BALASORE SCHOOL OF ENGINEERING

BRANCH- CSE AND ETC

SUBJECT:- DC&CN

SUB.CODE:- TH-2

SEM:- 4TH

PREPARED BY:- PRIYANKA PANDA

SHUBHASHISH DAS

CHAPTER-1

2-marks

Q-1-What is peer-to-peer process?(2016-w-old)

Ans-In a PP 2network, the "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. In other words, each computer on a P2P network becomes a file server as well as a client.

Q-2-State the advantages of layering.(2016,2018-w-old)

Ans-Layered architecture also makes it possible to configure different levels of security to different components deployed on different boxesenables develop loosely coupled systems.

- Layered architecture increases flexibility, maintainability, and scalability.
- Different components of the application can be independently deployed, maintained, and updated, on different time schedules.

Q-3-Define protocol.what is FTP?(2016-2017-2018w-new)

Ans-FTP protocol is used for copying a file from one host to another.But it deals with the problem such as -Two system have different file name , directory structure and text formats..

Protocol-A network protocol defines rules and conventions for communication between network devices. Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received

5-marks

Q-1-Define networking.What are advantage ofnetworking?(2016-2017)

Ans-Networking refers to the total process of creating and using computer networks, with respect to hardware, protocols and software, including wired and wireless technology.

File Sharing-The major advantage of a computer network is that is allows file sharing and remote file access. A person sitting at one workstation that is connected to a network can easily see files present on another workstation, provided he is authorized to do so. This saves him/her the hassle of carrying a storage device every time data needs to be transported from one system to another. Further, a central database means that anyone on that network can access a file and/or update it. If files are

stored on a server and all of its clients share that storage capacity, then it becomes easier to make a file available to multiple users.

Resource Sharing- Resource sharing is another important benefit of a computer network. For example, if there are twelve employees in an organization, each having their own computer, they will require twelve modems and twelve printers if they want to use the resources at the same time. A computer network, on the other hand, provides a cheaper alternative by the provision of resource sharing. All the computers can be interconnected using a network, and just one modem and printer can efficiently provide the services to all twelve users.

Inexpensive Set-Up- Shared resources mean reduction in hardware costs. Shared files mean reduction in memory requirement, which indirectly means reduction in file storage expenses. A particular software can be installed only once on the server and made available across all connected computers

Flexible Handling - A user can log on to a computer anywhere on the network and access his files. This offers flexibility to the user as to where he should be during the course of his routine. A network also allows the network administrator to choose which user on the network has what specific permissions to handle a file. For example, the network administrator can allot different permissions to User A andUser B for File XYZ. According to these permissions, User A can read and modify File XYZ, but User B cannot modify the file. The permission set for User B is read-only. This offers immense flexibility against unwarranted access to important data.

Increased Storage Capacity-- Since there is more than one computer on a network which can easily share files, the issue of storage capacity gets resolved to a great extent. A standalone computer might fall short of storage memory, but when many computers are on a network, the memory of different computers can be used in such a case. One can also design a storage server on the network in order to have a huge storage capacity.at once. This saves the expense of buying and installing the same software as many times for as many users.

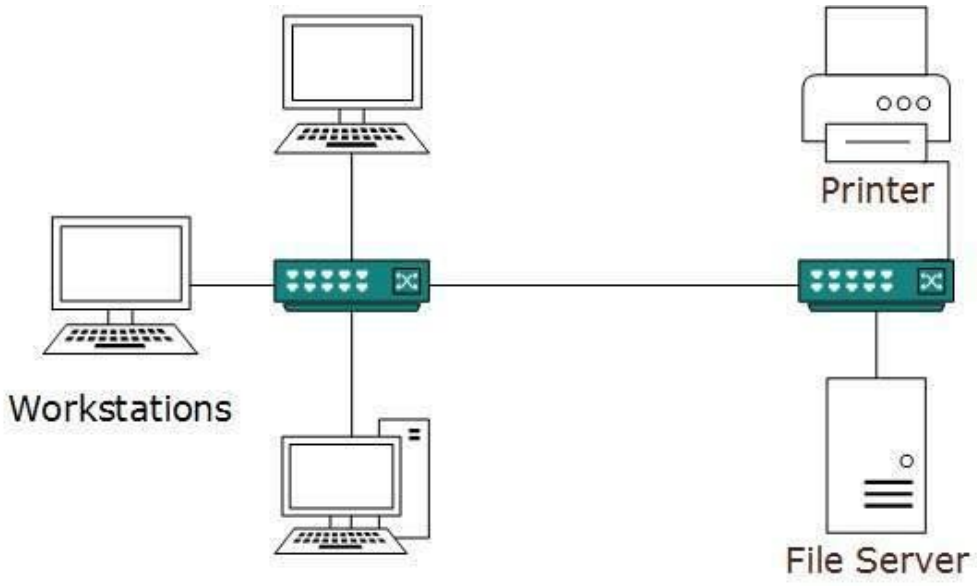
Q-2-Define network.Explain different types network?(2016,2017)

Ans-It is a collection of several computers and terminals and interconnected by oneor more than one transmission paths.

Local Area Network(LAN)

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

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



LANs are composed of inexpensive networking and routing equipment. It may contains local servers serving file storage and other locally shared applications. It mostly operates on private IP addresses and does not involve heavy routing. LAN works under its own local domain and controlled centrally.

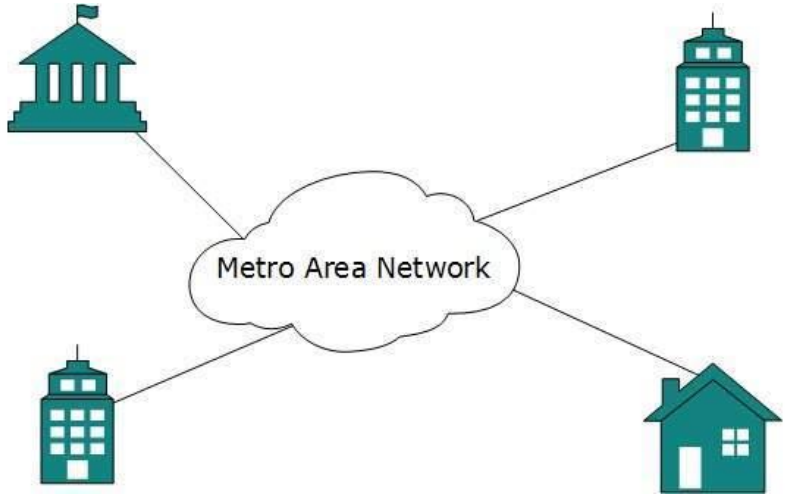
LAN uses either Ethernet or Token-ring technology. Ethernet is most widely employed LAN technology and uses Star topology, while Token-ring is rarely seen.

LAN can be wired,wireless, or in both forms at once.

Metropolitan Area Network(MAN)--

The Metropolitan Area Network (MAN) generally expands throughout a city such as cable TV network. It can be in the form of Ethernet,Token-ring, ATM, or Fiber Distributed Data Interface (FDDI).

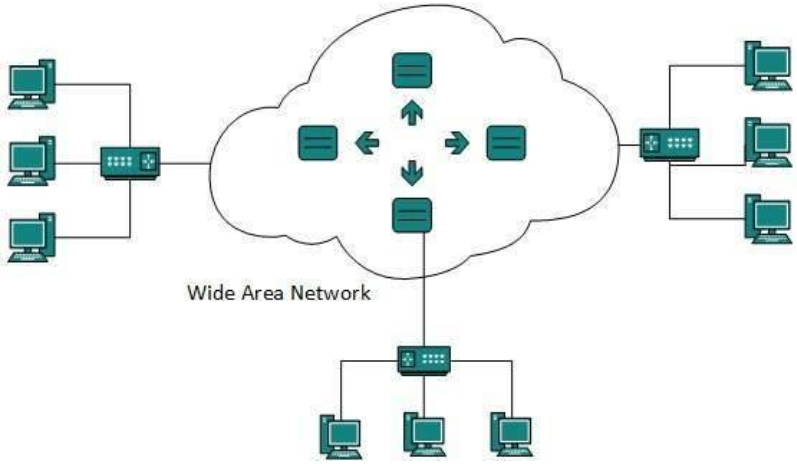
Metro Ethernet is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks. For example, MAN can help an organization to connect all of its offices in a city.



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

Wide Area Network(WAN)---

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



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

7-marks

Q-1-Explain 7 layers of OSI model.(2016(w)-2017(s))

Ans-The International Organization for Standardization (ISO) developed the Open Systems Interconnection (OSI) reference model in 1977 and finally 1983. It has since become the most widely accepted model for understanding network¬ communication Open Systems Interconnection (OSI) "The OSI model for network protocols is well-designed and very interoperable.It was developed too late to be accepted by the principal communications customers in industry and the military, who had already invested heavily in TCP/IP." And while serving as a good framework for protocols it is not ideal for actual high speed implementations.

Physical Layer This layer is the lowest layer in the OSI model. It helps in the transmission of data between two machines that are communicating through a physical medium, which can be optical fibres, copper wire or wireless etc. The following are the main functions of the physical layer:

Hardware Specification: The details of the physical cables, network interface cards, wireless radios, etc are a part of this layer.

Encoding and Signalling: How are the bits encoded in the medium is also decided by this layer. For example, on the copper wire medium, we can use different voltage levels for a certain time interval to represent '0' and '1'. We may use +5mV for 1nsec

to represent '1' and -5mV for 1nsec to represent '0'. All the issues of modulation is dealt with in this layer. eg, we may use Binary phase shift keying for the representation of '1' and '0' rather than using different voltage levels if we have to transfer in RF waves.

Data Transmission and Reception: The transfer of each bit of data is the responsibility of this layer. This layer assures the transmission of each bit with a high probability. The transmission of the bits is not completely reliable as there is no error correction in this layer.

Topology and Network Design: The network design is the integral part of the physical¬ layer. Which part of the network is the router going to be placed, where the switches will be used, where we will put the hubs, and how many machines is each switch going to handle, what server is going to be placed where, and many such concerns are to be taken care of by the physical layer. The various kinds of network topologies that we decide to use may be ring, bus, star or a hybrid of these topologies depending on our requirements.

Data Link Layer This layer provides reliable transmission of a packet by using the services of the physical layer which transmits bits over the medium in an unreliable fashion. This layer is concerned with :

Framing: Breaking input data into frames (typically a few hundred bytes) and caring about the frame boundaries and the size of each frame.

Acknowledgment: Sent by the receiving end to inform the source that the frame was received without any error.

Sequence Numbering: To acknowledge which frame was received.

Error Detection: The frames may be damaged, lost or duplicated leading to errors. The error control is on link to link basis.

Retransmission: The packet is retransmitted if the source fails to receive acknowledgment.

Flow Control: Necessary for a fast transmitter to keep pace with a slow receiver.

Network Layer The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:

Routing: This deals with determining how packets will be routed (transferred) from source to destination.

Subnet traffic control: routers can Instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.

Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.

Logical-physical address mapping: translates logical addresses, or names,into physical addresses.

Subnet usage accounting: has accounting functions to keep track of frames Forwarded by subnet intermediate systems, to produce billing information.

Transport Layer Fragmentation and Re-assembly: The data accepted by the transport layer from the session layer is split up into smaller units (fragmentation) if needed and then passed to the network layer. Correspondingly, the data provided by the network layer to the transport layer on the receiving side is re-assembled.

Types of service: The transport layer also decides the type of service that should be provided to the session layer. The service may be perfectly reliable, or may be reliable within certain tolerances or may not be reliable at all. The message may or may not be received in the order in which it was sent. The decision regarding the type of service to be provided is taken at the time when the connection is established.

Error Control: If reliable service is provided then error detection and error recovery operations are also performed. It provides error control mechanism on end to end basis.

Flow Control: A fast host cannot keep pace with a slow one. Hence, this is a mechanism to regulate the flow of information.

Connection Establishment / Release: The transport layer also establishes and releases the connection across the network. This requires some sort of naming mechanism so that a process on one machine can indicate with whom it wants to communicate.

Session Layer It deals with the concept of Sessions i.e. when a user logins to a remote server he should be authenticated before getting access to the files and application programs. Another job of session layer is to establish and maintain sessions. If during the transferof data between two machines the session breaks down, it is the session layer which reestablishes the connection.

It also ensures that the data transfer starts from where it breaks keeping it transparent to the end user. e.g. In case of a session with a database server, this layer introduces check points at various places so that in case the connection is broken and re-established, the transition running on the database is not lost even if the user has not committed. This activity is called Synchronization.

Another function of this layer is Dialogue Control which determines whose turn is it to speak in a session. It is useful in video conferencing.

Presentation Layer This layer is concerned with the syntax and semantics of the information transmitted. In order to make it possible for computers with different

data representations to communicate data structures to be exchanged can be defined in abstract way along with standard encoding. It also manages these abstract data structures and allows higher level of data structures to be defined an exchange. It encodes the data in standard agreed way (network format).
Character code translation: for example, ASCII to EBCDIC.

Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.

Data compression: reduces the number of bits that need to be transmitted on the network.

Data encryption: encrypt data for security purposes. For example, password encryption.

Application Layer The application layer enables the user, whether human or software, to access the network.

It provides user interface and support for services such as electronic mail, remote access and transfer, shared database management, and other types of distributed information services. The Domain Name System (DNS) is a supporting program that is used by other programs such as e-mail.DNS client/server program can support an e-mail program to find the IP address of an e-mail recipient.

CHAPTER-2

2-MARKS

Q-1-What is full duplex type of communication?how it is different from half duplex communication?(2017(s)

ANS-Full duplex -The two systems that can communicate in both directions simultaneously are called full duplex mode communications The most common example of a full duplex network is once again the telephone system. Both part can speak simultaneously during the telephone call and each part can hear the other at the same time.

Half duplex - In half duplex communications two computer communicate over a long, data typical travels in only one directions at a time because the base band network used for most LAN's supports only a single signal. This is called half duplex communications . An example of an Half duplex communications is two way radio set in which only one part can transmit at any one time and each pat must say 'over' to signal.

Q-2-Distinguish between analog & didgital datatransmission(2017,2018

Ans-

	ANALOG	DIGITAL
	An analog signal is a continuous wave that changes over a time period.	A digital signal is a discrete wave that carries information in binary form.
Representation	An analog signal is represented by a sine wave.	A digital signal is represented by square waves.
Description	An analog signal is described by	A digital signal is described by

	the amplitude, period or frequency, and phase.	bit rate and bit intervals.
Range	Analog signal has no fixed range.	Digital signal has a finite range i.e. between 0 and 1.
Distortion	An analog signal is more prone to distortion.	A digital signal is less prone to distortion.
Transmit	An analog signal transmit data in the form of a wave.	A digital signal carries data in the binary form i.e. 0 nad 1.
Example	The human voice is the best example of an analog signal.	Signals used for transmission in a computer are the digital signal.

Q-3-What do you mean by bit rate and baud rate?(2017(s)

Ans- The bit rate is the number of bits transmitted per second, whereas, the baud rate is the number of signal units transmitted per second and one signal unit is able to represent one or more bits. Therefore, baud rate is always less than or equal to the bit rate but never greater.

Q-4-What is line configuration?(2017(s)-2016(w))

Ans-Line configuration refers to the way two or more communication devices attached to a link. Line configuration is also referred to as connection. A Link is the physical communication pathway that transfers data from one device to another. For communication to occur, two devices must be connected in same way to the same link at the same time.

There are two possible line configurations.

1. Point-to-Point.
2. Multipoint.

Q-5-What do you mean by wireless transmission?(2016,2018)

Ans-Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.

5-MARKS

Q-1-Describe the formula to find the data transfer rate and channel capacity(shannon's formula).(2017(s)2016,2018

Ans-Data Transfer rate- The data transfer rate (DTR) is the amount of digital data that is moved from one place to another in a given time.

In general, the greater the bandwidth of a given path, the higher the data transfer rate. In computers, data transfer is often measured in bytes per second.

The highest data transfer rate to date is 14 terabits per second over a single optical fiber, reported by Japan's Nippon Telegraph and Telephone (NTT Do Como) in 2006.

Channel Capacity- In computer science the term channel capacity refers to the maximum data (information) that can be supported by the communication media connected to the systems in the network.

In simple words it indicates data traffic of channel(channel like co axial cable or optical fiber or any transmission media)

the Shannon–Hartley theorem states the channel capacity C, meaning the theoretical tightest upper bound on the information rate of clean data that can be sent with a given average signal power S through an analog communication channel subject to additive white Gaussian noise of power N,

is: $C=B\log_2(1+S/N)$ where

1. C is the channel capacity in bits per second;

2. B is the bandwidth of the channel in hertz ;

3. S is the average received signal power over the bandwidth measured in watts ;

4. N is the average noise or interference power over the bandwidth, measured in watts;S/N is the signal-to-noise ratio (SNR) or the carrier-to-noise ratio (CNR) of the communication signal to the Gaussian noise interference expressed as a linear power ratio (not as logarithmic decibels).

Q-2-What do you mean by parallel connection?Giveexample.What is the function of RJ_45?(2017(s))

ANS-<u>**Parallel connection**</u> Parallel connections have multiple wires running parallel to each other and can transmit¬ data on all the wires simultaneously. The speed of a parallel data link is equal to the number of bits sent at one time times the bit rate of each individual path; doubling the number of bits sent at once doubles the data rate. In practice, clock skew reduces the speed of every link to the slowest of all of the links.

RJ-45 Registered Jack-45, a RJ-45 is an 8-pin connection used for Ethernet network adapters. This connector resembles the RJ-11 or 6-pin connector used with telephones in the United States, but they're completely different. The picture is of a RJ-45 connector separated from the cable. This connector is most commonly connected to the end of Cat5 cable, which is connected between a computer network card and a network device such as a network router. This makes it ideal for devices that need to transfer high levels of data in real-time, such as video devices. Registered Jack-45, an eight-wire connector used commonly to connect computers onto a local-area networks (LAN), especially Ethernets. RJ-45 connectors look similar to the ubiquitous RJ-11 connectors used for connecting telephone equipment, but they are somewhat wider

Q-3-Explain different types of mode of transmission.(2017,2016)

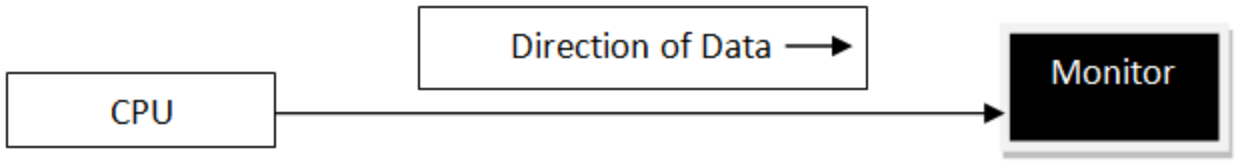
Ans- Transmission mode refers to the mechanism of transferring of data between two devices connected over a network. It is also called **Communication Mode**. These modes direct the direction of flow of information. There are three types of transmission modes. They are:

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

SIMPLEX Mode

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

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



HALF DUPLEX Mode

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

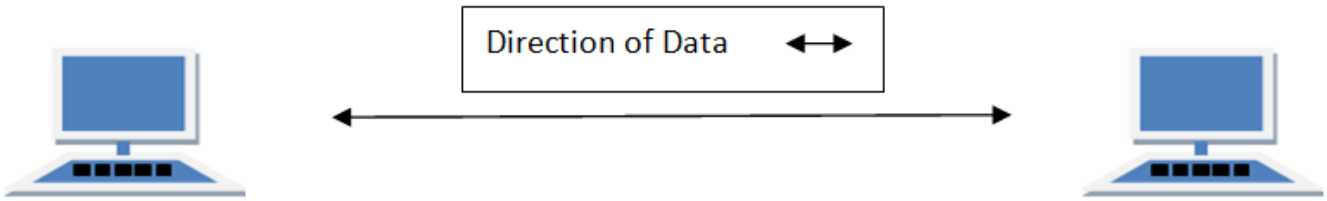
For example, on a local area network using a technology that has half-duplex transmission, one workstation can send data on the line and then immediately receive data on the line from the same direction in which data was just transmitted. Hence half-duplex transmission implies a bidirectional line (one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

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

FULL DUPLEX Mode

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

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



In full duplex system there can be two lines one for sending the data and the other for receiving data.

Q-4-Define transmission imparements.What are they?(2017(s)

Ans-When signals travel through the medium they tend to deteriorate. This may have many reasons as given:

- **Attenuation**

For the receiver to interpret the data accurately, the signal must be sufficiently strong.When the signal passes through the medium, it tends to get weaker.As it covers distance, it loses strength.

- **Dispersion**

  As signal travels through the media, it tends to spread and overlaps. The amount of dispersion depends upon the frequency used.

- **Delay distortion**

  Signals are sent over media with pre-defined speed and frequency. If the signal speed and frequency do not match, there are possibilities that signal reaches destination in arbitrary fashion. In digital media, this is very critical that some bits reach earlier than the previously sent ones.

- **Noise**

  Random disturbance or fluctuation in analog or digital signal is said to be Noise in signal, which may distort the actual information being carried. Noise can be characterized in one of the following class:

  - **Thermal Noise**

    Heat agitates the electronic conductors of a medium which may introduce noise in the media. Up to a certain level, thermal noise is unavoidable.

  - **Intermodulation**

    When multiple frequencies share a medium, their interference can cause noise in the medium. Intermodulation noise occurs if two different frequencies are sharing a medium and one of them has excessive strength or the component itself is not functioning properly, then the resultant frequency may not be delivered as expected.

  - **Crosstalk**

    This sort of noise happens when a foreign signal enters into the media. This is because signal in one medium affects the signal of second medium.

  - **Impulse**

    This noise is introduced because of irregular disturbances such as lightening, electricity, short-circuit, or faulty components. Digital data is mostly affected by this sort of noise.

7-MARKS

Q-1-Discuss the various transmission media available with neat diagram.(2017(s),2016,2018

Ans-Physical matter that carries transmission o Guided media:

• Transmission flows along a physical guide (Media guides the signal))

• Twisted pair wiring, coaxial cable and optical fiber cable o Wireless media (aka, radiated media)

• No wave guide, the transmission just flows through the air (or space)

• Radio (microwave, satellite) and infrared communications

Twisted-Pair Cable Twisted-pair cable is a type of cabling that is used for telephone communications and most modern Ethernet networks. A pair of wires forms a circuit that can transmit data. The pairs are twisted to provide protection against crosstalk, the noise generated by adjacent pairs.

When electrical current flows through a wire, it creates a small, circular magnetic field around the wire. When two wires in an electrical circuit are placed close together, their magnetic fields are the exact opposite of each other. Thus, the two magnetic fields cancel each other out. They also cancel out any outside magnetic fields. Twisting the wires can enhance this cancellation effect. Using cancellation together with twisting the wires, cable designers can effectively provide self-shielding for wire pairs within the network media.

Two basic types of twisted-pair cable exist: unshielded twisted pair (UTP) and shielded twisted pair (STP).

Unshielded Twisted Pair (UTP) UTP cable is a medium that is composed of pairs of wires.

UTP cable is used in a variety of networks. Each of the eight individual copper wires in UTP cable is covered by an insulating material. In addition, the wires in each pair are twisted around each other.

UTP cable often is installed using a Registered Jack 45 (RJ-45) connector . The RJ-45 is an eight-wire connector used commonly to connect computers onto a localarea network (LAN), especially Ethernets. Commonly used types of UTP cabling are as follows:

Category 1—Used for telephone communications. Not suitable for transmitting data.

Category 2—Capable of transmitting data at speeds up to 4 megabits per second (Mbps).

Category 3—Used in 10BASE-T networks. Can transmit data at speeds up to 10 Mbps.

Category 4—Used in Token Ring networks. Can transmit data at speeds up to 16 Mbps.

Category 5—Can transmit data at speeds up to 100 Mbps.

Shielded Twisted-Pair Cable -- Shielded twisted-pair (STP) cable combines the techniques of shielding, cancellation, and wire twisting

Each pair of wires is wrapped in a metallic foil . The four pairs of wires then are wrapped in an overall metallic braid or foil, usually 150-ohm cable. As specified for use in Ethernet network installations, STP reduces electrical noise both within the cable (pair-to-pair coupling, or crosstalk) and from outside the cable (EMI and RFI). STP usually is installed with STP data connector, which is created especially for the STP cable. However, STP cabling also can use the same RJ connectors that UTP uses. Although STP prevents interference better than UTP, it is more expensive and difficult to install.

Coaxial Cable- Coaxial cable so as named because it contains two conductors within the sheath.

At the centre of the cable is the copper core that actually carries the electrical signals. Surrounding the core is a layer of insulation and also it is called second conductor. The second conductor works as ground. There are two types of coaxial cable

1.RG8 used in LAN also known as thick Ethernet.

2.RG-58 used for LAN and known as thin Ethernet.

Advantage Less prone to interference than TP (due to (shield) More expensive than TP (quickly disappearing) used mostly for CABLE TV

Q-2-Define serial and parallel transmission .Explain function of both transmission with an example with suitable diagram.(2017(s))

ANS-Digital data transmission Data transfer is the manner in¬ which data is sent over the underlying medium. Transmission modes can be¬ divided into two fundamental categories: 1. Serial transmission 2. Parallel transmission

Parallel transmission -Parallel transmission allows¬ transfers of multiple data bits at the same time over separate medium. Parallel transmission is used with a¬ wired medium that uses multiple, independent wires. The signals on all wires are

synchronized so that a bit travels across each of the wires at precisely the same time. In fig there are 8 wires used to send 8 data bits at the same time Advantages High speed: it can send N bits at the same time a parallel interface can operate N times faster than an equivalent serial interface. Match to underlying hardware: Internally, computer and communication hardware uses parallel circuitry; a parallel interface matches the internal hardware well

Serial transmission Serial transmission sends one bit follows another. Most communication systems use serial mode We need only one communicating channel rather than n to transmit between two communicating device Advantages Serial networks can be extended over long distances at much less cost . Using only one physical wire means that there is never a timing problem caused by one wire being slightly longer than another. Serial transmission mechanisms can be divided into two broad categories

CHAPTER-3

2-MARKS

Q-1-What is functions of MODEM?(2016,2018

Ans-Modem stands for MOdulator/DEModulator. A **modem** converts digital signals generated by the computer into analog signals which can be transmitted over a telephone or cable line and transforms incoming analog signals into their digital equivalents

Q-2-Define signal t noise ratio.(2016(w))

Ans-Signal-to-noise ratio (abbreviated **SNR** or ***S/N***) is a measure used in science and engineering that compares the level of a desired signal to the level of background noise. SNR is defined as the ratio of signal power to the noise power, often expressed in decibels. A ratio higher than 1:1 (greater than 0 dB) indicates more signal than noise.

Q-3-What is data encoding?(2016,2018)

Ans-Encoding is the process of converting data into a format required for a number of information processing needs, including:

- Program compiling and execution
- Data transmission, storage and compression/decompression
- Application data processing, such as file conversion

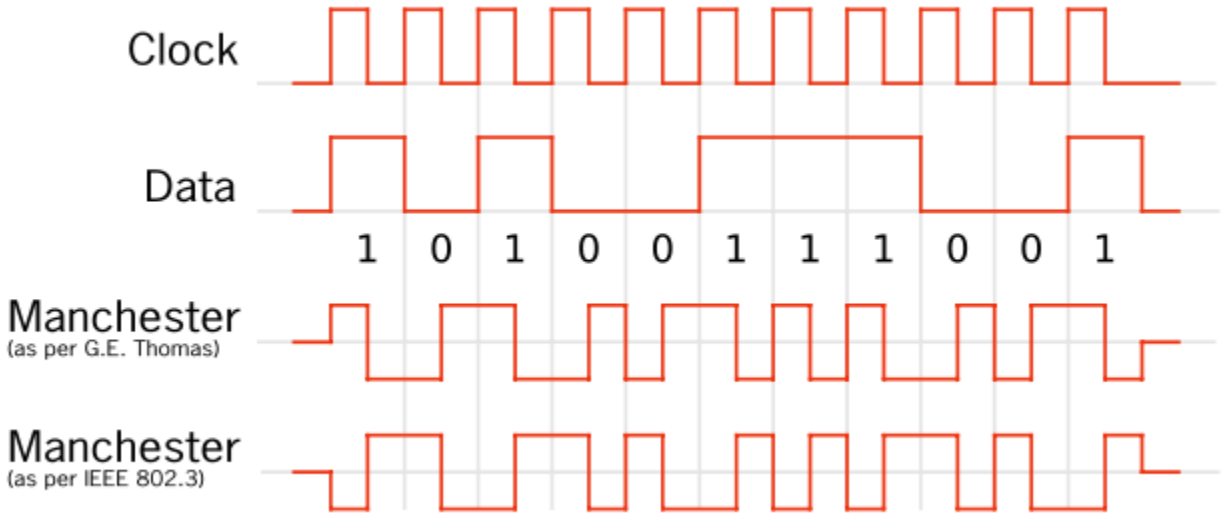
Encoding can have two meanings:

- In computer technology, encoding is the process of applying a specific code, such as letters, symbols and numbers, to data for conversion into an equivalent cipher.
- In electronics, encoding refers to analog to digital conversion.

5-MARKS

Q-1-Explain Manchester encoding methods with suitable example.(2016(w),2017,2018))

Ans-



Manchester encoding -The idea of RZ and the idea of NRZ-L are combined into the Manchester encoding scheme.

In Manchester encoding, the duration of the bit is divided into 2 halves .the voltage remains at one level during the 1st half and moves to the other level in 2nd half.,

The transmission at the middle of the bit provides synchronization.

In the Manchester encoding shown, logic 0 is indicated by a 0 to 1 transition at the centre of the bit and a logic 1 is indicated by a 1 to 0 transition at the centre of the bit.

Note that signal transitions do not always occur at the 'bit boundaries' (the division between one bit and another), but that there is always a transition at the centre of each bit. The following diagram shows a typical Manchester encoded signal with the corresponding binary representation of the data (1, 1, 0, 1, 0, 0) being sent. The waveform for a Manchester encoded bit stream carrying the sequence of bits 11011000100. Manchester scheme overcomes several problems associated with NRZ-L

Q-2-What is modulation? Explain analog to analog and digital modulation.(2017,2018(w))

Ans-Modulation

- In electronics and telecommunications**,** modulation is the process of varying one or more properties of a periodic waveform, called the carrier signal (high frequency signal), with a modulating signal that typically contains information to be transmitted.
- In telecommunications, modulation is the process of conveying a message signal, for example a digital bit stream or an analog audio signal, inside another signal that can be physically transmitted. Modulation of a sine waveform transforms a baseband message signal into a pass band signal.
- Today vast amounts of information are communicated using radio communications systems. Both analogue radio communications systems and digital or data radio communications links are used.
- There are many ways in which a radio carrier can be modulated to carry a signal, each having its own advantages and disadvantages. The choices of modulation have a great impact on the radio communications system.

- Some forms are better suited to one kind of traffic whereas other forms of modulation will be more applicable in other instances. Choosing the correct form of modulation is a key decision in any radio communications system design.

Basic Type Of Modulation

- There are three main ways in which a radio communications or RF signal can be modulated:

Amplitude Modulation(Am)

- In AM transmission, the carrier signal is modulated so that its amplitude varies with the changing amplitudes of the modulating signal.
- The frequency and phase of the carrier remain same; only the amplitude changes to follow variations in the information. The modulating signal is the envelope of the carrier.
- AM is normally implemented by using a simple multiplier because the amplitude of the carrier signal needs to be changed according to the amplitude of the modulating signal. As the name implies, this
- form of modulation involves modulating the amplitude or intensity of the signal.

- Amplitude modulation was the first form of modulation to be used to broadcast sound, and although other forms of modulation are being increasingly used, amplitude modulation is still in widespread use.

Frequency modulation(FM)

- In FM transmission, the frequency of the carrier signal is modulated to follow the changing voltage level of modulating signal.
- The peak amplitude and phase of the carrier signal remain constant, but as the
- amplitude of the information signal changes, the frequency of the carrier changes correspondingly.
- FM is normally implemented by using a voltage-controlled oscillator as with FSK.The frequency of the oscillator changes according to the input voltage which is the amplitude of the modulating signal

- Frequency modulation has the advantage that, as amplitude variations do not carry any information on the signal, it can be limited within the receiver to remove signal strength variations and noise. As a result is form of modulation has been used for many applications including high quality analogue sound broadcasting.

Phase modulation(PM)

- In PM transmission, the phase of the carrier signal is modulated to follow the changing voltage level of the modulating signal.
- The peak amplitude and frequency of the carrier signal remain constant, but as the amplitude of the information signal changes, the phase of the carrier changes correspondingly.
- It can be proved mathematically that PM is the same as FM with one difference. In FM, the instantaneous change in the carrier frequency is proportional to the amplitude of the modulating signal; In PM the instantaneous change in the carrier frequency is proportional to the derivative of the amplitude of the modulating signal.
- The frequency of the oscillator changes according to the derivative of the input voltage which is the amplitude of the modulating signal.
- Phase modulation, PM, is used in many applications to carry both analogue and digital signals. Keeping the amplitude of the signal constant, the phase is varied to carry the required information or signal.

- Phase modulation is widely used for transmitting radio waves and is an integral part of many digital transmission coding schemes that underlay a wide range of technologies like Wi-Fi, GSM and satellite television.

CHAPTER-4

2-MARKS

Q-1-What is significance of ATM?(2016,2018)

Ans-Asynchronous transfer mode (ATM) is a switching technique used by telecommunication networks that uses asynchronous time-division multiplexing to encode data into small, fixed-sized cells. This is different from Ethernet or internet, which use variable packet sizes for data or frames. ATM is the core protocol used over the synchronous optical network (SONET) backbone of the integrated digital services network (ISDN).

Q-2-Define error detection.Name two types of error detection methods.(2017,2018)

Ans-Detection The parity checking at the receiver can detect the presence of an error if the parity of the receiver signal is different from the expect parity. That means if 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. If presence of error is detected then the receiver will ignore the received byte and request for retransmission of the same byte to the transmitter.
Error Detection Four types of redundancy checks are used in data communication

1. Vertical Redundancy Check (VRC)
2. Longitudinal Redundancy Check (LRC)
3. Cyclic Redundancy Check (CRC)
4. Checksum

5-MARKS

Q-1-Distinguish between Asynchronous and Synchronous transmission.(2016(w)-2017(S))

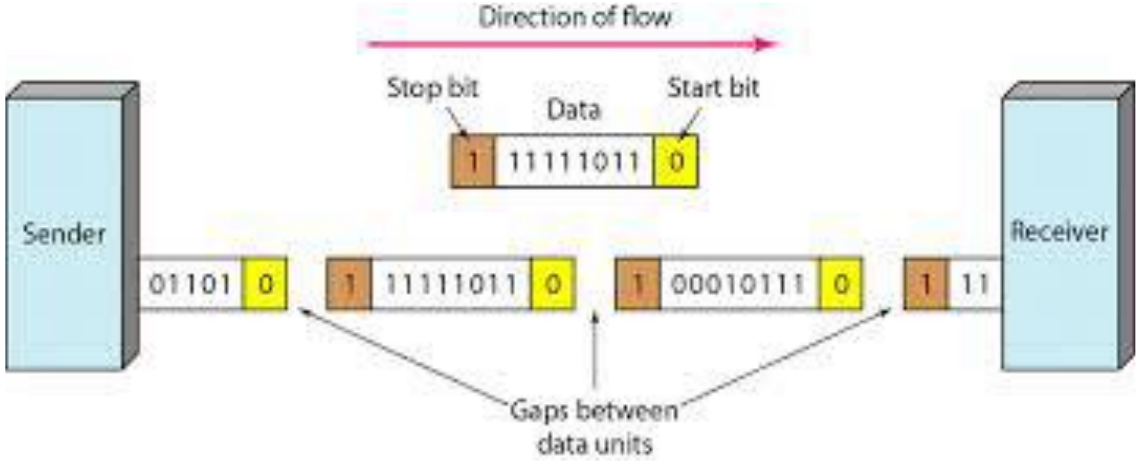
Ans-

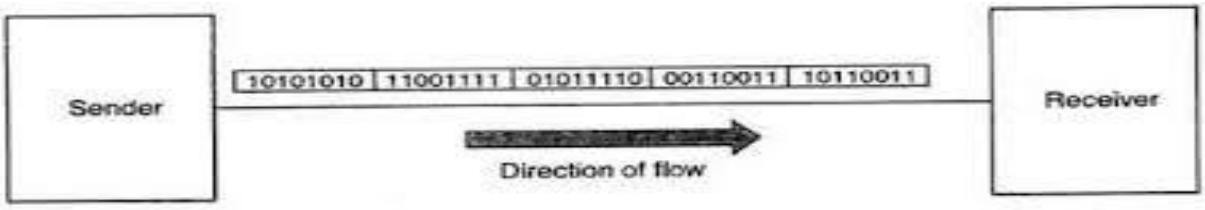
1. **Asynchronous transmission**
2. **Synchronous transmission**

Asynchronous transmission

- Small blocks of bits are sent at a time without any time relation between consecutive bytes .when no transmission occurs a default state is maintained corresponding to bit 1.
- Due to arbitrary delay between consecutive bytes, the time occurrences of the clock pulses at the receiving end need to be synchronized for each byte.
- This is achieved by providing 2 extra bits start and stop.

- **Start bit:** Without a synchronizing pulse, the receiver can't use timing to predict when the next group will arrive. To alert the receiver to the arrival of a new group, therefore an extra bit is added to the beginning of each byte. This bit usually a 0,is called a start bit
- **Stop bit:** To ensure the receiver know that the byte is finished; one or more additional bits are appended to end of the byte. These bits, usually 1s,are called stop bit





Synchronous Transmission

Synchronous Transmission

- In Synchronous transmission, we send bits one after another without start/stop bit or gapes. It is the responsibility of the receiver to group the bits.
- The advantage of the synchronous transmission is the speed. With no extra bits or gaps to introduce at the sending end and remove at the receiving end. Byte synchronization is accomplished in the data link layer

7-MARKS

Q-2-Define multiplexing.Explain different types of multiplexing.(2016(w)-2017(S),2018)

Ans-

- Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link. Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams.
- Communication is possible over the air (radio frequency), using a physical media (cable) and light (optical fiber). All mediums are capable of multiplexing.
- When more than one senders tries to send over single medium, a device called Multiplexer divides the physical channel and allocates one to each. On the other end of communication, a De-multiplexer receives data from a single medium and identifies each and send to different receivers.
- Transmitting two or more signals simultaneously can be accomplished by running multiple cables or setting up one transmitter receiver pair for each channel , but this is an expensive approach.
- A single cable or radio link can handle multiple signals simultaneously using a technique known as multiplexing.Multiplexing permits hundreds or even thousands of signals to be combined and transmitted over a single medium.
- A device called a multiplexer (often shortened to "mux") combines the input signals into one signal. When the multiplexed signal needs to be separated into its component signals (for example, when your email is to be delivered to its destination), a device called a demultiplexer (or "demux") is used.
- Multiplexing was originally developed in the 1800s for telegraphy. Today, multiplexing is widely used in many telecommunications applications, including telephony, Internet communications, digital broadcasting and wireless telephony.

Frequency Division Multiplexing

- When the carrier is frequency, FDM is used.
- FDM is an analog technology.
  - FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel.

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

Time Division Multiplexing

- TDM is applied primarily on digital signals but can be applied on analog signals as well.
- In TDM the shared channel is divided among its user by means of time slot.
- Each user can transmit data within the provided time slot only.
- Digital signals are divided in frames, equivalent to time slot i.e. frame of an optimal size which can be transmitted in given time slot.
- TDM works in synchronized mode. Both ends, i.e. Multiplexer and De-multiplexer are timely synchronized and both switch to next channel simultaneously

- When at one side channel A is transmitting its frame, on the other end De-multiplexer providing media to channel A.
- As soon as its channel A's time slot expires this side switches to channel B.
- On the other end De-multiplexer behaves in a synchronized manner and provides media to channel B. Signals from different channels travels the path in interleaved manner.
- Multiple signals can be transmitted if each signal is allowed to be transmitted for a definite amount of time. These time slots are so small that all transmissions appear to be in parallel.

1. **Synchronous TDM:** Time slots are pre assigned and are fixed. Each source is given its time slot at every turn due to it. This turn may be once per cycle, or several turns per cycle ,if it has a high data transfer rate, or may be once in a no. of cycles if it is slow. This slot is given even if the source is not ready with data. So this slot is transmitted empty.

2. **Asynchronous TDM:** In this method, slots are not fixed. They are allotted dynamically depending on speed of sources, and whether they are ready for transmission.

Wavelength Division Multiplexing

- Light has different wavelength (colors).
- In fiber optic mode, multiple optical carrier signals are multiplexed into on optical fiber by using different wavelengths.
- This is an analog multiplexing technique and is done conceptually in the same manner as FDM but uses light as signals.

- Further, on each wavelength Time division multiplexing can be incorporated to accommodate more data signals.

Code Division Multiplexing

- Multiple data signals can be transmitted over a single frequency by using Code Division Multiplexing. FDM divides the frequency in smaller channels but CDM allows its users to full bandwidth and transmit signals all the time using a unique Code. CDM uses orthogonal codes to spread signals.
- Each station is assigned with a unique code, called chip. Signals travels with these codes independently travelling inside the whole bandwidth. The receiver in this case, knows in advance chip code signal it has to receive signals.
- CDM is widely used in so-called second-generation (2G) and third-generation 3G wireless communications. The technology is used in ultra-high-frequency (UHF) cellular telephone systems in the 800-MHz and 1.9-GHz bands. This is a combination of analog-to-digital conversion and spread spectrum technology.
- CDM may be defined as a form of multiplexing where the transmitter encodes the signal using a pseudo-random sequence. CDM involves the original digital signal with a spreading code. This spreading has the effect of spreading the spectrum of the signal greatly and reducing the power over anyone part of the spectrum. On the other hand, the receiver knows about the code generated and transmitted by the transmitter and therefore, can decode the received signal. Each different random sequence corresponds to a different communication channel from multiple stations.
- Code Division Multiplexing assigns each channel its own code to make them separate from each other. These unique underlying codes, which ~hen decoded restore' the original desired signal while totally removing the effect of the other coded channels.Guard spaces are realized by using codes with orthogonal codes..Figure explains how all channels Ci, use the same frequency at the same time for transmission.

Q-3-What do you mean by Flow control?Discuss various technique used in Flow control.(2016(w)

Ans-

Flow Control

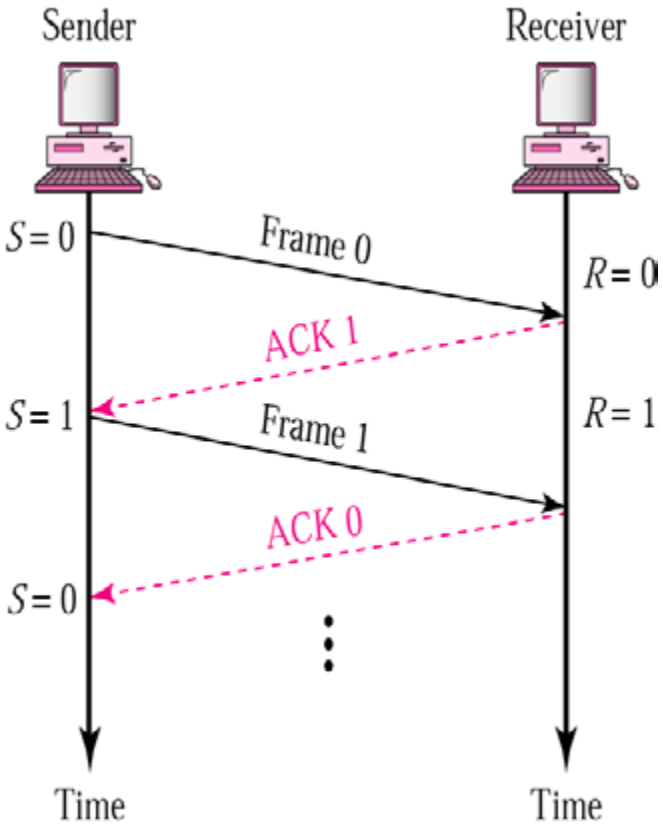
- A flow control is asset of procedures that tells the sender how much data it can transmit before it must wait for an ACK from the receiver.
- The flow of data must not be allowed to overwhelm the receiver.
- Any receiving device has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data.

- The receiving device must be able to inform the sending device before those limits are reached and to request that the transmitting device send fewer frames or stop temporarily
- Two types of mechanism can be deployed in the scenario to control the flow:

Stop -and -Wait

- In a stop- and- wait method of flow control, the sender waits for an ACK after every it sends.
- In the stop- and-wait method of flow control, the sender sends one frame and waits for an ACK before sending the next frame.
- Only when an ACK has been received is the next frame sent.
- This process of alternately sending and waitingrepeats until the sender transmit an end of

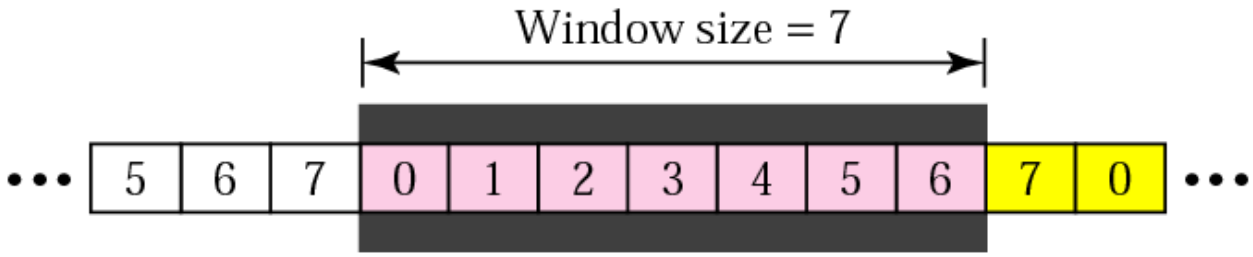
transmission frame



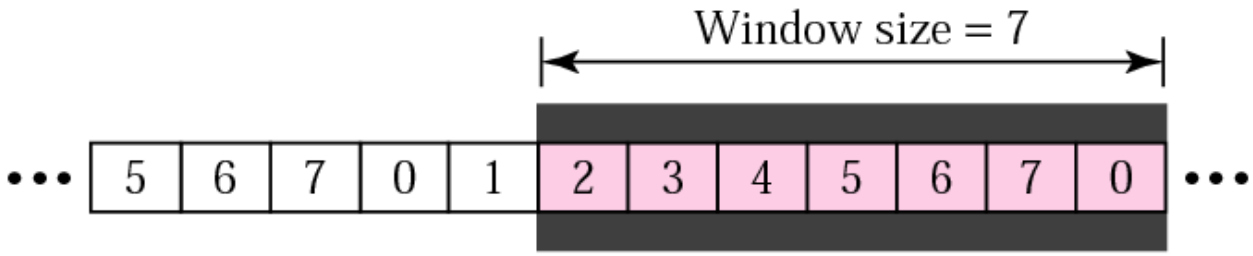
- The advantage of stop-and-wait is simplicity: each frame is checked and acknowledged before the next frame is sent.
- The disadvantage is inefficiency: the stop-and- wait is slow

Sliding Window

- In the sliding window method of flow control, the sender can transmit several frames before needing an acknowledgement.
- Frames can be sent one right after another.



a. Before sliding



b. After sliding two frames

- The receiver acknowledges only some of the frames using a single ACK to conform the receipt of multiple data frames
- In sliding window method of flow control, several frames can be in transit at a time.
- Sliding window refers imaginary box at both the sender and receiver.
- This window can hold frames at either end and provides an upper limit on the number of frames that can be transmitted before requiring an ACK.
- Frames may be acknowledged at any point without waiting for the window to fill up and may be transmitted as long as the window is not yet full.
- To keep track of which frames have been transmitted and which received, sliding window

introduces the identification scheme based on the size of the window.

- The frames are numbered modulo-n, which means they are numbered from 0 to n-1.
- For example, if n=8 the frames are numbered 0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1,.....

The window is n-1 .

- When the receiver sends an ACK , it includes the number of the next frame it excepts to receive.
- In other words to acknowledge the receipt of a string of frames ending in frame 4,the receiver sends an ACK containing the number 5.
- When the sender sees an ACK with the number 5, it knows that all frames up through number 4 have been received.

Q-6-How error is detected and corrected by using hamming codes?Expalin by giving examples.(2017,2018(s))

Ans-Hamming code is a set of error-correction codes that can be used to **detect and correct the errors**that can occur when the data is moved or stored from the sender to the receiver. It is **technique developed by R.W. Hamming for error correction**.

Redundant bits –

Redundant bits are extra binary bits that are generated and added to the information-carrying bits of data transfer to ensure that no bits were lost during the data transfer. The number of redundant bits can be calculated using the following formula:

$2^r > m + r + 1$

where, r = redundant bit, m = data bit

Suppose the number of data bits is 7, then the number of redundant bits can be calculated using:

$= 2^4 > 7 + 4 + 1$

Thus, the number of redundant bits= 4

Parity bits –

A parity bit is a bit appended to a data of binary bits to ensure that the total number of 1's in the data are even or odd. Parity bits are used for error detection. There are two types of parity bits:

1. **Even parity bit:**
   In the case of even parity, for a given set of bits, the number of 1's are counted. If that count is odd, the parity bit value is set to 1, making the total count of occurrences of 1's an even number. If the total number of 1's in a given set of bits is already even, the parity bit's value is 0.
2. **Odd Parity bit –**
   In the case of even parity, for a given set of bits, the number of 1's are counted. If that count is even, the parity bit value is set to 1, making the total count of occurrences of 1's an odd number. If the total number of 1's in a given set of bits is already odd, the parity bit's value is 0.

General Algorithm of Hamming code –

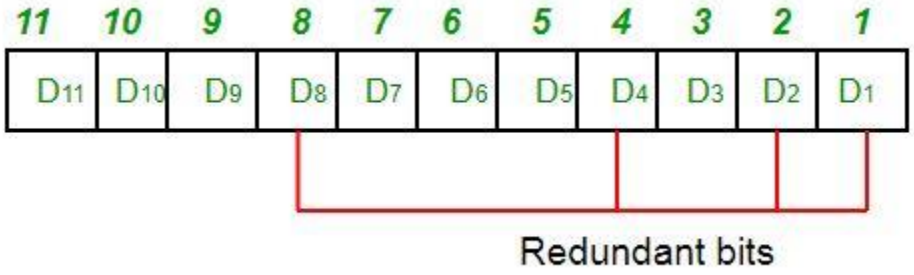
The Hamming Code is simply the use of extra parity bits to allow the identification of an error.

1. Write the bit positions starting from 1 in binary form (1, 10, 11, 100, etc).
2. All the bit positions that are a power of 2 are marked as parity bits (1, 2, 4, 8, etc).
3. All the other bit positions are marked as data bits.
4. Each data bit is included in a unique set of parity bits, as determined its bit position in binary form.
   a. Parity bit 1 covers all the bits positions whose binary representation includes a 1 in the least significant position (1, 3, 5, 7, 9, 11, etc).
   b. Parity bit 2 covers all the bits positions whose binary representation includes a 1 in the second position from the least significant bit (2, 3, 6, 7, 10, 11, etc).
   c. Parity bit 4 covers all the bits positions whose binary representation includes a 1 in the third position from the least significant bit (4–7, 12–15, 20–23, etc).
   d. Parity bit 8 covers all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit bits (8–15, 24–31, 40–47, etc).
   e. In general each parity bit covers all bits where the bitwise AND of the parity position and the bit position is non-zero.
5. Since we check for even parity set a parity bit to 1 if the total number of ones in the positions it checks is odd.

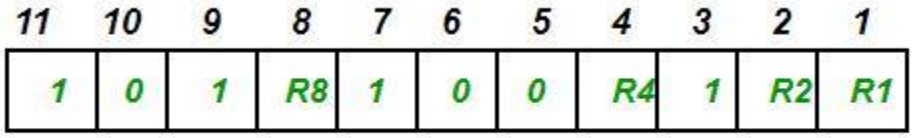
6. Set a parity bit to 0 if the total number of ones in the positions it checks is even.

Determininthe position of redundant bits – These redundancy bits are placed at the positions which correspond to the power of 2. As in the above example:

1 The number of data bits = 7
2 The number of redundant bits = 4
3 The total number of bits = 11
4 The redundant bits are placed at positions corresponding to power of 2- 1, 2, 4, and 8

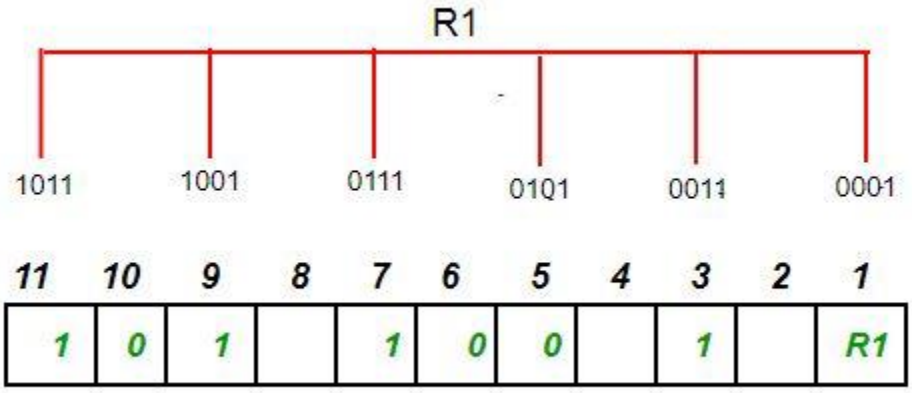


Suppose the data to be transmitted is 1011001, the bits will be placed as follows:

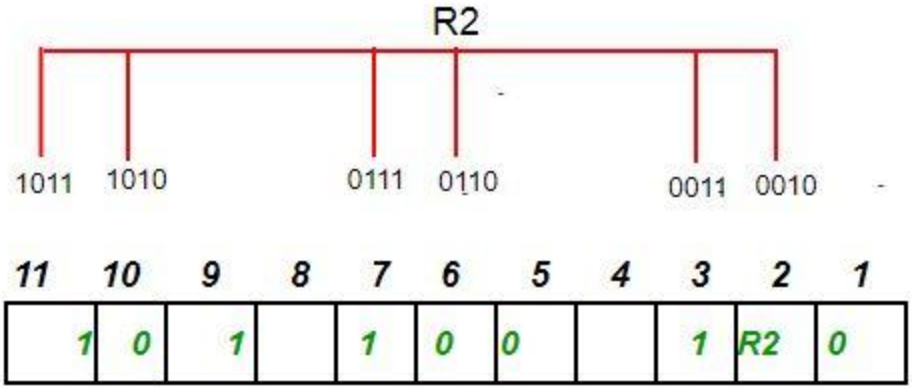


Determining the Parity bits –

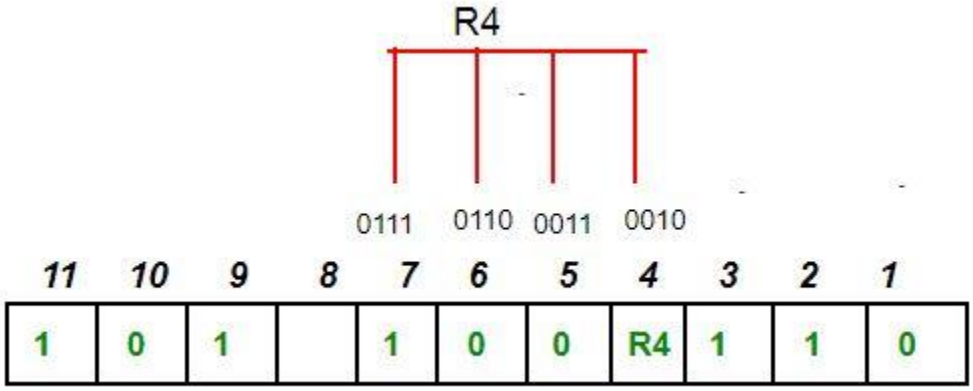
1. R1 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the least significant position.
   R1: bits 1, 3, 5, 7, 9, 11



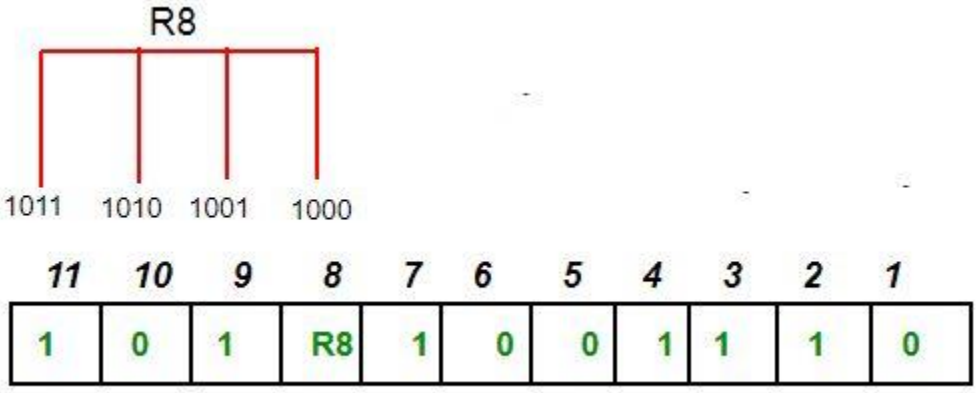
1. To find the redundant bit R1, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R1 is an even number the value of R1 (parity bit's value) = 0
2. R2 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the second position from the least significant bit.
   R2: bits 2,3,6,7,10,11



1. To find the redundant bit R2, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R2 is an odd number the value of R2(parity bit's value)=1
2. R4 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the third position from the least significant bit.
   R4: bits 4, 5, 6, 7

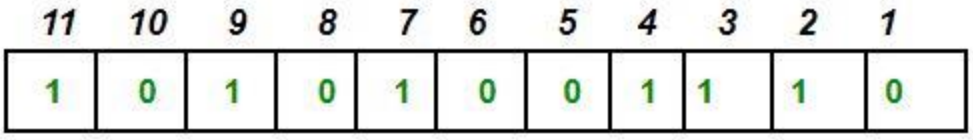


1. To find the redundant bit R4, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R4 is an odd number the value of R4(parity bit's value) = 1
2. R8 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit.
   R8: bit 8,9,10,11



To find the redundant bit R8, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R8 is an even number the value of R8(parity bit's value)=0.

Thus, the data transferred is:



Q-7-How error occurs in data transmission?List out the types of error occurs.Exlain how error is recovered and corrected?(2017,2018)

Ans-

- Error means a condition when output information is not same as input information.
- When transmission of digital signals takes place between two systems such as a computer, the transmitted signal is combined with the "Noise".
- The noise can introduce an error in the binary bits travelling from one system to other. That means 0 may change to 1 or a 1 may change to 0.Error must be detected and corrected.

Types of errors There are mainly two types of error occures

- **Single bit error:**

In a single bit error, only one bit in the data unit has changed.

- **Burst error:**

A burst error means two or more bits in the data unit have changed

CHAPTER-5

2-MARKS

Q-1-What is traffic management?(2016(w))

Ans-Network traffic management deals with the process of monitoring and controlling the activities of network besides transforming the network into a managed resource by improving performance, efficiency, and security. It also helps to operate, administer, and maintain the network systems.

Q-2-What is datagram?(2016(w)-2017)

Ans-A datagram is a unit of transfer assoicated with networking. A datagram has the following characteristics:

- Data is transmitted from source to destination without guarantee of delivery
- Data is frequently divided into smaller pieces and transmitted without a defined route or guaranteed order of delivery

Q-2-Define virtual circuit.(2016,2018,2017)

Ans-A virtual circuit is used in transportation of data over a packet switch computer network, in which it appears as if there is a physical path established between the final destination and source and through which all packets can be routed during the call.

As there is no resource allocation other than few space in circuit tables in case of virtual circuit and also the fact the packets does not have to carry the globally unique destination address, provides great advantages for using virtual circuit.

Q-3-What is function of Router.(2017(s))

Ans-A **router** is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork until it reaches its destination node

A router is connected to two or more data lines from different networks.[b] When a data packet comes in on one of the lines, the router reads the network address information in the packet to determine the ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey.

5-MARKS

Q-1-Explain X.25.(2016)-2017(s)(w))

Ans-X.25 X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN)¬ communication. X.25 was originally defined by the International Telegraph and Telephone Consultative¬ Committee (CCITT, now ITU-T) in a series of drafts and finalized in a publication known as The Orange Book in 1976. .X.25 is a family of protocols that was popular during the 1980s with telecommunications¬ companies and in financial transaction systems such as automated teller machines.

- X.25 is a standard suite of protocols used for packet switching across computer networks.
- The X.25 protocols works at the physical, data link, and network layers (Layers 1 to 3) of the OSI model.Each X.25 packets contains up to 128 bytes of data.
- The X.25 network handles packet assembly at the source device, delivery, and then dis-assembly at the destination.
  - X.25 packet delivery technology includes not only switching and network-layer routing, but also error checking and re-transmission logic should delivery failures occur. X.25 supports multiple simultaneous conversations by multiplexing packets and using virtual communication channels.
  - Based upon existing analog copper lines that experience a high number of errors Uses the virtual circuit approach. An X.25 WAN consists of packet-switching exchange (PSE) nodes as the networking

hardware, and leased lines, plain old telephone service connections or ISDN connections as physical links Provides a way to send packets across a packet-switched public data network.

- The redundant error checking is done at each node X.25 was originally designed more than 25 years ago to carry voice over analog telephone lines (dialup networks).
- Typical applications of X.25 today include automatic teller machine networks and credit card verification networks. X.25 also supports a variety of mainframe terminal/server applications.
- With the widespread acceptance of Internet Protocol (IP) as a standard for corporate networks, many X.25 applications are now being migrated to cheaper solutions using IP as the network layer protocol and replacing the lower layers of X.25 with Ethernet or ATM hardware.

Q-3-Expalin traffic management.(2017)

Ans-TYPES OF NETWORK TRAFFIC

Networks accommodate an increasingly complex set of data traffic. Identifying the type of traffic will help network administrators to facilitate the optimization of the network. Various types of traffic are:

Traffic Type	Example	Problem	Solution
Bursty Traffic	Downloads of FTP, graphic, video content	Consumes high bandwidth and Starves applications	Set constraint to limit access to bandwidth
Interactive Traffic	SSL transactions, IM, Telnet sessions	Susceptible to competition for bandwidth and results in poor response time	Prioritize over less essential traffic
Latency Sensitive Traffic	Streaming applications, Voice over IP, video conferencing	Susceptible to competition for bandwidth and results in poor response time	Set minimum and maximum bandwidth range based on priority
Non-Real Time Traffic	Email, batch processing applications	Consumes bandwidth during business hours	Schedule bandwidth during non-business hours

Q-4-What are various routing algorithm?(2017(s))

Ans-Routing is process of establishing the routes that data packets must follow to reach the destination. In this process, a routing table table is created which contains information regarding routes which data packets follow. Various routing algorithm are used for the purpose of deciding which route an incoming data packet needs to be transmitted on to reach destination efficiently.

Classification of Routing Algorithms: The routing algorithms can be classified as follows:

1. Adaptive Algorithms –

These are the algorithms which change their routing decisions whenever network topology or traffic load changes. The changes in routing decisions are reflected in the topology as well as traffic of the network. Also known as dynamic routing, these make use of dynamic information such as current topology, load, delay, etc. to select routes. Optimization parameters are distance, number of hops and estimated transit time.

Further these are classified as follows:

- **(a) Isolated –** In this method each, node makes its routing decisions using the the information it has without seeking information from other nodes. The sending nodes doesn't have information about status of particular link. Disadvantage is that packet may be sent through a congested network which may result in delay. Examples: Hot potato routing, backward learning.
- **(b) Centralized –** In this method, a centralized node has entire information about the network and makes all the routing decisions. Advantage of this is only one node is required to keep the information of entire network and disadvantage is that if central node goes down the entire network is done.
- **(c) Distributed –** In this method, the node receives information fro its neighbors and then takes the decision about routing the packets. Disadvantage is that the packet may be delayed if there is change in between interval in which it receives information and sends packet.

2. Non-Adaptive Algorithms –
These are the algorithms which do not change their routing decisions once they have been selected. This is also known as static routing as route to be taken is computed in advance and downloaded to routers when router is booted.
Further these are classified as follows:

- **(a) Flooding –** This adapts the technique in which every incoming packet is sent on every outgoing line except from which it arrived. One problem with this is that packets may go in loop and as a result of which a node may receive duplicate packets. These problems can be overcome with the help of sequence numbers, hop count and spanning tree.
- **(b) Random walk –** In this method, packets are sent host by host or node by node to one of its neighbors randomly. This is highly robust method which is usually implemented by sending packets onto the link which is least queued.

7-MARKS

Q-1-what do you men by switching ?Describe circuit switching and packet switching principle and working.(2016(w)-2017(w)(S))

Ans-Switching

- A switched network consist of a series of interlink nodes called switches.
- Switches are devices capable of creating temporary connection between two more devices linked to the switch.
- Switched networks are divide into three broad categories :

1. circuit switched network
2. packet-switched network
3. .Message-switched network

circuit switched network

- A circuit switched network consist of a set of switches connected by a physical link.
- A connection between two station is a dedicated path made up one or more links.
- Each link is normally divided into n channels by using FDM or TDM.

Message-switched network

- In message switching, each switch stores whole message and forward it to the next switch.

Packet Switching

- Packet switching can be used as an alternate to circuit switching. In the packet switched networks, data is sent in discrete units that have variable length. They are called as packets. There is a strict upper bound limit on the size of packets in a packet switch network. The packet contains data and various control information.

- The packet switched networks allow any host to send data to any other host without reserving the circuit. Multiple paths between a pair of sender and receiver may exist in a packet switched network.
- One path is selected between source and destination. Whenever the sender has data to send, it converts them into packets and forwards them to next computer or router. The router stores this packet till the output line is free.
- Then, this packet is transferred to next computer or router (called as hop). This way, it moves to the destination hop by hop. All the packets belonging to a transmission may or may not take the same route. The route of a packet is decided by network layer protocols.

Types of Packet Switching

The packet switching has two approaches: Virtual Circuit approach and Datagram approach. **Datagrams**

- In datagram packet switching each packet is transmitted in any order.
- Every packet contain full packet of source and destination. Every packet is treated as individual, independent transmission.
- Even if a packet is a part of multi-packet transmission the network treats it as though it existed alone. Packets in this approach are called **datagrams.**
- Datagram switching is done at the network layer. Figure show how a datagram approach is used to deliver four packets from station A to station X. All the four packets belong to same message but they may travel via different paths to reach the destination *i.e.* station X.

- Datagram approach can cause the datagrams to arrive at their destination out of order with different delays between the packets.
- Packets may also be lost or dropped because of lack of resources. The datagram networks are also referred as connectionless networks. Here connectionless means that the switch does not keep information about connection state. There are no connection establishment or tear down phases.
- The datagram can arrive at the destination with a different order from the order in which they were sent. The source and destination address are used by the

routers to decide the route for packets. Internet use datagram approach at the network layer.

Virtual Circuit

- All the packets belonging to a message are preserved in order.
- A single route is chosen between sender and receiver at the beginning of the session.
- All packets transmitted one after another along that route
- Virtual circuit transmission is implemented in two formats:
  1. Switched Virtual Circuits (SVC)
  2. Permanent Virtual Circuits (PVC)

Switched Virtual Circuits (SVC)

- It can be compared to dial up lines in circuit switching.
- In this method, a virtual circuit is created when it is needed and exists only during the transmission.
- Suppose station A wants to send three packets to station X.
- First station A request to establish the connection to station X.
- Once the connection takes place, the packets are sent one after another in a sequential order.
- When the last packet is received, the station A is acknowledged and the connection is released.
- Each time when A whishes to communicate with X a new route is established.

Q-3-Define congestion. What is effect of congestion?explain the methods of congestion control.(2017.2016,2018)

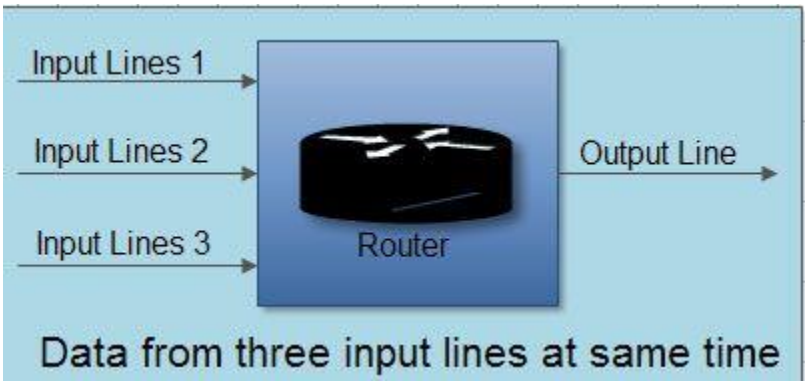
Ans-Congestion is an important issue that can arise in packet switched network. Congestion is a situation in Communication Networks in which too many packets are present in a part of the subnet, performance degrades. Congestion in a network may occur when the load on the network *(i.e.* the number of packets sent to the network) is greater than the capacity of the network *(i.e.* the number of packets a network can handle.)

Causing of Congestion:

The various causes of congestion in a subnet are:

• The input traffic rate exceeds the capacity of the output lines. If suddenly, a stream of packet start arriving on three or four input lines and all need the same output line. In this case, a queue will be built up. If there is insufficient memory to hold all the packets, the packet will be lost. Increasing the memory to unlimited size does not solve the problem. This is because, by the time packets reach front of the queue, they have already timed out (as

they waited the queue). When timer goes off source transmits duplicate packet that are also added to the queue. Thus same packets are added again and again, increasing the load all the way to the destination.

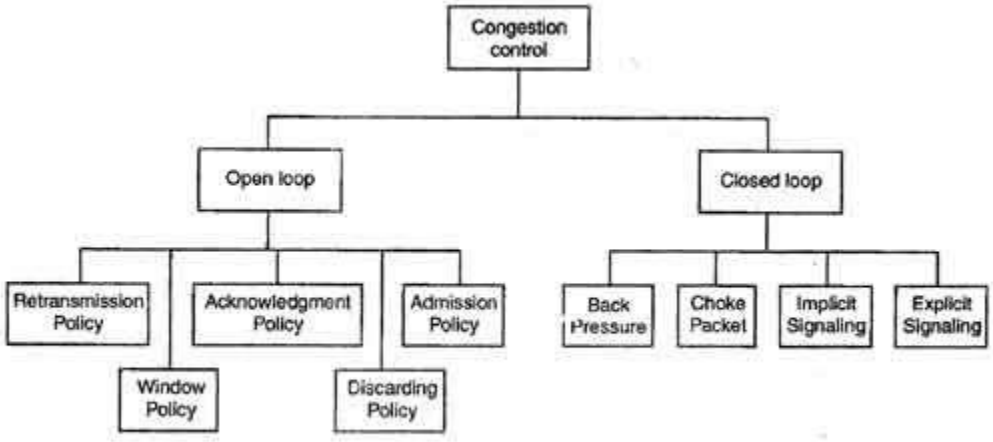


• The routers are too slow to perform bookkeeping tasks (queuing buffers, updating tables, etc.).
• The routers' buffer is too limited.
• Congestion in a subnet can occur if the processors are slow. Slow speed CPU at routers will perform the routine tasks such as queuing buffers, updating table etc slowly. As a result of this, queues are built up even though there is excess line capacity.

• Congestion is also caused by slow links.

How to correct the Congestion Problem:

Congestion Control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. Congestion control mechanisms are divided into two categories, one category prevents the congestion from happening and the other category removes congestion after it has taken place



Types of Congestion Control Methods

These two categories are:

1. Open loop
2. Closed loop

Open Loop Congestion Control

• In this method, policies are used to prevent the congestion before it happens.

• Congestion control is handled either by the source or by the destination.

• The various methods used for open loop congestion control are:

Retransmission Policy

• The sender retransmits a packet, if it feels that the packet it has sent is lost or corrupted.

• However retransmission in general may increase the congestion in the network. But we need to implement good retransmission policy to prevent congestion.

• The retransmission policy and the retransmission timers need to be designed to optimize efficiency and at the same time prevent the congestion.

Window Policy

• To implement window policy, selective reject window method is used for congestion control.

• Selective Reject method is preferred over Go-back-n window as in Go-back-n method, when timer for a packet times out, several packets are resent, although some may have arrived safely at the receiver. Thus, this duplication may make congestion worse.

• Selective reject method sends only the specific lost or damaged packets.

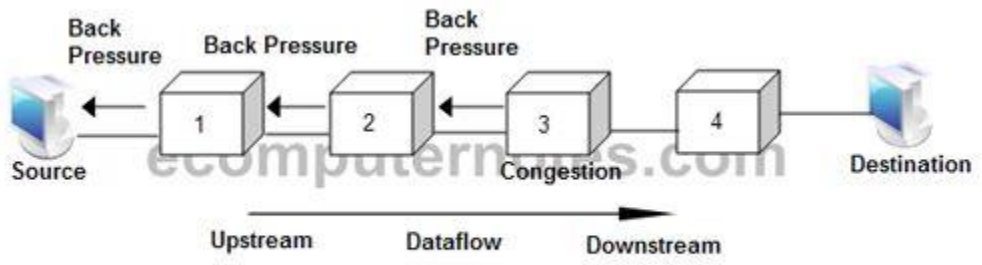
Closed Loop Congestion Control

• Closed loop congestion control mechanisms try to remove the congestion after it happens.

• The various methods used for closed loop congestion control are:

Backpressure

• Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow.



Backpressure Method

Congestion control algorithms

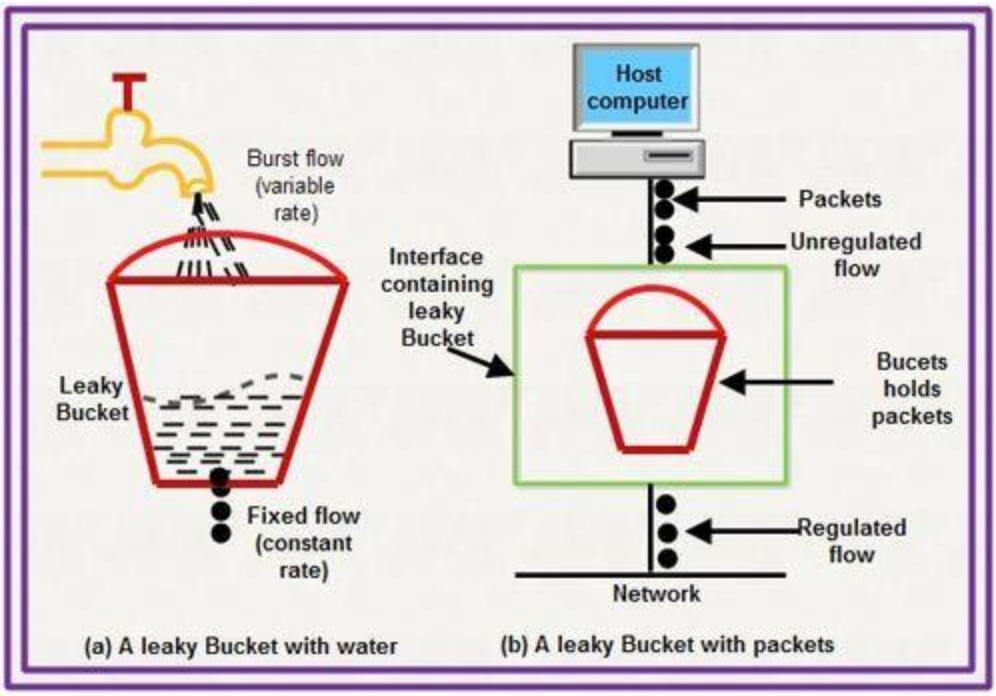
Leaky Bucket Algorithm

• It is a traffic shaping mechanism that controls the amount and the rate of the traffic sent to the network.

• A leaky bucket algorithm shapes bursty traffic into fixed rate traffic by averaging the data rate.

• Imagine a bucket with a small hole at the bottom.

• The rate at which the water is poured into the bucket is not fixed and can vary but it leaks from the bucket at a constant rate. Thus (as long as water is present in bucket), the rate at which the water leaks does not depend on the rate at which the water is input to the bucket.



• Also, when the bucket is full, any additional water that enters into the bucket spills over the sides and is lost.

• The same concept can be applied to packets in the network. Consider that data is coming from the source at variable speeds. Suppose that a source sends data at 12 Mbps for 4 seconds. Then there is no data for 3 seconds. The source again transmits data at a rate of 10 Mbps for 2 seconds. Thus, in a time span of 9 seconds, 68 Mb data has been transmitted.

CHAPTER-6

2-MARKS

Q-1-What is function of Ethernet?(2016(w),2017(s))

Ans-Ethernet is the most widely installed local area network (LAN) technology. Ethernet is a *link layer* protocol in the TCP/IP stack, describing how networked devices can format data for transmission to other network devices on the same network segment, and how to put that data out on the network connection. It touches both Layer 1 (the physical layer) and Layer 2 (the data link layer) on the OSI network protocol model. Ethernet defines two units of transmission, packet and frame.

Q-2-Define media Access Control.(2017(W))

Ans-In a local area network (LAN) or other network, the MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN.

Q-3-What is function of print server?(2017(s))

Ans-A **print server**, or **printer server**, is a device that connects printers to client computers over a **network**. It accepts **print** jobs from the computers and sends the jobs to the appropriate printers, queuing the jobs locally to accommodate the fact that work may arrive more quickly than the **printer** can actually handle.

5-MARKS

Q-1-Descibe the function of Bridges,Hub,Switch,Gateway(2016(w)-2017(w)(s)).

Ans-Bridge

- Bridge is physical device typically a box of two port which connect two network at Data Link Layer.
- A Bridge provides packet filtering at Data link layer .
- A bridge to join to existing LAN or two split one LAN in to two segment. Bridge operate in promiscuous mode.
- Data packet enter the bridge through either one of the port and the bridge then read the destination address in each packet header and decides how to process that packet . This is called packet filtering.
- If the destination address of a packet arriving from one network segment is that of a computer on the other segment, the bridge Tx it out from other port.
- If the destination address of a computer on a same network segment as the computer that generated it, the bridge discard the packet.

Gateway

architectures.

- It can translate TCP/IP to AppleTalk so computers supporting TCP/IP can communicate with Apple brand computers.

- Most gateways operate at the application layer, but can operate at the network or session layer of the OSI model.
- A gateway can translate information between different network data formats or network
- Gateways will start at the lower level and strip information until it gets to the required level and repackage the information and work its way back toward the hardware layer of the OSI model.

- To confuse issues, when talking about a router that is used to interface to another network, the word gateway is often used. This does not mean the routing machine is a gateway as defined here, although it could be.

Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Types of Hub

- **Active Hub :-** These are the hubs which have their own power supply and can clean , boost and relay the signal along the network. It serves both as a repeater as well as wiring center. These are used to extend maximum distance between nodes.
- **Passive Hub :-** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend distance between nodes.

Switch – A switch is a multi port bridge with a buffer and a design that can boost its efficiency(large number of ports imply less traffic) and performance. Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

Q-2-Define topology and explain different types of topologies.(2016(w)-2017(w)(s))

Ans- The way in which the connections are made of the physical devices is called the topology of the network.

Network topology specifically refers to the physical layout of the network, especially the locations of the computers and how the cable is run between them.

It is important to select the right topology for how the network will be used.

Each topology has its own strengths and weaknesses.

The four most common topologies are
o Mesh topology
o Bus topology

o Star topology

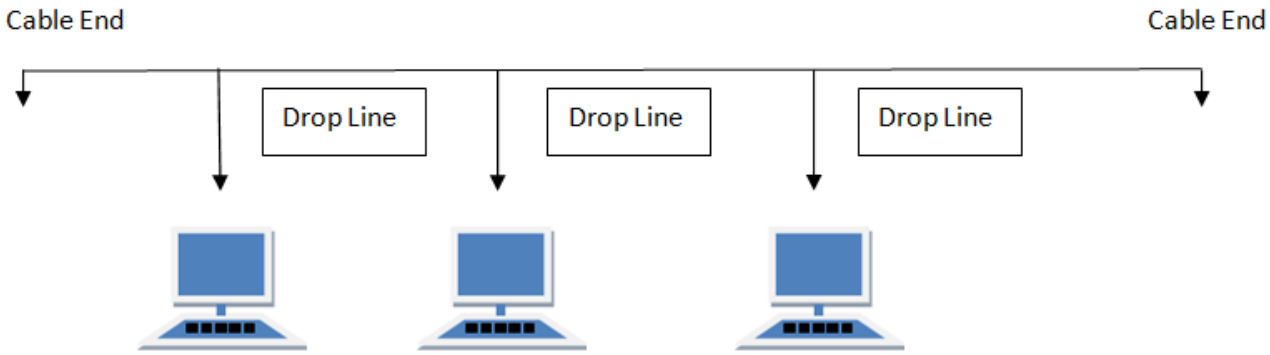
o Ring topology

o Tree Topology

o Hybrid Topology

BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

Advantages of Bus Topology

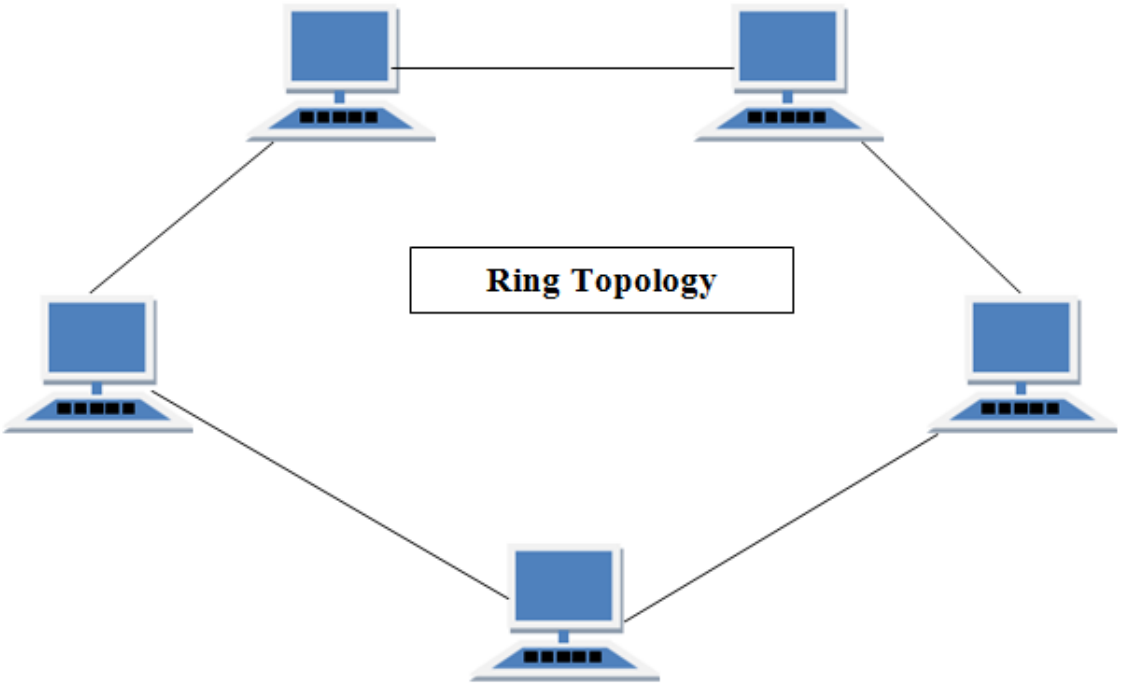
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.



Features of Ring Topology

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

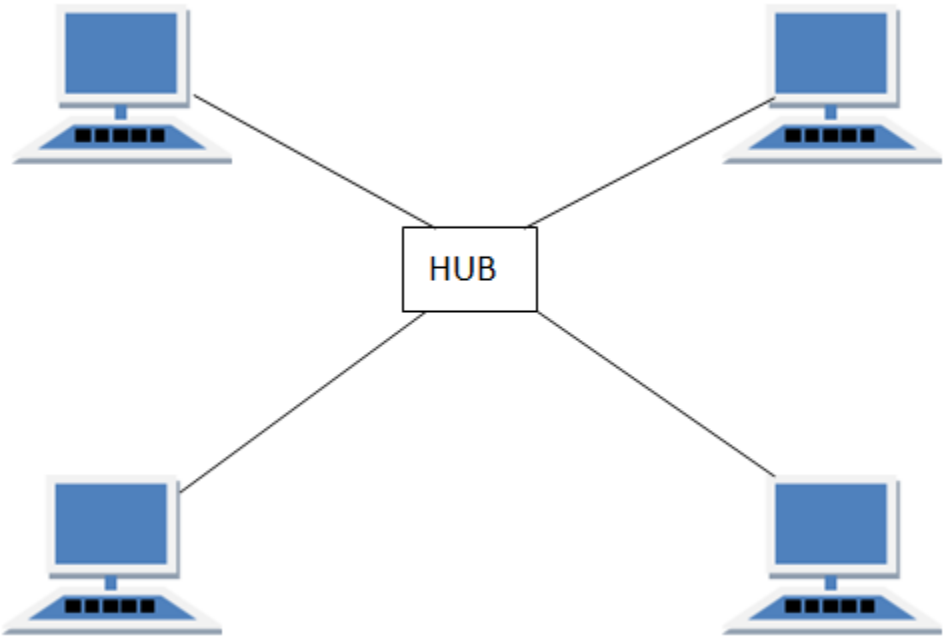
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

STAR Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has `n(n-1)/2` physical channels to link `n` devices.

There are two techniques to transmit data over the Mesh topology, they are :

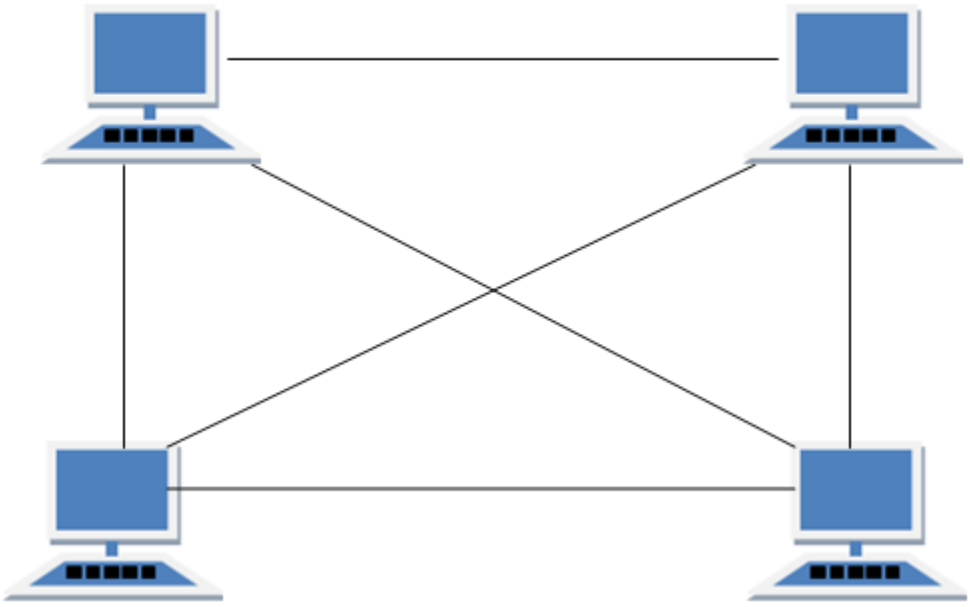
1. Routing
2. Flooding

MESH Topology: Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

MESH Topology: Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.



Types of Mesh Topology

1. **Partial Mesh Topology :** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology :** Each and every nodes or devices are connected to each other.

Features of Mesh Topology

1. Fully connected.
2. Robust.
3. Not flexible.

Advantages of Mesh Topology

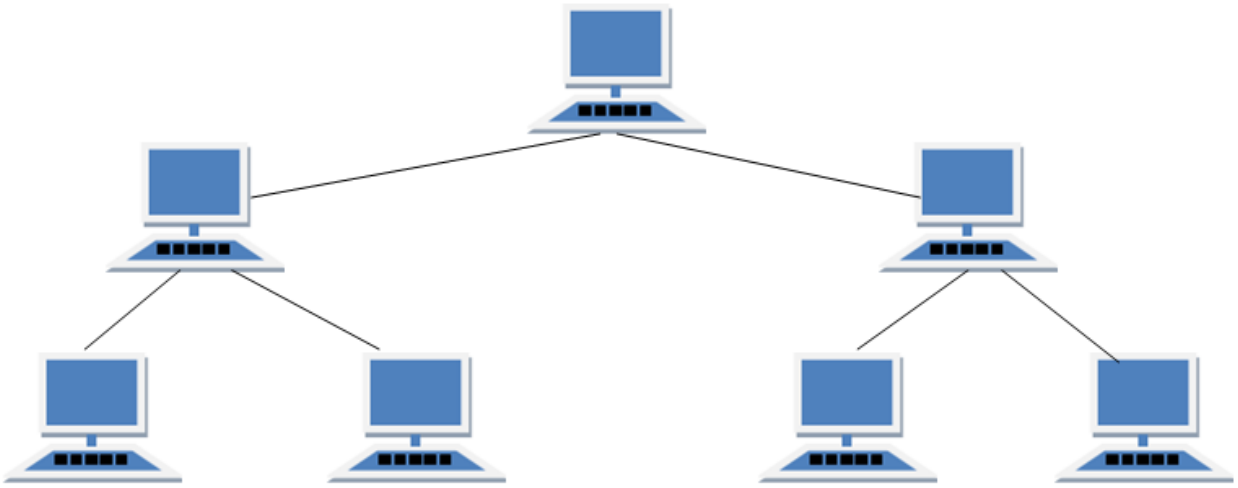
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

TREE Topology

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



Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

Advantages of Tree Topology

1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

Disadvantages of Tree Topology

1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

Q-3-Expalin CSMA/CD technique of accessing transmission channel.(2016(w),2017(s))

Ans-Carrier sense Multiple Access(CSMA)

- It was developed to minimize the chance of collision and to increase the performance.
- It requires that each station first listen to the medium before sending.
- It is based on the principle sense before transmit or listen before talk.

- It can reduce the possibility of collision, but it cannot eliminate it.
- In CSMA a station senses the carrier on the channel before starting its own transmission.
- The vulnerable time for CSMA is the propagation time Tp.
- propagation time needed for a signal to propagate from one end of the medium to the other.

When a station sends a frame, and any other station tries to send a frame during this time, a collision will result. When a channel is sense to be idle, a station can take one of the three different approaches to transmit a packet on to the channel.

CSMA with collision detection (CSMA/CD)

- CSMA/CD is the most commonly used protocol for LANs. CSMA/CD specifications were developed jointly by digital equipment corporation (DEC), Intel, and Xerox. This network is called as Ethernet. The IEEE802.3
- CSMA/CD stands for LAN are based on Ethernet specification.
- The basic protocol is that, a station with a message to send must monitor the channel to see if any other station is sending. If another station is sending, the second station must wait or defer, until the sending station has finished. Then it may send its message. If no station was sending at the time that it first listened, the station may send its message immediately. The term carrier sense indicates this listening before transmitting behaviour.
- **Carrier Sense Multiple Access/Collision Detect** (CSMA/CD) is the protocol for carrier transmission access in Ethernet networks.
- **Carrier-sense multiple access with collision detection** describes how the Ethernet protocol regulates communication among nodes
- On Ethernet, any station can send a frame at any time. Each station senses whether the medium is idle and therefore available for use. If it is, the station begins to transmit its first frame. If another station also tries to transmit at the same time, a collision occurs

and the frames are discarded and then a jamming signal is sent throughout the network in order to notify all stations of the collision.

- Each station then waits for a random period of time and retries. If another collision occurs, the time intervals from which the random waiting time is selected are increased step by step. This is known as exponential back off. The stations retry until

successful transmission of the frame.CSMA/CD is specified in the IEEE 802.3 standard.

Q-4-Explain FDDI.(2016(w),2017)

Ans- Fiber-Distributed Data Interface (FDDI)

- FDDI networks offered transmission speeds of 100 Mbps, which initially made them quite popular for high-speed networking. With the advent of 100-Mbps Ethernet, which is cheaper and easier to administer, FDDI has waned in popularity.

- FDDI (Fiber-Distributed Data Interface) is a standard for data transmission on fiber optic lines in that can extend in range up to 200 km (124 miles). The FDDI protocol is based on the token ring protocol. In addition to being large geographically, an FDDI local area network can support thousands of users.
- An FDDI network contains two token rings, one for possible backup in case the primary ring fails. The primary ring offers up to 100 Mbps capacity. If the secondary ring is not needed for backup, it can also carry data, extending capacity to 200 Mbps. The single ring can extend the maximum distance; a dual ring can extend 100 km (62 miles).
- FDDI is a product of American National Standards Committee X3-T9 and conforms to the open system interconnect (OSI) model of functional layering. It can be used to interconnect LANs using other protocols. FDDI-II is a version of FDDI that adds the capability to add circuit-switched service to the network so that voice signals can also behandled. Work is underway to connect FDDI networks to the developing Synchronous Optical Network

Function of FDDI

- The Fiber Distributed Data Interface (FDDI) specifies a 100-Mbps token-passing, dual-ring LAN using fiber-optic cable. FDDI is frequently used as high-speed backbone technology because of its support for high bandwidth and greater distances than copper.
- FDDI uses a dual-ring architecture with traffic on each ring flowing in opposite directions (called counter-rotating).
- The dual-rings consist of a primary and a secondary ring.
- During normal operation, the primary ring is used for data transmission, and the secondary ring remains idle.
- The primary purpose of the dual rings, as will be discussed in detail later in this chapter, is to provide superior reliability and robustness. Figure 1 shows the counter-rotating primary and secondary FDDI rings.

Q-5-Identify the Access technique model,Explain the features of all techniques.(2017(s))

Ans-Carrier sense Multiple Access(CSMA)

- It was developed to minimize the chance of collision and to increase the performance.
- It requires that each station first listen to the medium before sending.
- It is based on the principle sense before transmit or listen before talk.
- It can reduce the possibility of collision, but it cannot eliminate it.
- In CSMA a station senses the carrier on the channel before starting its own transmission.
- The vulnerable time for CSMA is the propagation time Tp.
- propagation time needed for a signal to propagate from one end of the medium to the other.

When a station sends a frame, and any other station tries to send a frame during this time, a collision will result. When a channel is sense to be idle, a station can take one of the three different approaches to transmit a packet on to the channel.
These three protocols are as follows:

Non-persistent CSMA

- In non-persistent CSMA, when a station having a packet to transmit and finds that the channel is busy, it backs off for a fixed interval of time.
- It then checks the channel again and if the channel is free then it transmits.

- The back-off delay is determined by the transmission of a frame, propagation time and other system parameter.
- If the channel is already in use, the station does not continuously sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission. But it waits a random period of time and again check for activity.

1-Persistent CSMA

- Any station wishing to transmit, monitor the channel continuously until the channel is idle and then transmit with probability one, hence the name 1-persistent.
- When two or more stations are waiting to transmit, a collision is guaranteed. Since each station will transmit immediately at the end of busy period. In this case each will wait a random amount of time and will then reattempt to transmit.
- As in the case with non-persistent CSMA, the performance of 1-persistent CSMA protocol depends only on the channel delay time.

P-Persistent CSMA:-

- To reduce the probability of collision in 1-persistent CSMA, not all allowed transmitting immediately, after the channel is idle.
- When a station becomes ready to send and its sense the channel to be idle, it either transmits with a probability p or it defers transmission by one time slot with a probability q=1-p.if the differed slot is also idle, the station either transmits with probability p or defers again with a probability q.this process is repeated until either packets are transmitted of the channel is busy.

CSMA with collision detection (CSMA/CD)

- CSMA/CD is the most commonly used protocol for LANs. CSMA/CD specifications were developed jointly by digital equipment corporation (DEC), Intel, and Xerox. This network is called as Ethernet. The IEEE802.3
- CSMA/CD stands for LAN are based on Ethernet specification.
- The basic protocol is that, a station with a message to send must monitor the channel to see if any other station is sending. If another station is sending, the second station must wait or defer, until the sending station has finished. Then it may send its message. If no station was sending at the time that it first listened, the station may send its message immediately. The term carrier sense indicates this listening before transmitting behaviour.
- **Carrier Sense Multiple Access/Collision Detect** (CSMA/CD) is the protocol for carrier transmission access in Ethernet networks.
- **Carrier-sense multiple access with collision detection** describes how the Ethernet protocol regulates communication among nodes
- On Ethernet, any station can send a frame at any time. Each station senses whether the medium is idle and therefore available for use. If it is, the station begins to transmit its first frame. If another station also tries to transmit at the same time, a collision occurs

and the frames are discarded and then a jamming signal is sent throughout the network in order to notify all stations of the collision.

- Each station then waits for a random period of time and retries. If another collision occurs, the time intervals from which the random waiting time is selected are increased step by step. This is known as exponential back off. The stations retry until

successful transmission of the frame.CSMA/CD is specified in the IEEE 802.3 standard.

CSMA with collision avoidance (CSMA/CA) Collision avoidance is used to improve the performance of the CSMA method by attempting to divide the channel somewhat equally among all transmitting nodes within the collision domain.

1. Carrier Sense

- Prior to transmitting, a node first listens to the shared medium (such as listening for wireless signals in a wireless network) to determine whether another node is transmitting or not.

2. Collision Avoidance

- If another node was heard, we wait for a period of time for the node to stop transmitting before listening again for a free communications channel.
- Request to Send/Clear to Send (RTS/CTS) may optionally be used at this point to mediate access to the shared medium. This goes some way to alleviating the problem of hidden nodes because, for instance, in a wireless network, the Access Point only issues a Clear to send to one node at a time.
- Transmission: if the medium was identified as being clear or the node received CTS to explicitly indicate it can send, it sends the frame in its entirety.

7-MARKS

Q-2-Discuss the features of Ethernet ,Token ring and Token Bus in LAN standards.(2016(w),2017)

Ans-Token Bus Network

- In this system, the nodes are physically connected as a bus, but logically form a ring with tokens passed around to determine the turns for sending. It has the robustness of the 802.3 broadcast cable and the known worst case behaviour of a ring. The structure of a token bus network is as follows:

Token Ring

- The most common local area network alternative to Ethernet is a network technology developed by IBM, called **token ring**.
- Where Ethernet relies on the random gaps between transmissions to regulate access to the medium, token ring implements a strict, orderly access method.
- A token-ring network arranges nodes in a logical ring, as shown below. The nodes forward frames in one direction around the ring, removing a frame when it has circled the ring once.
- The ring initializes by creating a**token**, which is a special type of frame that gives a station permission to transmit.
- The token circles the ring like any frame until it encounters a station that wishes to transmit data.
- This station then "captures" the token by replacing the token frame with a data-carrying frame, which encircles the network.
- Once that data frame returns to the transmitting station, that station removes the data frame, creates a new token and forwards that token on to the next node in the ring.
- Token-ring nodes do not look for a carrier signal or listen for collisions; the presence of the token frame provides assurance that the station can transmit a data frame without fear of another station interrupting.
- Because a station transmits only a single data frame before passing the token along, each station on the ring will get a turn to communicate in a deterministic and fair manner. Token-ring networks typically transmit data at either 4 or 16 Mbps.

Switched Ethernet

- It refers to the use of switches in an Ethernet network .This term was more commonly used when networks were being transitioned from hubs to switches. Today ,Ethernet switches are the norm ,even low cost 5-port unit is switch rather then a hub.
- An Ethernet LAN that uses switches to connect individual hosts or segments.
- In the case of individual hosts, the switch replaces the repeater and effectively gives the device full 10 Mbps bandwidth (or 100 Mbps for Fast Ethernet) to the rest of the network.
- This type of network is sometimes called a *desktop switched Ethernet.* In the case of segments, the hub is replaced with a switching hub. Traditional Ethernets, in which all hosts compete for the same bandwidth, are called shared Ethernets.
- Switched Ethernets are becoming very popular because they are an effective and convenient way to extend the bandwidth of existing Ethernets.
- Modern Ethernet implementations often look nothing like their historical counterparts.
- Where long runs of coaxial cable

provided attachments for multiple
stations in legacy Ethernet, modern
Ethernet networks use twisted pair
wiring or fiber optics to connect
stations in a **radial pattern**.

- Where legacy Ethernet networks

transmitted data at 10 megabits per
second (Mbps), modern networks can
operate at 100 or even 1,000 Mbps!

- Perhaps the most striking advancement in contemporary Ethernet networks is the use of **switched Ethernet**.
- Switched networks replace the shared medium of legacy Ethernet with a dedicated segment for each station.
- These segments connect to a switch, which acts much like an Ethernet bridge, but can connect many of these single station segments.

Q-3-Define Ethernet. Explain types of Ethernet.(2017(w))

Ans-Ethernet/IEEE 802.3 Frame

- 802.3 is the standard which Ethernet operates by. It is the standard for CSMA/CD (Carrier Sense Multiple Access with Collision Detection). This standard encompasses both the MAC and Physical Layer standards

- CSMA/CD is what Ethernet uses to control access to the network medium (network cable). If there is no data, any node may attempt to transmit, if the nodes detect a collision, both stop transmitting and wait a random amount of time before retransmitting the data.
- The original 802.3 standard is 10 Mbps (Megabits per second). 802.3u defined the 100 Mbps (Fast Ethernet) standard, 802.3z/802.3ab defined 1000 Mbps Gigabit Ethernet, and 802.3ae define 10 Gigabit Ethernet.
- Commonly, Ethernet networks transmit data in packets, or small bits of information. A packet can be a minimum size of 72 bytes or a maximum of 1518 bytes. The most common topology for Ethernet is the star topology.

10 Base-5 (Thick Ethernet)

IEEE-spec	802.3
Max. speed	10 Mbps

Cable	Standard Ethernet Coax Cable
Connectors	N-type
Terminators	50 ohm
Max. length of a segment	500m/1640ft
Max. number of taps per segment	100
Max. number of stations per network	1024
Min. distance between taps	2.5m/8.3ft
Max. length of transceiver cable	50m/164ft
Max. number of repeaters	4
Topology	Bus

BASE-2 (Thin Ethernet)

IEEE-norm	802.3
Maximum speed	10 Mbps
Cable	RG58
Connectors	BNC
Terminators	50 ohm
Max. length of a segment	185m/607ft
Max. number of taps per segment	30
Max. amount of stations per network	1024
Min. distance between taps	0.5m/1.65ft
Max. number of repeaters	4
Topology	Bus

10BASE-T(Twisted-Pair Ethernet)

IEEE-spec	802.3
Wire speed	10 Mbps
Cable type	UTP CAT 3, 4 and 5
Connector type	RJ45
Used pins	1 & 2, 3 & 6
Max. length of a segment	100m/328ft
Max. number of taps per segment	2
Max. amount of stations per network	1024
Max. amount of repeaters	4
Topology	Star

CHAPTER-7

2-MARKS

Q-1-Define Internet Protocol.(2016w)-2017(w))

Ans-IP Protocol

- The IP protocol and its associated routing protocols are possibly the most significant of the entire TCP/IP suite. IP is responsible for the following

IP addressing

- The IP addressing conventions are part of the IP protocol. Designing an IPv4 Addressing Scheme introduces IPv4 addressing and IPv6 Addressing Overview introduces IPv6 addressing.
- Host-to-host communications – IP determines the path a packet must take, based on the receiving system's IP address.

Q-2-What do you mean by Internetworking?(2016,2017)

Ans-Internetworking is the process or technique of connecting different networks by using intermediary devices such as routers or gateway devices.

Internetworking ensures data communication among networks owned and operated by different entities using a common data communication and the Internet Routing Protocol

Q-3-TCP?IP.(2016(w),2017)

Ans-TCP/IP protocol suite

- This section presents an in-depth introduction to the protocols that are included in TCP/IP. Although the information is conceptual, you should learn the names of the protocols.
- TCP/IP" is the acronym that is commonly used for the set of network protocols that compose the Internet Protocol suite. Many texts use the term "Internet" to describe both the protocol suite and the global wide area network.

5-MARKS

Q-1-Expalin the TCP/IP protocol suite.(2016-2017(w,s)

Ans-TCP/IP Model Layers

The TCP/IP model uses four layers that logically span the equivalent of the top six layers of the OSI reference model; this is shown (The physical layer is not covered by the TCP/IP model because the data link layer is considered the point at which the interface occurs between the TCP/IP stack and the underlying networking hardware.) The following are the TCP/IP model layers, starting from the bottom.

Physical network layer

- The physical network layer specifies the characteristics of the hardware to be used for the network.
- For example, physical network layer specifies the physical characteristics of the communications media.
- The physical layer of TCP/IP describes hardware standards such as IEEE 802.3, the specification for Ethernet network media, and RS-232, the specification for standard pin connectors.

Data-Link Layer

- The data-link layer identifies the network protocol type of the packet, in this instance TCP/IP.
- The data-link layer also provides error control and "framing."
- Examples of data-link layer protocols are Ethernet IEEE 802.2 framing and Point-to-Point Protocol (PPP) framing.

Network Layer

- The Internet layer, also known as the network layer or IP layer, accepts and delivers packets for the network.
- This layer includes the powerful Internet Protocol (IP), the Address Resolution Protocol (ARP), and the Internet Control Message Protocol (ICMP).

IP Protocol

- The IP protocol and its associated routing protocols are possibly the most significant of the entire TCP/IP suite. IP is responsible for the following:

IP addressing

- The IP addressing conventions are part of the IP protocol. Designing an IPv4 Addressing Scheme introduces IPv4 addressing and IPv6 Addressing Overview introduces IPv6 addressing.
- Host-to-host communications – IP determines the path a packet must take, based on the receiving system's IP address.

ARP Protocol

- The Address Resolution Protocol (ARP) conceptually exists between the data-link and Internet layers.

- ARP assists IP in directing datagram's to the appropriate receiving system by mapping Ethernet addresses (48 bits long) to known IP addresses (32 bits long).

ICMP Protocol

- The Internet Control Message Protocol (ICMP) detects and reports network error conditions. ICMP reports on the following:
- Dropped packets – Packets that arrive too fast to be processed
- Connectivity failure – A destination system cannot be reached

Transport Layer

- The TCP/IP transport layer ensures that packets arrive in sequence and without error, by swapping acknowledgments of data reception, and retransmitting lost packets.
- This type of communication is known as end-to-end. Transport layer protocols at this level are Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP). TCP and SCTP provide reliable, end-to-end service.
- UDP provides unreliable datagram service.

TCP Protocol

- TCP enables applications to communicate with each other as though they were connected by a physical circuit.
- TCP sends data in a form that appears to be transmitted in a character-by-character fashion, rather than as discrete packets. This transmission consists of the following:

SCTP Protocol

- SCTP is a reliable, connection-oriented transport layer protocol that provides the same services to applications that are available from TCP.
- Moreover, SCTP can support connections between systems that have more than one address, or multihued.
- The SCTP connection between sending and receiving system is called an association.

Application Layer

- The application layer defines standard Internet services and network applications that anyone can use.
- These services work with the transport layer to send and receive data. Many application layer protocols exist.
- The basic packet consists of a header with the sending and receiving systems' addresses, and a body, or payload, with the data to be transferred.
- As the packet travels through the TCP/IP protocol stack, the protocols at each layer either add or remove fields from the basic header.
- When a protocol on the sending system adds data to the packet header, the process is called data encapsulation.

Q-2-Discuss the format of IP datagram.(2017(s))

Ans-Format of an IP Datagram

The format of data that can be recognized by IP is called an IP datagram. It consists of two components, namely, the header and data, which need to be transmitted. The fields in the datagram, except the data, have specific roles to perform in the transmission of data. Every field in the IP datagram has a fixed size except for the IP Options field, which can be 20–60 bytes in length. The sending computer sends a message to the protocol in the same layer on the destination computer by using the header.

`Version`

This field specifies the version of IP used for transferring data. The size of the `Version` field is 4 bits. Both the sender and the receiver must use the same version of IP to ensure proper interpretation of the fields in the datagram.

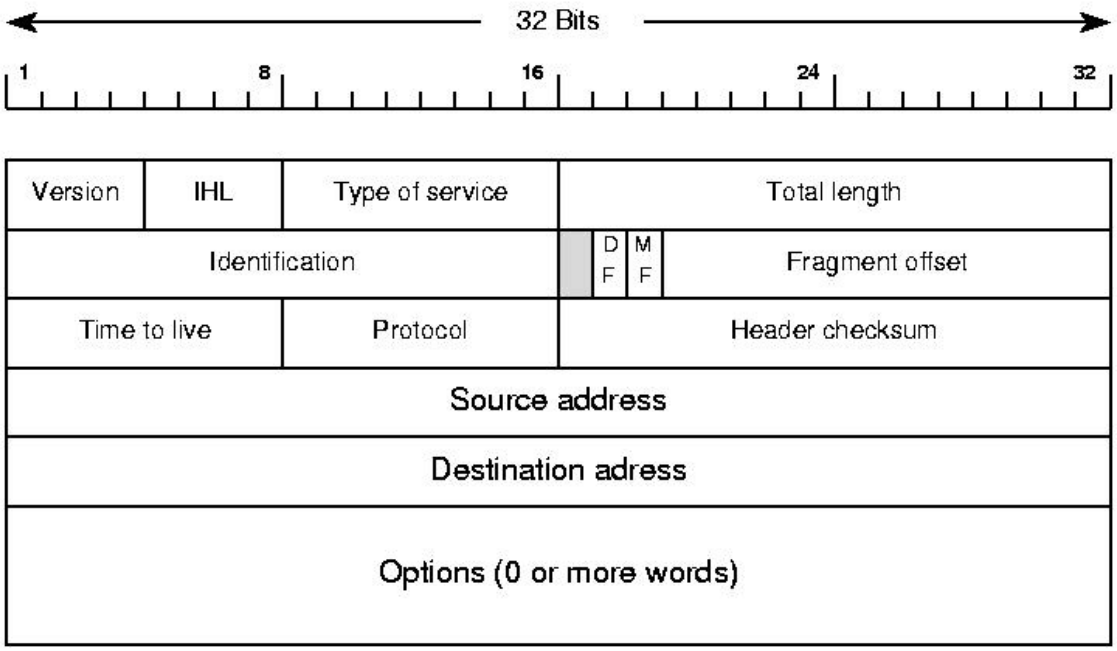
`Header Length`

The size of the `Header Length` or the `IHL` field is 4 bits. The `Header Length` field is used to specify the length of header, which can range from 20 to 60 bytes. You must multiply the value in this field by four to get the length of the IP header. For example, if the value in this field is `3`, the length of the header is `3*4`, which is 12 bytes.

`Total Length`

The `Total Length` field specifies the total length of the datagram. The size of the field is 16 bits. The `Total Length` field can be calculated as follows:

```
Total length of the datagram = Length of the header + Length of the data
```


32 Bits
1
8
16
24
32
Version
IHL
Type of service
Total length
Identification
D F
M F
Fragment offset
Time to live
Protocol
Header checksum
Source address
Destination adress
Options (0 or more words)