Textbook

1. Computer Network by Tannenbaum Pearson, India, 6th edition.

2. Java Network-Programming by Harord O'Reilly (Shroff Publishers)

What is Network?

It is a set of device connected by communication link.

What is Computer Network?

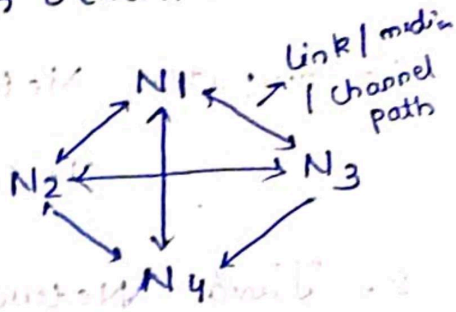
It means an interconnected collections of autonomous computer.

Communication

1. Sender
2. Receiver
3. Information
4. Medium
5. Protocol

Interconnected means if they are able to exchange information

Autonomous - means two computers which are interconnected are independent of each other.



Topology - Arrangement of networks

Types - ① Bus
② Ring
③ Star
④ Mess

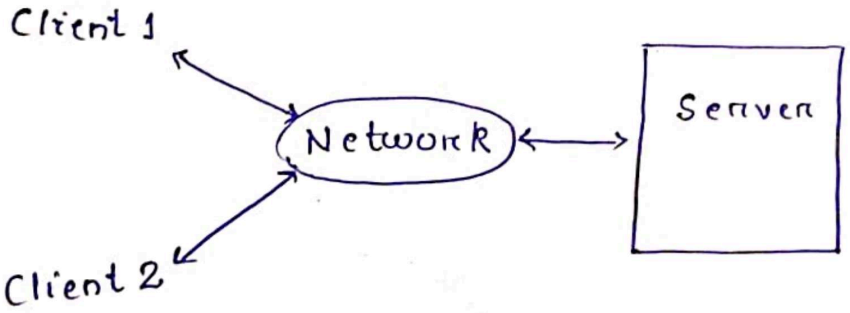
Uses of Computer Network

(Sharing of information)
↓
fruitful info

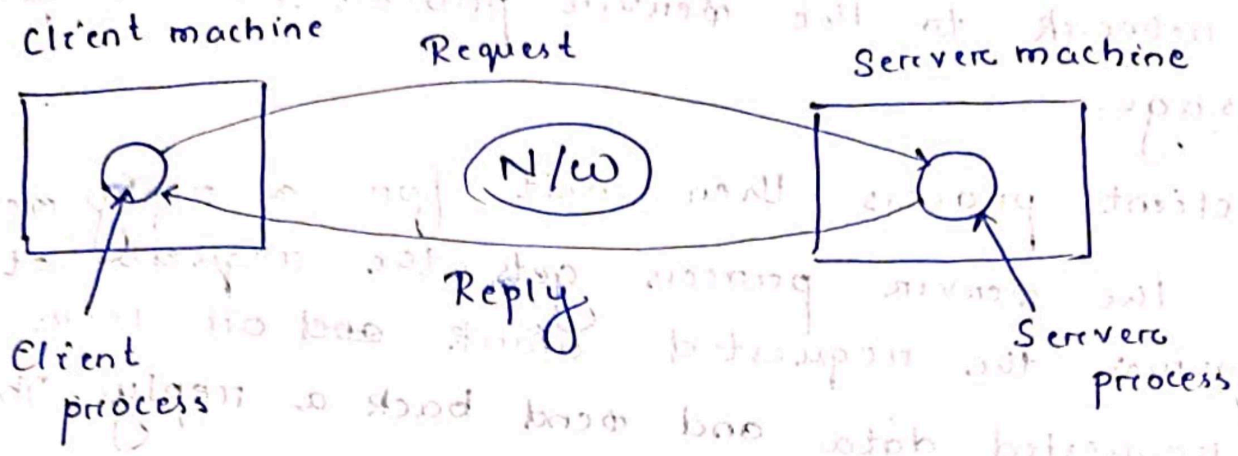
1. Access to information

Two basic model →

① Client - Server model

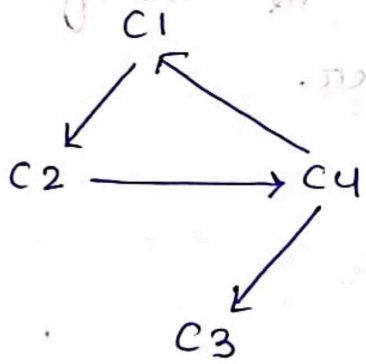


(Rough model)



(Client-server diagram)

② <u>Peer-to-peer system.</u>



* Every client behave like a server and transfers infos.

→ The <u>Client-Server Model</u> forms the basis of much network users.

→ The most popular realization is <u>web application</u> where a server generate web pages based on its data base in response to client request that may update the data base.

→ Communication between client and server takes place when the client process send a message over the network to the server process i.e request message.

→ The client process then wait for a reply message.

→ when the server process gets the request it performs the requested work ~~and~~ or looks up the requested data and send back a reply. This is called as client-server model.

Another model for Accessing information is peer to peer communication. Here, individuals who forms a loose group can communicate with others in the group i.e, there is no fixed division between client and server.

2. Person to Person Communication

e.g. Instagram, Facebook, etc.

Many internet users now rely on some form of instant messaging to communicate with other people on the Internet.

3. Electronic Commerce

e.g Flipkart, Amazon, Ordering books only, Government distributing tax online, Selling 2nd hand product online.

4. Entertainment

e.g Netflix, Amazon Prime, etc.
This has made huge strides in the home in recent years, with the distribution of music, radio and television programs, and movies over the Internet beginning to rival that of traditional mechanisms.

5. The Internet of Things

As the cost of sensing and communication drops, more and more measurement and reporting will be done with networks. This ongoing revolution, often referred to as the IoT.

Types of Computer Network

① Broadband Access Network - ~~Broa~~ ~~It is det~~
Broadband Access type of Network is delivered to home through copper wire, coaxle cable, optical fibre. The speed of broadband internet access increases i.e delivered on gigabits per second to individual home.

② Mobile and wireless access Network

e.g Hotspot, Bluetooth etc.

③ Content provider Network

e.g Cloud computing

Data center network serves the increasing growing demand of cloud computing and a design to move large amount of data between server in the data center and data center and also between the data center and rest of the internet.

④ Transit Network

→ When the content provider and your ISP (Internet Service Provider) are not directly connected they often rely on a transit network to carry the traffic between them.

→ Transit network charge both the ISP and the content provider for carrying traffic from end-to-end.

→ Transit Network are called as backbone networks because they have the role of carrying traffic between two end point.

⑤ Enterprise Network

→ In an organisation resource sharing as well as information sharing takes place with the help of this network.

→ Network called VPN connects the individual network at different sight into a logical network.
(VPN → Virtual Private Network)

→ The second goal of this type of network is to provide powerful communication medium among employees. Telephone calls between employees may be carried by the computer network instead of by the phone company. This technology is called as VOIP / IP telephony.
(VOIP → Voice Over Internet Protocol)

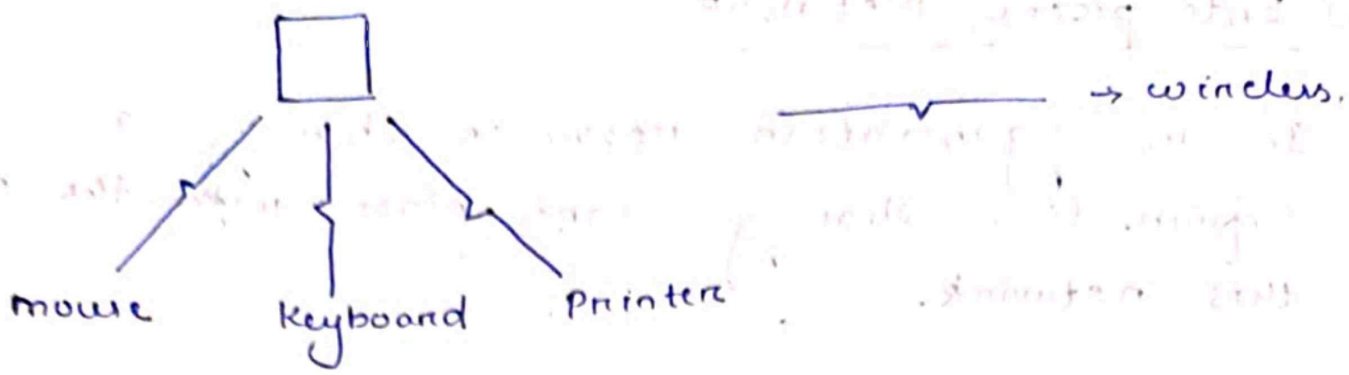
→ The third goal is doing business with customer and supplier.

Type of Network based on geographical coverage area

Network Technology from Local to Global

① PAN →(Personal Area Network)

→ PAN network make the device communicate over the range of the person.
e.g. Bluetooth.

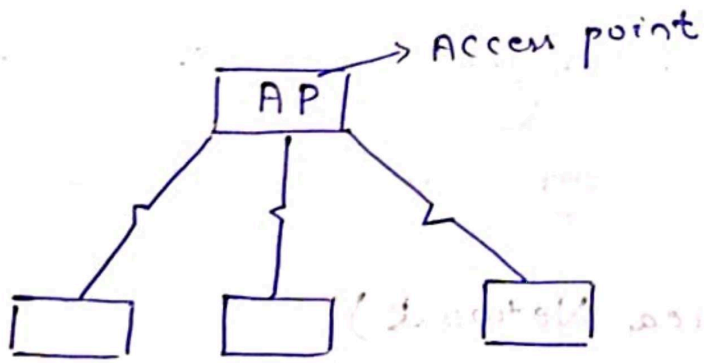


② <u>LAN</u> → (Local Area Network)

→ LAN is a private network that operates within and nearby a single building like home, office or factory.

→ LAN can be wireless or wired. In case of <u>wireless LAN</u> each computer talk to a device which is called as access point or router or base station.

→ This wireless LAN follows a standard i.e. IEEE 802.11 and ~~comonly~~ commonly called as wi-fi. It runs at a speed from 11 Mbps - 7 Gbps.

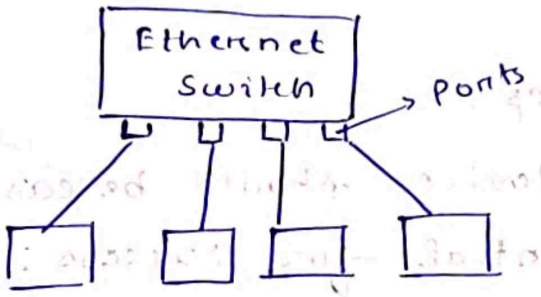


IEEE 802.11
wifi

→ Wired LAN uses copper or coaxle cable or optical fibre as transmission medium.

→ Wired LAN runs at a speed of 100 Mbps - 40 Gbps

→ Wired LAN have low latency, low packet loss and higher throughput than wireless LAN. The wired LAN follows a standard IEEE 802.3 commonly called as Ethernet.



IEEE 802.3

Ethernet

→ In case of wired LAN, each computer speaks the ethernet protocol and connects to the device called as switch.

→ A switch as multiple ports each of which connect to one other devices.

→ Both wireless and wired LAN can allocate resources statically or dynamically.

In case of static allocation the entire time is divided into discrete interval and use a Round Robin algorithm, allowing each machine to broadcast only when it's time slots comes up.

→ In case of dynamic allocation, the sharing is done either centralized or de-centralized.

→ In case of centralized there is a single entity like base station who determines who goes next.

→ In case of de-centralized there is no central entity, each machine decides for itself whether to transmit or not.

③ <u>Home Network</u>

It has some properties

1. The network and devices should be easily installed.
2. Low price is essential for success.
3. It needs sufficient capacity.
4. It should be secured and reliable in nature.

④ <u>MAN</u> → (Metropolitan ~~Access~~ Area Network)

e.g. Cable TV

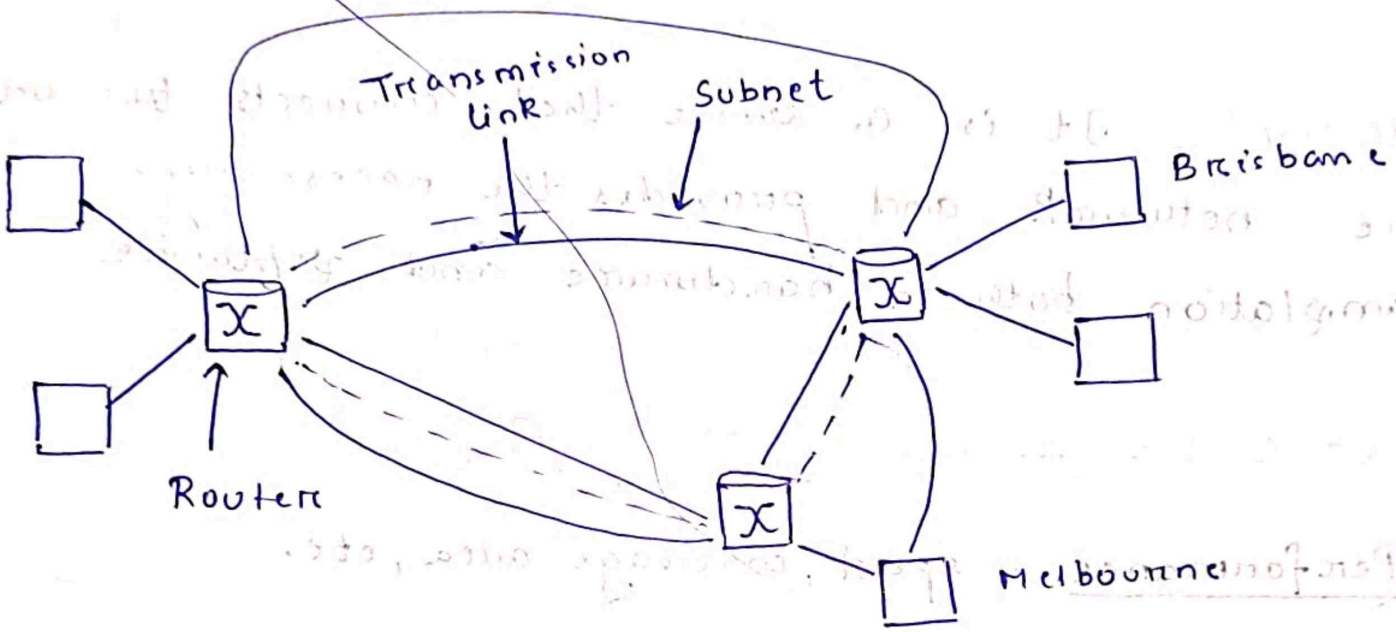
It covers a city.

⑤ <u>WAN</u> → (Wide Area Network)

It covers a continent or country.

It consists of two things → ① Host
② Communication subnet.

Host is owned by the customer and Communication subnet is owned by Network Service Provider (NSP).



WAN

Two types of Communication subnet →

① Transmission line - It is used to move packets between two machine and is made up of optical fibre or copper wires.

② Switching elements - e.g. Router, which are used to connect two or more transmission line.

⑥ Internetwork

Gateway - It is a device that connects two or more network and provides the necessary translation both in hardware and software.

What is the criteria of Network ?

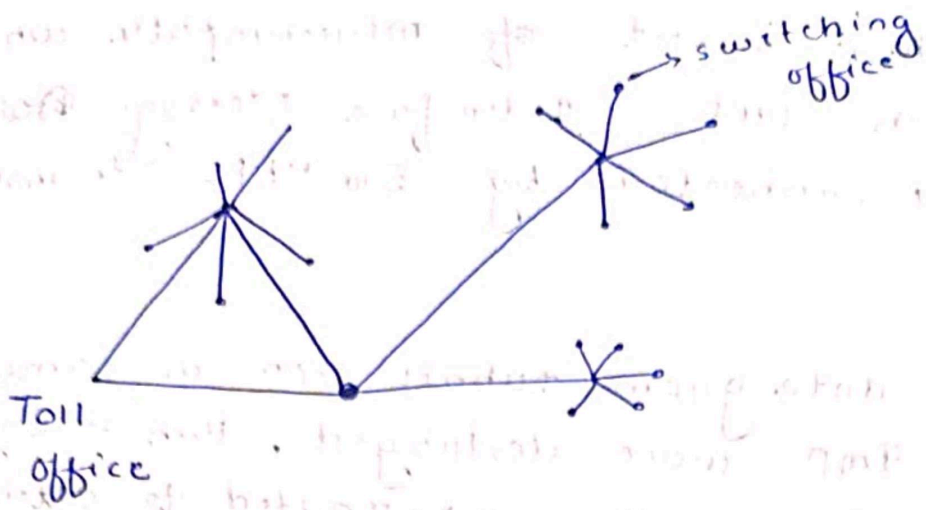
① **Performance** - speed, coverage area, etc.

② **Reliability**
It is measured by the frequency of failure, the time it takes a link to recover from a failure.

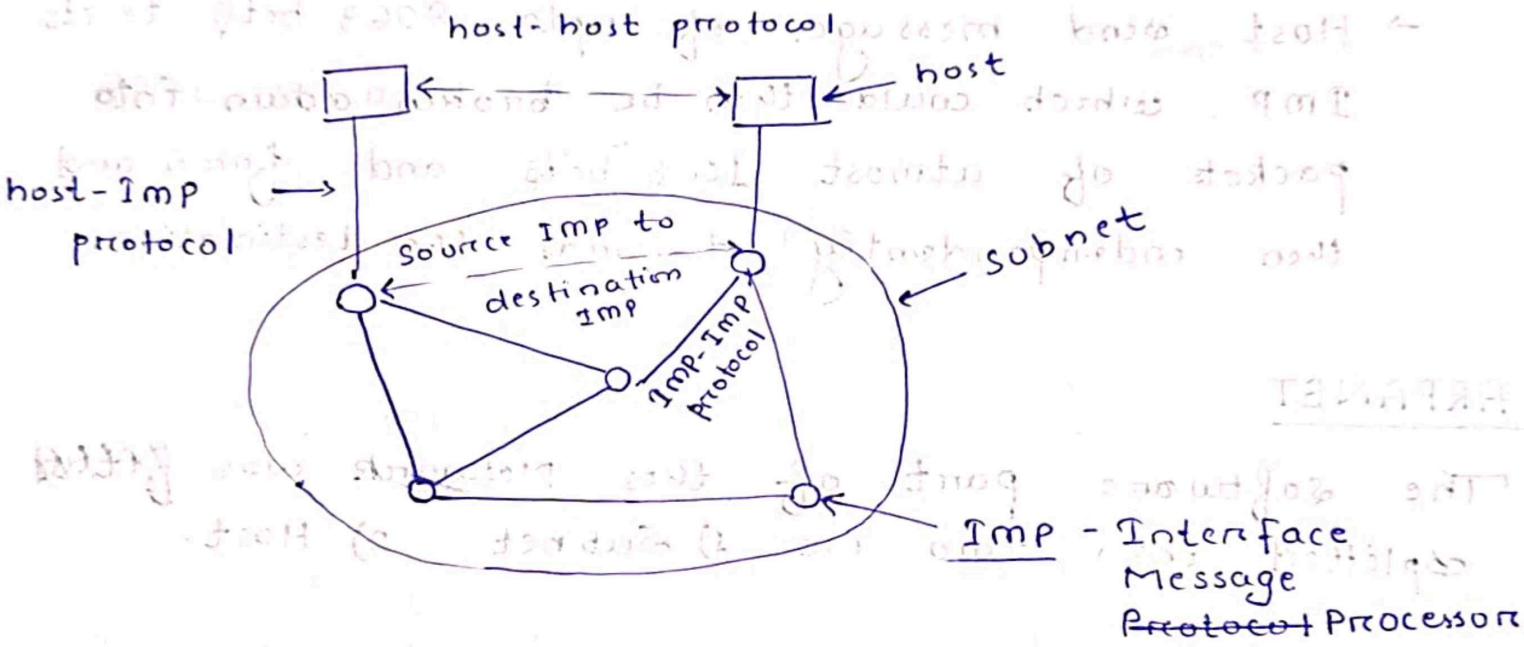
③ **Security** - Protecting data from unauthorized user.

Internet

① **The ARPANET**



Structure of telephone system



ARPANET DESIGN

→ The organization i.e ARPA stands for Advanced Research Project Agency. ~~Find~~

→ Find a solution to design a command and control network.

→ They started building a packet switched subnet where each host is having its own router.

→ The subnet consists of minicomputer which is called as IMP (Interface Message ~~Proto~~ Processor), connected by 56 KbPS transmission line.

→ It is a datagram subnet. So in some lines and IMP were destroyed, then message could be automatically re-routed to alternative path.

→ Host send messages of upto 8063 bits to its IMP which could then be broken down into packets of atmost 1008 bits and forward then independently towards the destination.

ARPANET

The software part of this Network was ~~fitted~~ splitted into two i.e 1) Subnet 2) Host.

Subnet - It consists of IMP-IMP Protocol then Source IMP - Destination IMP Protocol.

Outside subnet it consists of Host-Host Protocol then Host-IMP Protocol.

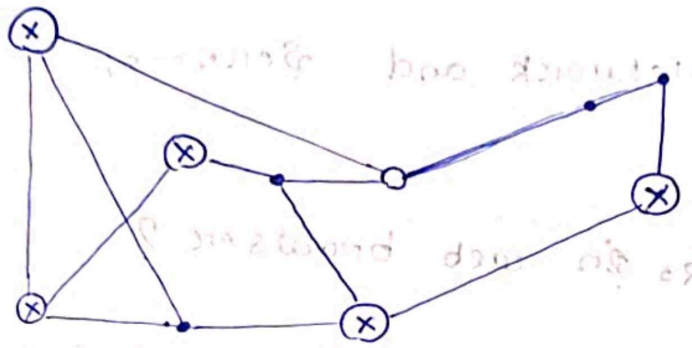
NSFNET

NSF → National Science Foundation

○ NSF Supercomputer Center

⊗ NSF Mid level N/w

• both



→ NSF built a backbone network to connect its 6 super computer center where each super computer was attached with a microcomputer called as fuzzball.

→ This fuzzball was connected with 56 Kbps leased lines and formed the subnet.

→ NSF also funded around 20 regional networks that connected to the backbone to allow users at thousands of university, lab and libraries to access any of the super computers and to communicate with each other.

→ It is also connected to the ARPANET through a link between IMP and fuzzball.

→ Later, NSF used fibre optics channel which increased the backbone capacity to 448 Kbps.

→ Further again, the backbone was upgraded to 1.5 Mbps. Later NSF signed a contract to diff. N/W operator to establish a NAP (Network Access Point) in order to enhance the communication of every regional N/W with every other.

ANS → Advanced Network and Services

How Internet works in web browser ?

→ User entered the Url on the web browser.

→ web browser take the Url and transfer it to the DNS system.

→ DNS will extract the IP address and send it back to the browser.

→ web browser will form a http request using a url IP address and client data.

→ web browser send that http request to the server IP address which is fetched by DNS.

ANSNET

Ethernet

ALOHANET

- Prior to Ethernet the concept of interconnecting the computer was taking place through short range radio devices, such type of network was called as Alohanet.

→ Here, a number of user terminals were connected to a central computer.

→ The communication between the each user terminal and central computer was taking place in two frequency.

① Upstream ↓ (User to CPC)

② Downstream ↓ (CC to User)

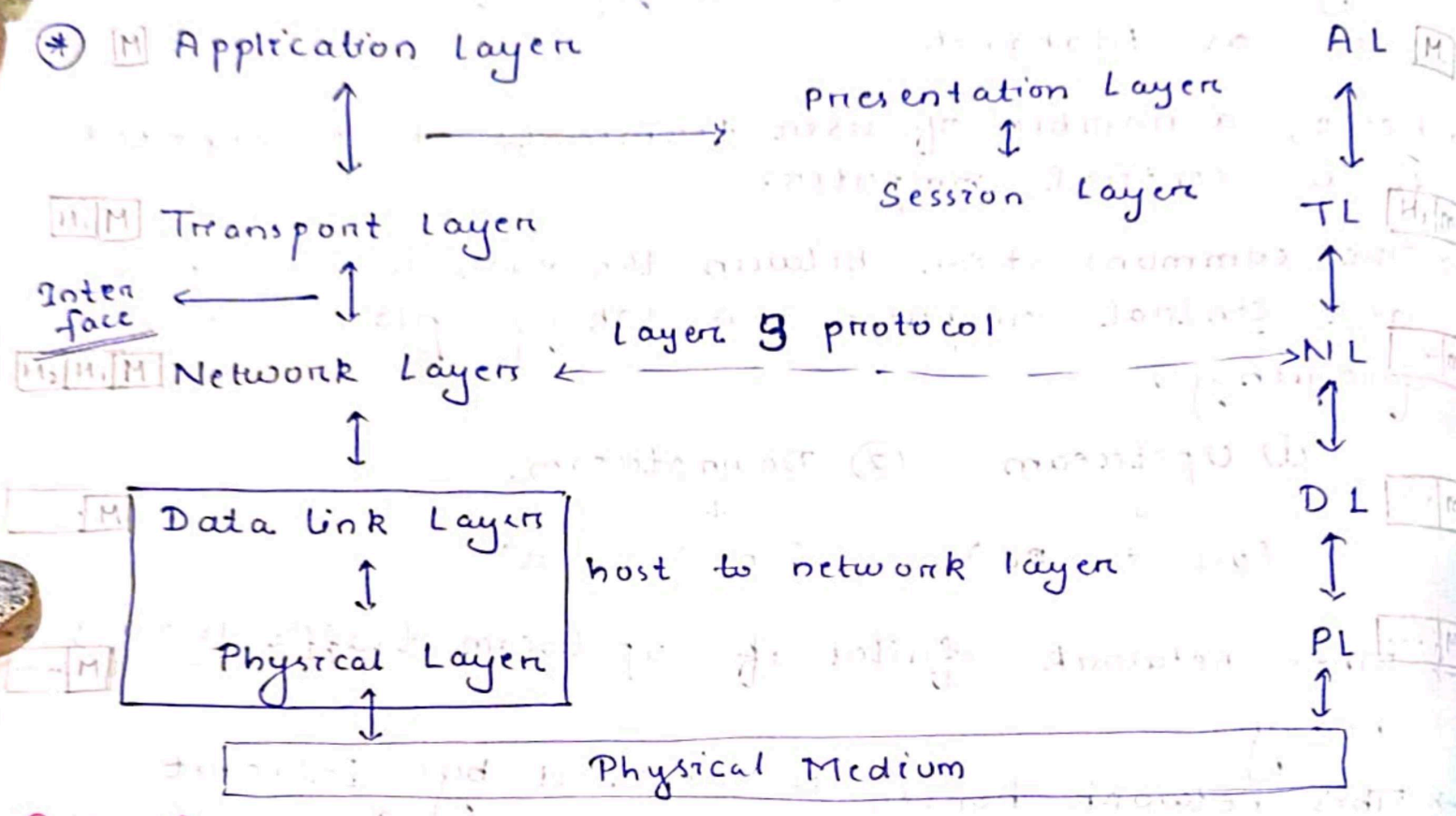
→ This network failed if upstream traffic is very heavy.

→ This network hence, is replaced by Ethernet where the transmission medium (Co-axial cable)

Improvement of Ethernet over Alohanet

1) Before transmitting a computer first listen to the cable to see if someone else is using or not. If so the computer held back until the current transmission is finished. Doing so, avoid interfering with existing transmission giving a much higher efficiency.

11) ALOHA didn't work like this because it was impossible for a terminal on one end to sense the transmission on a terminal on the other hand.



Interface

It defines which primitive operations and services the lower layer makes available to the upper ones.

Types of Services

There are 2 types of services -

1) Connection Oriented type of Service

→ This is the model after the telephone system.

→ Here, connection is established first then transfer of information takes place by using this connection and finally release the connection.

→ This type of connection is divided into 2 parts.

a) Reliable Connection Oriented

b) Unreliable Connection Oriented.

a) Reliable Connection Oriented

e.g. File Transfer.

The owner of the file wants to be sure that all the bits arrive correctly and in the same order they were sent.

This type of service has 2 variants -

i) Message Sequence

ii) Byte Stream

i) Message Sequence

→ Here message boundaries are preserved.

→ When 2 1024 bytes message are sent, they arrive as a 2 distinct 1024 byte message.

ii) Byte Stream

Here there is no message boundary that is when 2048 bytes of message arrives at the receiver it is difficult to say that whether 2 1024 bytes are received or 1 2048 bytes are received or 2048 1 byte is received.

b) Unreliable Connection Oriented

e.g Digital voice Transmission.

In this type of service bit of noise on the transmission line is heard from time to time.

2) Connectionless Oriented type of Service

→ This is a model after the postal system. Each message/letter carries the full destination address and each one is routed through the system independent of all others.

This type of service is divided into 3 parts-

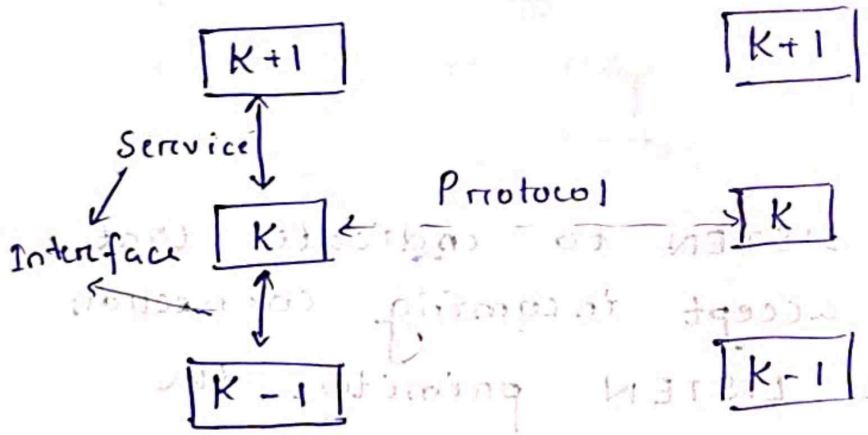
i) Unreliable Connectionless type of Service

e.g. Junk mail.

ii) Acknowledge connectionless service

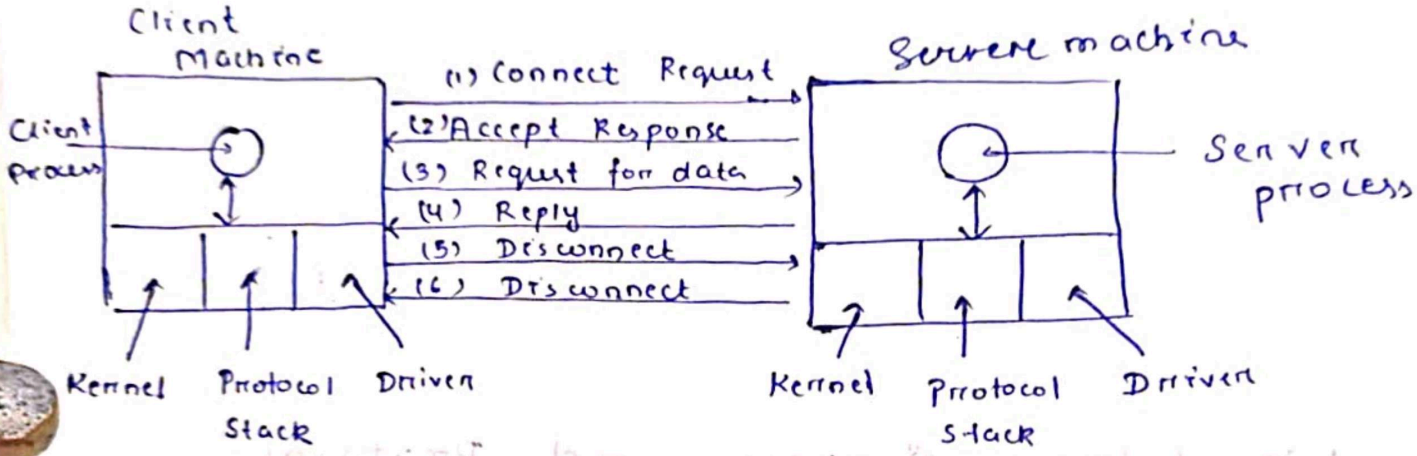
iii) Request - Reply connectionless type of service

Relationship between service and Protocol



Services Primitives

LISTEN
CONNECT
ACCEPT
RECEIVE
SEND
DISCONNECT



~~LISTen Primitive~~

1) LISTEN Primitive

The server execute LISTEN to indicate that it is prepared to accept incoming connection after executing the LISTEN primitive the server process is blocked until a request for connect appears.

CONNECT Primitive

→ Now, the client process execute CONNECT to establish a connection with the server.

Now the client process is suspended until there is a response. (ACCEPT)

→ When the connect packet arrives at the server it is been processed by the Operating System. When the system find that the packet is requesting a connection it sends an acknowledgement (ACCEPT Primitive).

→ The arrival of acknowledgement releases the client.

→ At this point the client and server are both running and they have a connection established between them.

→ Then the client execute SEND primitive to transmit its request followed by the execution of receive to get the reply.

→ The arrival of the request packet at the server machine unblock the server process so it can process the request.

→ If the transfer of information is done anyone can use DISCONNECT primitive to terminate the call.

Chapter-2

Physical Layer

→ Physical layer defines the mechanical, electrical and timing interface to the network.

Guided Transmission medium

The transmission medium that rely on physical cable or wire is called as guided transmission medium.

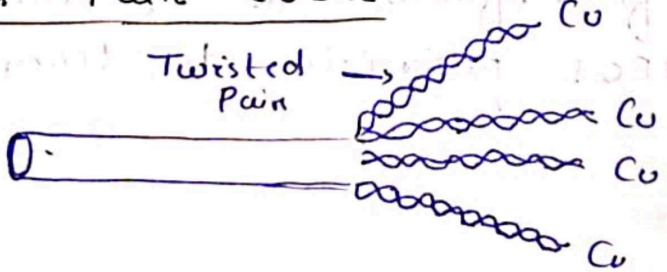
① Persistant Storage

→ Data is transported from one computer to another ~~with~~ by writing onto the magnetic tape or removable media, physically transporting the tape or disk to the destination machine and read them back.

→ It is cost effective for application where high bandwidth is the key factor.

→ Although the bandwidth is excellent but delay is very poor.

② Twisted Pair Cable



Cu → Copper wire

3UTP 5UTP 6UTP 7UTP

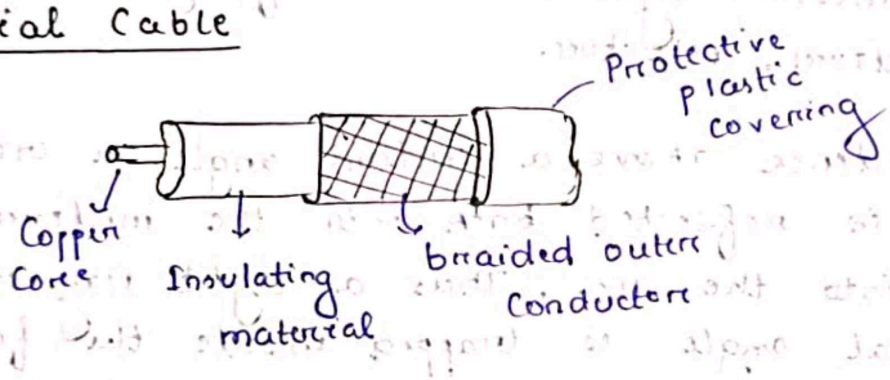
→ Twisted pair consists of two insulated wire made up of copper with 1mm thickness.

→ The wires are twisted together just like DNA molecule.

→ Twisting is done because two parallel wires constitute a fine 'antina'. When the wires are twisted the waves from different twist cancels out so the wire radiate less effectively.

→ It transmits either Analogue or Digital signal.

③ Coaxial Cable



→ It has better protection as, compared to twisted pair cable. Thus, it can transmit signal at higher speed and larger distance.

→ There are two kinds of cable ①. 50 Ω which is used for digital transmission and the other one is 75 Ω that is used for analog transmission and Cable TV.

→ It is a good combination of high bandwidth & excellent noise immunity as compared to twisted pair cable.

→ The bandwidth depends on cable quality, length of the cable and signal to Noise Ratio (SNR) of the data signal.

④ Power lines

→ Power lines deliver electrical power to houses and distribute the power to the electrical wiring within houses electrical devices.

⑤ Fiber Optics Cable

→ It is made up of glass or plastic and transmits signal in the form of light.
Light travels in a straight line as long as it is moving through a single uniform substance.

→ The optical transmission system consists of light source, transmission medium, detector.

→ For angle of incidence above a certain angle or critical value the light is reflected back into the medium, none of it escape into the air, Thus a light ray incident at or above critical angle is trapped inside the fiber and can transmit for many km with minimum loss.

Fibre Cable

→ Core is surrounded by a glass cladding with a low refractive index as compared to the refractive index of core. (to achieve TIR)

The cladding is protected by thin plastic jacket.

Advantages of fiber optics w.r.t co-axial cable

→ High bandwidth as compared to that of co-axial cable.

→ Attention $db = 10 \log_{10} \frac{\text{Transmitted power}}{\text{Received power}}$

Low Attenuation as compared to copper wire / co-axial cable.

→ Fiber optics cable are not been affected by electromagnetic interference.

→ Due to low attenuation, repeaters are needed only about every 50 Km where as incase of co-axial cable repeaters are required at every 5 Km.

Non-Guided Transmission Media (wireless Transmission)

① Electromagnetic Spectrum

When an antenna of appropriate size is attached to an electrical circuit. The electromagnetic waves can be broadcasted effectively and received by a receiver some distance away.

$$f = \frac{c}{\lambda}$$

$$\frac{df}{d\lambda} = \frac{d(c/\lambda)}{d\lambda} = c\frac{d\lambda^{-1}}{d\lambda} = \frac{-c}{\lambda^2}$$

$$\Rightarrow \Delta f = \frac{c\,\Delta\lambda}{\lambda^2}$$

from Δf, the data rate can be calculated provided $\Delta\lambda$ is given to you.

Q Consider $\lambda = 1.3 \times 10^{-6}$, $\Delta\lambda = 0.17 \times 10^{-6}$. Find out Δf

Ans $\Delta f = \dfrac{3\times10^{8} \times 0.17 \times 10^{-6}}{1.3 \times 1.3 \times 10^{-6} \times 10^{-6}}$

$= \dfrac{0.51}{1.69} \times 10^{14} = 0.301 \times 10^{14}$ Hz

$= 30 \times 10^{12}$ Hz

$= 30$ THz

→ The Electromagnetic spectrum is from 10^{4} Hz to 10^{16} Hz

→ In case wide band spectrum is used then two type of variation is possible.

ⓐ Frequency hopping spread spectrum

The transmitter hops from frequency to frequency 100 time per second.

e.g used in military communication i.e it makes transmission hard to detect and avoid jamming.

→ It offers good resistance to multipath fading because the direct signal will arrive first to the receiver. The reflected signal follows longer path and arrive late. By then the receiver may have changed frequency and no longer accept signal thus eliminating interference.

ⓑ Direct sequence spread spectrum

→ It spreads the signal over a wide frequency band.

→ It is used in 2nd generation mobile phone.

→ It has good spectral efficiency and noise immunity

① Radio Wave Transmission - It has a frequency range from 3KHz to 1 GHz.

→ These waves are easy to generate and can travel long distances.

→ They are omnidirectional and used for communication between both indoor and outdoor because they have a property that they can penetrate through the walls very easily.

→ They are used for AM and FM radio, television, cellular phones and wireless LAN.

② Microwave Transmission

→ It has a frequency range from 1GHz to 300GH

→ They can travel to longer distance.

→ They are unidirectional i.e they travel in straight line.

→ At high frequency they can't penetrate into the walls.

→ They provide communication between sender and receiver, cellular phone, ~~satal~~ satellite network and wireless LAN.

③ Infrared Transmission

→ They have a frequency range between 300GHz to 400 GHz.

→ These can't travel along long distance.

→ They are used for short distance or short range communication and use line of sight propagation.

→ They can't pass through solid object. They are used in remote control.

④ Light Transmission

Theoretical Basis for Data Communication

Information can be transmitted on transmission line by changing some physical property i.e voltage / current.

→ By representing the value of this voltage / current as a single value function of time $f(t)$ we can model the behaviour of the signal and analyze it mathematically.

Model

A periodic function $g(t)$ with a period of 'T' can be constructed as the sum of number of sines and cosines.

$$g(t) = \frac{1}{2}C + \sum_{n=1}^{\infty} a_n \sin(2\pi n f t) + \sum_{n=1}^{\infty} b_n \cos(2\pi n f t)$$

where C = Constant

$f = \frac{1}{T}$ which is called as fundamental frequency

a_n & b_n are the Sine and Cosine amplitude of the nth harmonic term

→ Such type of model is called as Fourier series.

→ From the Fourier series the function can be reconstructed if 'T' is known and the amplitudes are given.

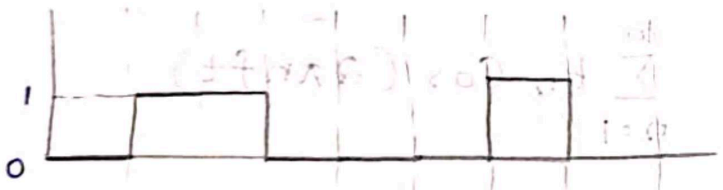
$$a_n = \frac{2}{T}\int_0^T g(t)\sin(2\pi n f t)\,dt$$

$$b_n = \frac{2}{T}\int_0^T g(t)\cos(2\pi n f t)\,dt$$

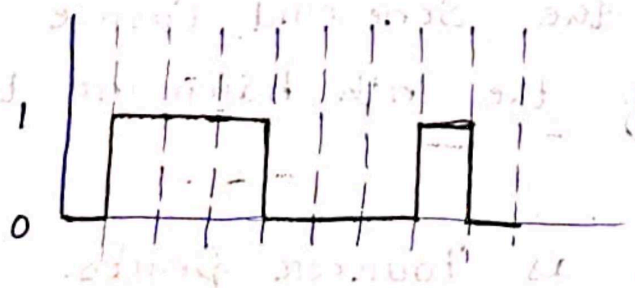
$$c = \frac{2}{T}\int_0^T g(t)\,dt$$

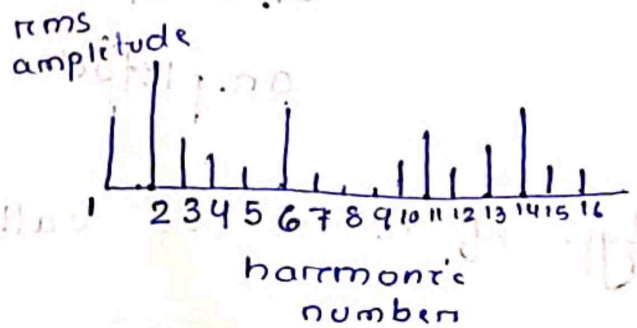
Bandwidth Limited Signal

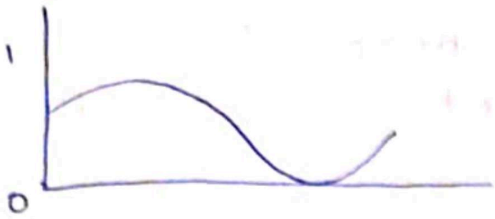
b = 01100010

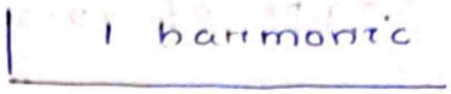


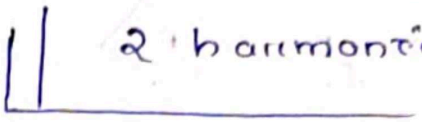
b = 01100010

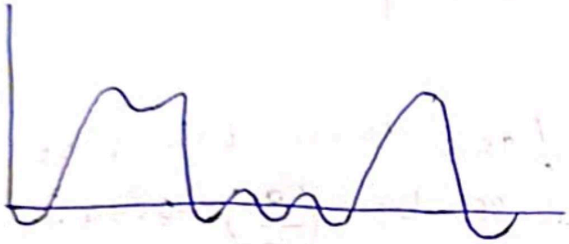


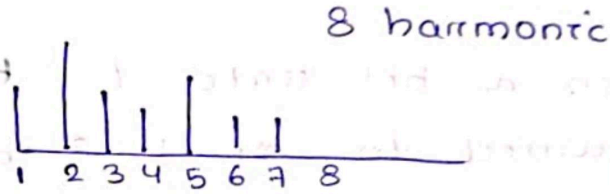












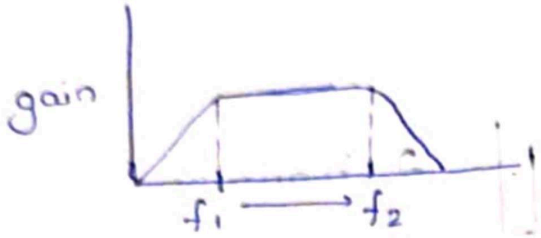
$$a_n = \frac{1}{\pi n}\left[\cos\left(\frac{\pi x}{4}\right) - \cos\left(\frac{3\pi x}{4}\right) + \cos\left(\frac{6\pi x}{4}\right) - \cos\left(\frac{7\pi x}{4}\right)\right]$$

$$b_n = \frac{1}{\pi n}\left[\sin\left(\frac{3\pi x}{4}\right) - \sin\left(\frac{\pi x}{4}\right) + \sin\left(\frac{7\pi x}{4}\right) - \sin\left(\frac{6\pi x}{4}\right)\right]$$

$$c = \frac{3}{4}$$

rms amplitude $= \sqrt{a_n^2 + b_n^2}$

The range of frequency without being strongly attunated (type of loss) is called <u>bandwidth</u>



Bandwidth = $f_2 - f_1$

* Unit of Bandwidth is bit per sec

→ Given a bit rate of b bits/sec then the time required to send 8 bits will be $\left(\frac{8}{b}\right)$ secs.

→ Frequency of 1st harmonic $\left(\frac{b}{8}\right)$ Hertz.

→ Telephone line has a cut-off frequency just above 3 KHz or 3000 Hz.

→ Find out number of harmonic passed →

B.W = 3KHZ

$f = b/8$

$$H_n = \frac{3000}{b/8} = \frac{24000}{b}$$

Q Consider bits/sec is 300. Find out the no. of harmonic passed.

$$H_n = \frac{2400}{300} = 80 \text{ harmonics.}$$

If bits/sec = 4800

$$H_n = \frac{2400}{4800} = 5 \text{ harmonics}$$

If bits/sec = 38400

$$H_n = \frac{\cancel{2400}\,5}{\cancel{3840}\,8} = \frac{5}{8} \approx 0 \text{ harmonic}$$

→ In most application an Analogue signal is sampled, converted to digital form on which operations are performed which is finally reconstructed to Analog form.

→ For data communication a signal i.e transmitted has infinite number of terms in its fourier transform. However with this signal needs to be transmitted through a channel having fixed bandwidth, band limiting is required.

→ The signal that runs from 0 to maximum frequency is called as <u>baseband signal</u>.

→ Signals that are shifted to occupy high range of frequency is called as passband signal.

Theorem - Nyquist

The maximum data rate of a channel

Maximum data rate = $2H \log_2 V$ bits/sec

↓ noiseless channel

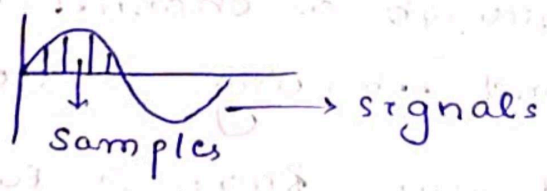
Maximum data rate = $H \log_2 (1+SNR)$

↓ noisy channel

$H = B \cdot \omega$

V = discrete level

→ According to Nyquist, if a arbitrary signal runs through a low pass filter of bandwidth 'H', the filtered signal can be completely reconstructed by making only 2H samples/sec.



→ Sampling the line faster than 2H times/sec is pointless because the higher frequency components are already been filtered out.

Noiseless Channel

B.W = 3 KHZ

→ If the Bandwidth is 3KHZ for a noiseless channel it means it can't transmit binary signal at a rate greater than 6000 bits/sec.

Q How much bandwidth is there in 0.1 micron of spectrum at a wavelength of 1 micron.

Ans

$$\Delta F = \frac{c\,\Delta\lambda}{\lambda^2}$$

$$= \frac{3\times10^{8}\times10^{-6}}{10^{-12}}$$

$$= 3\times10^{8-6+12}$$

$$= 3\times10^{14} \text{ Hertz}$$

Q It is desired to send a sequence of computer screen images over an optical fibre. The screen is 3840 × 2160 pixels, each pixel being 24 bits. There are 50 screen images per second. What data rate is needed?

Ans DR = 3840 × 2160 × 24 × 50 bits/sec.

Q Consider the noiseless channel transmitting a signal with 4 signal levels, find out the maximum bit rate assuming the bandwidth 3 KHz.

Ans. Max. ~~data~~ bit rate $= 2H \log_2 V$

$\boxed{V = 2}$

$= 2 \times 3$

$= 6$ KHz

Q Calculate maximum data rate if a noiseless 4KHz channel is sampled every 1 milisecond.

Ans $H = 4$ KHz $\quad f = 10^3$

M.D.R $= 2 \times 4 \log_2 2$

$=$ ~~8 KHz/s~~ 80 Kbits/sec

Q With the normal 4KHz channel shannon limit would not allow this. ~~For the~~

For the 4KHz channel we can make 8000 samples/sec. In this case if each sample is 1024 bits this channel can send 8.2 M bits/s

Q What is the channel capacity for bandwidth of 3KHZ and signal to noise ratio as 20 db.

Ans $SNR = 20$ db.

$\Rightarrow 10 \log_{10} SNR = 20$

$\Rightarrow$ ~~$\log_{10} SNR = 2$~~

$\Rightarrow \log_{10} SNR = 2$

$\Rightarrow SNR = 100$

$M.D.R = H \log_2 (1 + SNR)$

$= 3 \log_2 (101)$ $\quad (\log_2 (101) = 6.65)$

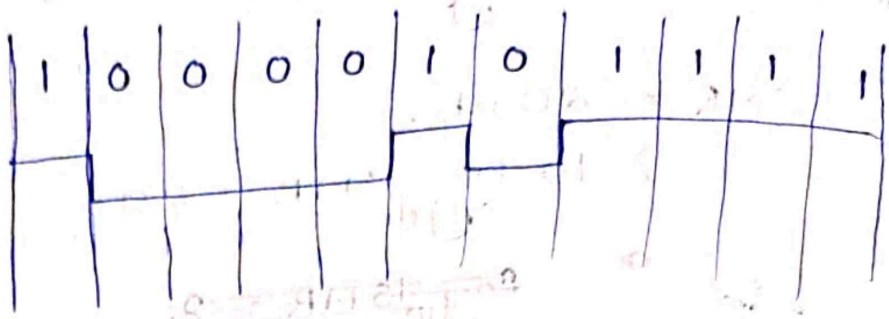
$= 19.97$

Digital Modulation

Baseband Transmission

a) bit stream

b) NRZ

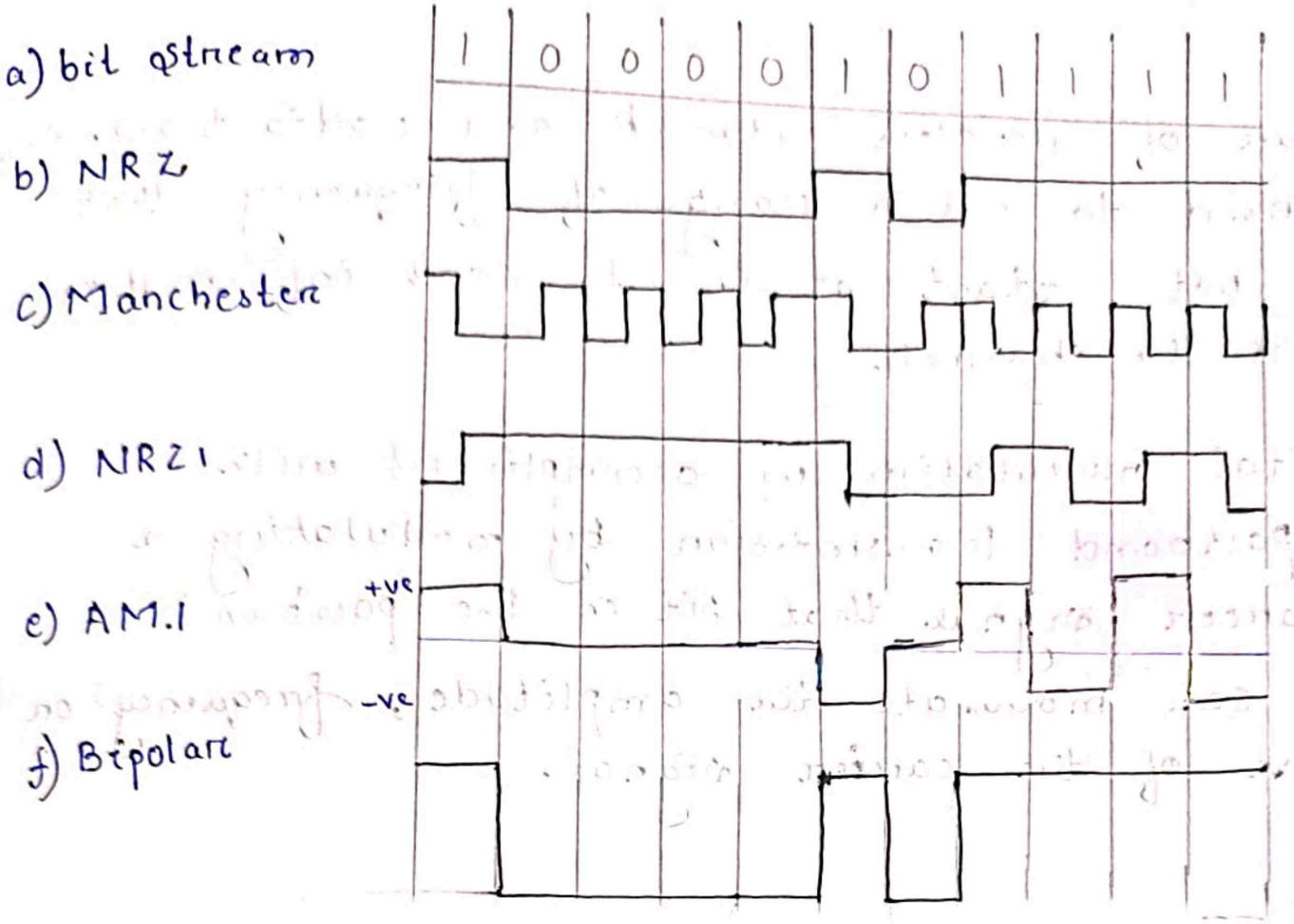


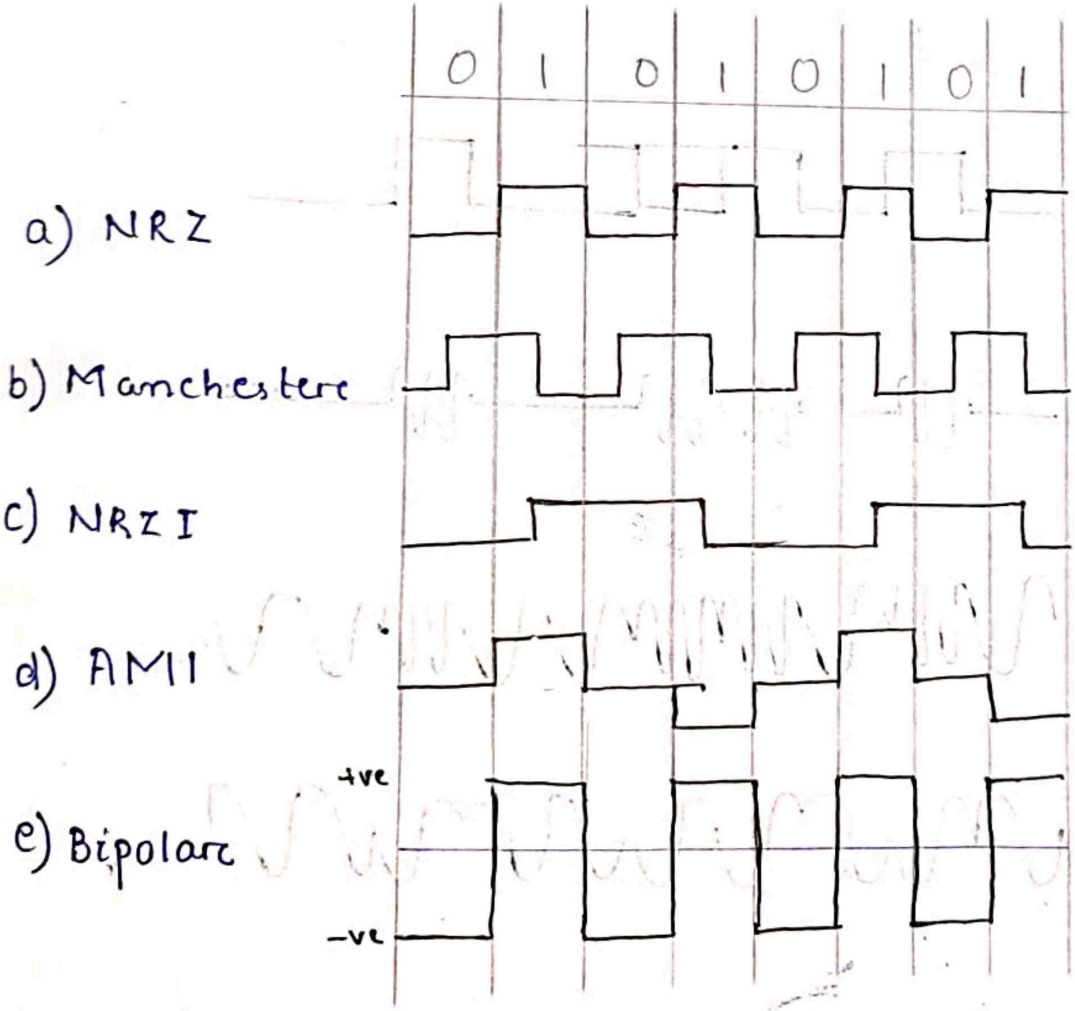
This type of coding technique is simple. Such type of coding techniques are called as line coding techniques

→ With NRZ the signal may cycle between the positive and negative levels, upto every 2 bits (incase of alternate 1 & 0)

→ It means that we need a bandwidth of atleast b/2 hertz when the bit rate is b bits/sec. Thus, we can't run NRZ faster without using additional bandwidth.

→ One strategy for improving the bandwidth is to use more than 2 signal level.

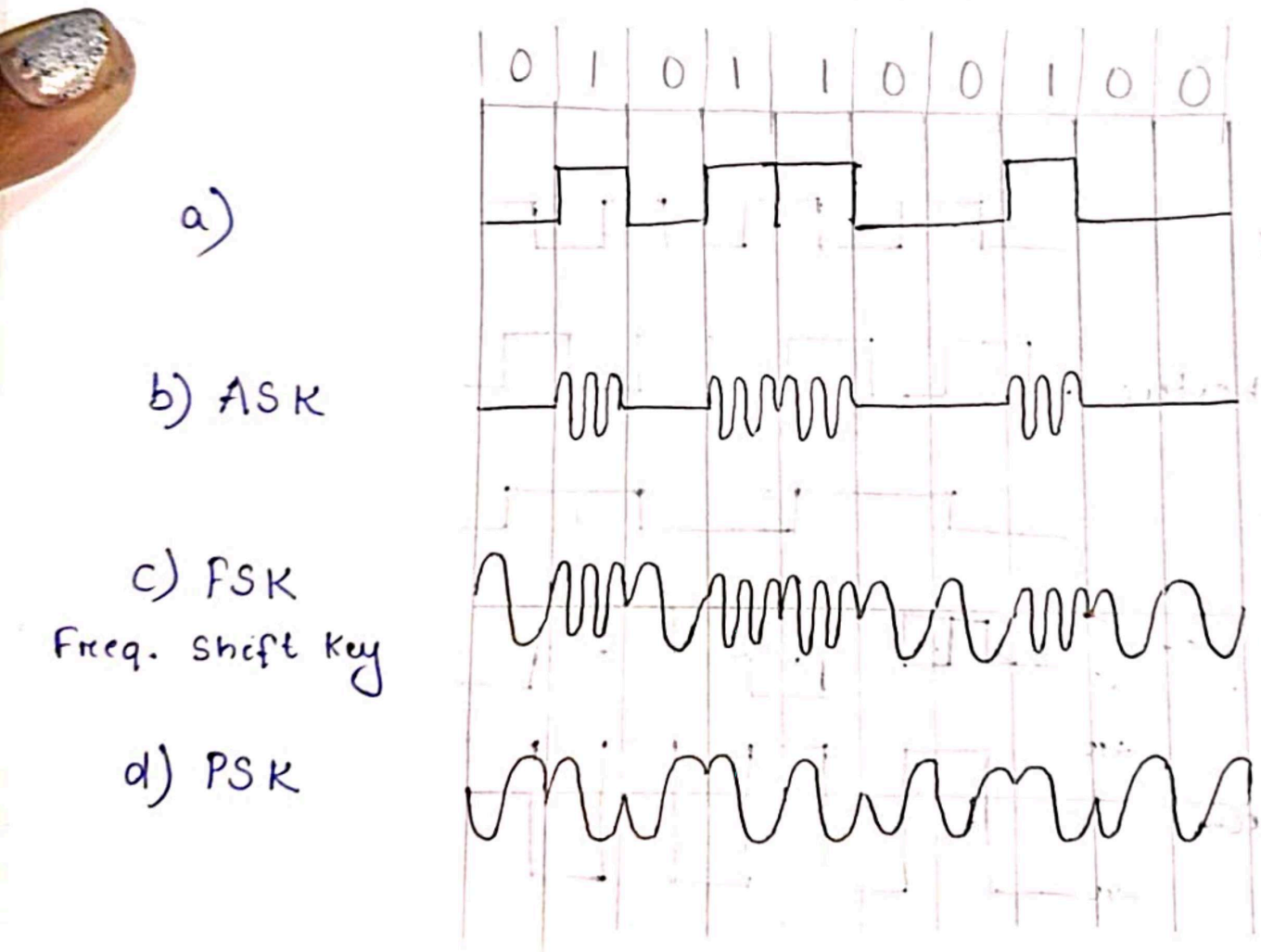

a) bit stream
1 0 0 0 0 1 0 1 1 1 1
b) NRZ
c) Manchester
d) NRZI
e) AMI
+ve
-ve
f) Bipolar

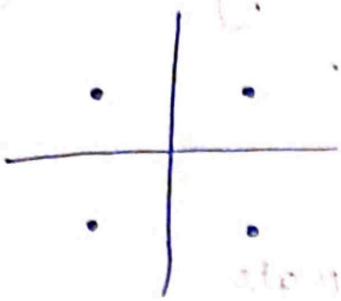

0 1 0 1 0 1 0 1
a) NRZ
b) Manchestere
c) NRZI
d) AMI
+ve
e) Bipolar
-ve

Passband Transmission

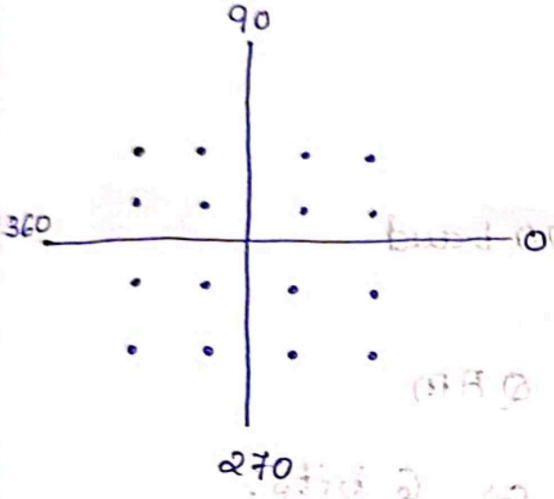
→ In case of wireless network and radio transmission we need to use a range of frequency that does not start at 0 to send information across the channel.

→ Digital modulation is accomplished with passband transmission by modulating a carrier signal that sit in the passband.
We can modulate the amplitude, frequency or phase of the carrier signal.





Constellation diagram



QAM-16

Here phase and amplitude changes.

QAM → Quadriture Amplitude Modulation.

<u>Bit rate</u> - No. of bits per sec

<u>Symbol</u> - Each sample will send one piece of information which is called as symbol.

<u>Symbol rate</u> - $\left(\frac{\text{No. of symbol transmitted}}{\text{sec}}\right) \times \frac{\text{No. of bits}}{\text{symbol}}$

↓

Symbol rate / baud rate

Q Calculate the baud rate for the given bit rate and type of modulation.

a) Bit rate = 2000 bps, FSK

Ans Bit rate is same as ~~FSK~~ Baud rate

$\Rightarrow$ Baud rate = 2000 baud

b) Bit rate = 2000 bps, ASK

Ans Baud rate = Bit rate = 2000 baud

c) Bit rate = 36000 bits/sec, 64 QAM

Each symbol is represented as 6 bits.

$$\text{Baud rate} = \frac{36000}{6} = 6000 \text{ bits/sec}$$

Q Calculate the bit rate for the given baud rate and type of modulation.

a) Baud rate = 1000 baud, FSK

b) Baud rate = 1000 baud, ASK

c) Baud rate = 1000 baud. BPSK

d) Baud rate = 1000 baud, 16-QAM.

Ans a) Bit rate = 1000 bits/sec

b) Bit rate = 1000 bits/sec

c) Bit rate = 1000 bits/sec

d) Each symbol is represented as 4 bits

Bit rate = 1000 x 4

= 4000 bits/sec.

Multiplexing

Multiplexing scheme have been designed to share lines (transmission lines) among many signals.

Frequency Division Multiplexing

- It divides the spectrum to frequency band with each user having exclusive possesion of some band in which to send a signal.
- AM Radio broadcasting is an example of FDM.
- To keep the channel well separated guard band is used.
- When sending digital data it is possible to divide the spectrum efficiently without using guard band.

Orthogonal Frequency Division Multiplexing

Here the channel bandwidth is divided into many sub-carrier that independently sends data.

Time Division Multiplexing

- Here the User take turns (in a Round-Robin manner) each one periodically getting the entire bandwidth for certain time interval.

Q Assume that a voice channel occupy a bandwidth of 4KHz. We need to multiplex 12 voice channel with a guard band of 500 Hz using FDM. Calculate the required bandwidth.

Ans $12 \times 4000\ Hz = 48000\ Hz$

$500 \times 11 = 5500\ Hz$

Bandwidth $= 48000 + 5500$

$= 53500\ Hz$

$= 53.5\ KHz$

* 12 voice channel (4KHz) → group

5 groups → supergroup

5 /10 supergroups → 1 mastergroup

Q A tape can hold 200 G bytes. A box 60 cm X 60 cm X 60 cm can hold about 1000 tapes. What are effective bandwidth if the destination is

a) an hour

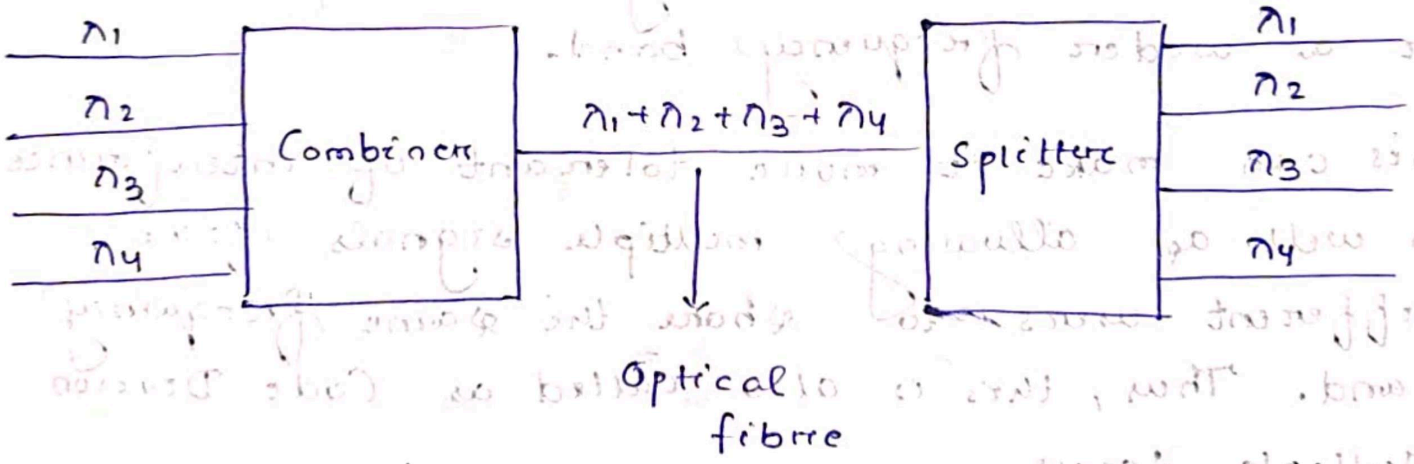
b) 24 hours away by road

Ans a) $200 \times 10^9 \times 8$ bits

$= 1600 \times 10^9$ bits

$$\text{Bandwidth} = \frac{\cancel{1600}^{\,4\,0.444} \times 10^9}{\cancel{3600}_{\,9}} = 444 \times 10^{11} \text{ bits/sec}$$

Wavelength Division Multiplexing



→ WDM is a form of FDM that multiplex multiple signals on an optical fibre using different wavelength of light.

→ The different wavelength of light are combined onto a single shared fibre for transmission to a distant destination.

→ At the far end the beam is split ~~over~~ up over as many fibres as there were on the input side.

→ Narrowing the spacing to 12.5 GHz supports 320 channel on a single fibre, further increasing the transmission capacity. Such system with large no. of channels and little space between each channel is called as Densed WDM.

Code Divison Multiplexing

→ CDM is a form of spread spectrum, communication in which a narrow band 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. Thus, this is also called as Code Divison Multiple Access.

→ In CDMA, each bit time is sub divided into m-short interval i.e called as chips. which are multiplied against the original data sequence.

→ Let us assume each station to be assigned with 8-bit code i.e called as chip sequence.

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)

To transmit a 1-bit a station send its chip sequence.

→ To transmit 0 it sends the negation of its chip sequence.

$S_1 = C = (-1\ +1\ -1\ +1\ +1\ +1\ -1\ -1)$

$S_2 = B + C = (-2\ 0\ 0\ 0\ +2\ +2\ 0\ -2)$

$S_3 = A + \bar{B} = (0\ 0\ -2\ +2\ 0\ -2\ 0\ +2)$

$S1 \cdot A = (+1\ -1\ +1\ +1\ +1\ -1\ -1\ -1)/8$

$= 0$

Q Suppose that A, B and C are simultaneously transmitting 0 bits using a CDMA system with the chip sequence

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)

What is the resulting chip sequence?

Ans Chip sequence

$A = (+1\ +1\ +1\ -1\ -1\ +1\ -1\ -1)$

$B = (+1\ +1\ -1\ +1\ -1\ -1\ -1\ +1)$

$C = (+1\ -1\ +1\ -1\ -1\ -1\ +1\ +1)$

Public Switched Telephone Network (PSTN)

Switching

The phone system has 2 parts

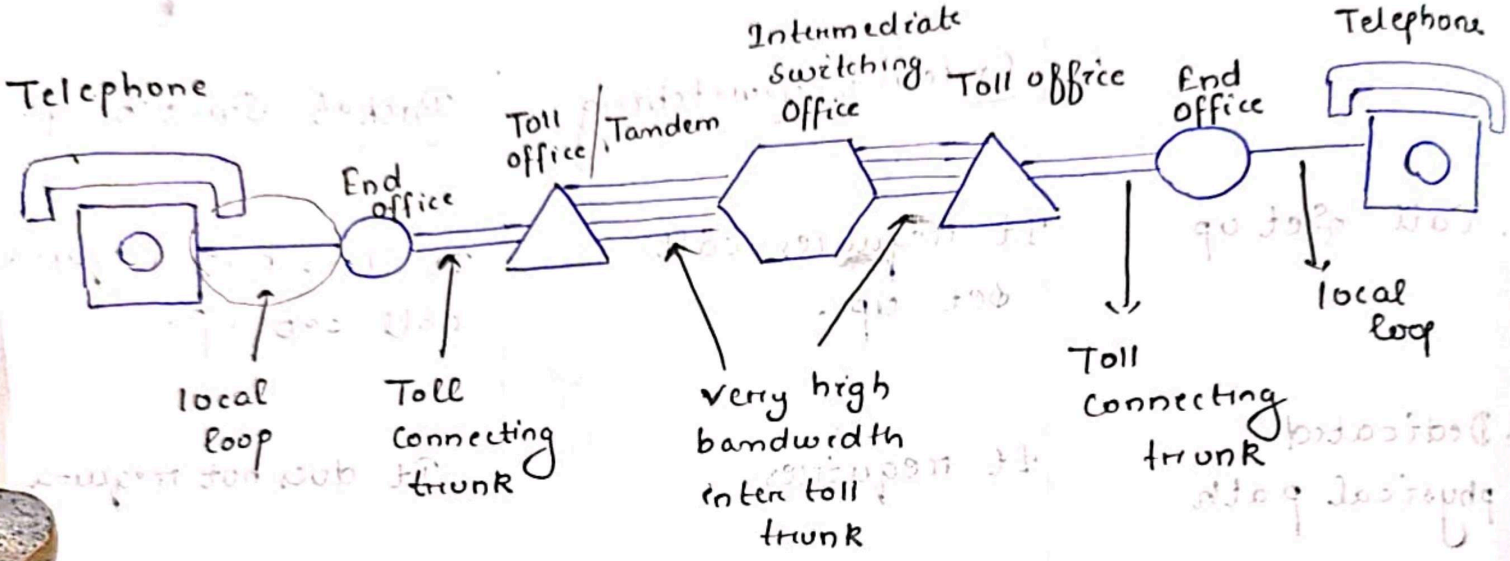
1) Outside plant → that consists of local loop and trunks

&

2) Inside plant → that consists of switches which are present in the switching office.

	Circuit Switching	Packet Switching
1. Call set up	It requires call set up.	It does not require call set up.
2. Dedicated physical path	It requires.	It does not require
3. Each packet follows the same rule.	It follows	It does not follow.
4. Packets arrive in order.	arrives	does not arrives.
5. Bandwidth available	It has fixed bandwidth.	It has dynamic bandwidth.
6. Store & forward transmission.	It does not require.	It requires.
7. Time of possible conjunction.	at set up time	at any time.

8. Potentially wasted bandwidth	wasted	not wasted



→ The wire connecting between the subscribers telephone and the end office is called as <u>local loop</u>.

→ If a subscriber attached to a given <u>end office</u> calls another subscriber attached to the same end office, then the communication takes place directly between the two local loop.

If the called telephone is attached to another end office, in such case each end office has a number of outgoing lines to one or more nearby switching office. which is called as <u>toll office</u> or <u>tandem office</u>. These lines are called as

toll connecting trunk.

→ If the caller and the calley don't have a toll office in common, a path will have to be established between the two toll office via high bandwidth inter toll trunk

Local Loop (Modem)

When a computer wish to send digital data over an analogue dial up line, the data must be first converted to analogue form for transmission over the local loop. This conversion is been done by a device i.e called as Modem.

A Modem is a device that accepts a serial stream of bits as input and produce a carrier modulated i.e Amplitude, Frequency, Phase is called as Modem.

Each modem samples 2400 times/sec.

Q If the voltage 0, 1, 2 and 3 Volts are used, every symbol consist of 2 bits, so a 2400 baud line can transmit (i) symbol/sec at a data rate of (ii)

Ans (i) 2400

(ii) 4800

TCM

Higher data rate requires a large set of symbols which results in an error, to reduce the chance of error standards for high speed modem use some of the symbol for error correction. This scheme is called as TCM (Trellis code Modulation).

Switching

The phone system has 2 parts

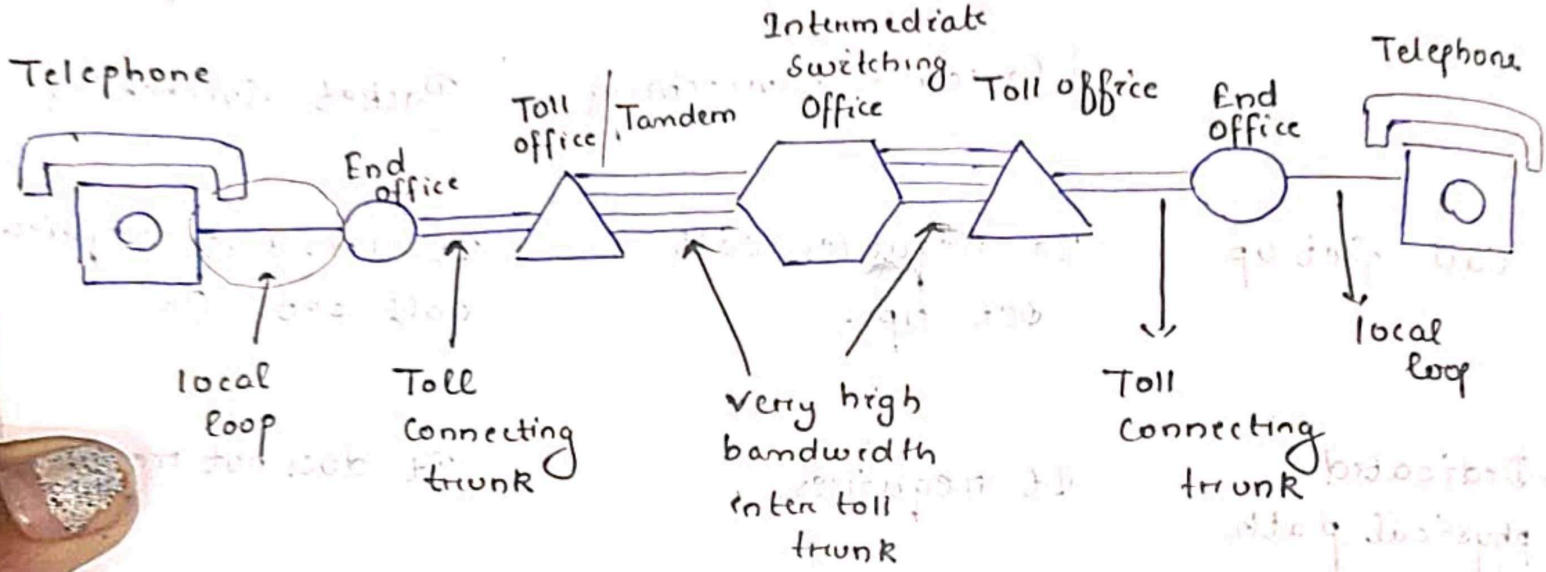
1) Outside plant → that consists of local loop and trunks

2) Inside plant → that consists of switches which are present in the switching office.

	Circuit Switching	Packet Switching
1. Call set up	It requires call set up.	It does not require call set up.
2. Dedicated physical path	It requires.	It does not require
3. Each packet follows the same rule.	It follows	It does not follow.
4. Packets arrive in order.	arrives	does not arrives.
5. Bandwidth available	It has fixed bandwidth.	It has dynamic bandwidth.
6. Store & forward transmission.	It does not require.	It requires.
7. Time of possible conjunction.	at set up time	at any time.

8. Potentially wasted bandwidth	wasted	not wasted

PSTN (Public Switched Telephone Network)



→ The wire connecting between the subscriber's telephone and the end office is called as <u>local loop</u>.

→ If a subscriber attached to a given <u>end office</u> calls another subscriber attached to the same end office, then the communication takes place directly between the two local loop.

If the called telephone is attached to another end office, in such case each end office has a number of outgoing lines to one or more nearby switching office. which is called as <u>toll office</u> or <u>tandem office</u>. These lines are called as

toll connecting trunk.

→ If the caller and the called don't have a toll office in common, a path will have to be established between the two toll office via high bandwidth inter toll trunk

Local Loop (Modem)

When a computer wish to send digital data over an analogue dial up line, the data must be first converted to analogue form for transmission over the local loop. This conversion is been done by a device i.e called as Modem.

A Modem is a device that accepts a serial stream of bits as input and produce a carrier modulated i.e Amplitude, Frequency, Phase is called as Modem.

Each modem samples 2400 times/sec.

Q If the voltage 0, 1, 2 and 3 Volts are used, every symbol consist of 2 bits, so a 2400 baud line can transmit (i) symbol/sec at a data rate of (ii).

Ans (i) 2400

(ii) 4800

TCM

Higher data rate requires a large set of symbols which results in an error, to reduce the chance of error standards for high speed modem use some of the symbol for error correction. This scheme is called as TCM (Trellis code Modulation).

Q A CDMA receiver gets the following chips

{0, 0 -2 +2 0 -2 0 +2}

Assuming the following chip sequence.

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)

Determine the information received by individual station.

A) R.S = 0 + 0 + 2 + 2 + 0 + 2 + 0 + 2 = 8/8 = 1 (sending 1 bit)

B) R.S = 0 + 0 - 2 - 2 + 0 - 2 + 0 - 2 = -8/8 = -1 (sending 0 bit)

C) R.S = 0 + 0 + 2 + 2 + 0 - 2 + 0 - 2 = 0/8 = 0

D) R.S 0 + 0 + 2 - 2 + 0 + 2 + 0 - 2 = 0/8 = 0

} remaining idle

T1 Carrier System

- In case of T1 carrier system 24 voice channels can be multiplexed. Each voice channel sends 8-bits of information among which 7-bits are used for data and 1-bit is used for signal.

- Thus, the data rate per channel is 7×8000 i.e 56 Kbps. and signalling information per channel 1×8000 i.e 8 Kbps.

→ Thus, a frame consists of 192 bits i.e $(24 \times 8) + 1$ extra bit is used for framing i.e 193 bits for every 125 μsec thus the gross data rate is 193×8000 i.e 1.544 Mbps.

T2 Carrier System

4 T1 combine to form 1 T2

Gross data rate is 4×1.544 Mbps = $\underbrace{6.176 \text{ Mbps}}_{\text{It should be this but}}$

It actually is 6.312 Mbps

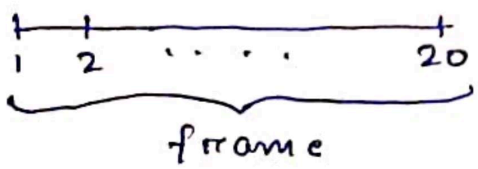
7 T2 → T3
6 T3 → T4

3G	4G	5G
→ introduced in 2001	introduced in 2009	introduced in 2018
→ use WCDMA	use LTE (Long term evaluation) and WiMax (IEEE 802.16)	use MIMO, mm Waves.
→ Uses normally circuit and packet switching both.	uses packet switching	uses packet switching
25 MHZ	100 MHZ	30 GHz - 300 GHz
→ higher security & international roaming.	high speed global mobility.	extremely high speed, low latency
→ provides broadband service	provides ultra broadband service.	provides wireless WWW

Q) We need to use TDM and combine 20 digital source each of 100 kbps. Each output slot carries 1 bit from each digital source, but 1 extra bit is added to each frame for synchronization.

) What is the size of an output frame in bits?

ns



$(20 \times 1) + 1 = 21$ bits.

ii) What is the output frame rate?

Ans 100 kbps = 100 bits/sec

$$\frac{bits}{sec} \times \frac{frames}{bit} = frames/sec$$

$$100 \times 10^3 \times 1 = 100\,kbps = 10^5\,bps$$

Each source = 100×10^3 bits/sec

Each source's contribution to the frame is 1 bit

How many frame's are being transmitted in 1 sec?

iii) What is the duration of the output frame?

Ans frame duration $= \frac{1}{10^5} = 10^{-5}$ sec $= 10\,\mu sec$

iv) What is the output data rate?

Ans Data rate (bps) $= \frac{frame}{sec} \times \frac{bits}{frame} = 10^5 \times 21$

$= 21 \times 10^5$ bps

$= 2.1$ Mbps.

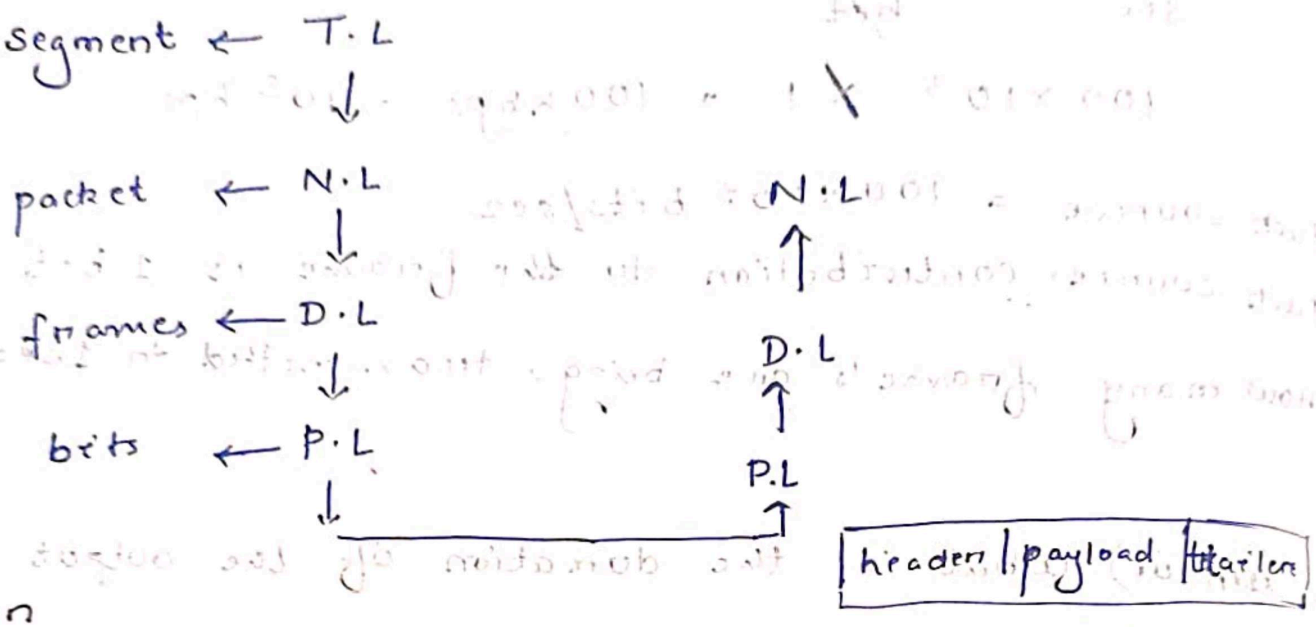
v) What is the efficiency of the system (ratio of useful bits to the total bits)?

Ans

Efficiency $= \frac{20}{21} = 0.95$

Chapter - 3

Data link Layer



Function

→ It provides well define service interface to the network layer.

→ Dealing with transmission error.

→ Regulate the flow of data so that slow receiver are not ~~swapped~~ swamped by fast receiver.

→ It introduces the concept of framing, hence, frame management is the important task of data link layer.

Design issue of Data Link Layer

① Service provided to Network layer.

Service is to transfer data from the network layer on the source machine to the network layer in the destination machine.

a) unack. connectionless service

b) acknowledged connectionless service.

c) acknowledged connection ~~less~~ oriented service.

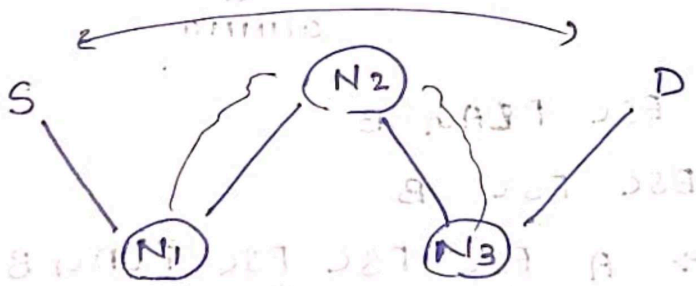
② Framing

→ To provide service to the network layer, the data link layer must use the service provided to it by the physical layer.

→ The data link layer detect and correct ~~the~~ error from the ~~information~~ ~~between~~ nodes to node ~~and not between source to node~~, from the information received by the physical layer.

→ Usual approach is to break the bits into frame and compute the checksum of each frame.

→ Converting the bits stream into frame is called as framing.



① ~~[illegible]~~ Byte Count

→ This method uses a field in the header to specify the number of characters in the frame.

→ When the data link layer at the destination see the character count, it knows how many characters follows and hence when the frame ends.

Byte Count

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

Frame-1	Frame-2	Frame-3	Frame-4
5 bytes	5 bytes	8 bytes	8 bytes

00000101

Let us assume it gets defected by noise then it becomes 7

(Disadvantage)

② Flag Byte with byte stuffing

→ Here each frame starts and ends with a special byte i.e called as flag byte.

Flag	Header	Payload	Trailer	Flag

01111110 01111110

A FLAG B → A ESC FLAG B

A ESC B → A ESC ESC B

A ESC FLAG B → A ESC ESC ESC FLAG B

A ESC ESC B → A ESC ESC ESC ESC B

↑

→ Basically, if both the flags given same 01111110 how it will recognize..

③ Flag Bits with bits stuffing

a) 0110 11111111111111111 0010

b) 0110 11111 011111011111010010

→ Here, the data frame rate contain arbitrary number of bits and also allow character ~~cood~~ code with an arbitrary no. of bits/sec. ~~the~~

→ Here, each frame begins and ends with a special pattern i.e., flag byte (01111110).

b) 0110 11111 011111011111010010

stuffed bits.

② Flag byte with byte stuffing:

→ Here, each frame starts and end with a special byte, called as flag byte.

A FLAG B → A ESC FLAG B

A ESC FLAG B → A ESC ESC FLAG B

A ESC B → A ESC ESC B

A ESC ESC B → A ESC ESC ESC ESC B

③ Flag bits with bits stuffing:

(a) 0110 11111111111111111110010

(b) 01101111110 11111011111010010

Stuffed bits

→ Here the data frame will contain arbitrary no. of bits and also allow character code with an arbitrary no. of bits per sec.

→ Here, each frame begins and ends with a special bit pattern i.e flag byte (01111110)

11/12/2023

Q. The following character encoding is used in datalink protocol

A: 01000111

B: 11100011

FLAG: 01111110

ESC: 11100000

Show the bit sequence (in binary) for the four character frame i.e A, B ESC FLAG when each of the framing method is used.

(a) Byte Count

(b) Flag byte with byte stuffing.

(c) Starting and ending bytes with bit stuffing.

Soln

(a) | 5 | A | B | ESC | FLAG |

00000101 01000111 11100011 11100000 01111110

(b) FLAG A B ESC ESC ESC FLAG FLAG

01111110 01000111 11100011 11100000 11100000

11100000 01111110 01111110

(c) FLAG A B ESC FLAG FLAG

01111110 01000111 11100011 11100000 01111110 01111110

0 0 0

Q2 You receive the following data fragment i.e 01100111 11001111 01111101. you know the protocol used is bit stuffing. Find out the data after destuffing.

Ans

01100111 11001111 01111101

↓ x x

01100111110111101111101

Q3. The following data fragments occurs in the middle of the data stream for which the byte stuffing algorithm is used.

A B ESC C ESC FLAG FLAG D

what is the output after stuffing?

=) ~~FLAG A B ESC ESC C ESC ESC ESC FLAG~~

giving it permission to send more data or atleast telling the sender how the receiver is doing.

② Rate based Flow Control:

The protocol has a built in mechanism that limits the rate at which sender may transmit the data without using feedback from the receiver.

③ Error Control:

An error might occur in a form of single bits or in the form of burst

→ What is the advantage of burst error?

Computer data are always sent in a form of blocks of bits. Suppose the block size is 1000 bits and the error rate is 1/1000 = 0.001 per bits. If error were independent, most block would contain an error.

If the error comes in burst of 100, only one to two blocks in 100 would be affected.

Disadvantages:

→ It is very difficult to correct.

Error correction and Detection

→ Error correcting code:

Two basic strategies are considered for dealing a error.

1) includes enough redundant information along with each block of data sent, to enable the receiver

⇒ FLAG A B (ESC) ESC C (ESC) ESC (ESC) FLAG
(ESC) FLAG D FLAG

Q4. A bit string 01111011111011111110 needs to be transmitted at the Data Link layer. What is the string actually transmitted after bit stuffing?

Ans: 01111011111 0 11111 1 0
0 0

⇒ 01111011111 0 0 11111 0 10

(3) Error Control — error correction
└ error detection

(4) Flow Control:

→ One of the design issue in the DLL is what to do with a sender that systematically wants to transmit frames faster than the receiver can accept it.

→ The sender keeps pumping the frame at a higher rate until the receiver is completely swamped.

→ Even if the transmission is error free, at a certain point, the receiver will be unable to handle the frames as they arrive and will start to lose some.

There are two approaches:

(1) Feedback based flow control:

The receiver sends back information to the sender

to deduce what the transmitted data must have been.

② Includes ~~enough~~ enough redundant information to allow the receiver to deduce that an error has occurred.

* This error correcting code is also called as forward error correction.

$m \rightarrow$ data word
$r \rightarrow$ redundant bits

$n = m + r$
↳ code word

Hamming distance (d):

The no. of bit position in which two code word differ is called hamming distance i.e if two code words are d-distance apart, it will require d single bit error to convert one into another.

```
10001001
10110001
---------
00111000
```

d = 3

* Error detecting and correcting properties of a code depends on the hamming distance.

① To detect d error a hamming distance d+1 is required because with such a code there is no way that d single bit error can change a valid code word into another valid codeword.

When the receiver see an invalid code word it will inform the transmitter that an error has occurred so re-transmit it.

② To correct d error you need a distance 2d code because that way the legal codewood are so far apart that even with d changes the original codewood is still closer than any other codewood, so it can be uniquely determined.

Q. Find the minimum hamming distance to be implemented in codewood for the following cases:

① Detection of 2 errors : $2+1 = 3$

② correction of 2 errors : $2d+1 = 2\times2+1 = 5$

③ Detection of 3 error or ~~detection~~ correction of 2 error:
4 3 5

④ Detection of 6 error or correction of 2 error:
6 5

Q. 16 bit messages are transmitted using a hamming code. How many check bits are needed to ensure that the receiver can detect and correct single bit error. Find out the bit pattern transmitted for the message. 1101001100110101. Assume that even parity is used in the hamming code.

Soln

$2^r \geq m+r+1$

~~$P_1 P_2 m_3 P_4 m_5 m_6 m_7 P_8 m_9 m_{10} m_{11}$~~ $r = 5$

P_1	P_2	m_3	P_4	m_5	m_6	m_7	P_8	m_9	m_{10}	m_{11}	m_{12}	m_{13}
0	1	1	1	1	0	1	1	0	0	1	1	0

m_{14}	m_{15}	P_{16}	m_{17}	m_{18}	m_{19}	m_{20}	m_{21}
0	1	1	1	0	1	0	1

0 1 1 1 1 0 1 1 0 0 1 1 0 0 1 1 1 0 1 0 1

Q An 8-bit message using even parity hamming code received as 101001001111. Find the 8-bit message after getting decoded assuming no error during transmission.

Ans 10101111

Error Detection

→ The detection scheme i.e polynomial code which is also called as cyclic Redundancy check (CRC)

→ Polynomial codes are based upon treating bit strings as representation of polynomials with coefficient of 0 and 1 only. A k-bits frame is regarded as a co-efficient list for a polynomial with k-terms ranging from x^0 to x^{k-1}. Such a polynomial is said to be ~~kod~~ degree k-1.

11001

$\Rightarrow x^4 + x^3 + x^0$

→ Long divison is carried out as modulo 2 or exclusive OR. A divisor is set "to go into" a dividend is the dividend has as many bits as the divisor.

Rules for CRC

1) When the polynomial code method is employed, the sender and receiver must agree upon a generator polynomial i.e. G(x) in advance.

→ Both the high and low order bits of the generator polynomial must be 1.

→ To compute the checksum for some frame with m bits, corresponding to the polynomial M(x), the frame must be larger than the generator polynomial.

→ The idea is to append a checksum to the end of the frame in such a way that the polynomial represented by the checksum frame is divisible by G(x).

→ When the receiver gets the checksum frame, it tries dividing it by G(x).

→ If there is a remainder, then there has been a transmission error.

```
        111101
1101 | 100100000
       1101
        1000
        1101
         1010
         1101
          1110
          1101
           0110
           0000
            1100
            1101
             001
```

→ checksum

Data word
↓
100100

Code word
↓
100100001

```
        111101
1101 | 1001000001
       1101
        1000
        1101
         1010
         1101
          1110
          1101
           0110
           0000
            1101
            1101
             000  → hence no error
```

Q The message 11001001 is to be transmitted using the CRC polynomial x^3+1 to protect it from error, what is the message that needs to be transmitted.

```
        11010011
1001 | 11001001000
       1001
        1011
        1001
         0100
         0000
          1000
          1001
           0011
           0000
            0110
            0000
```

```
1100
1001
----
1010
1001
----
 011
```

11001001011

Q. Find what is the condition for $G(x)$

Q. What is the remainder obtained by dividing $x^7 + x^5 + 1$. By the generator polynomial $x^3 + 1$

```
        1011011
1001 | 1010000010000
       1001
       ----
        0110
        0000
        ----
         1100
         1001
         ----
          1010
          1001
          ----
           0111
           0000
           ----
            1110
```

```
1110
1001
----
 1110
 1001
 ----
  1110
  1001
  ----
   111
```

$$\boxed{x^2 + x + 1}$$

Q A bit stream 10101010 is transmitted using the standard CRC method, the generator polynomial is $x^3 + x^2 + 1$. Show the actual bit stream transmitted. Suppose the 2nd bit from the left is inverted during transmission show that this error is detected at the receivers end.

```
1110
0000
----
 0111
 1011
 ----
  1110
  0000
  ----
```

Ans

```
        11011110
1101 | 10101010 000
       1101
       ----
        1111
        1101
        ----
         0100
         0000
         ----
          1001
          1101
          ----
           1000
           1101
           ----
            1010
            1101
            ----
             1110
             1101
             ----
              0110
              0000
              ----
               110   → checksum.
               ----
               0111
```

Code word → 10101010 110

```
        10101010
1101 | 11101010 110
       1101
       ----
        0111
        0000
        ----
         1110
         1101
         ----
          0111
          0000
          ----
           1110
           1101
           ----
            0111
            0000
            ----
             1111
```

```
1111
1101
----
 0100
 0000
 ----
  100   → error
```

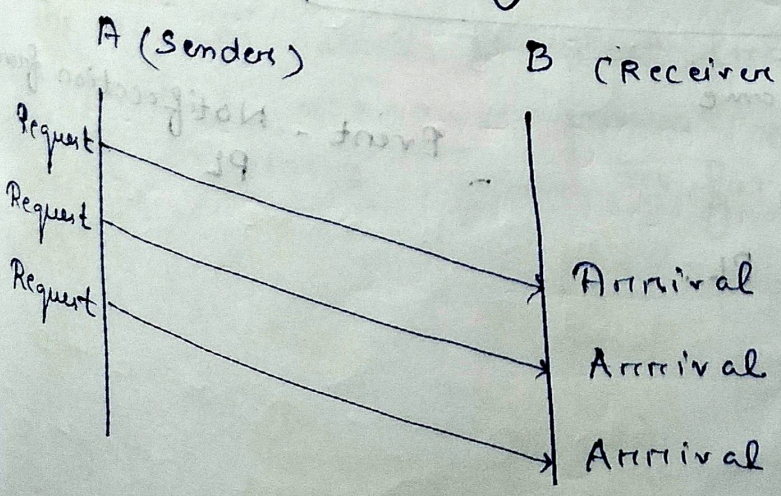
DLL Protocol

- Noiseless Channel
  - Simplex Protocol / Utopian Simplex Protocol
- Noisy Channel

Simplex Protocol

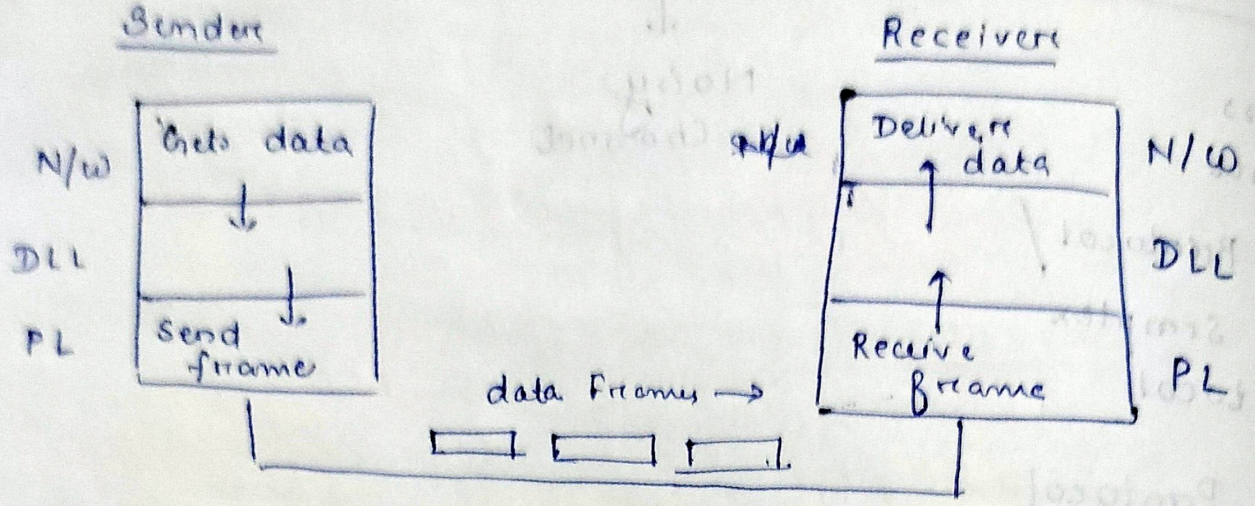
Assumptions

1) Unidirectional protocol : from sender to receiver
2) There is no flow control or error control.
3) It is assumed that both the sender and the receiver are always ready for data processing and both of them have infinite buffer.
4) In order to send 3 ~~times~~ frame 3 events occur ~~occur~~ at the sender side and 3 occurs in the receiver side.
5) The data frames are indicated by tilted box or line because (the height of the box defines the transmission time difference b/w the 1st bit and the last bit in the frame.



(Flow diagram)

Design

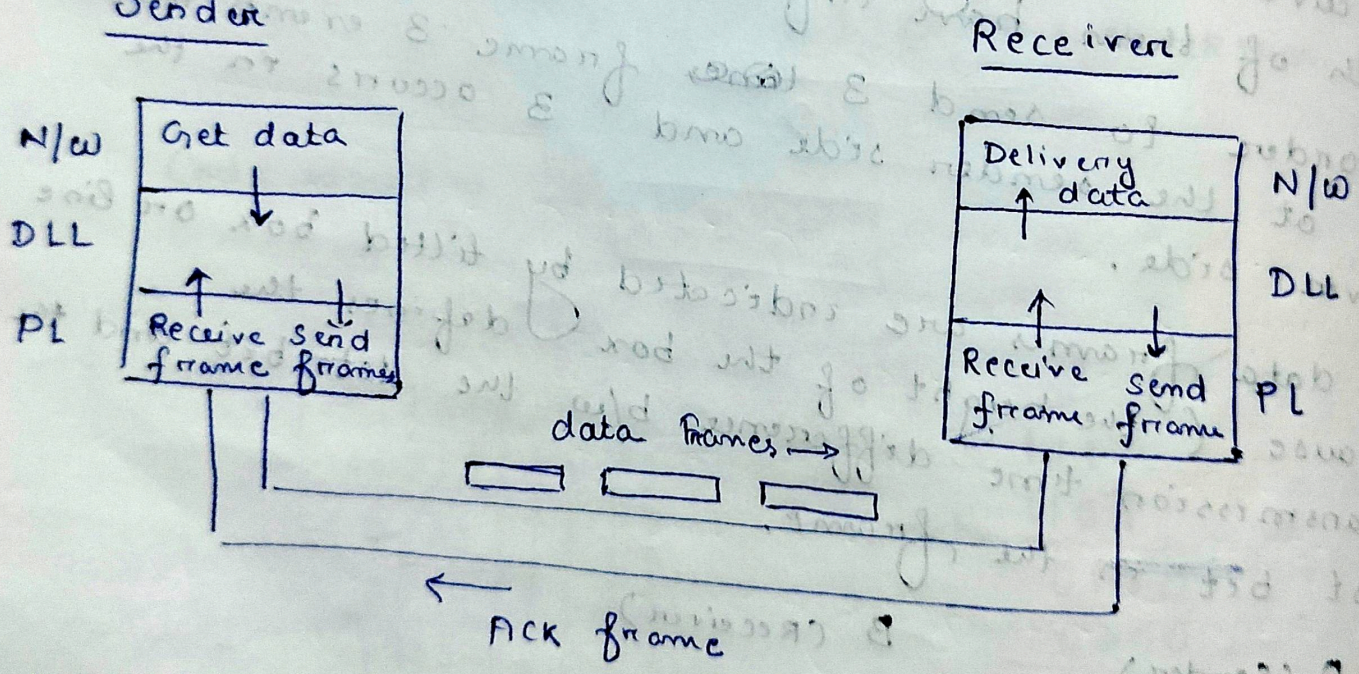


Event → Request from N/w

Event - Notification from PL

Simplex stop and wait protocol

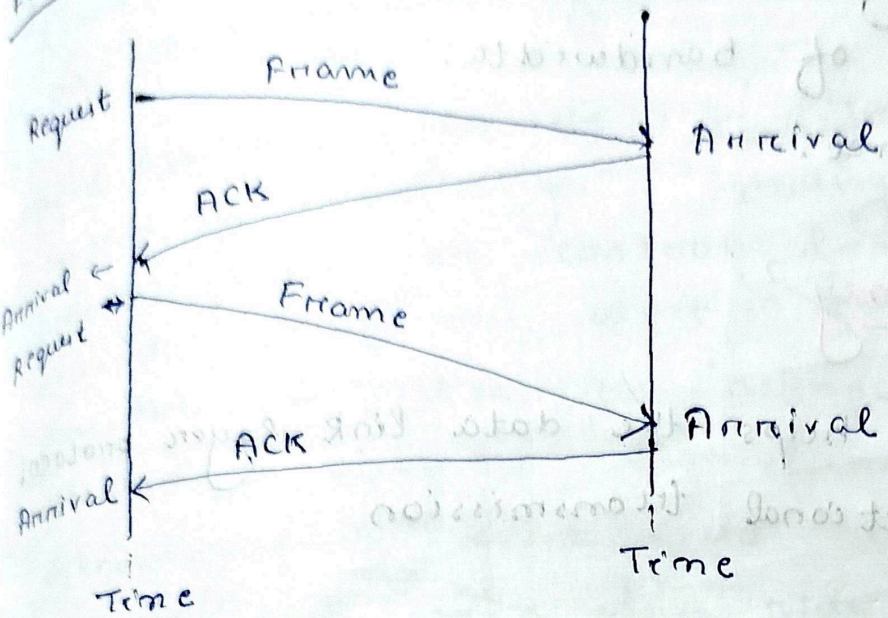
Design



Event → Request from N/w
→ Notification from PL.

Event - Notification from PL

Flow Diagram



→ Simplex Stop and wait Protocol is used for transmission of frames over noiseless channel.

→ It provides ~~unico~~ uni-directional data transmission with flow control facility but without error control facility.

→ Here, the receiver has finite processing speed.

→ If data frames arrives at the receiver end at a rate which is greater than its rate of processing than frames are dropped out.

→ To avoid this situation the receiver sends an acknowledgement for each frame upon its arrival.

→ The sender sends the next frame only when it receives a positive acknowledgement from the receiver that it is available for ~~the~~ further data processing.

Drawbacks

→ Transmits one frame at a time.

→ Poor utilization of bandwidth.

→ Poor performance.

Improving Efficiency

Piggybacking - It helps the data link layer protocol to achieve bidirectional transmission

Sliding window - Improves transmission efficiency by alarming the sender to have multiple bytes to be transmitted.

Piggybacking

→ **First approach** for the full duplex data transmission to each station using a separate link for simplex data traffic in different direction.

Each link consist of a forward channel (for data) and a reverse channel for acknowledgement.

In both cases, the capacity of the reverse channel is wasted.

→ **Second approach** - In this approach same link for data in both direction is used.

In this model the data frames from a→b are intermixed with the acknowledgement frame from a→b

By looking at the header portion in the incoming frame, the receiver tell whether it is a data frame or an acknowledgement frame.

Third Approach - When the data frame arrives instead of immediately ~~sen~~ sending a separate acknowledgement or control frames, the receiver research itself and wait in the N/w layer pass the next packet, the acknowledgement is attached to outgoing data frame (using the acknowledgement ~~get a~~ field in the frame header) i.e. the ack get a free ride on the next outgoing data frame. The technique of temporarily outgoing acknowledgement so that they can be hooked on to the next outgoing dataframe is called as piggybacking.

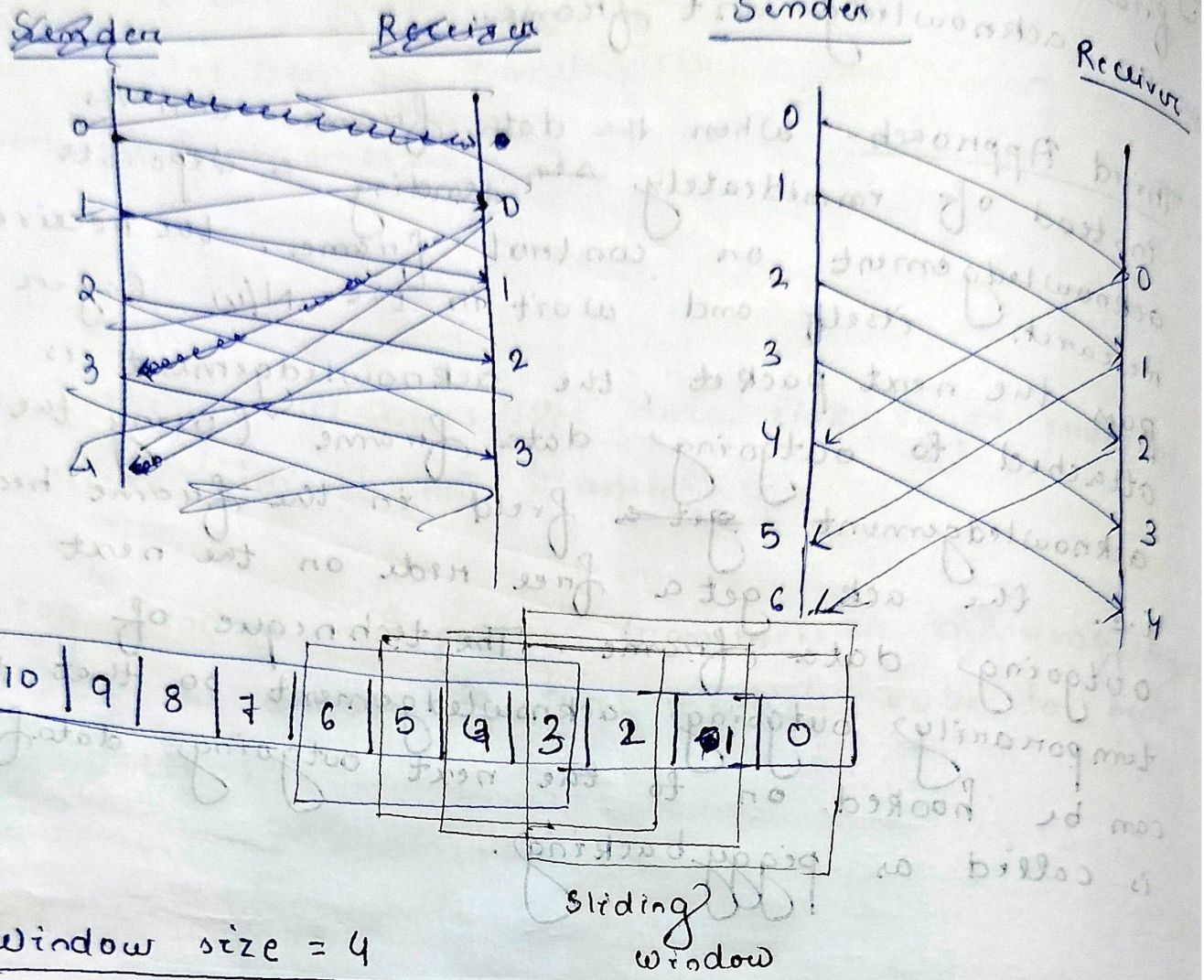
Advantage

1) Better use of available channel bandwidth
2) Less frames are send i.e lighter processing load at the receiver.

Disadvantage

1) How long should a data link layer wait for a packet onto which the acknowledgement is piggybacked. If data link layer bit longer than the sender's time out period, the frame will be re-transmitted, defeating the whole purpose of having acknowledgement. Thus, the solution is the data link layer will be wait for sometime else it will send a separate ACK frame instead of piggybacking.

Sliding Window Protocol



Window size = 4

→ Sends multiple frames at a time.

→ Number of frames to be send is based on window size.

→ Each frame is been provided with the sequence number. (in the header).

→ In sliding window protocol at any instant of time, the sender maintain a set off sequence number corresponding to frames it is permitted to send.

→ Similarly, the receiver also maintain a receiving window corresponding to the set of frames it is

permitted to accept.

0, 1, 2 → Send and received acknowledgement

3, 4, 5, 6 → Send but not received acknowledgement.

7, 8, 9, 10 → not yet send.

GO-BACK-N

→ The sender can send multiple frames before receiving the acknowldegement for the next frame.

→ If the acknowledgement of ~~the~~ the frame not received within an agreed time period or if the receiver send Negative Acknowledgement Frame (NAK), all frames in the current windows are transmitted.

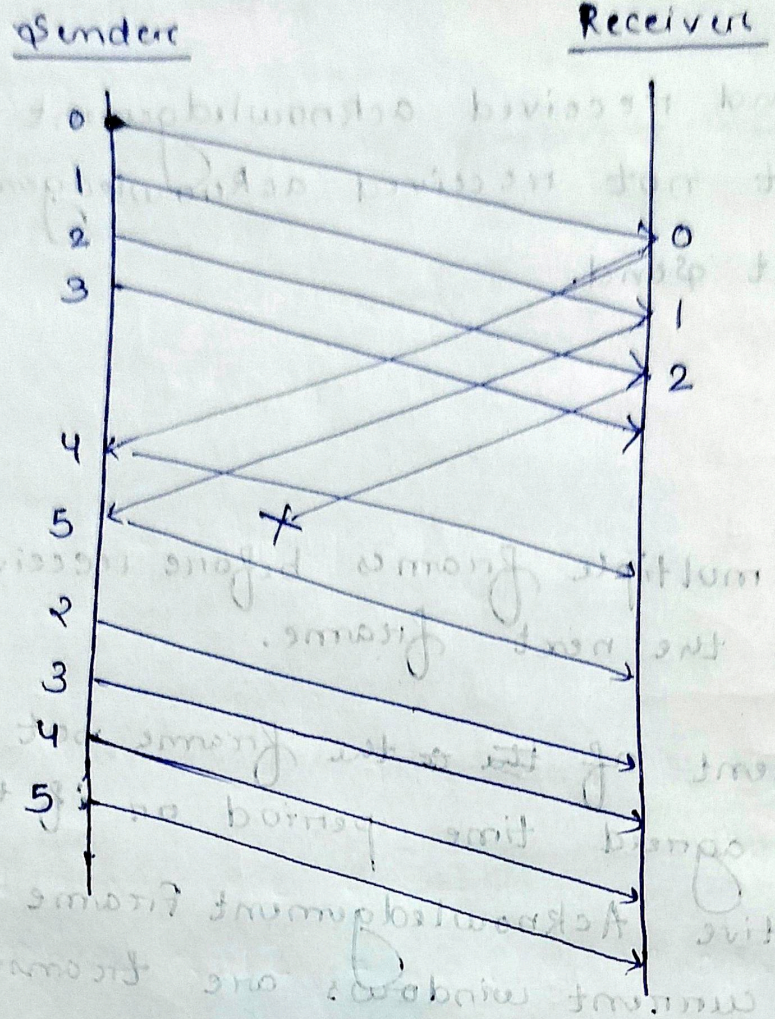
→ The size of the sending window determines the sequence number of the frames. and 'N' specify sender's window size.

~~Sender~~

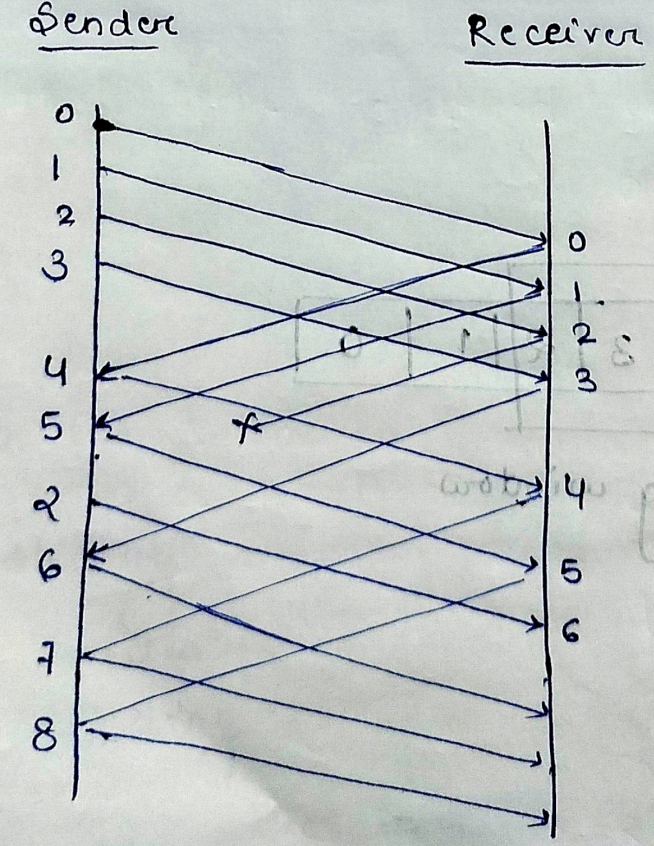
10	9	8	7	6	5	4	3	2	1	0

sliding window

window size = 4



Selective Repeat Protocol



→ GO-BACK-N protocol waste a lot of bandwidth in re-transmitted frame.

→ In Selective Repeat Protocol, only the erroneous or lost frame are re-transmitted while correct frames are received and buffered.

→ The receiver while keeping tracking of regular number buffers the frame in memory and send -ve acknowledgement for the frame which is missing or damaged.

→ The sender will send or re-transmit the frames for which negative acknowledgement is received.

Q A 3000 Km long T1 trunk (transmission line) is used to transmit 64 byte frame using GO-BACK-N protocol. If the propagation speed is 6 μs/Km, how many bits should the sequence number be?

Ans ~~Total time required to send a single frame~~

D.R T1 = 1.54 Mbps = 1.54×10^6 bps

64 byte frame = 64 × 8 = 512 bits

Total time required = 3000 × 6 = 18000 μs
= 18 mS

2 way transmission = 2 × 18 = 36 mS

512 bits → $\frac{64 \times 8}{1.54 \times 10^6}$ = 0.3 msec

Number of frames = $\frac{18 \times 2}{0.3}$ = 120

Q The distance from Earth to a planet is 9×10^{10} m, what is the channel utilization if a stop and wait protocol is used for frame transmission on a 64 Mbps point-to-point link. Assume that the frame size is 32 kilobyte and the speed of the light is 3×10^8 m/s.

Ans ~~Time of~~ propagation delay $= \frac{9 \times 10^{10}}{3 \times 10^8} = 300s$

Round trip transmission ~~delay~~ $= 2 \times 300s = 600s$ (RTT)

Frame size = 32 KB

Data rate $= 64 \times 10^6$ bps

Transmission delay $= \frac{256 \text{ K bits}}{64 \text{ M bits}} = 0.004$ sec

Total time required to transmit next frame

$600 + 0.004$

Q Consider a protocol that uses piggybacking, a sending window size is 4, and 400 bits frame. This protocol is used to transfer data over a 200 Kbps channel with a 4msec one-way propagation delay. Unfortunately, the receiver has no data to send back. It needs to send its acknowledgement in a separate frame. What is maximum

amount of time the receiver can wait before sending such that the bandwidth efficiency does not drop below 50%.

Ans At a time a sender can send $4 \times 400 = 1600$ bits

Data rate = 200 kbps = 200×10^3 bps

$$1b = \frac{1}{200 \times 10^3}$$

For 1600 bits $= \frac{1600}{200 \times 10^3} = 8$ ms.

↓

Transmission time

RTrip Time $= 2 \times 4 = 8$ msec.

Method requires

For the receiver to maintain a bandwidth efficiency of atleast 50%, it should send acknowledgement within the time taken for 1 RTT − Transit time = 0 sec.

i.e. the receiver needs to send acknowledgement immediately or within 0 msec after receiving data to maintain a bandwidth efficiency of atleast 50% or else the efficiency will drop.

Q Consider an error free 64 kbps satellite channel used to send 512 bytes data frame in one direction, with very short acknowledgement coming back the other way. What is the throughput (max) for window size = 1, 7, 15 and 127? The Earth satellite propagation time is 270 milliseconds

Throughput = $\frac{\text{window size} \times \text{Frame size}}{RTT}$

Generally, RTT = Propagation time + Transmission time + Acknowledgement time

Ans Data rate = 64×10^3 bps

for 1 b = $\frac{1}{64 \times 10^3}$

for 512 bytes = $\frac{\cancel{512}^{64} \times \cancel{8}}{\cancel{64}_{\cancel{8}} \times 10^3}$ = 64×10^{-3}

= 64 ms

Transmission time

~~Throughput for~~ RTT = 270 + 64 = 334 ms

Propagation time

Throughput for window 1 = $\frac{1 \times 512 \times 8}{334 \times 10^{-3}}$

= 12.26×10^3 bps

= 12.26 kbps

Throughput for window 7 = $\frac{7 \times 512 \times 8}{334 \times 10^{-3}}$

= 85.4 kbps

Throughput for window 15 = $\frac{15 \times 512 \times 8}{334 \times 10^{-3}}$

= 183.9 kbps

Throughput for window 127 = $\frac{127 \times 512 \times 8}{334 \times 10^{-3}}$

= 1557.02 Kbps

Chapter - 4

The Medium Access Control sublayer

→ A network provides either point-to-point connection or broadcast type of connection.

→ In Broadcast network, the key issue is how to determine who is ~~looking the~~ using the channel when there is competition among themselves.

→ The Broadcast Channel are referred as multi-access channel or Random Access Channel.

→ The protocol i.e used to determine who goes next on a multi-access channel belongs to a sub layer of the data-link layer called as ~~mac~~ MAC sublayer.

Channel Allocation Problem

→ The Central theme of this layer is how to allocate a single broadcast channel among competing user.

① Static Channel Allocation

→ This allocation is used in LAN and MAN.

→ FDM is a simple and efficient allocation mechanism

→ Consider mean time delay = T

→ A frame will be send on a channel whose capacity is capital C.

→ Assume that the frame arrives with a average arrival rate of λ frames/sec

→ The frame varies in length within average length of $\frac{1}{\mu}$ bits

→ The service rate of the channel is equal to μC frames/sec.

According to Queueing theory,

$$T = \frac{1}{\mu C - \lambda}$$

e.g

Let us consider $C = 100$ Mbps.

Mean frame length = 10^4 bits

Frame Arrival Rate = 5000 frames/sec

$T = 200\,\mu s$

100×10^6 bits — 1 sec

10^4 bit = $\frac{1}{10^8} \times 10^4 = 10^{-4}$ sec. = $100\,\mu s$.

→ If we neglect the delay time then in order to transmit 10^4 bits on a 100 Mbps network, we require $100\,\mu s$.

→ This occurs only when there is no confusion/contention for the channel.

→ Let us divide the single channel in a independent subchannel.

→ Each with capacity $\frac{C}{n}$ bits sec.

→ The mean input rate on each of the subchannel will be $\frac{\lambda}{n}$

$$T_N = \frac{1}{\mu\left(\frac{C}{N}\right) - \frac{\lambda}{N}}$$

$$= NT$$

i.e the mean delay for the divided channel is N time worse than if all the frames where magically arranged orderly in a big centralized

② Dynamic Channel Allocation

Assumptions

① **Independent traffic**

→ Once a frame is generated, the station is blocked and does nothing until the frame has been successfully transmitted.

② **Single Channel**

A single channel is available for all communication. All stations can transmit on it and all can receive from it.

③ Observable Collison

If 2 frames are transmitted simultaneously they overlap in time which leads to collison.

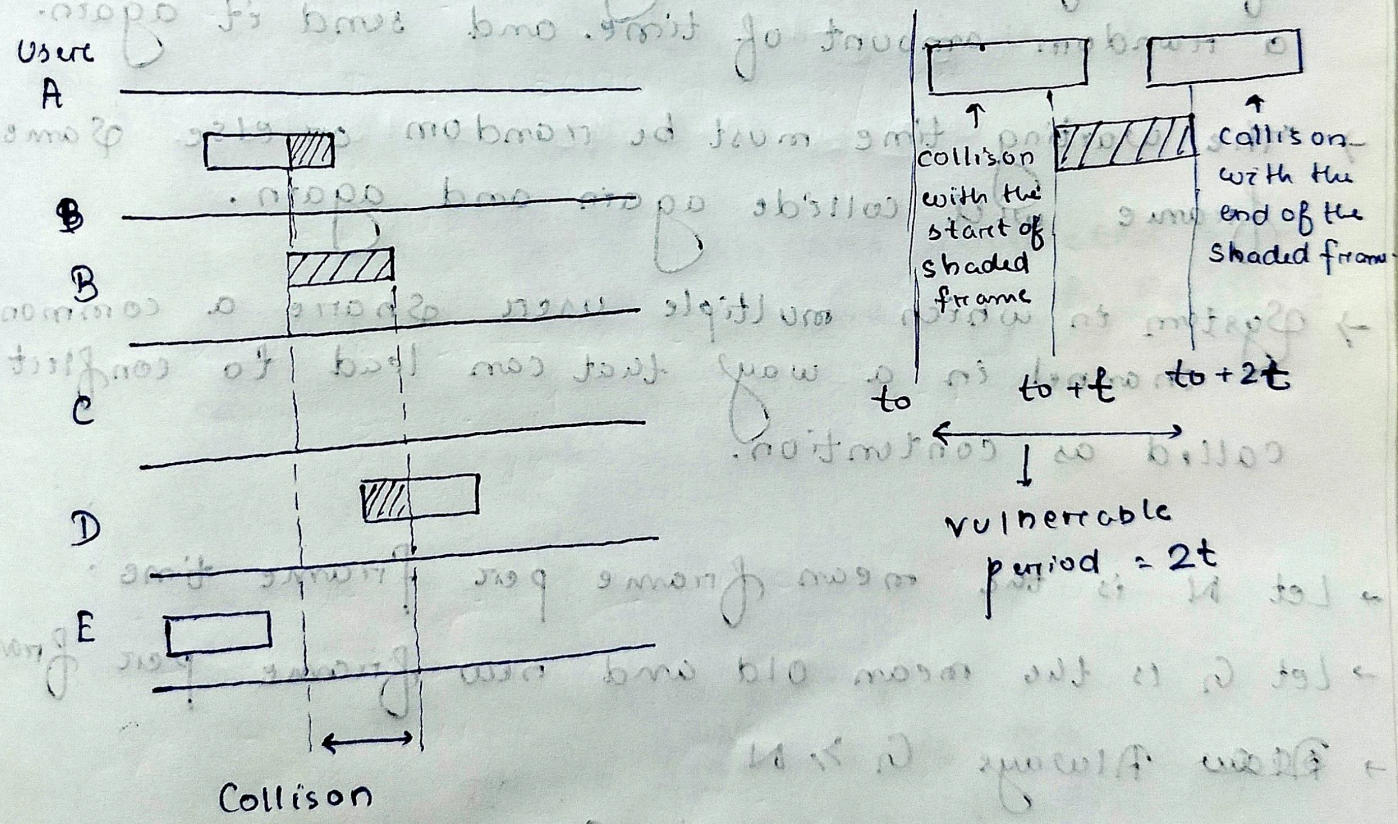
④ Continuous and Slotted Time.

Frame transmission can begin at any instant or time may be slotted or divided into discrete interval.

⑤ Carrier Sense or No carrier sense

Station can tell if the channel is in use before trying to use it or station also may not sense the channel before trying to use it.

ALOHA



ALOHA are of two types

① Pure

② Slotted

Pure ALOHA

→ The user transmit whenever they have data to send. There will be a collison and the colliding frame will be damaged.

→ If listening while transmitting is not possible for some reason then acknowldegment is required.

→ If the frame was destroyed, the sender just wait a random amount of time and send it again.

→ The waiting time must be random or else same frame will collide again and again.

→ System in which multiple user share a common channel in a way that can lead to conflict is called as contention.

→ Let N is the mean frame per frame time.

→ Let G is the mean old and new frame per frame t

→ Always $G \geq N$

→ At low load $N \approx 0$, $G \approx N$.

→ At high load $G > N$

→ Under all loads the throughput (the rate of successful message delivery over a channel)

$S = G P_0$ where P_0 is the probability that a frame doesn't suffer a collison.

$P_r(k) = \frac{G^k e^{-G}}{k!}$

probability of zero frame $P_0 = e^{-G}$

Under what condition the shaded portion arrives undamaged ?

→ let t is the time required to send a frame,

→ If another user sends a frame between t_0 and t_0+t the end of that frame will collide with the beginning of the shaded frame.

→ Similarly, any other frame started ~~with~~ b/w t_0+t and t_0+2t will bump into the end of the shaded portion.

→ The Probability that K-frames are generated ~~given~~ during a given frame time according to Poisson's distribution is

$$\boxed{P_r(K) = \frac{G^K \cdot e^{-G}}{K!}}$$

→ In an interval, 2 frame time long Mean number of frame generated is $2G$.

Thus, the probability of no other traffic ~~been~~ being initiated during the entire vulnerable period is

$$\boxed{P_0 = e^{-2G}}$$

$$\frac{dS}{dG} = 0$$

$$\Rightarrow \frac{d(Ge^{-2G})}{dG} = 0$$

$$\Rightarrow e^{-2G} + (-2Ge^{-2G}) = 0$$

$$\Rightarrow e^{-2G} - 2Ge^{-2G} = 0$$

$$\Rightarrow \cancel{e^{-2G}} = 2G\cancel{e^{-2G}}$$

$$\Rightarrow 1 = 2G$$

$$\Rightarrow G = \frac{1}{2} = 0.5$$

$$S = 0.5 \cdot e^{-2 \times 0.5}$$

$$= 0.5 \cdot e^{-1}$$

$$= \frac{0.5}{e} \approx 0.1845 \approx 18.45\%$$

(*) Vulnerable time = 2G

$P_0 = e^{-2G}$

max $G = \frac{1}{2}$

max $S = \frac{1}{2e} = 0.184$

Slotted Aloha

Vulnerable time = G

$P_0 = e^{-G}$

max $G = 1$

max $S = 0.36$

* Slotted aloha is better than Pure aloha.

→ Here time is divided into discrete interval, each interval corresponds to 1 frame.

→ Here vulnerable time is half of that of Pure ALOH

→ The slotted ALOHA peaks at $G = 1$ with a throughput of $\frac{1}{e} = 0.368$.

→ The best we can hope for using slotted ALOHA is 37% success, 26% collison and 37% slot remains empty.

→ The probability that will avoid collison or provides successful transmission is e^{-G}.

→ Probability of collison = $1 - e^{-G}$

→ Probability of a transmission requiring exactly k attempt i.e (k-1) collison followed by a success.

$$P_K = (1 - e^{-G})^{K-1} \cdot e^{-G}$$

→ The expected no. of transmission per carrier return is equal to

$$E = \sum_{K=1}^{\infty} K P_K = \sum_{K=1}^{\infty} K e^{-G} (1 - e^{-G})^{K-1} = e^{G}$$

Carrier Sense Multiple Access (CSMA)

- 1 persistent
- Non persistent
- p persistent

→ Protocol in which station listen for a carrier and act accordingly are called CSMA protocol.

1 persistent CSMA

→ When a station has data to be send, it first listen to the channel to see if anyone else is transmitting at that moment or not.

→ If the channel is busy the station wait until it becomes idle. When the station detect an idial channel, it transmits a frame.

→ If a collison occurs the station wait a random amount of time and then starts again.

→ The protocol is called as 1 persistent because the station transmit with the probability of 1 when it finds the channel idle.

Non-persistent

→ Before sending a stations sense ~~at~~ the channel, if no one else is sending, the station begin doing itself.

→ If the channel is already in use the station doesnot continuously check rather it waits a random period of ~~time~~ time and then it reach the algorithm.

p-persistent

→ It is basically used in slotted channel.

→ When a stations becomes ready to send it sense the channel. If it is ideal it transmits with the probability p whereas (1-p) probability will be send to the next slot.

→ If that slot is also ideal it either transmit or differ again with the probability of p and q.

CSMA/CD (Collison Detection)

① Transmission

② Contention

③ Idle

Q Each station send 256 byte frame in the ~~128 kbs~~ ~~128 kbs~~ 128 kilo bits per sec shared channel after every 10 seconds compare the max no. of stations supported by pure and slotted ALOHA.

Ans Data : 256 X 8 bits

Time : 10 sec

Data rate = 204.8 bits/sec

Total = N X 204.8

Channel bandwidth = 0.154 X 128 X 10^3

$$N = \frac{0.154 \times 128 \times 10^3}{204.8} \qquad \frac{CB}{B.W}$$

$$= 115$$

Slotted ALOHA

$$N = \frac{0.368 \times 128 \times 10^3}{204.8}$$

$$N = 230$$

Q A large population of ALOHA user manages to generate 50 requests per sec. including both original and re-transmission. Time is slotted in unit of 40 msec.

i) What is the chance of success on the first attempt?

Ans $P_K = e^{-40 \times 10^{-3}} = e^{-G}$

$= 96\%$

ii) What is the probability of exactly K-collison order of throughput.

Ans $P_K = (1 - e^{-G}) \cdot e^{-G}$

iii) Arrange the following protocol in ascending order of their throughput.

a) Slotted ALOHA

b) 1 persistent ALOHA

c) Pure ALOHA

d) .010 persistent CSMA

e) 0.5 persistent CSMA

f) Non-persistent CSMA

g) 0.1 persistent CSMA

Ans c) < a) < b) < e) < g) < d) < f)

Q What is the length of a contention slot in CSMA-CD for a) 2 Km twin lead cable (where signal propagation speed is 82% of the signal propagation speed in vaccuum)

Ans b) A 40 Km multimode fibre optics cable (signal propagation speed is 65% of the signal propagation speed in vacuum. Find the length of the contention slot / contention period.

Ans. a) $\text{speed} = \frac{82 \times 3 \times 10^8}{100} = 246 \times 10^6$

$$\frac{d}{t} = \text{speed}$$

$$\frac{2000}{246 \times 10^6} = t$$

$$= 8.13 \times 10^{-6}\ s = t$$ → propagation delay

Contention slot = 2 × propagation delay

$$= 2 \times 8 \times 10^{-6}\ s$$

$$= 16\ \mu s.$$

b) $\text{speed} = \frac{65}{100} \times 3 \times 10^8$

$$= 195 \times 10^6$$

$$t = \frac{40000}{195 \times 10^6} = \frac{4}{195} \times 10^{-2}$$

$$= 0.0204 \times 10^{-2}\ s$$

Contention slot = 0.0004 s.

CSMA/CD

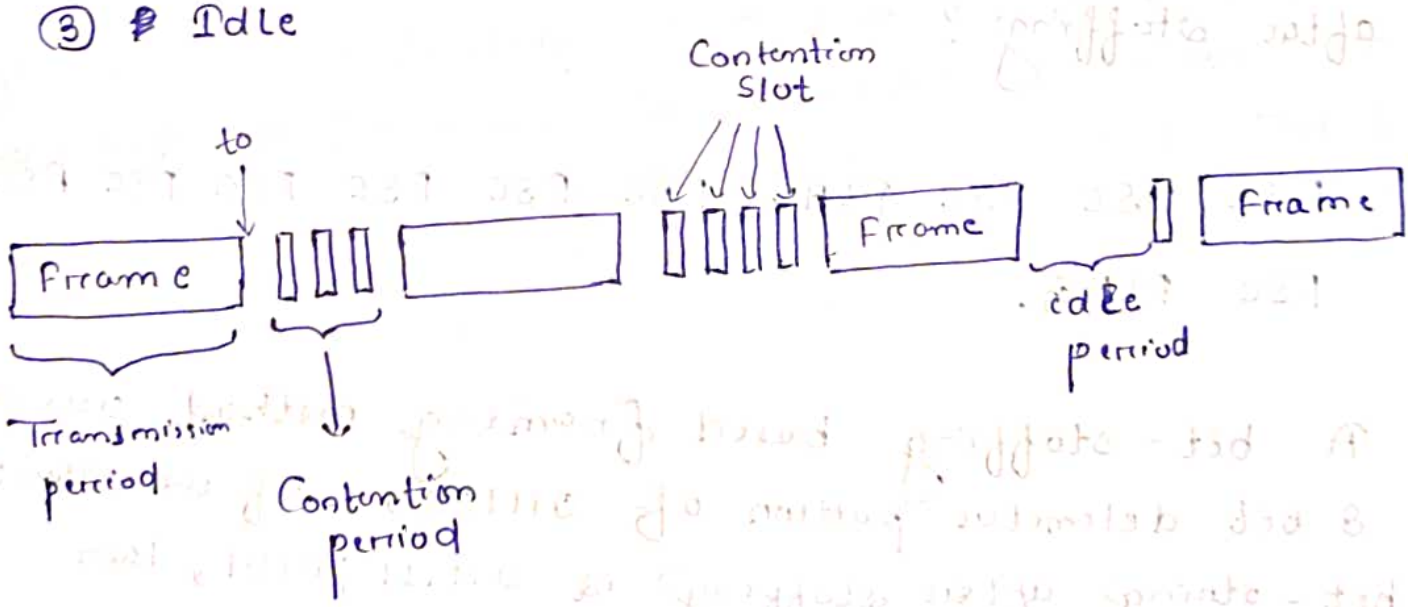
→ If two station sense the channel to be idle and begin transmitting simultaneously, they will both detect the collison immediately.

→ Rather than finish transmitting their frame, which are garbled anyway, they should abruptly stop transmitting as soon as the collison is detected.

→ Quickly terminating the damaged frame, it will save bandwidth and time.

→ This protocol consists of 3 states i.e.

1. Transmission
2. Contention
3. Idle



→ After a station detect a collison, it abode its transmission, wait a random period of time and then try again assuming that no other station has started transmitting in the mean time. Therefore, CSMA/CD consists of alternate contention and transmission period with idle period occuring when all the station are quite.

Assignment - 2

Q.2 The following data fragment occurs in the middle of a data stream for which the byte stuffing algorithm described in the text is used: ESC FLAG ESC ESC ESC FLAG. What is the output after stuffing?

Ans ESC ESC ESC FLAG ESC ESC ESC ESC ESC ESC ESC FLAG.

Q.3 A bit-stuffing based framing method uses an 8-bit delimeter pattern of 01111110. If the output bit-string after stuffing is 011111 ↑ 0101, then find the input-string.

Ans 011111010 1

Q.4 Consider a binary code that consists of only 4 valid codewords as : 00000, 01011, 10101, 11110. Let the minimum Hamming distance of the code be p and the maximum number of erroneous bits that can be corrected by the code be q. Determine the values of p and q?

Ans :- e.g

```
 00000
 11110
 -----
```

how many bits are not same is the hamming distance.

1 & 2 → 3
1 & 3 → 3
1 & 4 → 4
1 & 3 → 4
2 & 4 → 3
3 & 4 → 3

$\boxed{p = 3}$ → min hamming dist
$\boxed{q = 1}$ → hamming code corrects 1 bit

Q.8 Consider a 100Mbps link b/w an earth station (sender) and a satellite (receiver) at an altitude of 2100km. The signal propagates at a speed of 3×10^8 m/s. The time taken (in msec, rounded off to 2 decimal places) for the receiver to completely receive a packet of 1000 bytes transmitted by the sender is ___.

Ethernet (IEEE 802.3)

- Classic
- Switched

Classic Ethernet

→ It solves the multiple access problem using the technique that is CSMA, CSMA/CD, ALOHA.

The devices called switches are used to connect different computers.

→ It's speed is 3 – 10 MBps

→ It follows 1-persistant CSMA/CD.

Switched Ethernet

→ The devices called switches are used to connect different computers.

→ Its speed is 100, 1000, 10000, 40000, 100000

when its speed is 100Mbps – Fast Ethernet

when its speed is 1000Mbps – Gigabit Ethernet

when its speed is 10000Mbps – Gigabit Ethernet

when its speed is 40000Mbps – Gigabit Ethernet

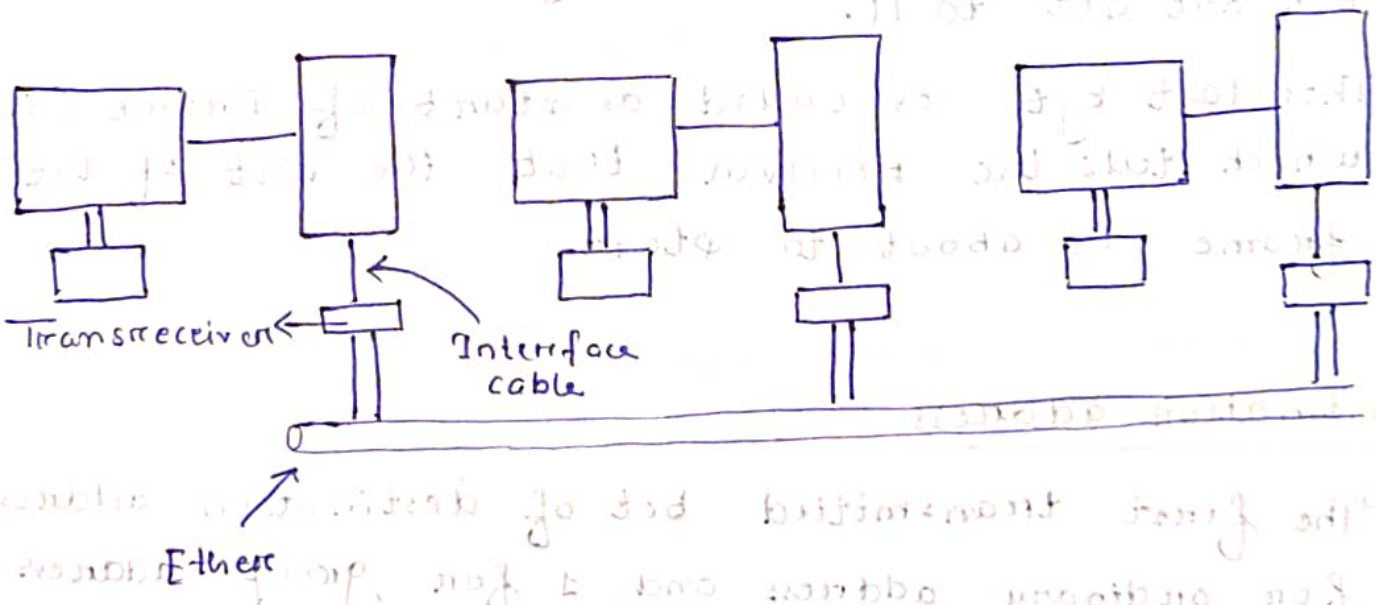
→ Ethernet is called so after the luminiferous Ether through which electromagnetic radiation propagate.

→ Every ethernet has a maximum cable length per segment over which the signal will propagate. To allow larger network, multiple cable can be connected by a device called as <u>Repeater</u>.

→ A Repeater is a physical layer device that receives, amplify and retransmit the signal in both the direction.

→ In case of Ethernet Manchester encoding technique is used.

→ An ethernet could contain multiple cable segment and multiple repeater but no two trans receiver could be more than 2.5 km apart and no path between any two transreceiver could traverse more than 4 repeater.



MAC Protocol

bytes

a)

8	6	6	2	0-1500	0-46	4
Preamble	Destination address	Source address	Type	data	Pad	Check sum

Ethernet

b)

Preamble	S F	Destination address	Source address	length	data	pad	Check sum

IEEE 802.3

Preamble - ~~Each~~ byte ~~containing a bit pattern of~~

→ It contain 8 bytes, each byte containing a bit pattern of 10101010 in case of Ethernet.

→ In case of 802.3 the last byte in which the last 2 bit are set to 11.

→ This last byte is called as start of frame (SOF) which tells the receiver that the rest of the frame is about to start.

Destination address

→ The first transmitted bit of destination address is 0 for ordinary address and 1 for group address. When the frame is send to group address all the station in the group receives it. (Multicasting)

→ The special address containing all the bits as 1 is accepted by all the station on the Network. (Broadcasting)

Source address

→ It is an unique address. The first 3 bytes of the address field are used for an organizational unique identifier which are been assigned unique identifier which are been assigned by IEEE and it indicates a manufacturer.

Manufacturers are assigned blocks of 2^{24} addresses. Each manufacturer assign the last 3 bytes of address and generate a complete address.

Type

→ The type ~~will te~~ field tell the receiver what to do with the frame.

Length

The length field will tell the length of the frame. If any number less than or equal to $\underset{\text{Hex}}{0\times600} = \underset{\text{Decimal}}{1536}$ is interpreted as length and any number greater than 1536 can be interpreted as type.

Data

Maximum 1500 bytes can be transmitted. In addition to there being a maximum frame length, there is also a minimum frame length.

While a data field is byte it causes problem i.e, when collision occurs, the transreceiver trunket the current frame which means that pieces of frame appear on the cable all the time thus in order to distinguish between the valid frame from the garbage, Ethernet requires must be atleast 64 bytes long from

destination address to check sum including both.

→ If the data portion of the frame is less than 46 bytes, the pad field is used to fill out the frame to the minimum size.

Check Sum

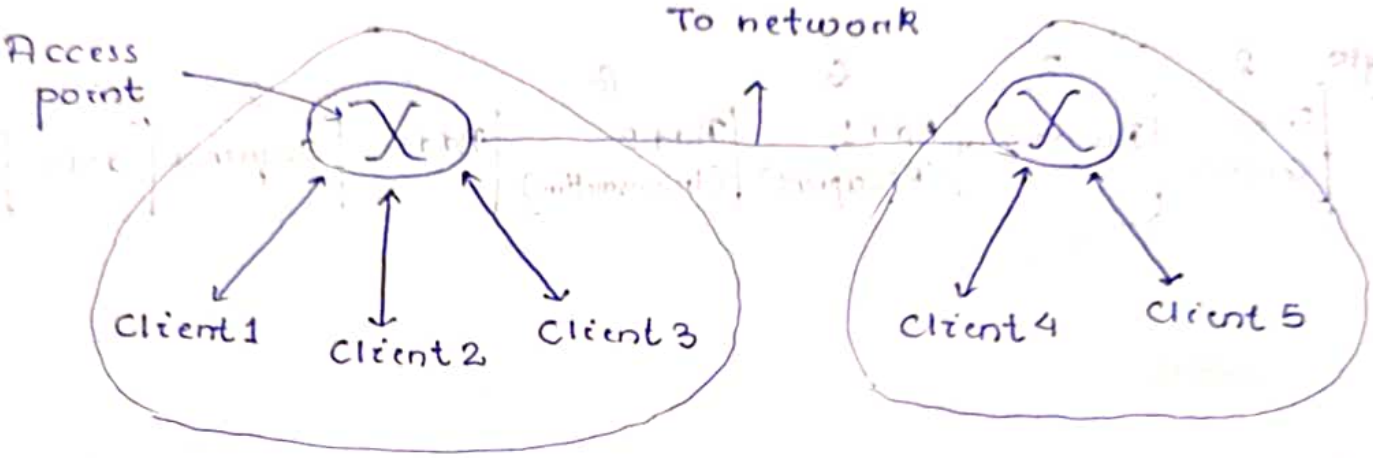
Checksum field provide 32-bit CRC.

* Classic Ethernet follows 1-persistant CSMA/CD i.e the station sense the channel when they have frame to send and send the frame as soon as the medium is idle. They monitor the channel for collison, and if there is a collison they abort the transmission with a small jam signal (of length 48 bits) and re-transmit after a random interval of time.

→ In general, after i collison a random number between 0 to $2^i - 1$ is choosen and that number of slot is skipped i.e after 10 collison the randomization interval is frozen at a maximum of 1023 slot. This algorithm is called as binary exponential backoff.

802.11 (Wireless LAN)

- Infrastructure mode
- Ad-hoc mode

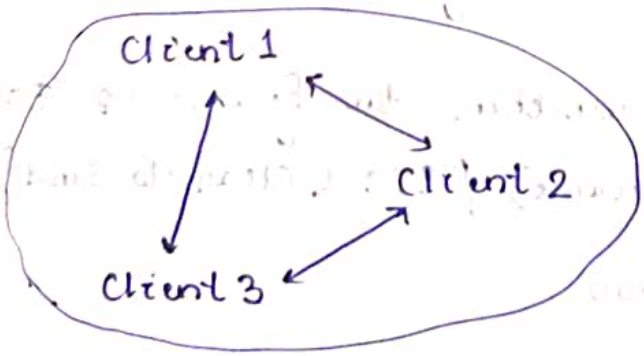


Infrastructure mode

→ In this mode, each client is associated with an Access point (AP) which is inturn connected to other network. The client send and receive its packet via the access point.

Several access point may be connected fogether by a wired network which is called as distributed system.

Ad-hoc mode



This mode is a collection of computer that are associated so that they can send frame to each other directly.

802.11 Frame Structure

Bytes	2	2	6	6	6	2	0-2312	4
	Frame Control	Duration	Add 1 (Recepient)	Add 2 (transmitter)	Add 3	Sequence	data	Check Sum

bits	Version = 00	Type = 10	Subtype = 0000	To DS	From DS	More Fragment	Retry	Power management	More data	Protected	Order
	2	2	4	1	1	1	1	1	1	1	1

→ data frame
→ control frame
→ management frame

Version - by default it is 00.

type - indicate whether frame is data / control / management.
→ if field is 10, type is data frame.

Subtype - Subtype field tells us whether the frame is ACK frame / RTS (Request to Send Frame) / CTS (Clear to Send)

→ For data frame, subtype is 0000.

To DS and From DS

→ These indicates whether the frame is going to or coming from the network connected to the access point.

More Fragment

→ More fragment will follow if 1.
→ No more fragment will follow if 0.

Retry -

It makes a re transmission of a frame sent earlier.

Power management

which means that sender is going into power save mode

More data

indicate that the sender has additional frame for the receiver.

Protected Frame

indicate that the frame body has been encrypted for security.

Order bit

Tells the receiver that the higher layer expect the sequence of frame to arrive in order.

Duration

It tells how long the frame and its ACK will occupy the channel in ns (nanosec).

Add 1 - Address of receiver

Add 2 - Address of Transmitter

Add 3 - Address of Access Point.

Sequence - Sequence no. of frame

Data - Maximum is 2312

Check Sum - 32-bit CRC

Management frame have the same format as data frame + a format for the data portion that ~~varies~~ varies with the subtype.

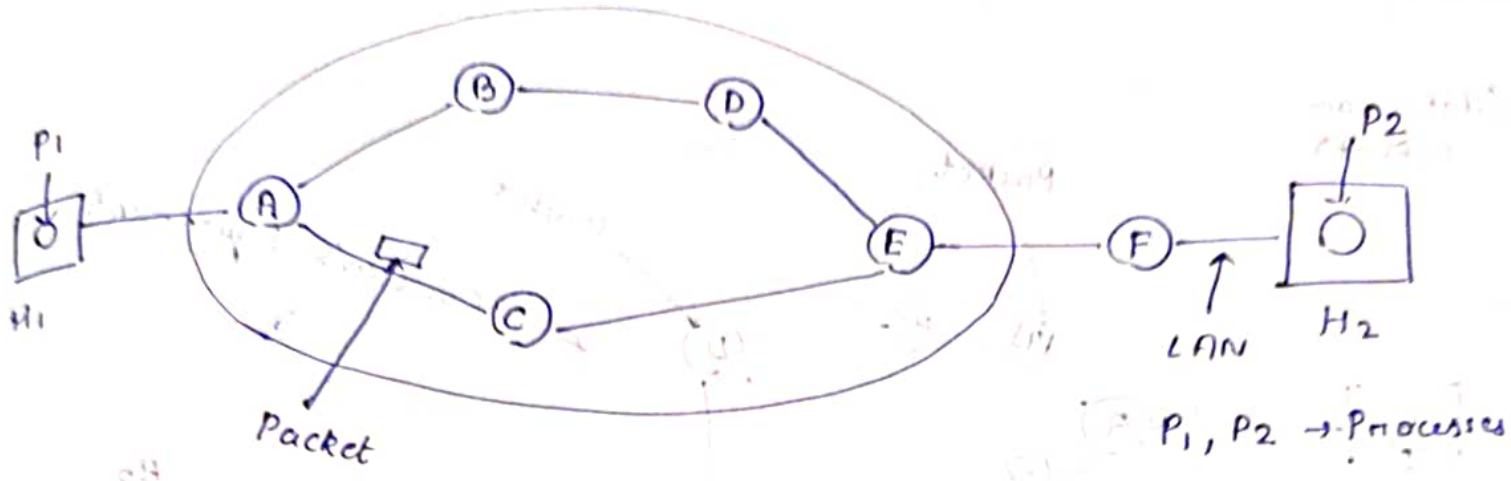
Control frame - They are short frame. Like all frames they have the frame control, duration and frame check sequence field. They may have only one address and no data portion. Most of the key information is present in the subtype field.

Chapter-5
Network Layer

→ The main function of N/w layer to get packets from the source to the destination.

The N/w Layer design issue:

1) Store and forward packet switching



→ The major component of N/w are the ISP's equipment (routers, switches) which are indicated in above circle and the customers equipment that are stored outside the circle. Host H1 is directly connected to anyone of the routers. Similarly Host H_2 is also connected to a router i.e F.

→ A Host send a packet which is stored in the router until it has fully arrived and the link has finished its processing by verifying the checksum. Then it is forwarded to the next router along the path until it reaches the destination host, where it is delivered. This mechanism is called as store and forward packet switching.

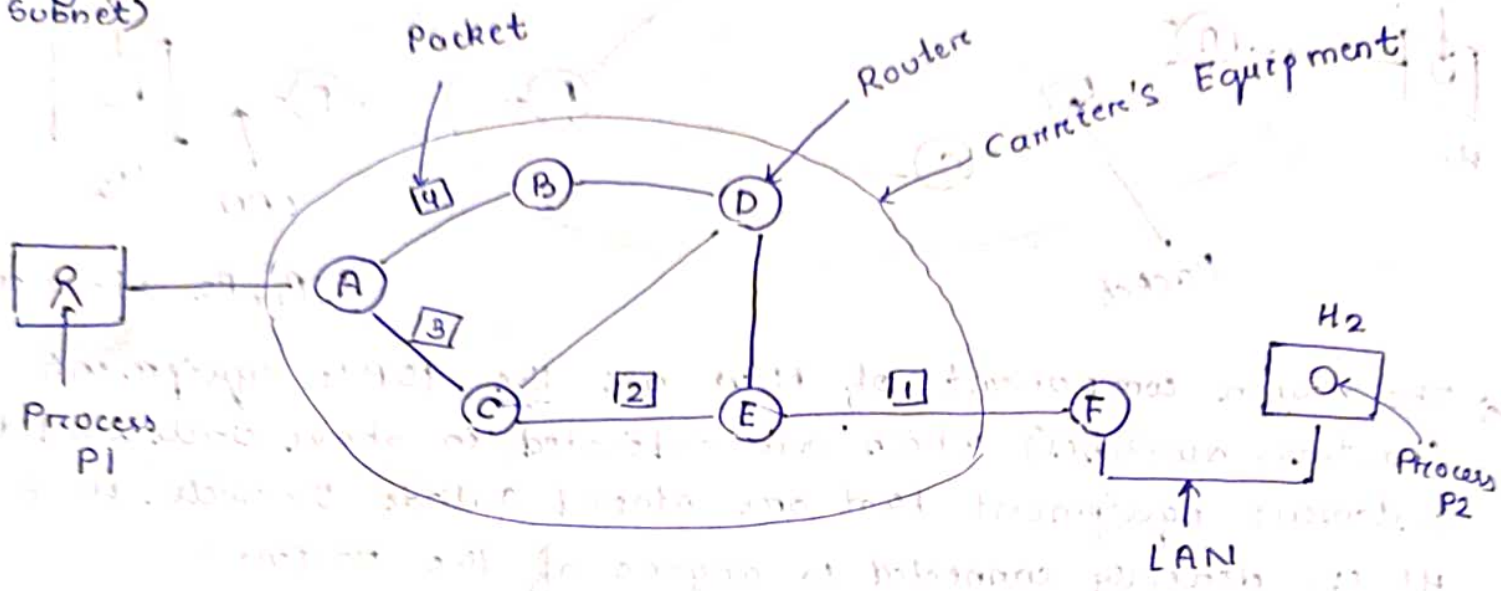
2. <u>Service provided to Transport Layer</u>

The N/w layer provides service to the transport layer at the N/w layer / transport layer interface. The services needs to be carefully designed with the following goal:

1) Service should be independent of router's technology.
2) The transport layer should be shielded from the no., type and topology of the routers present.
3) The N/w addresses made available to the transport layer should use a uniform numbering plan even across LANs and WANs

Implementation of Connectionless Service

(datagram Subnet)



A's table (initially)

Destn	Line
A	–
B	B
C	C
D	B
E	C
F	C

A's table (later)

Destn	Line
A	–
B	B
C	C
D	B
E	C
F	B

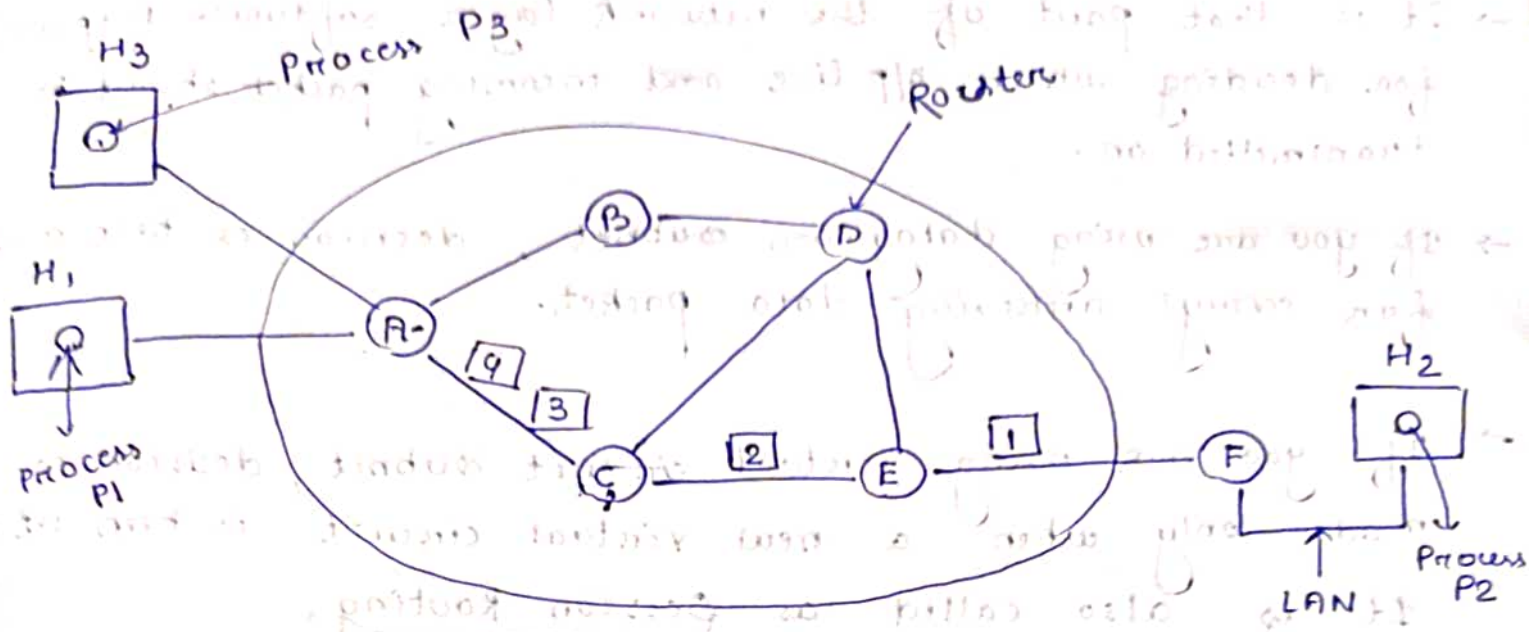
C's table (initially)

A	A
B	A
C	–
D	D
E	E
F	E

D's table

A	B
B	
C	
D	
E	
F	

Implementation of Connection Oriented Service



Such type of connection is called as virtual circuit connection and the subnet is called as virtual circuit subnet.

A's table

H_1	1
H_3	1

in

C	1
C	2

out

C's table

A	1
A	2

in

E	1
E	2

out

E's table

C	1
C	2

in

F	1
F	2

out

Routing Algorithm

→ It is that part of the network layer software responsible for deciding which o/p line and incoming packet should be transmitted on.

→ If you are using datagram subnet, decision is been made for every arriving data packet.

→ If you are using virtual circuit subnet, decision is made only when a new virtual circuit is been set up. It is also called as Session Routing.

The 2 processes are -

→ The 1st process is handle each packets as it arrives, looking up the outgoing line to use for it in the routing table. This process is called as Forwarding.

→ The 2nd process is filling and updating the routing table.

Properties of Routing Algorithm

1. Optimality.
2. Correctness
3. Robustness
4. Simplicity
5. Stability

RA is devided into two types -

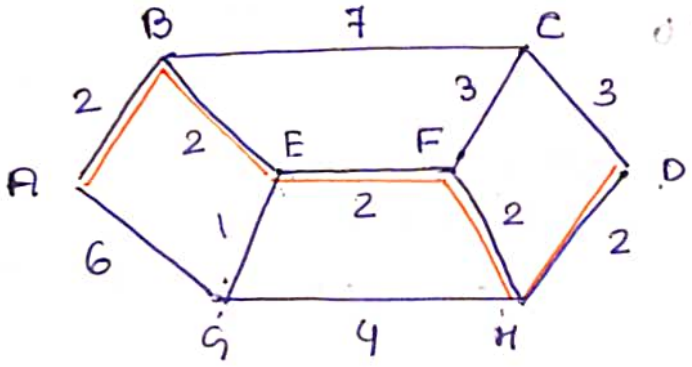
→ Non-adaptive

→ Adaptive

Non-Adaptive :- Do not base their routing decision on measurement or estimate of the current traffic and topology i.e. the choice of the root is computed in advance. This procedure is called as Static Router.

Adaptive - Change their routing decision based on measurement or estimate of the current traffic and topology. This procedure is called as Dynamic Routing.

① Shortest Path Routing Algorithm (Dijkstra)



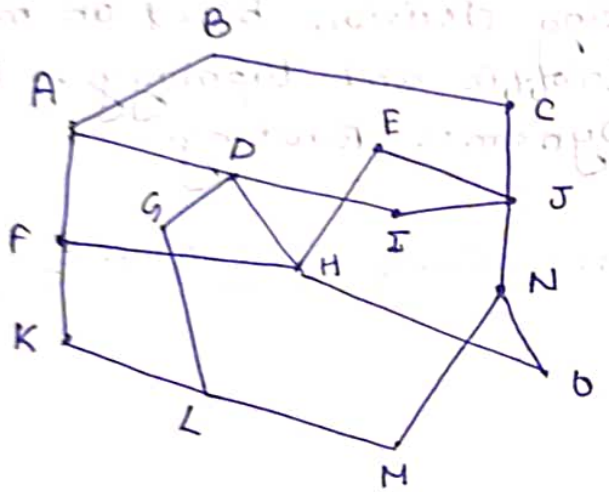
→ One way of measuring shortest path ~~routing~~ length is the no. of hops.

→ Another metric is the geographic distance in km.

→ Another metric is transmission delay and mean queuing

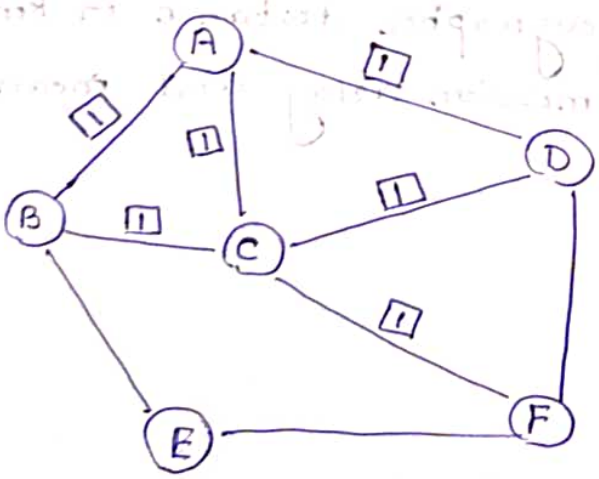
② Optimality Principle

→ This principle provides optimal routes without regards to network topology or traffic.



Flooding Algorithm
(static algorithm)

In which every incoming packet is send out on every outgoing line except the one it arrived on.



→ incoming to A will send B, C, D
→ incoming to B will send C & E
→ incoming to C will send B, D, F
→ incoming to D will send C & F
→ incoming to E will send F
→ incoming to F will send D & E

Limetations of Flooding Algorithm

① It generates vast no. of duplicate packets because of which the network may be blocked.

② It is wasteful if a single destination needs the packet.

③ In order to avoid these limitation, we can have a hop counter i.e present in the header which is decremented at each hop.

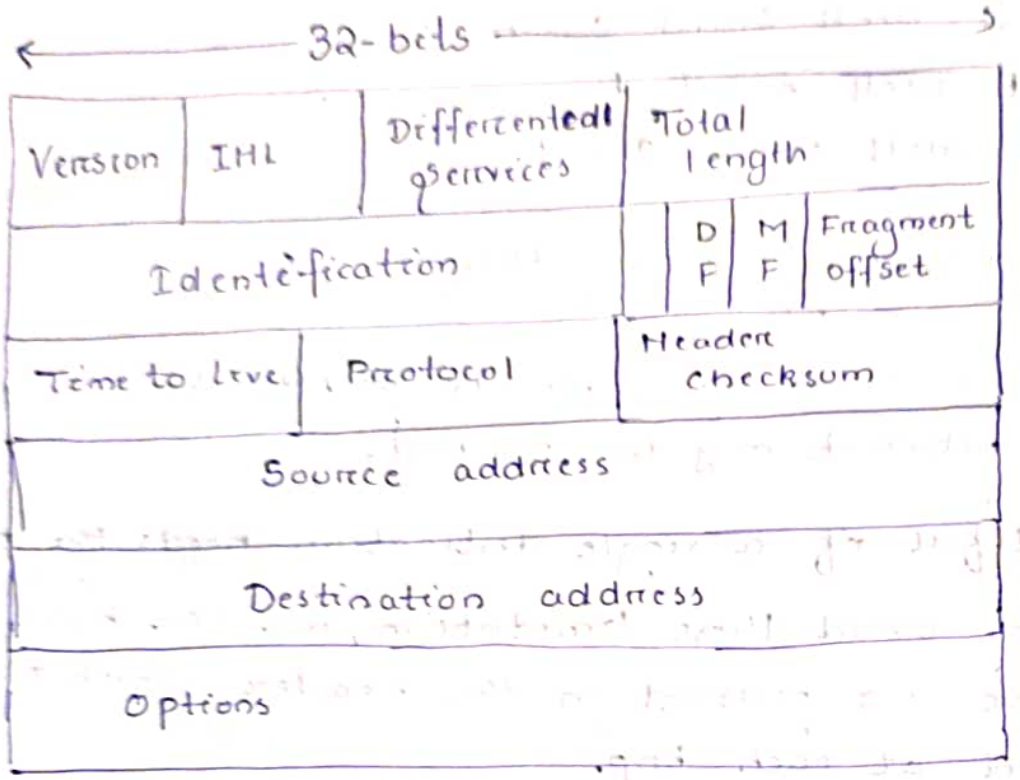
Second measure - To keep a track of the packet which has been flooded. In order to avoid sending them second time.

Application of Flooding Algorithm

① Military Application
② Wireless Networks
③ Destributed database application.

Network Layers in the Internet

IP ⟶ IPV4 / IPV6



Version

- Size - 4 bit
- It tells ~~of the~~ whether its is IPV4 or IPV6.
- Since it is IPV4 content is 0100.

IHL

- Size - 4 bit
- It tells us how many 32 words present in the header.
- Min - 5, Max - 50

Differentiated Services

- Earlier it was being called as Type of Service (TOS)
- Tells the packet with its service class
- Size - 8 bit

Among 8-bits, 1st 6-bits mark the packet with its service and the bottom 2 bits identify the network conjection.

→ Total length

Size - 16 - bits

Min size of IP datagram is 20 bytes and max is 65,535 bytes.

Identification

→ It identifies an IP datagram fragmant uniquely.

→ Size - 16 - bits

→ There are 3 flags each of one bit

→ 1st flag is reserved

→ 2nd flag, when it is set (1), do not fragmant.

→ More fragmant size is 1 bit.

→ ~~Fra~~ Fragment offset size is 13 bits

→ It tells where in the current packet this fragment belongs.

Time to live

→ Size - 8 bits

→ It indicates the max. time the datagram will be live in the internet system.

→ The time to live is measured in seconds.

→ Once the time reached to 0 the data given is lost.

Protocol -

→ It denotes which ~~wh~~ protocol is used in the data portion of datagram.

→ 6 is used for TCP and 17 is used for UDP.

→ length - 8 bit

Header check-sum -

length - 16 bit

Source address

Size - 32 bit

Destination address

Size - 32 bit

Option -

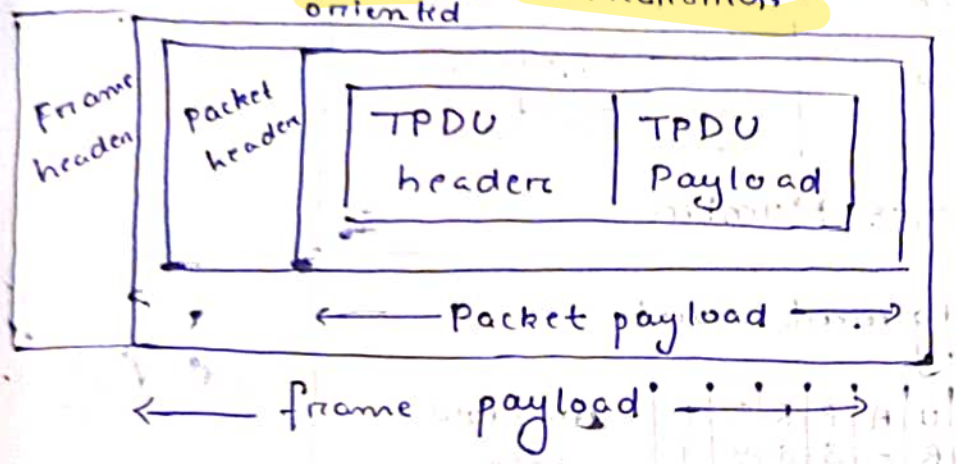
This field is used when the IHL is set more than 5.

Chapter-6
Transport Layer

→ This layer is the first one which breaks the information data supplied by the application layer into smaller units called as segments.

→ It is concerned with the reliability of transport and send data.

→ Protocols : TCP & UDP
(TCP: connection oriented; UDP: connectionless)



Nesting of data from TL to DLL.

UDP header - 8 bytes

← 32 - bits →

Source port	Destination port
UDP length	UDP checksum

→ The two port serves to identify the end point within the source & destination machine

→ When a UDP packet arrives its payload is handed to the process attached to the destination port.

→ Without the port field the transport layer could not know what to do with the packet. With them it

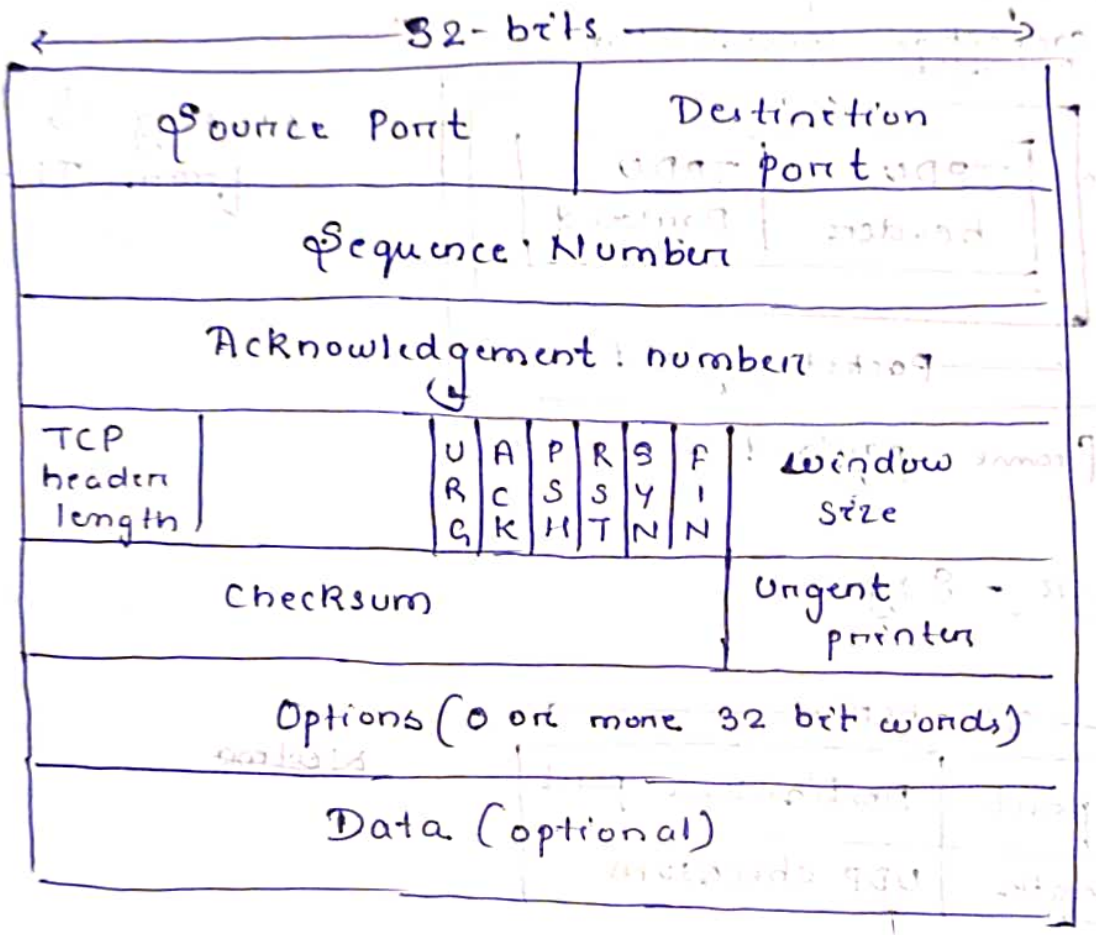
deliver the segment correctly.

UDP Length

→ It includes the 8 byte header and the data.

UDP CheckSum

TCP header



→ TCP was specifically designed to provide a reliable end to end byte stream over an unreliable inter-network.

→ A TCP entity accepts user data stream from local process, break them into pieces not exceeding 64 Kbyte and send each piece as a separate IP datagram.

→ When datagram containing TCP data arrives at a machine they are given to the TCP entity which reconstruct the original byte stream.

→ The IP layer gives no guarantee that the datagram will be delivered properly, so it is upto TCP to time out and retransmit them as needed.

→ It is also upto TCP to reassemble the datagram into messages in a proper sequence.

→ TCP service is obtained by both the sender and receiver creating end points known as sockets.

→ Each socket has a socket number that consists of IP address of the host and a 16-bit number local to that host which is called as port.

→ TCP header length tells us how many 32 bit words are contained in TCP header.

* URG is one, if the urgent pointer is being used.

→ This urgent pointer is used to indicate a byte offset from the current sequence number at which urgent data are to be found.

* ACK is one, to acknowledge ack is valid.
* PSH is one, indicates pushed data.
* RST is one, indicates reset a connection.
* SYN is one, ~~to~~ establish a connection
* FIN is one, release a connection.

* Window size - Tells if we are using a sliding window

Chapter-7

Application Layer

DNS (Domain Name System)

→ The essense of DNS is the invention of a hierarchical, domain-based naming scheme & a distributed database system for implementing this naming scheme.

→ It is primarily used for mapping host names and email destinations to IP addresses but can also be used for other purposes.

→ DNS works as follows-

① To map a name onto an IP address, an application program call a library procedure i.e called as resolver, passing it the name as a parameter.

② The resolver sends an UDP packet to the local DNS server, which then looks up the name and returns the IP address to the resolver, which then return it to the caller.

③ Armed with the IP address the program then establish a TCP connection with the destination or send its UDP packet.

Chapter- 8

Network Security

Fundamental Security Principle

The network security problem is to distinguish 3 essential security property i.e

1. Confidentiality
2. Integrity
3. Availability

Confidentiality - Keep information away from an unauthorized user

Integrity - Ensure that the information which is been received is the actual information

Availability - It deals with preventing system & services from becoming unusable.

Principles (8 principles)

1. Principle of economy of mechanism which is also called as principle of security.

Complex system tends to have more bugs as compared to that of simple system. User may not understand the complex system & use them in a wrong way or insecure way. Hence, simple system are good to use.

② Principle of fail safe default

This principle organise the access to the resources. It is better to make explicit rule about when one can access the resource than trying to identify the condition under which access the resource should be denied.

③ Principle of Complete Mediation

Every access to every resource should be checked for authority.

④ Principle of Least Authority

It is also called as POLA.

It states that any system should have enough authority to perform its task and know more.
(basic details/information about the data)

⑤ Principle of Privilege separation

It is better to split up the system into multiple complete component into simple component with all the privilege combination.

⑥ Principle of Least Common Mechanism

It states that we would minimize the amount of mechanism common to more than one user and dependent on by all user

⑦ Principle of open design

It states that the design should not be secret and generalized.

⑧ Principle of psychological acceptability

The system should be easy and understood.

Fundamental Cryptographic Protocol Principles

1) Redundancy - An encrypted message must contain some redundancy i.e information not needed to understand the message.

- It prevents active intruder from sending garbage and fooling the receiver into decrypting and acting on the plaintext.

2). Freshness - That measures to ensure that each message received can be verified as being fresh i.e sent very recently.

By doing this the active intruder are prevented from playing back old message