and every layer.
- Table 10.10.1 shows various layers and its functions.

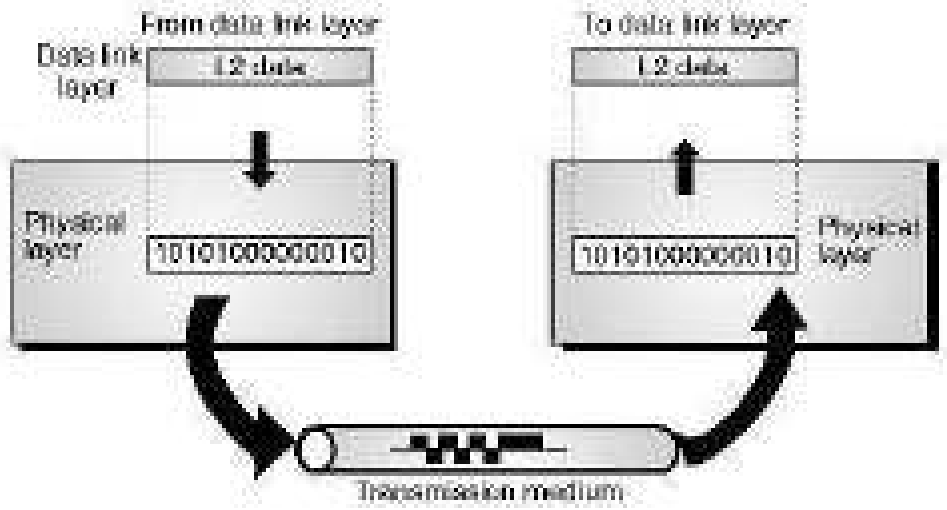
Table 10.10.1 : Functions of the layers of ISO-OSI model

Level	Name of the Layer	Functions
1.	Physical Layer	Make and break connections, define voltages and data rates, convert data bits into electrical signal. Decide whether transmission is simplex, half duplex or full duplex.

Level	Name of the Layer	Functions
2.	Data Link Layer	Synchronization, error detection and correction. To assemble outgoing messages into frames.
3.	Network Layer	Routing of the signals, divide the outgoing message into packets, to act as network controller for routing data.
4.	Transport Layer	Decides whether transmission should be parallel or single path, multiplexing, splitting or segmenting the data, to break data into smaller units for efficient handling.
5.	Session Layer	To manage and synchronize conversation between two systems. It controls logging on and off, user identification, billing and session management.
6.	Presentation Layer	It works as a translating layer.
7.	Application Layer	Retransferring files of information, LOGIN, password checking etc.

10.11 The Physical Layer :

- The physical layer defines the actual medium which is used for carrying data from one computer to another.
- The most commonly used physical layer is copper based electric cables and optical fiber cables.
- The physical layer encodes the binary data supplied by the data link layer into electric voltages, pulses of light or other impulses suitable for transmission over the network medium.
- The physical layer is responsible for sending bits from one computer to another.
- The physical layer is not concerned with the meaning of the bits, but it deals with physical connection to the network and with transmission and reception of signals.
- This level defines physical and electrical details such as what will represent a 1 or a 0, how many pins a network will have, how data will be synchronized and when the network adapter may or may not transmit the data.
- The position of the physical layer with respect to the transmission medium and the data link layer is shown in Fig. 10.11.1.



(S-62) **Fig. 10.11.1 : Physical layer**

Summary of functions performed by physical layer :

1. It defines the type of encoding i.e. how 0's and 1's are changed to signals.
2. It defines the transmission rate i.e. the number of bits transmitted per second.
3. It deals with the synchronization of the transmitter and receiver.
4. It deals with network connection types, including multipoint and point to point connections.
5. It deals with physical topologies i.e. bus, star, ring, or mesh.
6. It deals with the media bandwidth i.e. baseband and broadband transmission.
7. Multiplexing which deals with combining several data channels into one.
8. It defines the characteristics between the device and the transmission medium.
9. It defines the transmission mode between two devices i.e. whether it should be simplex, half duplex or full duplex.

Features of physical layer :

1. Physical layer is first layer of OSI model.
2. Protocol data unit generated by physical layer is **bit**.

3. The physical layer encodes the binary data supplied by the data link layer into electric voltages, pulses of light or other impulses suitable for transmission over the network medium.
4. The physical layer is responsible for sending bits from one computer to another.
5. Hubs and repeaters can operate in the physical layer.
6. It deals with physical topologies i.e. bus, star, ring, or mesh.
7. It provides services to the data link layer.

10.12 Data Link Layer :

W-04, S-07, W-09, W-11, S-12, W-15

MSBTE Questions

Q. 1 With the help of suitable diagram indicating the adjacent layers describe the functioning of Data Link Layer in the OSI reference models. **(W-04, 4 Marks)**

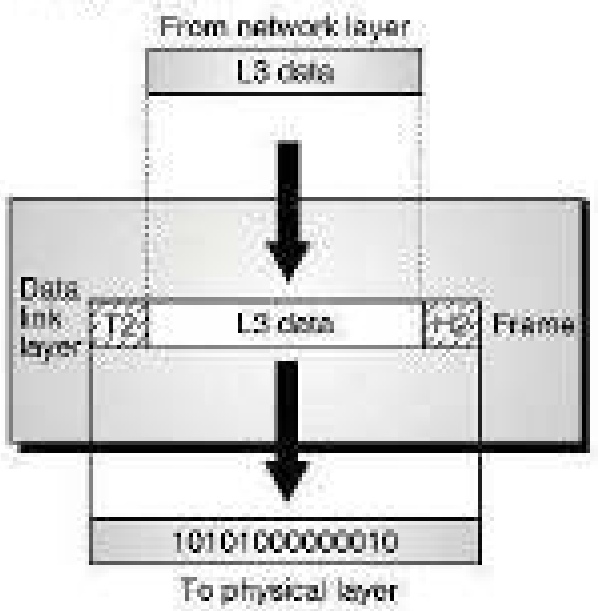
Q. 2 Draw the adjacent layers of DLL in OSI reference model and describe the major functions and responsibilities of DLL. Describe two sublayers of DLL. **(S-07, W-15, 8 Marks)**

Q. 3 Which layer of OSI reference model packages raw bits into frames ? Which sublayer of data link layer directly interacts with network card, also state it's functions ? **(W-09, 4 Marks)**

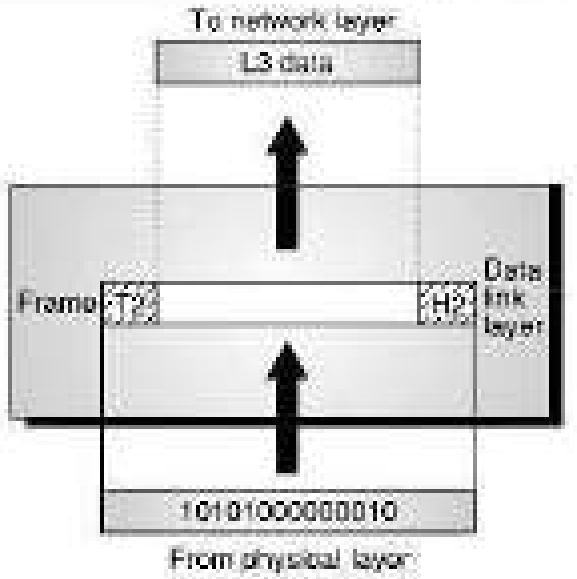
Q. 4 Explain working of only data link layer in detail. **(W-11, 4 Marks)**

Q. 5 Explain data link layer in detail. **(S-12, 4 Marks)**

– The DLL is responsible for reliable node to node delivery of the data. It accepts packets from the network layer and forms frames and gives it to the physical layer as shown in Fig. 10.12.1.



(G-63) **Fig. 10.12.1 (Contd...)**



(G-63) **Fig. 10.12.1 : Data link layer**

Features of data link layer :

1. Data link layer is second layer of OSI model.
2. Protocol data unit generated by data link layer is **frame**.
3. It is responsible for reliable node to node delivery of the data. It accepts packets from the network layer and forms frames and gives it to the physical layer.
4. Bridges, intelligent hubs and network interface cards are devices associated with the data link layer.
5. It provides a flow control mechanism to avoid a fast transmitter from over-running a slow receiver by buffering the extra bits.
6. It provides services to the network layer.

10.12.1 Functions of Data Link Layer :

S-06, S-07, W-08, S-10, W-10, W-11, S-13, S-14, W-15, S-17, S-18

MSBTE Questions

Q. 1 Describe the functions of data link layer. Describe two sublayers of data link layer. **(S-06, 8 Marks)**

Q. 2 Draw the adjacent layers of DLL in OSI reference model and describe the major functions and responsibilities of DLL. Describe two sublayers of DLL. **(S-07, W-15, 8 Marks)**

Q. 3 Give the functions of data link layer. **(W-08, S-10, S-18, 4 Marks)**

Q. 4 Which layer of OSI reference model packages raw bits into frames ? Which sublayer of data link layer directly interacts with network card, also state it's functions ? **(W-09, 4 Marks)**

Q. 5 What is OSI reference model ? Explain working of only data link layer in detail. **(W-11, 8 Marks)**

Q. 6 Explain the services provided by data link layer in OSI model. **(S-13, 4 Marks)**

Q. 7 State the names of two sublayers of data link layer. **(S-13, S-17, S-18, 2 Marks)**

Q. 8 State the functions of data link layer. **(S-17, 4 Marks)**

Following are the functions of data link layer :

1. **Framing :**

- The bits received from the network layer are divided into another type of data units called frames at the data link layer.

2. **Flow control :**

- It provides a flow control mechanism to avoid a fast transmitter from over running a slow receiver by buffering the extra bits.

3. **Physical addressing :**

- It adds a header to the frame which consists of the physical address of the sender and / or receiver of that frame.

4. **Error control :**

- A trailer is added at the end of the frame in order to achieve error control.
- It also uses a mechanism to prevent duplication of frames.

5. **Access control :**

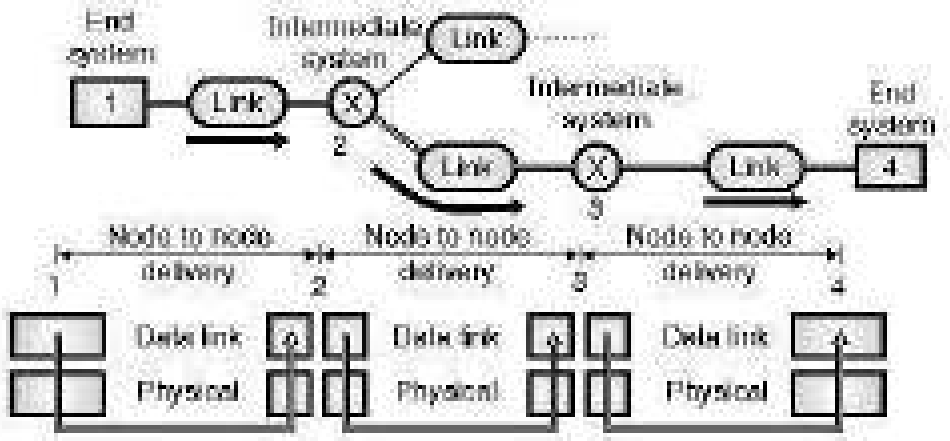
- The data link layer protocol perform an important function of determining which device has control over the link at any given time, when two or more devices are connected to the same link.
- The Institution of Electrical and Electronics Engineers (IEEE) felt the need to define the data link layer in more details, so they split it into two sub-layers :

1. **Logical Link Control (LLC) :**

- It establishes and maintains links between the communicating devices.

2. **Media Access Control (MAC) :**

- It controls the way multiple devices share the same media channel.
- The logical link control sub-layer provides Service Access Points (SAPs) that the other computers can refer to and use to transfer information from LLC to the network layer.
- The MAC sub-layer provides for shared access to the network adapter and communicates directly with the network interface cards.
- Network Interface Cards (NIC) have a unique 12-digit hexadecimal MAC address assigned before they leave the factory where they are manufactured.
- The MAC addresses are used to establish logical link between two computers on the same LAN.
- Bridges, intelligent hubs and network interface cards are devices associated with the data link layer.
- The data link layer is responsible for moving frames from one hop (node) to the next.
- Fig. 10.12.2 shows the node delivery by the data link layer.



(G-64) **Fig. 10.12.2 : Node to node delivery**

- Fig. 10.12.2 illustrates that the communication at data link layer takes place between two adjacent nodes.
- The data is being sent from end system-1 to end system-4 . To do so, partial data deliveries are made three times, from 1 to 2, from 2 to 3 and then from 3 to 4.

10.12.2 Framing :

- The bits to be transmitted is first broken into discrete frames at the data link layer.
- In order to guarantee that the bit stream is error free, the checksum of each frame is computed.
- When a frame is received, the data link there, recomputes the checksum. If it is different from the checksum present in the frame, then the data link layer knows that an error has occurred.
- It then discards the bad frame and sends back a request for retransmission.
- Breaking the bit stream into frames is called as framing. One way of doing it is by inserting time gaps between frames as shown in Fig. 10.12.3.

(G-178) **Fig. 10.12.3 : Framing**

- But practically this framing technique does not work satisfactorily, because networks generally do not make any guarantees about the timing.

– So some other methods are derived.

Framing methods :

Following methods are used for carrying out framing :

1. Character count
2. Starting and ending characters, with character stuffing.
3. Starting and ending flags with bit stuffing.
4. Physical layer coding violations.

10.12.3 Addressing :

– The data link layer protocol header contains the address of the sending computer as well as the receiving computer.

– The addresses used in this layer are the hardware (MAC) addresses.

– DLL protocols are not concerned with the delivery of packets to its ultimate destination, as long as the destination is on the same LAN.

– The only responsibility of a DLL protocol is to put the packet to the router on the local network which provides an access to the next network.

– So the destination address in the header of a DLL protocol will be that of a device on the local network and not that of the ultimate destination.

10.12.4 Access Control : S-03

MSBTE Questions

Q. 1 The IEEE 802 project divides the data link layer into two sub layers. Which sub layer of the data link layer communicates directly with the network interface card ? Describe its functions. **(S-03, 4 Marks)**

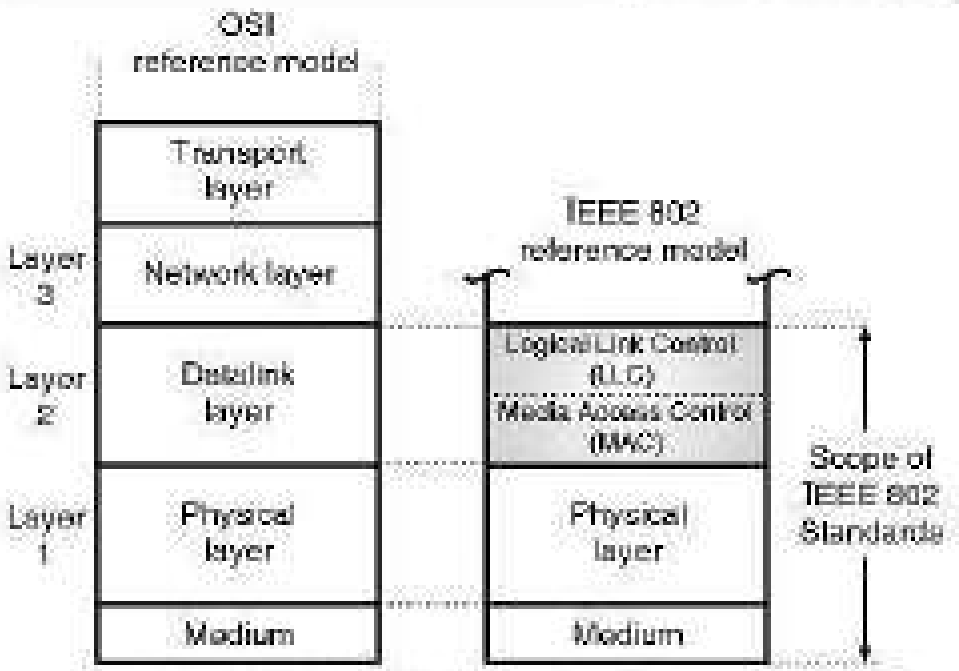
– The data link layer protocol determines which device has control over the link at any given time, when two or more devices are connected to the same link.

– The Institution of Electrical and Electronics Engineers (IEEE) felt the need to define the data link layer in more details, so they split it into two sub-layers :

1. MAC sublayer 2. LLC sublayer

– Fig. 10.12.4 shows the layered OSI model (partial) to show the position of MAC and LLC sublayers.

– We will discuss the broadcast protocols corresponding to the lower layers (1 and 2) of the OSI model as shown in Fig. 10.12.4.



(S-26S) **Fig. 10.12.4 : IEEE 802 protocol layers compared to OSI model**

– Fig. 10.12.4 relates the LAN protocols with the OSI architecture.

– This architecture was developed by IEEE 802 committee and it has been accepted as LAN standard.

– It is called as IEEE 802 reference model. Let discuss this model layer by layer.

Functions of Media Access Control sublayer (MAC) :

– To perform the control of access to media.

– It performs the unique addressing to stations directly connected to LAN.

– Detection of errors.

Functions of Logical Link Control (LLC) sublayer :

– Error recovery.

– It performs the flow control operation

– User addressing.

– It controls the way multiple devices share the same media channel.

– The logical link control sub-layer provides Service Access Points (SAPs) that the other computers can refer to and use to transfer information from LLC to the network layer.

– The MAC sub-layer provides for shared access to the network adapter and communicates directly with the network interface cards.

– Network Interface Cards (NIC) have a unique hexadecimal MAC address assigned before they leave the factory where they are manufactured.

– The MAC addresses are used to establish logical link between two computers on the same LAN.

10.12.5 Types of MAC :

W-03, S-05, W-06, S-07, W-09, W-12, S-15, S-17

MSBTE Questions

Q. 1 Describe the working of CSMA / CD protocol. **(W-03, S-05, W-09, 4 Marks)**

Q. 2 What is token passing ? **(W-06, W-12, 2 Marks)**

Q. 3 List all access methods. Explain any one. **(S-07, 4 Marks)**

Q. 4 What is token passing ? List any four protocols associated with application layer of OSI model. **(S-15, 4 Marks)**

Q. 5 State token passing. **(S-17, 2 Marks)**

- Two basic forms of MAC which are used in most of today's LAN are :
  1. Token passing method used by the token ring and FDDI.
  2. CSMA / CD i.e. carrier sense multiple access with collision detection

1. Token passing method :

- In this method, a special frame called token is passed from one workstation to the other.
- Only the system which posseses this token is allowed to transmit its data on the network.
- A workstation, after transmitting its data will release the token to the next workstation.
- This method is used by the token ring and FDDI systems.

2. CSMA/CD :

- The long form of CSMA/CD is carrier sense multiple access with collision detection.
- In this method when a workstation has to send some data, it checks the status of the network cable and if it is idle then sends the data.
- On CSMA/CD network the workstations can transmit simultaneously which results in packet collisions.
- So this system has a collision detection mechanism. When a collision is detected, the corresponding data is retransmitted. Thus the lost data will be retransmitted.

10.12.6 Carrier Sense Multiple Access (CSMA) :

W-05, W-06, S-18

MSBTE Questions

Q. 1 Describe carrier sense multiple access with collision detection. **(W-05, S-18, 4 Marks)**

Q. 2 What is CSMA ? **(W-06, 2 Marks)**

- The CSMA protocol operates on the principle of carrier sensing.
- In this protocol, a station listens to check the presence of transmission (carrier) on the cable and decides to act accordingly.

Non-Persistent CSMA :

- In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval of time..
- After this time, it again checks the status of the channel and if the channel is free it will transmit.

1-Persistent CSMA :

- In this scheme the station which wants to transmit, continuously monitors the channel until it is idle and then transmits immediately.
- The disadvantage of this strategy is that if two stations are waiting then they will transmit simultaneously and collision will take place.
- This will then require retransmission of lost data.

P-Persistent CSMA :

- The possibility of such collisions and retransmissions is reduced in the p-persistent CSMA.
- In this scheme all the waiting stations are not allowed to transmit simultaneously as soon as the channel becomes idle.
- A station is assumed to be transmitting with a probability "p".
- For example if p = 1/6 and if 6 stations are waiting then on an average only one station will transmit and others will wait.

Carrier Sense Multiple Access/Collision Detection (CSMA/CD) :

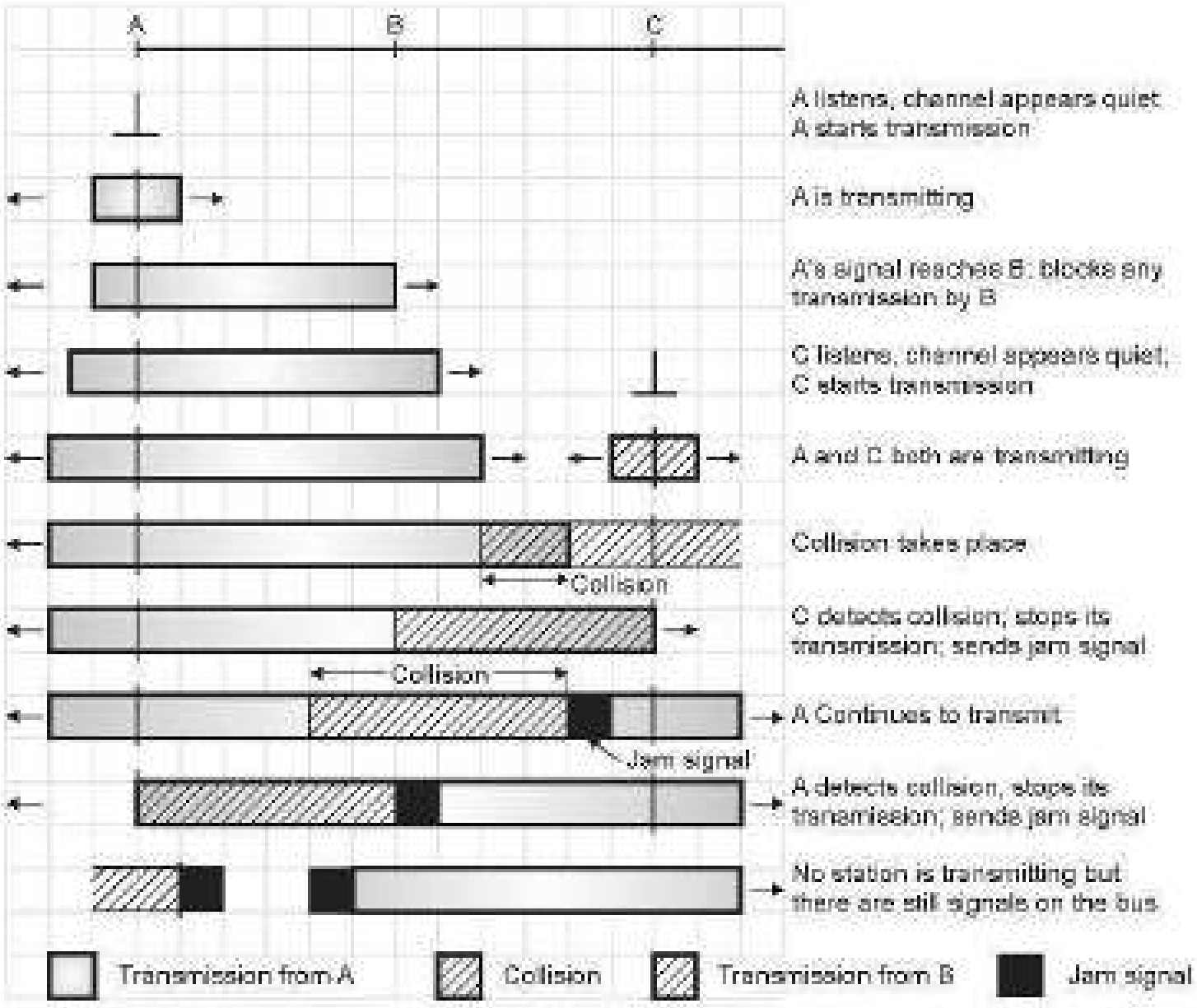
- The CSMA/CD specifications have been standardized by IEEE 802.3 standard. It is a very widely used MAC protocol.

Media Access Control :

- The problem in CSMA explained earlier is that a transmitting station continues to transmit its frame even though a collision occurs.
- The channel time is unnecessarily wasted due to this. In CSMA/CD, if a station receives other transmissions when

it is transmitting, then a collision can be detected as soon as it occurs and the transmission time can be saved.

- As soon as a collision is detected, the transmitting stations releases a jam signal.
- This jam signal will alert the other stations. The stations then are not supposed to transmit immediately after the collision has occurred.
- Otherwise there is a possibility that the same frames would collide again.
- After some "back off" delay time the stations will retry the transmission. If again the collision takes place then the back off time is increased progressively.
- A careful design can achieve efficiencies of more than 90% using CSMA/CD.
- This scheme is as shown in Fig. 10.12.5.



(G-273) **Fig. 10.12.5 : CSMA/CD scheme**

10.12.7 Space Error Control :

- The next problem to be dealt with is to make sure that all frames are eventually delivered to the network layer at the destination, in proper order.
- Generally the receiver sends back some feedback (positive or negative) to convey the information about whether it has received a frame or not.
- A positive acknowledgement (feedback) ACK indicates a successful and error free delivery of a frame.
- Whereas a negative acknowledgement (NAK) means that something has gone wrong and that particular frame needs to be retransmitted.
- Due to the presence of noise burst a frame may vanish completely. So the receiver does not receive anything and it does not react at all (no acknowledgement).
- This problem is overcome by introducing a timer in the data link layer. Its function of this timer is as follows.

Function of a timer :

- As soon as a sender transmits a frame, it also starts the data link timer.
- The timer timing is set by taking into account the factors such as the time required for the frame to reach the destination, processing time at the destination and the time required for the acknowledgement to return back.

- Normally the frame is received correctly and the acknowledgement will return back to the sender before the timer runs out.
- This shows that a frame has been received and the timer is cancelled.
- But if a frame is lost or acknowledgement is lost, then the timer will go off. This will alert the sender that there is some problem.
- The solution to this problem is that the sender retransmits the same frame.
- But when a frame is transmitted multiple times, there is a possibility that the receiver will receive the same frame two or more times and pass it to the network layer more than once. This is called as duplication.
- To avoid this each outgoing frame is assigned a distinct sequence number. This will help the receiver to distinguish retransmission.

10.12.8 Error Detection :

- This is a technique in which, the contents of the received frame are checked for presence of error.
- The PDU of DLL protocol contain the footer or trailer. This footer contains a Frame Check Sequence (FCS) field.
- The receiver system checks this field to detect the presence of any errors that have occurred during the transmission.
- The transmitting computer calculates a Cyclic Redundancy Check (CRC) value for the entire frame and includes it in the FCS field.
- The receiving system computes the CRC value again based on the received frame and compares it with the value in FCS field. If both values are same then no error.

10.12.9 Network Devices used in DLL :

The network devices used in DLL are :

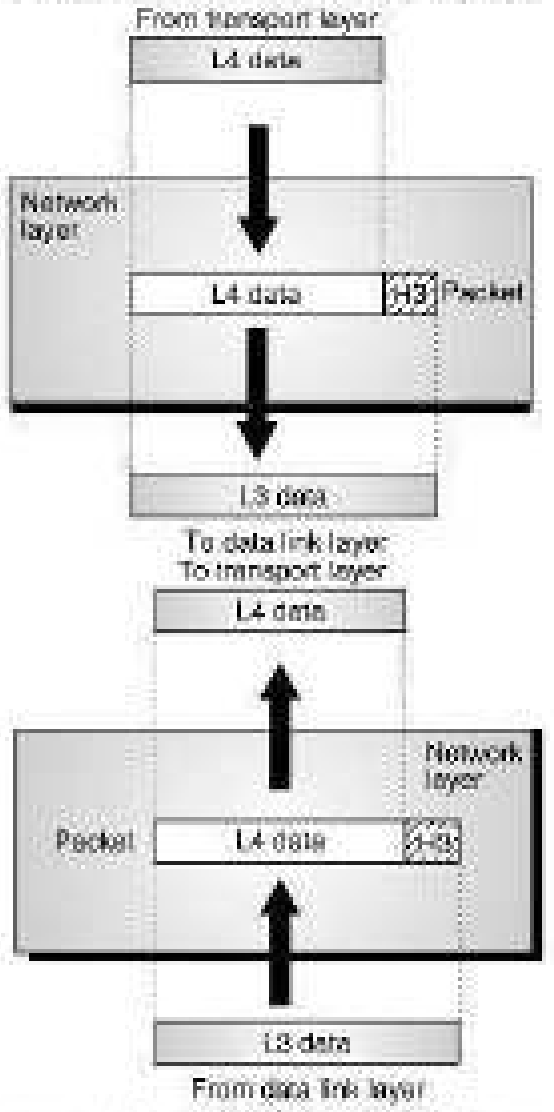
1. Bridges.
2. Intelligent hubs.
3. Network Interfacing Cards (NIC).

10.13 Network Layer : W-06, S-12

MSBTE Questions

Q. 1	Explain network layer.	(W-06, 4 Marks)
Q. 2	Explain network layer in detail.	(S-12, 4 Marks)

- The main function of this layer is to delivery packets from source to destination across multiple networks (links).
- If two systems are connected on the same link, then the network layer may not be needed.
- The relationship of the network layer to the data link and transport layer is shown in Fig. 10.13.1.



(G-65) **Fig. 10.13.1 : Network layer**

- The network layer is responsible for carrying the packet from the source all the way to destination.
- In short it is responsible for host-to-host delivery.
- The network layer has a higher responsibility than the data link layer, because the data link layer is only supposed to move the frames from one end of the wire to the other end.
- Thus network layer is the lowest layer that deals with the end to end transmission.

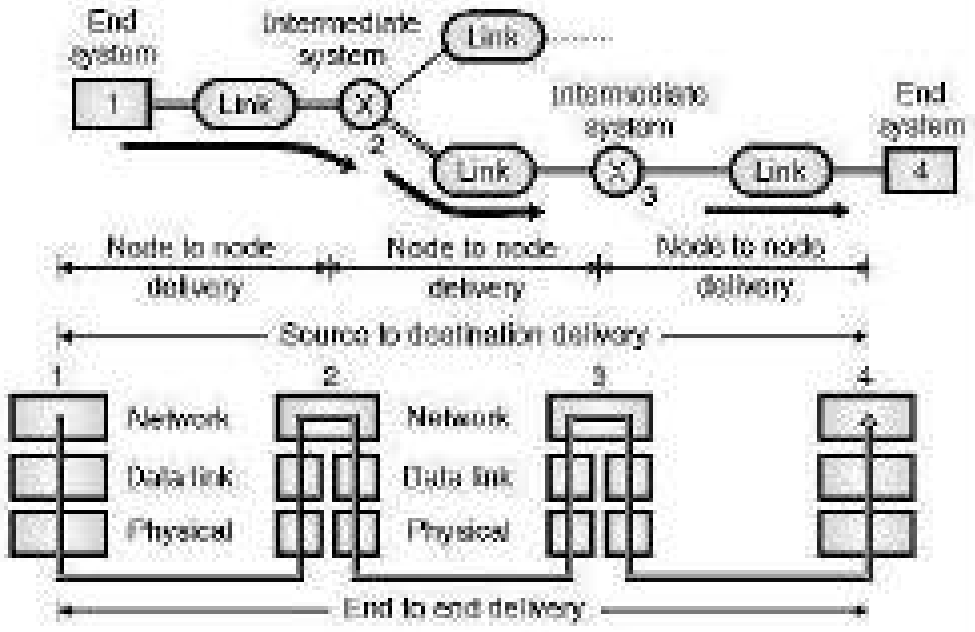
Functions of the network layer :

1. It translates logical network address into physical machine addresses i.e. the numbers used as destination IDs in the physical network cards.
2. It determines the quality of service by deciding the priority of message and the route a message will take if there are several ways a message can get to its destination.

3. It breaks the larger packets into smaller packets if the packet is larger than the largest data frame the data link will accept.
4. It is concerned with the circuit, message or packet switching.
5. It provides connection oriented services, including network layer flow control, network layer error control and packet sequence control.
6. Routers and gateways operate in the network layer.

– The network layer carries out the end to end source to destination delivery and routing.

– This is illustrated in Fig. 10.13.2.



(S-08) **Fig. 10.13.2**

– The sequence of events takes place as follows :

1. Network layer of end system-1 (source) sends the packet to the network layer of intermediate system-2 which is a router.
2. The router (2) decides the next node to which this packet should be sent on the basis of final destination. The next hop is the router (3). The network layer of 2 forward the packet to the network layer of router 3.
3. The network layer of 3 (which is again a router) will direct the packet to the network layer of end system-4.

Features of network layer :

1. Network layer is third layer of OSI model.
2. Protocol data unit generated by network layer is **Packet**.
3. Routers and gateways operate in the network layer.
4. The network layer carries out the end to end source to destination delivery and routing.
5. The network layer receives the packets from upper layer protocol and encapsulates them to form new packets.
6. Routers and Gateways are devices associated with the network layer.
7. It provides services to the transport layer.

10.13.1 Network Layer Duties :

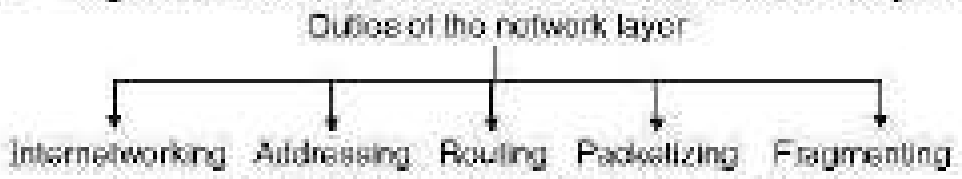
S-14, S-17, S-18

MSBTE Questions

Q. 1 What are the services provided by the network layer of OSI model ? **(S-14, S-18, 4 Marks)**

Q. 2 Explain the functions of presentation layer and network layer. **(S-17, 4 Marks)**

– Fig. 10.13.3 shows the set of duties of the network layer.



(S-13) **Fig. 10.13.3 : Duties of the network layer**

1. Internetworking :

– This is the main duty of network layer. It provides the logical connection between different types of networks.

2. Addressing :

– Addressing is necessary to identify each device on the Internet uniquely. This is similar to a telephone system.

– The addresses used in the network layer should be able to uniquely define the connection of a computer to the Internet universally.

3. Routing :

– In a network, there are multiple roots available from a source to a destination and one of them is to be chosen.

– The network layer decides which root is to be taken. This is called as routing and it depends on various criterions.

4. Packetizing :

– As discussed earlier, the network layer receives the packets from upper layer protocol and encapsulates them to form new packets.

– This is called as packetizing. A network layer protocol called IP (Internetworking Protocol), does the job of packetizing.

5. Fragmenting :

– The sent datagram can travel through different networks. Each router decapsulates the IP datagram from the received frame. Then the datagram is processed and encapsulated in another frame.

Other issues :

- The other issues which are not directly related to the duties of network layer but need to be discussed are :
  1. Address resolution.
  2. Multicasting.
  3. Routing protocols.

Other supporting protocols :

- The Internetworking Protocol (IP) needs the support of another protocol ICMP or ARP etc. in the network layer.

10.13.2 Connection Oriented and Connectionless Protocols :

W-08, S-14, W-14

MSBTE Questions

Q. 1 Define connection oriented protocol. **(W-08, 2 Marks)**

Q. 2 Describe connectionless and connection oriented protocols. **(S-14, 4 Marks)**

Q. 3 Explain connectionless and connection oriented protocol. Give the example for each type. **(W-14, 4 Marks)**

- There are two types of end to end protocols operating in the network and transport layers :
  1. Connection oriented protocols.
  2. Connectionless protocols.

1. Connection oriented protocols :

- In this type of protocols, a logical connection between the source and destination systems is established before any data is sent.

(d-1405) Fig. 10.13.4 : Connection oriented protocol

- After establishing the logical connection, the source system will transmit the data and destination system will acknowledge.
- If the acknowledgement is not received, then that packet is retransmitted.
- After successful completion of transmission the logical connection is terminated.
- The connection oriented protocols thus offer guaranteed service. However additional network traffic is generated by the connection establishment, acknowledgement and termination massager. The protocol header of this type of protocols are longer.
- TCP is an example of connection oriented protocol.

2. Connectionless protocols :

- A connectionless protocol will package the data and transmit it to the destination address without any logical connection between the sender and receiver.
- They do not even check whether the destination system is available or not. The destination system does not send any acknowledgment.
- Connectionless protocols do not guarantee, delivery of packets.
- Most of the LAN protocols in the network layer are in fact connectionless type. The examples are IP (Internet Protocol) and IPX.
- At the transport layer, both connection oriented as well as connectionless protocols are available.
- UDP is an example of connectionless protocol.

Summary of functions of network layer :

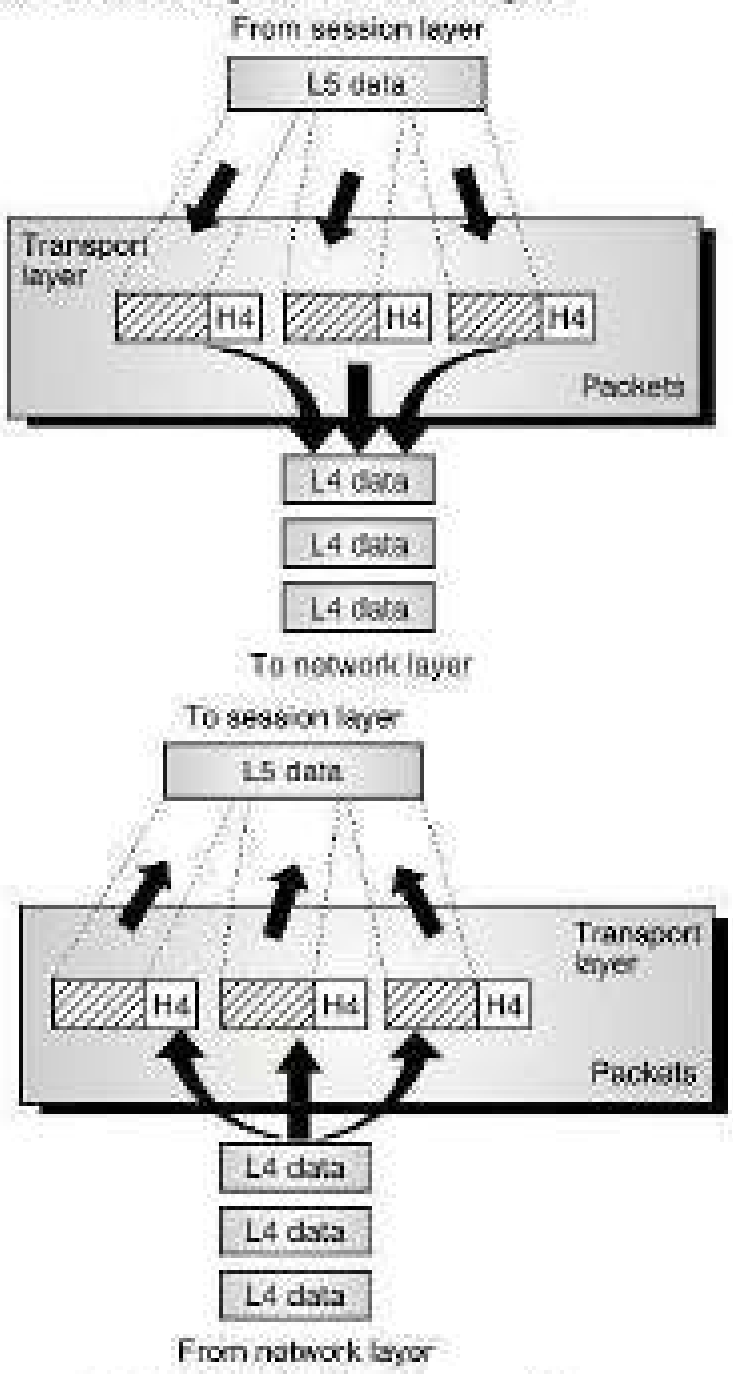
- The functions of the network layer are as follows :
  1. It translates logical network address into physical machine addresses i.e. the numbers used as destination IDs in the physical network cards.
  2. It determines the quality of service by deciding the priority of message and the route a message will take if there are several ways a message can get to its destination.
  3. It breaks the larger packets into smaller packets if the packet is larger than the largest data frame the data link will accept.
  4. It is concerned with the circuit, message or packet switching.
  5. It provides connection services, including network layer flow control, network layer error control and packet sequence control.

10.13.3 Network Connecting Devices :

- The devices operating in the network layer are :
  1. Routers.
  2. Gateways.

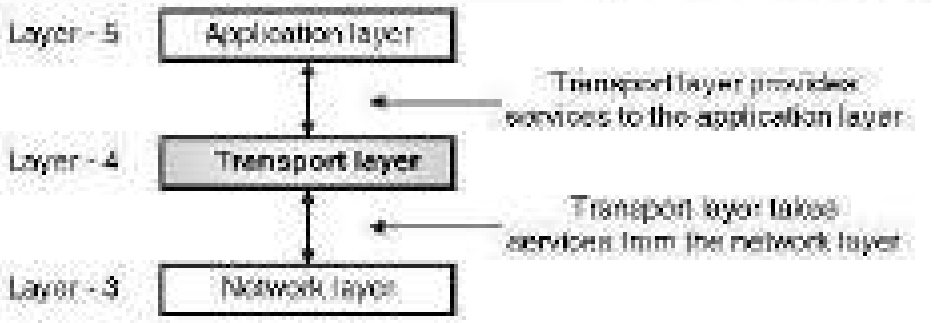
10.14 Transport Layer :

- The function of the transport layer is the process to process delivery of the entire message.
- It ensures that the whole message reaches the destination intact and in order, with both error control and flow control incorporated at the source and destination.
- Fig. 10.14.1 shows the relationship of the transport layer to the network layer and session layer.



(G-67) **Fig. 10.14.1 : Transport layer**

- The transport layer is the core of the OSI model. The application layer programs interact with each other using the services of the transport layer.
- Transport layer provides services to the application layer and takes services from the network layer.
- Fig. 10.14.2 shows the position of the transport layer in the 7-layer OSI model.
- The transport layer is fourth layer in this model. It connects the lower three layers to upper three layers of an OSI layer.



(G-1406) **Fig. 10.14.2 : Position of transport layer**

Features of Transport layer :

1. Transport layer is fourth layer of OSI model.
2. Protocol data unit generated by transport layer is **segment**.
3. Transport layer provides services to the application layer and takes services from the network layer.
4. Transport layer is meant for the process to process delivery .
5. Gateways are associated with the transport layer.
6. Transport layer provides services to the application layer and takes services from the network layer.

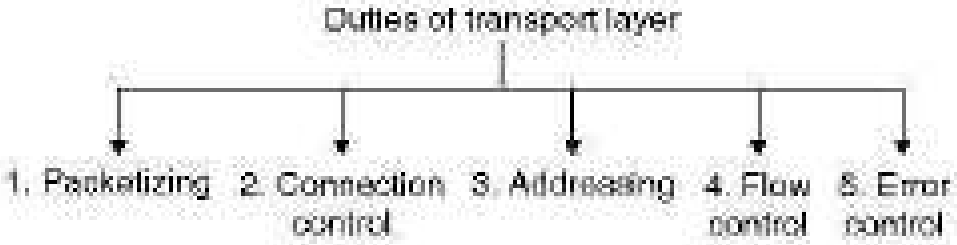
10.14.1 Duties of Transport Layer :

W-16

MSBTE Questions

Q. 1 Explain the services provided by the transport layer of the OSI model. **(W-16, 4 Marks)**

- Transport layer is meant for the process to process delivery and it is achieved by performing a number of functions.
- Fig. 10.14.3 lists the functions of a transport layer.



(G-1407) **Fig. 10.14.3 : Duties of transport layer**

1. Packetizing :

- The transport layer creates packets with the help of encapsulation on the messages received from the application layer. Packetizing is a process of dividing a long message into smaller ones.
- These packets are then encapsulated into the data field of the transport layer packet. The headers containing source and destination address are then added.
- The length of the message which is to be divided can vary from several lines (e-mail) to several pages.

- But the size of the message can become a problem. The message size can be larger than the maximum size that can be handled by the lower layer protocols.
- Hence the messages must be divided into smaller sections. Each small section is then encapsulated into a separate packet.
- Then a header is added to each packet to allow the transport layer to perform its other functions.

2. Connection control :

- Transport layer protocols are divided into two categories :
  1. Connection oriented.
  2. Connectionless.

Connection oriented delivery :

- A connection oriented transport layer protocol establishes a connection i.e. virtual path between sender and receiver.
- This is a virtual connection. The packet may travel out of order. The packets are numbered consecutively and communication is bi directional.

Connectionless delivery :

A connectionless transport protocol will treat each packet independently. There is no connection between them. Each packet can take its own different route.

3. Addressing :

- The client needs the address of the remote computer it wants to communicate with.
- Such a remote computer has a unique address so that it can be distinguished from all the other computers.

4. Flow and error control :

- For high reliability the flow control and error control should be incorporated.
- **Flow control :** We know that data link layer can provide the flow control. Similarly transport layer also can provide flow control. But this flow control is performed end to end and not across a single link.
- **Error control :** The transport layer can provide error control as well. But error control at transport layer is performed end to end and not across a single link. Error correction is generally achieved by retransmission of the packets discarded due to errors.

Congestion control and QoS :

- The congestion can take place in the data link, network or transport layer. But the effect of congestion is generally evident in the transport layer.
- Quality of Service (QoS) can be implemented in other layers but its actual effect is felt in the transport layer.
- The transport layer enhances the QoS provided by the network layer.

Summary of transport layer functions :

The transport layer performs the following functions :

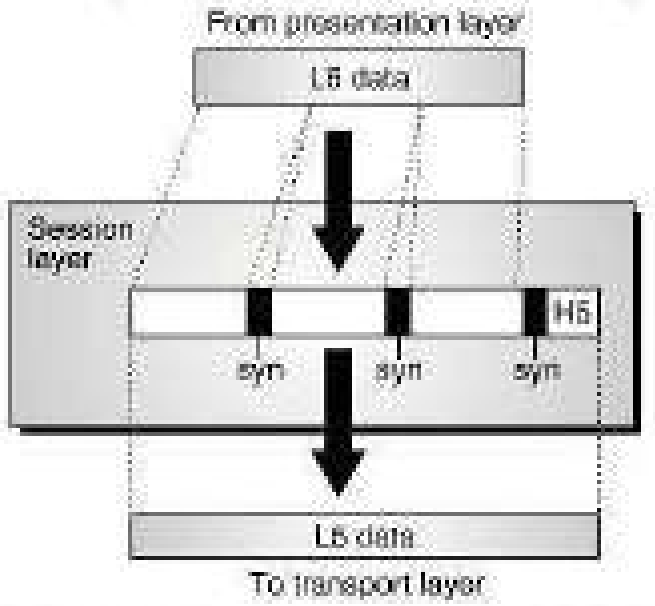
1. It divides each message into packets at the source and re-assembles then at the destination.
2. The transport layer header includes a service point address to deliver a specific process from source to a specific process at the destination.
3. The transport layer is capable of either connectionless or connection-oriented transfer of data.
4. It performs end to end flow control. Flow control is an important function of the transport layer.
5. It makes sure that the entire message arrives at the receiving transport layer without error.

10.15 The Session Layer : W-05

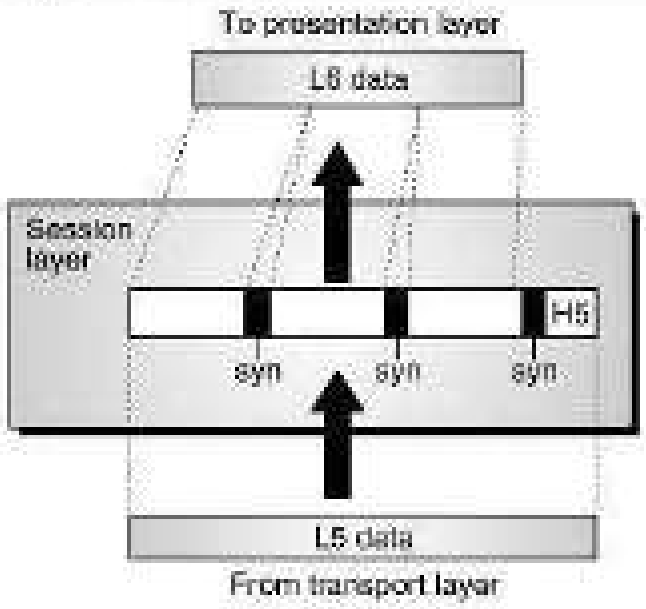
MSBTE Questions

Q. 1 Describe : Dialog control. (W-05, 2 Marks)

- The main functions of this layer are to establishes, maintains and synchronizes the communication between interested systems.
- Fig. 10.15.1 shows the relationship of the session layer to the transport layer and the presentation layer.



(G-68) **Fig. 10.15.1 : Session layer (Contd...)**



(G-68) **Fig. 10.15.1 : Session layer**

Functions :

- The session layer performs the following functions :
- It allows two systems to start dialog. The communication between two processes will take place either in half duplex or full duplex mode.
- The other function of this layer is synchronization.
- The session layer is not inherently concerned with security and the network logon process.
- The primary function of this layer is exchange of messages between two interested systems called as a **dialog.**
- A number of different services are provided by the session layer.
- These are grouped into subsets such as the Kernel Function Unit, the Basic Activity Subset and the Basic Synchronization Subset.
- However the two most important services provided by the session layer are :
  1. Dialog control.
  2. Dialog separation.

1. Dialog control :

- Dialog control is the means by which a sending and receiving systems initiate a dialog, exchange messages and finally end the dialog.

2. Dialog separation :

- It is a process of inserting a reference marker called as a checkpoint into the data stream travelling between the sending and receiving systems.
- This allows the checking of status of both the machines at the same point in time.
- This will also avoid any possible confusion and collision situation.

Features of Session layer :

1. Session layer is fifth layer of OSI model.
2. Protocol data unit generated by session layer is **data.**
3. The session layer is not inherently concerned with security and the network logon process.
4. The primary function of this layer is exchange of messages between two interested systems called as a **dialog.**
5. Gateways are associated with the session layer.
6. It provides services to the presentation layer.

10.16 Presentation Layer :

W-08, S-10, S-14, W-15, S-16, S-17

MSBTE Questions

Q. 1 Explain the following terms with respect to presentation layer :
1. Data encryption.
2. Data compression. **(W-08, 4 Marks)**

Q. 2 Explain role of presentation layer **(S-10, 4 Marks)**

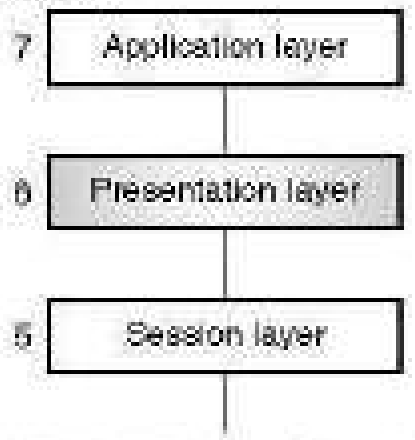
Q. 3 Describe the importance / role of presentation layer in OSI model. **(S-14, 4 Marks)**

Q. 4 Explain the following terms with respect to presentation layer :
1. Data encryption 2. Data compression **(W-15, 4 Marks)**

Q. 5 Describe presentation layer of OSI model. **(S-16, 4 Marks)**

Q. 6 Explain the functions of presentation layer and network layer. **(S-17, 4 Marks)**

- The presentation layer is the 6th layer the OSI model as shown in Fig. 10.16.1.
- Above it there is the application layer and below it there is the sessions layer.



(G-707) **Fig. 10.16.1 : Position of presentation layer**

- The presentation layer is related to the **syntax** and **semantics** of the information being exchanged between the interested systems.
- Some of the important responsibilities of the presentation layer are :
  1. Translation.
  2. Encryption.
  3. Compression.

1. Translation :

- The communication systems usually exchange the information in the form of strings of characters, numbers etc.
- This information needs to be changed into bit streams before transmission.
- This is essential because different systems use different encoding techniques. The presentation layer does the job of translation.
- The presentation layer at the sending end converts the information into a common format and the presentation layer at the receiving end will convert this common format into the one which is compatible to the receiver.

2. Encryption :

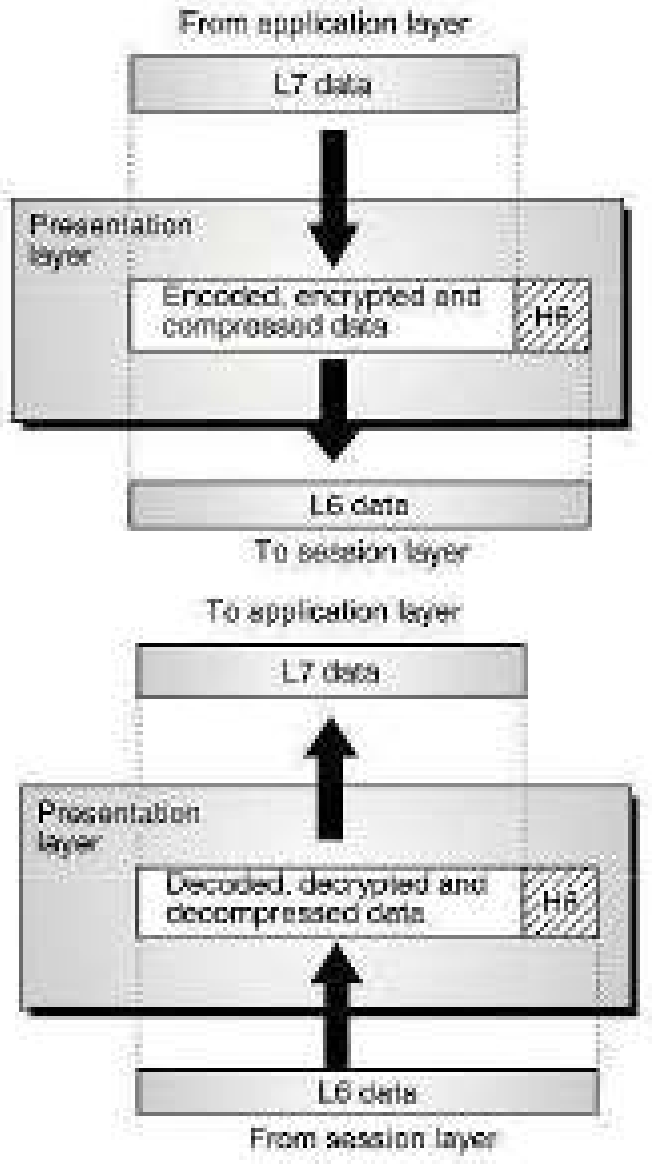
- For ensuring the security and privacy of the information that is being communicated, a process called data encryption is essential.
- Encryption is carried out at the sending end. In the encryption process, the sender transforms the original information to another form, and sends the transformed information.
- At the receiving end, an exactly opposite process called Decryption is carried out in which the received information is transformed back to its original form.
- Encryption and Decryption are carried out by the presentation layer.

3. Compression :

- The data compression technique is used for reducing the number of bits required to send an information.
- Data compression is essential for transmission of multimedia such as text, audio and video.

Relation with application and session layers :

- The relation of presentation layer with the application layer and session layer is illustrated in Fig. 10.16.2.
- The data from the application layer (L7 data) is encrypted, encoded and compressed at the presentation layer. A presentation layer header H-6 is also added as shown in Fig. 10.16.2.



(G-09) **Fig. 10.16.2 : Relation of presentation layer with the application layer and session layer**

- This is then sent to the session layer as L-6 data. These processes take place at the sending end of the system.
- While receiving the data from session layer, the operations carried out by the presentation layer are exactly opposite to those carried out while transmitting.
- The received data from the session layer undergoes decryption, decompression and decoding at the presentation layer.
- The header H-6 is detached from the data and then the L-7 data is sent to the application layer.

Functions of presentation layer :

- The presentation layer performs the following function :

1. It translates data between the formats the network requires and the format the computer expects (e.g. ASCII or EBCDIC).
2. It does the protocol conversion.
3. For security and privacy purpose it carries out encryption at the transmitter and decryption at the receiver.
4. It carries out data compression to reduce the banchwidth of the data to be transmitted.

– Unlike the session layer, which provides many different functions, the presentation layer has only one function.

– It basically functions as a pass through device. It receives primitives from the application layer and issues duplicate primitives to the session layer below it, using the Presentation Service Access Point (PSAP) and Session Service Access Point (SSAP).

Features of presentation layer :

1. Presentation layer is sixth layer of OSI model.
2. Protocol data unit generated by Presentation layer is **data.**
3. It translates data between the formats the network requires and the format the computer expects (e.g. ASCII or EBCDIC).
4. It does the protocol conversion.
5. Gateways are associated with the Presentation layer.
6. It provides services to the application layer.

10.17 Application Layer : W-03

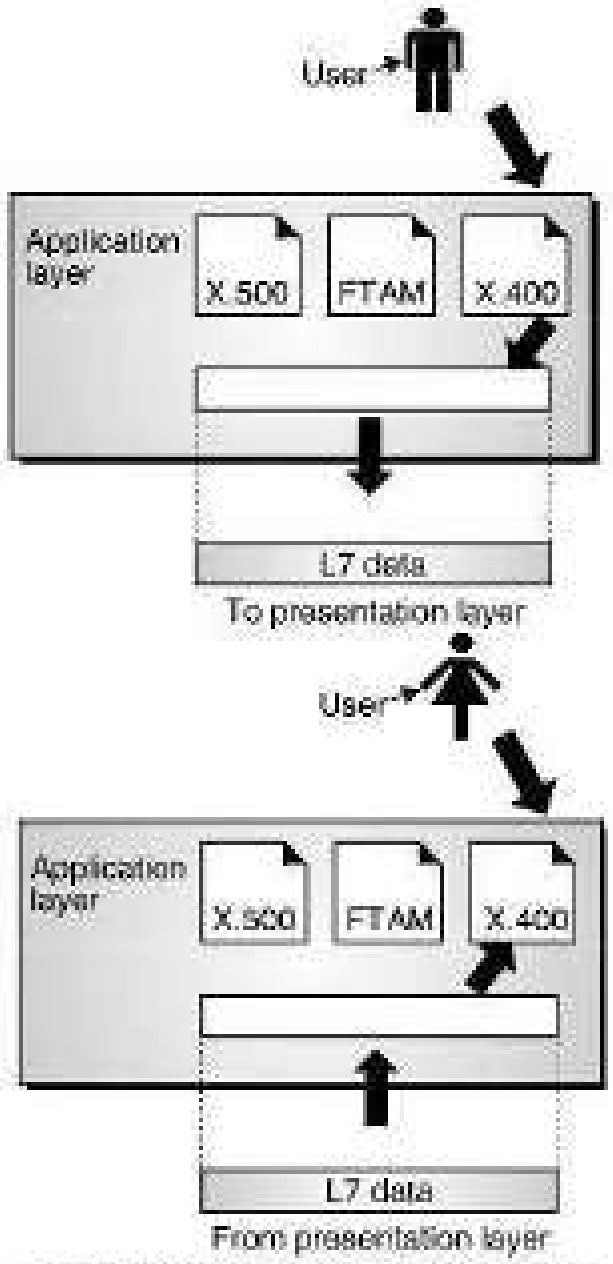
MSBTE Questions

Q. 1 With the help of suitable diagram indicating the adjacent layers, describe the functioning of Application Layer in OSI reference model. **(W-03, 4 Marks)**

– It is the topmost layer of OSI model. It provides services that directly support user application such as database access, e-mail and file transfer.

– It allows applications to communicate on the computer with applications on other computers as though they were on the same computer.

– The relationship of the application layer to the user and the presentation layer is shown in Fig. 10.17.1.



(G-70) **Fig. 10.17.1 : Application layer**

The application layer performs the following functions :

1. The application layer allows the creation of a virtual terminal which is the software version of a physical terminal. The user can log on to the remote host due to this arrangement.
2. The application layer provides File Transfer Access and Management (FTAM) which allows a user to access, retrieve manage or control files in a remote computer.
3. It creates a basis for forwarding and storage of e-mails.

Features of application layer :

1. It is the topmost layer of OSI model.
2. Protocol data unit generated by application layer is **data.**
3. It provides services that directly support user application such as database access, e-mail and file transfer.
4. Gateways are associated with the application layer.
5. It allows applications to communicate on the computer with applications on other computers as though they were on the same computer.
6. It creates a basis for forwarding and storage of e-mails.

10.17.1 Protocols Associated with the Application Layer : W-08, S-10, S-15

MSBTE Questions

Q. 1 Give the protocols associated with application layer of OSI reference model. **(W-08, 4 Marks)**

Q. 2 State any four protocols associated with application layer of OSI model. **(S-10, 4 Marks)**

Q. 3 What is token passing ? List any four protocols associated with application layer of OSI model. **(S-15, 4 Marks)**

- Some of the protocols which are associated with the application layer are :
  1. FTP : File Transfer Protocol
  2. DNS : Domain Name System
  3. DHCP : Dynamic Host Configuration Protocol
  4. BGP : Border Gateway Protocol
  5. RIP : Routing Information Protocol
  6. NFS : Network File System
- There are many application types which access network resources in different ways and for different reasons. The tools useful for the access also are located in the application layer.
- Some applications use protocols like SMTP (Simple Mail Transport Protocol) and POP3 (Post Office Protocol-3) for e-mail or protocols like SNMP for network administration, HTTP for www applications etc.

10.17.2 OSI Layers and Associated Protocols : S-11, S-13, S-16, W-16, S-18 I-Scheme : S-22

MSBTE Question

Q. 1 List the two protocols each associated with application layer, session layer, transport layer, network layer of OSI model. **(S-11, 4 Marks)**

Q. 2 State the layers at which the following protocols works :

1. ARP 2. PPP
3. SMTP 4. ICMP **(S-13, 4 Marks)**

Q. 3 State name of protocol used at different layers of OSI model. **(S-16, 4 Marks)**

Q. 4 Name the protocols used in :

1. Data link layer 2. Network layer
3. Transport layer 4. Presentation layer **(W-16, 4 Marks)**

Q. 5 State name of protocol used at different layers of OSI model. **(S-18, 4 Marks)**

Layer No.	Layer name	Protocols
7	Application	FTP, TFTP, SNMP, SMTP, DNS, Telnet, RIP, DHCP
6	Presentation	–
5	Session	Net BIOS, Net BEUI, SAP
4	Transport	TCP, UDP, SPX
3	Network	ARP, RARP, IP, ICMP, OSPF, BGP
2	Data link	SNAP, SLIP, PPP
1	Physical	Ethernet adapter, Token ring adapter, FDDI adapter

10.17.3 Merits of OSI Reference Model :

1. It distinguishes very clearly between the services, interfaces and protocols.
2. The protocols in OSI model are better hidden. So they can be easily replaced by new protocols as the technology changes.
3. OSI model is truly a general model.
4. This model supports connection oriented as well as connectionless services.

10.17.4 Demerits of OSI Model :

1. Sessions and presentation layers are not of much use.
2. This model was devised before the protocols were invented. So in real life there is a problem of fitting protocol into a model.

Review Questions

Q. 1 What is layered architecture ?

Q. 2 Define protocol.

Q. 3 Define peer.

Q. 4 What is network architecture ?

Q. 5 Name the two reference models.

Q. 6 What is OSI model ? Draw it.

Q. 7 Explain the interlayer communication in OSI layer.

Q. 8 Clearly explain the concept of data encapsulation.

Q. 9 Define :

1. Services and interfaces
2. Entities
3. Service access points
4. PDU

Q. 10 What is the meaning of connection oriented and connectionless services ?

Q. 11 Write about data encapsulation in OSI model.

Q. 12 How does the actual data transfer take place between two machines.

Q. 13 Write a note on : Virtual communication between layers.

Q. 14 Discuss the important design issues for various layers.

Q. 15 Write a note on connection oriented and connectionless services.

Q. 16 What is relationship between services and protocols ?

Q. 17 Draw the OSI reference model and explain the functions of different layers.

Q. 18 Explain horizontal communication in OSI model.

Q. 19 Explain the vertical communication in OSI model.

Q. 20 Define the following :

1. Packet
2. Frames
3. Datagram
4. Fragments

Q. 21 State the physical layer design issues.

Q. 22 Explain physical layer signaling.

Q. 23 Which network devices are used in the physical layer.

Q. 24 Explain various functions of DLL.

Q. 25 Explain the following with replace to DLL :

1. Framing
2. Addressing
3. Access control

Q. 26 What is media access control ? What are its types ?

Q. 27 Briefly explain token passing and CSMA/CD.

Q. 28 Explain error detection in DLL.

Q. 29 Explain the duties of network layer.

Q. 30 What is routing ?

Q. 31 Write a note on fragmenting.

Q. 32 Explain the functions of transport layer.

Q. 33 What is segmentation and reassembly.

Q. 34 Explain flow control at transport layer.

Q. 35 What are the main duties of the session layer.

Q. 36 What is dialog control and dialog separation ?

Q. 37 Explain the role of presentation layer.

Q. 38 What are the functions of application layer.

10.18 MSBTE Questions and Answers :

Q. 1 Which layer of the OSI model packages raw data bit into data frames ? **(S-03, W-10, S-14, S-18, 2 Marks)**

Ans. :

– The data link layer of the OSI model packages raw data bits into data frames.

Q. 2 Which layer of the OSI model packages raw data bit into data frames ? **(W-03, 2 Marks)**

Ans. :

– It is the data link layer, which packages the raw bits into data formats.

Q. 3 State and explain in brief at which the following protocol works :

1. ICMP
2. ARP
3. PPP
4. SMTP

(W-10, 4 Marks)

Ans. :

1. Network layer protocol
2. Network layer protocol
3. Data link layer protocol
4. Application layer

Q. 4 What is layered architecture ? **(S-12, 2 Marks)**

Ans. :

– Most networks are organised as a series of layers or levels.

– To reduce the design complexity networks are organised as a series of layer or levels, one above the other, is known as layered architecture.

Q. 5 Name two reference models. **(S-12, 2 Marks)**

Ans. :

1. OSI 2. TCP/IP

Q. 6 State the reasons for having a layered architecture in OSI reference model. **(W-16, 4 Marks)**

Ans. :

- The process of establishing a link between two devices to communicate and share information is complicated.
- There are many functions which are to be taken into consideration to allow an effective communication to take place.
- To organize all these functions in an organized way the designers felt the need to develop network architecture.
- In the network architecture various tasks and functions are grouped into related and manageable sets called **LAYERS.**
- A network architecture can be defined as a set of protocols that tell how every layer is to function.
- The reasons and advantages of using the network architecture are as follows :

1. It simplifies the design process as the functions of each layers and their interactions are well defined.
2. The layered architecture provides flexibility to modify and develop network services.
3. The number of layers, names of the layers, and the tasks assigned to them may change from network to network. But for all the networks, always the lower layer offers some services to its upper layer.
4. The concept of layered architecture in a new way of looking at the networks.
5. Addition of new services and management of network infrastructure becomes easy.
6. Due to segmentation (layered structure), it is possible to break difficult problems into smaller and more manageable tasks.
7. Logical segmentation allows parallel working by different teams on different tasks simultaneously.

Q. 7 Explain OSI model with neat diagram. Which layer of OSI model packages raw data bit into data frames ? Describe bit stuffing with one example. **(S-19, 8 Marks)**

Ans. :

Refer section 10.3.1 for OSI model and refer Q. 1.

10.19 I-Scheme Questions and Answers :

Summer 2019 [Total Marks - 16]

Q. 1 State functions of network layer. **(Section 10.10)** **(2 Marks)**

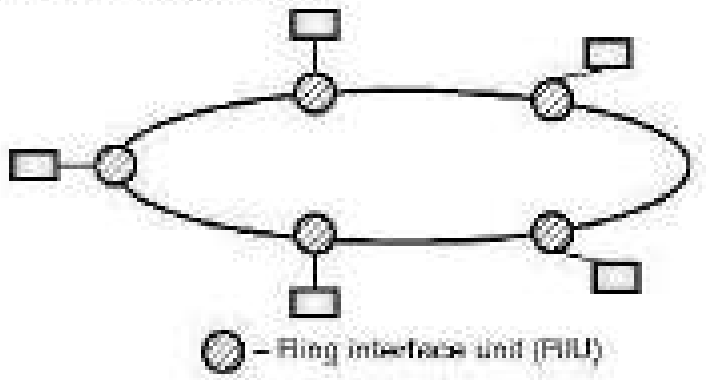
Q. 2 Draw and explain layered architecture of OSI model. **(Section 10.3.1)** **(4 Marks)**

Q. 3 Describe functions of physical layer and data link layer of OSI model. **(Section 10.10)** **(4 Marks)**

Q. 4 What is the MAC protocol used in token ring LAN's ? What happens if the token is lost ? **(6 Marks)**

Ans. :

- A token ring system is as shown in Fig. 1. It consists of a number of stations connected to the ring through a Ring Interface Unit (RIU).
- The RIU is basically a repeater, therefore it regenerates the received data frames and sends them to the next station after some delay.



(G-329) **Fig. 1**

Media access control (MAC) :

- In token bus system, the access to the medium (i.e. who will transmit) is controlled by the **special control frame called token.** It is a three byte frame.
- The token is passed from one station to the other round the ring.
- The sequence of token passing is dependent on the physical location of the stations connected to the ring. It is not dependent on logical number as in case of token bus system.
- A station which is in possession of the token only can transmit his frames. It may transmit one or more data frames but before the expiry of Token Holding Time (THT). Thus every station gets a fixed time to transmit its data.

- Typically this time is of 10 msec. After the THT, the token frame must be handed over to some other station.

Error conditions :

- There are two error conditions that may cause the token ring to break down. One of them is the case of lost token.
- If the token is lost, then there is no token on the ring.
- In order to overcome this problem, the IEEE 802 standard has specified that one station must be designed as active monitor.
- The monitor detects the lost token condition using a timer and time out mechanism and inserts a free token on the ring.

Winter 2019 [Total Marks - 08]

Q. 5 State the functions of any two layers of OSI model. **(Section 10.10)** **(4 Marks)**

Q. 6 Draw and explain OSI reference model. **(Sections 10.3 and 10.3.1)** **(4 Marks)**

Summer 2022 [Total Marks - 10]

Q. 7 List the protocols related to all layers of OSI reference model. **(Section 10.17.2)** **(4 Marks)**

Q. 8 Explain the working of OSI model layers. **(Sections 10.3, 10.3.1 and 10.3.2)** **(6 Marks)**

❑❑❑

Chapter 11

TCP / IP Model

Syllabus

Layered architecture, Data link layer : Nodes and links, Services, Two categories of links, Two sublayers, Link layer addressing, Three types of addresses, Address resolution protocol (ARP), Network layer : Addresses : Address space, Classful and classless addressing, Dynamic host configuration protocol (DHCP), Network address resolution (NAT), Transport layer protocol : Transport layer services, Connectionless and connection oriented protocol.

Chapter Contents

11.1 Network Models :

- In this chapter the idea of network model has been discussed first and then the TCP/IP protocol model has been discussed in detail.
- In order to define the computer network operations, two models have been derived. They are as follows :
  1. TCP/IP protocol model.
  2. OSI model.
- The International Standards Organisation (ISO) covers all aspects of network communication in the Open Systems Interconnection (OSI) model.
- An OSI model is a layered framework for the design of network systems that allows for communication across all types of computer systems.
- The purpose of each layer is to offer certain services to the higher layers.
- Layer n on one machine (source) will communicate with layer n on another machine (destination).
- The rules and conventions used in this communication are collectively known as the layer n protocol.
- Basically a protocol is an agreement between the two communicating machines about how the communication link should be established, maintained and released.

11.2 Protocol Layering :

Protocol :

- A protocol in data communication and networking is designed to define certain rules which are to be followed by both sender and the receiver and all the intermediate devices, so as to make the communication effective.

Protocol layering :

- For a simple type of communication, we need to use only one simple protocol.
- However for a complex type of communication, we need to divide the tasks among various layers.
- At each layer we need to use a protocol to carry out a specific task. This is known as **protocol layering.**

11.2.1 Scenarios :

Need of protocol layering :

- In order to understand the need of protocol layering, let us develop two simple scenarios as follows :

1. **First scenario :**

- In the first scenario, the communication between the source and destination is very very simple.
- Therefore only **one layer** will be sufficient to carry it out successfully.
- Assume that A and B are neighbours staying next to each other in the same building.
- They speak the same language and can talk face to face very easily and frequently.
- Therefore the communication between A and B can take place in one layer as shown in Fig. 11.2.1(a).

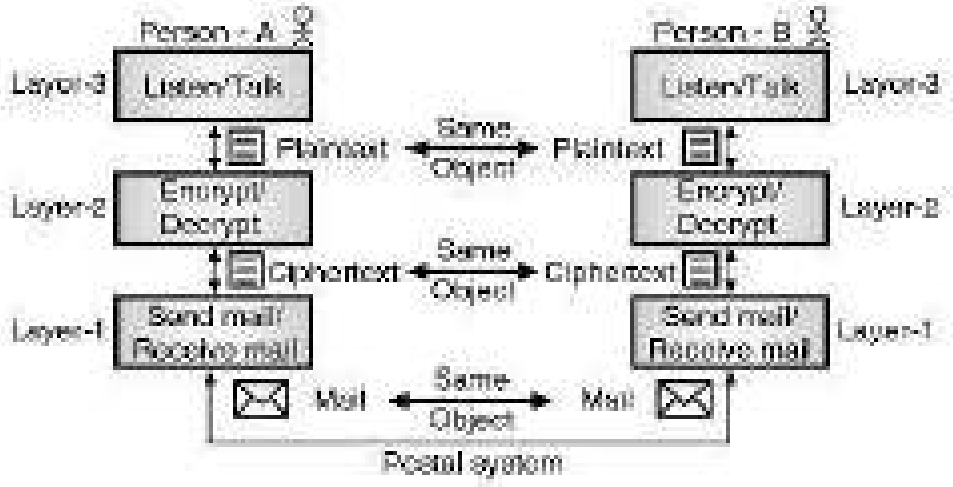
(S-2052) Fig. 11.2.1(a) : A single layer protocol

- Even in the simple single layer scenario, a set of rules must be followed.
- The set of rules which should be followed by both A and B are as follows :
  1. Both A and B should greet each other.
  2. They must choose proper words for communication.
  3. If A is speaking, B should remain silent and listen to A and vice versa.
  4. Both know that the communication should be bidirectional (dialog) and not unidirectional (monolog).
  5. They should say goodbye while leaving.

2. **Second scenario :**

- Now let us discuss the second scenario, in which person A has been offered a high-level position in his company and therefore he needs to relocate himself to company's another branch which is located in a city which is far away from person B.

- But A and B being very good friends wish to continue their communication about an innovative project to start a new business after their retirement.
- They choose the conventional mail through post office as their way of communication.
- But they do not want to reveal their ideas to anyone in case their mails are intercepted.
- Therefore both of them agree upon using the technique of **encryption and decryption.**
- Thus the sender encrypts the letter so that any intruder won't be able to read and understand the contents of the letter.
- Only the receiver knows how to decrypt it. So he will decrypt the received letter and understand its contents.
- From this discussion we conclude that the communication between A and B takes place in three layers as shown in Fig. 11.2.1(b).



(G-2063) **Fig. 11.2.1(b) : A three layer protocol**

- Let us assume that both persons A and B have three different machines or robots to perform the tasks specified at each layer.
- Refer Fig. 11.2.1(b) and imagine that person A sends the first letter to B. For this A talks to the robot at layer-3 as if it is person B.
- The layer-3 robot (or machine) listens to what A says and converts it into the **plaintext** i.e. a letter written in English.
- This letter is then sent to the robot or machine present at layer-2.
- This **plaintext** is encrypted by the machine at layer-2 to create the **ciphertext** which is sent to the machine present at layer-1.
- The robot/machine present at layer-1 will take the ciphertext, puts it in an envelope, write the addresses of sender and receiver over it and mails the envelope.
- At **person B's place,** the letter from the mailbox is picked up by the robot/machine at layer-1, the letter in the **ciphertext** is taken out of the envelope and gives it to the machine/robot at layer-2.
- The machine at layer-2, decrypts the ciphertext to obtain the **plaintext** and hands it over to the machine at layer-3.
- Finally the machine/robot present at layer-3 reads the plaintext as if person A is talking to person B.

Advantages of protocol layering :

1. It allows us to divide a complex task into many simpler tasks.
2. It allows us to separate the services from the implementation.
3. In practice, the communication does not always take place directly between the two end systems (A and B) but there are intermediate systems which need only some layers. Without the protocol layering the intermediate systems will be as complex as the two and system, thus making the entire system very complex and expensive.
4. It simplifies the design process as the function of each layer is well defined.
5. It provides flexibility to modify and develop network services.
6. Addition of new services and management of network infrastructure becomes easy.

Disadvantages of protocol layering :

1. We lose the touch with reality.
2. Sometimes the protocol layering can result in poor performance of protocol.

11.2.2 Principles of Protocol Layering :

I-Scheme : S-22

- There are two different principles of protocol layering. We will discuss them one by one.

1. First principle :

- According to the first principle, in order to have a successful bidirectional communication, each layer should be able to perform two opposite tasks one in each direction.

– For example layer-1 performs send and receive mail functions or layer-2 performs the encryption and decryption and so on.

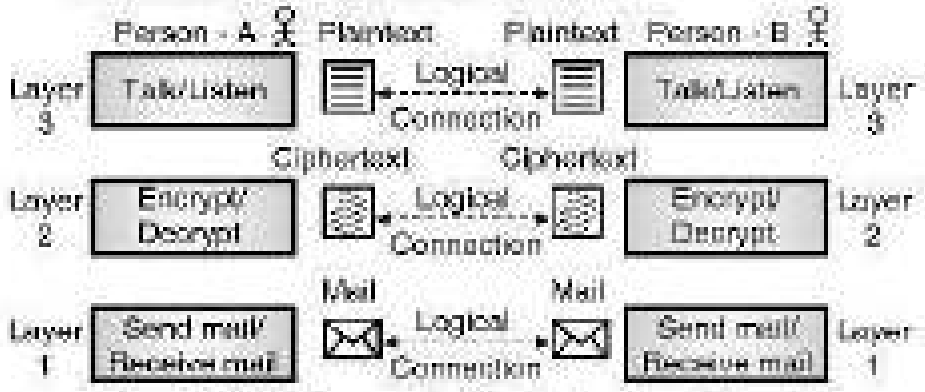
2. **Second principle :**

– According to the second principle, in protocol layering the two objects under each layer at both the ends should be the same.

– For example in Fig. 11.2.1(b), the object under the second layer at A as well as B is cipher text.

11.2.3 Logical Connections :

– We can think of the logical connection between each layer as shown in Fig. 11.2.2. This is after following the two principles of protocol layering.



(G-2064) **Fig. 11.2.2 : Concept of logical connections between the peer layers**

– Fig. 11.2.2 shows that there is a logical (imaginary) connection from a layer at A to the corresponding layer at B.

– The logical connection between each layer implies that there is a layer to layer communication.

– Due to logical connections, persons A and B can think that it is possible to send the object created from layer to the corresponding layer at the other end.

11.3 TCP/IP Protocol Model :

W-06, W-11, I-Scheme : W-19

BTE Questions

Q. 1 What is TCP/IP ? Explain its protocols. **(W-06, 4 Marks)**

Q. 2 Explain TCP / IP reference model with neat diagram. **(W-11, 8 Marks)**

– After discussing about the concept of protocol layering and about the logical communication taking place between layers, now it is time to introduce the **TCP/IP protocol model.**

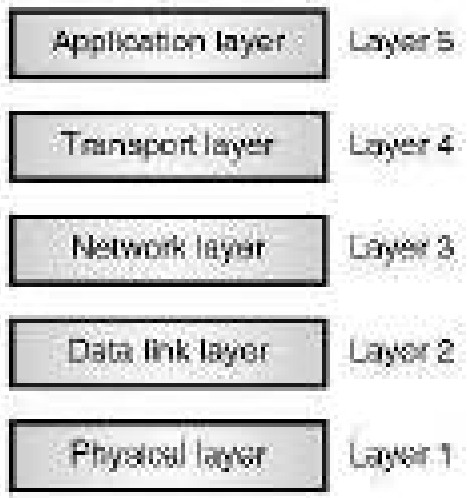
– TCP/IP is the short form of two important protocols namely Transmission Control Protocol/Internet Protocol.

– A **protocol model** is defined as the set of protocols organized in different layers. The TCP/IP protocol model is used in Internet today.

– TCP/IP is a hierarchical protocol model means that each upper layer protocol receives support and services from either one or more lower level protocols.

– In the original TCP/IP protocol model, there were four software layers built upon the hardware.

– But today's TCP/IP protocol model uses a five layer model as shown in Fig. 11.3.1.



(G-2065) **Fig. 11.3.1 : Layers in TCP/IP protocol model**

11.3.1 Layered Architecture :

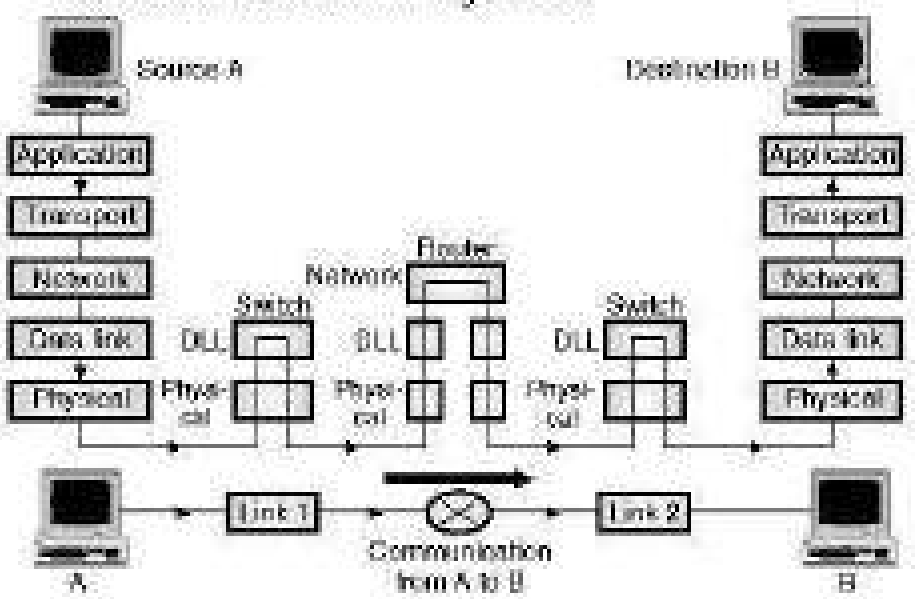
W-06, W-11, I-Scheme : W-19

MSBTE Questions

Q. 1 What is TCP/IP ? Explain its protocols. **(W-06, 4 Marks)**

Q. 2 Explain TCP / IP reference model with neat diagram. **(W-11, 8 Marks)**

– In order to understand how the communication takes place between various layers of TCP/IP protocol model, we have considered a small internetwork consisting of three LANs (links) with all LANs connected to each other via a router as shown in Fig. 11.3.2.



(G-2176) **Fig. 11.3.2 : Communication through an Internet**

– In Fig. 11.3.2, there are two computers A and B communicating with each other and three more devices namely : the link layer switch in link-1, the router and the link layer switch in link-2.

– Computer A is called as the **source host** and computer B is called as the **destination host.**

- Each device in the Internet has a specific role to play, depending on which each device uses a set of layers as shown in Fig. 11.3.2.
- All the five layers are involved in communication for the source and destination hosts A and B respectively.
- At the source host, a message is created at the application layer and then it is sent in down the layers in order to physically send it to the destination host.
- At the destination host this message is received at the physical layer and then it is delivered to the application layer via the other layers between the physical and application layers.
- At the router, as shown in Fig. 11.3.2 only three layers of TCP/IP protocol model are needed to be involved.
- Thus a router does not need the transport or application layers when it is being used only for routing.
- The router is connected to multiple links. At each link we use a switch which involves only two layers of the TCP/IP protocol model as shown in Fig. 11.3.2.
- However note that the link layer and physical layer protocols used by each link can be completely different.
- Thus the router may have to receive a packet from link-1 based on one pair of protocol and may have to deliver a packet to link-2 based on a totally different pair of protocols.
- Now consider a switch in Fig. 11.3.2 which shows that it has two different connections.
- But both of them belong to the same link. Therefore two different protocol pairs will not be involved.
- A switch has to deal with only one pair of DLL and physical layer protocols.

11.3.2 Layers in the TCP/IP Protocol Model :

S-11, S-14, S-16, S-17, I-Scheme : W-19

MSBTE Questions

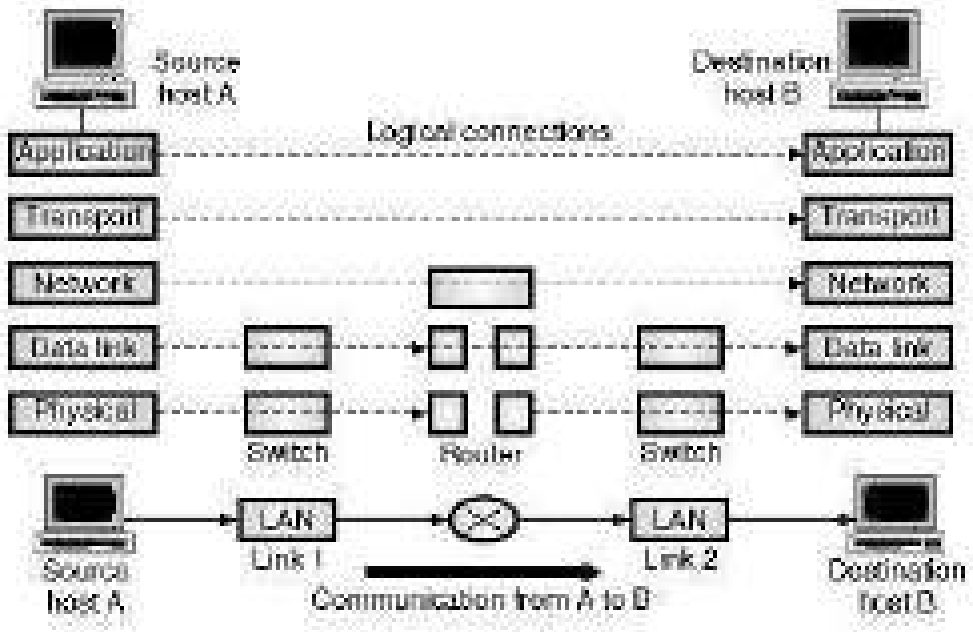
Q. 1 Describe TCP/IP model with suitable diagram. **(S-11, 4 Marks)**

Q. 2 Describe TCP/IP with neat sketch. Compare TCP/IP and OSI reference model. **(S-14, 4 Marks)**

Q. 3 Draw and explain layered structure of TCP/IP model. **(S-16, 4 Marks)**

Q. 4 Describe TCP/IP model with suitable diagram. **(S-17, 8 Marks)**

- Now we are going to discuss the functions and duties of various layers in the TCP/IP protocol model.
- In this section, we will think about the logical connections between various layers, so as to clearly understand the duties of each layer.
- The logical connections in a simple internetwork have been shown in Fig. 11.3.3.



(G-2177) **Fig. 11.3.3 : Logical connections between the layers of TCP/IP model**

- Each layer has some specific duties and we can use the logical connections to think about them easily.
- From Fig. 11.3.3 it is clear that the network, transport and application layers have an **end-to-end** duty. But the data link and physical layers have the **hop to hop** duty. (Hop is a host or router).
- In this way the upper three layers have a **domain of duty** of the entire Internet while the lower two have a domain of duty of only link.

Data unit created by every layer :

- We can think about the logical connections in a different way i.e. in terms of the **data unit** created by each layer.
- The names of data units (packets) created by different layers are as follows :

Layer	Data unit	Layer	Data unit
Application	Message	Datalink	Frame
Transport	Segment	Physical	Bits
Network	Datagram		

- The data unit (packet) created by the top three layers, should not be changed by a router or a link layer switch.
- However the data unit created at the lower two levels can be changed only by the router. The link layer switches cannot modify it.
- The second principle that we discussed for the protocol layering has been shown in Fig. 11.3.4.

(d-2178) **Fig. 11.3.4 : Identical objects in the TCP/IP model**

- Note that the objects shown below each layer related to each device are identical.

11.4 Overview of TCP/IP Architecture :

S-11, S-14, S-16, S-17

MSBTE Questions

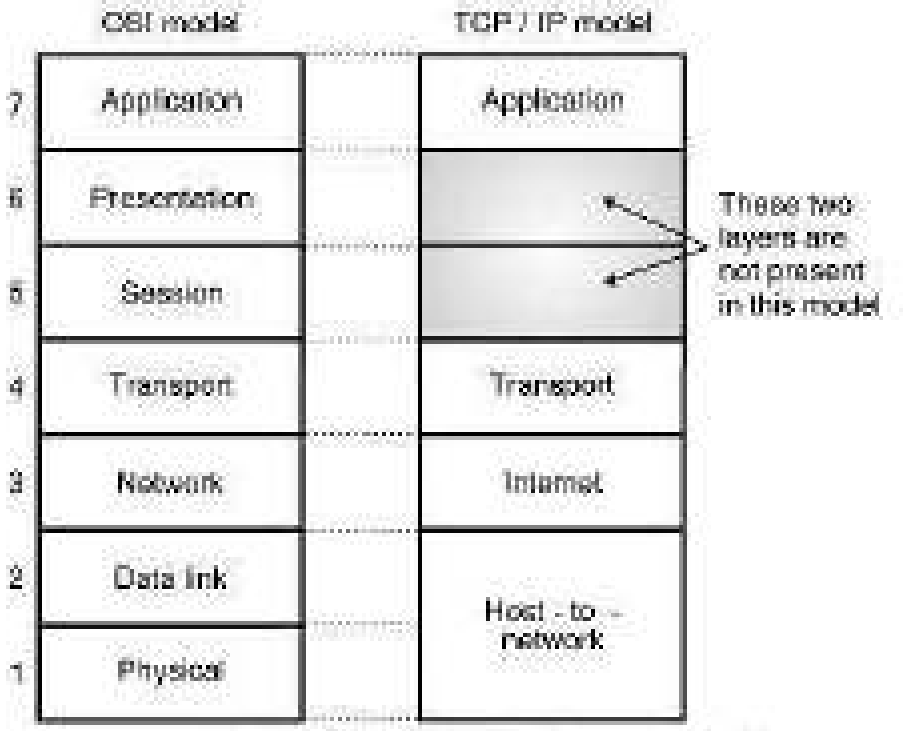
Q. 1 Describe TCP/IP model with suitable diagram. **(S-11, 4 Marks)**

Q. 2 Describe TCP/IP with neat sketch. Compare TCP/IP and OSI reference model. **(S-14, 4 Marks)**

Q. 3 Draw and explain layered structure of TCP/IP model. **(S-16, 4 Marks)**

Q. 4 Describe TCP/IP model with suitable diagram. **(S-17, 8 Marks)**

- Transmission Control Protocol and the Internet Protocol (TCP/IP) was developed by the Department of Defence's Projects Research Agency (ARPA, later DARPA) under its project on network interconnection.
- It is a set of protocols that allow communication across multiple diverse network.
- ARPA originally created TCP/IP to connect military networks together, but later on this protocol was also given to government agencies and universities free of cost.
- Since the TCP/IP was developed for military use, it became robust to failures and flexible to different types of networks.
- TCP/IP is the most widely used protocol for interconnecting computers and it is the protocol of the Internet.
- TCP/IP became the standard for interoperating Unix Computers, especially in military and university environments.
- With the development of the Hypertext Transfer Protocol (HTTP) for sharing Hypertext Markup Language (HTML) documents freely on the internet, the World Wide Web (WWW) was born and soon TCP/IP came into much use.
- Fig. 11.4.1 shows the TCP/IP reference model along with the OSI model used for comparison.



(d-71) **Fig. 11.4.1 : TCP/IP reference model**

11.4.1 Description of TCP/IP Model :

S-04, W-04, W-10, S-11, S-12, W-14, S-15

MSBTE Questions

Q. 1 Describe the functioning of application layer in TCP/IP reference model. **(S-04, W-04, 2 Marks, S-12, 4 Marks)**

Q. 2 Which of the following TCP/IP transport layer is faster. Justify your answer.
1. ICMP 2. TCP
3. IP 4. UDP **(W-10, S-11, 4 Marks)**

Q. 3 Describe the function of transport layer. **(S-11, 4 Marks)**

Q. 4 Give the name of protocols used by different layers of TCP/IP. Discuss the function of ARP and RARP. **(W-14, 4 Marks)**

Q. 5 Describe TCP / IP model with suitable diagram. Describe the function of each layer. **(S-15, 4 Marks)**

- As shown in Fig. 11.4.1, the TCP/IP model has only four layers.

Internet layer :

- This layer is called as the internet layer and it holds the whole architecture together.
- The task of this layer is to allow the host to insert packets into any network and then make them travel independently to the destination.
- The order in which the packets are received can be different from the sequence in which they were sent.
- Then the higher layers are supposed to arrange them in the proper order.
- Note that "internet" is being used as a generic term.
- The internet layer defines (specifies) a packet format and a protocol called Internet Protocol (IP).
- The internet layer is supposed to deliver IP packets to their destinations.
- So routing of packets and congestion control are important issues related to this layer.
- Hence TCP/IP internet layer is very similar to the network layer in OSI model as shown in Fig. 11.4.1.

Transport layer :

- This is the layer above the internet layer. Its functions are same as those of a transport layer in OSI model.
- This layer allows the peer entities of the source and destination machines to converse with each other.
- The end to end protocols used here are TCP and UDP (User Datagram Protocol).
- TCP is a reliable connection oriented protocol. It allows a byte stream transmitted from one machine to be delivered to the other machine without introducing any errors.
- TCP also handles the flow control.
- UDP (User Datagram Protocol) is the second protocol used in the transport layer.
- It is an unreliable, connectionless protocol and used for the applications which do not want the TCP's sequencing or flow control.
- UDP is also preferred over TCP in those applications in which prompt delivery is more important than accurate delivery. It is used in transmitting speech or video.

Application layer :

- TCP/IP model does not have session or presentation layers, because they are of little importance in most applications.
- The layer on top of transport layer is called as application layer.
- The protocols related to this layer are all high level protocols such as virtual terminal (TELNET), file transfer (FTP) and electronic mail (SMTP) as shown in Fig. 11.4.2.

Application layer	TELNET, FTP, SMTP, DNS, HTTP, NNTP
Transport	TCP UDP
Internet (Network)	IP
Host-to-network	ARPANET, SATNET LAN, Packet radio

Fig. 11.4.2

- Many other protocols have been added to these, over the years such as Domain Name Service (DNS), NNTP and HTTP etc.

Host-to-network layer :

- This is the lowest layer in TCP/IP reference model.
- The host has to connect to the network using some protocol, so that it can send the IP packets over it.
- This protocol varies from host to host and network to network.
- Out of all these, UDP is very fast because of the following reasons :

1. UDP is a connectionless protocol. So it does not have to establish a connection or terminate it.
2. It does not provide any flow control.
3. It does not provide any error control. Therefore less time is wasted in retransmission.
4. It does not provide any congestion control.

11.5 Detailed Description of Each Layer :

– In this section we are going to discuss the duties of various layers in TCP/IP.

11.5.1 Detailed Introduction to Physical Layer : S-15

MSBTE Questions

Q. 1 Describe TCP / IP model with suitable diagram. Describe the function of each layer. **(S-15, 4 Marks)**

– Physical layer is the lowest layer in the TCP/IP protocol model. The communication at the physical layer level is still **logical** because of the presence of a hidden layer (transmission media) under the physical layer.

– The **primary responsibility** of the physical layer is to carry the individual bits present in a frame across the link.

– The transmission media (wired or wireless) is used for connecting two devices to each other. Here it is important to understand that the transmission media does not actually carry the bits.

– Instead it carries the electrical or optical signals which represents the bits which are to be carried from one device to the other.

– That means the bits received in a frame from the data link layer are transformed into an electrical or optical signal and sent over the transmission media.

– Still we consider **bit** as the data unit for communication between physical layers of two communicating devices.

– For the transformation of bits to signal, several physical layer protocols are available.

Following are the functions of the physical layer :

1. To define the type of encoding i.e. how 0's and 1's are changed to signals.
2. To define the transmission rate i.e. the number of bits transmitted per second.
3. To deal with the synchronization of the transmitter and receiver.
4. To deal with network connection types, including multipoint and point-to-point connections.
5. To deal with physical topologies i.e. bus, star, ring, or mesh.
6. To deal with the media bandwidth i.e. baseband and broadband transmission.
7. Multiplexing which deals with combining several data channels into one.
8. To define the characteristics between the device and the transmission medium.
9. To define the transmission mode between two devices i.e. whether it should be simplex, half duplex or full duplex.

Note : Passive hubs, simple active hubs, terminators, couplers, cable and cabling, connectors, repeaters, multiplexers, transmitters, receivers, transceivers are associated with the physical layer.

11.5.2 Detailed Introduction to Data Link Layer : W-14, S-15

MSBTE Questions

Q. 1 Give the name of protocols used by different layers of TCP/IP. Discuss the function of ARP. **(W-14, 4 Marks)**

Q. 2 Describe TCP / IP model with suitable diagram. Describe the function of each layer. **(S-15, 4 Marks)**

– An internetwork consists of many LANs and WANs, connected to each other by routers.

– While travelling from source to destination a datagram has to travel through many overlapping sets of links.

– It is the responsibility of router to choose the best possible link for a datagram to travel.

– When a router does so, it is the responsibility of the data link layer to take the datagram across the link.

– The said link can be anything such as a wired LAN, a wireless LAN, or a link layer switch etc.

– Every type of link will use different types of protocols. The data link layer should be able to handle all the different types of protocols and move the packet through the link.

– The data link layer receives a datagram from the network layer and encapsulates it into a packet called as **frame.**

– There are no specific data link layer protocols defined by the TCP/IP model. Instead it supports all the standard protocols that can carry the datagram successfully over the link.

- The services provided by each data link layer protocol are different.

Following are the functions of data link layer :

1. **Framing :**

- The bits received from the network layer are divided into another type of data units called frames at the data link layer.

2. **Flow control :**

- It provides a flow control mechanism to avoid a fast transmitter from over-running a slow receiver by buffering the extra bits.

3. **Physical addressing :**

- It adds a header to the frame which consists of the physical address of the sender and / or receiver of that frame.

4. **Error control :**

- A trailer is added at the end of the frame in order to achieve error control. It also uses a mechanism to prevent duplication of frames.

5. **Access control :**

- The data link layer protocol perform an important function of determining which device has control over the link at any given time, when two or more devices are connected to the same link.
- The Institution of Electrical and Electronics Engineers (IEEE) felt the need to define the data link layer in more details, so they split it into two sub-layers :
  1. Logical Link Control (LLC).
  2. Media Access Control (MAC).

11.5.3 Detailed Introduction to Network Layer : W-14, S-15, I-Scheme : S-19

MSBTE Questions

Q. 1 Give the name of protocols used by different layers of TCP/IP. Discuss the function of ARP. **(W-14, 4 Marks)**

Q. 2 Describe TCP / IP model with suitable diagram. Describe the function of each layer. **(S-15, 4 Marks)**

- The primary responsibility of the network layer is to create a connection between the source and destination computers. The communication at the network layer level is called as host to host communication.
- The several routers present between the source and destination hosts choose the best route for each travelling packet.
- Therefore the two responsibilities of the network layer are : host to host communication and routing of the packet through the possible routers.
- The main protocol in the network layer of the Internet is IP (Internet Protocol). The format of the packet (datagram) at network layer is decided by IP.
- The routing of datagrams from their source to destination is also the responsibility of IP.
- It achieves this by making each router forward the datagrams to the next router in its path towards the destination.
- IP is a **connectionless** protocol. It does not provide services like **flow control, error control** or even the **congestion control.**
- Therefore it is dependent on the transport layer in case if an application needs these services.
- The routing protocols included in the network layer are of unicast (one-to-one) and multicast (one-to-many) nature.
- These routing protocols have a responsibility of creating the forwarding tables for the routers to help them in the process of routing.
- There are some auxiliary protocols at the network layer, that are designed to assist IP in its delivery and routing tasks.
- The examples of such protocols are ICMP, IGMP, DHCP, ARP etc.
- The functioning of these protocols is as follows :

Sr. No.	Protocol	Function
1.	ICMP	To help IP report problems when routing a packet
2.	IGMP	Helps IP in multitasking
3.	DHCP	To help IP to get the network layer address for a host.
4.	ARP	Helps IP to find the link layer address of a host or router.

Functions of the network layer :

1. It translates logical network address into physical machine addresses i.e. the numbers used as destination IDs in the physical network cards.
2. It determines the quality of service by deciding the priority of message and the route a message will take if there are several ways a message can get to its destination.
3. It breaks the larger packets into smaller packets if the packet is larger than the largest data frame the data link will accept.
4. It is concerned with the circuit, message or packet switching.
5. It provides connection oriented services, including network layer flow control, network layer error control and packet sequence control.
6. Routers and gateways operate in the network layer.

11.5.4 Detailed Introduction to Transport Layer : S-11, W-14, S-15

MSBTE Questions

Q. 1 Describe TCP/IP model with suitable diagram. Describe the function of transport layer. **(S-11, 8 Marks)**

Q. 2 Give the name of protocols used by different layers of TCP/IP. Discuss the function of ARP. **(W-14, 4 Marks)**

Q. 3 Explain the services provided by transport layer in TCP/IP Model. **(W-14, 4 Marks)**

Q. 4 Describe TCP / IP model with suitable diagram. Describe the function of each layer. **(S-15, 4 Marks)**

- The primary responsibility of the transport layer is also to provide an end to end connection.
- At the source host, the application layer sends a message to the transport layer which **encapsulates** it into a transport layer packet (which is also called as a **segment** or **user datagram**) and sends it through the logical connection (which is imaginary) to the transport layer of the destination host.
- In short the transport layer takes message from the application layer of source host and via the transport layer at the destination host delivers the message to the application layer at the destination.
- For the Internet applications, there are number of transport layer protocols designed to give specific service to various application programs.
- The main protocol in the transport layer is TCP (Transmission Control Protocol) which is a connection oriented protocol.
- The main task of TCP is to establish a logical connection between the transport layers of the source and destination hosts before actually transferring the data.
- Being connection oriented, the TCP is a reliable protocol which provides the following services to an application layer program :
  1. Flow control 2. Error control and
  3. Congestion control
- The other commonly used transport layer protocol is UDP (User Datagram Protocol).
- This is a connectionless protocol. Therefore it does not need to create any logical connection before transmitting the user datagrams.
- The UDP treats each datagram as a totally in dependent packet with absolutely no relation with the previous or next datagrams.
- UDP is a very simple protocol as compared to TCP. It does not provide flow control, error control or congestion control.
- UDP is an attractive protocol for certain application program specially for those who want to send small messages or those who do not afford retransmission of a packet if the packet is corrupted or lost.
- For new emerging applications in the field of multimedia, a new transport layer protocol has been designed which is called as SCTP (Stream Control Transmission Protocol).

Functions of transport layer :

- The transport layer performs the following functions :

1. It divides each message into packets at the source and re-assembles then at the destination.
2. The transport layer header H4 includes a service point address to deliver a specific process from source to a specific process at the destination.
3. The transport layer is capable of either connectionless or connection-oriented transfer of data.

4. It performs end to end flow control. Flow control is an important function of the transport layer.
5. It makes sure that the entire message arrives at the receiving transport layer without error.

11.5.5 Detailed Introduction to Application Layer : S-04, W-04, S-12, W-14, S-15

MSBTE Questions

Q. 1 Describe the functioning of application layer in TCP/IP reference model. **(S-04, W-04, 2 Marks, S-12, 4 Marks)**

Q. 2 Give the name of protocols used by different layers of TCP/IP. Discuss the function of ARP. **(W-14, 4 Marks)**

Q. 3 Describe TCP / IP model with suitable diagram. Describe the function of each layer. **(S-15, 4 Marks)**

- The logical connection between the application layers of source and destination hosts is **end-to-end** type.
- The communication between the application layers of source and destination hosts takes place through all the layers.
- The application layer communication is between **two processes.** A process is nothing but a program running at the application layer.
- Thus the primary responsibility of the application layer is the **process to process communication.**
- There are many predefined protocols at the application layer in the Internet. Some of these protocols are HTTP, WWW, SMTP, FTP, TELNET, SNMP etc. These protocols and their functions are shown in Table 11.5.1.

Table 11.5.1

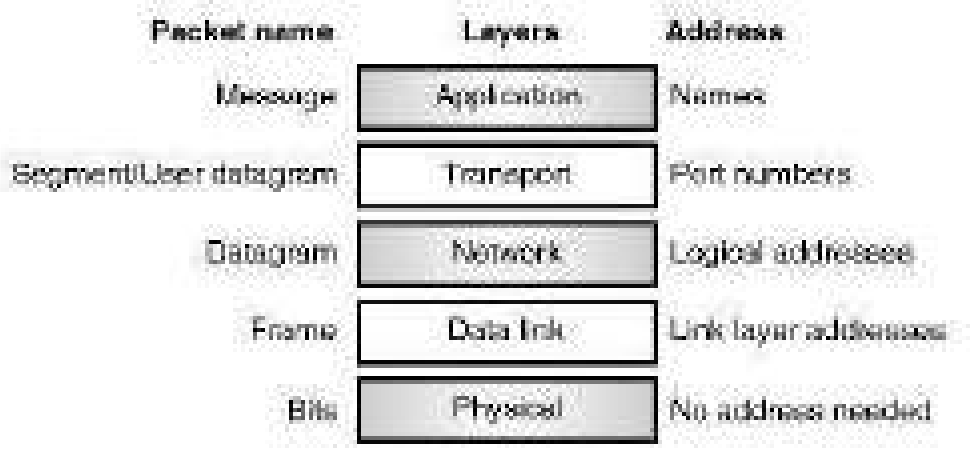
Sr. No.	Protocol	Function
1.	HTTP	As tool to access World Wide Web i.e. WWW.
2.	SMTP	It is the main protocol used in e-mail service.
3.	FTP	To transfer files from one host to the other.
4.	TELNET	To access a website remotely.
5.	SNMP	To manage the Internet.
6.	DNS	To find the network layer address of a computer.
7.	IGMP	To collect the membership in a group.

- The application layer performs the following functions :

1. The application layer allows the creation of a virtual terminal which is the software version of a physical terminal. The user can log on to the remote host due to this arrangement.
2. The application layer provides File Transfer Access and Management (FTAM) which allows a user to access, retrieve, manage or control files in a remote computer.
3. It creates a basis for forwarding and storage of e-mails.

11.6 Addressing :

- Addressing is another important concept related to the protocol layering in the Internet.
- There is a logical connection between the pair of layers as discussed earlier.
- For any communication to take place between a source and a destination, two addresses namely source address and destination address are needed.
- Thus we will need four pairs of such addresses corresponding to the data link, network, transport and application layers.
- There is no need of addresses at the physical layer because communication at the physical layer takes place in bits which cannot have an address.
- Fig. 11.6.1 shows the addressing at each layer.



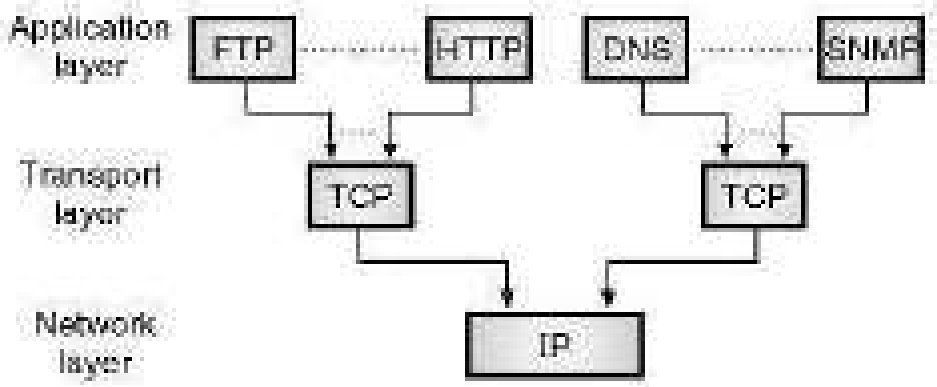
(S-2009) **Fig. 11.6.1 : Addressing in TCP/IP protocol model**

- Fig. 11.6.1 also shows the relationship between various layers, the addresses used in each layer and the name of the packet at each layer.
- We generally use the **names** to define the **site address** which provides the required services. For example **techmaxbook.com**, at the application layer.
- It is also possible to use the email address such as **jayantkatre@gmail.com.**

- The addresses at the transport layer are called as **port numbers.** These define the programs at the application layer of source and destination.
- There are several application layer programs running at a time. Port numbers are the local addresses which are used to distinguish between these programs.
- The addresses at the network layer are global in nature because the whole Internet is the scope of these addresses.
- The connection of a device to the Internet is uniquely defined by a network layer address.
- The addresses at the data link layer are called as the **MAC addresses.**
- These are the locally defined addresses. Each host or router in a network such as LAN or WAN always has a MAC address.

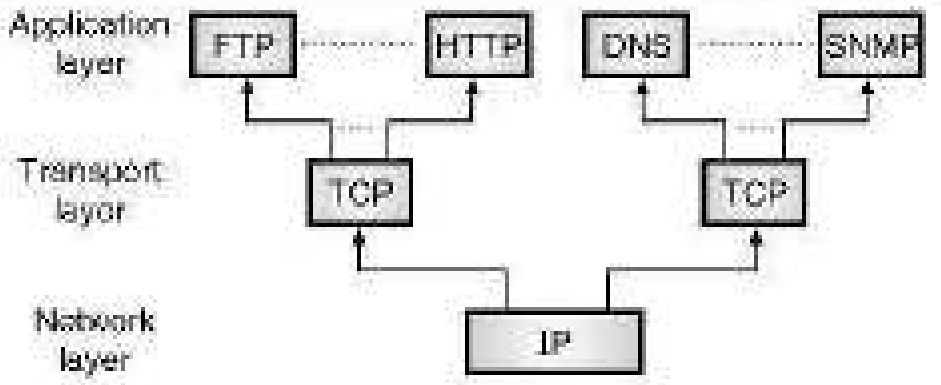
11.7 Multiplexing and Demultiplexing :

- In TCP/IP protocol, many protocols are being used at the same layer.
- Therefore multiplexing is needed at the source and demultiplexing is needed at the destination.
- In the process of **multiplexing** as shown in Fig. 11.7.1(a), a protocol at one layer in TCP/IP can encapsulate a packet (one at a time) from several protocols corresponding to the next higher layer in TCP/IP model.



(G-2070) **Fig. 11.7.1(a) : Multiplexing in TCP/IP**

- In the process of demultiplexing, a protocol will decapsulate and deliver a packet one at a time to several protocols belonging to the next higher layer in TCP/IP protocol model as shown in Fig. 11.7.1(b).



(G-2071) **Fig. 11.7.1(b) : Demultiplexing in TCP/IP**

- As shown in Fig. 11.7.1(a), at the transport layer two protocols TCP and UDP are capable of multiplexing the messages coming from various protocols at the application layer.
- Next the segments from TCP or user datagrams from UDP are accepted and multiplexed by IP at the network layer.
- IP can also multiplex the packets from some other protocols such as ICMP or IGMP etc.
- The frames at the data link layer level can carry the payload coming from the network layer protocols such as IP or ARP etc.

11.8 Connection Oriented and Connectionless Services :

- Any layer can offer two types of services to the layer above it.
  1. Connection oriented service.
  2. Connectionless service.

1. Connection oriented service :

- The connection oriented service is similar to the one provided in the telephone system.
- The service users of the connection oriented service undergo the following sequence of operation :
  1. Establish a connection.
  2. Use the connection.
  3. Release the connection.
- The connection acts like a tube. The sender pushes bits from one end of the tube and the receiver takes them out from the other end.
- The order is generally preserved. That means the order in which the bits are sent is same as the order in which they are received.
- Sometimes after establishing a connection, the sender and receiver can discuss and negotiate about parameters to be used such as maximum message size, quality of service and some other issues.

2. Connectionless service :

- The connectionless service is similar to the postal service.
- Each message (analogus to a letter) carries the full address of the destination. Each message is routed independently from source to destination through the system.
- It is possible that the order in which the messages are sent and the order in which they are received may be different.
- Applications such as electronic mail do not require any connections. The cost associated, complexity and overheads of reliable services is not required here.
- Such applications require high reliability of message arrival but no guarantee i.e. unreliable service will be acceptable for this application.
- The services in which acknowledgements are not sent to sender are unreliable connectionless services.
- Such services are called as **datagram** service which is similar to telegram service.
- However note that **acknowledged datagram service** can also be provided.
- One more type of service is the **request-reply service**. In this type, the sender transmits a single datagram which contains a request and the receiver send a reply to it.
- Table 11.8.1 lists various types of services and their examples.

Table 11.8.1 : Six different types of services

Sr. No.	Service	Type	Example
1.	Reliable message stream.	Connection oriented	Sequence of pages.
2.	Reliable byte stream.	Connection oriented	Remote login.
3.	Unreliable connection.	Connection oriented	Digitized voice.
4.	Unreliable datagram.	Connectionless	Electronic mail.
5.	Acknowledged datagram.	Connectionless	Registered e-mail.
6.	Request-Reply	Connectionless	Database query.

- The unreliable service is used only if the reliable service is not available or is too costly to afford.

11.8.1 Comparison of OSI and TCP/IP Models :

W-08, W-10, W-11, S-12, S-14, W-14, W-16

MSBTE Questions

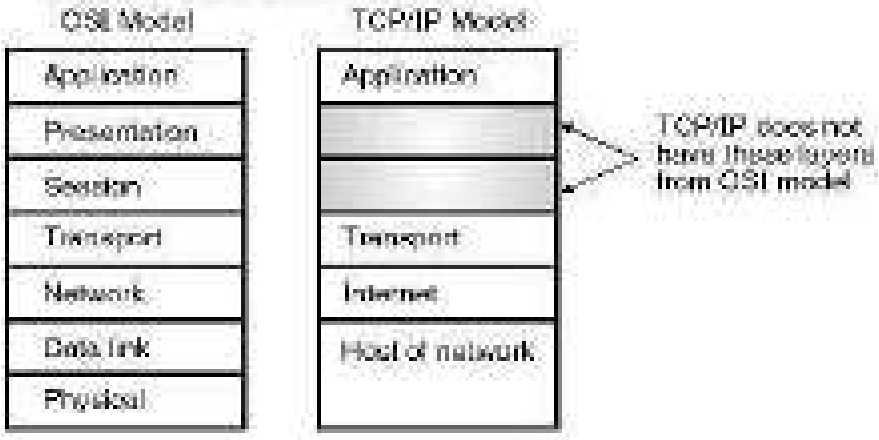
- **Q. 1** Differentiate between OSI and TCP/IP model with neat diagram. **(W-08, 8 Marks)**
- **Q. 2** Compare OSI and TCP/IP reference model **(W-10, 8 Marks)**
- **Q. 3** Compare OSI and TCP / IP (4 points) reference model with figure. **(W-11, 8 Marks)**
- **Q. 4** Compare and contrast TCP/IP network model, with OSI model. **(S-12, 4 Marks)**
- **Q. 5** Describe TCP/IP with neat sketch. Compare TCP/IP and OSI reference model. **(S-14, 4 Marks)**
- **Q. 6** Compare OSI reference model and TCP/IP network model. **(W-14, 4 Marks)**
- **Q. 7** Compare OSI and TCP/IP network model. **(W-16, 4 Marks)**

Similarities between OSI and TCP/IP Models :

- Following are some of the similarities between OSI and TCP/IP models :

1. In both the models the functions of layers is approximately same.
2. Both models use the concept of layered architecture.
3. The transport layers and the layers below it provide transport services independent of networks.
4. In both the models, the layers above transport layer are application oriented.

- Refer to Fig. 11.8.1 and Table 11.8.2 for the comparison of the two reference models.



(S-13) **Fig. 11.8.1 : Relationship between OSI and TCP/IP models**

Table 11.8.2 : Difference between OSI and TCP/IP model

OSI	TCP/IP
Has 7 layers	Has 4 layers
Transport layer guarantees delivery of packets.	Transport layer does not guarantee delivery of packets.
Horizontal approach.	Vertical approach.
Separate session layer.	No session layer, characteristics are provided by transport layer.
Separate presentation layer.	No presentation layer, characteristics are provided by application layer.
Network layer provides both connectionless and connection oriented services.	Network layer provides only connection less services.
It defines the services, interfaces and protocols very clearly and makes a clear distinction between them.	It does not clearly distinguish between service, interfaces and protocols.
The protocols are better hidden and can be easily replaced as the technology changes.	It is not easy to replace the protocols.
OSI is truly a general model.	TCP/IP cannot be used for any other application.
It has a problem of protocol fitting into a model.	The model does not fit any other protocol stack.

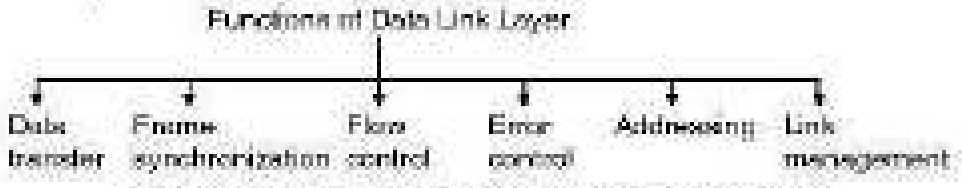
11.8.2 Demerits of TCP/IP Model :

1. TCP/IP model does not clearly distinguish the concepts of service, interface and protocol.
2. This model is not at all general and it cannot describe any protocol stack other than TCP/IP.
3. The host-to-network layer is not a layer at all in the normal sense. It is simply an interface.
4. The TCP/IP model does not even mention the physical and data link layers. A proper model should include both as separate layers.

11.9 Data Link Layer Design Issues (Functions of Data Link Layer) :

– The data link layer is supposed to carry out many specified functions.

– For effective data communication between two directly (physically) connected transmitting and receiving stations the data link layer has to carry out a number of specific functions as follows :



(L-664)**Fig. 11.9.1 : Functions of data link layer**

1. Services provided to the network layer :

– The data link layer provides a well defined service interface to the network layer.

– The principle service is transferring data from the network layer on sending machine to the network layer on destination machine.

– This transfer always takes place via the DLL.

2. Frame synchronisation :

– The source machine sends data in the form of blocks called frames to the destination machine.

– The starting and ending of each frame should be identified so that the frames can be recognized by the destination machine.

3. Flow control :

– The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.

4. Error control :

– The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

5. Addressing :

– When many machines are connected together (LAN), the identity of the individual machines must be specified while transmitting the data frames.

– This is known as addressing.

6. Control and data on same link :

– The data and control information is combined in a frame and transmitted from the source to destination machine.

- The destination machine must be able to separate out the control information from the data being transmitted.

7. **Link management :**

- The communication link between the source and destination is required to be initiated, maintained and finally terminated for effective exchange of data.
- It requires co-ordination and co-operation among all the involved stations. Protocols or procedures are required to be designed for the link management.

11.9.1 Nodes and Links :

- The type of communication taking place at the data link layer level is called as the **node to node communication.**
- A packet sent by a computer in the Internet will have to travel through different types of networks (LANs and WANs) before reaching the destination.
- All these LANs and WANs are connected to each other using routers.

Node :

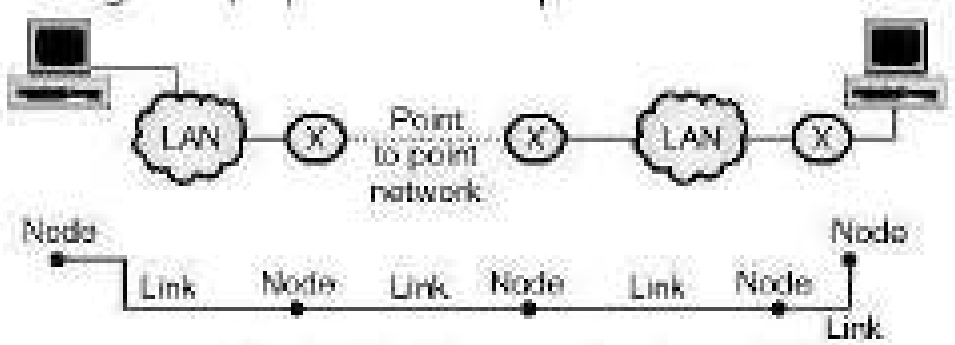
- We can define a **node** as the two end hosts and the routers inbetween them.

Link :

- The networks inbetween the two and hosts and the routers are called as **links.**

Source node and destination node :

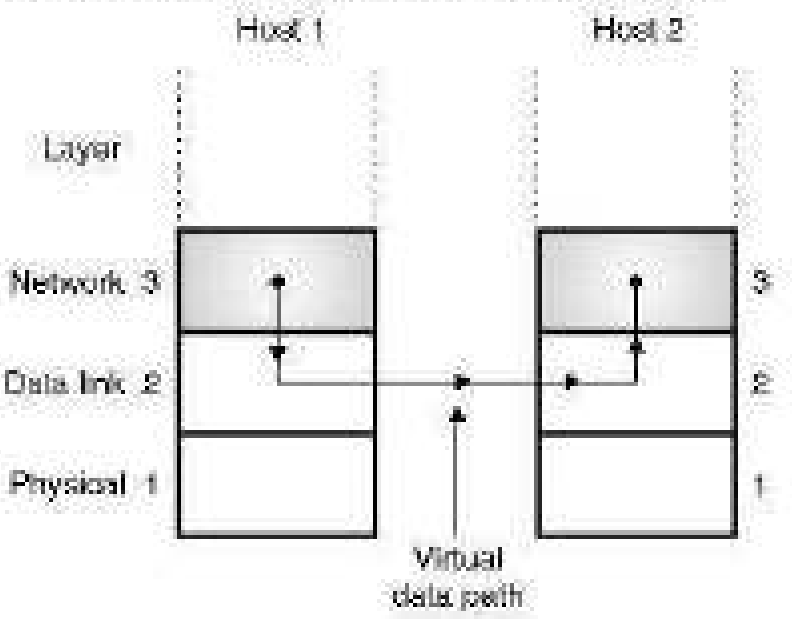
- The first node in the network is called as the source node while the last node is called as the destination node.
- Fig. 11.9.2, explains the concept of nodes and links.



(G-2073) **Fig. 11.9.2 : Concept of nodes and links**

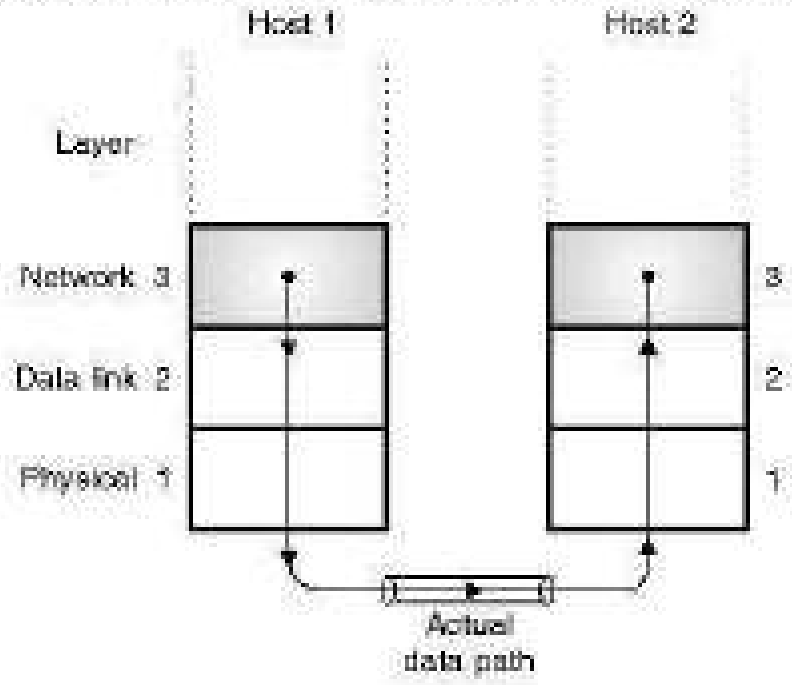
11.9.2 Services Provided to Network Layer :

- Network layer is the layer above the data link layer in the OSI model. So it is supposed to provide services to the network layer.
- The main service to be provided is to transfer data from the network layer on the sending machine to the network layer of the receiving machine.
- The virtual path followed for such a communication is shown in Fig. 11.9.3(a). It is not the actual path.



(L-665) **Fig. 11.9.3(a) : Virtual communication**

- The actual path followed by the data from sending machine to destination is shown in Fig. 11.9.3(b) which is via all the layers below the network layer, then the physical medium, then layers 1,2,3 of receiving machine.



(L-665) **Fig. 11.9.3(b) : Actual data path**

- However it is always easier to think that the communication is taking place through the data link layers (Fig. 11.9.3(a)) using a data link layer protocol.

11.9.3 Types of Services Provided :

- Data link layer can be designed to offer different types of services. Some of them are as follows :
  1. Unacknowledged connectionless service.
  2. Acknowledged connectionless service.
  3. Acknowledged connection oriented service.

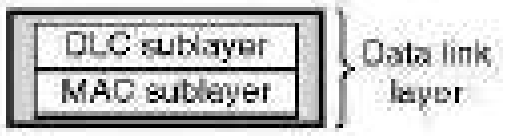
11.10 Two Sublayers :

11.10.1 Two Categories of Links :

- The medium which connects two nodes physically can be a cable or air.
- But the important point here is that the function of data link layer is to control how the medium is used.
- We can have a DLL which can utilize the capacity of the medium either fully or partially.
- A partially used medium is called as a **point to point link** whereas a fully used medium is called as the **broadcast link.**

11.10.2 Two Sublayers :

- We can divide the data link layer into two sublayers, in order to have a better understanding of its functionality and services provided by it.
- The two sublayers are as follows :
  1. Data link control sublayer (DLC).
  2. Media access control sublayer (MAC).
- The two sublayers are as shown in Fig. 11.10.1.



(G-2074) **Fig. 11.10.1 : Two sublayers in data link layer**

- The DLC sublayer is supposed to handle all the issues common to the point to point as well as broadcast links.
- However the MAC sublayer is supposed to handle the issues related only to broadcast links.

11.11 Three Types of Addresses :

- There are some data link layer protocols which define the following three types of addresses :
  1. Unicast address.
  2. Multicast address.
  3. Broadcast address.

11.11.1 Unicast Address :

- The meaning of the word **unicast** is **one-to-one** communication. A unicast address is assigned to each host or each interface of a router.
- Therefore if a frame is having a unicast destination address, then it is destined to go to only one entity in the link.
- The example of a unicast address is the LAN address. Ethernet addresses are 48 bit in length (six bytes) which is written as 12 hexadecimal digits separated by colons.
- The example of a link layer unicast address of a computer is as shown in Fig. 11.11.1(a).

A4 : 36 : 43 : 12 : 94 : E1

Fig. 11.11.1(a) : A unicast address

11.11.2 Multicast Address :

- There are some protocols, which define multicast addresses.
- The meaning of the word **multicasting** is **one-to-many,** communication. However the communication is local i.e. inside the link.
- The multicast link layer addresses are very commonly used in LANs, Ethernet.
- They are 48 bit(6 bytes) long and are written as 12 hexadecimal digits separated by colons as shown in Fig. 11.11.1(b).
- Note that in the multicast address, the second digit should be an even number in hexadecimal.

A2 : 36 : 47 : 15 : 92 : E1

Fig. 11.11.1(b) : Multicast address

11.11.3 Broadcast Address :

- There are some protocols, which define the broadcast addresses.
- The meaning of the word **broadcasting** is **one-to-all** communication.
- If a frame has a destination broadcast address, then it will be sent to all the entities connected in the link.
- The broadcast address are very commonly used in LANs, Ethernets. They are 48 bit (6 bytes) long with all the bits equal to 1.
- They are written as 12 hexadecimal digits separated by colons as shown in Fig. 11.11.1(c).

FF : FF : FF : FF : FF : FF

Fig. 11.11.1(c) : Broadcast address

11.12 ARP (Address Resolution Protocol) :

W-08, S-09, S-12, S-13, S-14, W-14, W-15, W-16

MSBTE Questions

Q. 1 What is MAC address ? **(W-08, S-09, 2 Marks)**

Q. 2 Explain function of ARP protocol. **(W-08, 4 Marks)**

Q. 3 Define IP-address. **(S-12, 2 Marks)**

Q. 4 What is MAC address ? Write the instruction to find MAC address. **(S-13, 2 Marks)**

Q. 5 What is ARP ? What are the functions of ARP ? **(S-13, 4 Marks)**

Q. 6 Describe meaning and function of :
1. MAC address 2. IP address. **(S-14, 4 Marks)**

Q. 7 Give the name of protocols used by different layers of TCP/IP. Discuss the function of ARP and RARP. **(W-14, 4 Marks)**

Q. 8 What is MAC address ? How it is located ? **(W-15, 4 Marks)**

Q. 9 Explain the protocols : ARP **(W-16, 4 Marks)**

- ARP as defined in RFC 826 is Ethernet Address Resolution Protocol.
- ARP provides service to IP, which make us think that it is in the link layer TCP/IP model (or DLL of OSI model).
- But its messages are carried by DLL protocol and are not capsulated within IP datagrams.
- That is why it can be called as a network layer protocol as well. Thus ARP occupies an unusual place in TCP/IP model.
- But the most important point is that ARP provides an essential service when TCP/IP is running on a LAN.
- An internet consists of various types of networks and the connecting devices like routers.
- A packet starts from the source host, passes through many physical networks and finally reaches the destination host.
- At the network level the hosts and routers are recognised by their IP addresses.

IP address :

- An IP address is an internetwork address. It is a universally unique address.
- Every protocol involved in internetworking requires IP addresses.

MAC address :

- The packets from source to destination hosts pass through physical networks.
- At the physical level the IP address is not useful but the hosts and routers are addressed by their MAC addresses.
- A MAC address is a local address. It is unique locally but it is not unique universally.
- The IP and MAC address are two different identifiers and both of them are needed, because a physical network can have two different protocols operating at the network layer at the same time.
- Similarly a packet may travel through different physical networks.
- So to deliver a packet to a host or a router, we require addressing to take place at two levels namely IP addressing and MAC addressing.
- Most importantly we should be able to map the IP address into a corresponding MAC address.

11.12.1 Mapping of IP Address into a MAC Address :

- We have seen the need of mapping an IP address into a MAC address.
- Such a mapping can be of two types :
  1. Static mapping.
  2. Dynamic mapping.

1. Static mapping :

- In static mapping a table is created and stored in each machine. This table associates an IP address with a MAC address.
- If a machine knows the IP address of another machine then it can search for the corresponding MAC address in its table.
- The limitation of static mapping is that the MAC addresses can change.
- These changed MAC addresses must be updated periodically in the static mapping table.

2. **Dynamic mapping :**

- In dynamic mapping technique a protocol is used for finding the other address when one type of address is known.
- There are two protocols used for carrying out the dynamic mapping. They are :
  1. Address Resolution Protocol (ARP).
  2. Reverse Address Resolution Protocol (RARP).
- The ARP is used for mapping an IP address to a MAC address whereas the RARP is used for mapping a MAC address to an IP address.

11.12.2 ARP Operation :

S-09, S-12, S-13, W-15

MSBTE Questions

Q. 1 How ARP is located ? **(S-09, 1 Mark)**

Q. 2 Why is ARP request broadcast but ARP reply unicast ? **(S-12, 4 Marks)**

Q. 3 What is MAC address ? Write the instruction to find MAC address. **(S-13, 2 Marks)**

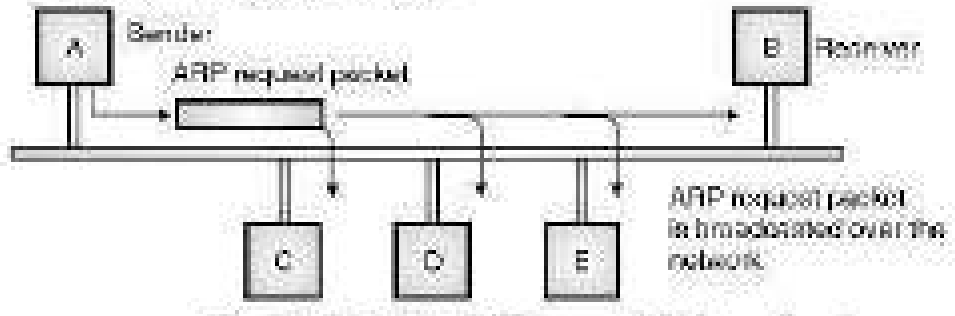
Q. 4 What is MAC address ? How it is located ? **(W-15, 4 Marks)**

- ARP is used for mapping an IP address to its MAC address. For a LAN, each device has its own physical or station address as its identification.
- This address is stored on the NIC (Network Interface Card) of that machine.

How to find the MAC address ?

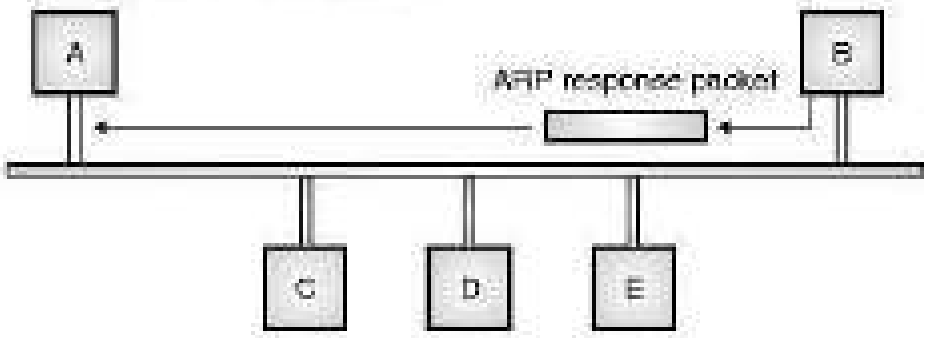
- When a router or a host (A) needs to find the MAC address of another host (B) the sequence of events taking place is as follows :

1. The router or host A who wants to find the MAC address of some other router, sends an ARP request packet. This packet consists of IP and MAC addresses of the sender A and the IP address of the receiver (B).
2. This request packet is broadcasted over the network as shown in Fig. 11.12.1(a).



(G-575) **Fig. 11.12.1(a) : ARP request is broadcast**

3. Every host and router on the network will receive the ARP request packet and process it. But only the intended receiver (B) will recognize its IP address in the request packet and will send an ARP response packet back to A.
4. The ARP response packet has the IP and physical addresses of the receiver (B) in it. This packet is delivered only to A (unicast) using A's physical address in the ARP request packet. This is shown in Fig. 11.12.1(b). Thus host A has obtained the MAC address of B using ARP.



(G-576) **Fig. 11.12.1(b) : ARP response unicast**

11.12.3 ARP Cache Memory :

- The use of ARP would be inefficient if A needs to broadcast an ARP request for each IP packet that is to be sent to B, because instead of broadcasting the request it could have broadcast the IP packet itself.
- So ARP is efficient only if the ARP reply is stored in cache memory (cached) for a while.
- This is due to the fact that a system generally sends hundreds of packets to the same destination.
- Thus the system that receives an ARP reply stores the mapping in the cache memory and keeps it for 20 to 30 minutes.
- So if packets are again sent to the same destination then it could use this mapping instead of broadcasting an ARP request.
- Before sending an ARP request, the system checks its cache to see if the mapping could be found.

11.12.4 ARP Packet Format : W-10

MSBTE Questions

Q. 1 List any two functions of ARP message fields. **(W-10, 2 Marks)**

- The ARP message format is as shown in Fig. 11.12.2. The various fields in it are as follows :

Hardware Type (16 bits)		Protocol type (16 bits)
Hardware length	Protocol length	Operation request 1, Reply 2
Sender hardware address		
Sender protocol address		
Target hardware address		
Target protocol address		

Fig. 11.12.2 : ARP message format

1. **HTYPE (Hardware Type) :** This 16 bit field defines the type of network on which ARP is being run. ARP is capable of running on any physical network.
2. **PTYPE (Protocol Type) :** This 16 bit field is used to define the protocol using ARP. Note that we can use ARP with any higher-level protocol such as IPv4.
3. **HLEN (Hardware length) :** It is an 8 bit field which is used for defining the length of the physical address in bytes. For example, this value is 6 for Ethernet.
4. **PLEN (Protocol Length) :** This field is 8 bit long and it defines the length of the IP address in bytes. For IPv4 this value is 4.
5. **OPER (Operation) :** It is a 16 bit field which defines the type of packet. The two possible types of packets are : ARP request (1) and ARP reply (2).
6. **SHA (Sender Hardware Address) :** This field is used for defining the physical address of the sender. The length of this field is variable.
7. **SPA (Sender Protocol Address) :** This field defines the logical address of the sender. The length of this field is variable.
8. **THA (Target Hardware Address) :** It defines the physical address of the target. It is a variable length field. This field contains all zeros for the ARP request packet, because the receivers physical address is not known to the sender.
9. **TPA (Target Protocol Address) :** This field defines the logical address of the target. It is a variable length field.

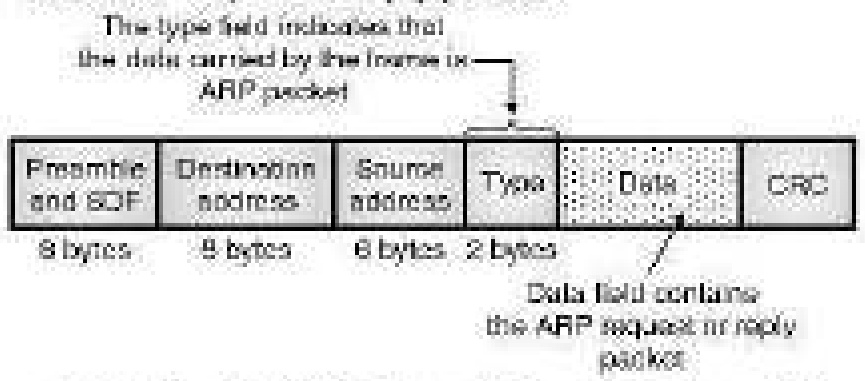
11.12.5 Encapsulation : S-16, W-16

MSBTE Questions

Q. 1 Explain the concept of encapsulation. **(S-16, 4 Marks)**

Q. 2 Describe the concept of encapsulation. **(W-16, 4 Marks)**

- An ARP packet (request or reply) is inserted directly into the data link frame. Such an insertion is known as encapsulation.
- Fig. 11.12.3 shows an example of encapsulation in which an ARP packet being encapsulated in an Ethernet frame. The type field shows that the data carried by the frame is an ARP request or reply packet.



(G-578) **Fig. 11.12.3 : Encapsulation of ARP packet**

11.12.6 Operation of ARP on Internet :

- The services of ARP can be used under the following working conditions when it is being operated on internet :
  1. The sender is a host and wants to communicate with another host which is on the same network.
  2. The sender is a host and wants to communicate with a host on another network.
  3. The sender is a router. It has received a datagram with a destination address of a host on another network.
  4. The sender is a router. It has received a datagram which is meant for a host in the same network.
- Now let us see how ARP works on the internet.

Operation :

1. The sender (host or router) knows the IP address of the target.
2. IP orders ARP to create an ARP request message. The request packet consists of senders physical and IP addresses plus the IP address of the target but the physical address of the target is not known.
3. This ARP request packet is sent to the data link layer. Here the ARP request packet is inserted in a frame.
4. Every router or host receives this frame because it is broadcast. All the machines except the target drop this packet as discussed earlier.
5. The target machine sends back a reply packet which contains the target's physical address. This reply is unicast and addressed only to the sender.

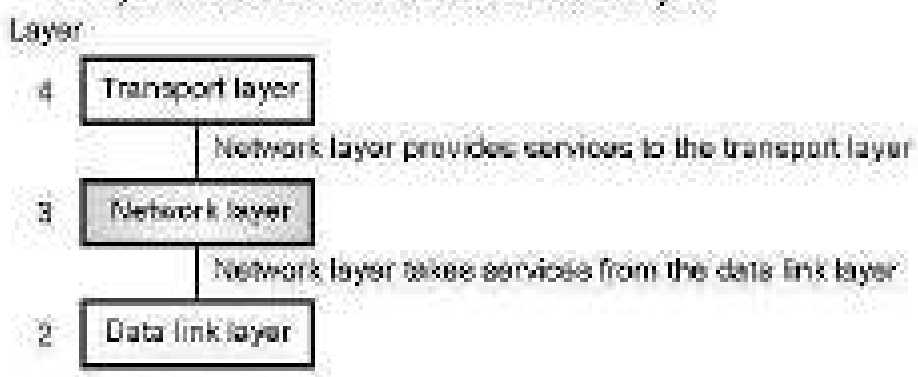
6. The sender receives the reply packet. Hence the physical address of the target has been obtained.
7. The IP datagram carrying data for the target machine is inserted in a frame and the frame is unicast to the target machine.

11.13 Network Layer :

- The network layer is responsible for carrying the packet from the source all the way to destination. In short it is responsible for host-to-host delivery.
- The network layer has a higher responsibility than the data link layer, because the data link layer is only supposed to move the frames from one end of the wire to the other end.
- Thus network layer is the lowest layer that deals with the end-to-end transmission.

Position of network layer :

- Fig. 11.13.1 shows the position of network layer in the 5 layer internet model. It is the third layer.



(G-433) **Fig. 11.13.1 : Position of network layer**

- It receives services from the data link layer and provides services to the transport layer.
- The network layer was designed to solve the problem of delivery through several links.
- The network layer is also called as the **Internetwork** layer.
- In addition to the host-to-host delivery the network layer is also responsible for **routing** the packets through the router.
- As a pure concept we can imagine that the Internet is a black box which connects a very large number of computers in the entire world together.
- But the Internet also is not a single network. It is infact the network of many networks or links.
- That means the Internet is an internetwork which is actually a combination of LANs and WANs.
- All these LANs and WANs are connected to each other via a connecting device such as a **router** which acts as a switch.

Routers :

- Routers have many ports or interfaces. When it receives a packet at one of its ports, it forwards the packet through another port to the next switch or the final destination.

11.13.1 Network Layer Services :

- The duty of the network layer in TCP/IP is to provide the host-to-host delivery of datagrams.
- In this section we are going to discuss the services that are expected from the network layer.
- At the sending end, the network layer will accept a packet from its transport layer, encapsulate the packet into datagram and will deliver the packet to the data link layer.
- At the destination, exactly opposite process takes place. That means, at the destination the received datagram is decapsulated to extract the packet from it and the packet is delivered to the transport layer.

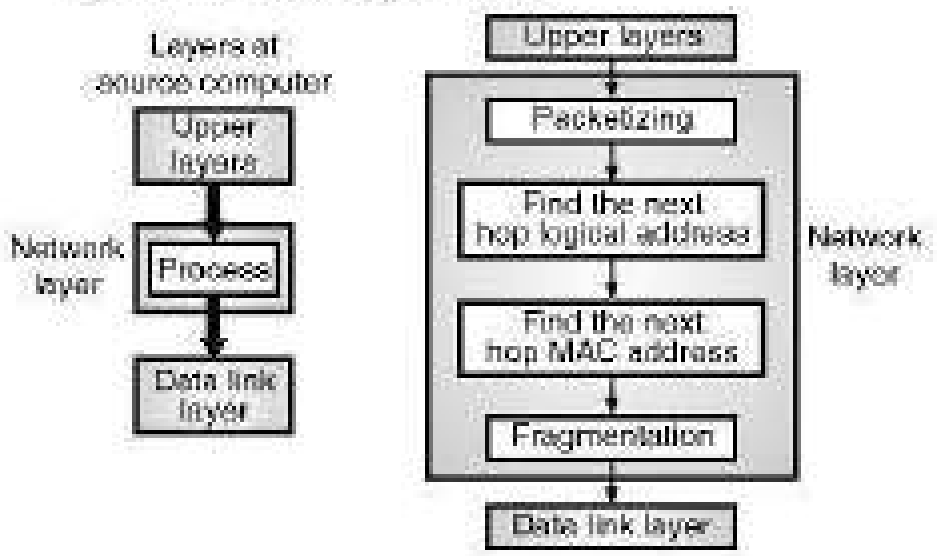
11.13.2 Logical Addressing :

- The two computers in communication with each other should have some universal identification system which is called as the **network layer address or logical address.**
- Thus the sending and receiving computers must have two network-layer addresses for them to communicate.

11.13.3 Services Provided at the Source Computer :

- The following four services are provided by the network layer at the source computer :
  1. Packetizing.
  2. To find the logical address of the next hop.
  3. To find the physical or MAC address for the next hop.
  4. Fragmentation of the datagram if necessary.
- These services are as shown in Fig. 11.13.2(b).
- The upper layers (transport and application) take services of the network layer. For this the upper layers send several pieces of information.

– The network layer processes these pieces of information and creates fragmented datagrams alongwith the next hop MAC address to finally deliver it to the data link layer as shown in Fig. 11.13.2(a).



(a) Network layer process (b) Network layer services

(G-1999) Fig. 11.13.2

1. Packetizing :

– **Packetizing** is the first duty of the network layer in which it encapsulates the payload (data received from the transport layer) in a packet at network layer at the source.

– Then at the destination the decapsulation process takes place.

– In this way the network layer is doing the job of a postal service in delivering the packages from source to destination.

At the source :

– At the sending end the events take place in the following sequence :

1. The payload (data) from the upper layer is received.
2. A header containing the source and destination address and some other information is added to the payload.
3. This packet is then delivered to the data layer.
4. If the payload is too large, then the host carries out **fragmentation** on it. Otherwise the host is not allowed to modify the contents of the payload.

2. Finding the logical address of the next hop :

– The datagram prepared with packetizing contains the source and destination addresses of the packet.

– The datagram is to be delivered to the next router.

– But the source and destination addresses in the datagram do not give any information about the logical address of the next hop.

– The network layer at the source computer finds the logical address of the next hop by consulting a routing table.

3. Finding MAC address of next hop :

– Note that it is the duty of data link layer (and not of network layer) to actually deliver the datagram to the next hop.

– And to do this the data link layer needs the physical or MAC address of the next hop.

– The network layer uses another table to map the logical address of next hop into the corresponding MAC address of next hop.

– However generally an auxiliary protocol called as ARP (Address Resolution Protocol) is used for this purpose.

4. Fragmentation :

– The datagram at this stage may not always be ready to be given to the data link layer.

– The LANs and WANs can carry the data of a limited size in a frame.

– If the data is longer than the maximum specified size for LANs and WANs then it is not possible to fit it in one frame.

– In such circumstances, the datagram should be **fragmented** in to smaller data units before passing it to the data link layer.

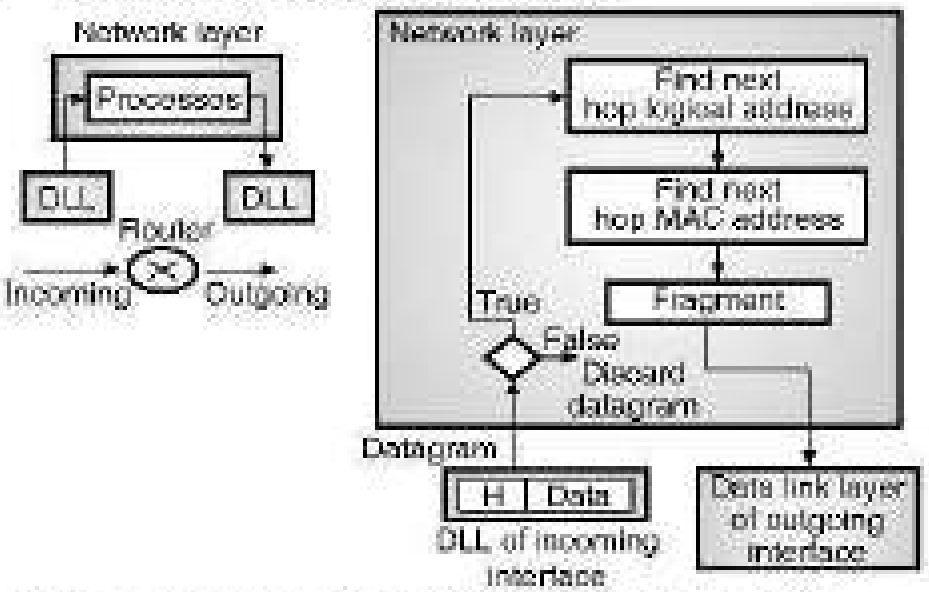
– The datagram header is copied into all these fragments so that all the necessary information in the datagram is present in every fragment.

– In addition to this some more information regarding the position of that fragment in the whole datagram should be added to the header of the fragment.

11.13.4 Services Provided at Each Router :

– The routers present in between the source and destination are supposed to check the source and destination addresses in the packet in order to forward it to the next network on the path.

- The router is not allowed to decapsulate the received packet unless it is too big and fragmentation needs to be carried out on it.
- The routers are not supposed to change the source and destination addresses.
- In the event of fragmentation, a router has to copy the header in all the fragments.
- At the router the services provided by the network layer are as follows :
  1. To find the next hop logical address.
  2. To find the next hop MAC address.
  3. To carry out fragmentation if required.
- Fig. 11.13.3 shows all these services.



(a) Process at the router (b) Services provided at the router

(c-2006) Fig. 11.13.3

- Before providing the services mentioned above the router checks the validity of the incoming datagram with the help of checksum.
- In checking the validation, the following two things are checked :
  1. Whether the datagram header is corrupted.
  2. Whether the datagram is delivered to the correct router.
- If the incoming datagram fails the validation test then it is simply discarded as shown in Fig. 11.13.3(b).

11.13.5 Services Provided at the Destination Computer :

- The sequence of events taking place at the destination is as follows :
  1. The network layer packet is received from the data link layer.
  2. The received packet is decapsulated and the payload is delivered to the upper layer protocol.
  3. If a large packet is fragmented by either the source host or a router, then the responsibility of the network layer at the destination is to wait until all fragments are received, reassemble them and deliver them to the upper layer protocol.
- The network layer at the destination computer is much simpler than that at the source computer or router.
- Before providing any service, the received datagram should be subjected to validation.
- If it passes the validation test then all the services mentioned above should be provided. Otherwise the datagram is discarded.
- The network layer also sets a reassembly timer when it receives fragments of a datagram that are to be reassembled.
- If the reassembly timer expires before arrival of all the fragments, then all data fragments are destroyed and an error message is sent that the entire fragmented datagram be sent again.

11.14 Routing and Forwarding :

- The other two important duties of the network layer, which are related to each other are routing and forwarding.

11.14.1 Routing :

- The responsibility of the network layer is to route the packets from its source to destination.
- The physical network through which the packets travel consists of LANs, WANs and routers.
- Due to this the source and destination are connected to each other via more than one routes.
- It is the responsibility of the network layer to find the best route out of all the possible routes.
- In order to achieve this goal, the network layer must have some concrete strategy for defining the best route.
- In the modern days, this is done by running an appropriate routing protocol which helps the routers to coordinate their knowledge about the neighbouring routers and prepare routing tables which can be used on the arrival of a packet.

- These routing protocols should be run before commencement of any communication.

11.14.2 Forwarding :

- We can define the process of forwarding as the action taken by a router when it receives a packet at one of its interfaces.
- A router takes such an action with the help of the decision making tables called as **forwarding table** or **routing table.**
- When a packet arrives at one of the interfaces of a router from one of the attached network, the router has to forward it to another attached network.
- The router has to make this decision with the help of a piece of information present in the packet header.
- This piece of information can be the **destination address** or a **lable.**
- The router can use this information to find the corresponding output interface number in the **forwarding table.**

11.14.3 Other Services :

- The other services expected from the network layer are as follows :
  1. Error control.
  2. Flow control.
  3. Congestion control.
  4. Quality of service (QoS).
  5. Security.

11.15 Network Layer (IP) Addresses :

- Each computer connected to the Internet should be identified uniquely. The identifier used for this purpose is called as the **Internet address** or IP address.
- The hosts and routers on the Internet have unique IP addresses.
- The current version of IP (Internet Protocol) is IPv4 whereas the advanced version is IPv6.
- The IPv4 address is a 32-bit address and it is used for defining the connection of a host or router to the Internet. **Thus an IP address is an address of the interface.**

Uniqueness of IP Addresses :

- The IP address is **unique** and **universal.** That means each IP address defines only **one connection** to the Internet.
- At any given time, no two devices connected to the Internet can have the same IP address.
- But if a device is connected to the Internet via two connections through two different networks, then it can have two different IP addresses.
- All the IPv4 addresses are 32 bit long and they are used in the source address and destination address fields of the IP header.
- The IP addresses for hosts are assigned by the network administrator. For Internet it has to be obtained from the network information center.

11.15.1 Address Space :

- The IPv4 protocol has an address space. It is defined as the total number of addresses used by the protocol.
- If N number of bits are used for defining an address then the address space will be 2^N addresses.
- For IPv4, N is 32 bits. Hence its address space is 2^{32} or 4, 294, 967, 296 (more than 4 billion).
- So theoretically more than 4 billion devices could be connected to the Internet.
- Thus **the address space** of IPv4 is 2^{32}.

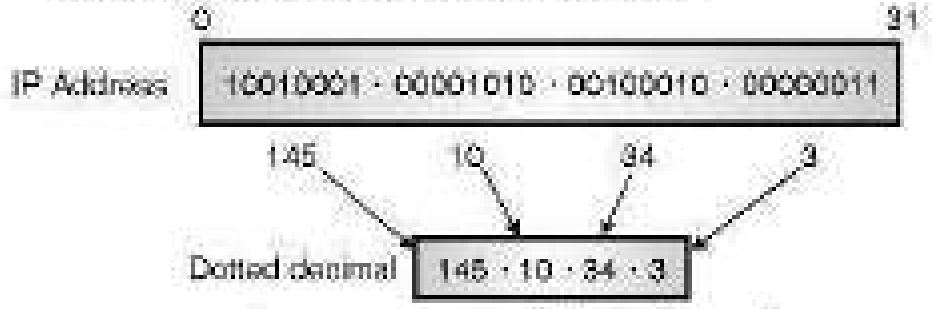
Notation :

- The IPv4 addresses can be shown use three different notations as follows :
  1. Binary notations (base 2).
  2. Dotted decimal notation (base 256).
  3. Hexadecimal notation (base 16).
- Out of these the **dotted decimal** notation is most commonly used.

Dotted decimal notation :

- This notation has become popular because of the two advantages it offers.
- This notation makes the IPv4 address more compact and easy to read.
- The 32 bit IPv4 address is grouped into groups of 8-bits each separated by decimal points (dots).

- Each 8-bit group is then converted into an equivalent decimal number as shown in Fig. 11.15.1.



(G-2001) **Fig. 11.15.1 : Dotted decimal notation**

- Each octet (byte) can take a value between 0 and 255. Therefore the IPv4 address in the dotted decimal notation has a range from 0.0.0.0 to 255.255.255.255.
- For example the IPv4 address of

  1001 0001.00001010 00100010 00000011 is denoted in the dotted decimal form as 145.10.34.3.

11.15.2 IPv4 Address Format :

- A 32 bit IPv4 address consists of two parts. The first part is called as **net id** i.e. network identification which identifies a network on the Internet and the second part is called as the **host id** which identifies a host on that network.
- Fig. 11.15.2 shows the IPv4 address format. Note that the **net id** and **host id** are of variable lengths depending on the class of address.
- Note that class D and E addresses are not divided into net id and host id for the reasons discussed later on.

(G-2002) **Fig. 11.15.2 : IPv4 address format**

11.15.3 Classful and Classless Addressing :

Classful addressing :

- The concept of IP addresses is few decades old. It uses the concept of **classes.** This architecture is called as the **classful addressing.**

Classless Addressing :

- Later on in mid 1990s a new architecture of addressing was introduced which was known as **classless addressing.**
- This new architecture has superseded the original architecture.
- In this section we are going to discuss the classful addressing.
- Even though the number of actual devices connected to Internet is much less than 4 billion, the address depletion has taken place due to flaws in the classful addressing scheme.
- We have run out of class A and B addresses. To overcome these problems, the super netting and subnetting has been tried as discussed earlier.
- But subnetting and supernetting also could not solve the problem of address depletion in IPv4.
- Due to increased number of Internet users, it was evident that a larger address space would be required as a long term solution to this problem.
- For this the length of the IP address should be increased which means the IP packet itself must be changed.
- A long term solution is to switch to IPv6. But a short term solution which uses the same address space has been deviced for IPv4. It is known as **classless addressing.**
- In the classless addressing, there are no classes but the address generation take place in blocks.
- The classless addressing was announced by the Internet authorities in 1996 in which blocks of variable length which do not belong to any class are used.

11.16 Host Configuration : DHCP :

I-Scheme : S-22

- DHCP (Dynamic host configuration protocol) is the first client server application program that is used after a host is booted.
- Thus it works as a bootstrap when the host is booted and is to be connected to the Internet, but does not know its IP address.
- A computer that makes use of the TCP/IP model must know its IP address.
- Along with its IP address it must also know the following information :
  1. Subnet mask of the computer
  2. IP address of the router, so that it can communicate with other networks.
  3. IP address of the name server so that it can use the names instead of addresses.
- All this information can be saved in a configuration file and accessed by computer when booting takes place. This is known as host configuration process.

- But what will happen if the workstation is discless or the computer is with a disc but it is being booted for the first time.
- If a computer is discless, then it is possible to store the operating system and networking software in the ROM.
- But this information is not known to the manufacture and therefore cannot be stored in ROM.
- This information is dependent on the configuration of individual machine and it defines which network the machine is connected to.

11.16.1 Previously used Protocols :

- Now a days DHCP has become the formal protocol for host configuration.
- But the two protocols which were used earlier for the same purpose were RARP and BOOTP.
- RARP is Reverse Address Resolution Protocol and BOOTP stands for Bootstrap protocol.

BOOTP :

- The Boot strap protocol (BOOTP) was being used exclusively prior to DHCP.
- This protocol is a client/server protocol and it is designed in such a way that the dements of RARP could be overcome.
- Due to the client / server nature of BOOTP, its server can be present anywhere in the Internet.
- Also it can provide all the information that we mentioned earlier.
- It removes all the restrictions faced by RARP on providing this information.
- The problem with BOOTP is that is a **static configuration protocol.**
- That means when a client asks BOOTP to find its IP address, the BOOTP server will go through a **table** which contains the IP addresses corresponding to the physical addresses of the client and sends the IP address of the requesting client.
- But there are some situations in which the static configuration protocol like BOOTP does not work properly.
- For example when a host moves from one physical network to the other, its physical address is bound to change.
- Or another example is when a host wants a temporary IP address for using over only a short period of time.
- It is not possible for BOOTP to handle the situations mentioned above due to its static nature.
- Instead we need a **protocol** with **dynamic configuration** to deal with deal with these situations.

11.16.2 DHCP :

- The Dynamic Host Configuration Protocol (DHCP) was devices by IETF in order to make the configuration automatic.
- Thus DHCP does not require an administrator to add an entry for each computer, to the database that a server uses.
- Instead, in DHCP a mechanism is provided for any computer to join a new network and obtain an IP address automatically with no manual intervention.
- This is known a plug and play networking.
- Thus DHCP allows the use of computers that run server software as well as computers that run client software.
- When a computer that runs client software is shifted to a new network, it can use DHCP to obtain configuration information automatically.
- DHCP assigns a permanent address to a nonmobile computer that run server software.
- This address will not change when the computer **reboots.**
- To accommodate both type of computers, DHCP makes use of a client server approach.
- When a computer boots, it will broadcasts a DHCP Request. In response a server sends a DHCP Replay. An administrator can configure a DHCP server to have two types of addresses.
- First is the permanent address that are assigned to server computers, and second type is a pool of addresses which can be assigned on the basis of demand, when a computer boots and sends a request to DHCP.
- The DHCP find the configuration information by accessing its database
- If the database contains a specific entry for the computer then the server returns the information from the entry.

– However if there is no such entry exists for the computer, then the server chooses the next IP address from the pool and assigns it to the computer.

What is DHCP :

– DHCP, as the name suggests, is a protocol used for dynamically configuring the hosts on a network, such as workstations, personal computers and printers.

– DHCP can help in assigning various types of information such as routing information, directory-services information and default web server and mail servers.

– However, the most important and commonly used information for which DHCP is used is the IP address and subnet mask information.

– DHCP was primarily designed for managing the network and the clients automatically.

– With DHCP, it is not necessary to configure the network and client information manually for individual hosts.

– In addition, DHCP can coexist with statically configured hosts with fixed IP addresses.

– DHCP can also carry out the allocation of certain configuration information to a host on a permanent basis.

– This protocol provides a four point information (IP address, subnet mask, IP address of router, IP address of name server) to a diskless computer or to a computer which is booted for the first time.

– It is a client / server protocol which is backward compatible to the BOOTP.

11.16.3 Advantages of DHCP :

– The use of DHCP on a network offers the following advantages :

1. It sets free the network administrator from the duties of setting up the configuration information, such as the IP address, the subnet mask, and the routing tables, manually. The DHCP simplifies network administration by doing these tasks automatically.
2. Avoids this and the sometimes the same IP address is assigned to two different hosts. The DHCP avoids this and the consequent malfunctioning of both the hosts from happening.
3. If the DHCP was not used, then the movement of computers from one network to another requires must be reconfigured. With DHCP, you can move the computers to different subnets or networks without the need to reconfigure them. In such situations, DHCP takes care of IP address assignment and other configuration details.
4. Mobile computers, such as laptops and palmtops, can easily get connected to different networks. They don't require reconfiguration any more as they get their configuration information from the DHCP server.
5. DHCP allocates IP addresses from a pool of IP addresses. In addition, when a computer gets disconnected, its released IP address is returned to the resource pool. Therefore, the possibility of having unused IP addresses are minimized.

11.16.4 Components of DHCP :

– The use of DHCP on a network requires the following three components :

1. **DHCP server :** It assigns the IP address and other information to the clients when they request for the information.
2. **DHCP client :** It communicates with the DHCP server to get the desired information regarding its configuration. This communication can take place when the computer starts. The user of the DHCP client can also initiate a DHCP client request to the DHCP server to renew its information.
3. **DHCP relay agent :** It is used to relay (forward) client requests to the DHCP server. This is required when the DHCP server is yet to assign the client an IP address. Without an IP address, a client cannot use IP routing on its own. A DHCP relay agent helps the client to communicate with the DHCP server when the client does not have an IP address.

– When a client starts, it has an IP address of 0.0.0.0. It sends a broadcast message containing its MAC address and the computer name.

– In response the DHCP server sends an offer message that contains the MAC address of the client, the IP address offered to that client, the lease period for which the IP address will remain valid and its own IP address.

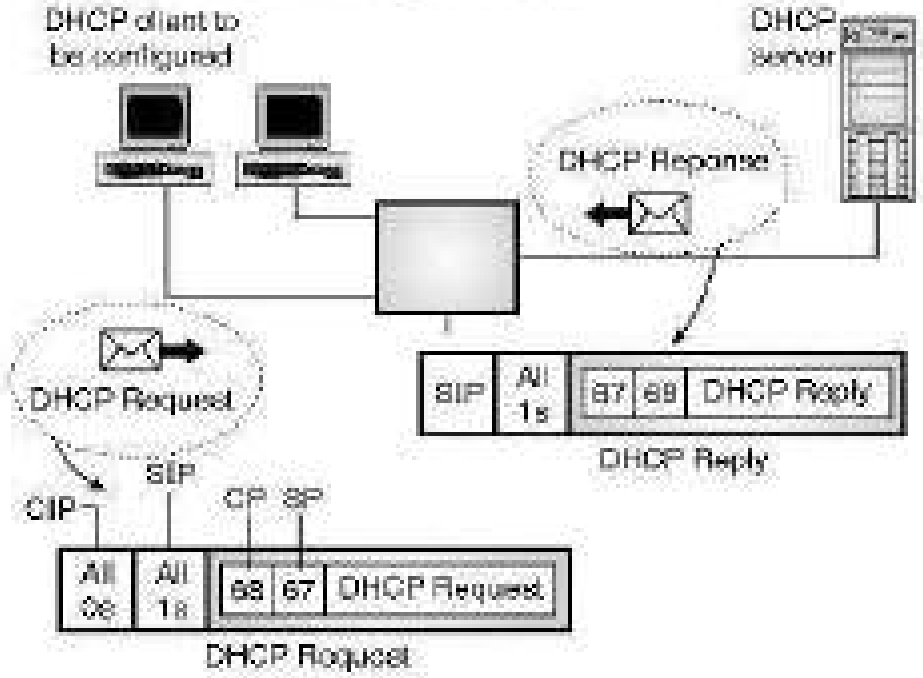
- The lease period is the time duration for which a client can use the IP address that has been assigned to it by the DHCP server.
- You can configure a DHCP server to set the lease time. When the client receives the IP address, it accepts the offer and then broadcasts the message that it has accepted the offer.

11.16.5 DHCP Operation :

- We will discuss the DHCP operation under two different operating conditions :
  1. DHCP client and server on the same network.
  2. DHCP client and server on different networks.

Operation on the same network :

- This situation is not a very common one. But sometimes the DHCP client and server happen to be on the same network as shown in Fig. 11.16.1.



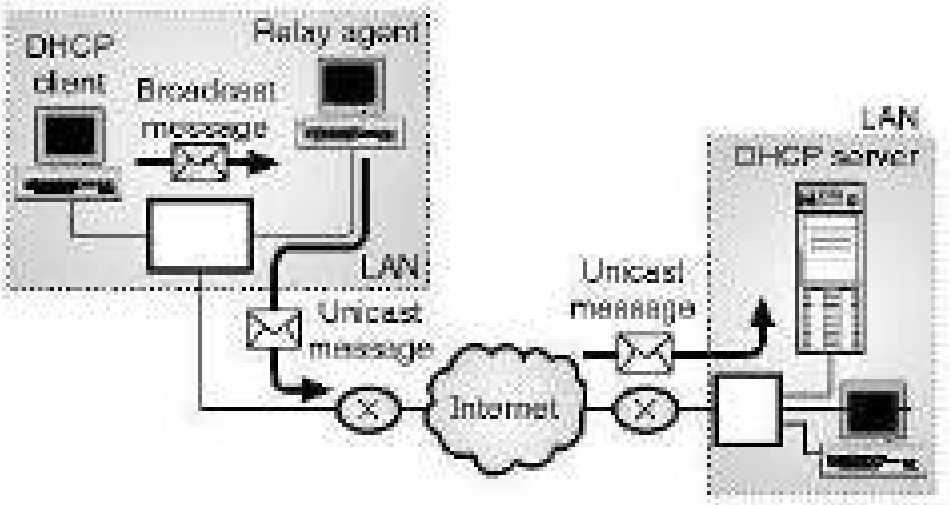
(G-1788) **Fig. 11.16.1 : Operation of DHCP when client and server are on the same network**

- The operation takes place as follows :

1. The DHCP server sends a passive open command on port 67 of UDP and waits for clients response.
2. The DHCP client sends an active open command on port 68 of UDP. This message is encapsulated in the UDP datagram with port 67 as destination port and port 68 as the source port. The UDP datagram is then encapsulated in an IP datagram. Note that the client at this time does not know its own IP address (i.e. the source address) and the server's IP address (destination address). Therefore the client uses an all zero address as source address and an all one address as destination address.
3. The server responds to this message by sending either a broadcast or a unicast message using port 67. It uses port 68 as the destination port. Broadcast address is used only for those system which do not allow the bypassing of ARP.

11.16.6 DHCP Operation on Different Networks :

- In this situation the DHCP client and server are on two entirely different networks, as shown in Fig. 11.16.2.



(G-1790) **Fig. 11.16.2 : DHCP operation when client and server are on different networks**

- In this situation a problem arises due to the broadcast nature of DHCP request. The client does not know the IP address of the server.
- Hence the DHCP request is a broadcast type (all 1s IP address). Any server does not allow the broadcast request to pass through it.
- So this request cannot reach the DHCP server.
- In order to solve this problem we can configure one of the hosts or router to operate as a relay agent as shown in Fig. 11.16.2.
- The relay agent knows the unicast address of the DHCP server.
- The relay will look for the broadcast request on port 67.
- As soon as it receives the broadcast request message, it encapsulates this message in a unicast datagram and sends it to the DHCP server.
- Such a unicast message is allowed to pass through by any router. Thus the request message reaches the DHCP server.
- The DHCP server sends its reply to the relay agent which in turn sends it to the DHCP client.

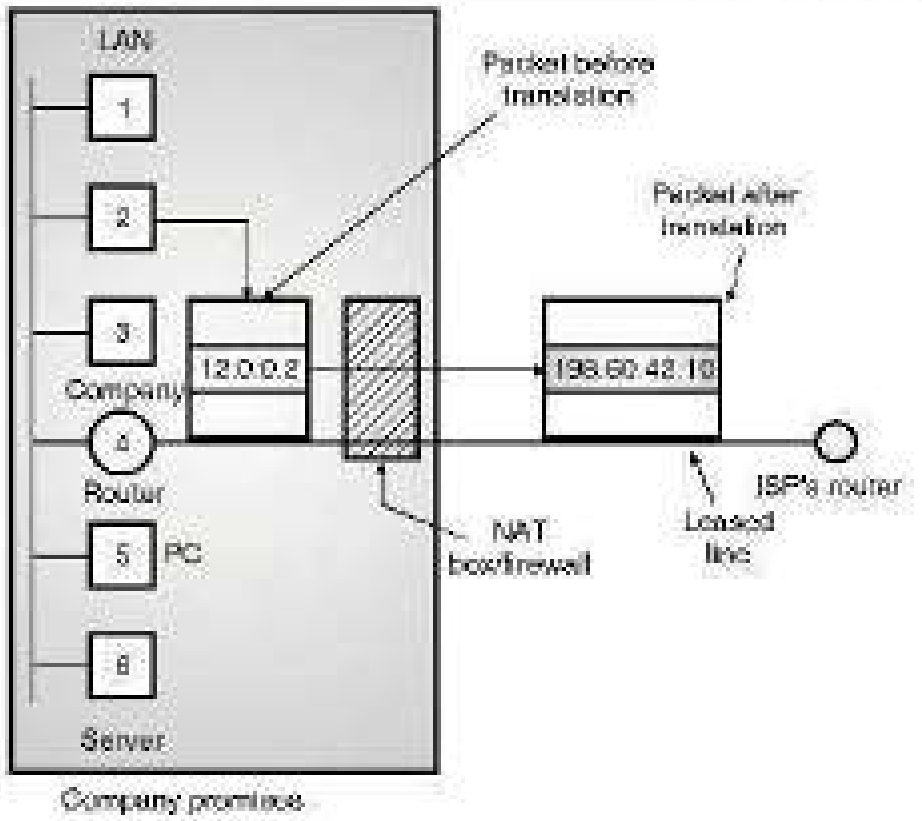
Note : In Fig. 11.16.2 only the message between the relay agent and client is it broadcast type. All the other messages are unicast types.

11.17 NAT – Network Address Translation :

- The problem that existing number of IP addresses is less than the actually required ones is practically important.
- A long term solution to this problem is that the whole Internet should be migrated from IPv4 to IPv6.
- This has begun, but will take year to get complete. (That means all the computers should have IPv6 addresses instead of IPv4 addresses).
- A quick solution to this problem is NAT i.e. Network Address Translation. It is described in RFC 3022.
- The basic idea in NAT is that each company is assigned a single IP address or at the most a small number of IP addresses so as to access the Internet.
- Within the company, every computer gets a unique IP address which is used for routing the internal traffic of the office.
- But when a packet goes out of the company, and goes to ISP, the translation of IP address takes place there.
- In order to make this scheme work, three ranges of IP addresses have been declared as private.
- Companies can use these addresses internally as per their requirement.
- However no packet containing these addresses is allowed to appear on the Internet. The three reserved ranges are as follows :

Range 1	10.0.0.0 to 10.255.255.255/8	16777216 Hosts
Range 2	172.16.0.0 to 173.31.255.255/12	1048 576 Hosts
Range 3	192.168.0.0 to 192.168.255.255/16	65 536 Hosts

- Generally most companies choose the addresses from the first range.
- Refer Fig. 11.17.1 which explains the operation of NAT. It shows that within the company premises, every machine has a unique address of the form 12.a.b.c.
- But when a packet leaves the company premises, it passes through the NAT box.
- This box converts the internal IP address 12.0.0.2 in Fig. 11.17.1 to the company's true IP address 198.60.42.10.

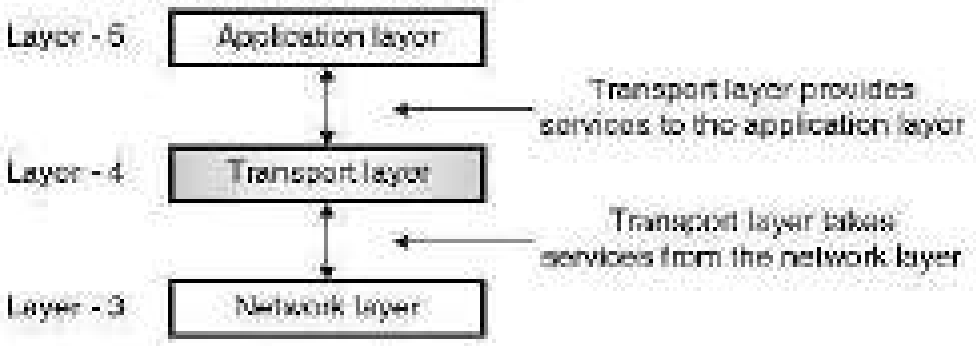


(e-551) **Fig. 11.17.1 : NAT**

- The NAT box is generally combined with a firewall. It is also possible to integrate the NAT box into company's router.

11.18 Transport Layer :

- The transport layer is the core of the Internet model. The application layer programs interact with each other using the services of the transport layer.
- Transport layer provides services to the application layer and takes services from the network layer.
- Fig. 11.18.1 shows the position of the transport layer in the 5-layer internet model.

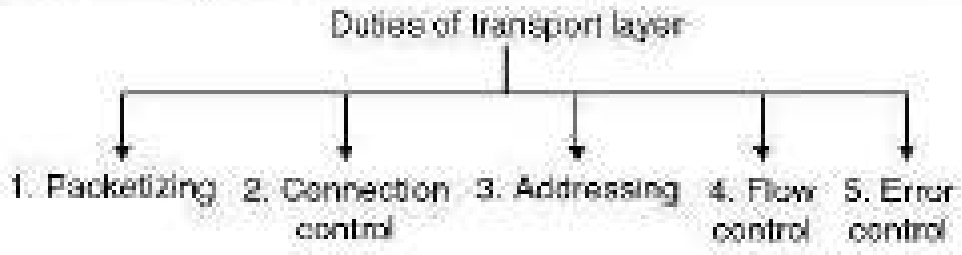


(e-552) **Fig. 11.18.1 : Position of transport layer**

- The transport layer is fourth layer in this model. It connects the lower three layers to upper three layers of an OSI layer.

11.18.1 Transport Layer Duties and Functionalities :

- Transport layer is meant for the process to process delivery and it is achieved by performing a number of functions.
- Fig. 11.18.2 lists the functions of a transport layer.



(G-1407) **Fig. 11.18.2 : Duties of transport layer**

1. Packetizing :

- The transport layer creates packets with the help of encapsulation on the messages received from the application layer.
- Packetizing is a process of dividing a long message into smaller ones.
- These packets are then encapsulated into the data field of the transport layer packet.
- The headers containing source and destination address are then added.
- The length of the message which is to be divided can vary from several lines (e-mail) to several pages.
- But the size of the message can become a problem. The message size can be larger than the maximum size that can be handled by the lower layer protocols.
- Hence the messages must be divided into smaller sections. Each small section is then encapsulated into a separate packet.
- Then a header is added to each packet to allow the transport layer to perform its other functions.

2. Connection control :

- Transport layer protocols are divided into two categories :

  1. Connection oriented. 2. Connectionless.

Connection oriented delivery :

- A connection oriented transport layer protocol establishes a connection i.e. virtual path between sender and receiver.
- This is a virtual connection. The packet may travel out of order.
- The packets are numbered consecutively and communication is bi directional.

Connectionless delivery :

- A connectionless transport protocol will treat each packet independently.
- There is no connection between them. Each packet can take its own different route.

3. Addressing :

- The client needs the address of the remote computer it wants to communicate with. Such a remote computer has a unique address so that it can be distinguished from all the other computers.

4. Flow and error control :

- For high reliability the flow control and error control should be incorporated.
- **Flow control :** We know that data link layer can provide the flow control. Similarly transport layer also can provide flow control. But this flow control is performed end to end and not across a single link.
- **Error control :** The transport layer can provide error control as well. But error control at transport layer is performed end to end and not across a single link. Error correction is generally achieved by retransmission of the packets discarded due to errors.

Congestion control and QoS :

- The congestion can take place in the data link, network or transport layer. But the effect of congestion is generally evident in the transport layer.
- Quality of Service (QoS) can be implemented in other layers but its actual effect is felt in the transport layer.
- The transport layer enhances the QoS provided by the network layer.

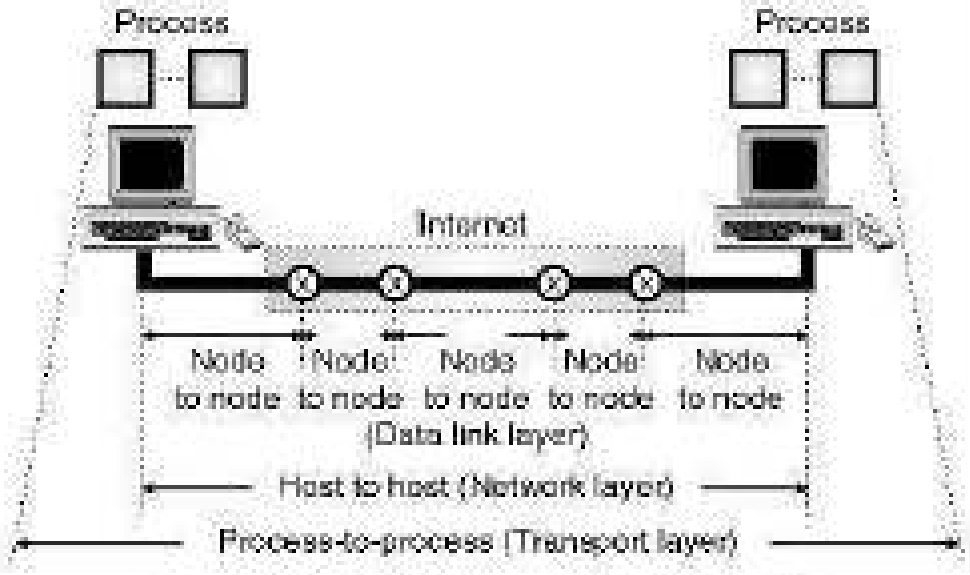
11.19 Transport Layer Services :

- In this section we are going to discuss the services provided by the transport layer.

11.19.1 Process-to-Process Communication :

- The data link layer performs a node to node delivery. The network layer carries out the datagram delivery between two hosts (host to host delivery).
- But the real communication takes place between two processes or application programs for which we need the **process-to-process delivery.**
- The transport layer takes care of the **process-to-process delivery.** In this a packet from one process is delivered to the other process.

- The relationship between the communicating processes is the client-server relationship. Fig. 11.19.1 demonstrates the three processes.



(G-594) **Fig. 11.19.1 : Types of data deliveries**

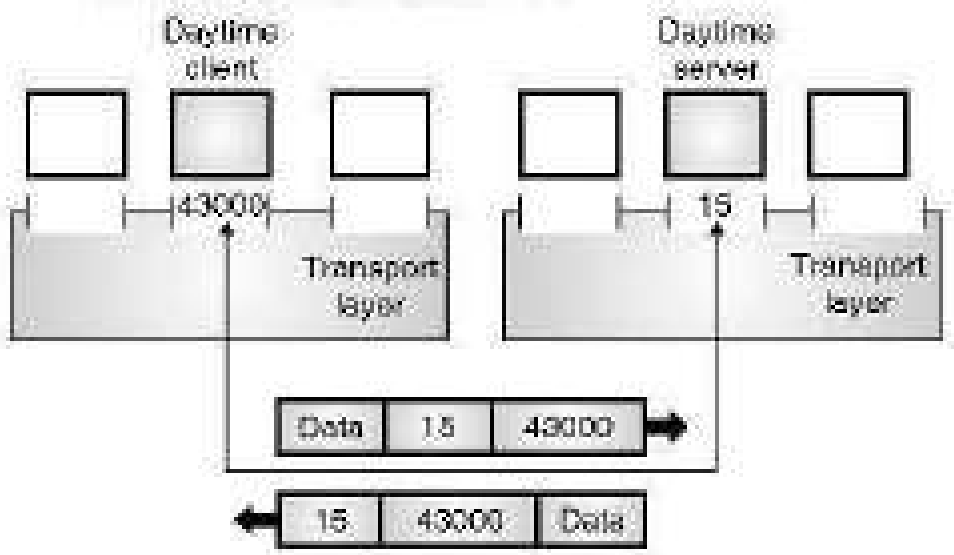
- There is a difference between host-to-host communication and process to process communication that we need to understand clearly.
- The host to host (computer to computer) communication is handled by the network layer.
- But this communication only ensures that the message is delivered to the destination computer. But this is not enough.
- It is necessary to handover this message to the correct process. The transport layer will take care of this.

11.19.2 Addressing : Port Number :

- There are several ways of achieving the process-to-process communication, but the most common method is using the client-server paradigm.
- **Client** is defined as the process on the local host. It needs services from another process called **server** which is on the other (remote) host.
- Both client and server have the same name. Some of the important terms related to the client-server paradigm are :

1. Local host
2. Remote host
3. Local process
4. Remote process

- We can use the IP addresses to define the local host and remote host. But this is not enough to define a process.
- In order to define a process, we have to use one more identifier called **Port Numbers.**
- In TCP/protocol model, the port numbers are integers and they are numbered between 0 and 65,535.
- At the data link layer we need a MAC address, at the network layer we need to use an IP address.
- A datagram uses the destination IP address to deliver the datagram and uses the source IP address for the destination's reply.
- At the transport layer a transport layer address called a **port number** is required to be used to choose among multiple processes running on the destination host.
- The destination port number is required to make the packet delivery and the source port number is needed to return back the reply.
- In the Internet model, the port numbers are 16 bit integers. Hence the number of possible port numbers will be 2^{16} = 65,535 and the port numbers range from 0 to 65,535.
- The client program identifies itself with a port number which is chosen randomly.
- This number is called as **ephemeral port number.** Ephemeral means short lived. It is used because life of a client is generally short.
- The server process should also identify itself with a port number but this port number can not be chosen randomly.
- The Internet uses universal port numbers for servers and these numbers are called as **well known port numbers.**
- Every client process knows the well known port numbers of the pre identified server process.
- For example, a Day time client process can use an ephemeral (temporary) port number 43000 for identifying itself, the Day time server process must use the well known (permanent) port number 15.
- This is illustrated in Fig. 11.19.2.



(G-595) **Fig. 11.19.2 : Concept of port numbers**

What is difference between IP Addresses and Port Numbers ?

- The IP addresses and port numbers have altogether different roles in selecting the final destination of data.
- The destination IP address is used for defining a particular host among the millions of hosts in the world.
- After a particular host is selected, the port number is used for identifying one of the processes on this selected host.

IANA Ranges :

- The port numbers are divided into three ranges by IANA (International Assigned Number Authority).
- The ranges are as follows :
  1. Well known ports.
  2. Registered ports.
  3. Dynamic or private ports.

1. **Well known ports :** The ports from 0 to 1023 are known as well known ports. They are assigned as well as controlled by IANA.
2. **Registered ports :** The ports from 1024 to 49,151 are neither controlled nor assigned by IANA. We can only register them with IANA to avoid duplication.
3. **Dynamic or private ports :** The ports from 49,152 to 63,535 are known as dynamic ports and they are neither controlled nor registered. They can be used by any process. Dynamic ports are also known as private ports and dynamic port are called as ephemeral ports.

Socket Address :

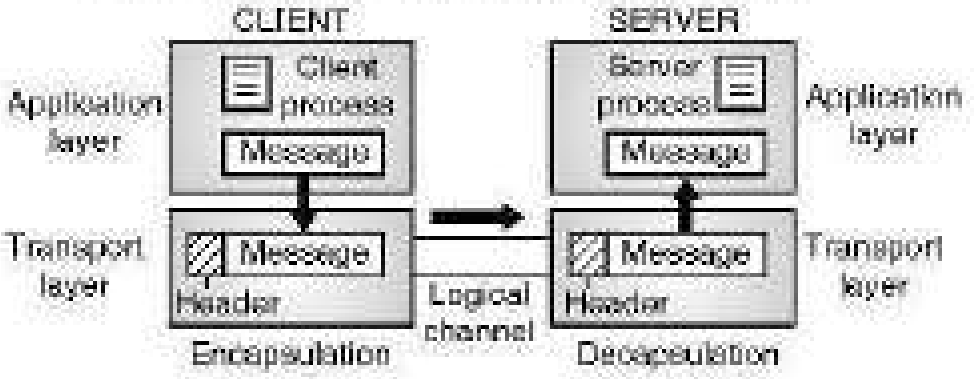
- Process to process delivery (transport layer communication) has to use two addresses, one is IP address and the other is port number at each end to make a connection.
- Hence a process to process delivery uses the combination of these two.
- The combination of IP address and port number is as shown in Fig. 11.19.3 and it is known as the socket address.

(c-154s) **Fig. 11.19.3 : Socket address**

- The client socket address defines the client process uniquely whereas the server socket address defines the server process uniquely.
- A transport layer protocol requires the client socket address as well as the server socket address. These two addresses contain four pieces.
- These four pieces go into the IP header and the transport layer protocol header.
- The IP header contains the IP addresses while the UDP and TCP headers contain the port numbers.
- If we want to use the transport layer services in the Internet, then we have to use a pair of socket addresses namely the clients socket address and the server's socket address.

11.19.3 Encapsulation and Decapsulation :

- The transport layer carries out the **Encapsulation** of the message at the sending end and then **Decapsulation** at the receiving end when two computers communicate. This process has been illustrated in Fig. 11.19.4.



(c-201z) **Fig. 11.19.4 : Encapsulation and decapsulation**

Encapsulation :

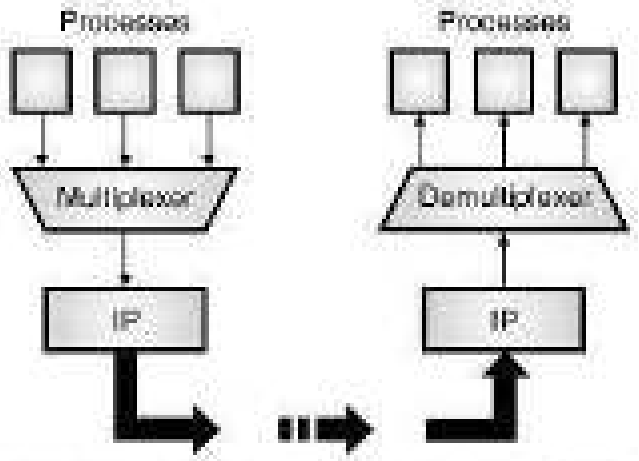
- At the sending end the process that has a message to send, will pass it to the transport layer alongwith a pair of socket addresses and some additional information.
- The transport layer adds its own header to this data. This packet at the transport layer in the Internet is known by different names such as **user datagram, segment or packet.**

Decapsulation :

- When the segment or datagram arrives at the receiving end, the header is isolated and destroyed, and the message is delivered to the process running at the application layer as shown in Fig. 11.19.4.
- The socket address of the sender process is then handed over to the destination process.

11.19.4 Multiplexing and Demultiplexing :

- The addressing mechanism allows multiplexing and demultiplexing taking place at the transport layer as shown in Fig. 11.19.5.



(G-597) **Fig. 11.19.5 : Multiplexing and demultiplexing**

Multiplexing :

- At the sending end, there are several processes that are interested in sending packets.
- But there is only one transport layer protocol (UDP or TCP). Thus it is a many processes-one transport layer protocol situation.
- Such a many-to-one relationship requires multiplexing.
- The protocol first accepts messages from different processes.
- These messages are separated from each other by their port numbers. Each process has a unique port number assigned to it.
- Then the transport layer adds header and passes the packet to the network layer as shown in Fig. 11.19.5.

Demultiplexing :

- At the receiving end, the relationship is one as to many. So we need a demultiplexer.
- First the transport layer receives datagrams from the network layer.
- The transport layer then checks for errors and drops the header to obtain the messages and delivers them to appropriate process based on the port number.

11.19.5 Flow Control :

- If the packets produced by the sender are at a rate X and the receiver is receiving them at a rate Y, then for X = Y, there will be a perfect balance observed in the system.
- But if X is higher than Y (source is producing packets at a rate which is higher than the rate at which the receiver is accepting them), then the receiver can be overwhelmed and has to **discard** some packets.
- And if X is less than Y (i.e. source is producing packets at slower rate than the rate of acceptance at the receiver) then system becomes **less efficient.**
- Flow control is related to the situation in which X > Y because it is very important to prevent data loss (due to discarding of packets) at the receiver site.

Pushing and pulling for flow control :

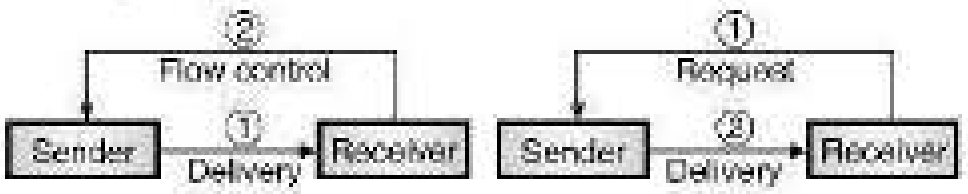
- There are two different ways of delivering the packets produced by the sender to the receiver. They are pushing or pulling.

1. **Pushing :**

   If the sender is sending the packets soon as they are produced, without receiving any prior request from the receiver then this type of deliver is called as **pushing.** Fig. 11.19.6(a) illustrates this concept.

2. **Pulling :**

   If the sender sends the produced packets only when they are requested by the receiver then the delivery is called as **pulling.** Fig. 11.19.6(b) illustrates the principle of pulling.



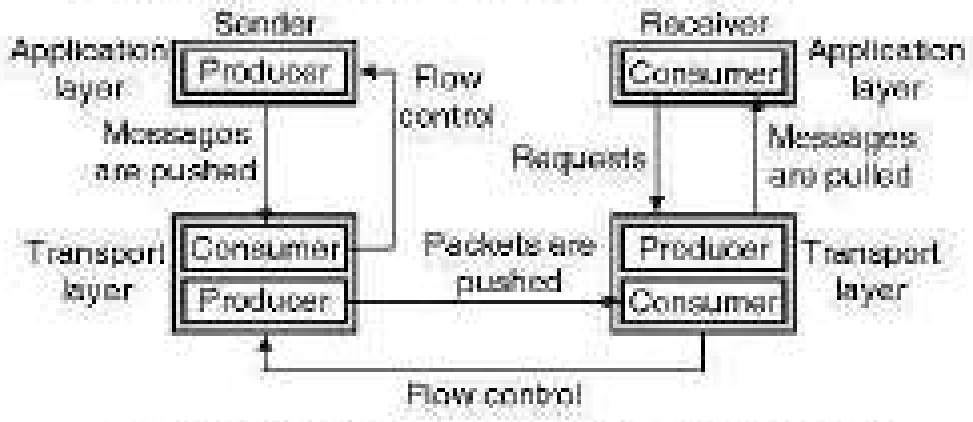
(a) Concept of pushing **(b) Concept of pulling**

(G-2013) **Fig. 11.19.6**

- In case of **pushing** type delivery, if the packets are being sent at a higher rate than that of receiving, then the receiver will be **overwhelmed,** and some received packets will have to be discarded.
- In order to avoid discarding of packets, the **flow control** will have to be exercised.
- For this the receiver has to warn the sender to stop the delivery when it is overwhelmed and it has to inform the sender again to start delivery when it (receiver) is ready to receive the packets.
- In case of **pulling type delivery,** the receiver is actually pulling the packets from the sender. It requests for the packets when it is ready.
- Therefore the flow control is not required in this case.

11.19.6 Flow Control at Transport Layer :

- The concept of flow control at transport layer has been illustrated in Fig. 11.19.7. It shows the communication taking place between a sender and a receiver.



(G-2014) **Fig. 11.19.7 : Flow control at transport layer**

- As shown in Fig. 11.19.7, there are four entities involved in this communication. They are as follows :
  1. Sender process.
  2. Sender transport layer.
  3. Receiver process.
  4. Receiver transport layer.
- We will discuss the flow control by considering the sending and receiving ends separately.

Sending end :

- The first entity on the sending end is the **sender process,** at the application layer.
- It works only as a **producer** which produces chunk of messages and pushes them to the transport layer on the sending end, as shown in Fig. 11.19.7.
- The second entity on the sending end is the **sender transport layer.** It has two different roles to play.
- First it acts as a **customer** and consumes all the messages produced and pushed by the producer.
- Then it encapsulates those messages into packets and pushes them to the receiver transport layer as shown in Fig. 11.19.7. Here it acts as a **producer.**

Receiving end :

- The first entity on the receiving end is the **receiver transport layer.** It also has two different roles to play.
- It acts as a **consumer** for the packets pushed by the senders transport layer and it also acts as the **producer.**
- It has decapsulate the messages and deliver them to the application layer as shown in Fig. 11.19.7.
- However the delivery of decapsulated messages to the application layer is a **pulling type delivery.**
- That means the transport layer waits till the application layer process requests for the decapsulated messages.

Flow control :

- As shown in Fig. 11.19.7, the flow control is needed for atleast two cases. First is from transport layer of sender to the application layer of sender.
- And secondly form the transport layer of receiver to the transport layer of sender.

Buffers :

- It is possible to implement the flow control in many different ways.
- One of the ways of implementation is to use two **buffers** one each at the sending and receiving transport layers.
- A **buffer** is nothing but a set of memory locations which can temporarily hold (store) packets.
- It is possible to exercise flow control communication by sending signals from the consumer to producer.
- The **flow control** at the **sending end** takes place as follows : As soon as the buffer at the transport layer becomes full it sends the stop message to its application layer in order to stop the chunk of messages that are being pushed into the buffer.
- The second flow control takes place at the receiver transport layer as follows : As soon as the buffer at receiver transport layer becomes full, it will inform the sender transport layer to stop pushing the packets.
- Whenever the buffer becomes partially empty, it again informs the sender transport layer to start sending the packets again.

11.19.7 Error Control :

Need of error control :

- In the Internet, the network layer protocol IP has the responsibility to carry the packets from the transport layer at the sending end to the transport layer at the receiving end.
- But IP is unreliable. Therefore transport layer should be made reliable, in order to ensure reliability at the application layer.

- We can make the transport layer reliable by adding the **error control service** to the transport layer.

Duties of error control mechanism :

- Following are the important responsibilities of the error control mechanism introduced at the transport layer :
  1. To find and discard the corrupted packets.
  2. To keep the track of lost and discarded packets and to resend them.
  3. Identify the duplicate packets and discard them.
  4. To buffer out of order packets until the missing packets arrive.
- In the error control process, only the sending and receiving transport layers are involved.
- That means it is assumed that the chunk of messages exchanged between the application layers and transport layers are error free.
- The concept of error control at the transport layer level is demonstrated in Fig. 11.19.8.

(G-2015) **Fig. 11.19.8 : Concept of error control at the transport layer**

- The receiving transport layer manages the error control by communicating with the sending transport layer about the problem.

Sequence numbers :

- In order to exercise the error control at the transport layer following two requirements should be satisfied :
  1. The sending transport layer should know about the packet which is to be resent.
  2. The receiving transport layer should know about the packets which are duplicate or the ones that have arrived out of order.
- The requirements can be satisfied only if each packet has a unique **sequence number.**
- If a packet is either corrupted or lost the receiving transport layer will somehow inform the sending transport layer about the sequence number of those packets and request it to resend those packets.
- Due to the unique sequence number assigned to each packet it is possible for the receiving transport layer to identify the duplicate packets received.
- The out of order packets can also be recognized by observing gaps in the sequence numbers of the received packets.
- Packet numbers are given sequentially. But the length of the sequence number cannot be too long because the sequence number is to be included in the header of the packets.
- If the header of a packet allows 'm' bits per sequence number, then the range of sequence number will be from 0 to 2^m-1. For example if m = 3 then the range of sequence numbers will be from 0 to 7.
- Thus sequence numbers are modulo 2^m.

Acknowledgement :

- The receiver side can send an acknowledgement (ACK) signal corresponding to each packet or each group of packets which arrived safe and sound.
- The question is what happens if a received packet is corrupted ? The answer is that the receiver simply discards the corrupted packet and does not send any ACK signal for it.
- The sender can detect a lost packet with the help of a timer. A timer is started at the sending end as soon as a packet is sent.
- If the ACK does not arrive before the expiry of the timer, then the sender treats the packet to be either lost or corrupted and resends it.
- The receiver silently discards the duplicate packets. It will either discard the out of order packets or stored until the missing packet is received.
- Note that every discarded packet is treated as a lost packet by the sender.

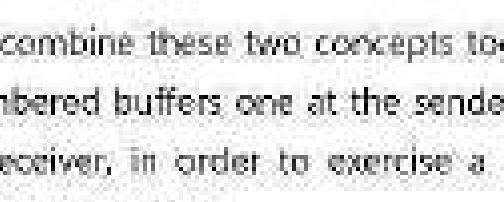
11.19.8 Combination of Flow and Error Control :

- Till now we have discussed the following important concepts :
  1. We need to use buffers at the sending and receiving ends for exercising the flow control.
  2. Also we have to use the sequence numbers and acknowledgements for exercising the error control.

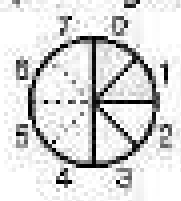
- We can combine these two concepts together by using two numbered buffers one at the sender and the other at the receiver, in order to exercise a combination of flow and error control.
- At the sending end, when a packet, is prepared to be sent, the number of the next free location (x) in the buffer is used as the sequence number of that packet.
- As soon as the packet is sent, its copy is stored at location (x) in the sending end buffer and the sender waits for the acknowledgement from the receiver.
- On reception of the acknowledgement of the sent packet, the copy of that packet is purged to make the memory location (x) free again.
- At the receiver, when a packet having a sequence number "y" arrives, it is stored at the memory location "y" in the receiver buffer until the receiver application layer is ready to receive it.
- The receiver will send the ACK message back to sender to inform it that packet "y" has arrived.

Sliding window :

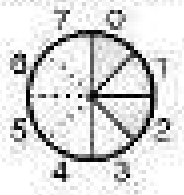
- As the sequence numbers are modulo 2^m, we can use a circle as shown in Fig. 11.19.9 to represent the sequence number from 0 to $2^m - 1$.



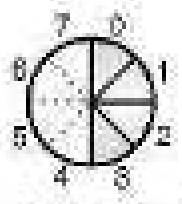
(a) Sliding window in the circular format



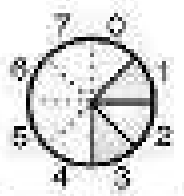
(b) Two packets have been sent



(c) Three packets have been sent



(d) Four packets have been sent. The window is full



(e) Packet 0 has been acknowledged and the window slides

(S-2017) **Fig. 11.19.9**

- We can represent the buffer as a set of slices, called as the **sliding window** which will occupy a part of the circle at any time.
- In Fig. 11.19.9, we have assumed that m = 3. Therefore $2^m - 1 = 7$ and the sequence numbers are from 0 to 7. Hence the number of memory locations in a buffer will also be 8 i.e. 0 to 7.
- The sliding windows will correspond to the sender as well as receiver.
- On the sending side, when a packet is sent we will mark the corresponding slice.
- Therefore when marking of all the slices is done, it means the **sending buffer is full,** and it cannot accept any further messages from the application layer as shown in Fig. 11.19.9(d).
- When the acknowledgement for segment "0" arrives at the sending end, the corresponding segment (segment 0) is unmarked and window slides ahead by one slice as shown in Fig. 11.19.9(e). The size of the **sending window** is 4.
- Note that the sliding window is just an abstraction. In actual practice, computer variables are used to hold the sequence number of the next packet to be sent and the last packet sent.

Sliding window in the linear format :

- This is another way to diagrammatically represent a sliding window. It is as shown in Fig. 11.19.10.
- The principle of this type of sliding window is same as that of the circular representation. The linear format is the most preferred format. It needs less space on paper.
- Fig. 11.19.10(a), (b), (c) and (d) are the sliding windows presented in the linear format corresponding to Figs. 11.19.9(b), (c), (d) and (e) respectively in the circular presentation.

(a) Two packets have been sent

(b) Three packets have been sent

(c) Four packets have been sent. The window is full.

(d) Packet 0 has been acknowledged and the window slides

(S-2015)**Fig. 11.19.10 : Sliding windows presented in the linear format**

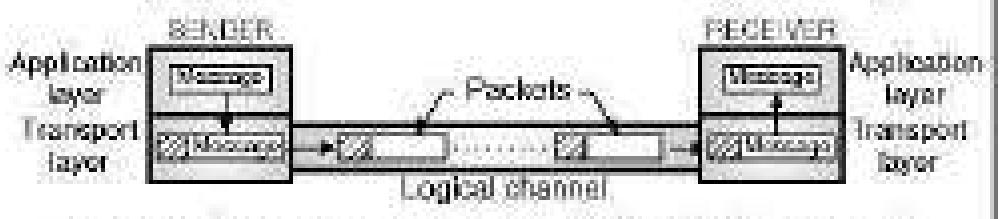
11.20 Transport Layer Protocols :

- We have discussed a few transport layer services in the previous section. By combining a set of these services as per requirement, we can create a transport layer protocol.

- It is important to understand the behavior of these general protocols, before we discuss the transport layer protocols such as UDP and TCP.
- In this section we will discuss the following protocols :
  1. Simple protocol.
  2. Stop and wait protocol.
  3. Go back N (GBN) protocol.
  4. Selective repeat protocol.
  5. Bidirectional protocol. (Piggybacking).
- Initially we will discuss all these protocols as **simplex** i.e. **unidirectional** protocols and then we will see how to make them the **full duplex** i.e. **bidirectional** protocols.

11.20.1 Simplex Protocol :

- This is the simplest type of connectionless protocol which has the following characteristics :
  1. No flow control.
  2. No error control.
  3. The receiver does not get overwhelmed.
- Because the receiver does not get overwhelmed due to the incoming packets even at very high rate, the receiver can handle any packet immediately as soon as it is received.
- The principle of operation (or protocol layout) of the simple protocol has been illustrated in Fig. 11.20.1(a).



(G-2179) **Fig. 11.20.1(a) : Layout of the simple protocol**

Operation :

At the sender :

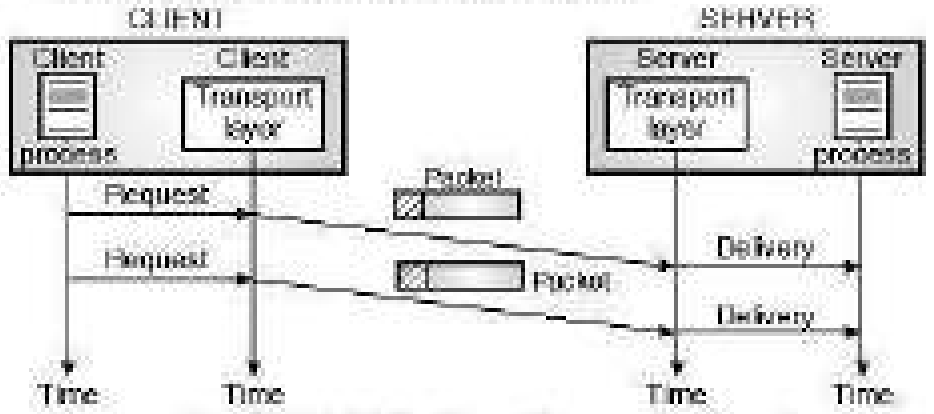
- The application layer at the sender, sends its message to the transport layer.
- The sender transport layer receives the message and makes a packet out of it.
- This packet is then sent over the logical channel between the transport layers on the two ends.

At the receiver :

- The network layer at the receiver (not shown in Fig. 11.20.1(a)) delivers the received packet to the transport layer.
- The receiver transport layer extracts the message from the packet (decapsulation) and sends the message to the application layer.

Flow Diagram :

- The communication between the sender and receiver using the simple protocol has been shown in Fig. 11.20.1(b).
- The sender keeps sending the packets, without taking the receiver into consideration at all.

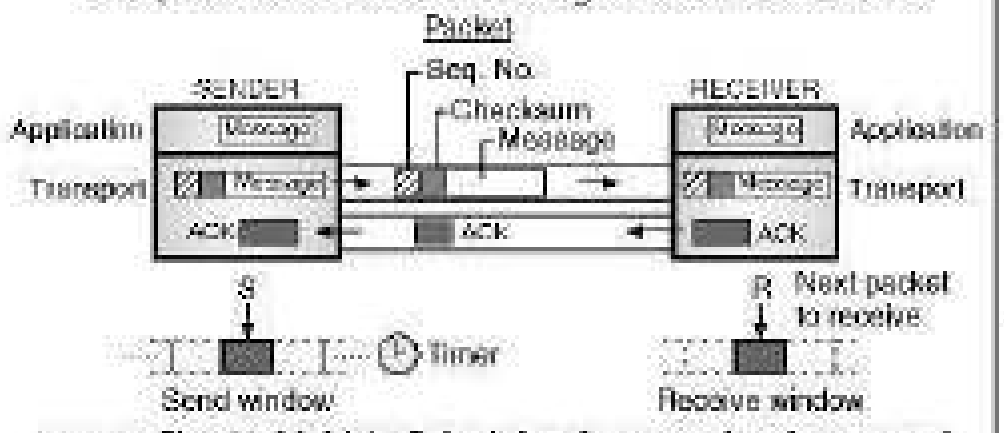


(G-2181) **Fig. 11.20.1(b) : Flow diagram for the simple protocol**

11.20.2 Stop and Wait Protocol :

- The second transport layer protocol that we will discuss now is a **connection oriented** protocol called as **stop and wait protocol.**
- The operation of this protocol are as follows :
  1. It is a connection oriented protocol.
  2. It provides both flow and error control.
  3. Sender sends one packet at a time and waits for its acknowledgement from receiver before sending the next packet.
  4. A checksum is added to each data packet so as to detect a corrupted packet.
  5. At the receiver, the checksum in each packet is checked. If found incorrect, the receiver considers it as the corrupted packet and discards it silently. Such a packet is not acknowledged by the receiver.
  6. If the sender does not receive an acknowledgement for a packet within a predecided time, it understands that the packet is either corrupted or lost.
  7. The sender starts a timer everytime it sends out a packet. If it receives the acknowledgement for the packet before the expiry of the timer, it stops the timer, and sends the next packet. But if the timer expires before the arrival of acknowledgement, the sender resends the previous packet which was either corrupted or lost.

– Fig. 11.20.2(a) shows the principle of the stop and wait protocol. Note that at any given time there can be only one packet and one acknowledgement in the channel.



(G-2182) **Fig. 11.20.2(a) : Principle of stop and wait protocol**

Sequence number :

– In this protocol, sequence numbers and acknowledgement numbers are used for preventing duplicate packets.

– As shown in Fig. 11.20.2(b), an additional field is created in the packet header of each packet to hold its sequence number.

(G-2183) **Fig. 11.20.2(b) : Packet**

– A very important consideration about the sequence number is the range of sequence numbers.

– In order to provide an unambiguous communication with the minimum packet size, we look for the smallest range of sequence numbers.

– Let x be the sequence number of a packet, then the next sequence number should be (x + 1). There is no need for (x + 2). We can show it using the following discussion.

– Suppose that a packet with the sequence number x has been sent by the sender. Then the following three things can possibly happen.

1. **Everything is normal :**

– The first possibility is that the packet reaches its destination safe and sound without getting corrupted or lost. The receiver sends the acknowledgement for it.

– The acknowledgement reaches the sender safe and sound.

– The sender sends the next packet having a sequence number of (x + 1).

2. **Packet corrupted or lost :**

– The second possibility is that the sent packet either gets corrupted or gets lost and does not reach the receiving end at all.

– The receiver discards the corrupted packet silently. In either case (corrupted or lost packet), the acknowledgement is not sent back.

– The sender waits for the timer to expire and resends the packet numbered x. The receiver sends back the acknowledgement for it.

3. **The acknowledgement is corrupted or lost :**

– The packet (numbered x) arrives safe and sound at the receiving end for which it sends an acknowledgement back to the sender.

– However the acknowledgement either get corrupted or gets lost on its way back.

– Therefore the sender resends the packet (numbered x) again after the expiry of the timer.

– Thus packet x has a duplicate now. The receiver will understand this fact because it was expecting packet numbered (x + 1) to arrive but instead it received the packet numbered x again.

Conclusions :

– From the above discussion we can conclude that sequence numbers x and x + 1 are required so that the receiver can distinguish between cases 1 and 3 discussed above.

– But it is not necessary to number the packet as (x + 2).

– In case 1, we can number the packet as x again because both the packets (x and x + 1) are acknowledged by the receiver and neither the sender nor the receiver has any ambiguity about it.

– Finally in the case 2 and 3, the new packet is (x + 1) and not (x + 2).

– Therefore we conclude that only two sequence numbers x and x + 1 are needed and x +2 is not needed.

– So let x = 0 then (x + 1) = 1.

– Thus there will be only two sequence numbers 0 and 1 and the packet sequence would be 0, 1, 0, 1, 0... and so on. Due to the presence of only two distinct sequence numbers, this is called as modulo-2 arithmetic.

Acknowledgement numbers :

- For both types of packets i.e. data packets and acknowledgements, the same sequence numbers should be suitable.
- For this to happen successfully the following convention is used.
- The acknowledgement number always indicates the sequence number of the **next packet** that the receiver is expecting to receive.
- For example, the packet with a sequence number 0 arrives at the receiver safe and sound.
- Then the corresponding ACK sent by the receiver will have a number 1 on it which means that the next expected packet to be received is packet 1.
- Similarly if packet 1 arrives safe and sound then ACK with acknowledgement 0 is sent back which means that packet – 0 is the next expected packet at the receiver.
- The **control variable** at the sender is called as the **sender (s)** and it points to the only slot present in the send window as shown in Fig. 11.20.2(a).
- Similarly the **control variable** at the receiving end called as the **Receiver (R)** and it points to the only slot present in the receive window as shown in Fig. 11.20.2(a).

Efficiency of stop and wait protocol :

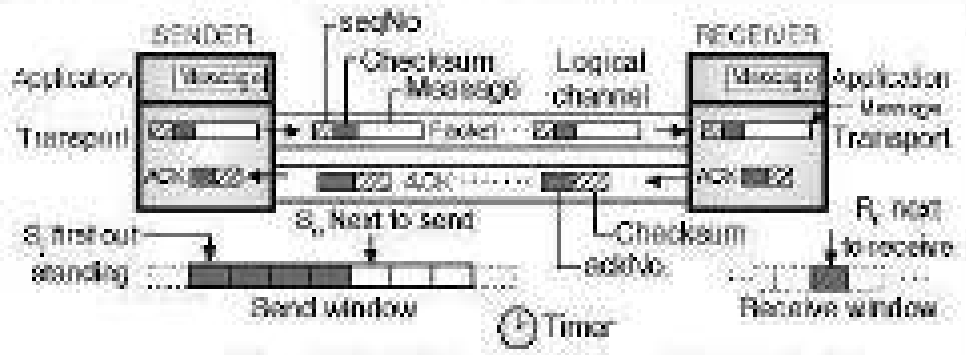
- The efficiency of the stop and wait protocol is very very low. This is because it sends a packet and simply waits for its ACK before sending the next packet.
- This is a gross underutilization of the communication channel especially if the channel is **thick and long.**
- A channel is thick if it has a large bandwidth and it is **long** if it has a long round trip time.
- The product of these two parameters is called as **bandwidth delay product.**
- A channel is equivalent to a pipe. If it is underutilized, then it will be called inefficient.
- The number of bits a sender can transmit through the channel can be measured from the value of bandwidth delay product.
- On all these accounts the stop and wait protocol proves to be extremely inefficient.

Pipelining :

- In networking and even other areas, a task is started before the ending of previous task. This is known as **pipelining.**
- In the stop and wait protocol, the senders sends a packet and waits for its acknowledgement before sending the next packet.
- This shows that there is no pipelining in the stop and wait protocol.
- But in the other protocols that we are going to discuss after the concept of pipelining will be used.
- Therefore it is possible for the sender to send several packets before it receives only acknowledgements for the previously sent packets.
- The process of pipelining improves the efficiency of the protocol.

11.20.3 Go Back-N Protocol (GBN) :

- The efficiency of transmission can be improved by transmitting multiple packets while the sender is waiting for acknowledgment.
- That means we should allow more than one outstanding packets even when the sender is waiting for acknowledgement because this will keep the channel busy.
- A protocol which can achieve this goal is our next protocol called Go Back-N (GBN) protocol.
- The most important part in the operation of GBN protocol is that we can send several packets before receiving acknowledgement. But the receiver can buffer only one packet.
- A copy of every sent packet is kept by the sender until it receives the acknowledgement of that packet.
- Fig. 11.20.3(a) shows the outline of GBN protocol which explains its principle of operation. Note the simultaneous presence of multiple packets and multiple acknowledgements in the channel at any given time.



(G-2186) **Fig. 11.20.3(a) : Principle of Go Back-N (GBN) protocol**

Sequence numbers :

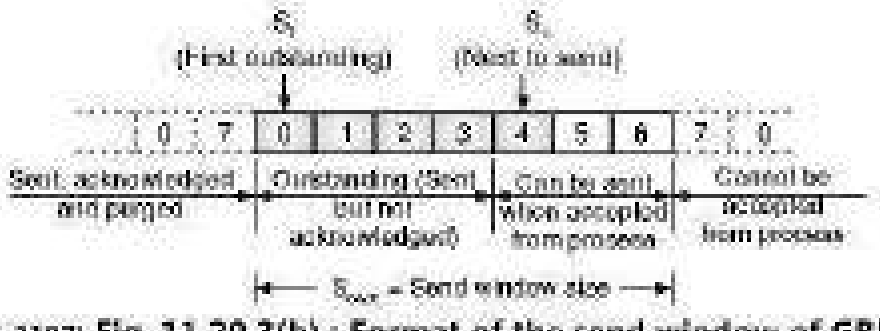
- In GBN protocol, the sequence numbers are modulo 2^m, where **m** denotes the size of sequence number field in bits.

Acknowledge numbers :

- In the GBN protocol, the acknowledgement number is cumulative and it carries the sequence number of the next packet that is expected to be received at the receiver.
- If the ackNo = 6, its an indication that the receiver has received all the packets having sequence number upto 5 safe and sound.
- Hence the receiver is expecting the packet with seq. No = 6 to arrive next.

Send window :

- We can define the send window as an imaginary box, which covers the sequence numbers of the data packets that can be sent.
- The **maximum size** of the send window is $(2^m - 1)$ for the reasons discussed later on in the chapter.
- In each send window position (it can slide), some sequence numbers indicate the packets that have been already sent whereas the other sequence numbers indicate the data packet that are to be sent.
- In this chapter we assume that the send window size is fixed and has been set to its maximum possible value. But in some protocols the send window size is variable.
- The structure of a send window for the GBN protocol with m = 3 has been shown in Fig. 11.20.3(b). Note that the window size = $2^m - 1 = 2^3 - 1 = 7$.



(G-2187) **Fig. 11.20.3(b) : Format of the send window of GBN**

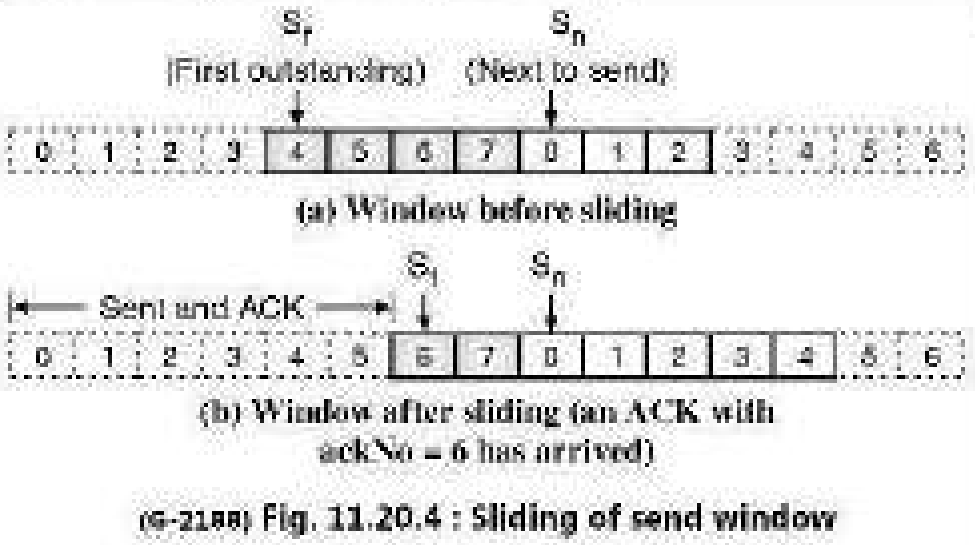
- At any given time, the send window divides the possible sequence numbers into four regions.
- As shown in Fig. 11.20.3(b), the first region corresponds to the portion to the left of the send window.
- It consists of the sequence numbers which belong to the packet which are already acknowledged.
- The sender does not keep any copy of these packets.
- The second region which is shaded in Fig. 11.20.3(b) contains the sequence numbers belonging to the packets that are already sent but not acknowledged by the receiver.
- That means the exact status of these packets is not known.
- These packets are called as **outstanding packets.**
- The third range, which is not shaded in Fig. 11.20.3(b), contains the sequence numbers belonging to the packets which the sender can send.
- But the corresponding data is yet to be received from the application layer.
- And finally the fourth range, which is at the right of the send window in Fig. 11.20.3(b), consists of the sequence numbers that cannot be used by the sender until the send window slides to the right hand side.

Size and location of send window :

- There are three variables that define the size and location of the send window at any given time. They are :
  1. S_f : Send window, the first outstanding packet.
  2. S_n : Send window ; the next packet to be sent.
  3. S_{size} : Send window, size.
- The sequence number of the first (oldest) outstanding packet is defined by the variable S_f.
- The sequence number, that will be assigned to the next packet to be sent is defined by the variable S_n.
- And finally the size of the send window which is fixed in GBN protocol is defined by the variable S_{size}.

Sliding of send window :

- A send window will slide right on the arrival of acknowledgements.
- Fig. 11.20.4 shows the send window before sliding and after the arrival of an acknowledgement with ackNo = 6.



(G-2188) **Fig. 11.20.4 : Sliding of send window**

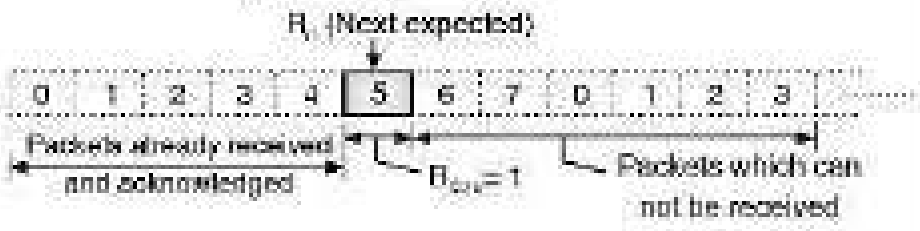
- This means that all packets upto seq.No = 5 have reached safe and sound and the receiver is expecting the packet with seq.No = 6 to arrive.

Conclusion :

- From all this discussion we conclude that the send window will slide by one or more slots when the sender receives an errorfree ACK whose ackNo is greater than or equal to S_f and less than S_n.

Receive window :

- The receive window has two tasks : First it has to ensure that correct data packets are received and second is to make sure that correct acknowledgements are sent.
- The size of receive window in the GBN protocol is always 1. Therefore, the receiver is always expecting a specific packet to arrive.
- That means the receiver will discard any packet which arrives out of order and the sender has to resend the discarded packet.
- The receive window for the GBN protocol is shown in Fig. 11.20.5. It has only one variable R_n, i.e. receive window, next packet expected.



(G-2189) **Fig. 11.20.5 : Structure of receive window of GBN**

- The sequence numbers to the left of the receive window correspond to the already received and acknowledged packets.
- The sequence numbers to the right of receive window correspond to the packets which cannot be received.
- The receiver discards any packet that belongs to these two ranges. It will only accept that packet whose sequence number exactly matches with the value of R_n.
- Like the sliding window, the receive window also slides but only by one slot at a time.
- On reception of a correct packet, the receive window slides to $R_n = (R_{n-1}) \text{ modulo } 2^m$.
- If a corrupted packet is received, the receive window does not slide at all.

Timers :

- Ideally there should be one timer per packet, which is sent. In GBN protocol only one timer is used.
- The reason for this is that the timer for the first outgoing packet will always expire first. If so, then all the outstanding packets will be resent by the sender.

Resending the packets :

- As stated earlier, on the expiry of the only timer (also called as time out), all the outstanding packets will be resent.
- As an example, let us assume that the sender has already sent the packet having seq.No 6 ($S_n = 7$) but the time out takes place (that means the only timer in GBN has expired).
- If $S_f = 3$, then it is an indication that the packets 3, 4, 5 and 6 are all outstanding packets i.e. they are sent but not acknowledged.
- Hence, as soon as the timer expires, the sender will go back and resend all the outstanding packets i.e. packets 3, 4, 5 and 6.
- This is the reason behind the name of this protocol which Go Back N.
- The sender goes back by N slots and resends all the packets from there as soon as the timer expires.

Send window size :

- Now we are going to discuss, why in GBN protocol the size of send window should be less than 2^m.
- Let m = 2. Therefore the size of the send window will be $2^{m-1} = 3$. With this send window size if all the acknowledgements are lost and the timer expires, then the sender resends all packets.
- As the receiver is expecting packet 3 and not 0, it will successfully identify the resent packet 0 as the duplicate and discard it.

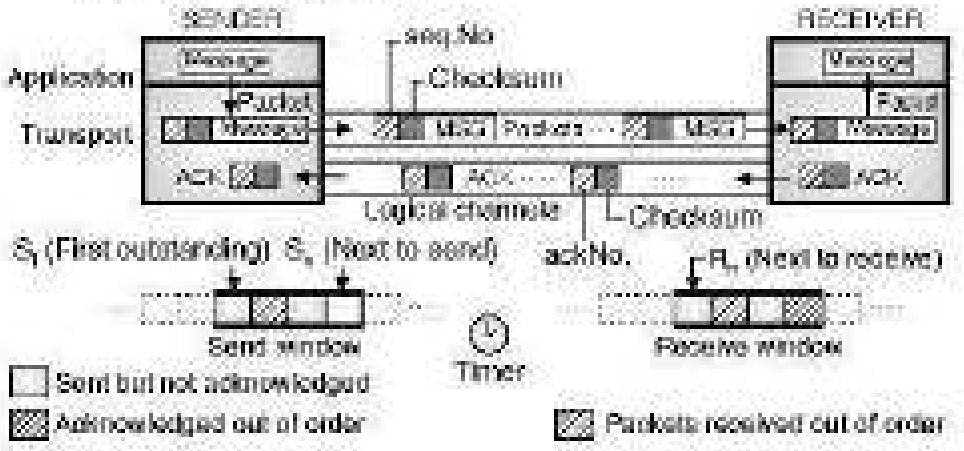
- But if the send window size is $2^m = 4$, and if all the acknowledgement are lost and the timer expires, then the sender will retransmit packet 0.
- But this time, the receiver also is expecting packet 0 to arrive (next cycle). Hence it won't treat the resent packet 0 as the duplicate packet and won't discard it.
- In fact the duplicate packet 0 is accepted as the legitimate packet 0 of the next cycle. This is an error.
- From this example we conclude that the size of send window in GBN protocol should be **less than 2^m**.

Comparison of GBN with stop and wait :

- The GBN and stop and wait protocols are somewhat similar to each other.
- The stop and wait protocol is actually a GBN protocol with only two sequence numbers (0 and 1) and send window size of 1.
- In stop and wait protocol, the modulo 2 arithmetic is used whereas in GBN protocol, modulo 2^m arithmetic is said to have been used.
- Thus stop and wait protocol is a GBN protocol with m = 1.

11.20.4 Selective Repeat Protocol :

- The process at the receiving end is simplified in the GBN protocol to a great extent.
- This is because R_n is the only variable which is to be tracked by the receiver ant the out of order received packets need not be buffered. They are to be simply discarded.
- But the problem with this protocol is its **inefficiency** if the underlying protocol tends to loose a lot of packets.
- This is because everytime with the loss of a packet the sender has to send all the outstanding packets.
- It is possible that some of these packets may have been received without any error but out of order.
- If the network congestion is already existing, then it will become worse due to these frequently resent packets.
- The worsened network congestion will result in the loss of more packets which leads to retransmission on of more packets and so on.
- This is called as an **avalanche effect** which may eventually cause total collapse of the network.
- In order to overcome these problems of the GBN protocol, a new protocol has been deviced which is called as the **Selective Repeat Protocol.**
- This new protocol, as the name suggests, resends only **selected packets**, that are actually corrupted or lost. It does not resend all the outstanding packets like the GBN protocol.
- This will reduce the number of resent packets and therefore reduces the possibility of network congestion.
- The principle of selective repeat protocol has been illustrated in Fig. 11.20.6.



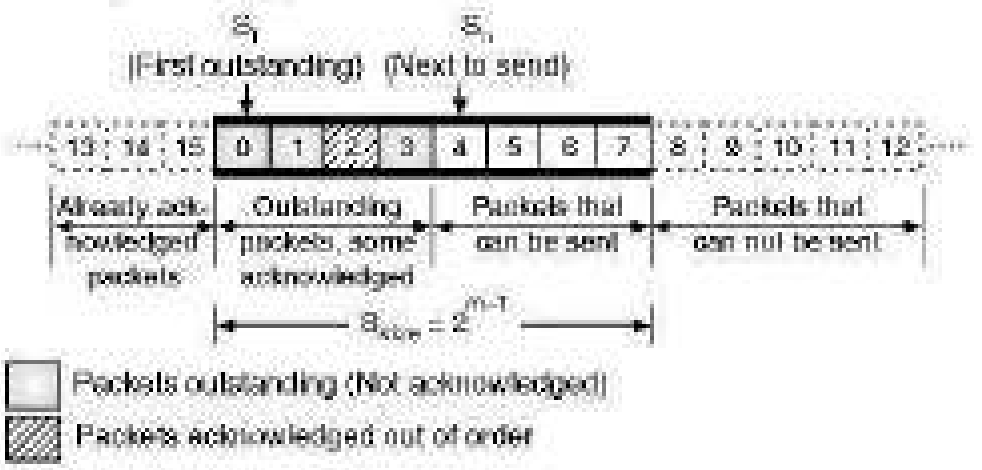
(G-2190) **Fig. 11.20.6 : Outline of selective repeat protocol**

Windows :

- In the selective request protocol also there are two windows used : a send window and a receive window.
- However these windows are different from those in the GBN protocol. In this protocol the maximum size of send window is (2^{m-1}).
- This size is much smaller than that in the GBN protocol. Also the size of receive window is same as that of the send window.

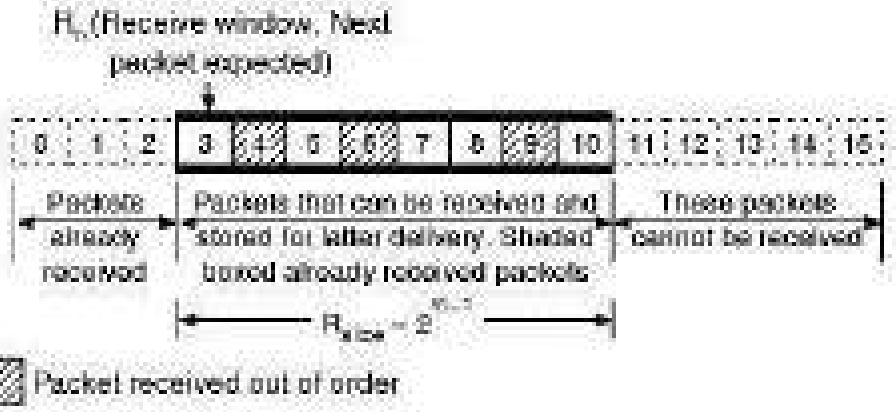
Send and receive windows :

- If m = 4, then the maximum size of the send window is $2^{m-1} = 2^3 = 8$ (It is 15 in the GBN protocol). Fig. 11.20.6(a) shows the structure of the send window.



(G-2191) **Fig. 11.20.6(a) : Send window for selective repeat protocol**

- Fig. 11.20.6(b) shows the structure of receive window in the selective repeat protocol. Note that it is totally different from that in the GBN protocol.



(G-2192) **Fig. 11.20.6(b) : Receive window for selective repeat protocol**

- The receive window here has the same size as that of the send window (Maximum size = 2^{m-1}).

Principle :

- In the selective repeat protocol, the packets equal to the size of the receive window are allowed to arrive out of order.
- The receiver is allowed to keep them until it has a set of consecutive packets which can be delivered to the application layer.
- As the send and receive windows are of the same size, all the packets in the send window can arrive out of order at the receiver and the receiver is allowed to store them until it can deliver them to the application layer.
- However the selective repeat is a reliable protocol. Therefore the receiver is not expected to deliver packets out of order to the application layer.
- The structure of the receiver window for selective repeat protocol is as shown in Fig. 11.20.6(b). It shows that there are packets received out of order.
- These packets have to wait for the earlier transmitted packets to arrive before all of them are finally delivered to the application layer.

Timer :

- Theoretically in SR protocol a timer is assigned to each outstanding packet in the send window. When a timer expires, only the corresponding packet is resent.
- This is totally different from the GBN protocol which has only one timer for a group of outstanding packets.
- But practically, almost all the transport layer protocols which are based on selective repeat principle use only one timer.

Acknowledgements :

- In GBN protocol, the ackNo is cumulative. It carries the number of the next expected packet to be received.
- It also confirms that all the previous packets have been received safe and sound.
- But in the SR protocol it is totally different. In SR the ackNo defines the sequence number of only one packet which is received safe and sound.
- It does not give any feedback about the other packets.

Window sizes :

- The maximum size of send and receive windows in the SR protocol is 2^{m-1} that means $2^m/2$ i.e. half of 2^m.
- If m = 2, all the acknowledgements are lost and if the time out takes place (i.e. timer expires) then sender retransmits packet 0.
- But the receiver window is expecting packet 2 and not packet 0.
- Hence the receiver will identify packet 0 as the duplicate packet and will discard it. (The sequence number 0 is not in the window).
- Now imagine that the window size is 3, all acknowledgements lost and the timer expires. Now the sender will resend packet 0.
- At this time the receiver is also expecting packet 0 of the next cycle to arrive (0 is the part of the window).
- Therefore the receiver cannot recognize that packet 0 is a duplicate packet. This is an error.
- That is why in S.R. protocol, the maximum size of the send and receive windows is 2^{m-1} or half of 2^m.

11.20.5 Bidirectional Protocols Piggybacking :

- Note that in all the protocols discussed so far the data packets flow in only one direction and acknowledgements travel in the opposite direction.
- Therefore all these four protocols are said to be **unidirectional protocols.**
- However in reality the data packets are travelling in both the directions, client to server and vice versa.
- The acknowledgements also are travelling in both the directions.
- Thus all the transport layer protocols in real life are bidirectional. We can improve the efficiency of these bidirectional protocols with a technique called **piggybacking.**

- In piggybacking, the data packet going from A to B can also carry acknowledgement for the data packet arrived from B to A.
- Similarly a data packet sent by B to A can carry acknowledgement for the data packet arrived from A to B.

11.20.6 The Internet Transport Protocols (TCP and UDP) :

- The Internet has two main protocols in the transport layer. One of them is connection oriented and the other one supports the connectionless service.
- TCP (Transmission Control Protocol) is a connection oriented protocol and UDP (User's Data Protocol) is the connectionless protocol.
- UDP is basically just IP with an additional short header.

Review Questions

Q. 1 Why is ARP request broadcast but ARP reply unicast ?

Q. 2 State the names of two network models.

Q. 3 Define the word protocol.

Q. 4 What is protocol layering ?

Q. 5 Explain the concept of logical connections.

Q. 6 Draw the layers of TCP/IP model.

Q. 7 Explain the layered architecture of TCP/IP model.

Q. 8 Explain in detail the physical layer in TCP/IP model.

Q. 9 Explain in detail the data link layer in TCP/IP model.

Q. 10 Explain in detail the network layer in TCP/IP model.

Q. 11 Explain in detail the transport layer in TCP/IP model.

Q. 12 Explain in detail the application layer in TCP/IP model.

Q. 13 Name any three network layer protocols.

Q. 14 Write a short note on : IP.

Q. 15 State various functions of network layer.

Q. 16 State the two most important transport layer protocols.

Q. 17 State various duties of transport layer.

Q. 18 State any four application layer protocols.

Q. 19 Explain the concept of encapsulation in TCP/IP.

Q. 20 Explain the concept of decapsulation in TCP/IP.

Q. 21 Write a note on following in TCP/IP model :

1. Addressing.
2. Multiplexing and demultiplexing.

Q. 22 Compare OSI and TCP/IP model.

11.21 MSBTE Questions and Answers :

Q. 1 List two DHCP protocols. **(W-15, S-17, 2 Marks)**

Ans. :

BOOTP and DHCP.

Q. 2 Explain and BOOTP. **(W-15, 2 Marks)**

Ans. :

Bootstrapping protocol :

What is Bootstrapping ?

- What happens when a computer first begins operation ? The process is known as Bootstrapping.
- When a user turns on the computer, the hardware first searches permanent storage device, usually disks, for a device that contains a special program called a **boot program** at location zero.
- When the boot program runs, it allows the storage device to read and load additional software (e.g. operation system) finally after loading all the software, the operating system allows a user to run his application program.

Bootstrap Protocol (BOOTP) :

- The RARP is reverse address resolution protocol. It uses a computer's hardware address to identify machine, It cannot be used on networks that dynamically assign hardware addresses.
- The RARP protocol has three drawbacks, first, RARP operates at low level. Second, it requires a packet exchange between client machine and a computer that answers its request and third, it uses a computer hardware address to identify machine.
- In order to overcome these drawbacks of RARP, researchers developed the BOOTstrap protocol (BOOTP). Later, the Dynamic Host Configuration Protocol (DHCP) was developed which is the successor to BOOTP.
- BOOTP is more efficient than RARP because a single BOOTP message specifies many items needed at the time of starting a computer.

- These items are : computer's IP address, the address of router and the address of a server.
- BOOTP also consists of a vendor-specific field in the reply in which a hardware vendors can send additional information.
- BOOTP messages are carried by the UDP and UDP messages are encapsulated in IP datagrams for delivery.
- Thus with BOOTP all responsibility for reliable communication is with the client. BOOTP uses UDP which is a connectionless unreliable protocol for message delivery.
- Messages can be delayed, lost, delivered out of order or duplicated. But IP does not provide a checksum for data therefore, the UDP datagram could arrive with some bits corrupted.
- To reduce the number of errors, BOOTP requires that UDP use checksums.
- It also specifies that requests and replies should be sent with the do not fragment bit set to accommodate those clients having a very small memory and therefore cannot reassemble datagrams.
- If datagrams are lost then, BOOTP uses the conventional technique of **timeout** and retransmission.

11.22 I-Scheme Questions and Answers :

Summer 2019 [Total Marks - 10]

Q. 1 Describe major functions of network layer in TCP/IP protocol suite. **(Section 11.5.3)** **(4 Marks)**

Q. 2 Describe the process of DHCP server configuration. **(6 Marks)**

Ans. :

Stepwise procedure for configuring the DHCP server :

- The stepwise procedure for setting up a DHCP server is as follows :

Step 1 : Modify the netmasks line of the / etc/ ns switch.conf file.

Step 2 : Start the DHCP wizard by issuing the following command line :

/usen/sadm/admin/bin/dhcpmgr

The wizard will ask you the following information select or enter the information as follows :

Data storage format :

Name service to store host records :

Length of lease :

Network address :

Subnet mask

Network type

Router :

Step 3 : Verify your configuration information and click finish.

Step 4 : When you are prompted to configure addresses for the server, click Yes.

The Add Address to network wizard is displayed.

Step 5 : Enter the following information :

Number of IP addresses.

Name of the mapping server.

Starting IP address.

Configuration macros to be used for configuring the client.

Lease type.

Step 6 : Verify your configuration information and click Finish.

Step 7 : In the Address Properties window enter the client id field = 01 followed by the MAC address of the RAID controller.

Step 8 : Modify the service options.

Step 9 : Verify that the BOOTP service is running.

Step 10 : After turning on the power, ping the address.

Winter 2019 [Total Marks - 16]

Q. 3 Draw and explain TCP/IP model. **(Sections 11.3 and 11.3.1)** **(4 Marks)**

Q. 4 Explain configuration of TCP/IP protocol in network. **(Sections 11.3, 11.3.1 and 11.3.2)** **(6 Marks)**

Q. 5 Explain the process of DHCP server configuration. **(Refer Q. 2)** **(6 Marks)**

Summer 2022 [Total Marks - 10]

Q. 6 Describe the process of DHCP server configuration. **(Section 11.16)** **(4 Marks)**

Q. 7 Explain ARP, subnetting and supernetting with example. **(Sections 11.2.2)** **(6 Marks)**

❑❑❑

Chapter 12

IP Addressing

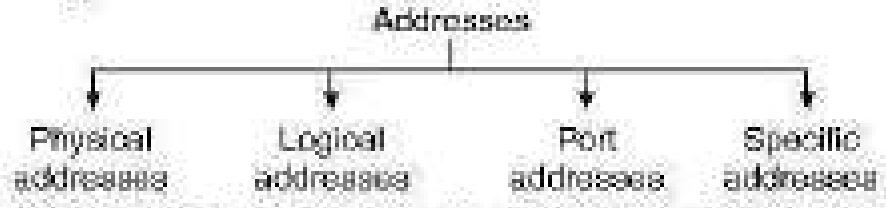
Syllabus

Introduction, Addressing mechanism in the Internet IP addressing - IP address classes, Classless IP addressing, Subnetting, Supernetting, Masking, IPv4 and IPv6, Comparison of OSI and TCP/IP network models.

Chapter Contents

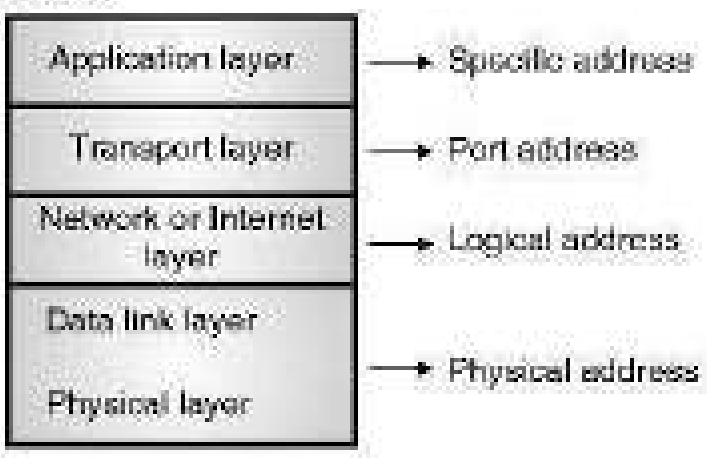
12.1 Addressing :

- When the computers wish to communicate with one another, they need to know the address of each other. Each computer has its own address.
- The addresses can be of different types such as physical addresses or logical address.
- In an internet employing the TCP/IP protocols, four levels of addresses are used by the computers :
  1. Physical address.
  2. Logical address (IP).
  3. Port address.
  4. Specific address.
- Fig. 12.1.1 shows the classification of addresses.



(G-75) **Fig. 12.1.1 : Classification of addresses in TCP/IP**

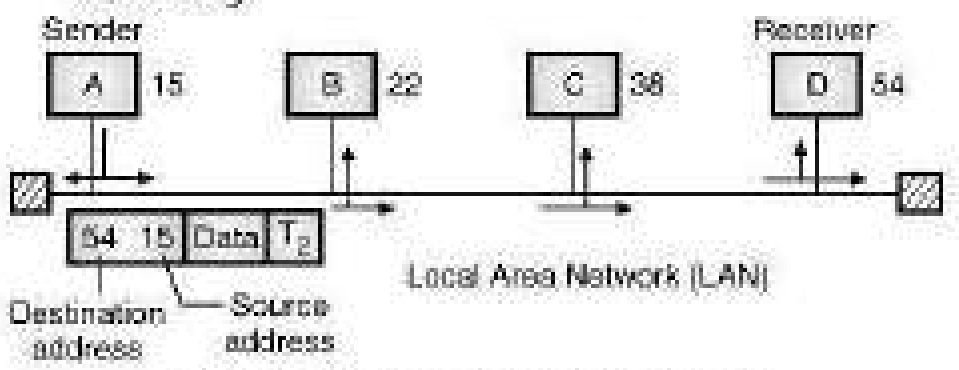
- Each of these addresses is associated with a specific layer of TCP/IP architecture as demonstrated in Fig. 12.1.2.



(G-76) **Fig. 12.1.2 : Relation between TCP/IP structure and addresses**

12.1.1 MAC Address (Physical Address) :

- The packets from source to destination hosts pass through physical networks.
- At the physical level the IP address is not useful but the hosts and routers are recognized by their MAC addresses.
- A MAC address is a local address. It is unique locally but it is not unique universally.
- The IP and MAC address are two different identifiers and both of them are needed, because a physical network can have two different protocols at the network layer at the same time.
- Similarly a packet may pass through different physical networks.
- So to deliver a packet to a host or a router, we require two levels of addressing namely IP addressing and MAC addressing.
- Most importantly we should be able to map the IP address into a corresponding MAC address.
- The size and format of the physical address varies depending on the nature of network.
- The Ethernet (LAN) uses a 48-bit (6-byte) physical address which is imprinted on the network interfacing card (NIC).
- Refer Fig. 12.1.3 which explains the concept of physical addressing.



(G-77) **Fig. 12.1.3 : Physical addresses**

- The sender computer with a physical address of 15 wants to communicate with the receiver computer with a physical address 54.
- The frame sent by the sender consists of the destination address, sender's address, encapsulated data and a trailer (T_2) that contains the error control bit.
- When this frame travels over the bus topology, every computer receives it and tries to match it with its own physical address.
- If the destination address in the frame header does not match with the physical address it will simply drop the frame.
- At receiver computer (D), the destination address matches with its physical address (54). So the frame is accepted and decapsulation is carried out to recover the data.
- The example of a 48 bit or 6 byte physical address is as follows. It contains 12-hexadecimal digits.

08 : 63 : 4C : 81 : 08 : 1D

12.1.2 Logical Addresses (IP Addresses) :

W-09, W-11, S-16

MSBTE Questions

Q. 1 What is IP addressing ? Explain the classes of IP addressing. **(W-09, W-11, 8 Marks)**

Q. 2 Define IP addressing. List IP address classes with their range of addresses. **(S-16, 4 Marks)**

- Logical addresses are required to facilitate universal communications in which different types of physical networks can be involved.
- The logical address is also called as the IP (Internet Protocol) address.
- The internet consists of many physical networks interconnected via devices like routers.
- Internet is a packed switched network that means the data form the source computer is sent in the form of small packets carrying the destination address upon them.
- A packet starts from the source host, passes through many physical networks and finally reaches the destination host.
- At the network level, the hosts and routers are recognised by their **IP addresses** or logical addresses.
- An IP address is an internetwork address. It is a universally unique address.
- Every protocol involved in internetworking requires IP addresses.
- The logical address used in internet is currently a 32-bit address. The same IP address can never be used by more than one computer on the Internet.

12.1.3 Port Address :

- The modern computers are designed to run multiple processes on it simultaneously.
- The main objective of internet is the process to process communication. For this purpose it is necessary to lable or name the processes.
- Thus the processes need addresses. The lable assigned to a process is called as a port address. It is a 16 bit address.

12.1.4 Specific Addresses :

- Some applications have user friendly addresses. The examples of specific addresses are the e-mail addresses or the MSBTE Resource Locators (URL).

12.2 IPv4 Addresses :

W-09, W-11, S-16

MSBTE Questions

Q. 1 What is IP addressing ? Explain the classes of IP addressing. **(W-09, W-11, 8 Marks)**

Q. 2 Define IP addressing. List IP address classes with their range of addresses. **(S-16, 4 Marks)**

- Each computer connected to the Internet should be identified uniquely. The identifier used for this purpose is called as the **Internet address** or IP address.
- The hosts and routers on the Internet have unique IP addresses.
- The current version of IP (Internet Protocol) is IPv4 whereas the advanced version is IPv6.
- The IPv4 address is a 32-bit address and it is used for defining the connection of a host or router to the Internet. **Thus an IP address is an address of the interface.**

12.2.1 Uniqueness of IP Addresses :

- The IP address is **unique** and **universal.** That means each IP address defines only **one connection** to the Internet.
- At any given time, no two devices connected to the Internet can have the same IP address.
- But if a device is connected to the Internet via two connections through two different networks, then it can have two different IP addresses.
- All the IPv4 addresses are 32 bit long and they are used in the source address and destination address fields of the IP header.
- The IP addresses for hosts are assigned by the network administrator. For Internet it has to be obtained from the network information center.

12.2.2 Address Space :

- The IPv4 protocol has an address space. It is defined as the total number of addresses used by the protocol.

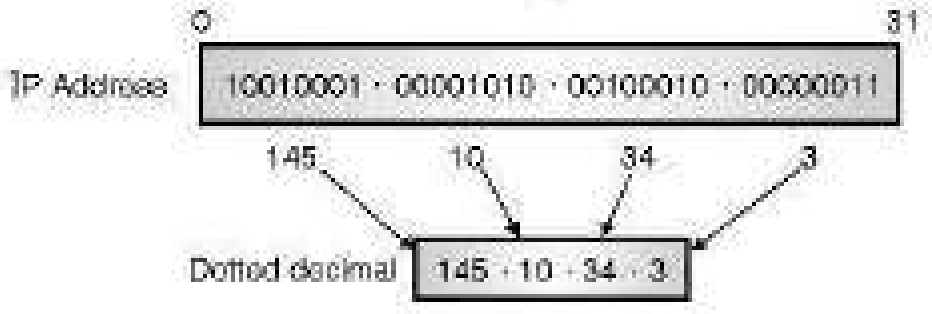
- If N number of bits are used for defining an address then the address space will be 2^N addresses.
- For IPv4, N is 32 bits. Hence its address space is 2^{32} or 4, 294, 967, 296 (more than 4 billion).
- So theoretically more than 4 billion devices could be connected to the Internet.
- Thus **the address space** of IPv4 is 2^{32}.

12.2.3 Notation :

- The IPv4 addresses can be shown use three different notations as follows :
  1. Binary notations (base 2).
  2. Dotted decimal notation (base 256).
  3. Hexadecimal notation (base 16).
- Out of these the **dotted decimal** notation is most commonly used.

Dotted decimal notation :

- This notation has become popular because of the two advantages it offers. This notation makes the IPv4 address more compact and easy to read.
- The 32 bit IPv4 address is grouped into groups of 8-bits each separated by decimal points (dots).
- Each 8-bit group is then converted into an equivalent decimal number as shown in Fig. 12.2.1.



(S-2002) **Fig. 12.2.1 : Dotted decimal notation**

- Each octet (byte) can take a value between 0 and 255. Therefore the IPv4 address in the dotted decimal notation has a range from 0.0.0.0 to 255.255.255.255.
- For example the IPv4 address of 1001 0001.00001010 .00100010 .00000011 is denoted in the dotted decimal form as 145.10.34.3.

12.2.4 IP Address Assignment : S-09, W-12

MSBTE Questions

Q. 1 Explain the concept of IP address assignment. **(S-09, 4 Marks)**

Q. 2 Explain IP address assignment. **(W-12, 4 Marks)**

- The network administrators need to assign IP addresses to the system on their network. This address needs to be a unique one.
- The IP address consists of two parts namely a network identifier and a host identifier.
- All the computers on a particular subnet will have the same network identifier but different host identifiers.
- The Internet Assigned Numbers Authority (IANA) assigns network identifiers to avoid any duplication of addresses.

12.2.5 IPv4 Address Format :

- A 32 bit IPv4 address consists of two parts. The first part is called as **net id** i.e. network identification which identifies a network on the Internet and the second part is called as the **host id** which identifies a host on that network.
- Fig. 12.2.2 shows the IPv4 address format. Note that the **net id** and **host id** are of variable lengths depending on the class of address.

(S-2002) **Fig. 12.2.2 : IPv4 address format**

- Note that class D and E addresses are not divided into net id and host id for the reasons discussed later on.

12.3 Classful Addressing :

- The concept of IP addresses is few decades old. It uses the concept of **classes.**
- This architecture is called as the **classful addressing.**
- Later on in mid 1990s a new architecture of addressing was introduced which was known as **classless addressing.**
- This new architecture has superseded the original architecture.
- In this section we are going to discuss the classful addressing.

12.3.1 IPv4 Address Classes :

W-08, S-10, W-10, W-11, W-12, S-13, S-14, W-14, S-15, W-15, S-16, W-16, S-17, S-18, I-Scheme : S-22

MSBTE Questions

Q. 1 What are the different IP address classes ? Explain any one in brief. **(W-08, W-15, S-17 4 Marks)**

Q. 2 Explain any four IP address classes. **(S-10, 4 Marks)**

Q. 3 Describe the various IP address classes. **(W-10, 4 Marks)**

Q. 4 What is IP addressing ? Explain the classes of IP addressing. **(W-11, 8 Marks)**

Q. 5 Explain IP address classes. **(W-12, 8 Marks)**

Q. 6 What is IP address ? State the IP address classes. **(S-13, 2 Marks)**

Q. 7 Which different classes are used for IP addressing ? Describe each in brief. **(S-14, 4 Marks)**

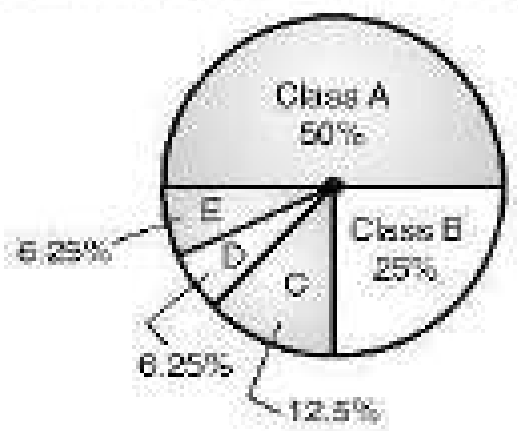
Q. 8 List different classes of IP address. **(W-14, 2 Marks)**

Q. 9 Describe different IP address classes. **(S-15, 4 Marks)**

Q. 10 Define IP addressing. List IP address classes with their range of addresses. **(S-16, 4 Marks)**

Q. 11 Describe the various IP address classes with suitable examples. **(W-16, S-18, 4 Marks)**

- In the classful addressing architecture, the IP address space has been divided into five classes : A, B, C, D and E.
- Fig. 12.3.1 shows the percentage of occupation of the address space by each class.
- The number of class A addresses is the highest i.e. 50 % and those of classes D and E is the lowest i.e. 6.25 %.



Class	No. of addresses	
A	2^{31}	50%
B	2^{30}	25%
C	2^{29}	12.5%
D	2^{28}	6.25%
E	2^{28}	6.25%

(G-2003) **Fig. 12.3.1 : Classful addressing occupation of address space**

12.3.2 Formats of Various Classes :

W-08, S-10, W-10, W-11, W-12, S-14, W-15, W-16, S-17, S-18, I-Scheme : S-19, W-19

MSBTE Questions

Q. 1 What are the different IP address classes ? Explain any one in brief. **(W-08, 4 Marks)**

Q. 2 Explain any four IP address classes. **(S-10, 4 Marks)**

Q. 3 Describe the various IP address classes. **(W-10, 4 Marks)**

Q. 4 What is IP addressing ? Explain the classes of IP addressing. **(W-11, 8 Marks)**

Q. 5 Explain IP address classes. **(W-12, 8 Marks)**

Q. 6 Which different classes are used for IP addressing ? Describe each in brief. **(S-14, 4 Marks)**

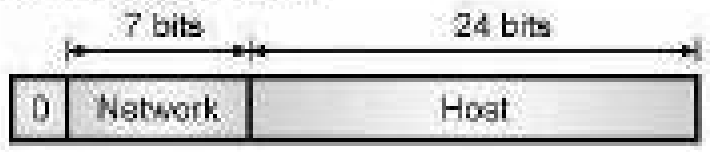
Q. 7 What are the different IP address classes ? Explain any one in brief. **(W-15, 4 Marks)**

Q. 8 Describe the various IP address classes with suitable examples. **(W-16, S-18, 4 Marks)**

Q. 9 State different IP address classes. Explain any one in brief. **(S-17, 4 Marks)**

Class A format :

- The formats used for IPv4 address are as shown in Fig. 12.3.2. The IPv4 address for class A networks is shown in Fig. 12.3.2(a).

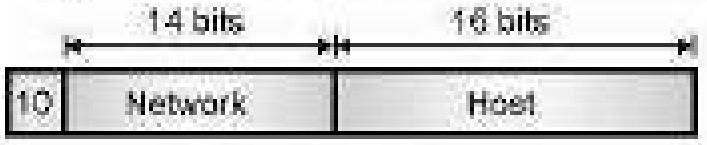


(G-531) **Fig. 12.3.2(a) : Class A IPv4 address formats**

- The network field is 7 bit long as shown in Fig. 12.3.2(a) and the host field is of 24 bit length.
- So the network field can have numbers between 1 to 126.
- But the host numbers will range from 0.0.0.0 to 127.255.255.255.
- Thus in class A, there can be 126 types of networks and 17 million hosts.
- The "0" in the first field identifies that it is a class A network address.

Class B format :

- The class B address format is shown in Fig. 12.3.2(b).
- The first two fields identify the network, and the number in the first field must be in the range 128 - 191.

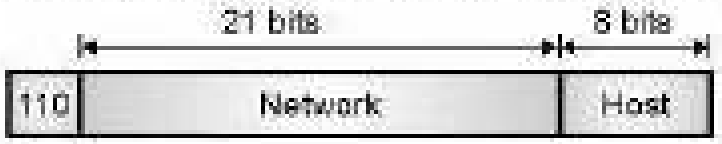


(G-532) **Fig. 12.3.2(b) : Class B format**

- Class B networks are large. Host numbers 0.0 and 255.255 are reserved, so there can be upto 65,534 (216-2) hosts in a class B network. Most of the 16,382 class B addresses have been allocated. The first block covers address from 128.0.0.0 to 128.255.255.255 and the last block covers from 191.255.0.0 to 191.255.255.255.
- **Example :** 128.89.0.26, for host 0.26 on net 128.89.

Class C format :

- The class C address format is shown in Fig. 12.3.2(c).



(G-533) **Fig. 12.3.2(c) : Class C format**

- The first block in class C covers addresses from 192.0.0.0 to 192.0.0.255 and the last block covers addresses from 223.255.255.0 to 223.255.255.255.

Class D format :

- The class D address format is shown in Fig. 12.3.2(d).

1110	Multicast address

Fig. 12.3.2(d) : Class D format

- The class format allows for upto 2 million networks with upto 254 hosts each and class D format allows the multicast in which a datagram is directed to multiple hosts.

Class E address format :

- Fig. 12.3.2(e) shows the address format for a class E address. This address begins with 11110 which shows that it is reserved for the future use.

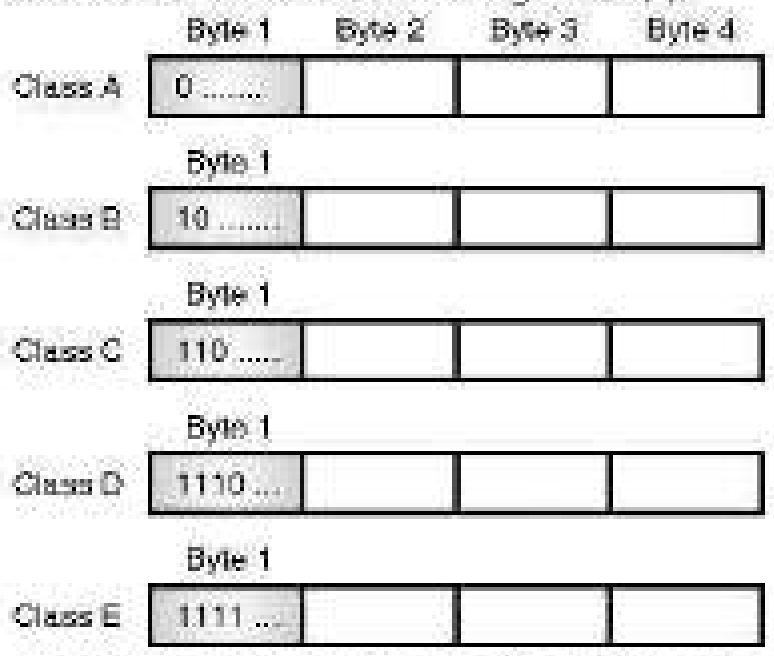
11110	Reserved for future use

Fig. 12.3.2(e) : IPv4 address for class E network

- The 32 bit (4 byte) network addresses are usually written in dotted decimal notation. In this notation each of the 4 bytes is written in decimal from 0 to 255.
- So the lowest IP address is 0.0.0.0 i.e. all the 32 bits are zero and the highest IPv4 address is 255.255.255.255.

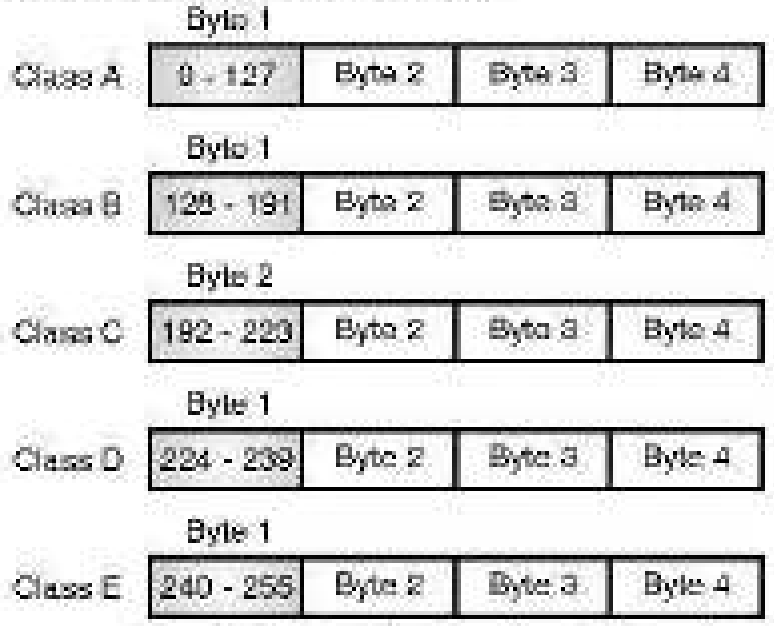
12.3.3 How to Recognize Classes ?

- When an IPv4 address is given to us either in the binary or dotted decimal notation, we can find the class of the address.
- If the given address is in the binary notation then we can identify its class by inspecting the first few bits of the address. This is as shown in Fig. 12.3.3(a).



(G-2004) **Fig. 12.3.3(a) : Finding the address class**

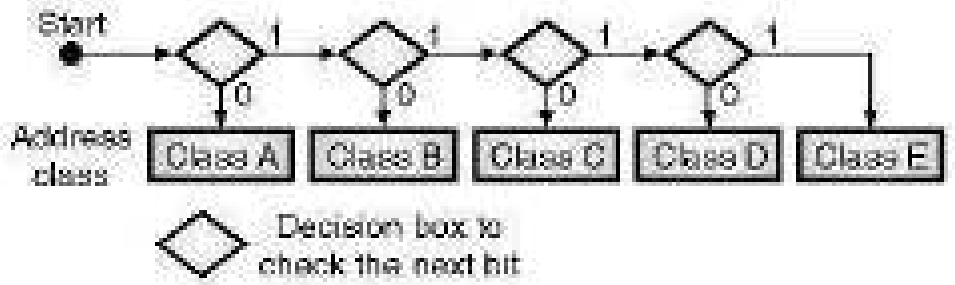
- If the given address is in the dotted decimal notation then we can identify the address class by inspecting the first byte of the address.
- This is as shown in Fig. 12.3.3(b).



(G-2005) **Fig. 12.3.3(b) : Finding the address class**

- It is important to note here that there are some special addresses which fall in class A or E.
- These special addresses are to be treated as the exceptions to the classful addressing. We have discussed them later in the chapter.
- In computers, the IPv4 addresses are generally stored in the binary notation format. Therefore it is possible to write an algorithm which can identify the address class by using the continuous checking process.

– The principle of such an algorithm has been shown in Fig. 12.3.4.



(G-2006) **Fig. 12.3.4 : Algorithm to identify address class**

12.3.4 Two Level Addressing :

– The IPv4 addressing is used for defining a destination for an Internet packet at the network layer.

– At the time when classful addresses were designed, the Internet was considered as the network of networks.

– In other words the whole Internet was divided into a number of smaller networks with many hosts connected to each network.

– Normally an organization which wants to connect to the Internet creates a network and the Internet authorities allocate a block of address to the organization. These addresses can be in class A, B or C.

– All the addresses allotted to an organization belong to a single block. Therefore each IPv4 address in classful addressing system is made up of two parts namely **net id** and **host id** as shown in Fig. 12.3.5.

(G-2007) **Fig. 12.3.5 : Two level addressing in classful addressing**

– The job of the **net id** is to define a network and that of the **host id** is to define a particular host in that network.

– As shown in Fig. 12.3.5 if n bits define **net id** then the remaining (32-n) bits define **host id.**

– The value of "n" is not same for all the classes. Infact it is depend on the class as shown in Table 12.3.1.

Table 12.3.1

Class	Value of n
A	n = 8
B	n = 16
C	n = 24

12.3.5 Extracting Information in a Block :

– A block is nothing but a range of addresses. For any given block we would be interested to extract the following three pieces of information :

1. The total number of addresses in the block.
2. The first address of the block.
3. The last address in the block.

– Before extracting all this information, we have to identify the class of the address as discussed earlier.

– Once we find the class of the block, we will have the values of "n" (the length of **net id** in bits) and (32 – n) i.e. the length of the **host id** in bits.

– It is now possible to obtain the three pieces of information mentioned above as shown in Fig. 12.3.6.

1. Total number of addresses in the block :

– The total number of IPv4 addresses in the given block will be equal to,

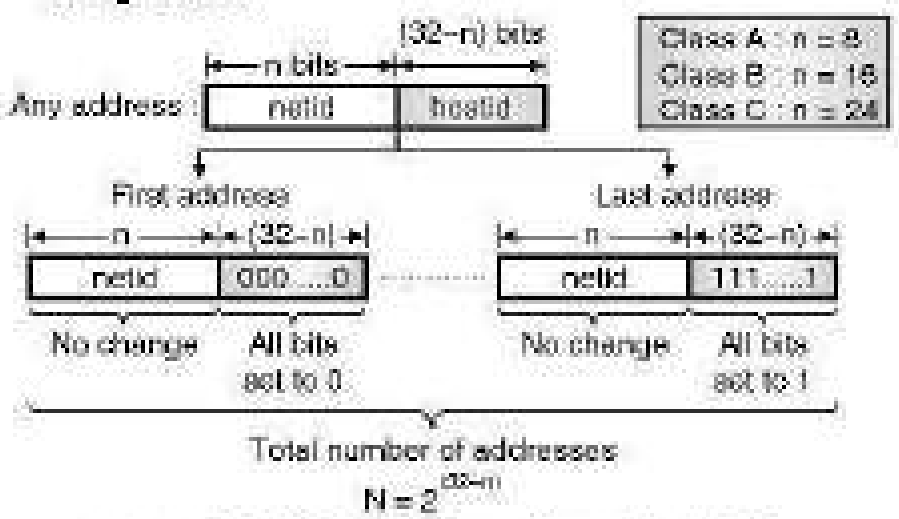
$$N = 2^{(32 - n)} \qquad \ldots(12.3.1)$$

2. First address in the block :

– The first address in the given block can be obtained by keeping the leftmost "n" bits in the address as it is and setting all the (32 – n) rightmost bits to 0 as shown in Fig. 12.3.6.

3. Last address in the block :

– The last address in the given block can be obtained by keeping the leftmost "n" bits in the address as it is and then setting all the (32 – n) rightmost bits to 1 as shown in Fig. 12.3.6.

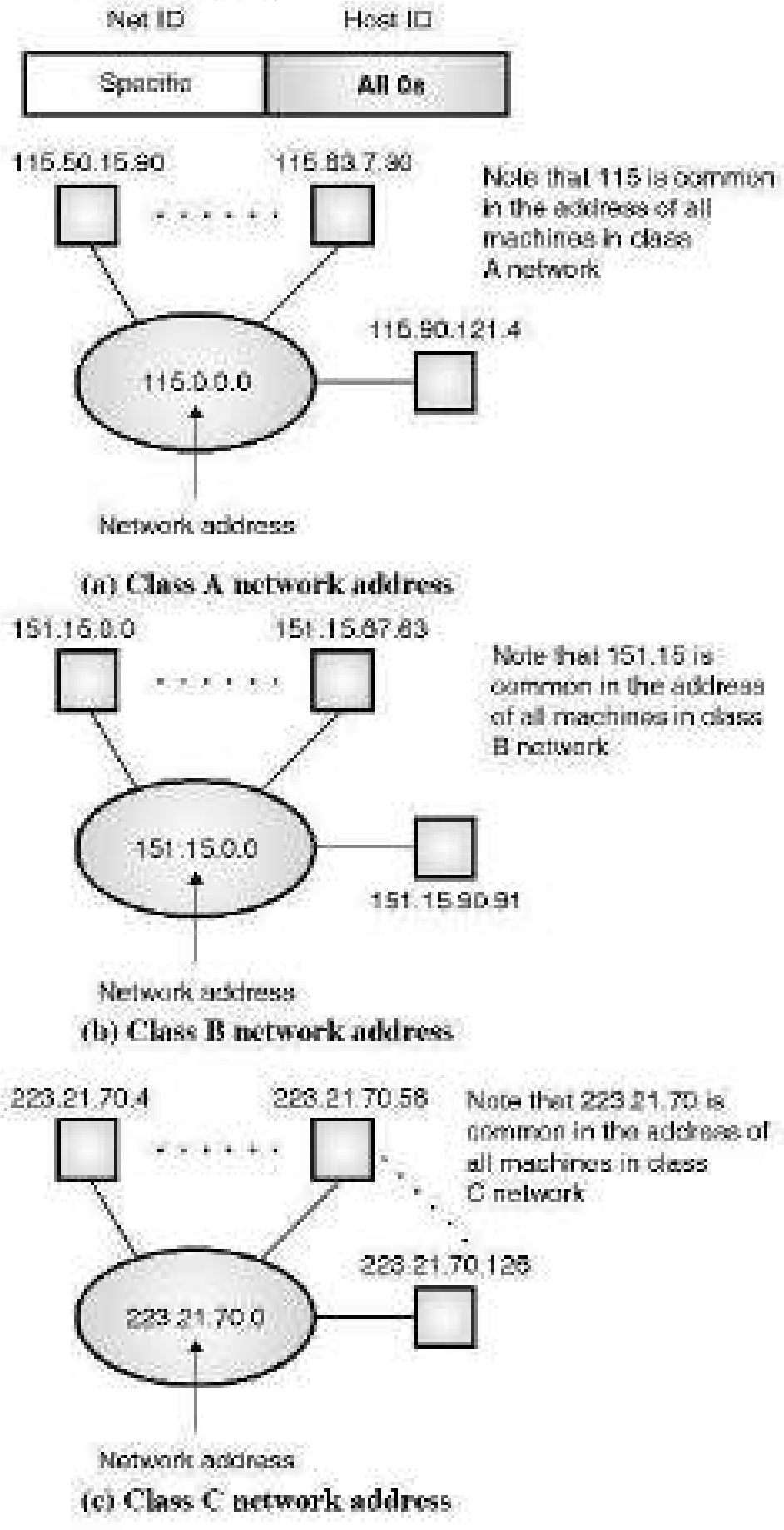


(G-2008) **Fig. 12.3.6 : Information extraction in classful addressing**

12.3.6 Network Address :

– The network address is an address that defines the network itself. It cannot be assigned to a host

– Fig. 12.3.7 shows the examples of network addresses for different classes.



(a) Class A network address

(b) Class B network address

(c) Class C network address

(G-556) Fig. 12.3.7

– The following examples will enable you to find the network address.

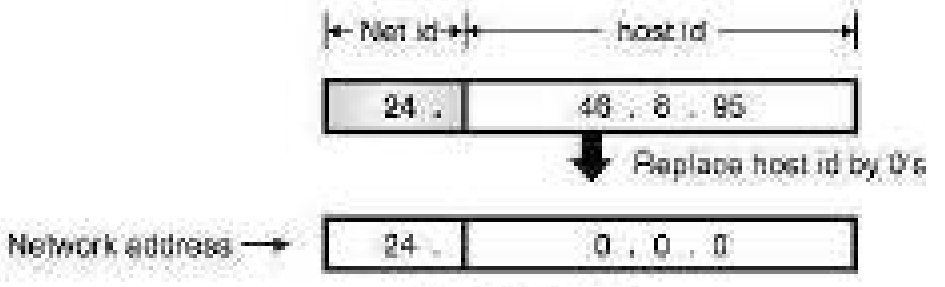
Ex. 12.3.1 : For the address 24.46.8.95 identify the type of network and find the network address.

Soln. :

– Examine the first byte. Its value is 24 i.e. it is between 0 and 127. So it is a class A network.

– So only the first byte defines the Net id. So we can find the network address by replacing the host id with 0s.

– The process of obtaining the network address is shown in Fig. P. 12.3.1.



(G-557) Fig. P. 12.3.1

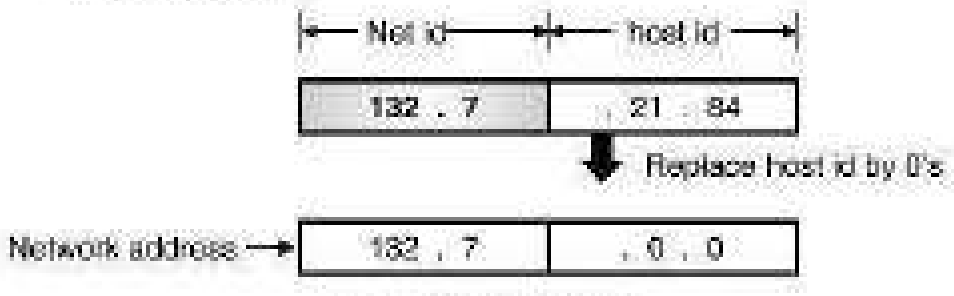
– So the network address is 24.0.0.0.

Ex. 12.3.2 : For the address 132.7.21.84 find the type of network and the network address.

Soln. :

– Examine the first byte. It is 132 i.e. between 128 and 192. So it is a class B network.

– So the first two bytes define the net id. Replace the host id with 0's to get the network address as shown in Fig. P. 12.3.2.



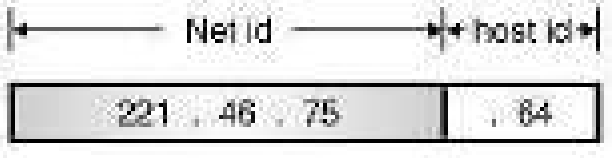
(G-558) Fig. P. 12.3.2

– So the network address is 132.7.0.0.

Ex. 12.3.3 : Find the class of the network if the address is 221.46.75.64.

Soln. :

– The first byte is 221 i.e. between 192 and 255. So this is a class C network. The net id and host id are as shown in Fig. P. 12.3.3.



(G-559) Fig. P. 12.3.3

What is the difference between net id and network address ?

– The network address is different from a net id. A network address has both net id and host id, with 0s for the host id.

Where to use the network address ?

– The network address is used to route the packets to the desired location.

12.3.7 Network Mask or Default Mask :

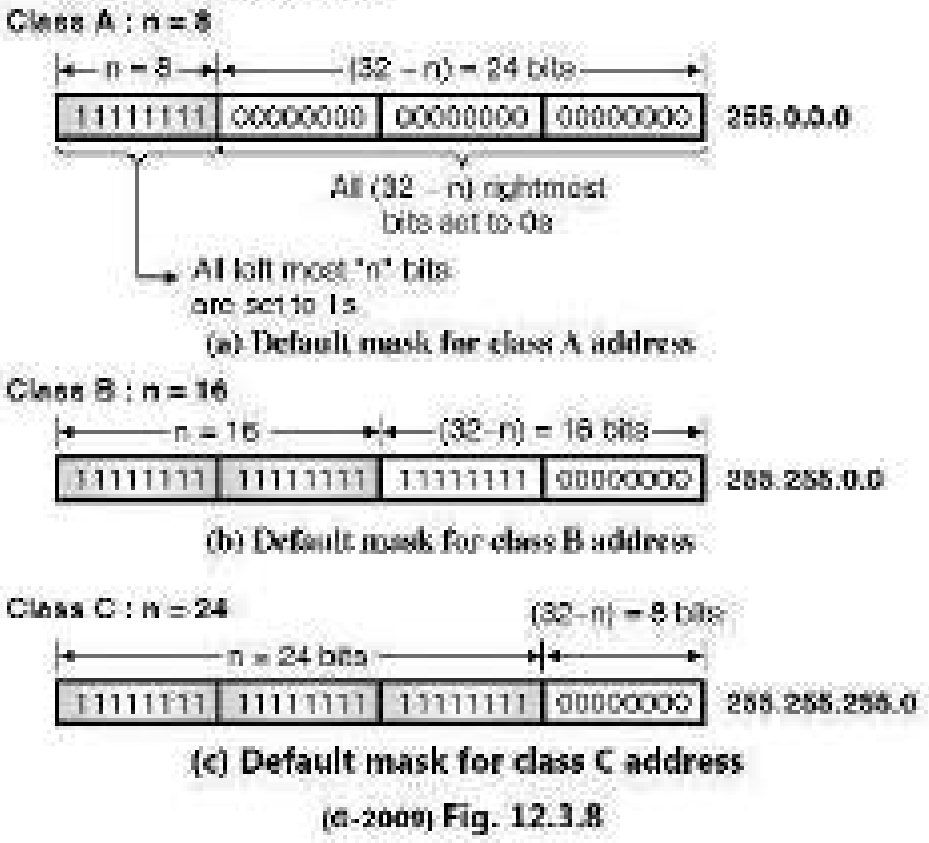
- Earlier we have discussed the methods for extracting different pieces of information.
- But all these methods are theoretical methods which are useful in explaining the concept.
- But practically these methods are not used. When a packet arrives at the input of the router in the Internet, it uses an algorithm to extract the **network address** from the destination address in the received packet.
- This can be achieved by using a **network mask.**

Definition of default mask :

- A **network mask** or **default mask** in classful addressing is defined as a 32-bit number obtained by setting all the "n" leftmost bits to 1s and all the (32 – n) rightmost bits to 0.

12.3.8 Default Masks for Different Classes :

- We know that the value of n is different for different classes. Therefore their default masks also will be different.
- The default masks for class A, B and C addresses are as shown in Fig. 12.3.8.



(a) Default mask for class A address

(b) Default mask for class B address

(c) Default mask for class C address

(G-2009) **Fig. 12.3.8**

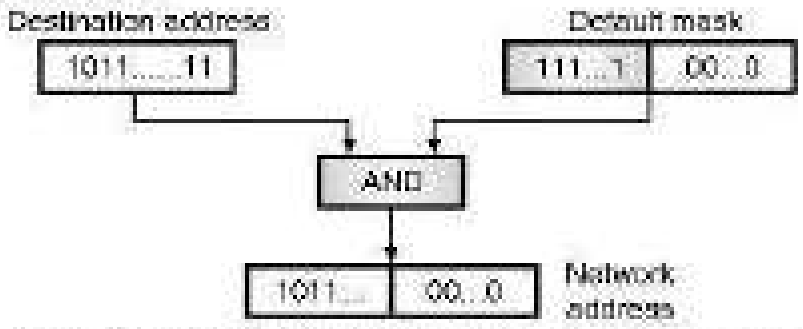
- Table 12.3.2 enlists the default masks of the three classes of IPv4 addresses.

Table 12.3.2 : Default masks

Address class	Default mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

12.3.9 Finding Network Address using Default Mask :

- The router uses the AND operation for extracting the network address from the destination address of the received packet.
- The router ANDs the destination address with the default mask to extract the network address as shown in Fig. 12.3.9.



(G-2010) **Fig. 12.3.9 : Finding a network address using the default mask**

- It is possible to use the default mask to find the number of addresses and the last address in the block.

12.3.10 Three Level Addressing : Subnetting :

S-08, W-10, S-12, S-13, S-14, W-14, W-15, S-16, W-16, S-17, I-Scheme : S-22

MSBTE Questions

Q. 1 What is subnet masking ? **(S-08, S-13, 4 Marks, W-10, 2 Marks)**

Q. 2 Explain subnet masking. **(S-12, 4 Marks)**

Q. 3 What is meant by subnet ? How to use subnet masking to create two subnets ? **(S-14, 4 Marks)**

Q. 4 Explain sub-netting and super-netting with example. **(W-14, 4 Marks)**

Q. 5 Describe the term subnet masking. **(W-15, 4 Marks)**

Q. 6 State meaning of : 1. Subnetting 2. Supernetting with suitable examples. **(S-16, 4 Marks)**

Q. 7 Explain the terms :
1. Subnetting
2. Supernetting
3. Masking
4. Classless IP addressing with suitable examples. **(W-16, 8 Marks)**

Q. 8 Explain subnet masking. **(S-17, 4 Marks)**

- As discussed earlier, the originally designed IP addresses were with two level addressing with **net id** and **host id.**
- The two level addressing is based on the principle that in order to reach a host on the Internet, we have to reach the network first and then the host.

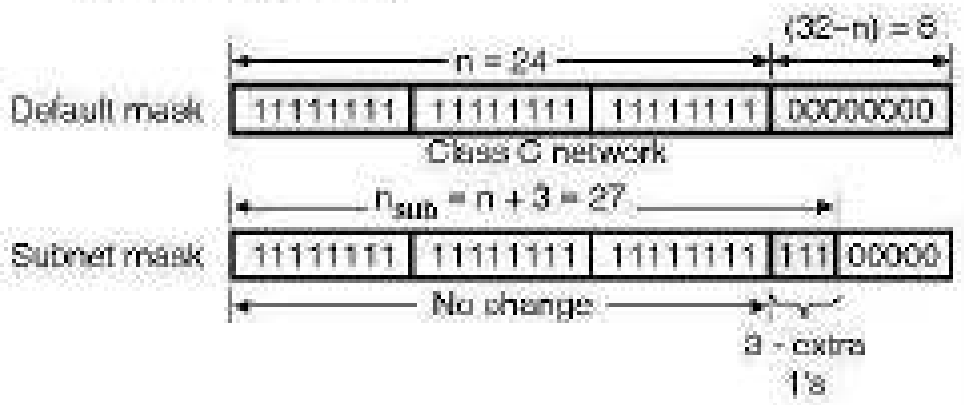
- But very soon it became evident that the two level addressing would not be sufficient for the following two reasons :
  1. First it was needed to divide a large network of an organization (to which a block in class A or B is allotted) into many smaller **subnets** (subnetworks) for improved management and security.
  2. Second reason is more important. The blocks in class A and B were almost depleted and the blocks in class C were smaller than the needs of most organization. Therefore the organizations had to divide their allotted class A or B block into smaller subnetworks and share them.

Definition of subnetting :

- We can define the **subnetting** as the principle of splitting a block of addresses into smaller blocks of addresses.
- In the process of **subnetting** we divide a big network into smaller subnetworks or **subnets.**
- Each such subnet has its own **subnet address.**

Subnet mask :

- The **network mask** or **default** mask that we discussed earlier is used when the given network is **not** to be divided into smaller subnetworks i.e. when **subnetting** is **not** to be done.
- But when the given network is to be divided into smaller subnets i.e. when subnetting is to be done, we need to create a **subnet mask** for each subnet.
- Fig. 12.3.10 shows the format of a subnet mask. Each subnet has its own **net id** and **host id.**
- If we want to divide a network into 8 subnets then the corresponding subnet mask will have three extra 1's because $2^3 = 8$, as compared to the default mask, as shown in Fig. 12.3.10.

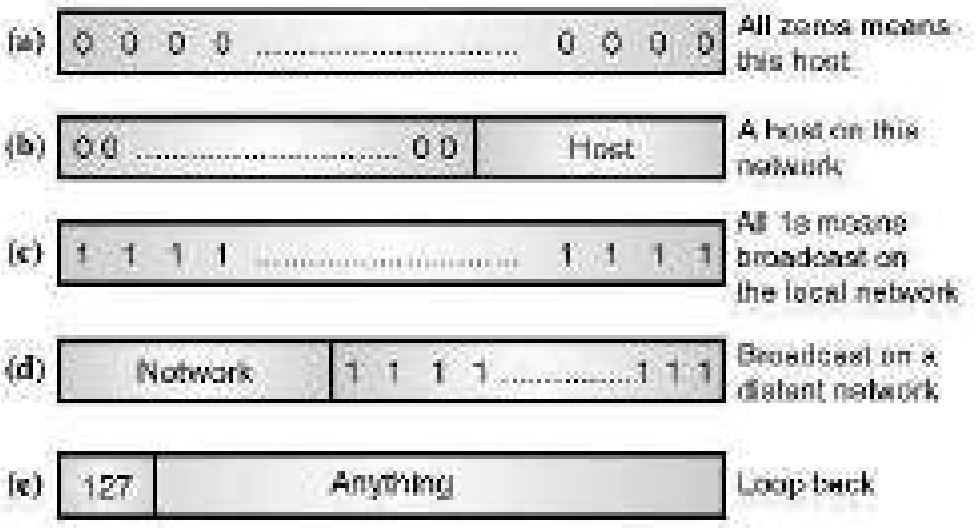


(G-2011) **Fig. 12.3.10 : Default and subnet masks**

- In Fig. 12.3.10, we have shown the default mask and subnet mask when a class C network is to be divided into 8 subnets.

12.3.11 Special IP Addresses :

- Fig. 12.3.11 shows some special IP addresses.



(G-540) **Fig. 12.3.11 : Special IP addresses**

- All zeros means this host or this network and all 1s means broadcast address to all hosts on the indicated network.
- The IP address 0.0.0.0 is used by the hosts when they are being booted but not used afterward.
- The IP addresses with 0 as the network number refer to their own network without knowing its number as shown in Fig. 12.3.11(b).
- The address having all ones is used for broadcasting on the local network such as a LAN as shown in Fig. 12.3.11(c).
- Refer Fig. 12.3.11(d). This is an address with proper network number and all 1s in the host field. This address allow machines to send broadcast packets to distant LANs anywhere in the Internet.
- If the address is "127 Anything" as shown in Fig. 12.3.11(e) then it is a reserved address **loopback testing.** This feature is also used for debugging network software.

12.3.12 Limitations of IPv4 : W-08, S-18

MSBTE Questions

Q. 1 Give the limitations of IPv4. **(W-08, S-18, 4 Marks)**

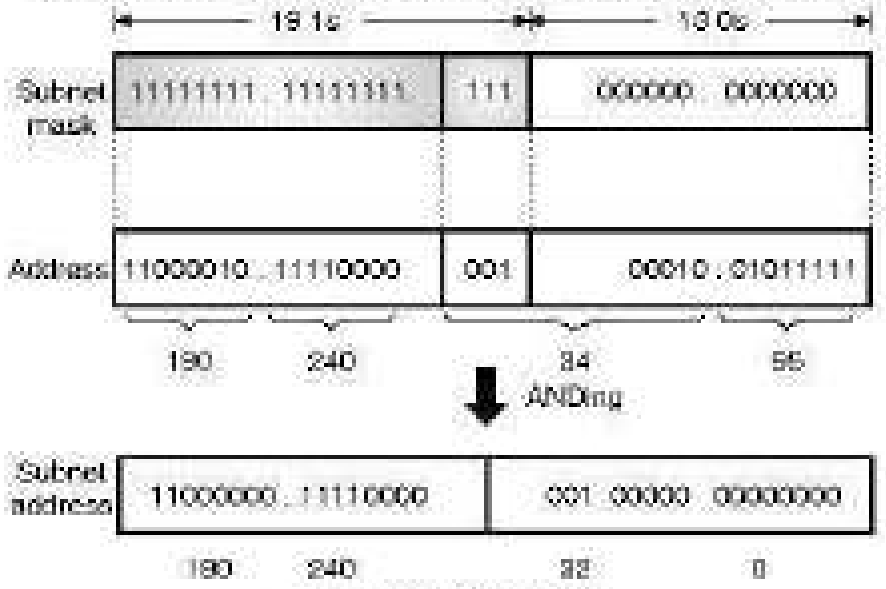
- The most obvious limitation of IPv4 is its address field. IP relies on network layer addresses to identify end-points on networks, and each networked device has a unique IP address.

- IPv4 uses a 32-bit addressing scheme, which gives it 4 billion possible addresses. With the proliferation of networked devices including PCs, cell phones, wireless devices, etc., unique IP addresses are becoming scarce, and the world could theoretically run out of IP addresses.
- If a network has slightly more number of hosts than a particular class, then it needs either two IP addresses of that class or the next class of IP address.
- For example, let us say a network has 300 hosts, this network needs either a single class B IP address or two class C IP addresses.
- If class B address is allocated to this network, as the number of hosts that can be defined in a class B network is $(2^{16} - 2)$, a large number of host IP addresses are wasted.
- If two class C IP addresses are allocated, as the number of networks that can be defined using a class C address is only (2^{21}), the number of available class C networks will quickly exhaust.
- Because of the above two reasons, a lot of IP addresses are wasted and also the available IP address space is rapidly reduced.
- Other identified limitations of the IPv4 protocol are: Complex host and router configuration, non-hierarchical addressing, difficulty in re-numbering addresses, large routing tables, non-trivial implementations in providing security, QoS (Quality of Service), mobility and multi-homing, multicasting etc.
- To overcome these problems the internet protocol version 6 (IPv6) which is also known as internet protocol, next generation (IPng) was proposed.
- In IPv6 the internet protocol was extensively modified for accommodating the unforeseen growth of the internet.
- The format and length of the IP addresses has been changed and the packet format also is changed.

Ex. 12.3.4 : A router inside an organization receives the same packet with a destination address 190.240.34.95. If the subnet mask is /19 (first 19-bits are 1s and following bits are 0s). Find the subnet address.

Soln. :

- To find the subnet address, AND the destination address with the subnet mask as shown in Fig. P. 12.3.4.



(G-944) **Fig. P. 12.3.4**

- Thus the subnet address is 190.240.32.0.

12.4 Classless Addressing : W-16

MSBTE Questions

Q. 1 Explain the terms :
1. Subnetting.
2. Supernetting.
3. Masking.
4. Classless IP addressing with suitable examples. **(W-16, 8 Marks)**

- Eventhough the number of actual devices connected to Internet is much less than 4 billion, the address depletion has taken place due to flaws in the classful addressing scheme.
- We have run out of class A and B addresses. To overcome these problems, the classless addressing is now being tried out.
- In the classless addressing, there are no classes but the address generation take place in blocks.

Address blocks :

- Address block is defined as the range of addresses.
- In the classless addressing, when an entity wants to get connected to the internet, a block (range) of addresses is granted to it.
- The size of this block i.e. number of addresses depends on the size of the entity as well as its nature.
- That means for a small entity such as a household only one or two addresses will be given whereas for a larger entity like an organization, thousands of addresses can be allotted.

Restrictions :

- Some of the restriction on classless address blocks have been imposed by the internet authorities in order to simplify the process of address handling.
  1. The addresses in a block should be continuous, i.e. serial in manner.
  2. The total number of addresses in a block has to be equal to some power of 2 i.e. 2^1, 2^2, 2^3 ..etc.
  3. The first address should be evenly divisible by the number of addresses.

12.4.1 Supernetting :

W-14, S-16, W-16, I-Scheme : S-22

MSBTE Questions

Q. 1 Explain sub-netting and super-netting with example. **(W-14, 4 Marks)**

Q. 2 State meaning of : 1. Subnetting 2. Supernetting with suitable examples. **(S-16, 4 Marks)**

Q. 3 Explain the terms :
1. Subnetting
2. Supernetting
3. Masking
4. Classless IP addressing with suitable examples. **(W-16, 8 Marks)**

- The class A and class B addresses are almost depleted. But class C addresses are still available.
- But the size of class C address with a maximum number of 256 addresses does not satisfy the needs of an organization. More addresses will be required.
- The solution to this problem is **supernetting.**
- In supernetting an organization combines several class C blocks to create a large range of addresses i.e. several networks are combined to create a supernetwork.
- By doing this the organization can apply for a set of class C blocks instead of just one.

Example of supernetting :

- If an organization needs 1000 addresses, they can be obtained by using four C blocks (one C block corresponds to 256 addresses).
- The organization can then use these addresses as one supernetwork as a whole.

Note : The classful addressing is almost obsolete now and it is being replaced with classless addressing.

12.4.2 Who Decides the IP Addresses ?

- No two IP addresses should be same. This is ensured by a central authority that issues the prefix or the network number portion of the IP address.
- Locally an ISP is to be contacted in order to get a unique IP address prefix.
- At the global level the Internet Assigned Number Authority (IANA) allots an IP address prefix to the ISP.
- Thus it is ensured that the IP addresses are not duplicated.
- Conceptually IANA is a wholesales and ISP is a retailer of the IP addresses because ISP purchases IP addresses from IANA and sells them to the customers.

12.4.3 Registered and Unregistered Addresses :

W-08, S-18

MSBTE Questions

Q. 1 Explain registered and unregistered IP addresses. **(W-08, S-18, 4 Marks)**

- Registered IP addresses are required for computers which are accessible from the Internet but not every computer that is connected to the Internet.
- For security reasons, networks use firewalls or some other technologies for protecting the computers.
- The firewalls will enable the workstations to access the Internet but do not allow the other systems on the Internet to access them.
- These workstations are given the unregistered private IP addresses.
- These addresses are assigned by the network administrator without obtaining them from an ISP (Internet Service Provider) or IANA.
- These are special network addresses in each class as shown in Table 12.4.1.
- These addresses are to be used for private networks and are called **unregistered addresses.**
- We can choose any of these unregistered address while building our own private network.

Table 12.4.1 : IP addresses for private networks

Class	Network address
A	10.0.0.0 through 10.255.255.255
B	172.16.0.0 through 172.31.255.255
C	192.168.0.0 through 192.168.255.255

12.4.4 Solved Examples :

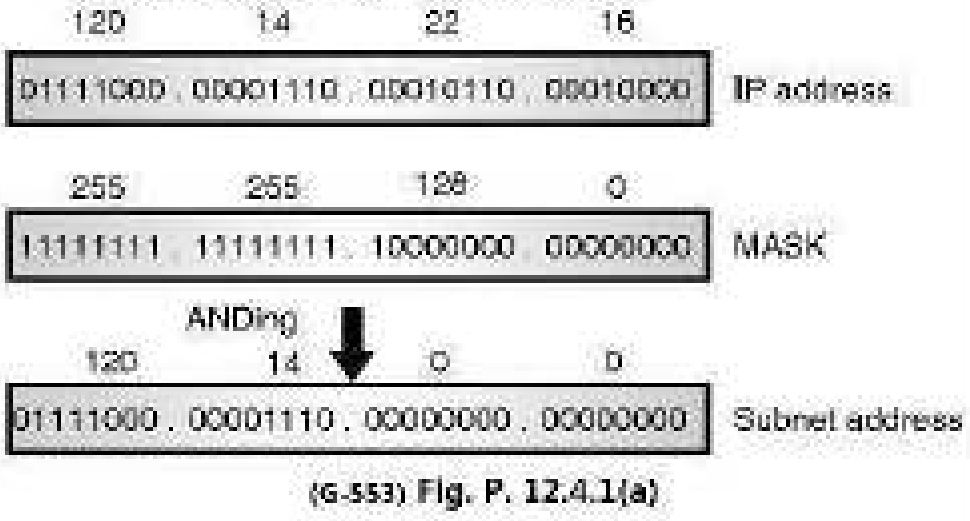
Ex. 12.4.1 : Find the sub-network address and the host id for the following :

Sr. No.	IP address	MASK
(a)	120.14.22.16	255.255.128.0
(b)	140.11.36.22	255.255.255.0
(c)	141.181.14.16	255.255.224.0
(d)	200.34.22.156	255.255.255.240

Soln. :

Step 1 : To find the subnet address :

– In order to find the subnet address we have to AND the IP address and the mask as follows :



(G-553) **Fig. P. 12.4.1(a)**

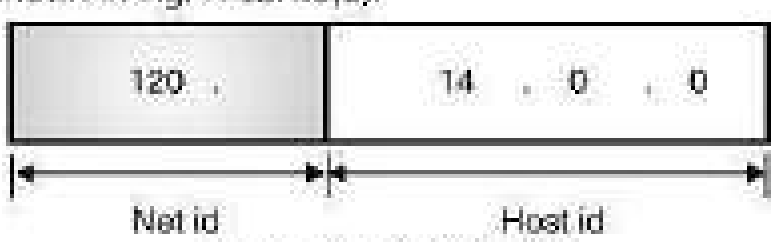
– So the subnet address is 120.14.0.0.

– Similarly we can find the other subnet addresses.

Step 2 : Host id :

– Examine the first byte of the subnet address. It is 120 which is between 0 and 127. Hence this is a class A network.

– So only the first byte corresponds to the net id and the remaining three bytes correspond to the host id as shown in Fig. P. 12.4.1(b).



(G-554) **Fig. P. 12.4.1(b)**

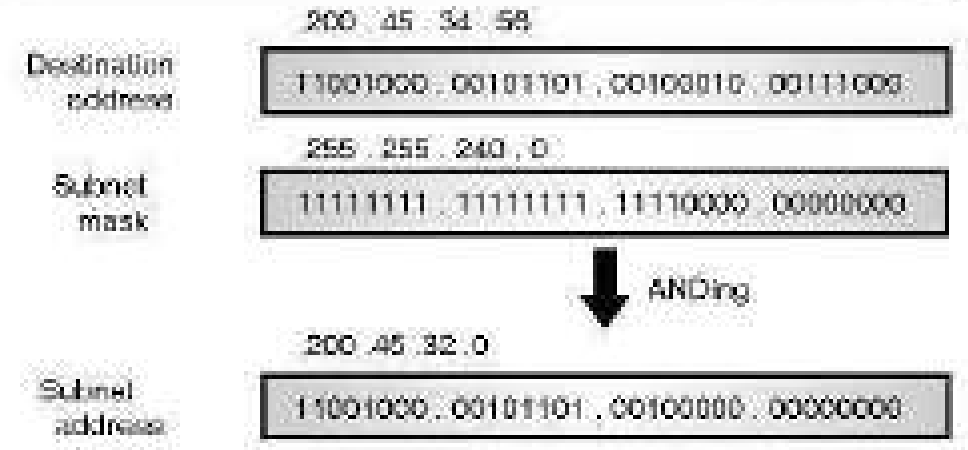
– So the host id is 14.0.0.

– Similarly we can find the other host id.

Ex. 12.4.2 : What is the subnet address if the destination address is 200.45.34.56 and subnet mask is 255.255.240.0 ?

Soln. :

– To find the subnet address we have to AND the IP address and the subnet mask as shown in Fig. P. 12.4.2.



(G-556) **Fig. P. 12.4.2**

– Thus the required subnet address is 200.45.32.0.

Ex. 12.4.3 : A company is granted a site address 201.70.64.0. The company needs six subnets. Design the subnets.

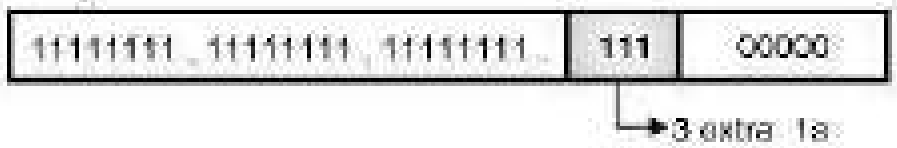
S-13, S-15, 4 Marks

Soln. :

– This is a class C network. So the default mask is 255.255.255.0

– As we need 6 subnets, we need three extra 1s. So the subnet mask is 255.255.255.200

– In the binary form the subnet mask is as shown in Fig. P. 12.4.3.



(G-557) **Fig. P. 12.4.3**

– In order to have six subnets, we can have 6 different combinations of the 3-extra 1s as shown in Table P. 12.4.3.

Table P. 12.4.3

Combination	Subnet Number
0 0 0	Subnet 1
0 0 1	Subnet 2
0 1 0	Subnet 3
0 1 1	Subnet 4
1 0 0	Subnet 5
1 0 1	Subnet 6

Ex. 12.4.4 : A class B network on internet has a subnet mask of 255.255.240.0. What is the maximum number of hosts per subnet ?

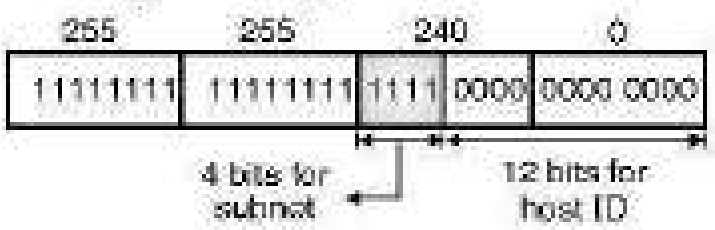
S-11, 4 Marks

Soln. :

– The structure of class B address is as shown in Fig. P. 12.4.4(a).

(G-564) **Fig. P. 12.4.4(a) : Class B address**

– The given subnet mask is 255.255.2400. So it is as shown in Fig. P. 12.4.4(b).



(G-565) **Fig. P. 12.4.4(b) : Subnet mask**

– Thus there are 4 extra 1s as shown in Fig. P. 12.4.4(b). So there will be 16 subnets and each subnet can have 2^{12} = 4096 hosts.

Ex. 12.4.5 : A class A network on the internet has a subnet mask of 255.255.224.0. What is the maximum number of hosts per subnet ?

S-05, 4 Marks

Soln. :

– A subnet mask of 255.255.224.0 corresponds to the following pattern.

255	255	244	0
11111111	11111111	111	00000	00000000

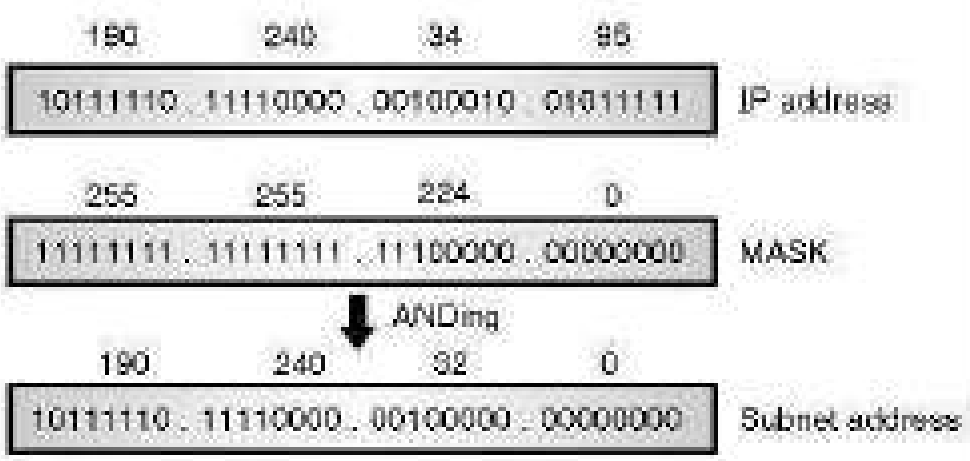
– Due to 3 additional 1s (shaded portion) there will be 2^3 = 8 subnets and the number of hosts per subnet will be 2^{13} = 8192.

Ex. 12.4.6 : A router inside an organization receives the same packet with a destination address 190.240.34.95. If the subnet mask is 19 (First 19 bits are 1s and following bits are 0s). Find subnet address.

S-09, 4 Marks

Soln. :

– The subnet address can be obtained by ANDing the destination address with the mask as follows :



(G-1003) **Fig. P. 12.4.6**

– As shown in Fig. P. 12.4.6, the subnet address is 190.240.32.0.

12.5 Classless Addressing in IPv4 :

– Eventhough the number of actual devices connected to Internet is much less than 4 billion, the address depletion has taken place due to flaws in the classful addressing scheme.

– We have run out of class A and B addresses. To overcome these problems, the super netting and subnetting has been tried as discussed earlier.

– But subnetting and supernetting also could not solve the problem of address depletion in IPv4.

– Due to increased number of Internet users, it was evident that a larger address space would be required as a long term solution to this problem.

– For this the length of the IP address should be increased which means the IP packet itself must be changed.

– A long term solution is to switch to IPv6. But a short term solution which uses the same address space has been deviced for IPv4. It is known as **classless addressing.**

– In the classless addressing, there are no classes but the address generation take place in blocks.

– The classless addressing was announced by the Internet authorities in 1996 in which blocks of variable length which do not belong to any class are used.

12.5.1 Variable Length Blocks :

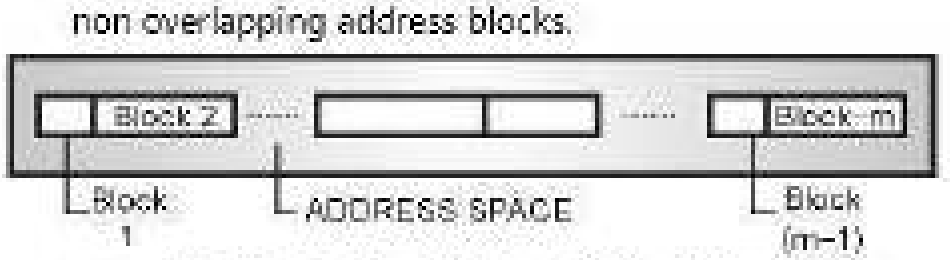
– Address block is defined as the range of addresses.

– In the classless addressing, when an entity wants to get connected to the internet, a block (range) of addresses is granted to it.

– The size of this block i.e. number of addresses depends on the size of the entity as well as its nature.

– That means for a small entity such as a household only one or two addresses will be given whereas for a larger entity like an organization, thousands of addresses can be allotted.

– Fig. 12.5.1 shows how the address space is divided into non overlapping address blocks.



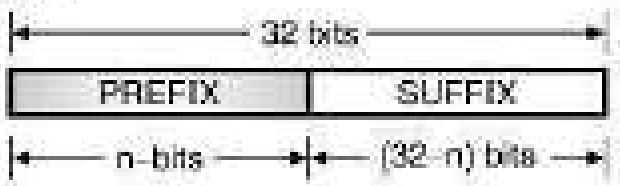
(G-1004) **Fig. 12.5.1 : Variable length blocks in classless addressing**

Two level addressing :

- We have discussed the two level addressing for classfull addressing which divided an address into two parts namely : net id and host id.

(G-1805) **Fig. 12.5.2 : Two layer addressing in classfull addressing**

- The **net id** and **host id** define the network and host respectively. It is possible to use the same idea in the classless addressing as well.
- A block of addresses granted to an organization is divided into two parts called as the **prefix** and the **suffix.**
- The role of prefix is same as that of the net id whereas as the role of suffix is same as that of the host id.
- Thus in a block granted to an organization, all the addresses will have the **same prefix** but each address will have a different **suffix.**
- Thus the prefix defines the network (organization to which the address block has been granted) while the suffix defines individual hosts on the network.
- The concept of two level addressing in classless addressing using the prefix and suffix is as shown in Fig. 12.5.3.



(G-1806) **Fig. 12.5.3 : Two level addressing using prefix and suffix for classless addressing**

- The IPv4 address is 32 bit long out of which the prefix will be of length "n" which can take any value from 0 to 32 and the length of the suffix will be (32 – n) bits.
- Note that the value of "n" i.e. length of the prefix depends on the length of the address block allotted (granted) to an organization.

Ex. 12.5.1 : Find out the values of prefix and suffix lengths in classless addressing if all the available addresses in IPv4 is to be considered as one single block.

Soln. :

- The total addresses in IPv4 is 2^{32} = 4,294,967,296.
- We have to consider this as one block hence the prefix length n = 0. Whereas all the hosts will have their individual addresses. So all the 32 bits will be allotted to the suffix length.

Ex. 12.5.2 : For the same data of the previous example find out the values of prefix and suffix lengths if all the available IPv4 addresses are divided into 4,294,967,296 blocks with each block having only one host.

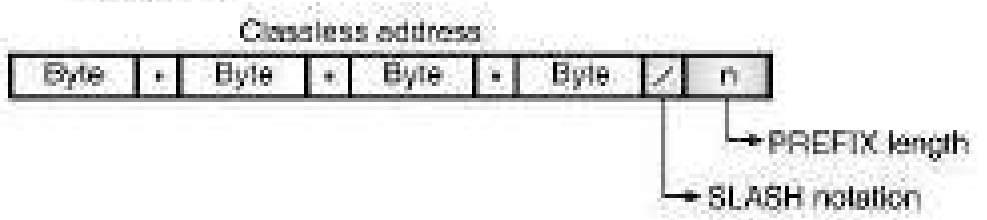
Soln. :

- Here the prefix length for each block is n = 32, and the suffix length would be (32-n) = 0. The address of the single host in each block will be same as its block address itself.

Note : The two previous examples show that the prefix number n and the number of addresses in a block are inversely proportional to each other. With increase in the value of n, the number of addresses in a block will decrease.

12.5.2 The Slash Notation (CIDR Notation) :

- If an address (classful or classless) is given to us and we want to extract information from it, then the net id in classful addressing or the prefix in classless addressing are extremely important and useful to us.
- However it is not easy to identify the prefix bits in a given classless address. It is easy to identify the net id from the given classful address.
- For a given classless address it is not possible to find the prefix length because the given address can belong to a block with any prefix length.
- Therefore, in classless addressing it is essential to include the prefix length to each address if the block of the given address is to be found.
- Hence the prefix length "n" is added to the classless address separated by a **slash** and the notation is known as the **slash notation.**
- Fig. 12.5.4 demonstrates a classless address with slash notation.



(G-1807) **Fig. 12.5.4 : Slash notation**

– The slash notation is also called as Classless Interdomain Routing or CIDR notation.

12.5.3 Network Mask :

– We have discussed the concept of network mask in the classful addressing.

– The same concept is also applicable in the classless addressing as well.

– A **network mask** in classless addressing is a 32 bit number. With its 'n' left most bits (corresponding to the prefix) all set to 1s and the remaining (32-n) bits corresponding to the suffix all set to 0s.

Ex. 12.5.3 : For the following addresses identify the number of prefix bits and write down the network mask :
1. 12.26.25.79 / 8
2. 130.12.230.156 / 16

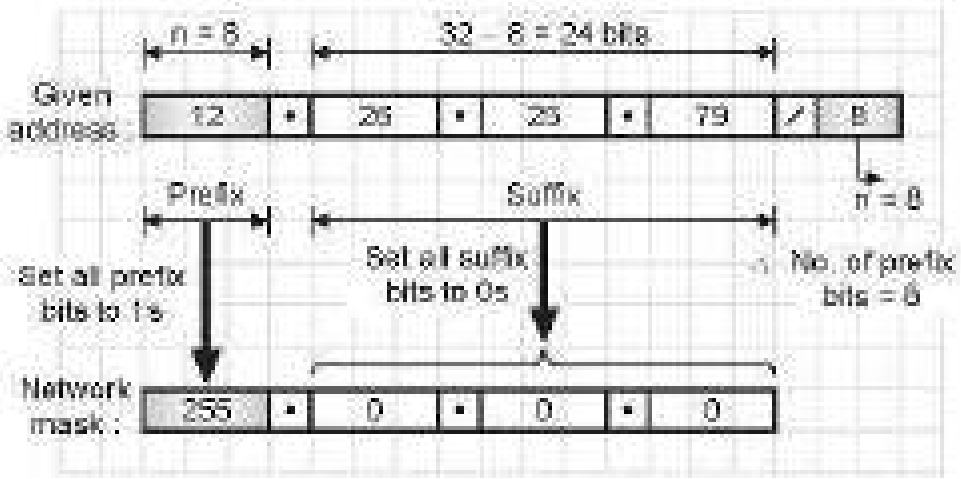
Soln. :

1. Classless CIDR address : 12.26.25.79 / 8

– As per the slash notation we have n = 8 i.e. number of prefix bits is 8.

– Therefore the number of suffix bits = 32 – 8 = 24.

– In order to obtain the network mask the prefix bits all set to 1s and the suffix bits all set to zero as shown in Fig. P. 12.5.3(a).



(G-1898) **Fig. P. 12.5.3(a)**

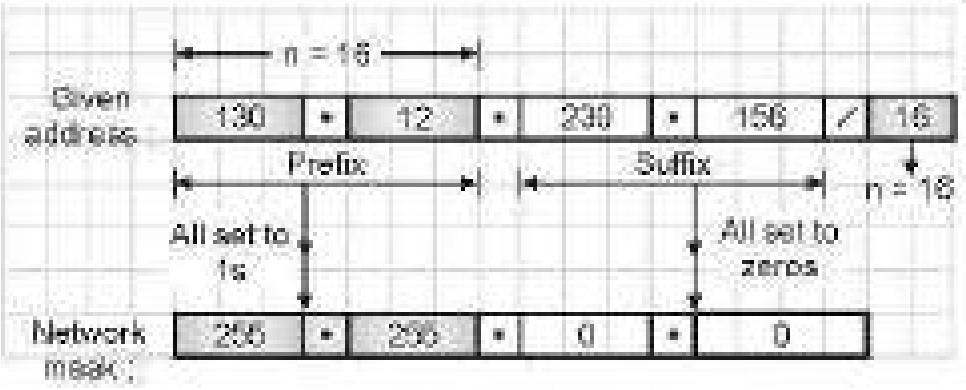
– Thus the network mask = 255.0.0.0

2. Classless CIDR Address : 130.12.230.156 / 16

– As per the slash notation, n = 16 i.e. number of prefix bits is 16.

– Number of suffix bits = 32 – 16 = 16.

– In order to obtain the network mask, set all the prefix bits to 1s and set all the suffix bits to 0s as shown in Fig. P. 12.5.3(b).



(G-1899) **Fig. P. 12.5.3(b)**

– Thus the network mask = 255.255.0.0

12.5.4 Extracting the Block Information :

– We can extract all the required information from the given classless address in the CIDR notation.

– The information that we can obtain is as follows :
1. The first address (network address)
2. The number of addresses.
3. The last address.

– We can obtain the number of addresses in a block as follows :

$$\text{Number of addresses in a block } N = 2^{(32-n)} \quad \ldots(12.5.1)$$

Where n = Number of prefix bits.

– The first address or network address in block can be obtained by ANDing the address with the network mask.

First address = (Any address) AND (Network mask)

...(12.5.2)

– OR what we can do is keep the 'n' leftmost bits of any address as it is and set the remaining (32-n) bits to 0s.

– This is equivalent to the ANDing operation mentioned above.

– In order to obtain the last address in the block we have to add the first address with the number of addresses in the block directly.

∴ Last address = First address + Number of addresses in the block ...(12.5.3)

– It is also possible to obtain the last address by ORing the address with complement of the network mask.

∴ Last address = (Any address) OR [NOT (Network Mask)]

...(12.5.4)

– One more way of obtaining the last address of the block is to keep all the "n" left most bits (prefix bits) as it is and set all the (32-n) bits (suffix bits) to 1s.

Ex. 12.5.4 : If an address in a block is given in CIDR classless notation as 64.32.16.8 / 27 then find the following :

1. Number of addresses in the block (N)
2. The first address and 3.The last address.

Soln. :

Step 1 : Find n :

Given address = 64.32.16.8 / 27

Hence n = 27 from the slash notation.

∴ n = 27 bits.

∴ Prefix bits = 27, suffix bits = 32 – 27 = 5

Step 2 : Number of addresses in the block (N) :

$$N = 2^{(32-n)} = 2^5 = 32$$

Step 3 : Find the first address :

– Refer Fig. P. 12.5.4(a) to obtain the first address in the block. For this we have to AND the given address with the network mask.

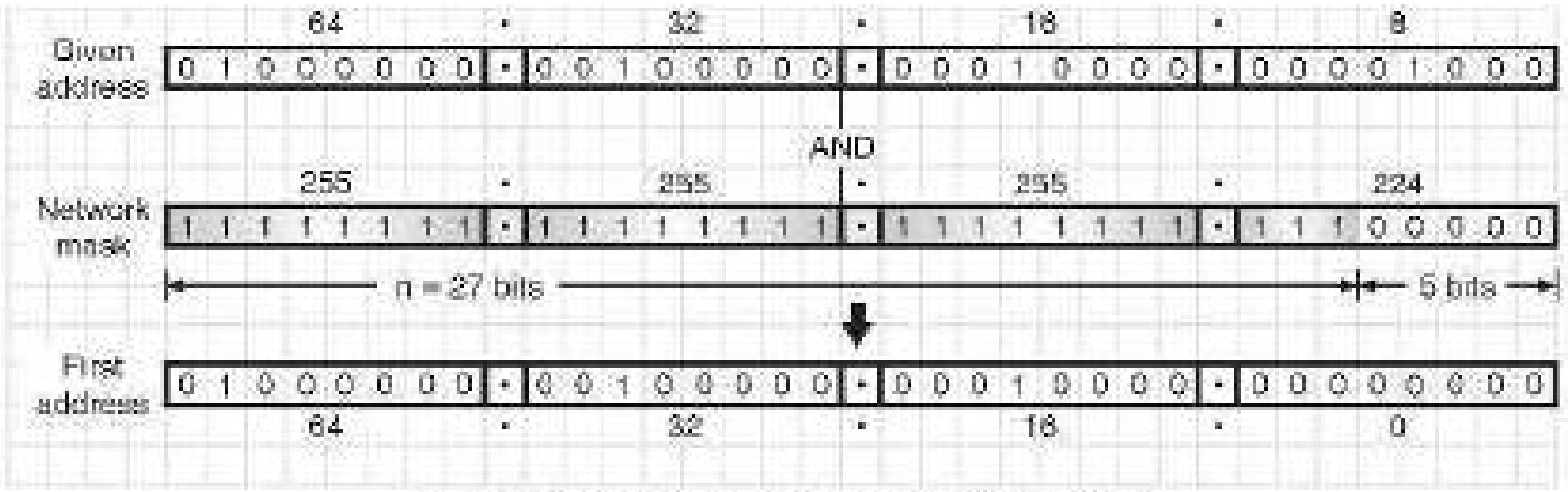
	n	(32 – n)
Network mask =	27 ones	5 zeros

∴ Network mask = 255.255.255.224

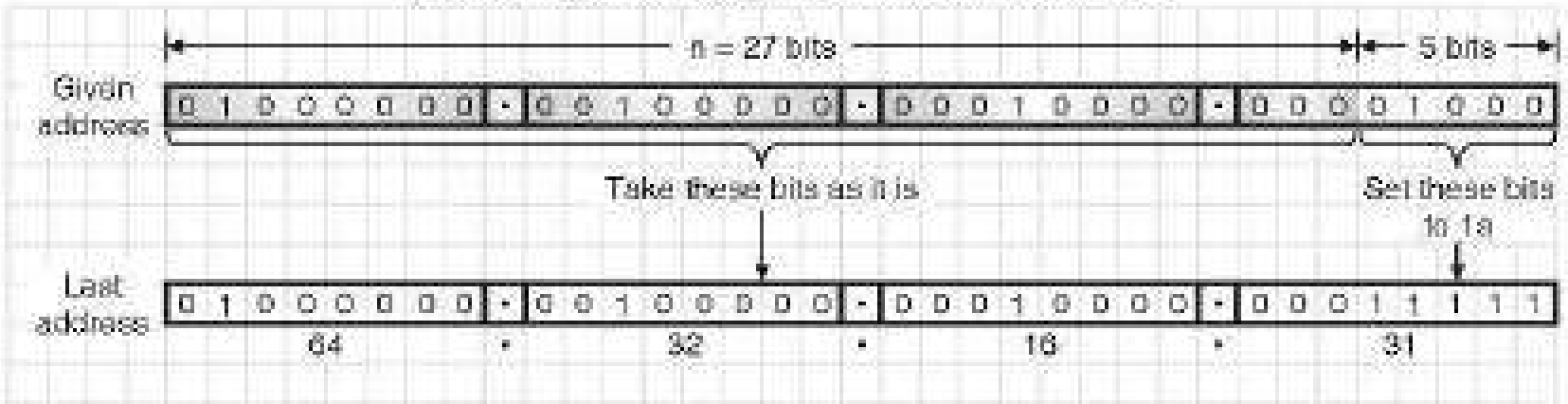
– For ANDing write the given address and network mask in their binary notations as shown in Fig. P. 12.5.4(a).

∴ From Fig. P. 12.5.4(a) we get the first address in the block as :

First address = 64.32.16.0 **...Ans.**



(G-1810) **Fig. P. 12.5.4(a) : First address in the block**



(G-1811) **Fig. P. 12.5.4(b) : Last address**

Step 4 : Find the last address :

– To obtain the last address in the block, we have to keep the left most 27 bits in the given address as it is and set the remaining 5 bits to 1s as shown in Fig. P. 12.5.4(b).

– ∴ From Fig. P. 12.5.4(b) we get the last address in the block as follows :

Last address = 64.32.16.31

Ex. 12.5.5 : For the classless address 129.65.33.01 / 24 find the following :

1. Number of addresses in the block (N)
2. The first address.
3. The last address.

Soln. :

Step 1 : Find n :

Given address = 129.65.33.01 / 24 hence n = 24 from the slash notation.

$\therefore$ n = 24 bits

$\therefore$ Prefix bits = 24, suffix bits = 32 – 24 = 8

Step 2 : Number of addresses in the block (N) :

$$N = 2^{(32-n)} = 2^8 = 256 \quad \text{...Ans.}$$

Step 3 : Find the first address :

– Refer Fig. P. 12.5.5(a) to obtain the first address in the block. For this we have to AND the given address with the network mask.

Address :	AND	1	2	9	.	6	5	.	3	3	.	0	1
Network mask :		2	5	5	.	2	5	5	.	2	5	5	.	0
First address (AND)		1	2	8	.	6	5	.	3	3	.	0

(G-1812) **Fig. P. 12.5.5(a) : First address in the block**

	n	(32 – n)
Network mask =	24 ones	8 zeros

$\therefore$ Network mask = 255.255.255.0

– For ANDing write the given address and network mask in their dotted decimal notations as shown.

– $\therefore$ From Fig. P. 12.5.5(a) we get the first address in the block as :

First address = 129.65.33.0 **...Ans.**

Step 4 : Find the last address :

– To obtain the last address in the block, we have to keep the left most 24 bits in the given address as it is and set the remaining 8 bits to 1s as shown in Fig. P. 12.5.5(b).

Address :	1	2	9	.	6	5	.	3	3	.	0	1
					As it is						Set to 1	
Last address :	1	2	9	.	6	5	.	3	3	.	255

(G-1813) **Fig. P. 12.5.5(b) : Last address in the block**

– From Fig. P. 12.5.5(b) we get, the last address in the block is as follows :

Last address = 129.65.33.255 **...Ans.**

12.5.5 Block Allocation :

– Now let us understand how to allocate the blocks in the classless addressing. The global authority for the block allocation is ICANA means Internet Corporation for Assigned Names and Addresses.

– But the individual addresses of the Internet users is not allotted by the ICANA. Instead ICANA will assign large blocks of addresses to various ISPs or large organizations. These ISPs or organization will assign addresses to the individual Internet users from their allotted blocks.

Restrictions :

– Some of the restriction on classless address blocks have been imposed by the internet authorities in order to simplify the process of address handling.

1. The addresses in a block should be continuous, i.e. serial in manner.
2. The total number of addresses in a block has to be equal to some power of 2 i.e. 2^1, 2^2, 2^3 ...etc.
3. The first address should be evenly divisible by the number of addresses.

12.5.6 Relation to Classful Addressing :

– The classful addressing may be imagined as the special case of classless addressing such that the blocks of addresses in class A, B and C type addresses will have the prefix lengths $n_A = 8$, $n_B = 16$ and $n_C = 24$.

– Table 12.5.1 lists the prefix lengths for class A to F classful addresses and using this information we can change a block in classful addressing to a block in classless addressing.

Table 12.5.1 : Prefix lengths for classful addressing

Class	Prefix length	Class	Prefix length
A	/ 8	D	/ 4
B	/ 16	E	/ 4
C	/ 24		

12.5.7 Subnetting :

– The concept of subnetting in classless addressing domain is similar to that discussed for the classful addressing.

– The subnetting is used for creating a three level hierarchy in the classless addressing domain.

– An organization or an ISP have a block of addresses granted to them.

– It can divide these addresses into several subgroups and each subgroup of addresses is assigned to a **subnetwork or subnet.**

– The subnetworks may be subdivided further if the organization want it that way.

12.5.8 Designing Subnets :

Let N = Total number of addresses granted to an organization.
n = Prefix length
N_{sub} = Assigned number of addresses to each subnetwork
n_{sub} = Prefix length for each subnetwork
S = Total number of subnetworks.

- Now follow the steps given below to ensure that the subnetworks operate properly.

Steps to follow :

- The number of addresses in each subnetwork should always be equal to a power of 2. I.e. 2^0, 2^1, 2^2....etc.
- We can use the following expression to find the prefix length of each sunetwork.

$$n_{sub} = n + \log_2 \left[\frac{N}{N_{sub}}\right] \quad ...(12.5.5)$$

- The starting address in each subnet should be divisible by the number of addresses in that subnework. To achieve this we need to first assign address to larger networks.

Note : These restrictions are similar to those applied when addresses to network were allocated.

12.5.9 Finding Information about Each Network :

- After designing the subnetworks, we can find the information about the subnets such as starting and last addresses, we can use the same procedure that was used to find the information about each network in the Internet.

Ex. 12.5.6 : A block of addresses granted to an ISP is given by 130.34.13.64 / 26. These addresses are to be divided into four subnetworks with equal number of hosts. Design the subnetworks and obtain all the information about each subnet.

Soln. :

Step 1 : Find total number of addresses (N) :

- From the given address we get n = 26 (prefix length).
- Hence the number of addresses in the whole network will be :

$$N = 2^{(32-n)} = 2^{(32-26)} = 2^6 = 64$$

- The first address in this block will be 130.34.13.64 / 26 whereas the last address will be 130.34.13.127 / 26.
- These values have been obtained using the procedure that we have discussed earlier.

Subnet design :

Step 2 : Find number of hosts per subnetwork :

- There are four subnetworks with equal number of guests.

∴ Number of hosts per subnetwork is given by,

$$N_1 = N_2 = N_3 = N_4 = \frac{N}{4} = \frac{64}{4} = 16 \quad \textbf{...Ans.}$$

- Note that the first requirement that 64 / 16 should be a power of 2 has been satisfied here.

Step 3 : Find the prefix lengths of the subnets :

- The prefix lengths of the four subnets are given by,

$$n_1 = n_2 = n_3 = n_4 = n + \log_2 \left[\frac{N}{N_{sub}}\right]$$

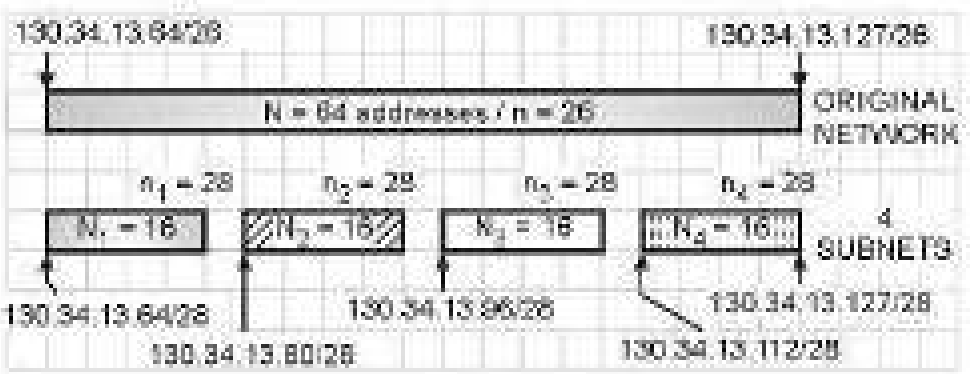
$$= 26 + \log_2 \left[\frac{64}{16}\right]$$

$$= 26 + \log_2 4$$

∴ $n_1 = n_2 = n_3 = n_4 = 28$ **...Ans.**

Step 4 : Starting and ending addresses of all the subnets :

- Refer Fig. P. 12.5.6 which shows all the starting and ending addresses of the 4-subnets.



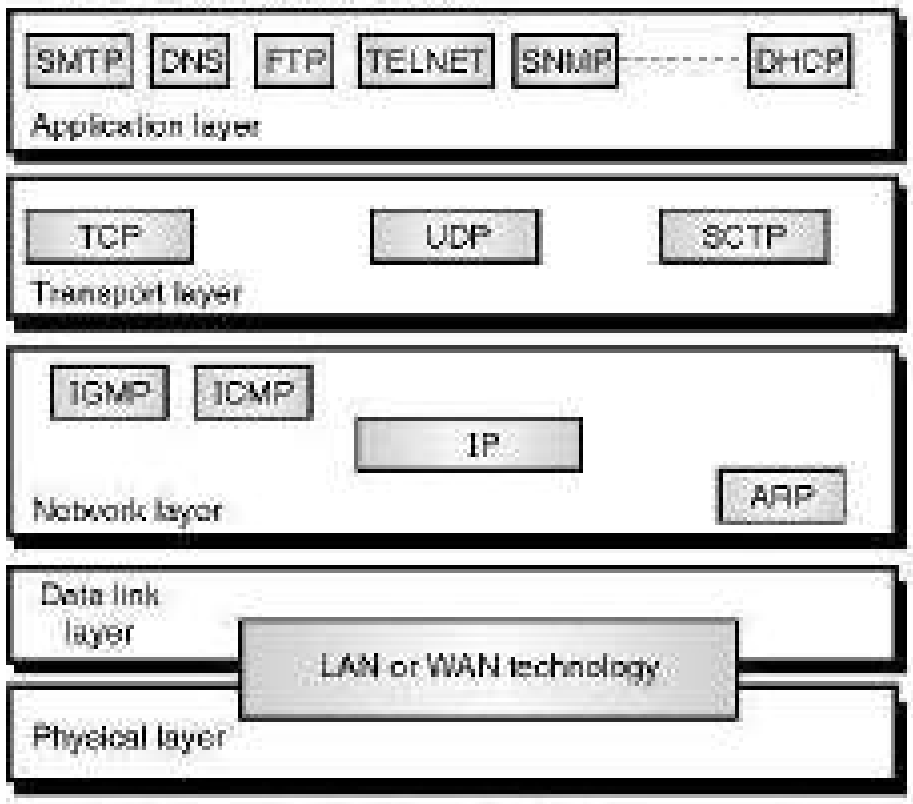
(6-1814) **Fig. P. 12.5.6**

- It should be noted from Fig. P. 12.5.6 that all the starting addresses should be divisible by the number of addresses in the subnet i.e. by 16.

12.6 Network Layer Protocols :

- The main protocols corresponding to the network layer in the TC/IP suite as well as Internet layer are : ARP, IP, ICMP and IGMP.
- Out of these protocols the network layer in version 4 is main protocol and other three are auxiliary protocols.

- The responsibility of main protocol i.e. **Internet protocol version 4** is packetizing, forwarding and packet delivery at the network layer.
- **ICMPv4** (Internet control message protocol) helps (Internet protocol version 4 (IPv4) for handling the errors which can occur in the network layer delivery.
- To help IPv4 in multicasting, **IGMP** (Internet group management protocol) is used.
- In mapping of network layer addresses to link layer addresses **ARP** (address resolution protocol) is used to join the network and data link layers.
- Fig. 12.6.1 shows the position of network layer protocols in the TCP/IP protocol suite.



(G-2234) **Fig. 12.6.1 : Position of network layer protocols in TCP/IP protocol suite**

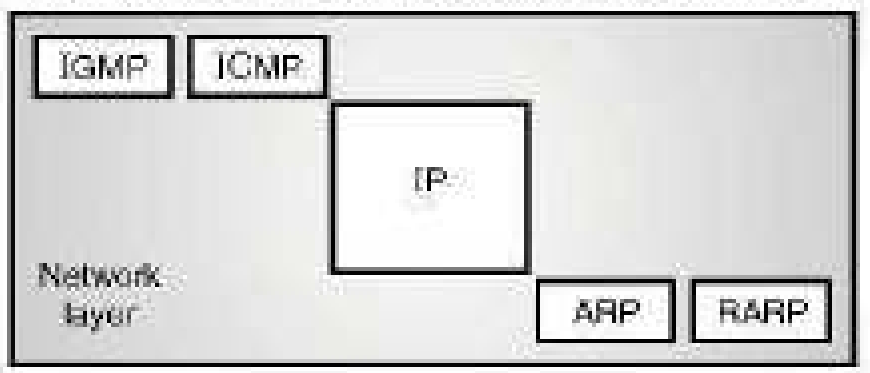
- IPv4 is connectionless and unreliable datagram protocol. It is also known as **best-effort delivery service.**
- The meaning of best-effort is that IPv4 packet can be lost, corrupted, arrive out of order or delayed and IPv4 can create network congestion.
- For reliability there should be pairing of IPv4 with a reliable transport layer protocol (e.g. TCP).
- To know the concept of best effort delivery we can take an example of post office.
- To deliver the regular mail, the post office does its best but it will not succeed always.
- In case of loss of unregistered letter, the post office will not take responsibility. To find out the loss and solve the problem is upto the sender or would-be recipient.
- The post office will not take any record or track of letter and in case of loss or damage it cannot send any notification to a sender.
- For packet switched network IPv4 is a connectionless protocol which uses datagram approach.
- That means, handling of each datagram is independent and to the destination each datagram can follow a different route.
- This implies that datagram could arrive out of order if it is sent by the same source to the same destination.
- During transmission also some datagram could be lost or corrupted.
- To handle and to take care of all these problems, IPv4 relies on a high-level protocol.

12.7 Internet Protocol Version 4 (IPv4) :

- We have already discussed the addressing mechanism, delivery and forwarding for the IP packets.
- Now we will discuss the format of IP packet in the next few sections.
- In the discussion we will see that an IP packet consists of a base header and options which are sometimes useful in controlling the packet delivery.

12.7.1 Position of IP :

- The main protocols corresponding to the network layer in the TCP/IP suite as well as Internet layer are : ARP, RARP, IP, ICMP and IGMP. This is as shown in Fig. 12.7.1.



(G-524) **Fig. 12.7.1 : Protocols at network layer**

- Out of these protocols IP is the most important protocol.
- It is responsible for host to host delivery of datagrams from a source to destination. But IP needs to take services of other protocols.
- IP takes help from ARP in order to find the MAC (physical) address of the next hop.

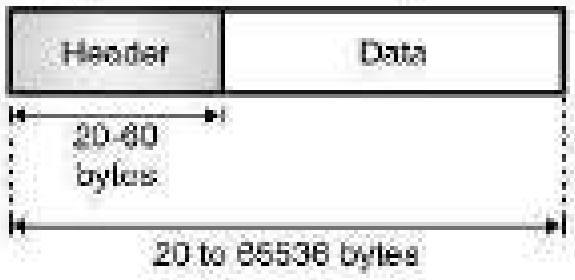
- IP uses the services of ICMP during the delivery of the datagram packets to handle unusual situations such as presence of an error.
- IP is basically designed for unicast delivery. But some new Internet applications as well as multimedia need multicast delivery.
- So for multicasting, IP has to use the services of another protocol called IGMP.
- IPv4 is the current version of IP whereas IPv6 is the latest version of IP.

12.7.2 Internet Protocol (IP) :

- The Internet Protocol is the host to host delivery protocol which belongs to the network layer and is designed for the Internet.
- IP is used as the transmission mechanism by the TCP / IP protocols.
- That means the TCP or UDP packets are encapsulated in the IP packet and the IP carries it from source to destination.
- IP is a connectionless datagram protocol with no guarantee of reliability.
- It is an unreliable protocol because it does not provide any error control or flow control.
- IP can only detect the error and discards the packet if it is corrupted.
- If IP is to be made more reliable, then it must be paired with a reliable protocol such as TCP at the transport layer.
- Each IP datagram is handled independently and each one can follow a different route to the destination.
- So there is a possibility of receiving out of order packets at the destination. Some packets may even be lost or corrupted.
- IP relies on a higher level protocol to take care of all these problems.
- The version of IP that we are going to discuss is called as IPv4 i.e. IP version 4.
- IP is also called as a **best effort delivery protocol.** The meaning of the term best effort delivery is that the IP packet can get lost or corrupted or delayed.
- They may arrive out of order at the destination or may create congestion in the network.

12.7.3 Datagrams :

- Packets in IP layer are called datagrams. Fig. 12.7.2 shows the typical format of an IP packet.

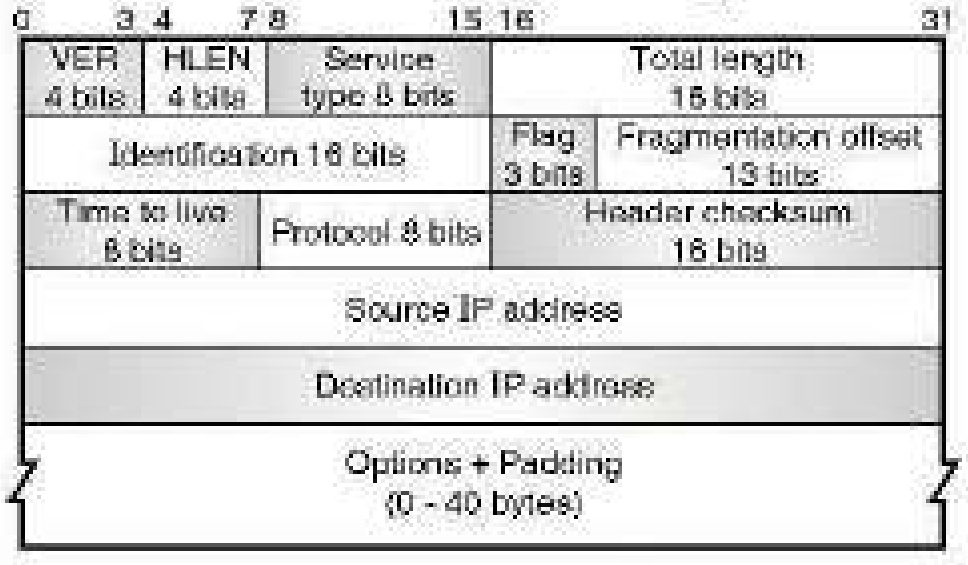


(G-525) **Fig. 12.7.2 : IPv4 datagram format**

- A datagram has two parts namely the header and data as shown.
- The length of datagram is not fixed. It varies from 20 bytes to 65536 bytes.
- The length of the header is 20 to 60 bytes. The information necessary for the routing and delivery of the datagram has been stored in the header.
- The other part of the datagram is the data field which is of variable length.
- It is a custom in TCP/IP to show the header in 4-byte (32 bit) sections.

12.7.4 IPv4 Header Format :

- The IP frame header contains routing information and control information associated with datagram delivery. The IP header structure is as shown in Fig. 12.7.3.



(G-2082) **Fig. 12.7.3 : IPv4 header format**

- Various fields in the header format are as follows :

1. VER (Version) :

- This is a 4 bit field which is used to define the version of IP protocol. The current version of IP is 4 i.e. IPv4 but in future it may be completely replaced by the latest version of IP i.e. IPv6.

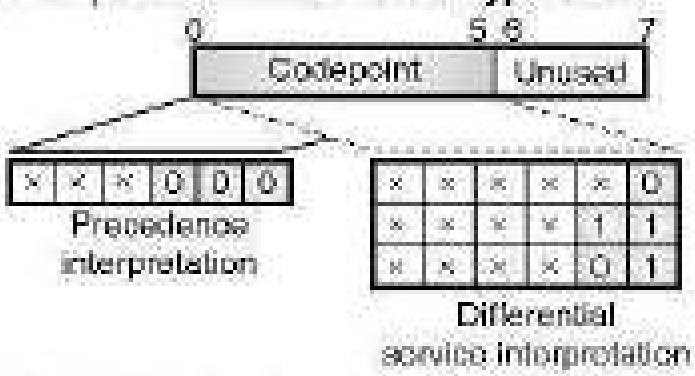
- This field will indicate the IP software running on the processing machine that this datagram belongs to IPv4 version.
- If the processing machine is using some other version of IP, then the datagram will be discarded.

2. HLEN (Header length) :

- This 4-bit long field is used for defining the length of the datagram header in 4-byte words.
- The value of this field is multiplied by 4 to get the length of the IPv4 header which varies between 20 and 60 bytes.
- When there are no options, the value of this field is 5 and the **header length** is 5 × 4 = 20 bytes.
- When the value of option field is maximum the value of HLEN field is 15 and the corresponding header length is maximum i.e. 15 × 4 = 60 bytes.

3. Service type :

- In the earlier designs of IP header, this field was called as **Type of Service (TOS)** field and its job was to define how the datagram should be handled.
- At that time, a part of this field used to define the precedence of datagram and the remaining part used to define the type of service out of different possible services such as low delay, high throughput etc.
- But now the interpretation of this field has been changed by IETF. This field is now supposed to define a set of **differential services.** Fig. 12.7.4 illustrates the new interpretation of the **service type** field.



(G-2083) **Fig. 12.7.4 : New interpretation of service type field**

- As seen in Fig. 12.7.4, in the new interpretation, the service type field is divided into two subfields namely, the 6 bit **codepoint** subfield and a 2 bit **unused** subfield.
- We can use the 6-bit **codepoint** subfield in two different ways, as follows :
  1. For the purpose of precedence interpretation.
  2. For the differential service interpretation.

Precedence interpretation :

- If the three right most bits are zeros, then the three leftmost bits are interpreted the same as the precedence bits in the service field (old interpretation).
- That means it is compatible with the old interpretation of this field.
- The precedence interpretation is used for defining the priority level of this datagram (from 0 to 7) in the situations like congestion.
- In the event of congestion, the datagrams with lowest precedence (0) will be discarded first.

Differential service interpretation :

- When the three rightmost bits are not all zeros, the 6 bit codepoint subfield is used for differential service interpretation.
- In that case these 6 bits can be used for defining a total of 56 (64 – 8) services, on the basis of the priorities assigned by the Internet or local authorities as per Table 12.7.1.

Table 12.7.1 : Values of codepoints

Category	Codepoint	Assigning authority
1.	× × × × × 0	Internet
2.	× × × × 1 1	Local
3.	× × × × 0 1	Temporary or Experimental

- The first, second and third categories contain 24, 16 and 16 service types respectively.
- The Internet authorities assign the first category. The local authorities assign the second while the third one is temporary and can be used for experimental purposes.

4. Total length :

- This 16 bit field is used to define the total length of the IP datagram.
- The total length includes the length of header as well as the data field.
- The field length of this fields is 16 bits so the total length of the IP datagram is restricted to $(2^{16} - 1)$ = 65535 bytes out of which 20 to 60 bytes constitute the header and the remaining bytes are reserved to carry data from upper layers.

- This field allows the length of a datagram to be upto 65,535 bytes, although such long datagrams are impractical for most hosts and networks.
- All hosts must be prepared to accept datagram of upto 576 bytes, regardless of whether they arrive whole or in the form of fragments.
- The hosts are recommended to send datagram larger than 576 bytes only if the destination is prepared to accept larger datagram.
- We can find the length of data by subtracting the header length from the total length.
- As stated earlier the header length can be obtained by multiplying the contents of HLEN field by four.

  ∴ Length of data = Total length – header length
- The total length (maximum value) of 65,535 bytes might seem to be large but in future the size of IP datagram is likely to increase further because the improvement in technology will allow more bandwidth.

Why do we need the total length field ?

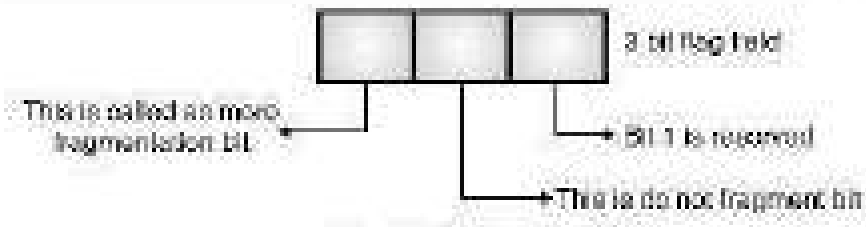
- We might feel that the **total length** field is not at all required because the host or router will drop the header and trailer when it receives a frame.
- Then why to include this field ?
- The answer to this question is that in many situations we do not need this field at all.
- But in some special situations, only the datagram is not encapsulated in the frame but there are some padding bits as well that are included.
- In such situations, the machine (host or router) that decapsulates the datagram, needs to check the **total length** field so as to understand how much is the data and how much is the padding ?

5. **Identification :**

- This field is used to identify the datagram originating from the source host.
- When a datagram is fragmented, the contents of the identification field get copied into all fragments.
- This identification number is used by the destination to reassemble the fragments of the datagram.

6. **Flags :**

- **Flags :** This is a three bit field. The 3 bits are as shown in Fig. 12.7.5.

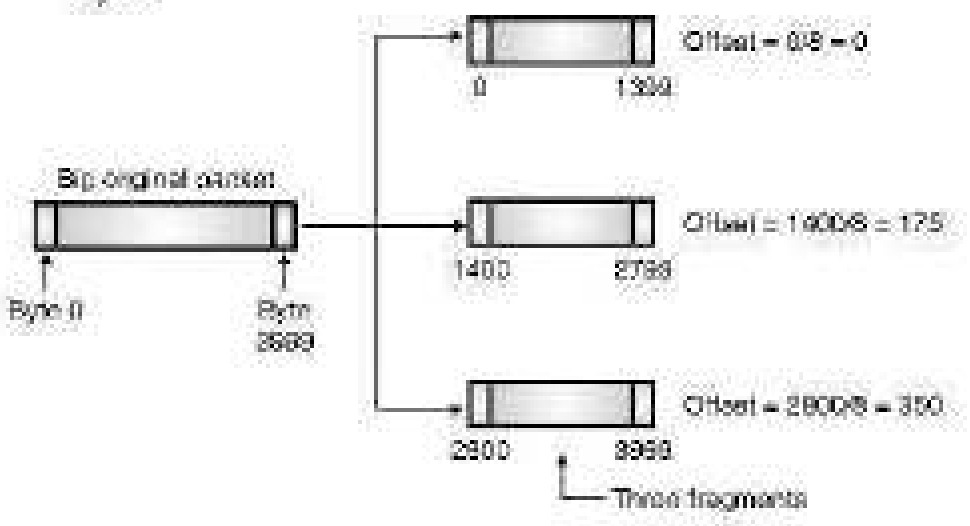


(G-527) **Fig. 12.7.5 : Flag bits**

- First bit is reserved, and it should be 0.
- The second bit is known as the "Do Not Fragment" bit. If this bit is "1" then machine understands that the datagram is not to be fragmented.
- But if the value of this bit is 0 then the machine should fragment the datagram if and only if necessary.
- The third bit is known as "More Fragment Bit" (M). M = 1 indicates that the datagram is not the last fragment and M = 0 indicates that this is the last or the only fragment.

7. **Fragmentation offset :**

- This is a 13 bit field which is used to indicate the relative position of this fragment with respect to the complete datagram.
- It is the offset of the data in the original datagram measured in units of 8 bytes.
- To understand this refer Fig. 12.7.6.
- The original IP packet (datagram) contains 4000 bytes numbered from 0 to 3999. It is fragmented into three fragments.
- The first fragment contains 1400 bytes numbered from 0 to 1399.
- The offset for this fragment is 0/8 = 0. Similarly the offsets for the other two fragments are 1400/8 = 175 and 2800/8 = 350 respectively as shown in Fig. 12.7.6.
- The offset is measured in units of 8 bytes. Because the length of the offset field is 13 bits, so the fragments should be of size such that first byte number is divisible by 8.



(G-528) **Fig. 12.7.6 : Example of fragmentation**

8. Time to Live (TTL) :

- This is an 8-bit field which controls the maximum number of routers visited by the datagram during its lifetime.
- A datagram has a limited lifetime for travelling through an Internet.
- Originally the TTL field was designed to hold the **timestamp.** This timestamp value was decremented by one, everytime the datagram visits a router.
- As soon as the timestamp value reduces to zero the datagram is discarded. But for this scheme to become successful, all the machines must have synchronized clocks and they must know the time taken by a datagram to travel from one router to the other.
- Today the TTL field is used to **control** the maximum number of hops i.e. router by a datagram.
- At the time of sending a datagram, the source host will store a number in the TTL field. This number is approximately twice the maximum number of routers present between any two hosts.
- Everytime this datagram visits a router, this value is decremented by one. If after decrementing, the value of TTL field reduces to zero then that router discards the datagram.

Need of TTL field :

- Sometimes the routing tables in the Internet get corrupted, due to which a datagram may travel between two or more routers for a very long time but never ever gets delivered to the destination host.
- The TTL field is needed in such situations for **limiting the lifetime of a datagram.**
- The TTL field is also used to **limit the journey of a packet intentionally.** For example if a packet is to be confined to a local network only then a 1 is stored in the TTL field of this packet.
- As soon as it reaches the first router, then TTL field value is decremented from 1 to 0 and the packet will be discarded.

9. Protocol :

- This is an 8-bit field which is used for defining the higher level protocol which uses the services of IP layer.
- The data from different high level protocols can be encapsulated into an IP datagram. These protocols could be UDP, TCP, ICMP, IGMP etc.
- The protocol field contents would tell the name of the protocol at the final destination to which this IP datagram is to be delivered.
- At the destination, the value of this field helps in the process of demultiplexing.
- Table 12.7.2 shows some of the values of this field corresponding to different high level protocols.

Table 12.7.2

Value	Protocol	Value	Protocol
1	ICMP	17	UDP
2	IGMP	89	OSPF
6	TCP		

10. Header checksum :

- A checksum in IP packet covers on the header only. Since some header fields change, this field is recomputed and verified at each point that the Internet header is processed.

11. Source address :

- This field is used for defining the IP address of the source. It is a 32 bit field.

12. Destination address :

- This field is used for defining the IP address of the destination. It is also a 32 bit field.

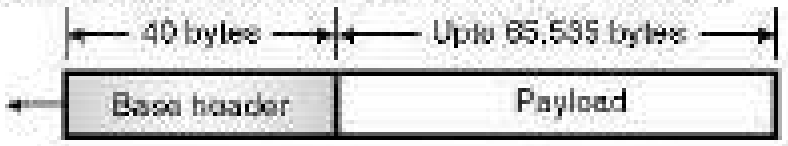
13. Options :

- Options are not required for every datagram. They are used for network testing and debugging.
- We have discussed all the options in detail, later in this chapter.

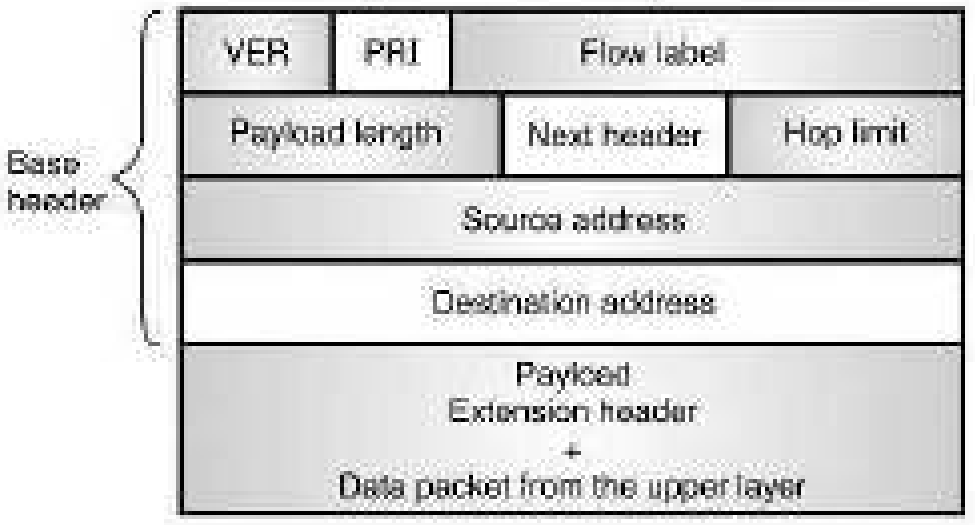
12.8 IPv6 Packet Format :

- Fig. 12.8.1(a) shows IPv6 packet. Fig. 12.8.1(b) shows the packet format (Base header) of IPv6. Each packet can be divided into two parts viz : base header and payload.
- Base header is the mandatory part and payload is an optional one. The payload follows the base header.
- The payload is made up of two parts.
  1. An optional extension headers.
  2. The upper layer data.

– The base header is 40 byte long whereas the payload consisting of the extension header and upper layer data can have information worth upto 65, 535 bytes.



(6-2245)**Fig. 12.8.1(a) : IPv6 packet**



(6-550) **Fig. 12.8.1(b) : Format of an IPv6 datagram (Base header)**

Base header :

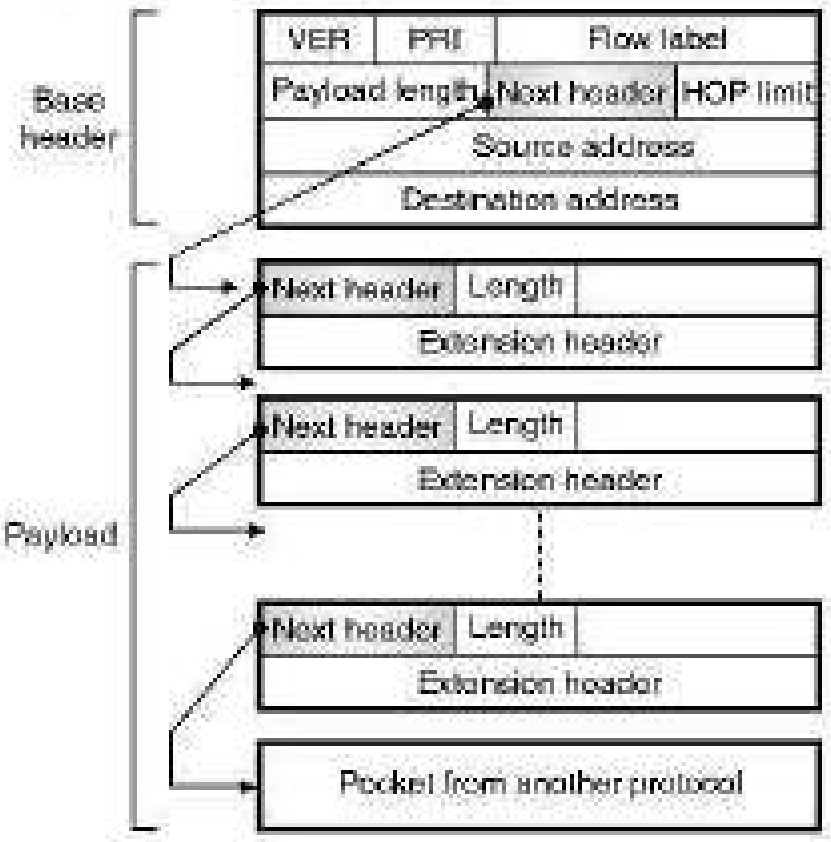
– Fig. 12.8.1(b) shows the base header. It has eight fields. These fields are as follows :

1. **Version (VER) :** The contents of this 4 bit field defines the version of IP such as IPv4 or IPv6. If VER = 6, then the version is IPv6.
2. **Priority :** This 4 bit field contents defines the priority of the packet which is important in connection with the traffic congestion.
3. **Flow label :** It is a 24 bit (3 byte) field which is supposed to provide a special handling for a particular flow of data.
4. **Payload length :** The contents of the 16 bit or 2 byte length field are used to indicate the total length of the IP datagram excluding the base header. That means it gives the length of only the payload part of the datagram.
5. **Next header :** It is an 8 bit field which defines the header which follows the base header in the datagram.
6. **Hop limit :** Contents of this 8 bit (1 byte) field have the same function as TTL (time to live) in IPv4.
7. **Source address :** It is a 16 byte (128 bit) Internet address which corresponds to the originator or source which has produced the datagram.
8. **Destination address :** This is a 16 byte (128 bit) internet address which corresponds to the address of the final destination of datagram. But this field will contain the address of the next router and not the final destination if source routing is being used.

12.8.1 Payload :

– The meaning and format of payload field in IPv6 is different as compared to payload field in IPv4.

– Fig. 12.8.2 shows payload field in IPv6.



(6-2246) **Fig. 12.8.2 : IPv6 payload**

– In IPv6, the payload is combination of zero or more extension headers (options) which is followed by data from other protocols such as UDP, TCP etc.

– In IPv4, option is a part of the header, whereas in IPv6 it is designed as extension headers.

– Depends on the situation the payload can have as many extension headers as required.

– Extension header is made up of two mandatory fields : next header and the length which is followed by information which is related to the particular option.

– Value of next header field i.e. code defines which type of the next header is (e.g. source routing options, fragmentation option etc.)

– The last next header describes the protocol which carries the datagram.

– Some next header codes are listed in Table 12.8.1.

Table 12.8.1 : Next header codes

Sr. No.	Code	Next header code
1.	00	HOP by hop option
2.	02	ICMPv6
3.	06	TCP
4.	17	UDP
5.	43	Source routing option
6.	44	Fragmentation option
7.	50	Encrypted security payload
8.	51	Authentication header
9.	59	Null (no next header)
10.	60	Destination option

12.8.2 IPv6 Addressing :

– IPv6 is the next generation Internet Protocol designed as the next step of the IP version 4. IPv6 was designed to enable high-performance and larger address space.

– This was achieved by overcoming many of the weaknesses of IPv4 protocol and by adding several new features.

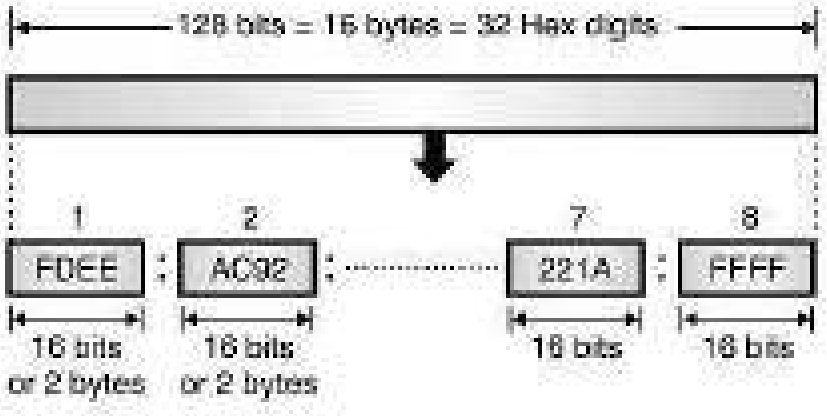
– The IPv6 was developed due to the address depletion of IPv4.

– The structure of IPv6 address is fundamentally different than that of IPv4. Therefore there is absolutely no possibility of address depletion taking place in future.

IPv6 Address :

– An IPv6 address is 128 bit long. It consists of 16 bytes as shown in Fig. 12.8.3.

– Thus the IPv6 address is 4 times longer than that of IPv4.



(a-545) **Fig. 12.8.3 : IPv6 address**

12.8.3 Notations :

– An address is stored in the computers in the binary form. But it is impossible for humans to handle a 128 bit binary address.

– Therefore many notations have been proposed to represent the IPv6 addresses, so that they become easier to handle for human beings.

– Some of the proposed notations are :

1. Dotted decimal notation.
2. Colon hexadecimal notation.
3. Mixed representation.
4. CIDR notation.

1. Dotted decimal notation :

– In order to maintain the compatibility with IPv4 addresses, We may feel tempted to use the dotted decimal notation.

– But practical observation is that this notation is convenient only for the 4 byte address of IPv4.

– It is not at all convenient for the 16 byte IPv6 addresses as it seems too long.

– Therefore this notation is very rarely used.

2. Colon hexadecimal notation :

– The 128 bit address can be made more readable and easy to handle. IPv6 has specified the **colon hexadecimal notation.**

– IPv6 uses a special notation called hexadecimal colon notation. In this, the total 128 bits are divided into 8 sections, each one is 16 bits or 2 bytes long.

– The 16 bits or 2 bytes in binary correspond to four hexadecimal digits of 4-bits each.

– Hence the 128 bits in hexadecimal form will have 8 × 4 = 32 hexadecimal digits.

– These are in groups of 4 digits as shown and every group is separated by a colon as shown in Fig. 12.8.4.

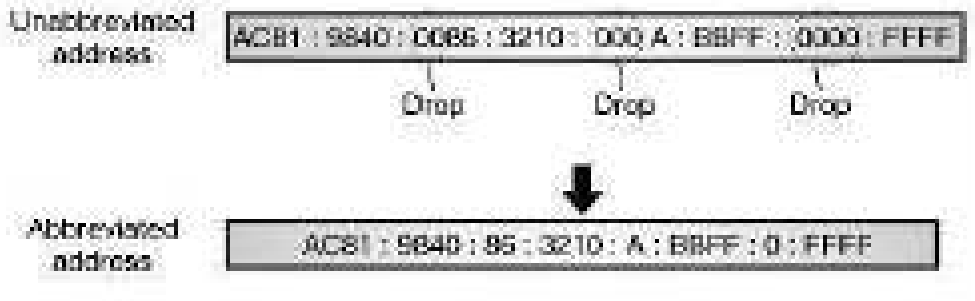
AC 81 : 9840 : 0086 : 3210 : 000A : BBFF : 0000 : FFFF

Fig. 12.8.4 : Colon hexadecimal notation

- IPv6 uses 128-bit addresses. Only about 15% of the address space is initially allocated, the remaining 85% being reserved for future use.
- These unused addresses may be used in the future for expanding the address spaces of existing address types or for totally new uses.

12.8.4 Abbreviation :

- The IPv6 address, in hexadecimal format contains 32 digits and it is very long.
- But in this address many hex digits are zero.
- We can take advantage of this to shorten the address by abbreviating it. A section corresponds to four digits between any two colons.
- The leading zeros in a section can be omitted to reduce the length of the address as shown in Fig. 12.8.5.

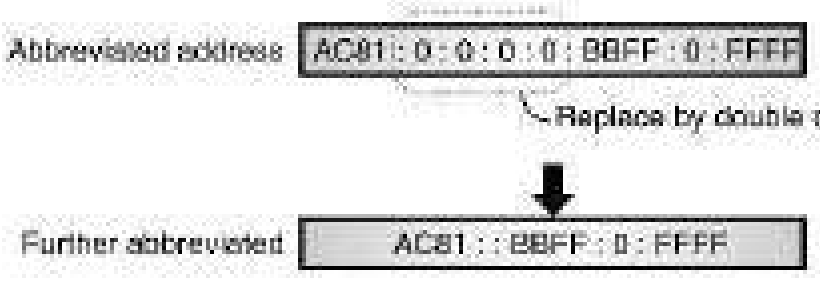


(G-546) **Fig. 12.8.5 : Abbreviated address**

- Note that only the leading zeros can be dropped but the trailing zeros can not be dropped.
- This is illustrated in Fig. 12.8.5. Thus due to abbreviation the length of the address has reduced to 24 hex digits from 32.

Further abbreviation :

- We can make further abbreviation if there are consecutive sections consisting of only zeros. This is known as **zero compression.**
- We can remove the zeros completely and replace them with double colon as shown in Fig. 12.8.6.



(G-547) **Fig. 12.8.6 : Further abbreviation (Zero compression)**

- This further abbreviation has reduced the address length to just 13 hex digits.
- It is important to note that abbreviation can be done only once per address.
- Also note that if there are two sets of zero sections, then only one of them can be abbreviated.

3. **Mixed representation :**

- Sometimes, the IPv6 address is represented using a mixed representation which combines the **colon hex** and **dotted decimal** notations.
- This notation is appropriate during the transition time during which an IPv4 address is being embedded in IPv6 address.
- In the mixed representation the rightmost 32 bits correspond to the IPv4 address Hence they are represented by the dotted decimal notation.
- Whereas the leftmost 96 bits (6 sections) are represented in colon hex notation.

4. **CIDR notation :**

- The type of addressing used in IPv6 is **hierarchical addressing.** Therefore IPv6 allows classless addressing and CIDR notation.
- Fig. 12.8.7 illustrates the CIDR address with a 60 bit prefix. It has been discussed later on in this chapter, how we can divide an IPv6 address into a prefix and a suffix.

(G-2132) **Fig. 12.8.7 : CIDR address**

Ex. 12.8.1 : IPv6 uses 16-byte addresses. If a block of 1 million addresses is allocated every picosecond, how long will be the addresses last ?

Soln. :

1. Total number of address bits = $16 \times 8 = 128$
2. Number of addresses = $2^{128} = 3.4 \times 10^{38}$
3. One picosecond = 1×10^{-12} seconds
4. 1 million addresses = 1×10^{6} address

$\therefore$ 1 picosecond = 1×10^{6} addresses

$\therefore x = 3.4 \times 10^{38}$

$\therefore x = \frac{3.4 \times 10^{38}}{1 \times 10^{6}} \times 1$ picoseconds

$= 3.4 \times 10^{32}$ picoseconds

$= 3.4 \times 10^{20}$ seconds

$= 9.44 \times 10^{16}$ hours

$= 3.9352 \times 10^{15}$ days

$= 1.0781 \times 10^{13}$ years

12.9 Comparison between IPv4 and IPv6 :

S-10, S-11, S-12, S-13, S-14, W-14, S-15, W-15, S-16, W-16, S-17, S-18, I-Scheme : W-19

MSBTE Questions

Q. 1 Compare IPv4 and IPv6. **(S-10, S-12, S-13, S-15, W-15, S-17, 4 Marks)**

Q. 2 Compare IPv6 and IPv4 protocols. **(S-11, 4 Marks)**

Q. 3 Compare IPv4 and IPv6 (four points). **(S-14, W-14, S-18, 4 Marks)**

Q. 4 Differentiate between IPv4 and IPv6. (two points) **(S-16, 2 Marks)**

Q. 5 Differentiate IPv4 and IPv6. **(W-16, 4 Marks)**

IPv4	IPv6
In IPv4 there are only 2^{32} possible ways to represent the address (about 4 billion possible addresses)	In IPv6 there are 2^{128} possible way (about 3.4×10^{38} possible addresses)
The IPv4 address is written by dotted-decimal notation, e.g. 121.2.8.12	IPv6 is written in hexadecimal and consists of 8 groups, containing 4 hexadecimal digits or 8 groups of 16 bits each, e.g. FABC: AC77: 7834:2222:FACB: AB98: 5432:4567.
The basic length of the IPv4 header comprises a minimum of 20 bytes (without option fields). The maximum total length of the IPv4 header is 60 bytes (with option fields), and it uses 13 fields to identify various control settings.	The IPv6 header is a fixed header of 40 bytes in length, and has only 8 fields. Option information is carried by the extension header, which is placed after the IPv6 header.
IPv4 header has a checksum, which must be computed by each router	IPv6 has no header checksum because checksums are, for example, above the TCP/IP protocol suite, and above the Token Ring, Ethernet, etc.
IPv4 contains an 8-bit field called Service Type. The Service Type field is composed of a TOS (Type of Service) field and a procedure field.	The IPv6 header contains an 8-bit field called the Traffic Class Field. This field allows the traffic source to identify the desired delivery priority of its packets
The IPv4 node has only Stateful auto-configuration.	The IPv6 node has both a stateful and a stateless address autoconfiguration mechanism.
Security in IPv4 networks is limited to tunneling between two networks	IPv6 has been designed to satisfy the growing and expanded need for network security.
Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length.
IPsec support is optional.	IPsec support is required
No identification of packet flow for QoS handling by routers is present within the IPv4 header.	Packet flow identification for QoS handling by routers is included in the IPv6 header using the Flow Label field.

IPv4	IPv6
Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IPv4 address to a link layer address.	ARP Request frames are replaced with multicast Neighbour Solicitation messages.
Must be configured either manually or through DHCP.	Does not require manual configuration or DHCP.
ICMP Router Discovery is used to determine the IPv4 address of the best default gateway and is optional	ICMP Router Discovery is replaced with ICMPv6 Router Solicitation and Router Advertisement messages and is required.
Header includes options	All optional data is moved to IPv6 extension headers.

Review Questions

Q. 1 Write a note on IP.

Q. 2 What is the name of a packet in IP ?

Q. 3 Explain the IP header.

Q. 4 Compare IPv4 and IPv6

Q. 5 State limitations of IPv4.

Q. 6 Explain the addressing scheme in IPv4 and IPv6.

Q. 7 Given an IP address, how will you extract its net id and host id.

Q. 8 What is subnetting in IP network, explain with suitable examples.

Q. 9 A network on the Internet has a subnet mask of 255.255.240.0. What is the maximum number of hosts it can handle ?

12.10 I-Scheme Solved Examples :

Ex. 12.10.1 : Your company has the network id 165.130.0.0. You are responsible for creating subnets on the network, and each subnet must provide at least 1000 host ids.
What subnet mask meets the requirement for the minimum number of host ids and provides the highest number of subnets ?

S-19, 6 Marks

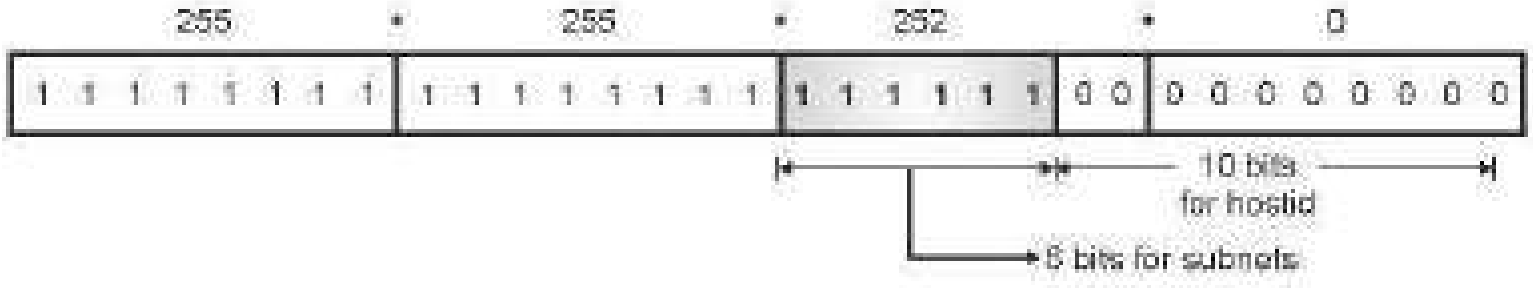
Soln. :

Given : Network id = 165.130.0.0
Each subnet should have at least 1000 hosts.

To Find : Subnet mask.

- **Type of network :** From network id, since the first byte is between 128 and 191. Hence this is a class B network with a 16 bits network id, and a 16 bit host id as shown in Fig. P. 12.10.1(a).
- Therefore total number of hosts = $2^{16} - 2 = 65,534$. As we want to have at least 1000 hosts per subnet, it is necessary to have 10 bits reserved for host id because $2^{10} = 1024$.
- The remaining 6 MSB bits out of 16 host id bits will be made 1 as shown in Fig. P. 12.10.1(b)
- Hence there will be $2^6 = 64$ subnets.
- The required subnet mask = 255. 255. 252. 0 as shown in Fig. P. 12.10.1(b).

(L-928) **Fig. P. 12.10.1(a) : Class B address**



(L-929) **Fig. P. 12.10.1(b) : Subnet mask**

12.11 I-Scheme Questions and Answers :

Summer 2019 [Total Marks - 10]

Q. 1 Describe types of IP address classes. **(Section 12.3.2)** **(4 Marks)**

Q. 2 Your company has the network id 165.130.0.0. You are responsible for creating subnets on the network, and each subnet must provide at least 1000 host ids. What subnet mask meets the requirement for the minimum number of host ids and provides the highest number of subnets ? **(Ex. 12.10.1)** **(6 Marks)**

Winter 2019 [Total Marks - 08]

Q. 3 List classes of IP addressing with their IP address range. **(Section 12.3.2)** **(2 Marks)**

Q. 4 Compare IPv4 and IPv6 (Any four points). **(Section 12.9)** **(4 Marks)**

Summer 2022 [Total Marks - 08]

Q. 5 List classes of IP addresses. **(Section 12.3.1)** **(2 Marks)**

Q. 6 Explain ARP, subnetting and supernetting with example. **(Sections 12.3.10 and 12.4.1)** **(6 Marks)**

❑❑❑