①

Computer N/W: number of separate computers inter connected for communication forms a computer network.

(*) It replaces the old model of single computer serving all computational needs of an organization.

(*) N/W comes in different size, shape and forms.

Distributed System: is a S/W System built on top of network.

Uses of Computer networks

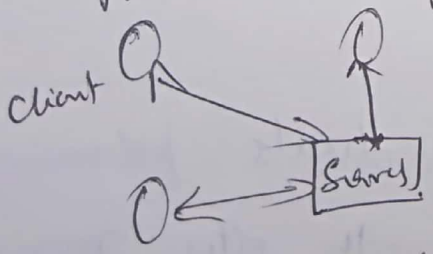
- Business applications
- Home applications
- Mobile users
- Social issues

① **Business Applications**

Client Server

In any organization computer N/W is required for sharing of resource (Resour Sharing) the resource may be ~~prog~~ S/W resource like programs, data (information) (or) H/W resource like printer, CD-drive, Scanner etc.

most of the company needs to share customer data, product information, inventories, financial statement, tax info etc among the employees, it happens through Computer N/W.



② VPN (virtual private Network) may be used to join the individual N/W at different sites

with one extended NW

Communication medium among employees. through E-mail & chatting applications.

IP-telephony / Voice over IP (VoIP): Telephone calls b/n Employees may be carried out by Compute Network

Desktop sharing: Remote workers can see and interact with graphical Computer Screen.

E-Commerce: ① B2C => Order items online

② B2B => Bike manufacturer orders for tires from Supplier

③ G2C => Govt distributing tax forms electronically.

④ C2C => Olx

⑤ P2P => music sharing

Home Applications:

Internet access provides the home users with connectivity to remote computers

Home users can access information, Communicate, by products and services with e-commerce.

E-Books, E-journals. etc

peer-to-peer Comm^n => individuals forming group can Communicate with other group. without central database

Peer to peer can be used to share music & video. Twitter service, instant messaging.

IPTV based on IP technology. instead of Cable TV

Ubiquitous computing computing is embedded into everyday life. i.e Smart homes.

Mobile users: Mobile computers such as laptops and hand held computers connectivity to internet enables the mobile users to use their devices for all the applications like access info, online shopping comm etc. wireless N/W and mobile computing are related but not identical.

Wireless	Mobile	Applications
NO	NO	Desktop in office
NO	yes	Note Books.
yes	NO	N/W in unwired building
yes	yes	Access internet with handheld device

Texting, Smart phone, GPS, m-Commerce,

Network Hardware:

Transmission technology: point-to-point lines (transmission) where the transmission is exactly with one sender and one receiver. also called unicast

Broad-cast transmission: Transmission to all destinations from one sender. Some broadcast systems also support transmission to a subset of machines. This Concept is multicasting.

Classification of N/W based on Distance Scale

interprocessor Distance	processor located in same	
1 m	Square meter	→ personal area N/W
10 m	Room	local area N/W
100 m	Building	local area N/W
1 Km	Campus	local area N/W
10 Km	City	MAN.
100 Km	Country	WAN
1000 Km	Continent	WAN
10,000 Km	planet	→ The Internet

Personal Area N/W (PAN) wireless N/W that connects a Computer with peripherals using Bluetooth Bluetooth N/W use master-slave paradigm

Local Area network (LAN): (a) wireless LAN using 802.11 (b) Switched Ethernet privately owned N/W.

LAN are used connect PC and consumer electronic to share resources like printe and exchange information. When LANs are used by companies they are called Enterprise Network.

Wired LANs runs at 100 Mbps to 1 Gbps. (802.3) Ethernet
Wireless LAN runs at 11 to 100 mbps 802.11

Virtual LAN : The physical LAN can be devided into small logical LANs

MAN (Metropolitan Area Network) : The network that covers city Ex Cable television

WiMAX IEEE 802.16.

WAN (Wide Area network) ~~Spans~~ Covers large geographical area like country or continent. Connects the Computers in the branch offices at different cities. WAN contains Hosts and Subnet, Subnet contains transmission lines and switching elements

transmission lines may be Copper wire, fiber optics or even radio links, generally Companies takes leased lines from telecommunication Company

Switching elements (Routers) : are Specialized computers that connects 2 more transmission lines.

Comparision b/n LAN/WAN

Network Software

Now the Software is the main concern for N/W design.

protocol Hierarchies

To reduce the network design complexity most N/W are organized as stack of layers (or) levels built one above the other.

* The name * Content * function of each layer. is different from N/W to N/W

Each layer provides service to higher layer by hiding how the services are implemented - like information hiding, data abstraction etc

protocol : is the agreement b/n the communicating system on how Comm^n is to happen

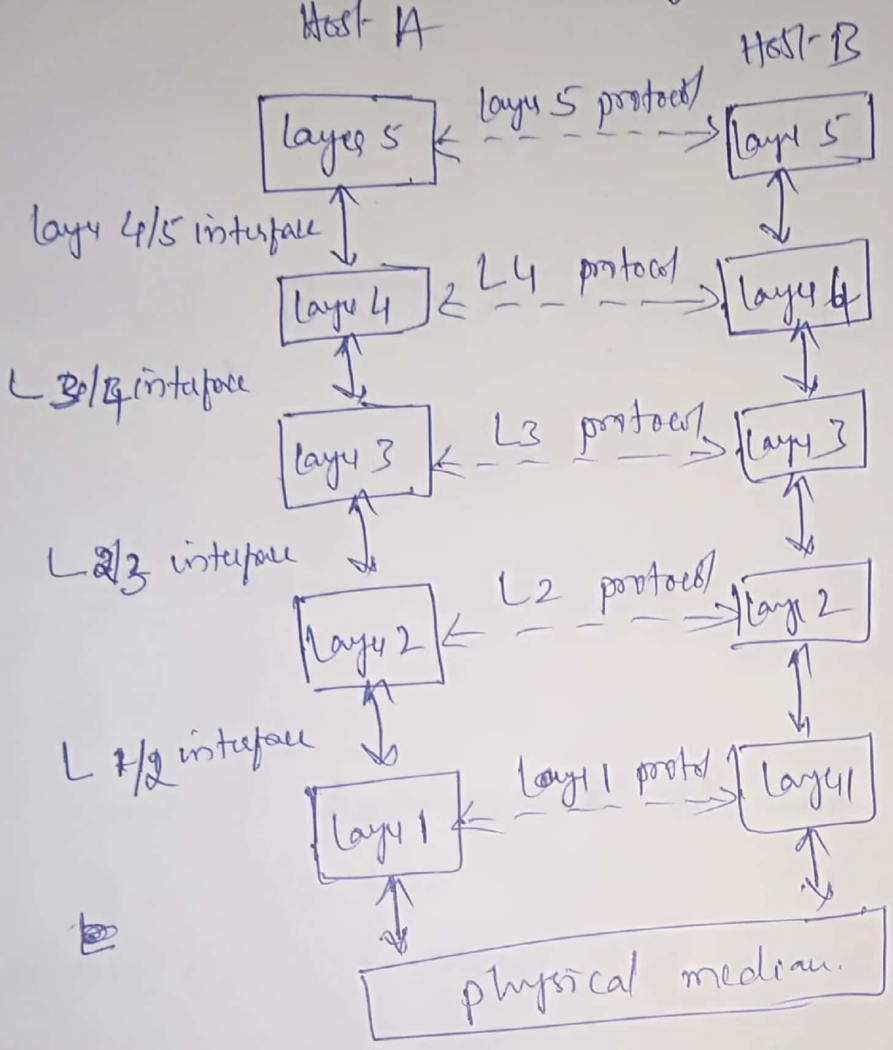
Layer n protocol : The rules and policies used when an n^{th} layer on one machine Communicates with n^{th} layer on the other machine

peers : the entity (may be process, H/W, device) on different machines but at same layer. using protocols for Comm^n

~~on the layer of architecture~~.

N/W Arch A set of layers and protocol. is called network architecture. on reality the data.

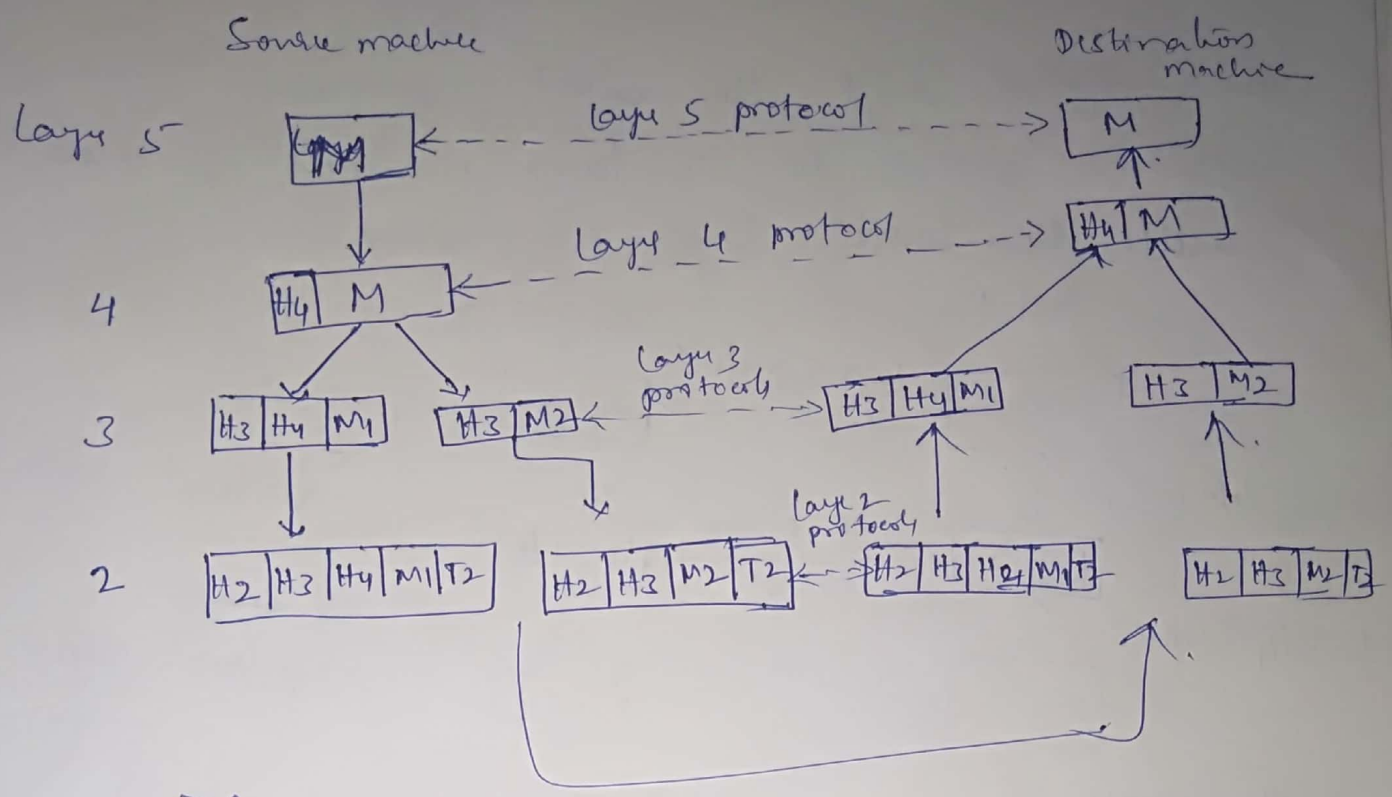
~~no data~~. and the control information flows one layer is passed to the layer immediately below it until the lowest layer is reached



Between each pair of adjacent layers is an interface that defines the primitive operations and services that the ~~lower~~ $n-1^{th}$ layer offers to the n^{th} layer

The list of protocols used by the system, one protocol per layer, is called protocol stack

Network architecture, protocol stack & the protocol are the main concern in computer



information flow from Source machine to Destination machine

M: is the message generated an application program at layer 5 on Source machine and given to layer 4. The layer 4 adds Header in front of message to identify and passes to layer 3.

Header: includes the control information such as address, seq no, size, time to allow the Layer 4 on destination machine to deliver the message.

If the size exceeds, the layer 3 ~~protocol~~ breaks the incomming message into smaller units called packets by prepending layer 3 header to each packet. So Message M is split into M_1 & M_2 that will be transmitted Separately

layer 3 decides which of the outgoing line to use and pass the packets to layer 2. The layer 2 adds each piece not only header but also trailer and gives the resulting unit to layer 1 for physical transmission

At the receiving machine message moves upwards from layer to layer by with ~~address~~ headers being removed at each layer.

Design Issues for the layer.

(1) Reliability : The design issues that makes the network to operate correctly even though it is made up of collection of components that are themself unreliable. so (a) errors detection & retransmissions (or) errors detection & correction.

(2) Routing finding a working paths in the multiple paths b/n source and Destination in a large network.

(2) Evolution of the network. overtime N/w grows larger and new designs emerge that need to be connected to the existing N/w.

Addressing (or) Naming : every layer needs a mechanism for identifying the sender & receiver

that are involved in communication

Internetworking: As the message transmits across the different networks with a differences in the maximum size of the message is that the n/w can transmit. This leads to mechanisms for. disassembling, transmitting and then reassembling messages.

Scalability: The network should continue to work well even when the N/W gets large.

(3) Resource allocation N/W provides services to hosts from their available resources such as. channel Band Width, memory etc. To allocate resources mechanisms are required to divide and allocate the resources so that one host does not interfere with another too much. So multiplexing, is one of the methods

flow Control How to keep fast sender from ~~swamping~~ of swamping a slow receiver.

Congestion Control over loading of N/W

Qos (Quality of Service): real-time delivery, high throughput

(4) Security: Confidentiality, Authentication & integrity.

Connection oriented / connection less. service

Service primitives: The service primitive tell the service to perform some action. The set of primitive depends on the nature of service provided.

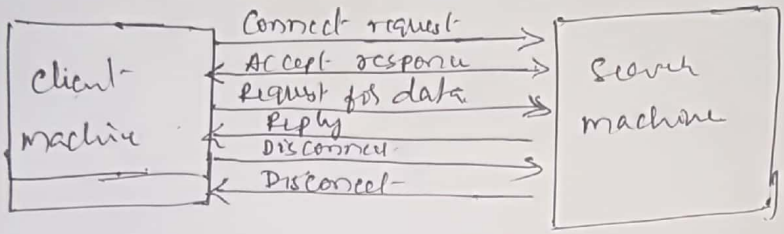
The primitive for connection-oriented services are

1	LISTEN	Block waiting for an incoming Connection
2	CONNECT	Establish connection
3	ACCEPT	Accept the incoming connection
4	RECEIVE	Block waiting for an incoming message
5	SEND	Send a message
6	DISCONNECT	Terminate connection

A protocol is the set of rules governing the format and meaning of the packet/message to be exchanged b/n machines

Service is the set of operations that a layer provides to the layer above it.

Service primitives for client server interaction



Reference model: The N/W architectures used as reference to design N/W are OSI Reference model and TCP/IP model.

The OSI Reference model

* It is based on the proposal developed by International Standards Organization (ISO) to standardize the protocols used in various layer.
* This model is ISO OSI (Open System Interconnection) model as it deals with all the systems open for communication. with other systems.

* OSI model divides the task of moving information b/n networked computers into 7 layers
* ISO OSI has 7 layers. The principles that were applied to arrive at the seven layers.

a) a layer should be created where different abstraction is needed

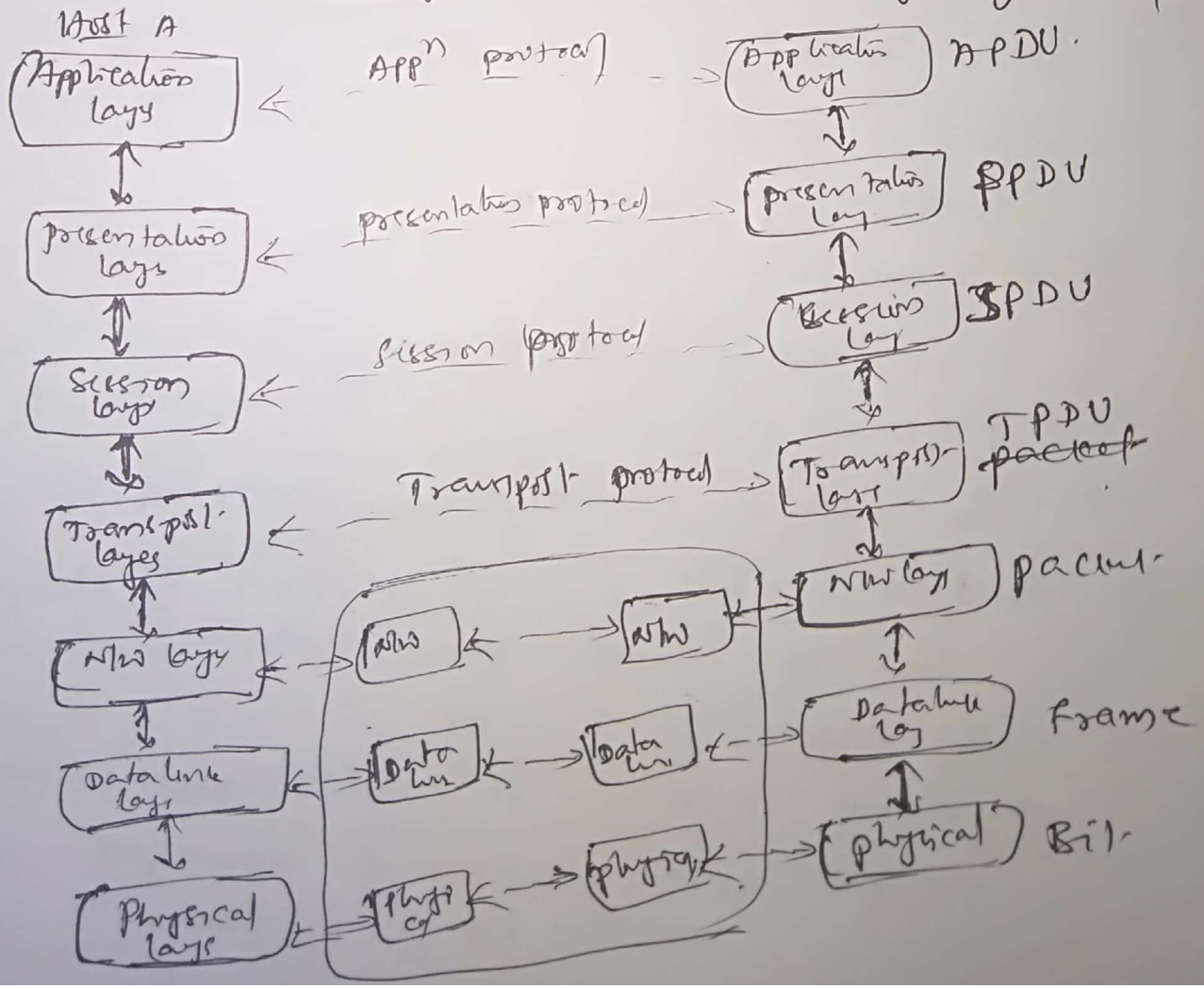
b) Each layer should perform a well defined function

c) ~~Each~~ The function of each layer should ~~be~~ match with internationally standardized protocols

d) Information flow ~~acer~~ across (b/n layers) the interface should be minimum.

e) The number of layers should be large ~~eag~~ enough so that the functions in each layer should not be overloaded and should be optimum

OSI model 7 layers is an imaginary model



Physical layer : ⊛ Concerned with transmitting raw bits over comm^{n} channel.

⊛ It deals with mechanical electrical specifications of the interface and transmission medium.

⊛ Representation of bits : How the bits must be encoded to signal (electrical / optical) and also defines type of encoding i.e how 0 & 1 are changed to signal (NRZ - Manchester etc)

⊛ Data Rate : No. of bits transmitted per second is defined by physical layer.

⊛ physical topology : defines how devices are connected to make a network (star, Bus etc)

⊛ Transmission modes : defines the direction of transmission btw devices (Simplex, half duplex, full duplex)

Data link layer : It makes the physical layer to appear error-free to the upper layer. (NW layer)

function of DLL are

* framing : divides the stream of bits received from NW layer into manageable data units called frames
* physical addressing : Adds the header to the frame to define sender and receiver of the frame
* flow control : If the receiver is slower than sender then it imposes flow control mechanism to avoid overloading of receiver
* Error control : It adds mechanisms to detect- detect and retransmit damaged ~~bits~~ (or) lost frames, it also have mechanism to avoid duplicate
⊛ Access control : When more than device are

are connected to same link, DLL protocols determine which device has control over link.

Network layer: It is responsible for source-to-destination delivery of packets across multiple network links. If two systems are connected to different N/W with connecting devices b/n n/w then there is a need for N/W layer. The functions of N/W layer

* Logical Addressing: If packet need to cross the network boundary it needs addressing system to distinguish the source & destination (IP address)
* Routing: Selecting the best route across the network from source to destination

Transport layer: Responsible for process to process delivery of entire message.

* Service point Addressing: It adds service point address (port address) to deliver the message from a specific process on sender computer to specific process on destination computer as more than one process can run on the same system
* Segmentation & Reassembly: Message is divided into transmittable segments with each segment having sequence number. to help in re-assembly at destination
* Connection control: It can be either connection oriented or connection less (TCP/UDP)

(*) Flow control : flow control is for end-to-end rather than single link

(*) Error control performed for process to process rather than single link

Session Layer : The session layer is the network dialog controller. It establishes, maintains and synchronizes the ~~network dialog control~~ the interaction among communicating systems.

(*) Dialog control : Allows two systems to enter into dialog

(*) Synchronization : The session layer allows a process to add check points checkpoints / synchronization points to a stream of data.

Presentation layer : This layer is concerned with the syntax and semantics of the information exchanged b/w two systems.

(*) ~~Translation~~

(*) Translation : As the different computers use different binary encoding systems, the presentation layer is responsible for interoperability b/w these different encoding methods.

At sender : changes information from sender dependent formal to common formal

At receiver changes from common formal to receiver dependent formal

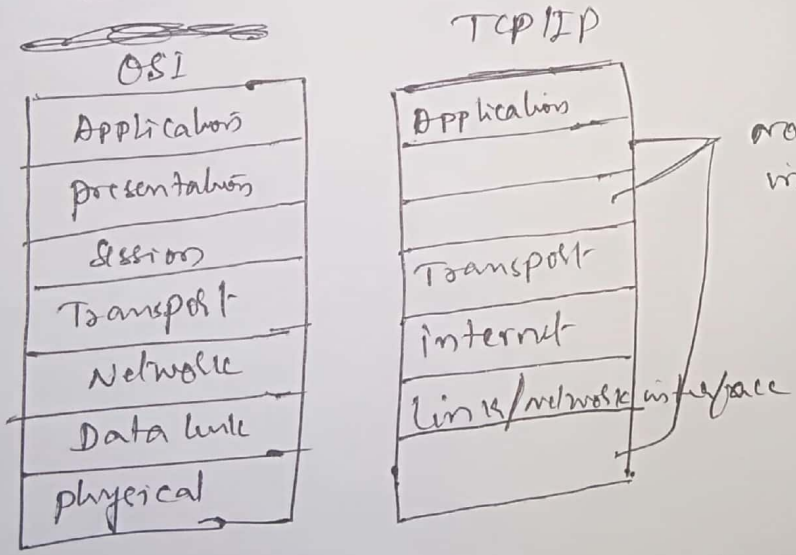
(*) Encryption : Encryption and decryption for secured transmission of data.

(*) Compression : Data compression is important in the transmission of multimedia such as text, audio and video.

(*) Application layer. : It enables the user (or) human to access the network. It provides the user interfaces and support for services such as Email, Remote access file transfer. etc

* File transfer, access & management
* Mail service

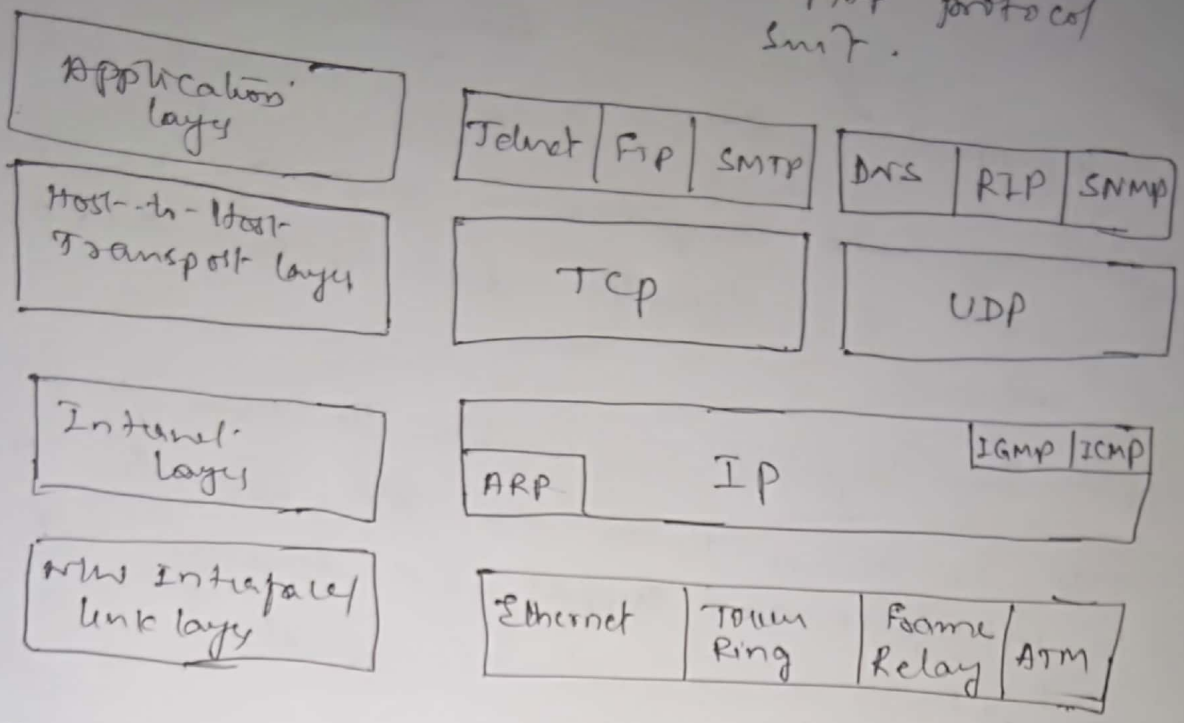
TCP/IP Reference model



Link layer: It is the combination of physical & Data link layer. It is responsible for placing TCP/IP packets on the network medium & receiving TCP/IP packets from the network medium. It includes LAN technologies like Ethernet, Token ring, WAN technologies like Frame relay, ATM, X.25,

TCPIP

TCP/IP protocol suit.



FTP

SMTP

DNS

RIP

SNMP

TCP

UDP

ARP

IGMP

ICMP

Internet layer (*) Responsible for transfer of information across multiple NW through use of gateway & routers

(*) It deals with routing of packets with congestion control

(*) It uniquely address the machines that are attached to internet

(*) Internet layer provides connectionless packet transfer. IP packets are routed independently may on different path. IP packets are also called ~~data~~ Datagrams

The core protocols of Internet layer.

IP (Internet protocol) Responsible for IP addressing, fragmentation & Reassembling of packets.

ARP (Address resolution protocol): ~~Responsible~~ Associates the logical address with physical address (MAC). ARP is used to find physical address of node when its internet address is known.

RARP (Reverse) allows to discover its internet address (IP address) when the host physical address is known

ICMP (Internet control message protocol): It is a mechanism used by host and gateways to send notifications of datagram problems back to the sender.

IGMP (Internet Group message protocol) is used to facilitate the simultanious transmission of messages to a group of recipients

Transport layer: provides session & Datagram Comm^n service to application layer.

Data conversion (ASCII ⟺ EBCDIC etc), encryption/decryption and session layer functions are performed in ~~Application~~ ~~Transport~~ layer of TCP/IP. It is a host-to-host protocol

The core protocols are

TCP : provides one-to-one, connection-oriented, reliable comm^n service, responsible for establishment of TCP connection, sequencing, acknowledging and recovery of packet lost during transmission

UDP provides a one-to-one or one-to-many connection less unreliable comm^n service

Application layer : It refers to the programs that initiate communication in first place.

~~The~~ TCP/IP application layer protocols are

HTTP is used to transfer files that make up the web-pages of the WWW.

FTP : is used for interactive file transfer

SMTP : used to transfer of mail messages and attachements

Telnet : Terminal emulating protocol used for remote login to host.

DNS : used to resolve host-name to an IP address

SNMP (Simple network Management protocol) used by network management consoles and n/w devices (routers, bridges, and intelligent hubs) to collect and exchange network management information.

OSI	TCP/IP
(1) 7 layers.	(1) 4 layers.
(2) Uses strict layering resulting in vertical layers	(2) uses loose laying resulting in horizontal / hierarchical layering
(3) Supports both connectionless & connection-oriented comm^{n} in the n/w layer, but only connection - oriented comm^{n} in transport layer	(3) Supports only connectionless in n/w layer but both in Transport layer.
(4) It distinguishes b/n service Interface and protocol	(4) Does not clearly distinguish b/n service interface & protocol.
(5) protocols are better hidden and can be replaced relatively easily as technology changes	(5) protocols are not hidden and cannot be replaced easily
(6) OSI model was devised before the corresponding protocols were designed	(6) The protocols came first and the model was a description of the existing model.

Examples of Networks

(1) The Internet (2) ARPANET (Advance Research projects Agency) in 1967 (3) NSFNET (National Scientific foundation)

International Standard world

ISO A voluntary organization founded in 1946

Members are ANSI (US), BSI (G Britain), France, Germany and other 153 countries

ISO issues standards on vast number of subjects ranging from nuts & Bolts to Computer Nw.

NIST (national Institute of standards and Technology) is a part of the U.S Dept. of Commerce. also called national Bureau of Standards (NBS) it issues ~~stds~~ standards mandatory for purchases made by US Govt.

IEEE (Institute of Electrical and Electronics Engineers) develops standards in the area of electrical engineering and Computing. It is the largest professional organization in the world.

IEEE's 802 committee has ~~stds~~ standardized many kinds of LAN.

Internet Standard World

① IAB (Internet Architecture Board)

IAB was reorganized in ~~1983~~ 1989 as

② IRTF (Internet Research Task Force) which concentrates on long term research.

③ IETF (Internet Engineering Task Force) to deal with short-term engineering issues

W3C (World Wide Web Consortium) develops protocols and guide lines to facilitate the long term growth of the web

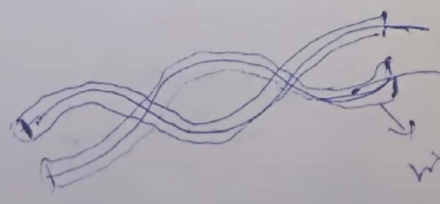
802.3 ethernet, 802.4 ⇒ token Bus 802.5 ⇒ token Ring
802.10 ⇒ virtual LANs and security 802.11 ⇒ WiFi, 802.15 ⇒ Bluetooth, 20 bee (PAN) 802.16 ⇒ WiMAX

Guided Media:

① **Magnetic media:** One of the common ways to transport data from one computer to other using Magnetic tape disk, CD, DVD etc

② **Twisted pair:** 2 insullated copper wires about 1mm thickness twisted in helical form just like DNA. Twisting of wires cancels the waves from different wires (twist)

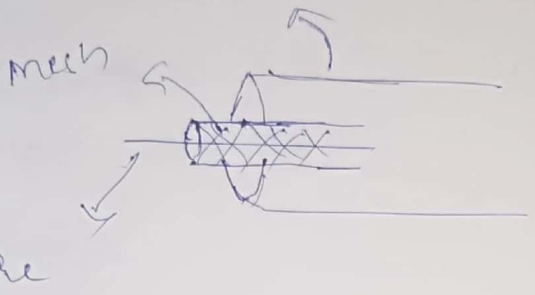
- Twist provides better immunity to external noise
- Signals is carried as the difference in voltage b/w the 2 wires
- used for transmitting either analog or Digital informations.
- Band width depends on the thickness of the wire and distance travelled.
- Used in telephone and Computer networks.
- Twisted pair comes in several types
- Cat-5 contains more twist per metre than cat-3
- more twist results in less cross talk & better Quality signal over long distance supports upto 1Gbps Ethernet LAN. (Cat-3 ⇒ 100Mbps)
- Cat-6 & Cat-7 can support upto 10Gbps



Co-axial Cable: Better shielding and greater bandwidth than UTP can span for longer distance at higher speed

Two types of Co-ax → 50Ω Base band cable used for digital transmission

→ 75Ω Broad Band Cable insulation: for analog transmission TV cable



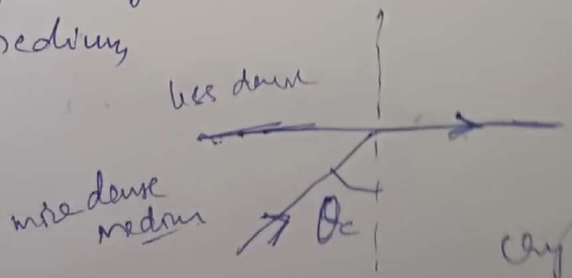
Fiber optics: used for long distance transmission in network backbone for high speed LAN

There 3 components light source transmission medium and a detector. presence of light ⇒ 1
absence of —o— ⇒ 0

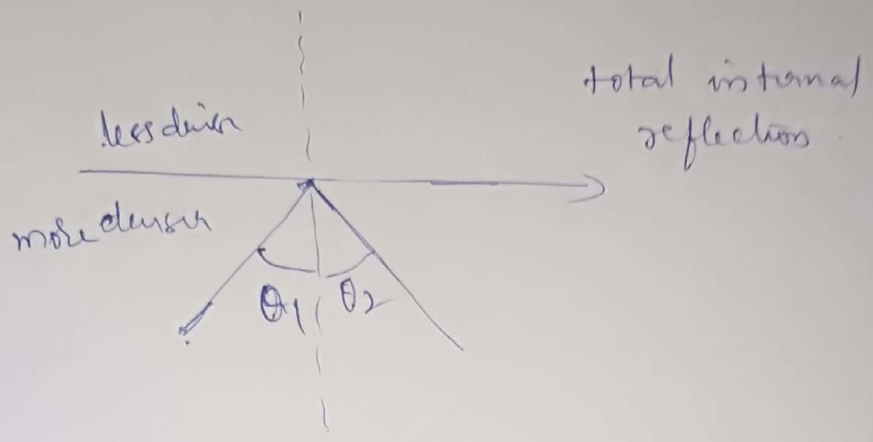
Light source ⇒ Electrical signal to light

detector ⇒ light signal to electrical

Critical Angle: The critical angle is the angle of incidence where the angle of refraction is 90°. The light must travel from an optically more dense medium to an optically less dense medium



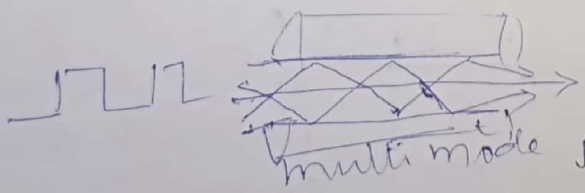
When the angle of incidence becomes greater than the critical angle the ray of light is not refracted but instead completly reflect back with the denser medium and is known as total internal reflection



When the light rays pass from one medium to another the amount of refraction depends on the property of the two media.

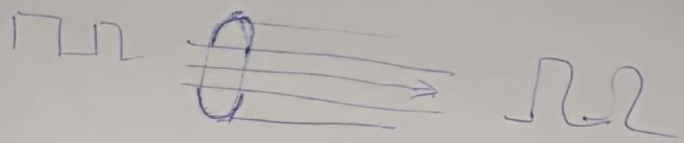
Because total internal reflection the light can propogate for many km

Multimode fiber : many different rays will be bouncing around different angles. Each ray is said to have a different mode, so fibers having this property is called a multi mode fiber.



Single mode fiber : The light can propogate only in a straight line without bouncing. Single mode fiber are more expensive

and can transmit 100 Gbps for 100 km without amplification



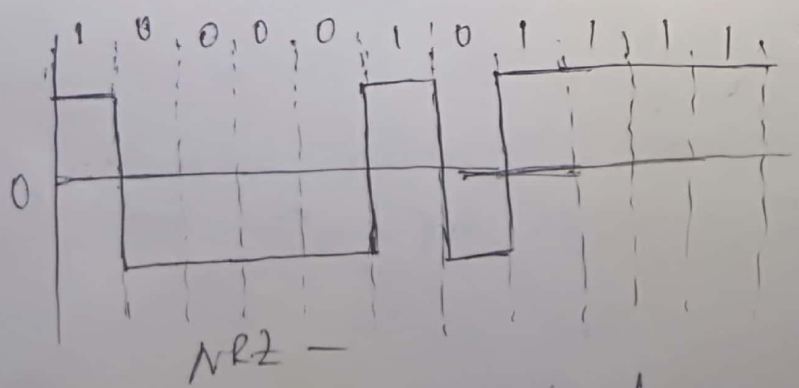
Digital modulation. The process of converting between bits and signals that represent them is called Digital modulation.

The methods that directly converts bits into a signal are called Baseband transmission or common for wires.

The methods that regulate the amplitude, phase (or) the frequency of a carrier signal to convey bits results in pass Band Transmission (Band & frequencies). It is common in wireless and optical channels.

Baseband Transmission

NRZ (Non-Return-to-Zero) +ve voltage to represent 1 and -ve voltage to represent 0



(*) NRZ may cycle between the +ve & -ve levels upto every 2 bits (in case of alternate 1 & 0) So NRZ requires more bandwidth which is limited resource

(*) Long run of 0's & 1's leaves the signals unchanged (*) poor Band width efficiency.

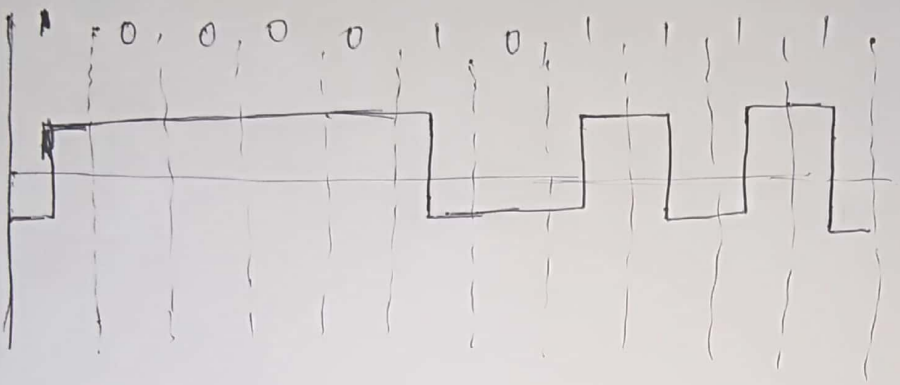
which makes difficult to decode correctly at the receiver end.

NRZ-I (Non-Return-to-Zero Inverted):

Coding 1 as transition and a 0 as no transition

(or) vice versa. It is a twist on NRZ

(*) USB (Universal Serial Bus) uses NRZI.



(*) In NRZ-I still the long runs of 0 causes a problem.

Manchester Encoding:

(*) ~~Synchronous clock encoding system. Here 0's is represented by a negative to +ve transition and 1 is represented~~

(*) Synchronous clock encoding System

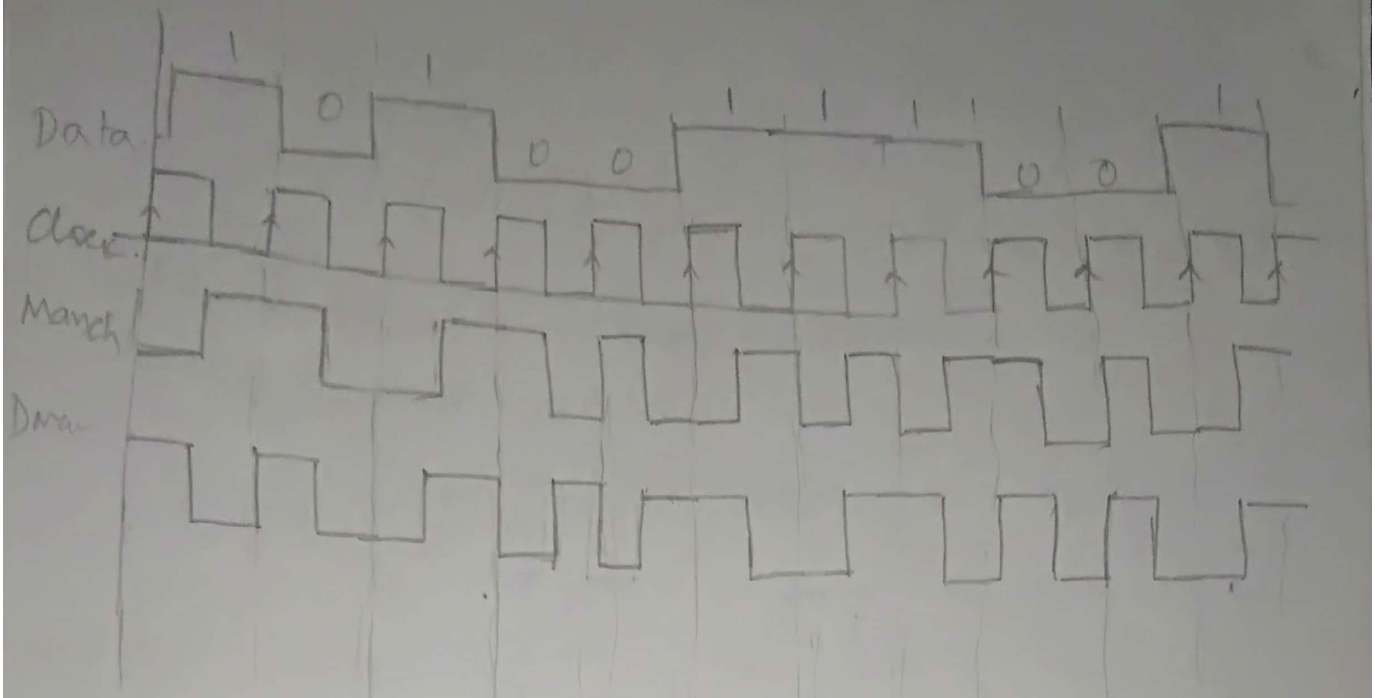
(*) Transition from low to high (⌐) represents logic 1

(*) Transition from High to low (¬) represents logic 0

Advantage the signal synchronizes itself; minimizes the error rate and optimizes reliability

~~Disadvantage is~~

In manches coding the clock signal is XOR-ed with the data signal to get the modulated signal as shown below.



Differential Manchester - Encoding.

(*) There always occurs a transition in the middle of the bit interval.

(*) If 0 the transition occurs at the beginning of bit interval.

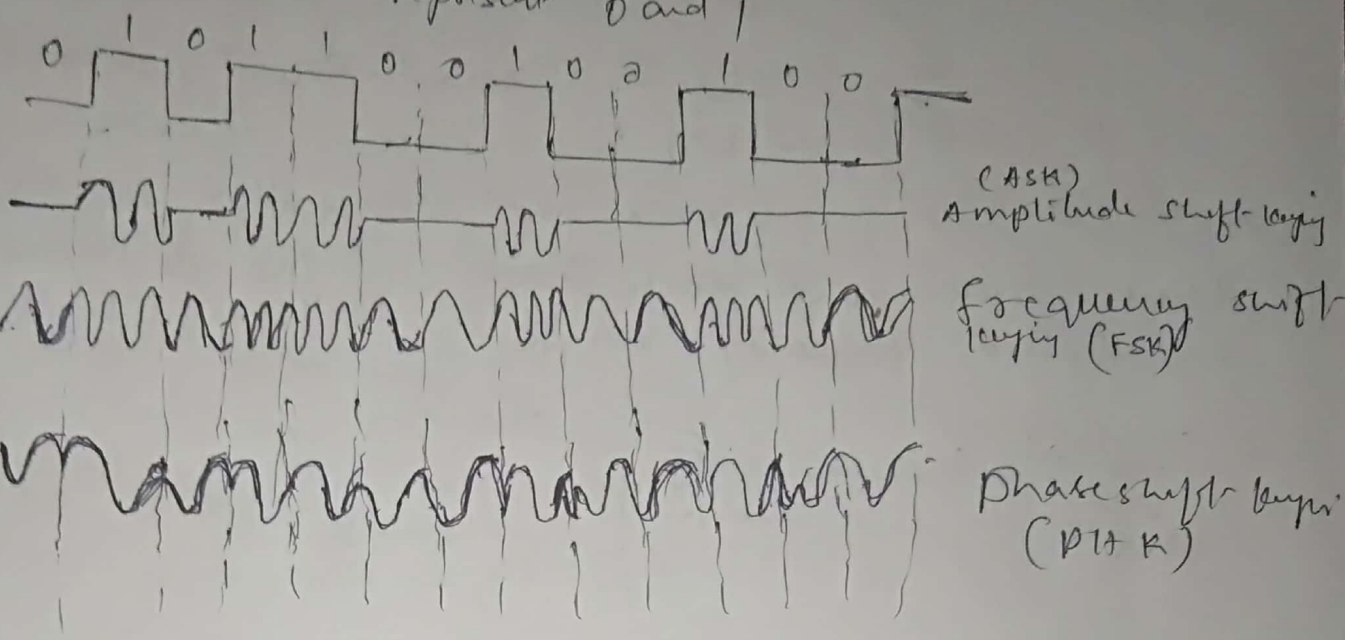
(*) If 1 no transition occurs at the beginning of bit interval.

Pass Band transmission

Digital modulation is done with passband transmission by modulating a carrier signal. That is in the pass band we can modulate Amplitude, frequency (or) phase of the carrier signal.

9.

① ASK (Amplitude Shift keying):- two different amplitudes are used to represent 0 and 1



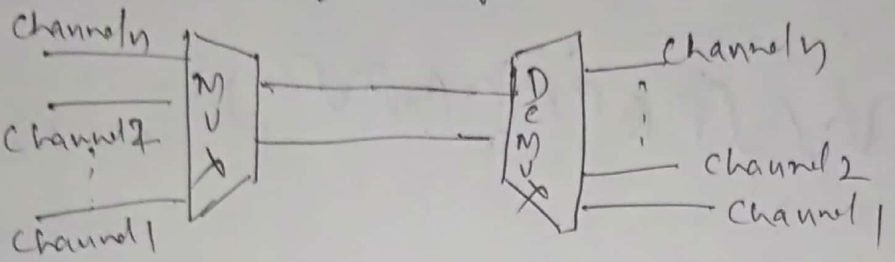
Multiplexing

Sharing of available channel among large number of source and destination is called Multiplexing.

Frequency division multiplexing (FDM), TDM (Time Division Multiplexing)

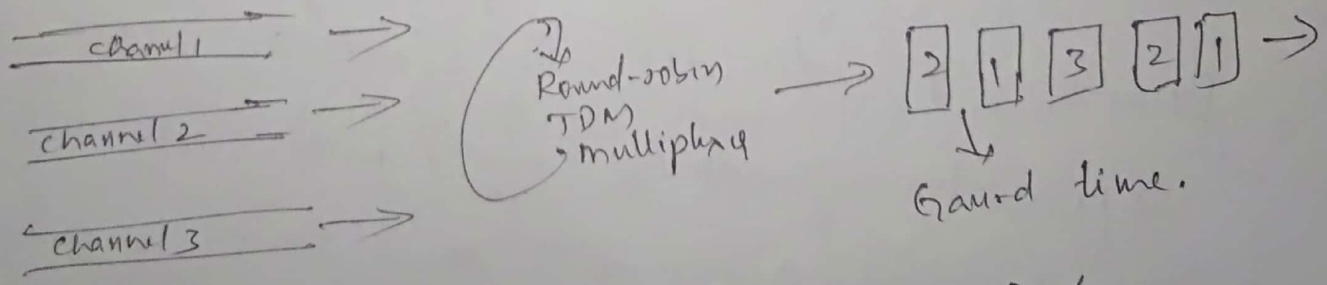
FDM : It divides the frequency spectrum into different frequency bands. with each user having exclusive aquision of some band to send their signal. The excess band width in each channel is called Gaurd Band which keeps the channels well seperated.

In voice grade telephone channels the filter limit the usable band width to 3100Hz per voice-grade channel but 4000Hz is allocated per channel. So 900Hz is Gaurd Band used to avoid interference b/n two successive channels. In FDM no. of signals are transmitted at the same time and each source transfer its signal in allotted frequency range.



Time division multiplexing (TDM)

In TDM each user gets ~~time~~ entire bandwidth for a little burst of time periodically. All signals operate at the same frequency but at different times.



Code Division multiplexing (CDM) / Code Division multiple Access (CDMA)

allows each station to transmit over the entire frequency spectrum all the time. and multiple simultanious transmissions are seperated using coding theory (people talk in different language)

In CDMA each station is assigned a unique m-bit code called chip sequence. For example

To transmit a 1 bit a station may transmit a pattern of m=8 i.e (-1 -1 -1 +1 +1 -1 +1 +1) and to transmit 0 bit it sends the negation of its chip sequence ie +1 +1 +1 -1 -1 +1 -1 -1.

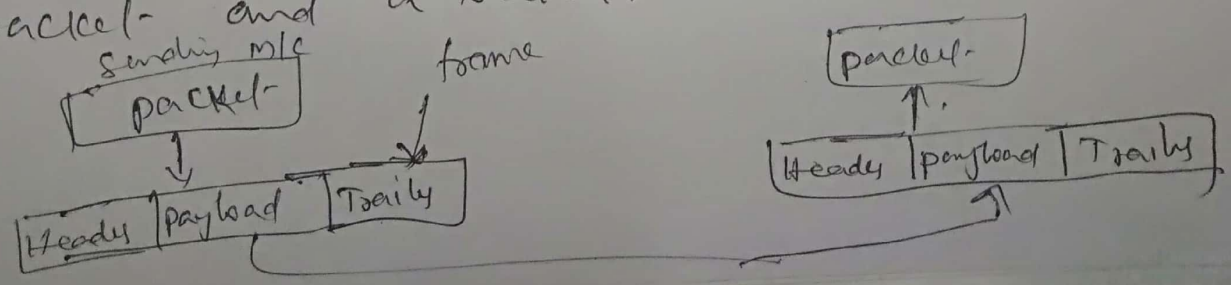
Data link Layer

Second layer of OSI model which takes services from the physical layer and provides services to the network layer.

The functions of data link layer framing error handling, flow regulation, error control physical addressing and Access control.

DLL → MAC (Media Access Control) (how to access media)
DLL → LLC (Logical Link Control) layer.
(frame synchronization, flow control, error checking)

To accomplish the functions the data link layer takes the packets from N/w layer and encapsulates them into frames for transmission. Each frame contains a frame header, payload holding the packet and a trailer.



Design issues

Services provided to the N/w layer.
The principle service is transferring data from N/w layer on source machine to N/w layer on destination m/c.

The actual service offered can vary from system to system. Three reasonable possibilities that are commonly provided are

(1) unacknowledged connection less service
(2) Acknowledged connectionless service
(3) Acknowledged connection - oriented service

unacknowledge connection less service

Source machine sends frames to the destination m/c without having the destination machine ACK them.

* No logical connection is established beforehand or released afterward.
* If frame is lost, no attempt is made to detect the loss or recover from it from the data link layer.
* Ethernet is the good example which uses this service.

Acknowledged Connectionless Service :

Framing: Raw data coming the physical layer is breaking the bit stream into frames and computi the checksums for each frame to detect errors and if necessary Correct errors.

When the ~~checksum~~ frame arrives at the destination the check is recomputed and if the new checksum is different from the received one the DLL knows that has occured

Some of the methods of breaking up bit streams into frames are

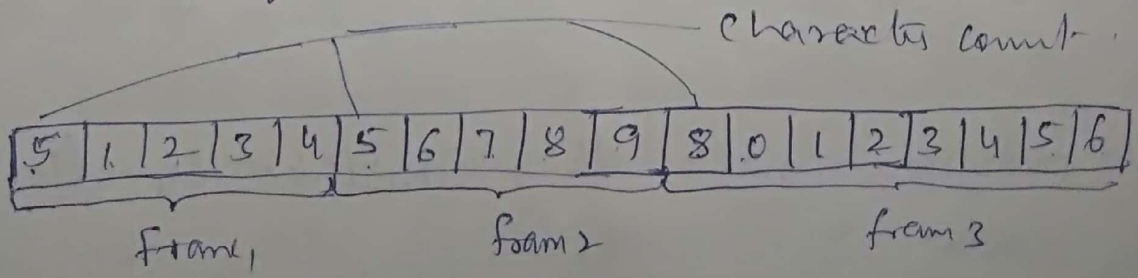
(1) Character Count (2) flag byte with byte stuffing

(3) Starting and ending flags with bit stuffing

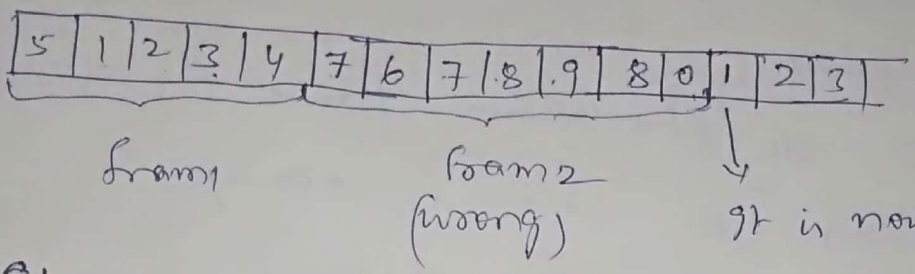
Character Count method.

(*) ~~USB~~ A field in the header specifying the number of Characters in the frame.

(*) The destination checks the character count and knows Characters follow and where the end of the frame is.

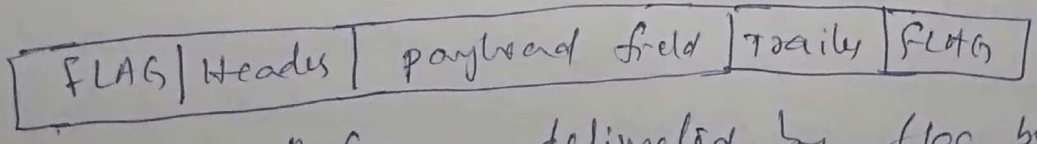


The problem with this method is if characters count changes during transmission then the destination will receive the data out of synchronization and receiver may not be able to identify the start of the next frame.



Flag bytes with byte stuffing method (Byte/character stuffing)

- Each frame start and end with special Bytes called Flag Byte.
- flag byte is both starting and ending ~~delimiter~~ delimiter.
- The receiver searches for the flag byte to find end of the current flame
- Two continuous FLAG bytes indicate the end of one flame and start of the next flame



A frame delimited by flag bytes

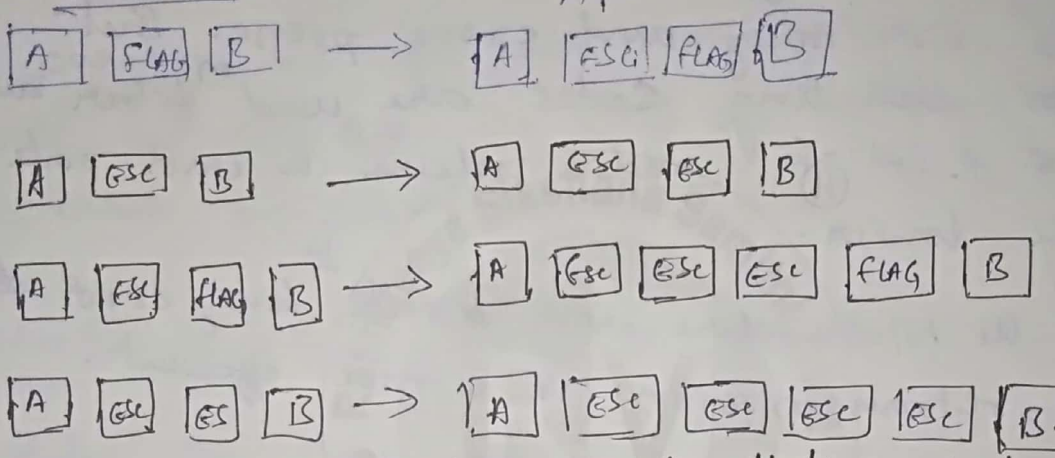
- The problem with this method is the FLAG bytes ~~data~~, bit pattern may occur in data
- The solution is the sender data link layer.

will insert a special escape byte (ESC) just before the each accidental flag ~~data~~ byte in the data.

(*) ~~At~~ DLL at receiver end removes Esc byte before data is given to N/W layer.

(*) ESC byte also occurs in data then one more ESC byte will be stuffed.

Original Data → After stuffing



So frame flag byte can be distinguished from one in data by presence/absence of ESC Byte before it.

Starting and Ending flags with bit stuffing.

(*) Each frame begines and ends with a special bit pattern 01111110 (0x7E) whenever a sends

(*) In Byte stuffing it uses 8 bits stuffing which may overload.

(*) Framing done at ~~by~~ bit level

(*) frames can contain arbitrary number of bits made up of units of any size.

(*) The sender stuffes 0 bit automatically when it encounters 5 consecutive 1's in the data.

(*) USB uses bit stuffing method.

(*) The receiver when it receives 5 consecutive 1's followed by 0, it automatically destuffs 0 bit.

Ex 01101111111111111111110010

⇓

0110 111110111110111110010010

↑ ↑ ↑

Stuffed bits

Error-Detecting Codes.

(*) Error-correcting codes are used in wireless links with noisy and error prone. But error detecting codes are used on fiber and Cat-5 & Cat-6 media where the error rate is much lower.

(*) In the N/W where error rate is low, error detection and retransmission is more efficient.

Error detecting codes are.

(1) parity method (2) checksums method

(3) Cyclic Redundancy Checks (CRC)

parity method

Single parity : A single parity bit is added to the original data so that the number of 1's in the ~~code word~~ codeword is EVEN for even parity (or) odd for ODD parity.

Ex if data is 1011010 Codeword in Even parity is 10110100 and codeword in ODD parity is 10110101

A codeword with single parity can have a distance of 2 if any single bit error is has occured.

(*) Single bit parity can detect 1-bit error.

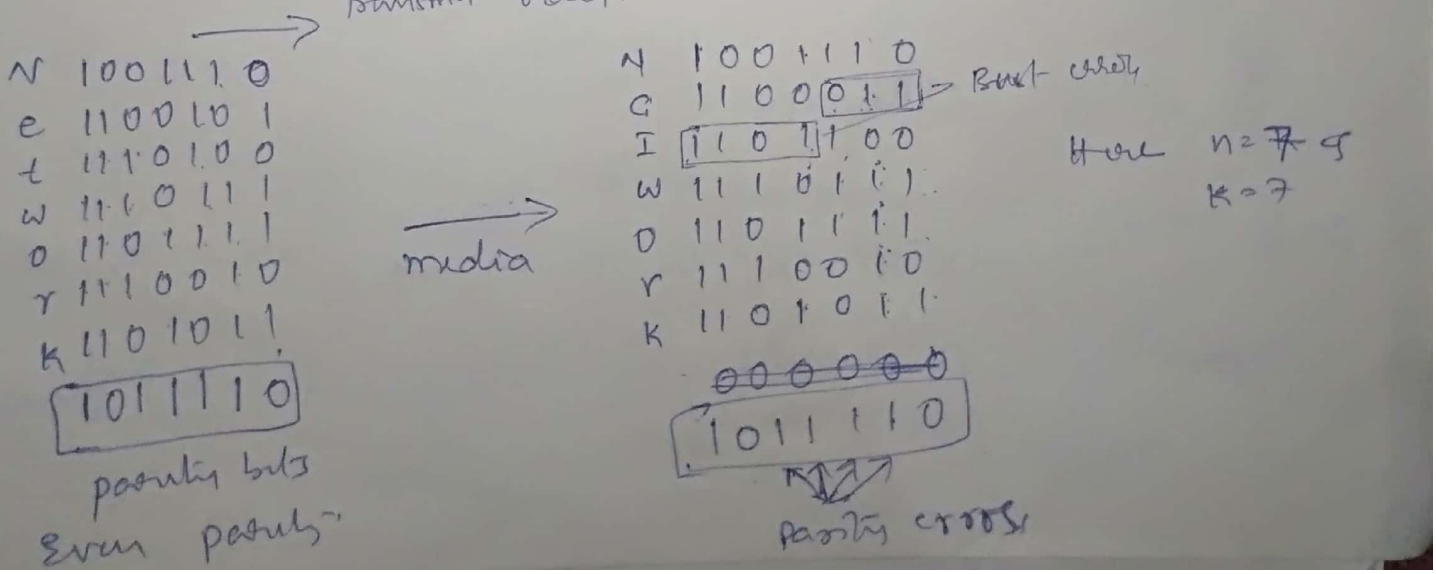
This single bit detection can be improved if each block to be sent is regarded as rectangular matrix of 'n' bits wide and 'k' bit high. and compute 1 parity bit for each row, upto k bit errors will be detected as long as there is atmost 1 error in each row.

Interleaving : computing the parity bit in a different order than order in which the data bits are transmitted.

(*) Compute parity bit for each ~~Columns~~ of n columns and send the data bits as k rows.

(*) ~~Send~~ Each row is sent from left to right ~~starting~~ starting from ~~bottom~~ top row to bottom row

(*) The last row sent will be the n-parity bits



(*) So this method uses n parity bits on block of nk data bits to detect a single burst error of length n (or) less.

(*) The burst of length n+1 will be detected.

Check Sum method

(*) The check sum methods are based on the running sum of the data bits of the message.

(*) The check sum is generally placed at the end of the message

At sender (*) If m bit check sum is used then data to be transmitted Td is grouped into segment of m bit

(*) All m bits of segment are added.

(*) The result of sum is 1's complemented

(*) obtained value is the checksum.

(*) Data & Checksum are transmitted

At Receiver. The same process is done on the received data along with check sum.

(1) if recomputed check sum is 0 (zero) the data is Non-erroniously

(2) Else erroniously.

Note : This concept is used in calculating the check sum in IP Header, TCP Header & UDP Header

Ex Given data : 10011001111000100100100100000100

(*) Assum data unit divided into segment of 8 bit

10011001 11100010 00100100 10000100

(*) Add all the segments

Sum = 1000100011

(*) Two extra bits so wrapped around

00100011 + 10 = 00100101

(*) Compute 1's complement 11011010

∴ Checksum is 11011010

The data + checksum

Data	checksum 11011010

is transmitted

At the received.

(*) The received data unit is divided into group of 8 bit

(*) All segments with checksum segment is added

Sum of bits in data segment = 00100100

checksum segment = 11011010

11111111

Complement value = 00000000 so the received data is non-erroneous

Cyclic Redundancy check (CRC)

(*) It is an error detecting code also known as polynomial code

(*) Polynomial codes treats bit string as the representation of polynomials with the co-efficients 0 and 1

(*) The highest order of the polynomial is called the degree of the polynomial

Eg: 110001 is presented in polynomial as

$1x^5 + 1x^4 + 0x^3 + 0x^2 + 0x^1 + 1x^0$

$= x^5 + x^4 + 1$ so the degree is 5 of polynomial is 5

(*) polynomial arithmetic is using modulo 2 (*)

(*) when polynomial code method is employed then Sender and Receiving must agree upon on Generator polynomial G(x).

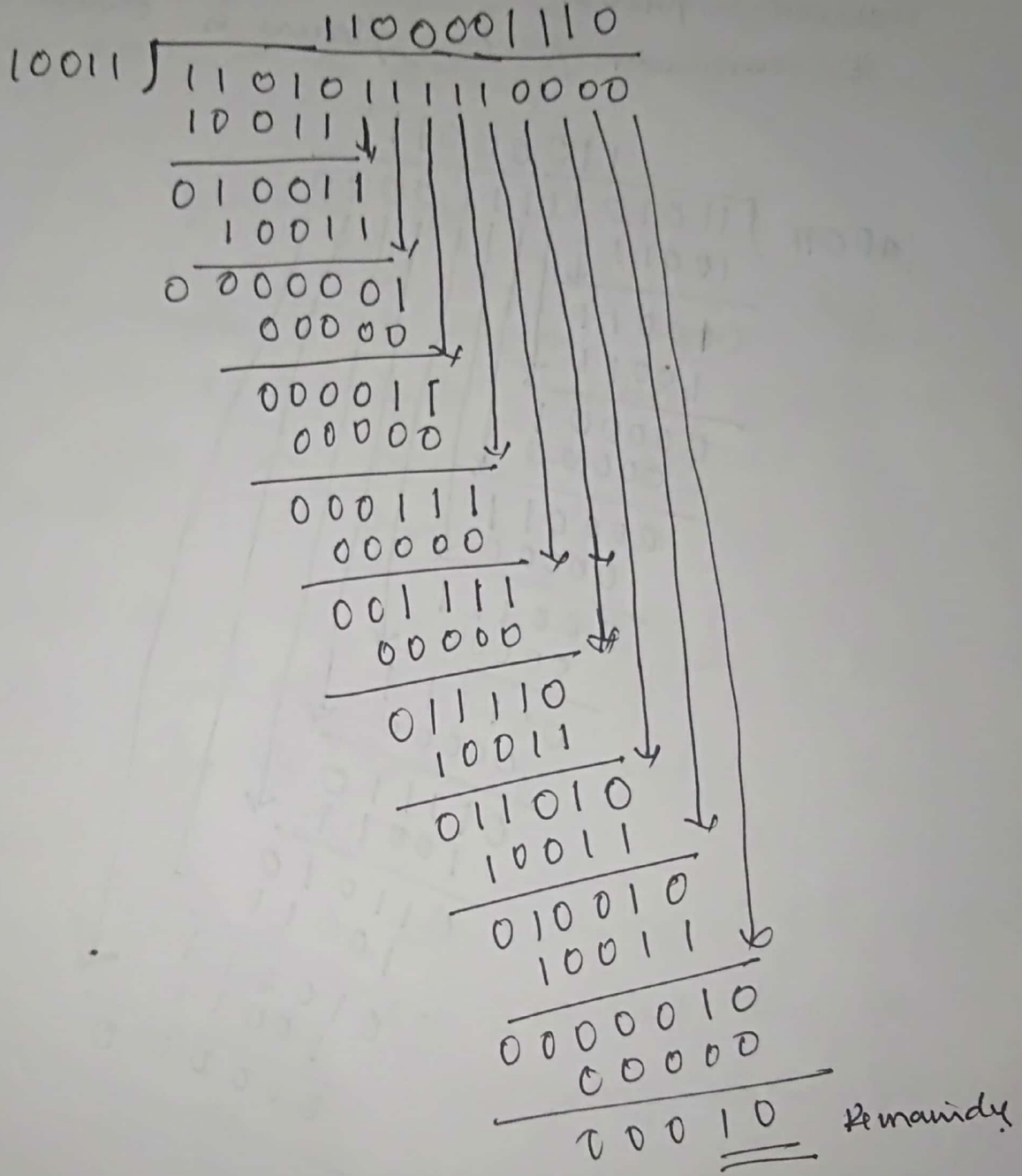
Algorithm to Compute CRC

1. Let G(x) is the polynomial of degree r; then Append r zero (0) bits to the lower-order of and of the frame which makes m+r bits
2. Divide the bit string M(x) of length m+r bits by G(x) using modulo 2 division
3. Modulo subtract the remainder from M(x) of length m+r to get T(x)

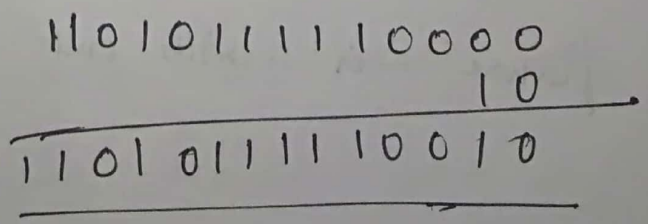
Frame: 1101011111

G(x) = 10011

Frame after appending 4 0's : 11010111110000

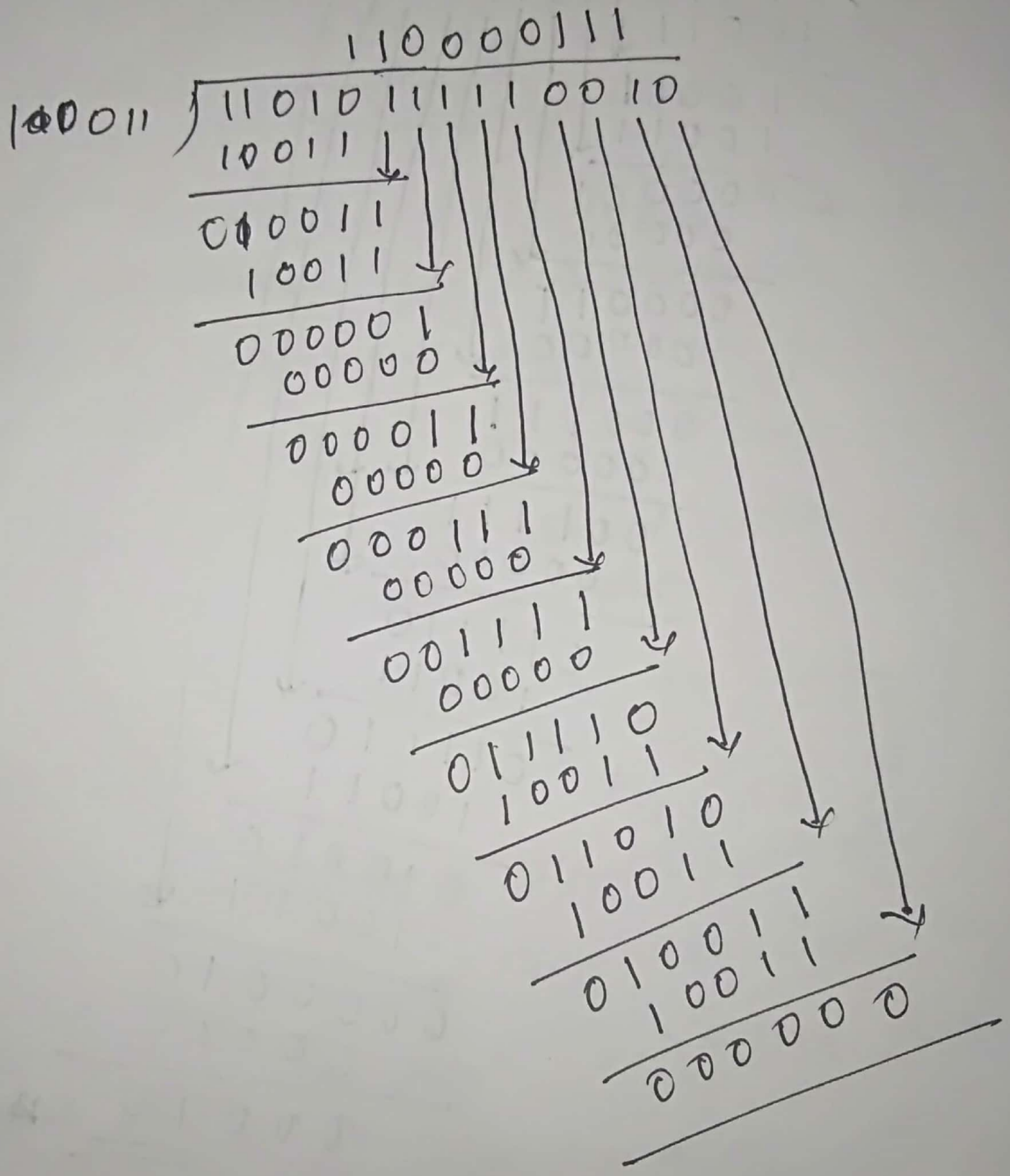


∴ Frame to be transmitted is



@ the receiver the received frame is divided by the same generator polynomial G(x) and if the remainder = 0 then no error in received frame.

if remainder ≠ 0 frame is erroneous.



So. remainder is zero ∴ the received frame is with out errors.

Note: The physical layer process and the Data Link layer process runs on ~~dedicated HW~~ NIC and rest of Link layer & network layer runs on the CPU as a part of OS. (device driver)

Sliding window protocols

To achive ~~Duplex~~ full-duplex seperate link may establishing for each direction and the each link will have one forward link for data and Reverse link for ACK. In both cases the Band width of Reverse channel is almost wasted.

So use single link for data in both directions

Piggybacking: The technique of temporarily delaying out going ACK. so that they can be hooked onto the next out-going data frame is known as piggybacking. This leads to better utilization of channel Band width. because ACK field in the header costs only few bits where as seperate frame would need a header checksum etc

Dis advantage of piggybacking is

* How long should the data link layer wait for a packet onto which piggyback the ACK of the data. link layer waits longer than the sender time out period, the frame will be retransmitted.

* Sliding window is a protocol for reliable and sequential delivery of data frames.
* Data link layer protocols
* flow control and error control protocols
* ~~pipe~~ Based on pipelining and provides reliability
* There are 3 types of sliding window protocols based window size (i.e efficiency, complexity and Buffer Requirement)
  1. 1-bit sliding window
  2. Go-Back-n sliding window
  3. Selective Repeat sliding window

In all sliding window protocols the ~~type of~~ Concept of Sending window and receiving window plays imp role

Sending window : The logical / imaginary ~~box~~ box that maintains the sequence number of the frames that are permitted to send

Receiving window: The logical / imaginary box that maintains the sequence number of frames permitted to ~~Receive~~ accept at the receiver.

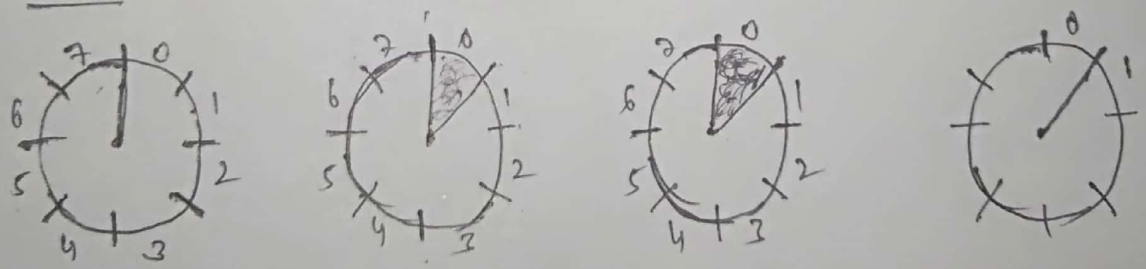
Note: ① Sending and Receiver window size may not be same.

② If window size n then the sender needs to have n buffers to hold the frames for retransmission.

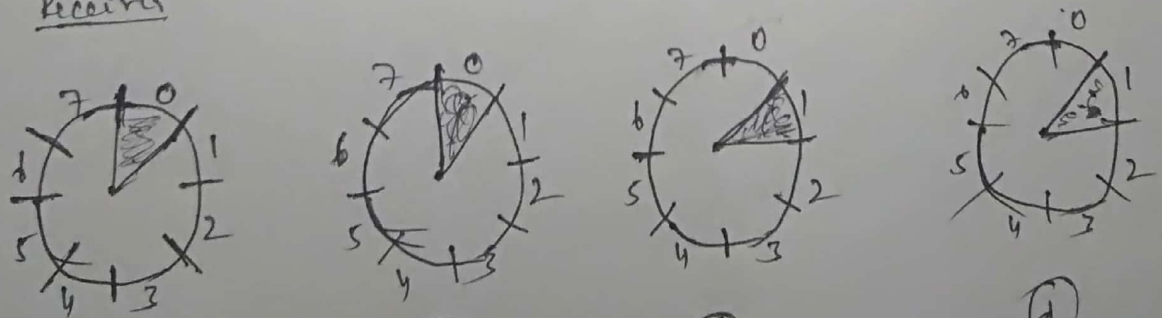
1-bit Sliding window protocol:

Window Size 1 means the data link layer only accepts the frames in the order one at a time

Sender



Receiver



(a) Initially

(b) First frame sent

(c) First frame Received.

(d) First Ack is received.

1-bit sliding window protocol uses stop and wait as sender transmit a flame and waits for ACK before sending the next one

In the above diagram the window size - 1 and the length of the sequence number is 3 i.e the sequence number of flame ~~are~~ can be from 0 to 7

@ initially no flames are ~~outstad~~ outstanding. so the lower and upper edges of the senders window are equal