CMR INSTITUTE OF TECHNOLOGY	USN			
Internal Assesment Test – I Answer Key				
Subject : Computer Networks				Code : 17MCA31
Date : 07/09/2018	Duration : 90 mins	Max Marks : 50	Sem : III	Branch : MCA

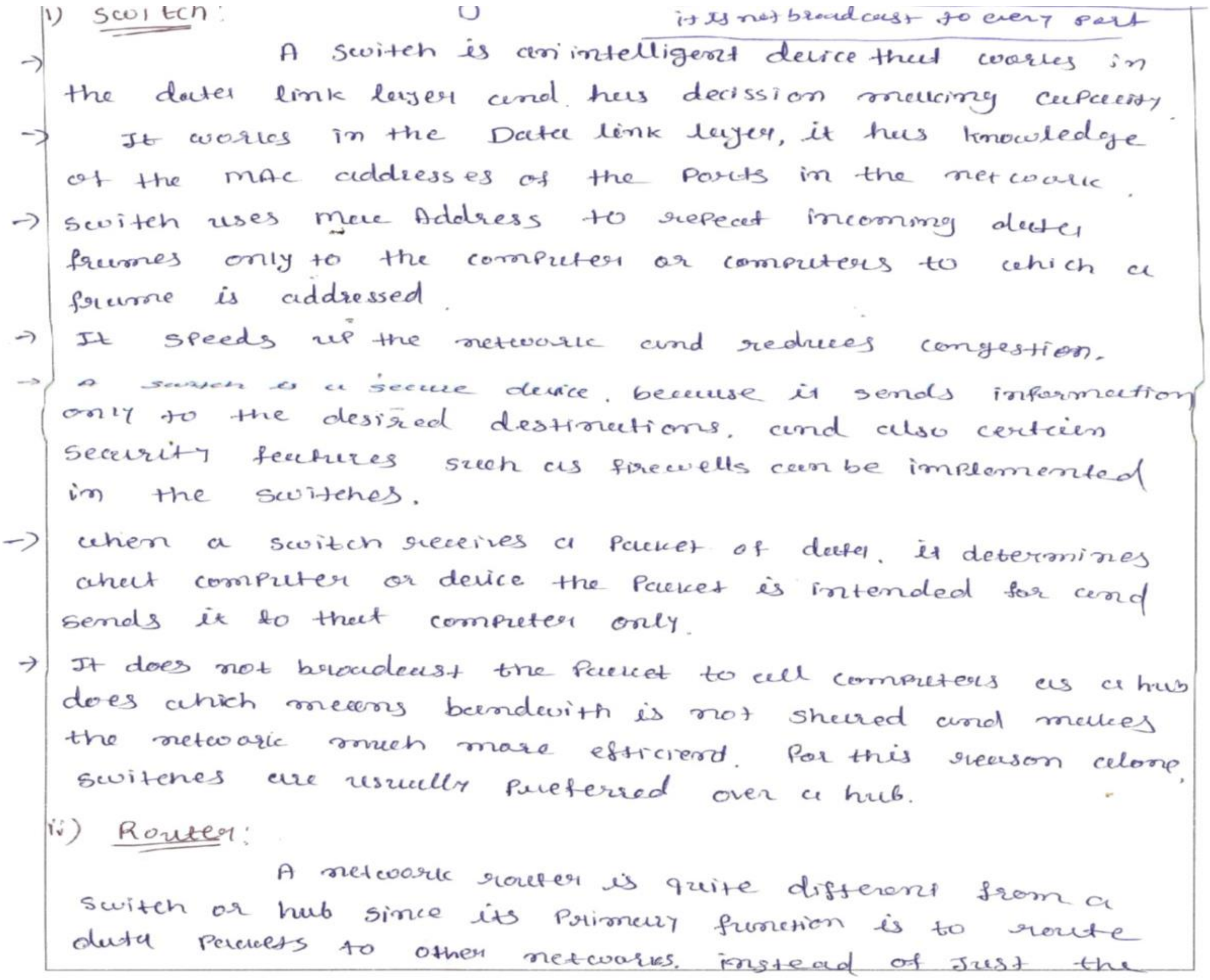
			OBE	
	Answer FIVE FULL Questions,choosing ONE Full Question From Each Module	Marks	CO	RBT
1	**Explain the uses of computer networks. define the Terms :switch, hub, router.**	[10]	CO1	L1

Use of Computer Networks?

A computer network, often simply referred to as a network, is a group of computers and devices interconnected by communications channels that facilitate communications among users and allows users to share resources and information. In the 1960s, the Advanced Research Projects Agency (ARPA) started funding the design of the Advanced Research Projects Agency Network (ARPANET) for the United States Department of Defense. It was the first computer network in the world. Development of the network began in 1969, based on designs developed during the 1960s.

Computer networks are collections of autonomous computers, e.g., the Internet They have many uses:

Business Applications » Home Applications » Mobile Users » Social Issues »



1) Switch:

it is not broadcast to every port

-> A switch is an intelligent device that works in the data link layer and has decission making capacity

-> It works in the Data link layer, it has knowledge of the MAC addresses of the Ports in the network.

-> switch uses Mac Address to repeat incoming data frames only to the computer or computers to which a frame is addressed.

-> It speeds up the network and reduces congestion.

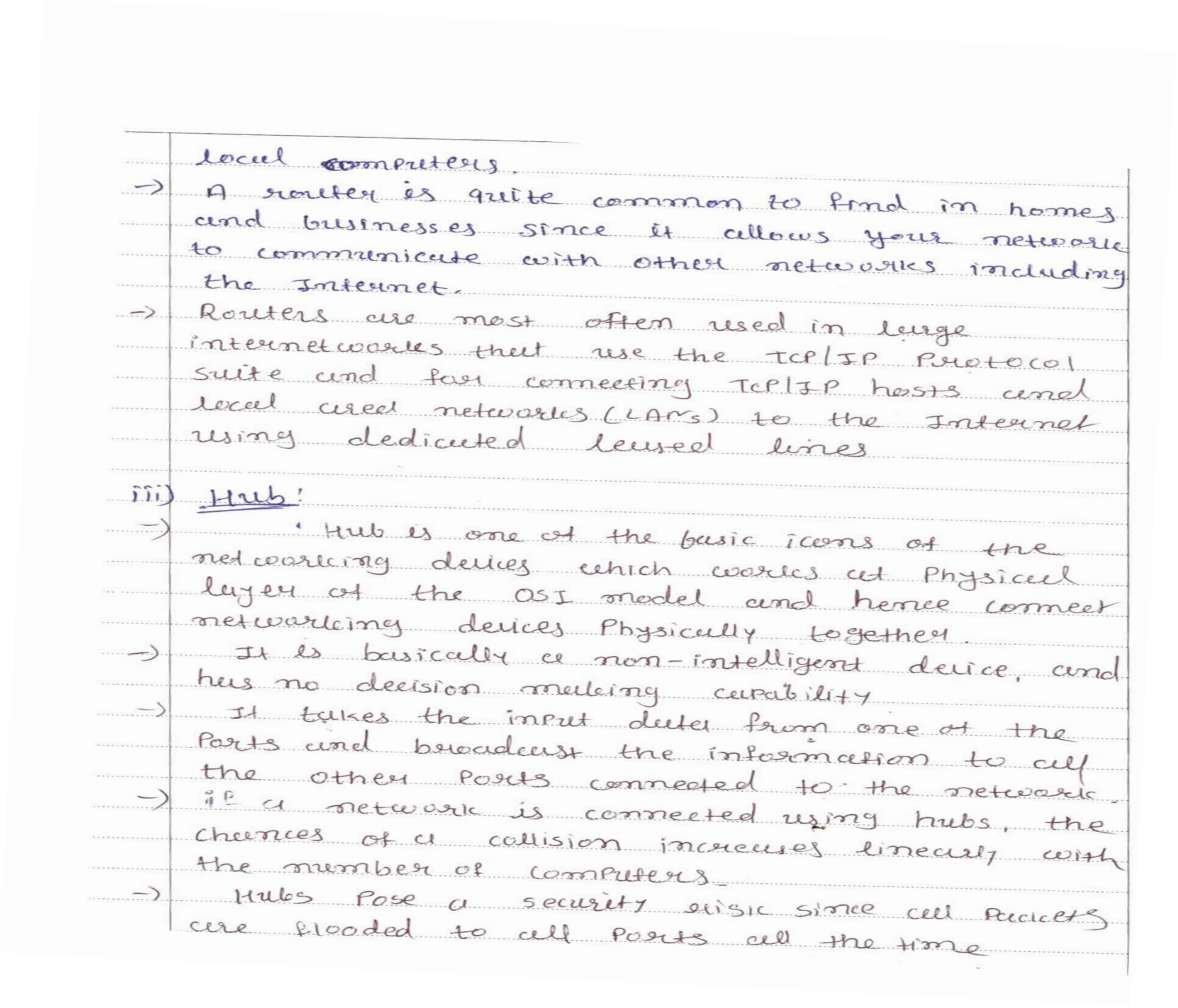
-> A switch is a secure device, because it sends information only to the desired destinations, and also certain security features such as firewalls can be implemented in the switches.

-> when a switch receives a Packet of data, it determines what computer or device the Packet is intended for and sends it to that computer only.

-> It does not broadcast the Packet to all computers as a hub does which means bandwith is not shared and makes the network much more efficient. For this reason alone, switches are usually Preferred over a hub.

ii) Router:

A network router is quite different from a switch or hub since its Primary function is to route data Packets to other networks, instead of just the



local computers.

→ A router is quite common to find in homes and businesses since it allows your network to communicate with other networks including the Internet.

→ Routers are most often used in large internetworks that use the TCP/IP Protocol suite and for connecting TCP/IP hosts and local area networks (LANs) to the Internet using dedicated leased lines

iii) Hub:

→ 'Hub is one of the basic icons of the networking devices which works at Physical layer of the OSI model and hence connect networking devices Physically together.

→ It is basically a non-intelligent device, and has no decision making capability

→ It takes the input data from one of the Ports and broadcast the information to all the other Ports connected to the network.

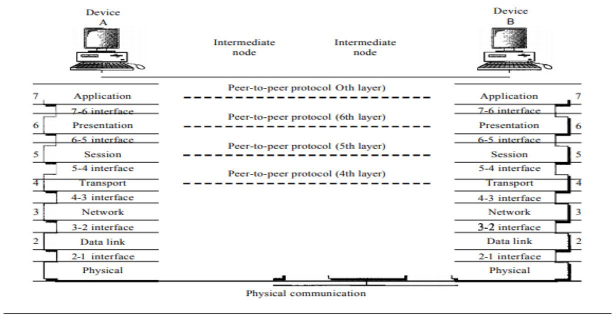
→ if a network is connected using hubs, the chances of a collision increases linearly with the number of computers.

→ Hubs Pose a security risk since all Packets are flooded to all Ports all the time

2 **Draw the OSI network architecture. Explain each layer in detail.** [10] CO2 L2

the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection model. It was first introduced in the late 1970s.

The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network



LAYERS IN THE OSI MODEL

1) Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium.

It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to Occur.

Representation of bits. The physical layer data consists of a stream of bits (sequence of Os or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding (how Os and Is are changed to signals).

Data rate. The transmission rate-the number of bits sent each second-is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.

Synchronization of bits. The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.

Physical topology. The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology (every device is connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), a bus topology (every device is on a common link), or a hybrid topology (this is a combination of two or more topologies).

Transmission mode. The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex. In simplex mode, only one device can send; the other can only receive. The simplex mode is a one-way communication. In the half-duplex mode, two devices can send and receive, but not at the same time. In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

2) Data Link Layer

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer).

Other responsibilities of the data link layer include the following:

Framing. The data link layer divides the stream of bits received from the network layer into manageable data units called frames. The data link layer is responsible for moving frames from one hop (node) to the next.

Physical addressing. If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.

Flow control. If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

Error control. The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.

Access control. When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time

3)Network Layer

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.

If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery. Figure shows the relationship of the network layer to the data link and transport layers.

Logical addressing. The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.

Routing. When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

4)Transport Layer

The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

Service-point addressing.

Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address).

The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

Segmentation and reassembly.

A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

Connection control.

The transport layer can be either connectionless or connection oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.

flow control.

at this layer is performed end to end rather than across a single link.

error control

at this layer is performed process-to process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

5)Session Layer

The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems. The session layer is responsible for dialog control and synchronization.

Specific responsibilities of the session layer include the following:

Dialog control. The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.

Synchronization. The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

6) Presentation Layer

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

Translation. The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods.

Encryption. To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

Compression. Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

7). Application Layer

The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

In Figure shows the relationship of the application layer to the user and the presentation layer. Of the many application services available, the figure shows only three: XAOO (message-handling services), X.500 (directory services), and file transfer, access, and management (FTAM). The user in this example employs XAOO to send an e-mail message.

Specific services provided by the application layer include the following:

Network virtual terminal. A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.

File transfer, access, and management. This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

Mail services. This application provides the basis for e-mail forwarding and storage.

Directory services. This application provides distributed database sources and access for global information about various objects and services.

3 Explain a simplex stop-and-wait protocol for an error free channel [10] CO2 L2

In this method of flow control, the sender sends a single frame to receiver & waits for an acknowledgment.

• The next frame is sent by sender only when acknowledgment of previous frame is received.

• This process of sending a frame & waiting for an acknowledgment continues as long as the sender has data to send.

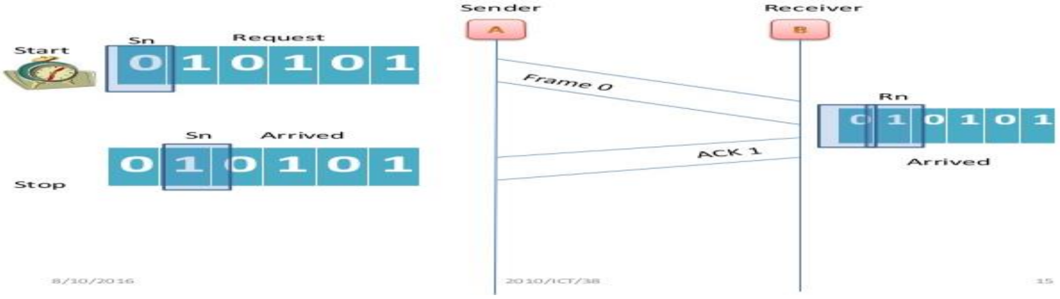
• To end up the transmission sender transmits end of transmission (EOT) frame.

• The main advantage of stop & wait protocols is its accuracy. Next frame is transmitted only when the first frame is acknowledged. So there is no chance of frame being lost.

• The main disadvantage of this method is that it is inefficient. It makes the transmission process slow. In this method single frame travels from source to destination and single acknowledgment travels from destination to source. As a result each frame sent and received uses the entire time needed to traverse the link. Moreover, if two devices are distance apart, a lot of time is wasted waiting for ACKs that leads to increase in total transmission time.

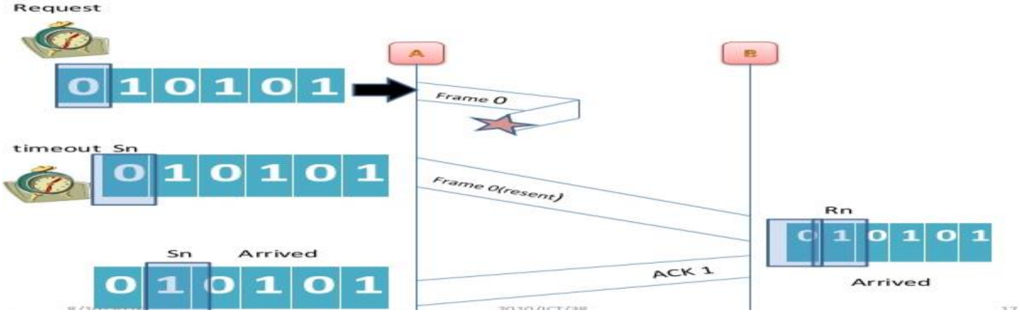
Case 1:-

- Sender sends the frame 0 to the destination and simultaneously a timer is started.
- The destination accepts the frame since it was expecting frame 0.
- Receiver sends an acknowledgement ACK 1 informing the sender that it has successfully received frame 0 and is expecting for frame1.
- This acknowledgement reaches sender before the timer of frame 0 expires.

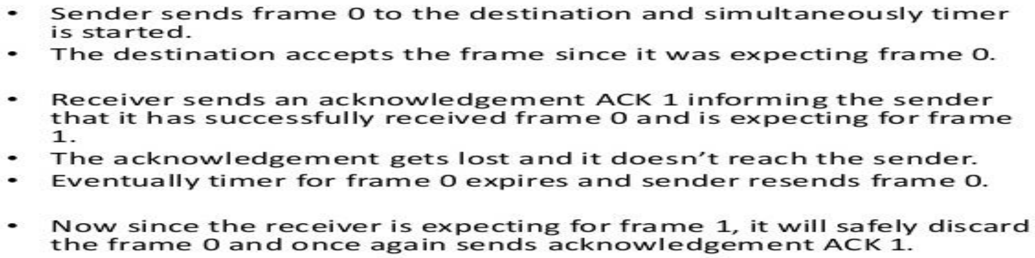


Case 2:-

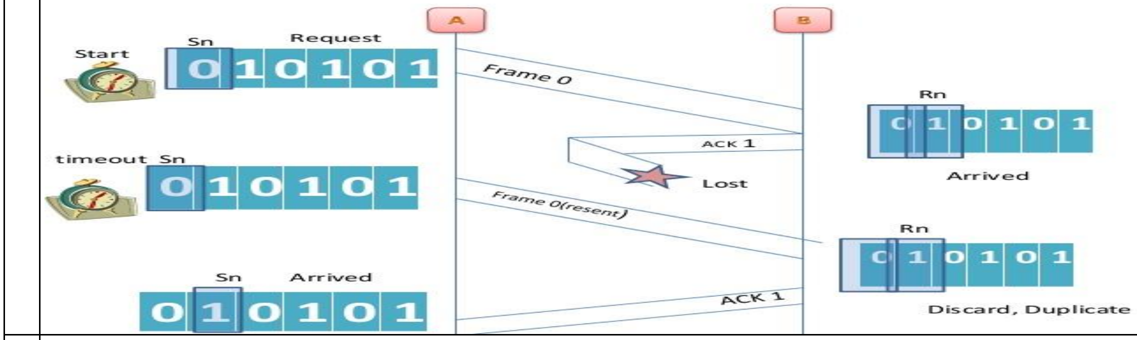
- sender sends frame 0 to the destination and simultaneously timer is started
- Frame o is lost before reaching the destination.
- Since destination didn't receive frame 0 no acknowledgement is sent.
- Eventually timer for frame 0 expires and sender resends frame 0.
- This process continues until it reaches acknowledgement for frame 1.



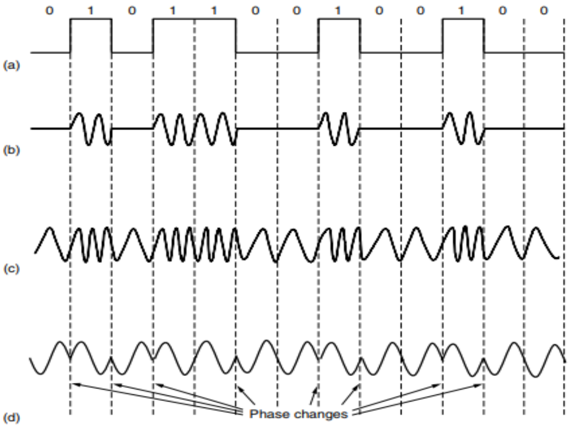
Case 3:-



- Sender sends frame 0 to the destination and simultaneously timer is started.
- The destination accepts the frame since it was expecting frame 0.
- Receiver sends an acknowledgement ACK 1 informing the sender that it has successfully received frame 0 and is expecting for frame 1.
- The acknowledgement gets lost and it doesn’t reach the sender.
- Eventually timer for frame 0 expires and sender resends frame 0.
- Now since the receiver is expecting for frame 1, it will safely discard the frame 0 and once again sends acknowledgement ACK 1.



4 **Show the NRZ,NRZI and Manchester encoding for the bits pattern 0101100100100.** [10] CO2 L2



5 **What is Sliding window? Explain Types of Sliding Window.** [10] CO3 L2

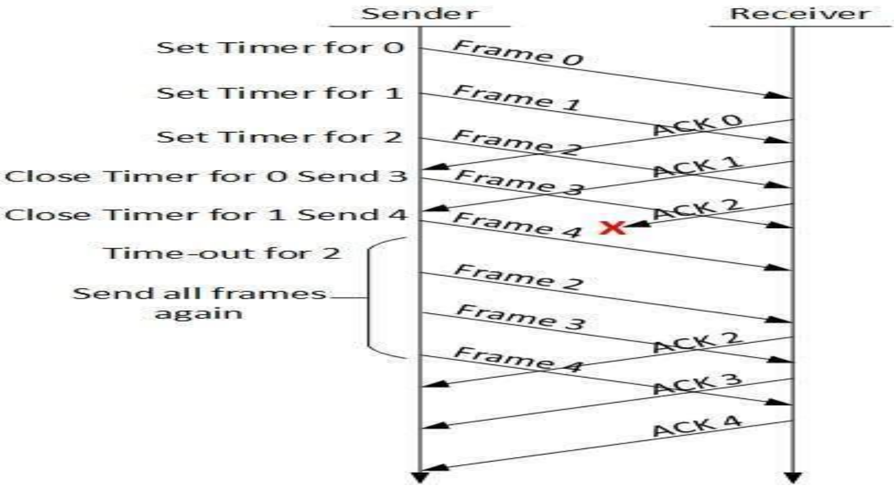
data frames were transmitted in one direction only. In most practical situations, there is a need to transmit data in both directions. One way of achieving full-duplex data transmission is to run two instances of one of the previous protocols, each using a separate link for simplex data traffic (in different directions). Each link is then comprised of a ‘‘forward’’ channel (for data) and a ‘‘reverse’’ channel (for acknowledgements). In both cases the capacity of the reverse channel is almost entirely wasted.

A better idea is to use the same link for data in both directions. After all, in protocols 2 and 3 it was already being used to transmit frames both ways, and the reverse channel normally has the same capacity as the forward channel. In this model the data frames from A to B are intermixed with the acknowledgement frames from A to B. By looking at the kind field in the header of an incoming frame, the receiver can tell whether the frame is data or an acknowledgement.

Types of Sliding window:-

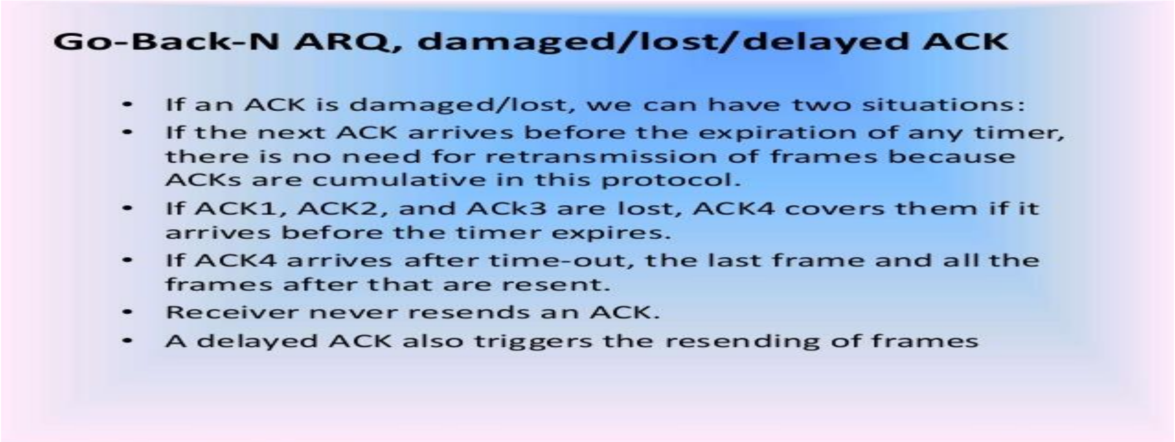
1)GO-BACK-N

Stop and wait ARQ mechanism does not utilize the resources at their best.When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window.



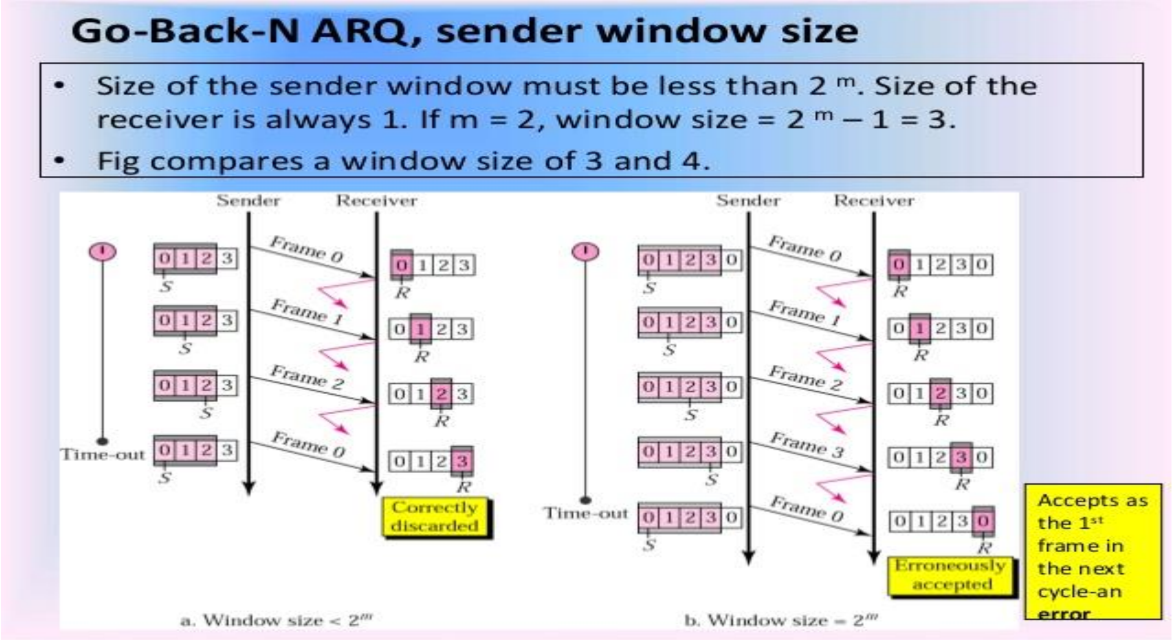
The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.

When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.



Go-Back-N ARQ, damaged/lost/delayed ACK

- If an ACK is damaged/lost, we can have two situations:
- If the next ACK arrives before the expiration of any timer, there is no need for retransmission of frames because ACKs are cumulative in this protocol.
- If ACK1, ACK2, and ACk3 are lost, ACK4 covers them if it arrives before the timer expires.
- If ACK4 arrives after time-out, the last frame and all the frames after that are resent.
- Receiver never resends an ACK.
- A delayed ACK also triggers the resending of frames



Go-Back-N ARQ, sender window size

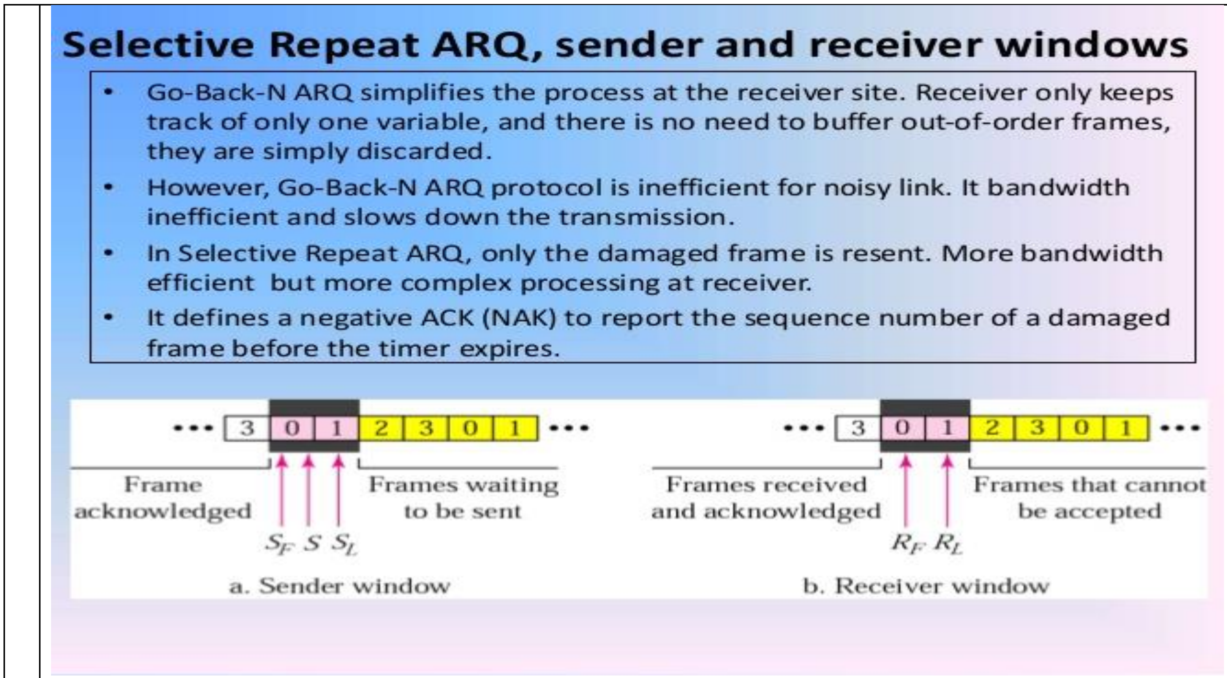
- Size of the sender window must be less than 2 ^{m}. Size of the receiver is always 1. If m = 2, window size = 2 ^{m} – 1 = 3.
- Fig compares a window size of 3 and 4.

a. Window size < 2^m

b. Window size = 2^m

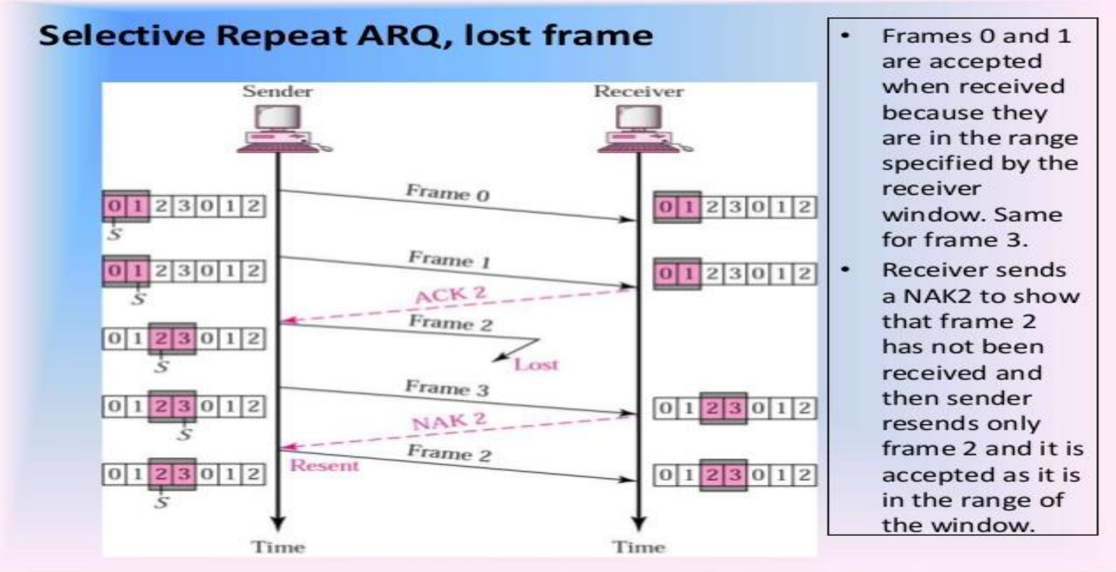
2) Selective Repeat ARQ

In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.



Selective Repeat ARQ, sender and receiver windows

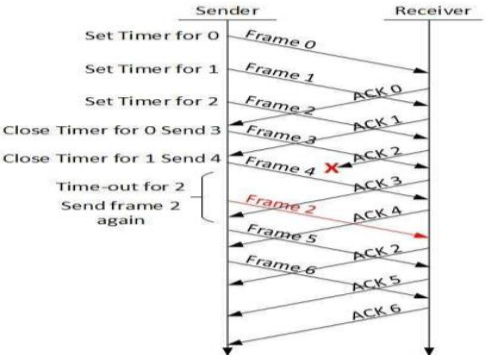
- Go-Back-N ARQ simplifies the process at the receiver site. Receiver only keeps track of only one variable, and there is no need to buffer out-of-order frames, they are simply discarded.
- However, Go-Back-N ARQ protocol is inefficient for noisy link. It bandwidth inefficient and slows down the transmission.
- In Selective Repeat ARQ, only the damaged frame is resent. More bandwidth efficient but more complex processing at receiver.
- It defines a negative ACK (NAK) to report the sequence number of a damaged frame before the timer expires.



Selective Repeat ARQ, lost frame

- Frames 0 and 1 are accepted when received because they are in the range specified by the receiver window. Same for frame 3.
- Receiver sends a NAK2 to show that frame 2 has not been received and then sender resends only frame 2 and it is accepted as it is in the range of the window.

In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged.



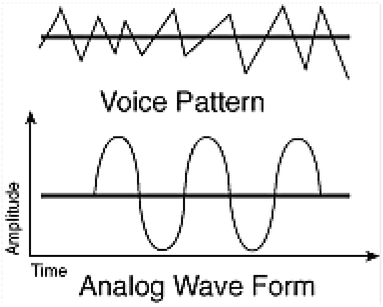
The sender in this case, sends only packet for which NACK is received.

6	**Explain Analog and Digital Signal.** **Analog and Digital Transmission** There are a number of differences between analog and digital transmission, and it is important to understand how conversions	[10]	CO2 L3

between analog and digital occur. Let's look first at the older form of transmission, analog.

Analog Transmission

- The term analog data refers to information that is continuous. For example, an analog clock that has hour, minute, and second hands gives information in a continuous form; the movements of the hands are continuous.
- Analog data, such as the sounds made by a human voice, take on continuous values. When someone speaks, an analog wave is created in the air. This can be captured by a microphone and converted to an analog signal or sampled and converted to a digital signal. An analog signal has infinitely many levels of intensity over a period of time.
- As the wave moves from value A to value B, it passes through and includes an infinite number of values along its path.
- An analog wave form (or signal) is characterized by being continuously variable along amplitude and frequency. In the case of telephony, for instance, when you speak into a handset, there are changes in the air pressure around your mouth. Those changes in air pressure fall onto the handset, where they are amplified and then converted into current, or voltage fluctuations. Those fluctuations in current are an analog of the actual voice pattern—hence the use of the term *analog* to describe these signals



- Analog facilities have limited bandwidth, which means they cannot support high-speed data. Another characteristic of analog is that noise is accumulated as the signal traverses the network.

- As the signal moves across the distance, it loses power and becomes impaired by factors such as moisture in the cable, dirt on a contact, and critters chewing on the cable somewhere in the network. By the time the signal arrives at the amplifier, it is not only attenuated, it is also impaired and noisy.

- One of the problems with a basic amplifier is that it is a dumb device. All it knows how to do is to add power, so it takes a weak and impaired signal, adds power to it, and brings it back up to its original power level. But along with an increased signal, the amplifier passes along an increased noise level.

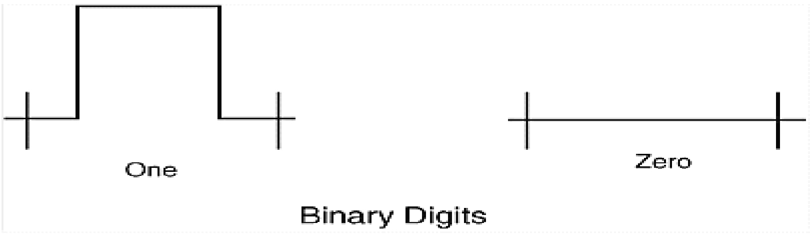
- So in an analog network, each time a signal goes through an amplifier, it accumulates noise. After you mix together coffee and cream, you can no longer separate them. The same concept applies in analog networks: After you mix the signal and the noise, you can no longer separate the two, and, as a result, you end up with very high error rates.

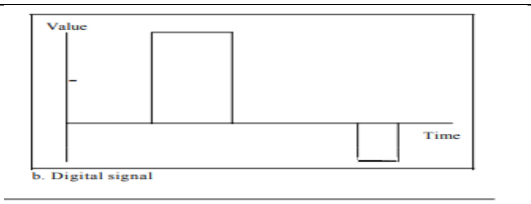
Digital Transmission

- digital data refers to information that has discrete states. Digital data take on discrete values. For example, data are stored in computer memory in the form of Os and 1s.

- A digital signal, on the other hand, can have only a limited number of defined values. They can be converted to a digital signal or modulated into an analog signal for transmission across a medium. Digital transmission is quite different from analog transmission.

- For one thing, the signal is much simpler. Rather than being a continuously variable wave form, it is a series of discrete pulses, representing one bits and zero .Each computer uses a coding scheme that defines what combinations of ones and zeros constitute all the characters in a character set (that is, lowercase letters, uppercase letters, punctuation marks, digits, keyboard control functions).





b. Digital signal

- How the ones and zeros are physically carried through the network depends on whether the network is electrical or optical. In electrical networks, one bits are represented as high voltage, and zero bits are represented as null, or low voltage. In optical networks, one bits are represented by the presence of light, and zero bits are represented by the absence of light.
- The ones and zeros—the on/off conditions—are carried through the network, and the receiving device repackages the ones and zeros to determine what character is being represented. Because a digital signal is easier to reproduce than an analog signal, we can treat it with a little less care in the network. Rather than use dumb amplifiers, digital networks use *regenerative repeaters*, also referred to as *signal regenerators*. As a strong, clean, digital pulse travels over a distance, it loses power, similar to an analog signal.
- The digital pulse, like an analog signal, is eroded by impairments in the network. But the weakened and impaired signal enters the regenerative repeater, where the repeater examines the signal to determine what was supposed to be a one and what was supposed to be a zero. The repeater regenerates a new signal to pass on to the next point in the network, in essence eliminating noise and thus vastly improving the error rate.

7 **What is Digital Modulation? Explain FDMA,TDMA and CDMA techniques i**

detail.

[10] CO2 L2

Frequency Division Multiple Access (FDMA)

- FDM (Frequency Division Multiplexing) takes advantage of passband transmission to share a channel. It divides the spectrum into frequency bands, with each user having exclusive possession of some band in which to send their signal. AM radio broadcasting illustrates FDM.
- The allocated spectrum is about 1 MHz, roughly 500 to 1500 kHz. Different frequencies are allocated to different logical channels (stations), each operating in a portion of the spectrum, with the interchannel separation great enough to prevent interference. For a more detailed example,

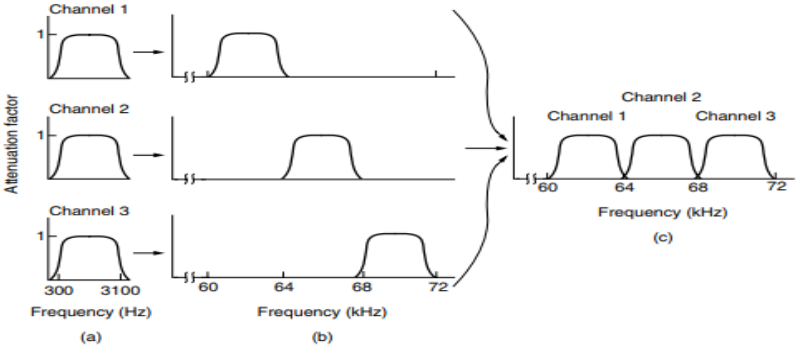
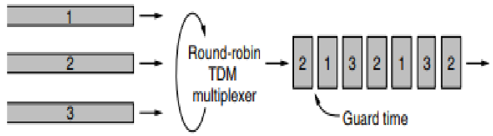


Figure 2-25. Frequency division multiplexing. (a) The original bandwidths. (b) The bandwidths raised in frequency. (c) The multiplexed channel.

- we show three voice-grade telephone channels multiplexed using FDM. Filters limit the usable bandwidth to about 3100 Hz per voice-grade channel. When many channels are multiplexed together, 4000 Hz is allocated per channel. The excess is called a guard band. It keeps the channels well separated. First the voice channels are raised in frequency, each by a different amount.
- Then they can be combined because no two channels now occupy the same portion of the spectrum. Notice that even though there are gaps between the channels thanks to the guard bands, there is some overlap between adjacent channels.
- The overlap is there because real filters do not have ideal sharp edges. This means that a strong spike at the edge of one channel will be felt in the adjacent one as nonthermal noise.

Time division multiple access (TDMA)

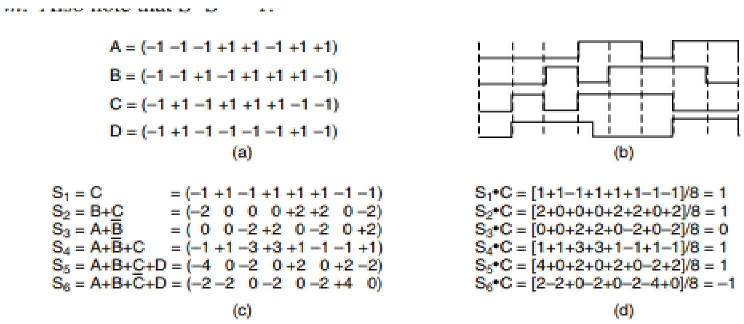
- An alternative to FDM is TDM (Time Division Multiplexing). Here, the users take turns (in a round-robin fashion), each one periodically getting the entire bandwidth for a little burst of time.
- An example of three streams being multiplexed with TDM is shown in Fig. Bits from each input stream are taken in a fixed time slot and output to the aggregate stream. This stream runs at the sum rate of the individual streams.
- For this to work, the streams must be synchronized in time. Small intervals of guard time analogous to a frequency guard band may be added to accommodate small timing variations.



- 1 2 3 Round-robin TDM multiplexer 2 1 3 2 1 3 Guard time 2 Figure. Time Division Multiplexing (TDM). TDM is used widely as part of the telephone and cellular networks. To avoid one point of confusion, let us be clear that it is quite different from the alternative STDM (Statistical Time Division Multiplexing). The prefix ‘‘statistical’’ is added to indicate that the individual streams contribute to the multiplexed stream not on a fixed schedule, but according to the statistics of their demand. STDM is packet switching by another name.

Code division multiple access (CDMA)

- There is a third kind of multiplexing that works in a completely different way than FDM and TDM. CDM (Code Division Multiplexing) is a form of spread spectrum communication in which a narrowband signal is spread out over a wider frequency band.
- This can make it more tolerant of interference, as well as allowing multiple signals from different users to share the same frequency band. Because code division multiplexing is mostly used for the latter purpose it is commonly called CDMA (Code Division Multiple Access).
- CDMA allows each station to transmit over the entire frequency spectrum all the time. Multiple simultaneous transmissions are separated using coding theory. Before getting into the algorithm, let us consider an analogy: an airport lounge with many pairs of people conversing. TDM is comparable to pairs of people in the room taking turns speaking.
- FDM is comparable to the pairs of people speaking at different pitches, some high-pitched and some low-pitched such that each pair can hold its own conversation at the same time as but independently of the others. CDMA is comparable to each pair of people talking at once, but in a different language.
- The French-speaking couple just hones in on the French, rejecting everything that is not French as noise. Thus, the key to CDMA is to be able to extract the desired signal while rejecting everything else as random noise. A somewhat simplified description of CDMA follows.



$A = (-1\ -1\ -1\ +1\ +1\ -1\ +1\ +1)$
$B = (-1\ -1\ +1\ -1\ +1\ +1\ +1\ -1)$
$C = (-1\ +1\ -1\ +1\ +1\ +1\ -1\ -1)$
$D = (-1\ +1\ -1\ -1\ -1\ -1\ +1\ -1)$

(a)

(b)

$S_1 = C = (-1\ +1\ -1\ +1\ +1\ +1\ -1\ -1)$
$S_2 = B+C = (-2\ 0\ 0\ 0\ +2\ +2\ 0\ -2)$
$S_3 = A+\bar{B} = (0\ 0\ -2\ +2\ 0\ -2\ 0\ +2)$
$S_4 = A+\bar{B}+C = (-1\ +1\ -3\ +3\ +1\ -1\ -1\ +1)$
$S_5 = A+B+C+D = (-4\ 0\ -2\ 0\ +2\ 0\ +2\ -2)$
$S_6 = A+B+\bar{C}+D = (-2\ -2\ 0\ -2\ 0\ -2\ +4\ 0)$

(c)

$S_1 \bullet C = [1+1-1+1+1+1-1-1]/8 = 1$
$S_2 \bullet C = [2+0+0+0+2+2+0+2]/8 = 1$
$S_3 \bullet C = [0+0+2+2+0-2+0-2]/8 = 0$
$S_4 \bullet C = [1+1+3+3+1-1+1-1]/8 = 1$
$S_5 \bullet C = [4+0+2+0+2+0-2+2]/8 = 1$
$S_6 \bullet C = [2-2+0-2+0-2-4+0]/8 = -1$

(d)

Figure 2-28. (a) Chip sequences for four stations. (b) Signals the sequences represent (c) Six examples of transmissions. (d) Recovery of station C’s signal.

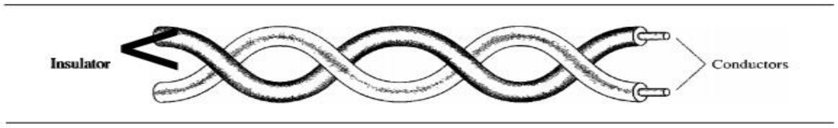
- During each bit time, a station can transmit a 1 (by sending its chip sequence), it can transmit a 0 (by sending the negative of its chip sequence), or it can be silent and transmit nothing.
- We assume for now that all stations are synchronized in time, so all chip sequences begin at the same instant. When two or more stations transmit simultaneously, their bipolar sequences add linearly. For example, if in one chip period three stations output +1 and one station outputs −1, +2 will be received.
- One can think of this as signals that add as voltages superimposed on the channel: three stations output +1 V and one station outputs −1 V, so that 2 V is received. For instance, in Fig. 2-28(c) we see six examples of one or more stations transmitting 1 bit at the same time.
- In the first example, C transmits a 1 bit, so we just get C’s chip sequence. In the second example, both B and C transmit 1 bits, so we get the sum of their bipolar chip sequences, namely: (−1 −1 +1 −1 +1 +1 +1 −1) + (−1 +1 −1 +1 +1 +1 −1 −1) = (−2000 +2 +2 0 −2) To recover the bit stream of an individual station, the receiver must know that station’s chip sequence in advance.
- It does the recovery by computing the normalized inner product of the received chip sequence and the chip sequence of the station whose bit stream it is trying to recover. If the received chip sequence is S and the receiver is trying to listen to a station whose chip sequence is C, it just computes the normalized inner product, S C.

8 **What is Communication Media? Explain Guided Media.** [10] COL2 1

A guided medium can be used to construct a point-to-point link or a shared link with multiple attachments. In the latter case, each attachment introduces some attenuation and distortion on the line, limiting distance and/or data rate. Figure 4.1 depicts the electromagnetic spectrum and indicates the frequencies at which various guided media and unguided transmission techniques operate. In this chapter we examine these guided and unguided alternatives. In all cases, we describe the systems physically, briefly discuss applications, and summarize key transmission characteristics.

1)**GUIDED MEDIA** Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable. A signal traveling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

Twisted-Pair Cable A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together, as shown in Figure 7.3.



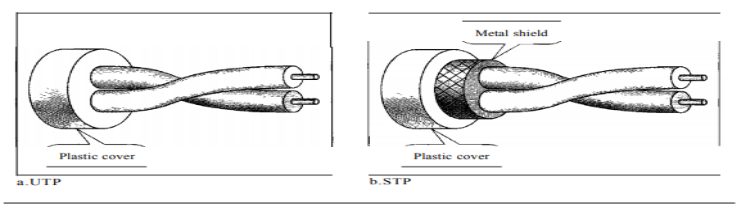
One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.

If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources (e,g., one is closer and the other is farther). This results in a difference at the receiver. By twisting the pairs, a balance is maintained.

For example, suppose in one twist, one wire is closer to the noise source and the other is farther; in the next twist, the reverse is true. Twisting makes it probable that both wires are equally affected by external influences (noise or crosstalk). This means that the receiver, which calculates the difference between the two, receives no unwanted signals. The unwanted signals are mostly canceled out. From the above discussion, it is clear that the number of twists per unit of length (e.g., inch) has some effect on the quality of the cable.

Unshielded Versus Shielded Twisted-Pair Cable

The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP). IBM has also produced a version of twisted-pair cable for its use called shielded twisted-pair (STP). STP cable has a metal foil or braidedmesh covering that encases each pair of insulated conductors. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive. Figure 7.4 shows the difference between UTP and STP. Our discussion focuses primarily on UTP because STP is seldom used outside of IBM.



Categories

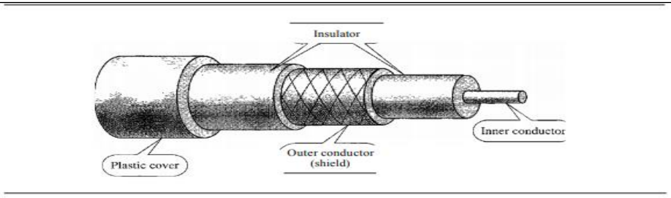
The Electronic Industries Association (EIA) has developed standards to classify unshielded twisted-pair cable into seven categories. Categories are determined by cable quality, with 1 as the lowest and 7 as the highest. Each EIA category is suitable for specific uses. Table 7. I shows these categories.

Applications

Twisted-pair cables are used in telephone lines to provide voice and data channels. The local loop-the line that connects subscribers to the central telephone office commonly consists of unshielded twisted-pair cables. The DSL(Digital Subscriber Line)lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables. Local-area networks, such as lOBase-T and lOOBase-T, also use twisted-pair cables.

Coaxial Cable

Coaxial cable (or coax) carries signals of higher frequency ranges than those in twistedpair cable, in part because the two media are constructed quite differently. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.



Coaxial Cable Standards
Coaxial cables are categorized by their radio government (RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and type of the inner insulator, the construction of the shield, and the size and type of the outer casing. Each cable defined by an RG rating is adapted for a specialized function.

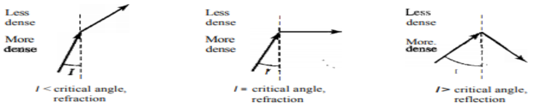
Coaxial Cable Connectors
To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayone-Neill-Concelman (BNC), connector. Figure three popular types of these connectors: the BNC connector, the BNC T connector, and the BNC terminator. The BNC connector is used to connect the end of the cable to a device, such as a TV set. The BNC T connector is used in Ethernet networks to branch out to a connection to a computer or other device. The BNC terminator is used at the end of the cable to prevent the reflection of the signal.

Performance
As we did with twisted-pair cables, we can measure the performance of a coaxial cable. We notice in Figure 7.9 that the attenuation is much higher in coaxial cables than in twisted-pair cable. In other words, although coaxial cable has a much higher bandwidth, the signal weakens rapidly and requires the frequent use of repeaters.

Applications
Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10,000 voice signals. Later it was used in digital telephone networks where a single coaxial cable could carry digital data up to 600 Mbps. However, coaxial cable in telephone networks has largely been replaced today with fiber-optic cable. Cable TV networks also use coaxial cables. In the traditional cable TV network, the entire network used coaxial cable. Later, however, cable TV providers replaced most of the media with fiber-optic cable; hybrid networks use coaxial cable only at the network boundaries, near the consumer premises. Cable TV uses RG-59 coaxial cable.

Another common application of coaxial cable is in traditional Ethernet LANs . Because of its high bandwidth, and consequently high data rate, coaxial cable was chosen for digital transmission in early Ethernet LANs. The 10Base-2, or Thin Ethernet, uses RG-58 coaxial cable with BNE connectors to transmit data at 10 Mbps with a range of 185 m. The lOBase5, or Thick Ethernet, uses RG-11 (thick coaxial cable) to transmit 10 Mbps with a range of 5000 m. Thick Ethernet has specialized connectors.

Fiber-Optic Cable
A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. To understand optical fiber, we first need to explore several aspects of the nature of light. Light travels in a straight line as long as it is moving through a single uniform substance. If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes direction. Figure 7.10 shows how a ray of light changes direction when going from a more dense to a less dense substance.


Less dense
More dense
I
I < critical angle, refraction
Less dense
More dense
I
I = critical angle, refraction
Less dense
More. dense
I
I > critical angle, reflection

As the figure shows, if the angle of **incidence I** (the angle the ray makes with the line perpendicular to the interface between the two substances) is less than the critical angle, the ray refracts and moves closer to the surface.
If the angle of incidence is equal to the critical angle, the light bends along the interface. If the angle is greater than the critical angle, the ray reflects (makes a turn) and travels again in the denser substance.
Note that the critical angle is a property of the substance, and its value differs from one substance to another. Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.

Propagation Modes Current technology supports two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics. Multimode can be implemented in two forms: step-index or graded-index (

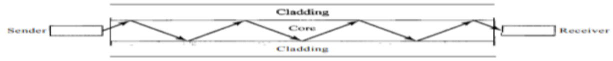
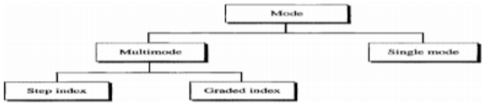


Figure 7.12 *Propagation modes*

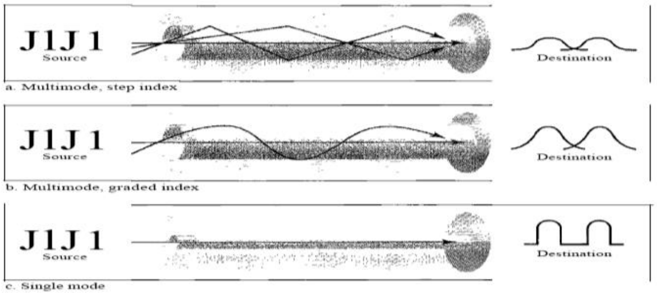


Multimode:-

Multimode is so named because multiple beams from a light source move through the core in different paths. How these beams move within the cable depends on the structure of the core, as shown in Figure 7.13. In multimode step-index fiber, the density of the core remains constant from the center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. At the interface, there is an abrupt change due to a lower density; this alters the angle of the beam's motion. The term step index refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber.

A second type of fiber, called multimode graded-index fiber, decreases this distortion of the signal through the cable. The word index here refers to the index of refraction. As we saw above, the index of refraction is related to density. A graded-index fiber, therefore, is one with varying densities. Density is highest at the center of the core and decreases gradually to its lowest at the edge. Figure shows the impact of this variable density on the propagation of light beams.

Figure 7.13 *Modes*



a. Multimode, step index

b. Multimode, graded index

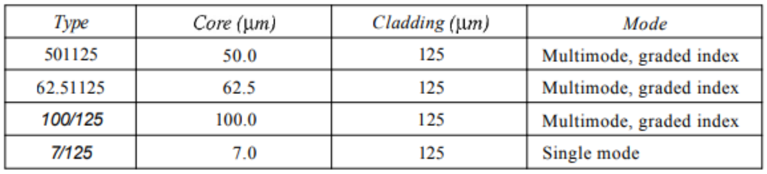
c. Single mode

Single-Mode:-

Single-mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal. The single mode fiber itself is manufactured with a much smaller diameter than that of multimode fiber, and with substantiallY lower density (index of refraction). The decrease in density results in a critical angle that is close enough to 90° to make the propagation of beams almost horizontal. In this case, propagation of different beams is almost identical, and delays are negligible. All the beams arrive at the destination "together" and can be recombined with little distortion to the signal.

Fiber Sizes

Optical fibers are defined by the ratio of the diameter of their core to the diameter of their cladding, both expressed in micrometers. The common sizes are shown in Table Note that the last size listed is for single-mode only.



Type	*Core (μm)*	*Cladding (μm)*	*Mode*
501125	50.0	125	Multimode, graded index
62.51125	62.5	125	Multimode, graded index
100/125	100.0	125	Multimode, graded index
7/125	7.0	125	Single mode

Cable Composition

Figure 7.14 shows the composition of a typical fiber-optic cable. The outer jacket is made of either PVC or Teflon. Inside the jacket are Kevlar strands to strengthen the cable. Kevlar is a strong material used in the fabrication of bulletproof vests. Below the Kevlar is another plastic coating to cushion the fiber. The fiber is at the center of the cable, and it consists of cladding and core.

Fiber-Optic Cable Connectors

The subscriber channel (SC) connector is used for cable TV. It uses a push/pull locking system. The straight-tip (ST) connector is used for connecting cable to networking devices. It uses a bayonet locking system and is more reliable than SC. MT-RJ is a connector that is the same size as RJ45.

Performance

The plot of attenuation versus wavelength in Figure 7.16 shows a very interesting phenomenon in fiber-optic cable.

Attenuation is flatter than in the case of twisted-pair cable and coaxial cable. The performance is such that we need fewer (actually 10 times less) repeaters when we use fiber-optic cable.

Applications
Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective. Today, with wavelength-division multiplexing (WDM), we can transfer data at a rate of 1600 Gbps. The SONET network that we discuss in Chapter 17 provides such a backbone. Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network. Optical fiber provides the backbone structure while coaxial cable provides the connection to the user premises. This is a cost-effective configuration since the narrow bandwidth requirement at the user end does not justify the use of optical fiber. Local-area networks such as 100Base-FX network (Fast Ethernet) and 1000Base-X also use fiber-optic cable

Advantages and Disadvantages of Optical Fiber:-
Advantages Fiber-optic cable has several advantages over metallic cable (twistedpair or coaxial).

Higher bandwidth. Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable. Currently, data rates and bandwidth utilization over fiber-optic cable are limited not by the medium but by the signal generation and reception technology available.

Less signal attenuation. Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.

Immunity to electromagnetic interference. Electromagnetic noise cannot affect fiber-optic cables.

Resistance to corrosive materials. Glass is more resistant to corrosive materials than copper.

Light weight. Fiber-optic cables are much lighter than copper cables.

Greater immunity to tapping. Fiber-optic cables are more immune to tapping than copper cables. Copper cables create antenna effects that can easily be tapped.

Disadvantages There are some disadvantages in the use of optical fiber:-
Installation and maintenance. Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.

Unidirectional light propagation. Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.

Cost. The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.

9 **Explain Hamming code for Error detection and Error Correction.** [10] CO2 L2

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.

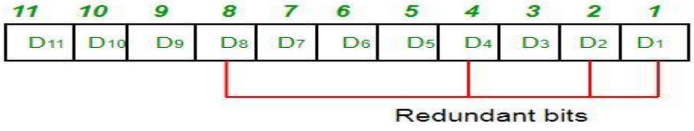
1. Write the bit positions starting from 1 in binary form (1, 10, 11, 100, etc).
2. All the bit positions that are a power of 2 are marked as parity bits (1, 2, 4, 8, etc).
3. All the other bit positions are marked as data bits.
4. Each data bit is included in a unique set of parity bits, as determined 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.

Determining the position of redundant bits –

These redundancy bits are placed at the positions which correspond to the power of 2.

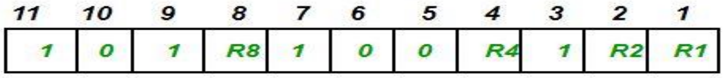
As in the above example:

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



11	10	9	8	7	6	5	4	3	2	1
D11	D10	D9	D8	D7	D6	D5	D4	D3	D2	D1

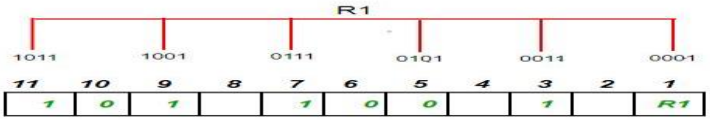
Suppose the data to be transmitted is 1011001, the bits will be placed as follows:



11	10	9	8	7	6	5	4	3	2	1
1	0	1	R8	1	0	0	R4	1	R2	R1

Determining the Parity bits –

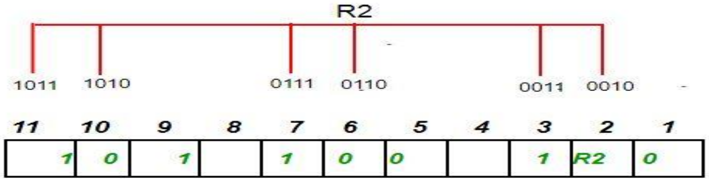
1. R1 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the least significant position.
   R1: bits 1, 3, 5, 7, 9, 11



11	10	9	8	7	6	5	4	3	2	1
1	0	1		1	0	0		1		R1

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

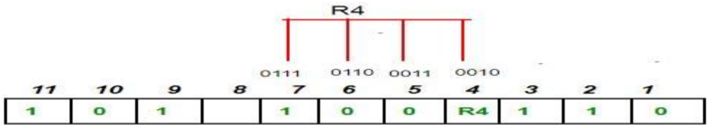


11	10	9	8	7	6	5	4	3	2	1
1	0	1		1	0	0		1	R2	0

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

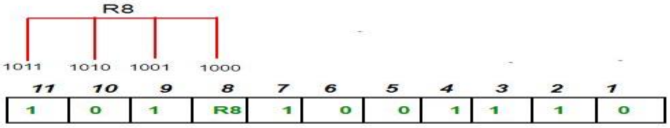
R2 is an odd number the value of R2(parity bit’s value)=1

3. 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



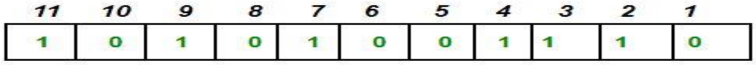
To find the redundant bit R4, we check for even parity. Since the total number of 1’s in all the bit positions corresponding to R4 is an odd number the value of R4(parity bit’s value) = 1

4. 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



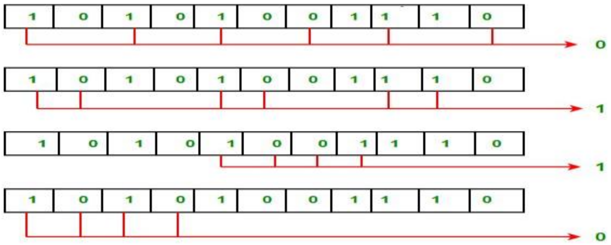
To find the redundant bit R8, we check for even parity. Since the total number of 1’s in all the bit positions corresponding to R8 is an even number the value of R8(parity bit’s value)=0.

Thus, the data transferred is:



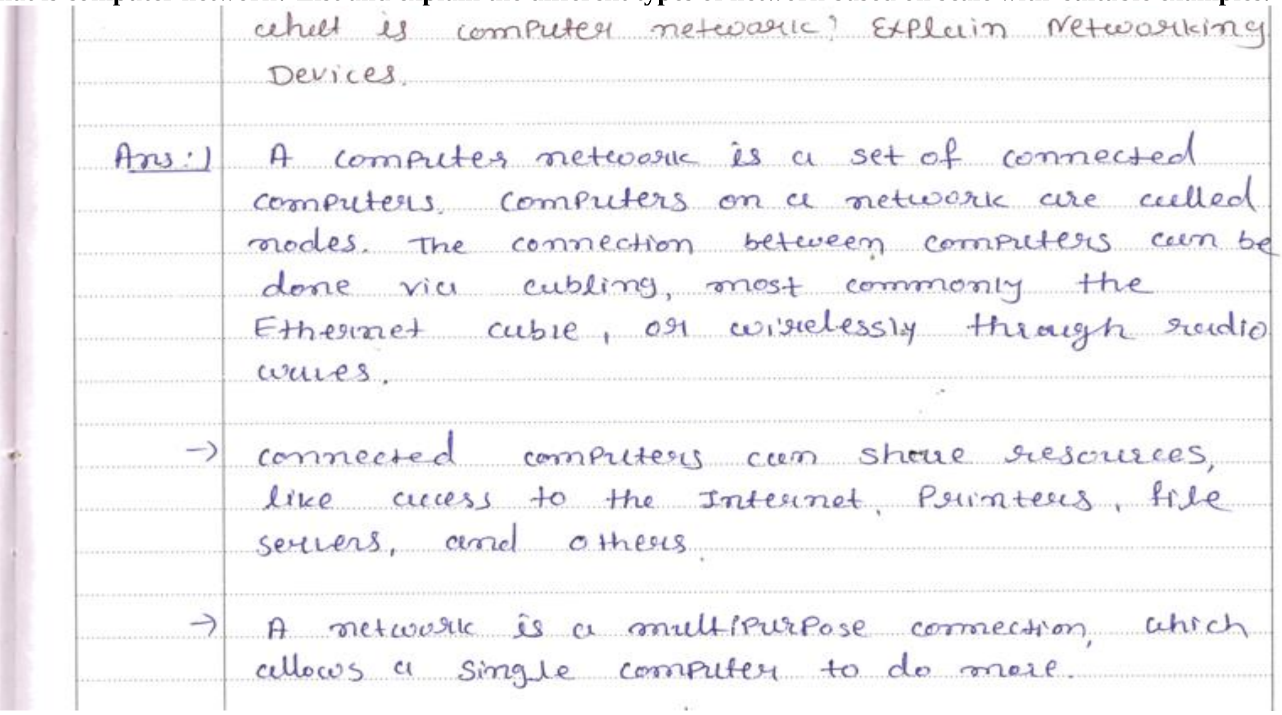
11	10	9	8	7	6	5	4	3	2	1
1	0	1	0	1	0	0	1	1	1	0

Error detection and correction –
Suppose in the above example the 6th bit is changed from 0 to 1 during data transmission, then it gives new parity values in the binary number:



The bits give the binary number as 0110 whose decimal representation is 6. Thus, the bit 6 contains an error. To correct the error the 6th bit is changed from 1 to 0.

10	**What is computer network? List and explain the different types of network based on scale with suitable examples.**	[10]	CO2	L1

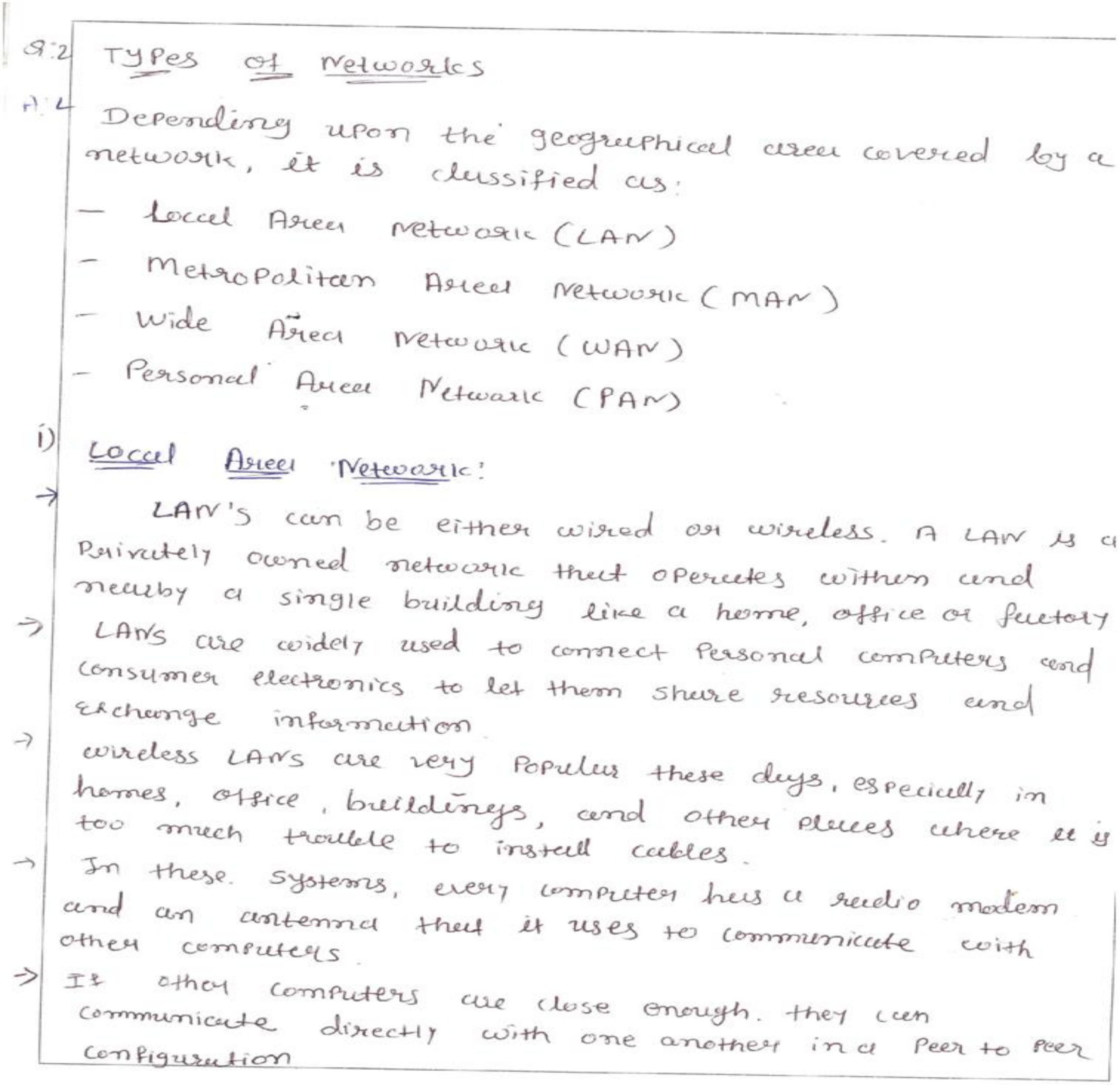


what is computer network? Explain Networking Devices.

Ans:) A computer network is a set of connected computers. computers on a network are called nodes. The connection between computers can be done via cabling, most commonly the Ethernet cable, or wirelessly through radio waves.

→ connected computers can share resources, like access to the Internet, Printers, file servers, and others.

→ A network is a multiPurPose connection, which allows a single computer to do more.



Q:2 Types of Networks

A: 4 Depending upon the geographical area covered by a network, it is classified as:

- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)
- Personal Area Network (PAN)

i) Local Area Network:

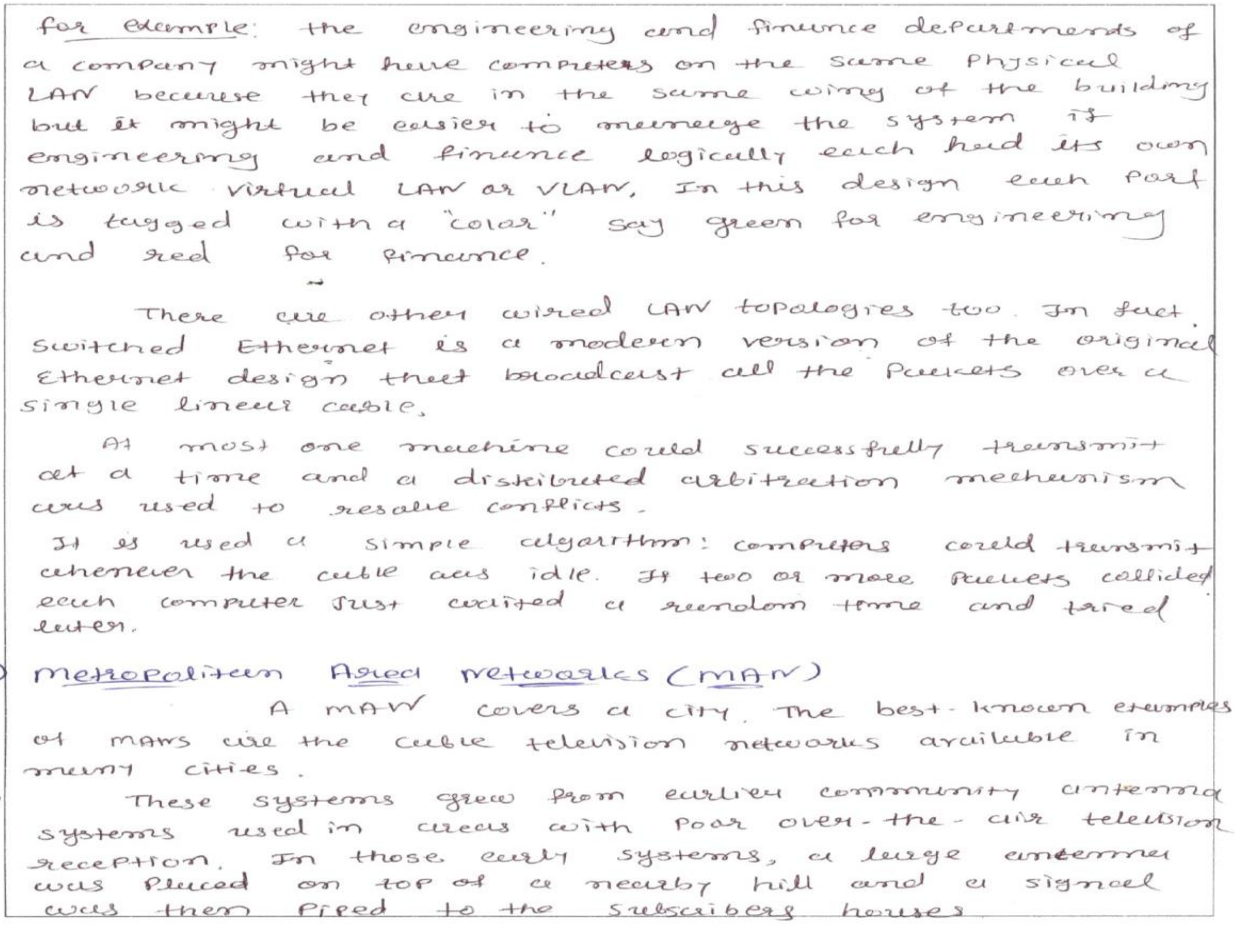
→ LAN's can be either wired or wireless. A LAN is a Privately owned network that operates within and nearby a single building like a home, office or factory

→ LANs are widely used to connect Personal computers and consumer electronics to let them share resources and Exchange information

→ wireless LANs are very Popular these days, especially in homes, office, buildings, and other places where it is too much trouble to install cables.

→ In these systems, every computer has a radio modem and an antenna that it uses to communicate with other computers.

→ If other computers are close enough. they can communicate directly with one another in a Peer to Peer configuration



-> for example: the engineering and finance departments of a company might have computers on the same Physical LAN because they are in the same wing of the building but it might be easier to manage the system if engineering and finance logically each had its own network virtual LAN or VLAN, In this design each Port is tagged with a "color" say green for engineering and red for finance.

-> There are other wired LAN topologies too. In fact, switched Ethernet is a modern version of the original Ethernet design that broadcast all the packets over a single linear cable,

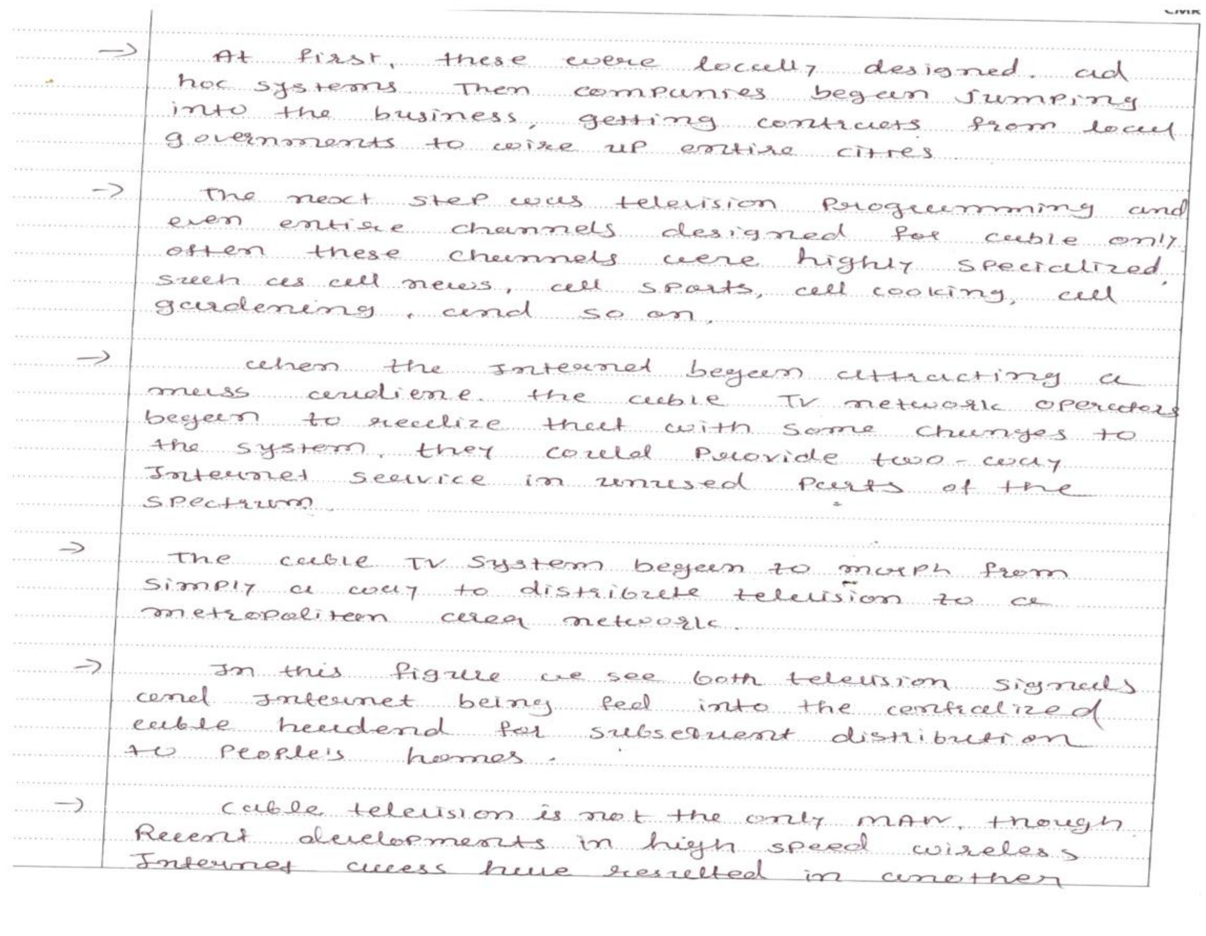
-> At most one machine could successfully transmit at a time and a distributed arbitration mechanism was used to resolve conflicts.

-> It is used a simple algorithm: computers could transmit whenever the cable was idle. If two or more packets collided each computer just waited a random time and tried later.

2) Metropolitan Ared networks (MAN)

-> A MAN covers a city. The best-known examples of MANs are the cable television networks available in many cities.

-> These systems grew from earlier community antenna systems used in areas with poor over-the-air television reception. In those early systems, a large antenna was placed on top of a nearby hill and a signal was then piped to the subscribers houses



-> At first, these were locally designed. ad hoc systems Then companies began jumping into the business, getting contracts from local governments to wire up entire cities.

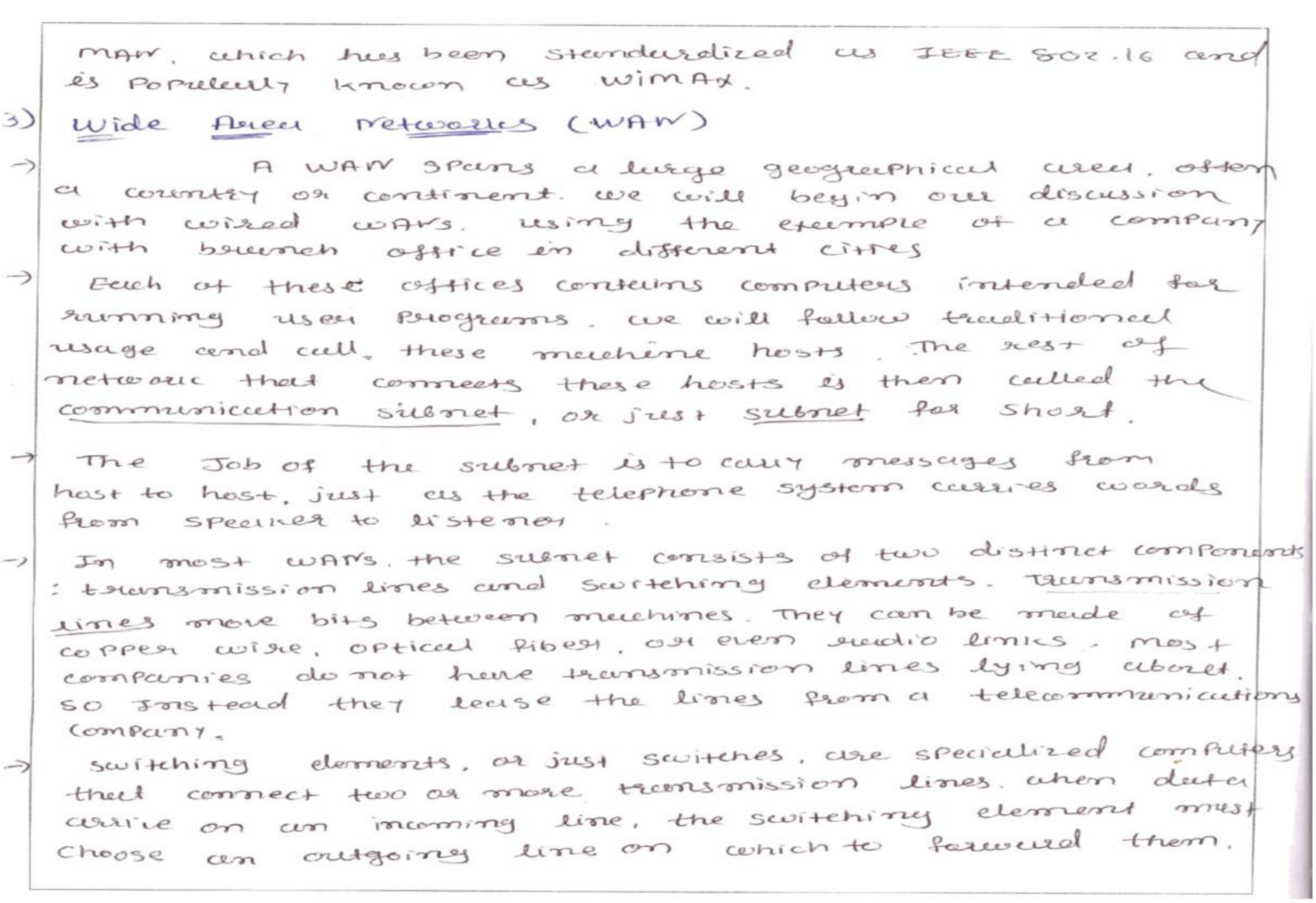
-> The next step was television programming and even entire channels designed for cable only. often these channels were highly specialized, such as all news, all sports, all cooking, all gardening, and so on.

-> when the Internet began attracting a mass audience. the cable TV network operators began to realize that with some changes to the system, they could provide two-way Internet service in unused parts of the spectrum.

-> The cable TV system began to morph from simply a way to distribute television to a metropolitan area network.

-> In this figure we see both television signals and Internet being feed into the centralized cable headend for subsequent distribution to people's homes.

-> Cable television is not the only MAN, though. Recent developments in high speed wireless Internet access have resulted in another



MAN, which has been standardized as IEEE 802.16 and is popularly known as WiMAX.

3) Wide Area Networks (WAN)

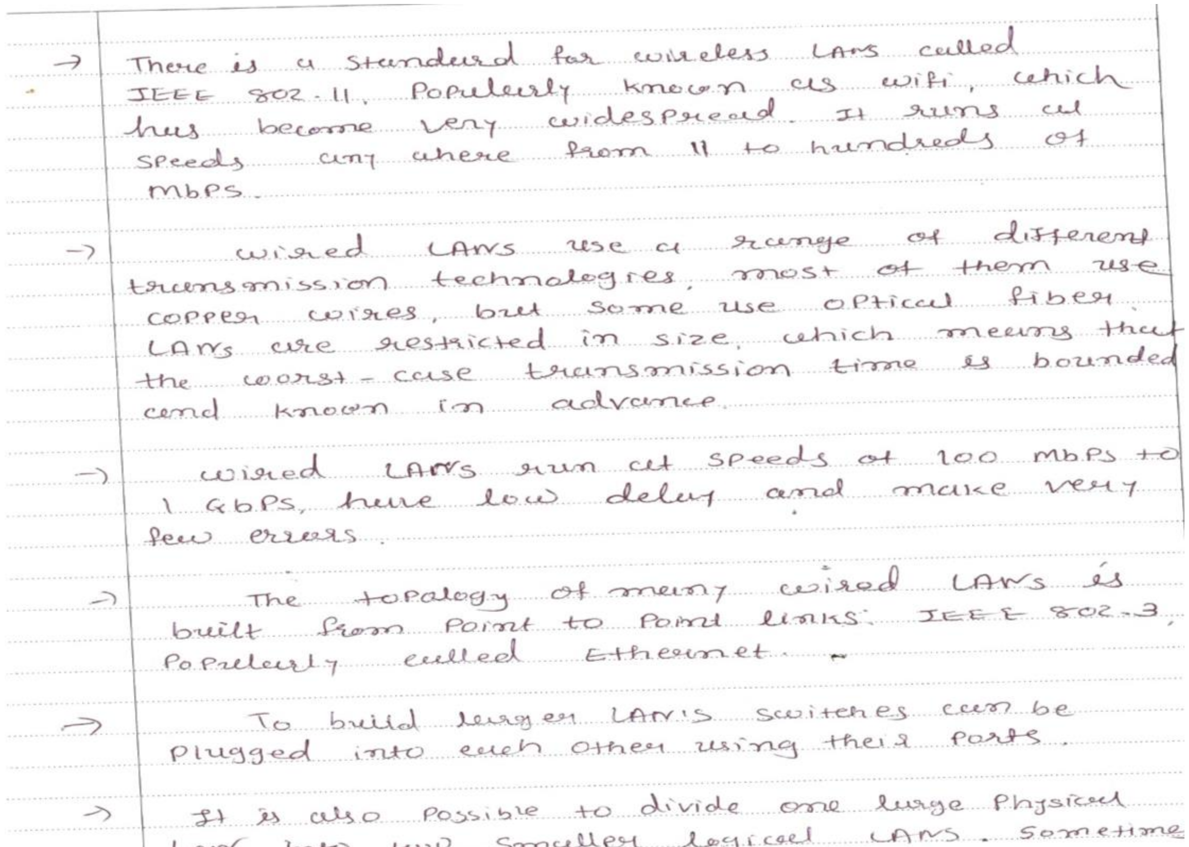
→ A WAN spans a large geographical area, often a country or continent. We will begin our discussion with wired WANs, using the example of a company with branch office in different cities

→ Each of these offices contains computers intended for running user programs. We will follow traditional usage and call these machine hosts. The rest of network that connects these hosts is then called the communication subnet, or just subnet for short.

→ The Job of the subnet is to carry messages from host to host, just as the telephone system carries words from speaker to listener.

→ In most WANs, the subnet consists of two distinct components: transmission lines and switching elements. Transmission lines move bits between machines. They can be made of copper wire, optical fiber, or even radio links. Most companies do not have transmission lines lying about. So instead they lease the lines from a telecommunications company.

→ Switching elements, or just switches, are specialized computers that connect two or more transmission lines. When data arrive on an incoming line, the switching element must choose an outgoing line on which to forward them.



→ There is a standard for wireless LANs called IEEE 802.11, popularly known as WiFi, which has become very widespread. It runs at speeds anywhere from 11 to hundreds of Mbps.

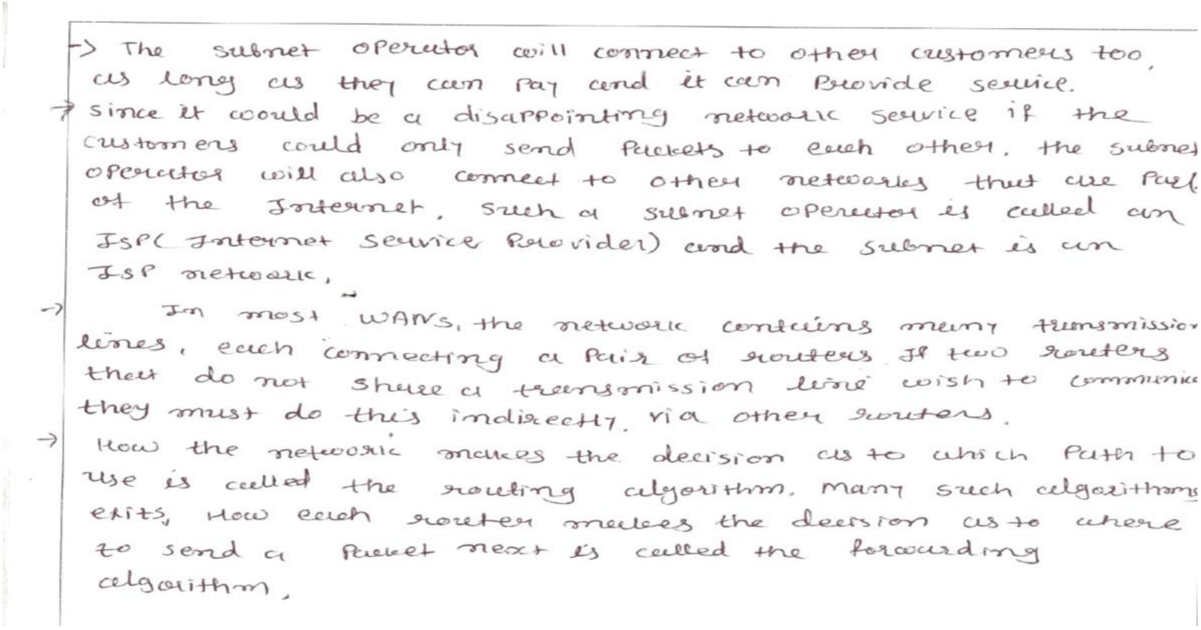
→ Wired LANs use a range of different transmission technologies, most of them use copper wires, but some use optical fiber. LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance.

→ Wired LANs run at speeds of 100 Mbps to 1 Gbps, have low delay and make very few errors.

→ The topology of many wired LANs is built from point to point links. IEEE 802.3, popularly called Ethernet.

→ To build larger LAN'S switches can be plugged into each other using their ports.

→ It is also possible to divide one large physical LAN into two smaller logical LANs. Sometime the layout of the network equipment does no match the organization's structure.



→ The subnet operator will connect to other customers too, as long as they can pay and it can Provide service.

→ since it would be a disappointing network service if the customers could only send Packets to each other, the subnet operator will also connect to other networks that are Part of the Internet, such a subnet operator is called an ISP(Internet service Provider) and the subnet is an ISP network,

→ In most WANs, the network contains many transmission lines, each connecting a Pair of routers. If two routers that do not share a transmission line wish to communica they must do this indirectly, via other routers.

→ How the network makes the decision as to which Path to use is called the routing algorithm. Many such algorithms exits, How each router makes the decision as to where to send a Packet next is called the forwarding algorithm,