CW

12/2/24

Data Communication network by Frousen - 3rd ed. (Book)
①
② Reference :- Tanning bum
ii) Stallings

Lab (CCNA guidance by Richard dell/Todd Lammle - pdf book)

- Packet tracer / gns3 — we need to install the one of them. (we have to do a mini proj (3 months))
- Socket programming (Basically based on c/c++)
(network programming by Richard Stevens - pdf book)

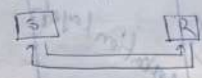
CW

16/2/24

/Computer

- Computer networks — set of devices connected with each other. the purpose of the connection is data communication.

- Protocol - It is a set of rules which guides the communication.



Eg - TCP, UDP, HTTP, FTP etc.
(transmission control protocol) (IP - Internet protocol)

- Attinuation -

← Can't head the signal
(amplitude lost) (Headache)
signal

Decreasing distance → increasing amplitude → the sound is more clear & readable
Attinuation this process is

write the eg of everything (def, diagram)

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. [Essentially, it allows connected devices to communicate with each others, regardless of any differences in their internal processes, structure or design.] ||

It is the loss of signal strength in computer networking connections. It can be caused by internal or external factors & can be measured in decibels (dB) / voltage (V). It may cause signals to become distorted / indiscernible.

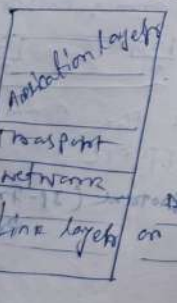
History of CN (just read) → 1970 ARPANET (by America)

• OSI - Open System Interconnection.

OSI is OSI reference model v/s TCP/IP reference model.

It is consist of different layers. It has 7 layers.

• TCP/IP - 4 layers



Data link or physical

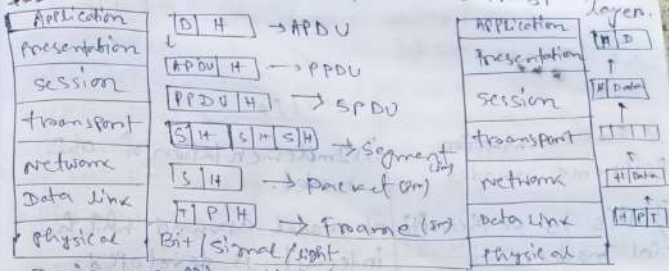
[Image is set of datas (0, 1)]

• Application layer Protocol - https (Hypertext transfer Protocal secured)

• Packet is diff from the frame.

• Header stores information in every layers. The infos are dependent upon the layers type of (It references to supplemental data placed at the beginning of a block of data being stored / transmitted)

• Port address is associated with transport layer.



• Extention - It is a suffix added to the name of a file to indicate the file's layout (in terms of how the data within the file is organized). It decides the orientation of the file/folder etc. Extention is the type/format of any file. Eg - .png, .pdf etc.

• TCP assures the connection oriented transmission

• UDP assures the connection less (user datagram Protocal)

Eg - used in movie (this type of Protocal)

(It is a communications protocol for time-sensitive application like gaming, playing videos etc)

• Types of address (in CN) - i) MAC / physical address

ii) IP (OL) / logical (N) address

iii) Port address (T) / process

(func of transport layer)

• Congestion - Lots of datas in a channel (like single traffic) It is controlled by some congestion control algorithms. It is when network nodes & links are overloaded with traffic (lots of data). It makes the end user's network slow. It is often related to latency, throughput & bandwidth.

Types of Protocal - 2 types.

SNMP (simple Network management Protocal)

ICMP (Internet control message Protocol)

Q(7) - OSI reference module v/s TCP/IP reference model.

OSI	TCP/IP
i) ~~Implementation~~ Reference model	i) Implementation of OSI model.
ii) This is a theoretical model.	ii) model around which internet is developed
iii) Has 7 layers	iii) Has only 4 layers
iv) Considered as reference tool.	iv) Considered more reliable
v) Stricter boundaries for the protocols	v) Protocols are not strictly defined.
vi) vertical approach	vi) Horizontal approach
vii) Has separate session & presentation layer.	vii) combines the session & presentation layers in the application layer.
viii) model was developed before the development of protocols	viii) Protocols were developed first & then the model was developed.
ix) Protocal Independent Standard.	ix) Protocal dependent Standard.
x) supports connection-less & connection-oriented communication in the network layer.	x) supports only connection less communication in the network layer.

OSI model - It is a reference framework model that explains the process of transmitting data between computers. It is divided into 7 layers that work together to carry out specialised network functions, allowing a more systematic approach to networking.

1) ~~Physical layer~~ - Application layer - At the very top of the OSI reference model stack of layers, we find the application layer which is implemented by the network applications. this applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network & for displaying the received infos to the user. Eg - Application - Browser, Skype messenger etc. It is also called desktop layer. Device/Protocol used here - SMTP. (this is also upper/Software layer)

2) Presentation layer - It is also called translation layer. The data from the application layer is extracted here & manipulated as per the required format to transmit over the network. Device/Protocol used here - JPEG, MPEG, GIF. (this is also upper/software layer)

3) Session layer - This layer is responsible for the establishment of connection, maintenance of sessions, & authentication. & also ensures security. This is also known as uppers or software layers. device/protocol

used here - NetBIOS, PPTP.]]

4) transport layer - It provides services to the application layer & takes service -s from the network layer. The data in the transport layer is referred to as segments. It is responsible for the End to End delivery of the complete message. [The transport layer also provides the acknowledgment of the successful data transmission & re-transmits the data if an error is found. It is called as Heart of the OSI model. It is operated by the OS. It is a part of the OS & communicates with the application layer by making system calls. Device/ Protocol used - TCP, UDP, NetBIOS, PPTP.]]

5) network layer - The network layer works for the transmission of data from one host to the other, located in different networks. [It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the no. of routes available. The sender & receiver's IP addresses are placed in the header by the network layer. segment in this layer is referred as packet. It is implemented by networking devices such as routers & switches.]]

6) Data link layer - this layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, [over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the host using its MAC address. It has 2 sublayers (LLC, MAC) [logical link control, media access control]. packet in the DLL is referred to as Frame. DLL is handeled by NIC (network interface card)].]

7) Physical layer - It is the lowest layer of OSI reference model. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. [It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received & convert it into 0s & 1s & send them to the Data link layer, which will put the frame back together.]]

TCP/IP - It stands for transmission control Protocol & IP stands for internet Protocal. It takes care of how data is transferred in a network. It breaks down the data into smaller packets that can be shared across a network effectively. Layers of TCP/IP

1) Application layer - It consists of HTTP (Hypertext transfer Protocal), FTP (File transfer protocal) etc. It is called the application layer because it consists of application data. It is composed of application, Presentation & session layer.

2) Transport layer - the transfer of data is done in this layer. It is responsible for maintaining the communication b/w the sender & receiver. TCP & UDP is used for this purpose.

3) network layer - It consists of IP & Internet control message Protocal (Icmp). IP takes care of the destination host address & makes sure the connection is maintained. Icmp reports errors in case the connection is not Proper.

4) Link layer - The Protocal in this layers works in the link b/w different devices in the network. It includes Protocal for Ethernet & Address resolution Protocal.

Application layer Protocal - It is a set of rules that define the language that network applications use to communicate with each other.

19/9/24

Function of each layers

func of transport layer → 1) connection
2) type of connection (connected / less)

" " network " → 1) logical address
2) To find the path from Source to destination.

" " Data link " → 1) Flow control
2) Error correction
3) Error detection.
4) Framing 5) Access control

" " physical " → 1) data is converted into to the signal
2) All the signals are composed by this
3) Bit synchronization layer.

(1) Application layer

i) network virtual terminal - It allows a user to log on to a remote host.

ii) FTAM - File transfer access & management. This application allows a user to access file in a remote host, retrieve files in remote host &

iii) mail services - Provides email service

iv) Directory services - It Provides distributed database sources & access for global info

about various objects & services.

② Presentation layer - i) Translation - for eg. ASCII to EBCDIC

ii) Encryption / Decryption - It is used for encrypting or decrypting data.

iii) Compression - Reduces the no. of bits that need to be transmitted on the network.

③ session layer - i) session establishment, maintenance & termination - The layer allows the 2 processes to establish, use & terminate a connection.

ii) Synchronization - this layer allows a process to add check points that are considered synchronization points in the data.

iii) Dialog controller - The session layer allows 2 systems to start communication with each other in half-duplex or full-duplex.

④ Transport layer - i) segmentation & Reassembly - this layer accepts the message from the session layer & breaks the message into smaller units (segments). Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.

ii) Service point addressing - To deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus, by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

iii) Services provided by transport layer - Connection-oriented & connectionless service.

⑤ network layer - i) Routing - The network layer protocols determine which route is suitable from source to destination. This func. of network layer is known as routing.

ii) logical addressing - To identify each device on internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely & universally.

⑥ Data link layer - i) Framing, ii) physical addressing, iii) error control, iv) flow control, v) access control.

⑦ physical layer - i) bit synchronization, ii) bit rate control, iii) physical topologies, iv) transmission mode.

② TCP, U/S UDP
(reliable) (Best before delivery)

Congestion control algo Imp Q.32

1. Leaky bucket algo (Imp) } Briefly describe about congestion control algo (leaky/token bucket)
2. Token bucket algo (Imp)

Protocols in the network layer

1. Routing (map) 2. Routed (car)

Protocol - Create an optimized route from source to destination. eg- IP, SAP, Application

- Carry the data from s to d
- to fetch the data from s → d.

Static routing | Dynamic routing

Dynamic routing

- Intra domain - same type
- Inter domain - different type (autonomous system) → A set of networks that is maintained by the independent data.

Intra domain →
- Distance vector routing protocol (Bellmann ford) → RIP (Routing Information Protocol)
- Linked state routing protocol (Dijkstra) → OSPF routing protocol

- LAN communication → DLL is responsible
- outside LAN communication → network layer is responsible for wide comm.

APDU - It stands for application protocol data unit. [It is the communication format b/w a card & off-card applications] It consists of the data that is received & header that contains info about corresponding layer & what is happening in that layer.

PPDU - It stands for presentation protocol data unit. It consists of APDU & header ---- layer.

SPDU - It stands for session protocol data unit. [It is a unit of info transmitted b/w peer entities] It consists of multiple segments, PPDU & headers that ---- layer.

Segment - The data in the transport layer is referred to as segments. ~~It consists of multiple segment~~ In transport layer the whole data is divided into multiple segments & there is a header with every segments that ---- layer.

Packet - segment in the network layer is referred as packet. network layer is consists of segment & header ---- layer.

Frame - It is a digital data transmission unit. It is a data unit used in the data link layer of the OSI model. It consists of

Packet, trailer & header → layers.

Bit / signal - It is produced in physical layers of OSI model. It is the smallest unit of data [It is also known as binary digit. These are encoded using electrical signals & pulses of light transferred through a computer network.]

TCP	UDP
(1) Connection oriented	(1) connectionless.
(2) It is reliable.	(2) It is best before delivering.
(3) Rearranges packets in order.	(3) No inherent order.
(4) Full form	(4) Full form
(5) It has high reliability, Critical-less transmission time.	(5) It is best before delivering, efficient transmission time.
(6) It is slower.	(6) It is fast.
(7) It reads a data as a byte streaming of data - Read as a byte stream.	(7) sent & read individually.
(8) Error checking & recovery.	(8) simply error checking, no error recovery.
(9) Acknowledgement segments.	(9) No acknowledgment

Types of address in cn -

i) physical address / MAC - It is also known as media access control address. It is an unique identifier for a network interface controller (NIC) or network adapter. It's a hardware address that identifies each node on a network, such as a computer or printer.

ii) logical address / IP - It is a virtual address that the CPU generates when a program is running. It's used by the CPU to access the actual physical memory location. [It may differs from physical address due to the operation of an address translator or mapping func. It is also known as internet protocal address / IP address.

iii) Port / process address - It is a 16-bit unsigned int. number that ranges from 0 to 65535 [It's an unique no. assigned to every application on a computer. Ports are virtual points where network connections start & end. They are software-based & managed by computer's operating system.] It is also known as process address / PID or process id

Types of protocal

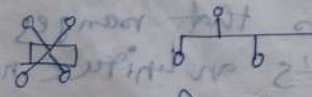
i) Snmp (Sh) — It stands for simple network management protocal. It is a network protocal used for the management & monitoring of network-connected devices in internet protocal networks. It is a part of TCP/IP protocal suite.

ii) Icmp — It stands for internet control message protocal. It is a network layer protocal that devices use to communicate problems with data transmission. Icmp messages communicate info about network connectivity issues back to the source of the compromised transmission.

(Ptc) 23/2/24

CW physical layer → (If want to read, then read)

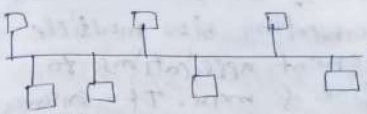
• Topology — It means geographical layout of devices.



There are following types of topology

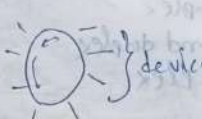
Bus topology
Ring
Star
Hybrid
& many more

Bus topology - There is a central bus & all devices are connected with that.

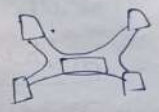


Benifits - i) Easy to implement (main advantage)

Disadvantage - i) collision (0 & 5v we will get 5v)

Ring t -  devices

Disadvantage - If there is a cut then it can't proceed.

Start t - 

Disadvantage - If there is a synchronised device it can't proceed.

LAN
MAN
WAN

• Broadcast domain

Communication type - 3 types. i) 1 to all (Broadcasting) ii) 1 to many (multicasting) iii) Unicasting (1 to 1)

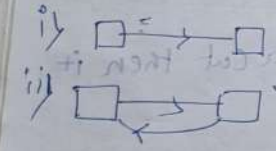
LAN - All the machines under a broadcast domain is called LAN.

• What is the need of multicasting?

It is a communication method that allows a sender to send a single copy of data across LANs/WANs to multiple recipients. It is used in CN to improve communication b/w multiple devices, allow different applications to run at the same time & more. It conserves network bandwidth, reduces data traffic, prevents unwanted messages, support many to many communication etc.

Types of communication –

i) Simplex
ii) Half duplex
iii) Duplex



iv) No one is going to stop, both will be talking

Medium/media – It is a communication channel that connects nodes. Transmission media are the physical paths that signals travel through.

Types of the medium – 2 types.

i) Guided medium (wire) – The m. which guide the signal
ii) Unguided medium (Air) – The m. that covers a certain area.

Guided medium

types – Fiber optics, RJ 45, twisted pair cable, coaxial cable etc. STP, UTP (shielded & unshielded twisted pair)

Unguided medium

types – Radio waves, microwaves, infrared waves etc

• Advantages & disadvantages of guided & unguided medium.

Guided medium –

Advantages – i) Data security is high (as data signals are passed through defined path) ii) Data transmission is faster in compared to unguided media iii) There is no signals interferences in unguided media. iv) There is no effect in data transmission due to weather.

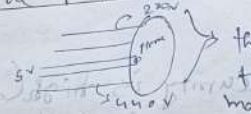
Disadvantages – i) Difficult to setup (as wiring is required for all nodes) ii) Expensive because many wires are required. iii) Not suitable for portable devices.

Unguided medium –

Advantages – i) Easy setup as no wiring is required for individual nodes. ii) Portable service as nodes can be moved easily from 1 location to another. iii) new nodes can be easily connected as just sharing password (like in WiFi). iv) not expensive

Disadvantages – i) Data security is in risk as signals can be hacked. ii) Transmission of data may be affected by weather condition. iii) signal interference if there exists many wireless signals. iv) slower as compared to guided medium.

External Parameters



→ these wire will deviate the 5V for their electro magnetic field. (cross-talk)

It is a signal transmission issue that disrupts the data communication b/w computers that are interconnected. It reduces the strength & data transfer speed.

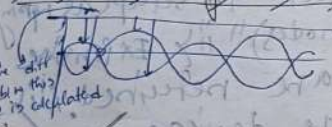
Twisted Pair - To overcome (↑) this problem.

Colour coding of wire

10 base T

↳ 10 mbps [mega bit per s] [this wire can convey 10mb data per s]

[this means 100 meters] (we will get 7518-max)



the diff b/w this 2 is calculated

Why twisted pair is implemented? (also figure to read for next day)

It is implemented to reduce crosstalk & electromagnetic interference. Twisted pair cabling system is a cable consisting of 1 or several pairs of copper wires. These wires are twisted together & around each other & are insulated with a dielectric polymeric compound.

If twisting helps to minimize the electromagnetic radiation & resists external interference. So, twisted pair is implemented.

Colour coding of wire - It helps us to determine the color code of the wire & it's color.

Baseband, broadband technology (just read)

What is the meaning of 10 base T? (include this & like this)

It is an ethernet standard for local area networks (LANs) that uses twisted pair cabling to transmit 10 megabits per second (mbps). Here,

i) 10 - the transmission speed in mbps

ii) BASE - Baseband transmission is used

iii) T = Twisted-pair cable.

Switching technique → packet switching (eg - texting multiples)

→ circuit switching (eg - calling someone)

Diff b/w them (imp)

It is the process of transmitting data from senders to receivers.

Circuit S. - when the communication is sendero to receiver & no 3rd party can enters into this. It has no real time communication (if it is not under net work)

Packet S. - It where the communication is real time communication.

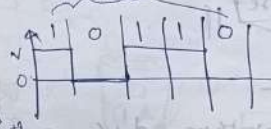
virtual switching

Diff b/w Packet & Circuit switching.

Circuit s.	Packet s.
i) physical path b/w source & destination.	i) No physical path.
ii) All packets use same path.	ii) Packets travel independently.
iii) Reserve the entire bandwidth in advance.	iii) Does n't reserve.
iv) Bandwidth wastage	iv) No bandwidth wastage.
v) No store & forward transmission	v) Supports store & forward transmission.
vi) 3rd party can enter into the communication.	vi) 3rd party can't enter, it is a real time communication.
vii) An uniform path is followed throughout the session	vii) No — followed end to end through the session.
viii) Delay is uniform	viii) Delay isn't uniform.
ix) Ideal for voice communication.	ix) mainly used for data transmission.
x) without connection it can't exist as the connection needs to be present on a physical layer.	x) A connection is n't necessary, as it can exist without one too.

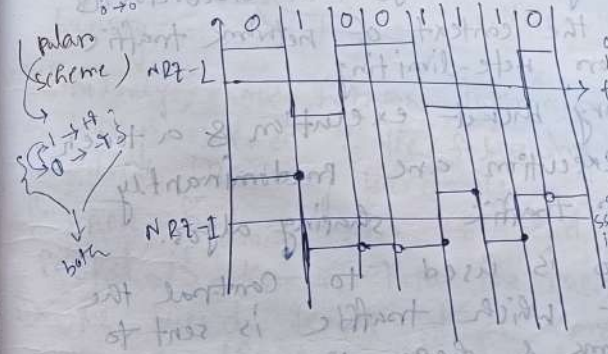
- Bit schemes
  - String (v imp) (min 8 marks) (4 pics)
  - Line coding (v imp) (classification of polars)
    - NRZ (not return to zero)
    - RZ
    - i) Manchester
    - ii) Differential manchester

NRZ (unipolar scheme)

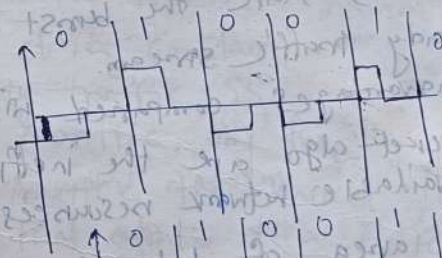


(Prefix with points pto)

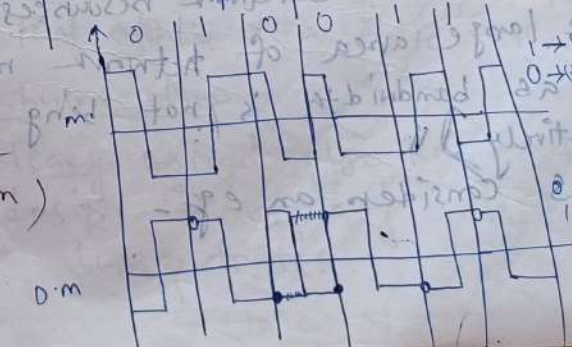
Polar (scheme) → NRZ-L, NRZ-I, both



RZ (Polar)

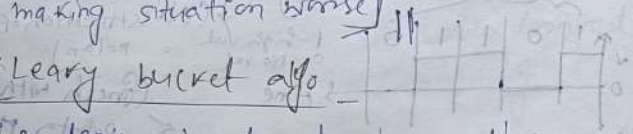


Polar (biphase m. & DM)



Congestion control algo

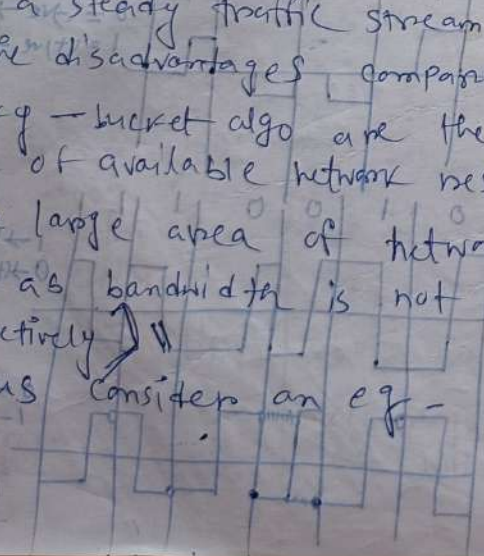
i) Effects of congestion - i) As delay increases performance decreases.
ii) If delay increases, retransmission occurs making situation worse.



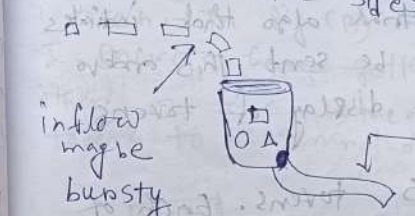
1) Leaky bucket algo

i) The leaky bucket algorithm discovers its use in the context of network traffic shaping or rate-limiting.
ii) A leaky bucket execution & a token bucket execution are predominantly used for traffic shaping algos.
iii) This algo is used to control the rate at which traffic is sent to the network & shape the burst traffic to a steady traffic stream.
iv) The disadvantages compared with the leaky-bucket algo are the inefficient use of available network resources.
v) The large area of network resources such as bandwidth is not being used effectively.

Let us consider an eg -



Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at constant rate. When the bucket is full with water, additional water entering spills over the sides & is lost.



Similarly, each network interface contains a leaky bucket & the following steps are involved in leaky bucket algo -
i) When host wants to send packet, packet is thrown into the bucket.
ii) The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
iii) Bursty traffic is converted to an uniform traffic by the leaky bucket.
iv) In practice the bucket is a finite queue that outputs at a finite rate.

2) Token-bucket algo

i) The leaky bucket algo has a rigid o/p design at an avg rate independent of the bursty traffic.

iii) So in order to deal with the bursty traffic we need a flexible algo so that the data isn't lost. One such algo is token bucket algo

iii) It is a control algo that indicates when traffic should be sent. This order comes based on the display of tokens in the bucket.

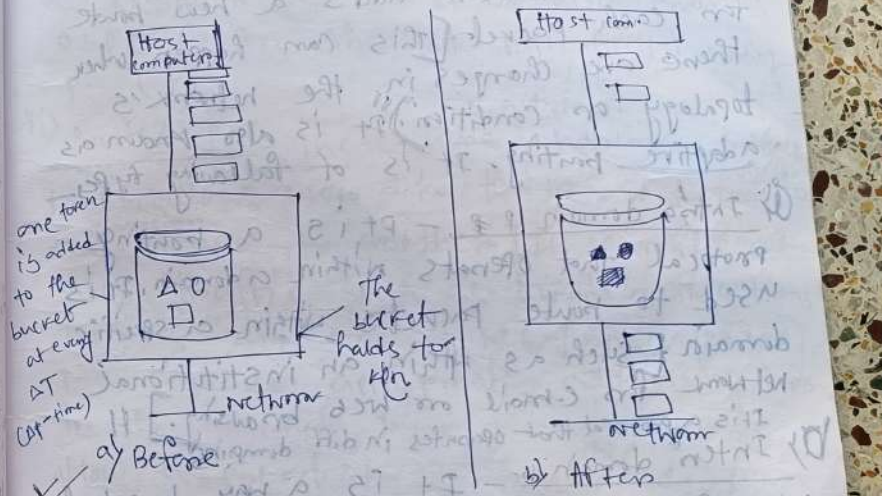
iv) The bucket contains tokens. Each of the tokens defines a packet of predetermined size. Tokens in the bucket are deleted for the ability to share a packet.

v) When tokens are shown, a flow to transmit traffic appears in the display of tokens.

vi) No tokens means no flow sends its packets. Hence, a flow transfers traffic up to its peak burst rate in good tokens in the bucket.

Steps of algo -
i) In regular intervals tokens are thrown into the bucket.
ii) The bucket has a maximum capacity.
iii) If there is a ready packet, a token is removed from the bucket, & the packet is sent.
iv) If there is no token in the bucket, the packet can't be sent.

Let's understand with an eg
In the figure(a) we see a bucket holding 3 tokens, with 5 packets waiting to be transmitted. For a packet to be transmitted, it must capture & destroy 1 token. In fig (b) we see that 3 of the 5 packets have gotten through, but the other 2 are stuck waiting for more tokens to be generated.



Protocols in the network layers - There are 2 types of protocols in the network layer.

i) Routing protocol - It is a process where routers exchange information to select the best path for a packet to travel/ route by - maps, IP, OSPF etc.

It is of following types -

① Static routing - A method of manually configuring the computer network by the network administrator.

② Dynamic routing - A technique that updates the routing table with a new route when a router adds a new route for each packet. [This can happen when there are changes in the network's topology or condition.] It is also known as adaptive routing. It is of following types

i) Intra domain p. - It is a routing protocol that operates within a domain. It is used to route packets within a specific domain [such as within an institutional network for e-mail or web browsing.] It is a protocol that operates in diff domains.

ii) Inter domain p. - It is a way to control data flow in internet b/w routing domain controller (PDC) computers. [It is often used to multicast b/w internet domains.]

It is of following types -

I) Distance vector routing p. - [A distributed algo that works by each router sending updates to it's neighbours about the best path to each destination. On other words] DVRP is a routing p. that determines the best route for data packets based on distance. It is based on the Bellman-Ford algo. It is also known as RIP or Routing Information Protocol. (eg)

II) Linked state p. - LSR is a dynamic routing algo that calculates the best path for transmitting data packets within a computer network. It is also known as OSPF (Open shortest path first) routing p. (eg)

iii) Routed p. - These are network protocols that allow [carries] users data from one network to another [receivers] [It carries out user traffic such as emails, file transfers & any kind of web traffic. Routed p. provide appropriate addressing info in its internet layer (network layer) to allow a packet to be forwarded from 1 network to another] Eg - IP, Appletalk & IPX.

VLAN [can] communication - It stands for local area network. It is a network of computers & devices that share a common communications line or wireless link to a server within specific geographical area. It is of 2 types -

i) Wired LANs - These use physical wires such as ethernet cables or fiber optics to connect devices. They are appropriate for fixed installations that require regular & uninterrupted data transfer.

ii) Wireless LANs (WLANs) - These use radio signals (Wi-Fi) to connect computers instead of cables. [WLANs use high frequency radio waves instead of cable for communications.]

Eg of LAN - networking in home, office, Wi-Fi etc.

MAN - It stands for metropolitan area network. It is a network that connects computers & devices within a metropolitan area, which can be a single large city, multiple cities & towns or any given large area with multiple buildings. It is usually several LANs interconnected by dedicated backbone connections. It allows people to connect LANs & offers greater security than a WAN.

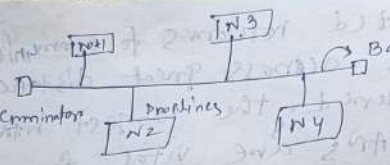
WAN - A wide area network is a computer network that connects smaller networks over a large geographical area. WANs within are not tied to a specific location, so they allow localized networks to communicate with one another across great distances. Internet is considered as the largest WAN in the world. WANs are vital for international business & also essential for daily uses.

Topology - It is geographical layout of devices. It is the way that defines the structure, & how these components are connected to each other.

Types - The arrangement of a network that comprises nodes & connecting lines via sender & receiver is referred to as topology.

Type -

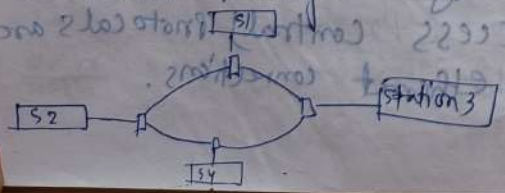
i) Bus topology - It is a network type in which every computer & network device is connected to a single cable. It is bidirectional. It is a multi-point connection & non-robust topology because if the backbone fails the topology crashes. Here various MAC (media Access Control) protocols are followed by LAN ethernet connections.



Advantages - i) Easy to implement.
ii) N devices need N drop lines & 1 central wire known as backbone.
iii) Less cost

Disadvantages - i) collision
ii) It requires lots of cabling.
iii) If the common cable fails, then the whole system will crash down.
iv) security is very low.
v) Adding new devices will cause the slow down of networks.

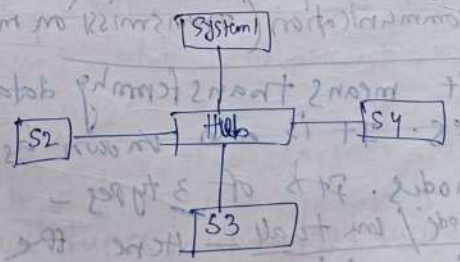
2) Ring topology - In a n.t., it forms a ring connecting devices with exactly 2 neighboring devices. The data flows in one direction, i.e it is unidirectional, but it can be made bi-directional by having 2 connections b/w each N/w (network) [dual ring t.]. The most common access method of n.t is token passing.



Advantages - i) The data transmission is high speed
ii) The possibility of collision is min
iii) Cheap to install & expand.
iv) Less costly than star t.

Disadvantages - i) The failure of a single node in the network can cause the entire network to fail.
ii) Less secure
iii) Trouble shooting is difficult
iv) The addition of stations in b/w or the removal of stations can disturb the whole t.

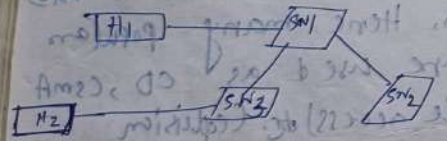
3) Star t. - In S.t, all the devices are connected to a single hub through a cable. The hub is the central node & all others nodes are connected to it. Active hubs have repeats in them. Here many popular ethernet LAN p. are used as CD, CSMA (Carrier sense multiple access) etc. (Collision detection)



Advantages - i) Easy to set up.
ii) No. of ports required is N & no. of hub required is 1.
iii) It is robust.
iv) Easy to fault identification & isolation.
v) cost-effective.

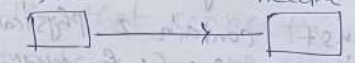
Disadvantages - i) cost of installation is high.
ii) If the hub fails, the whole system will crash down.
iii) performance is based on the single hub.

Broadcast domain - It is a logical division of a computer network. Here, all nodes can reach each others by sending & receiving broadcast messages at the D.L.L.



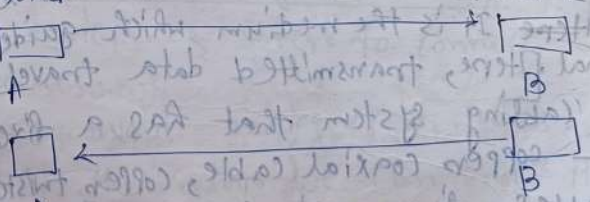
Types of communication (Transmission modes in CN) - It means transferring data b/N 2 devices. It is also known as communication modes. It is of 3 types -

i) Simplex / simple mode / one to all - Here the communication is unidirectional, [as on a one-way street] only 1 of 2 the devices on a link can transmit, the other can only receive. It is used can use the entire capacity of the channel to send data in 1 direction. Eg - keyboard, traditional monitors.



ii) Half-duplex / half duplex mode / 1 to many - Here, each station (device) can both transmit & receive, but not at the same time. When 1 device is sending, the other can only receive, & vice versa. [The half-duplex mode is used in cases where there is no need for communication in both directions at the same time. The entire capacity of the channel can be utilized for each direction. Eg - walkie-talkie etc.

Channel capacity = Bandwidth * propagation delay



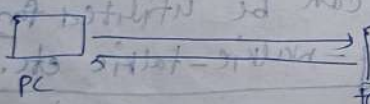
iii) Full-duplex / duplex / full-duplex mode / unicasting or 1 to 1 - Here, both stations (devices) can transmit & receive simultaneously. [Here,

signals going in 1 direction share the capacity of the link with signals going in another direction. This sharing can occur in 2 ways—

i) there the link must contain 2 physically seperate transmission paths (1 for sending & 1 for receiving)

ii) or, the capacity is divided b/w signals traveling in both directions. It is used when the communication in both directions is required all the time.

Channel Capacity = 2 * Bandwidth * Propagation delay



Types of medium —

i) Guided medium — It is also known as wired media. It is the medium which guides the signal. Here, transmitted data travels through cabling system that has a fixed path. Eg— copper coaxial cable, copper twisted pair cables, fiber-optic cables etc.

ii) Unguided media — It is also known as wireless media. It is the medium that covers a certain area. Here, the transmitted data travels through free space in form of electromagnetic signal. Eg— Radio waves, Infrared, microwaves.

Twisted pair — It is a type of communication cable that connects home & business computers to the telephone company. It consists of 1 or more pairs of insulated copper wires twisted around each other. It helps minimize electromagnetic radiation & the twisting helps resist external interference. It also helps to limit interference with other adjacent twisted pairs (Cross-talk).

Color coding of wire — It — Color wiring color codes are the wire's colors used to connect electrical devices & ckts. different colored wires have diff purpose. These codes help us to follow the safety rules.

Reasons for wiring color coding — i) It makes it easier & safer to connect electrical devices.

ii) To avoid mixing up of wires.

iii) By the color we can know it's func. of the wire

Evolution

According to the old standard color codes in India — i) Red color is used for live.

ii) Black — neutral

iii) Green — to protect the earth/ground.

New terminologies of Indian S.C.E.

For single-phase wire system

i) Brown color – live
ii) Blue – neutral
iii) Green – earth

For three-phase power supply

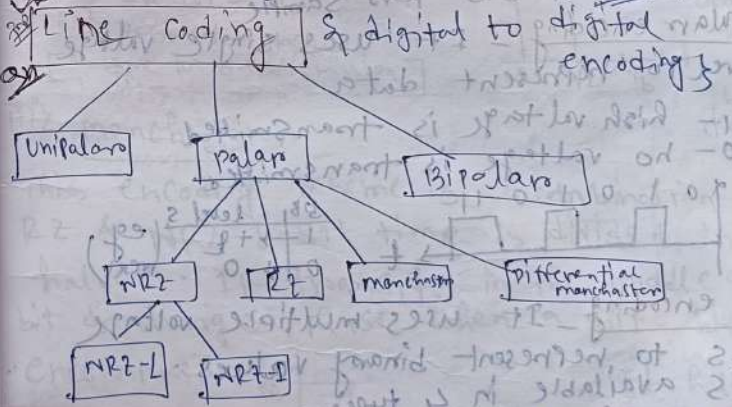
i) The combination of Red, yellow, Blue for the active power conductors.
ii) Black – neutral
iii) Green or Green-yellow – for protective ground.

Switching technique – In large networks, there may be more than 1 paths for transmitting data from sender to receiver. selecting a path that data must take out of the available options is called switching. There are 2 types of popular switching techniques:

i) Circuit switching – When a dedicated path is established for data transmission b/w sender & receiver, it is called circuit switching. When any network node wants to send data, be it audio, video, text or any other type of info, a call request signal is sent to the receiver & acknowledged back to ensure availability of decided path. This dedicated path is then used to send data. Eg – calling someone.

ii) Packet switching – As we discussed, the major problem with circuit switching is that needs a dedicated line for transmission. In packet switching, data is broken down into small packets with each packet having source & destination address, travelling from one router to next routers. Eg – multiple texting etc.

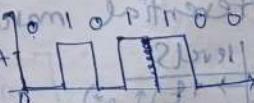
Line coding – (analog to digital & digital to digital encoding)



Line coding – It is defined as the process of converting binary data to a digital signal.

Binary data 0 1 0 1 1 0 0

Line coding →

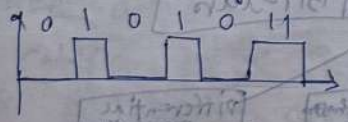


Characteristics – i) signal level & data level.
ii) pulse rate & bit rate } not taught needed
iii) DC component
iv) self synchronization

Pulse rate – It is defined as the no. of pulses per second & a pulse is defined as the min amount of time required to transmit a symbol.

Bitrate – It is defined as the no. of bits (s. If 1 pulse corresponds to 1 bit then pulse rate equals to bit rate. But if pulse carries more than 1 bit than pulse rate is lower than bit rate.
Bitrate = pulse rate × $\log_2 L$ = pulse rate × m
where, $L = 2^m$
m = no. of bits per sample

Unipolar encoding – It uses single voltage level to represent data
1 – high voltage is transmitted
0 – no voltage is transmitted

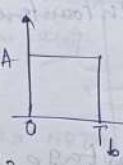


bits | levels
1 → +q
0 → 0
(eg next)

Polar encoding – It uses multiple voltage levels to represent binary values.
It is available in 4 types –
i) polar not return to zero (NRZ)
ii) Return to zero (RZ)
iii) manchester → Biphase
iv) Differential manchester

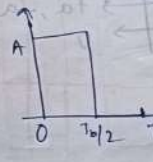
bits | levels
1 → +q
0 → -q
(eg right)

ii) NRZ – It uses 2 different voltage levels to represent binary values. It has 2 variants – i) NRZ-L (Level signals)
ii) NRZ-I (signals gets inverted)



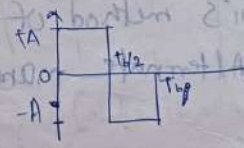
– within T_b, pulse not return to zero.

iii) RZ – Problem with NRZ is that receiver can not conclude when a bit ended & when next bit is started, in case sender & receiver's clock are not synchronized.
RZ uses 3 voltage levels
+ve val – 1
–ve val – 0
zero val – none
[0 = –ve to 0 transmission
1 = +ve to 0 transmission]



– Pulse occupies half of bit duration $T_b/2$

iii) manchester –
This encoding scheme is a combination of RZ & NRZ-L. Bit time is divided in 2 halves. It transits in the middle of the bit & change phase when a diff. bit is encountered.



– at half duration this is transition from high to low or low to high.

[For manchaster –
1 = –ve to +ve transition
0 = +ve to –ve transition]

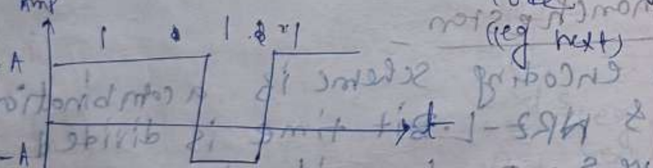
iv) **Differential manchester** – This encoding scheme is a combination of RZ & RZ-I. It also transmit at the middle of the bit but change phase only if 1 is encountered.
for this, 0 – transition
1 – No transition

Bipolar encoding – It uses 3 voltage levels, +ve, -ve, & zero. zero voltage represents binary 0 & bit 1 is represented by altering +ve & -ve voltages.

bits | levels
1 → +a, -a
0 → 0

There are 3 amplitudes in bipolar, so it is even reffered as pseudo ternary code. (eg next)

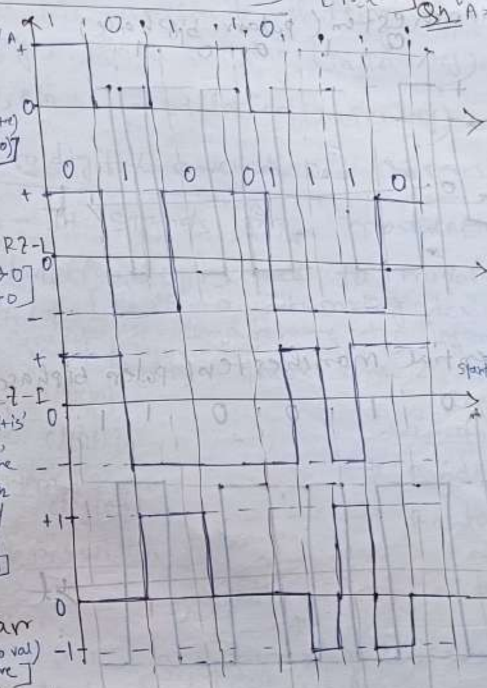
eg.



Here bit 1 is named as +a & -a alternatively, so this method of bipolar is reffered as Alternate marked Inversion (AMI)

① NRZ (not return to zero) [Polar] Qn [V = voltage, A = Amplitude]

Imp



Unipolar [1 – high val (+ve), 0 – No val (0)]

polar NRZ-L [0 ⇒ +ve → 0, 1 = -ve → 0]

Polar NRZ-I [1st bit as it is of NRZ-L, then if there is bit 1 then transmission change will happen]

[if 1st 1 then starts from -ve, after that if 0 – no change, if 1 (2nd) – then terminate 1st 1 & then start 2nd 1 from +ve (interchanging)]

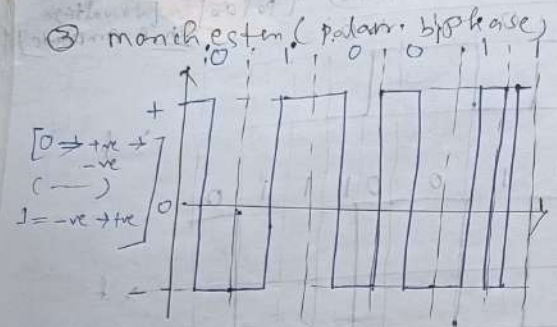
bipolar [0 → 0 (no val), 1 → +ve / -ve]

[if 1st 1 → (+)ve, 2nd 1 → (-)ve like this (interchanging)]

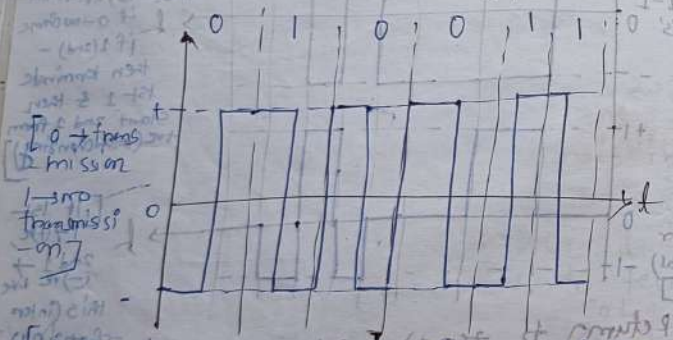
② RZ (Return to zero) [Polar]

③ [0 ⇒ -ve → 0 (at 1/2 it will return as polar)
1 = +ve → 0 (- - - -)]

③ manchester (polar biphase)



④ Differential manchester (polar biphase)



[1st will be as it is like manchaster but will be reverted i.e like RZ but as it is manchaster so, will not return to 0)

i.e for 1st 0 ⇒ −ve → +ve
1 = NO transmission (⊥)

then, 0 = transmission (⊓⊔)
1 = no transmission (⌐ ⌐)

i.e [from it that no transmission will happen interchangely (intently)]

Digital communication 1/3/24

Q.5) ASK, FSK, PSK amplitude shifting, frequency shifting, phase shifting. (In Prac copy)

Q.6) AM, FM, PM - (modulation) (In Prac copy)

• Analog to digital conversion

modem - It stands for modulation & demodulation. It is used to modulate & demodulate [] it is a networking device that is used to connect the computer to the internet where it converts data signals into digital & analog forms.

In physical layer there are 2 device →
" DLL (layer 2) → Bridge, switch
" Network (layer 3) → Router
Repeater
Hub

multilayer switch

it is a networking device that combines the functions of a traditional layer 2 switch with those of a layer 3 router. [on the other words, it is a computer networking device that switches on OSI layer 2 like an ordinary network switch & provides extra functions from higher OSI layers]

Sometimes multilayered switch acts as routers

Q.7) write short note on modem?

A modem is a computer hardware device that converts data from a digital format into a format suitable for an analog transmission [medium such as telephone

os radio. The term is short for modulator-demodulator. These are essential for connecting to the internet & for sending & receiving data over networks. It works by modulating digital signals into analog & demodulating analog back to the digital signals. This allows computers & other devices to communicate with each other. There are many diff. types of modems such as modems that uses cable tv lines to provide internet access (most commonly used), DSL modems etc.

Advantages
- ↑ signal can't be 0, if tensed to 0.
- Data = frames

i) connecting LANs with internet, ii) Providing secure connection, iii) converting d into a sig. & vice versa. Disadvantage - i) Lacking traffic maintenance, ii) lack of mobility, iii) dependence on service providers.

Diff. b/w repeaters & amplifiers.

↓ It regenerates the signal, it can't identify sig.

↓ It don't regenerate the sig. it amplifies the sig.

Repeater

1. It regenerates the signal, if the provided original signal is weak.
2. It takes high i/p power & provides low o/p power.
3. It is generally used in stationary environment.
4. Typically used for digital signals, such as ethernet (fibers optic signals.
5. Regenerates the original sig, removing any noise/interference.
6. Can extend the range of a network transmission to regenerate the signal.
7. More expensive than amplifiers.
8. Provides greater range & signal quality.

Amplifier

1. It increase the amplitude of the signal.
2. It takes low i/p Powers & provides high o/p power.
3. It is generally used in mobile & remote area network.
4. Typically used for analog sig-s, such as audio/video.
5. Amplifies the entire signal, including any noisy interferences.
6. It limited range, typically a few hundred feet or less.
7. Relatively inexpensive than repeaters.
8. Doesn't provide a greater range & signal quality.

Repeater → ▭ ← two port

If there are more than 1 sig-s it can't identify all signals. It is suitable for 1-to-1 comm. [1 data is coming & 1 is going]

(disadv.) ⇒ to overcome this problem Hub is generated.

It is a network node that amplifies & regenerates signals as they pass through a network. They are used to-

[i) Increase the network's reach
ii) Restore a damaged or weak sig.
iii) Service remote nodes.
iv) Repurpose a weak/broken signal.

It works by - i) Picking up a signal from the transmitter, ii) Amplifying it, iii) Transmitting it to the receiver, iv) changing the frequency of the channel, v) Amplifying the received input signal to a higher frequency domain so that it is reusable

Q:9) Reapeater V/s Hub.

Repeaters	Hub
① Defination	① Defination
② It has 2 ports	② It has multiple ports.
③ It addresses the incoming packet to another port.	③ It addresses the incoming packet to all other ports.
④ It amplifies & transmits the sig.s of incoming packets to the other side of the segments.	④ The data packets are received at the hub are forwarded to all the connected devices in the network.
⑤ Less intelligent device than hub.	⑤ It isn't considered as intelligent device.
⑥ It is expensive	⑥ It is less expensive
⑦ There are 2 types of repeaters Analog & digital repeaters.	⑦ There are 3 types of network hub – active, passive, intelligent hub.
⑧ Problem	⑧ Soln of the Problem

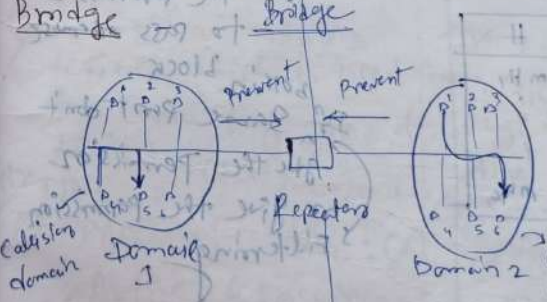
Hub - It is a networking device that connects multiple devices in a computer network. Hubs are also known as repeaters or concentrators. they are central connection point in [It's main func is to receive data signals from connected devices & broadcast them to all other connected devices. Each connected devices is on the same subnet & receives all data sent to the hub. They are less complicated than a switch, that can isolate data transmission to specific devices

shortnote

Quantization - While converting A to D. the final will be 0 or 1, is measured whether by quantization. Quantization in digital communication can be defined as the process of conversion of infinite continuous values into a set of discrete finite values. (Rest in Pen copy)

Amplifier - It is an electronic device that increases the voltage, current, or power of a signal. It is used in wireless communications & broadcasting, & in audio equipment of all kinds. there are multiple types of amplifiers voltage, current, Power, RF, audio, operational amplifiers (opg-amps) (egs) (Pen from diff.)

Bridge

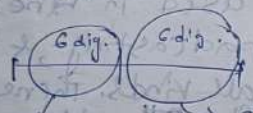


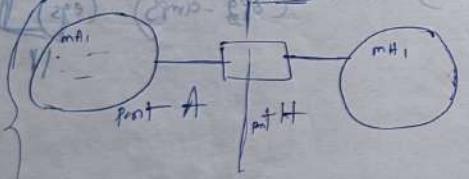
It is a device that connects multiple network segments into one. They are passive devices that operate at the d.l.l of the OSI model. the funcs of a bridge -

to reduce the collision/ break the collision domain filtering is needed, that's why bridge is needed.

i) Connecting networks.
ii) Extending a network's physical size.
iii) Storing MAC addresses
iv) Data load filtering.
v) Preventing looping problems. There are 2 common models of bridging local & remote
① Local bridging - Bridges link LAN switches with local cables. ② Remote bridging - Bridges connect via a WAN.

MAC address - 48 bit binary address representation by 12 hexadecimal no. (Physical)





A	H
MA1	mH1
MA6	mH6

Source destination
If S & d is diff. it should give the permission to pass otherwise block.
If same port don't give the permission
Filtering

9/3/24

Diff b/w hub & switch

Hub	Switch
① Layer - Physical layer. Hubs are classified as layer 1 devices per the OSI model.	DLL layer [network switches operate at layer 2 of the OSI model]
② Data transmission form - Electrical signal/bits	NO ③F ③STP
③ ports - 4/12 ports	③F ③ STP Frame(L2 switch) Frame & packet (L3 switch)
④ Device type - Passive device (without S/W)	It is multi port bridge. 24/48 ports.
⑤ Transmission type - may be unicast, multicast/broadcast.	Active device (with S/W) & network device.
⑥ Func - To connect a network / personal computers together, they can be joined through a central hub	First broadcast, then unicast & multicast as needed.
	Allow to connect multiple device & port can be arranged & can create security also

Hub v/s Bridge

Hub	Bridge
① It is a network device which is used for connecting no. of device. (def)	① It is also a network device which is used to connect 2 diff LAN working on same protocol (def)
② Types - 2	② Types (bridging) - 3.
② Types of hub: (2) Active & passive.	② Types of bridge: (3) Source route, transparent & translation
③ It doesn't perform data filtration.	③ It performs data filtration.
④ There are multiple ports are used in hub.	④ ~~While bridge performs~~ But in bridge

port for incomming & another port of outgoing.

(5) ~~They con~~ It connects the LAN's segment.

(4) It connects 2 diff. LAN working on same Protocol.

(6) It operates on the physical layer of OSI model.

(6) It operates on the d.l.l. of the OSI model.

Q.12) Bridge v/s switch

S/W driven — Hardware driven

Switch	Bridge
(1) Defination	(1) Defination
(2) It can have a lot of ports	(2) It can have 2/4 ports only
(3) ~~No filtration~~ 3F property	(3) ~~Filtration~~ No 3F property
(3) It performs the packet forwarding by using hardwares such as ASICS hence it is hardware based.	(3) It performs the packet forwarding by using S/W so it is S/W based.
(4) The task of error checking is performed by ~~S~~ a switch.	(4) A bridge can't perform the error checking.
(5) It has buffers.	(5) It may not have a buffer.
(6) The switching method in case of a switch can thus be store forward, fragment free/cut through.	(6) The ~~bridge~~ switching method in case of a bridge is store & forward.
(7) STP	(7) NO STP

Switch's func

FFF → Filtering → flooding → 3F function
↓
forwarding

Hub doesn't have FFF.

multiple Communication can be done with the same domain. switch can break the collition domain too.

Q.13) What do you mean by the 3F function of switch?

3F stands for FFF where 1st F means forwarding 2nd F means ~~floating~~ flooding & 3rd F means ~~function~~ filtering

- table created by the bridge = MAC table
- " " switch = CAM " (Content addressable table)

multilayer switch — will work as both switch & router (prov)

Switch — Spanning tree protocol (STP) (prov from diff.)

Device (Lim) forwarding

— It is a very famous algo of switch. STP works in DLL to overcome the loop / looping problem.

A switch is a component that can connect / disconnect the conducting path in an electrical ckt. Switches can either complete / break an electric ckt, allowing / preventing current to flow through it. It can be used for many diff. purposes;

① It can be used for industrial equipment,
② It ... consumer & commercial devices,
③ ... in the networking to receive incoming data packets & redirect them to their destination / ...
④ It can be found beneath each key on a computer keyboard.

Diff. types of switches include - ① SPST-NO (single pole single throw normally open) ② SPST-NC (Single pole single Throw normally closed)

What do you mean by TTL = 255

ⓐ short note on TTL.
It stands for time-to-live. It is a numerical value that indicates how long data should be valid & available before a computing system discards it. [In networking, TTL prevents data packets from moving across the h/w indefinitely. In applications, it manages data caching & improves performance.

[TTL logic is a digital logic design that uses bipolar junction transistors to act on direct-current pulses. TTL gates are made up of at least two transistors & other components such as resistors & diodes.] → Transistor-to-transistor logic (TTL)

TTL = time to live
↓
The time that which the following will be activated

Pkt
Error detection methods -

Error → single bit / burst (multiple bit)

i) Parity check — we can set it by even parity / odd parity
i.e. if even parity write 1 or 0 acc to the 1 or 0 Parity

0 1 0 1 1 0 1 0

Parity check → even parity (error)

ii) CRC check
iii) Hamming code [It is error correction method]
iv) LRC (Longitudinal Redundancy Check) etc.

Parity check - It parity check is a method that detects errors & checks the Integrity of data. It parity check works by adding an extra bit, or a parity bit, to each data unit the receiver agrees to use the same even / odd parity bit scheme as the sender. It is not an infallible error checking method. For eg it's possible that 2 bits could be in error in a transmitting, offsetting each other. (like eg)

CRC cyclic redundancy check - Remainder Part & data part are send to the receiving section. If the receiving section is same, the ... is same.

It is an error-detecting code (used in digital networks & storage devices) to detect accidental changes to digital data. It is a mathematical technique that provides a way to detect errors in transmitted data by appending a special code, called a checksum, to the original information.

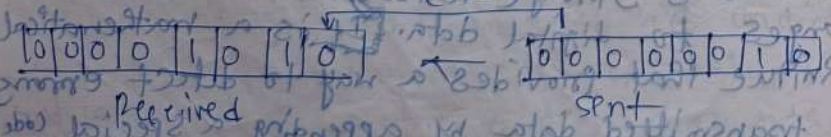
This checksum is then recalculated at the receiving end to verify the integrity of the data. It is used in a variety of networking protocals, including ethernet, TCP/IP etc. They are also used in storage devices.

Hamming code - It is a network technique that detects & corrects errors, in data transmission b/w network channels. It is a forward errors correction (FEC) technique that's used when consistency is more important than transmission efficiency. It can detect upto 2 errors & correct one errors per word. It is commonly used in errors correction code (ECC) RAM.

Redundant bits - This are extra binary bits that are generated & added to the information carrying bits of data transfer to ensure that no bits were lost during the data transfer.

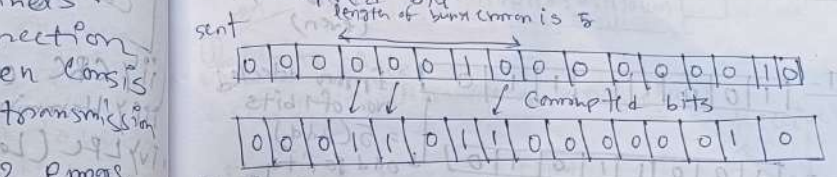
Errors → single-bit error
→ Burst errors.

(1) Single bit error - The only 1 bit of a given data unit is changed from 1 to 0 or from 0 to 1.



(2) Burst error - The two / more bits are changed from 0 to 1 or vice versa is known a burst error.

The length of a burst error is determined from the first corrupted bit to the last corrupted bit.



- A Parity bit is a check bit which is added to a block of data for error detection purposes. Parity is of 2 types -

(1) Even Parity - Here the total no. of 1 bits in the message is made even.

(2) Odd Parity - Here the total no. of 1 bits in the message is made odd.

Error detection by adding Parity bit

Sender's end - While creating a frame, the sender counts the numbers of 1s in it & adds the parity bit in following way,

In case of even parity, If no. is 1s / 0s

Data frame -

Frame with even parity bit

Frame with odd parity bit: 1 0 0 1 1 0 1 1

Eg-②

Received frame

Case I - 1 0 0 1 1 0 1 0 — no error, no. of 1 bit = 4 (even)

Case II - 1 0 0 1 1 1 1 0 — Error detected, no. of 1 bits = 5 (odd), odd parity

Case III - 1 0 0 1 1 0 1 0 — Failure to detect error, no. of 1 bits = 4 (even)

- We can add parity bit to the LSB/MSB. Even parity

[① It is actually multiple bit error

③ Burst error — 2 or more consecutive bits in the data unit have changed from 1 to 0 & 0 to 1

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

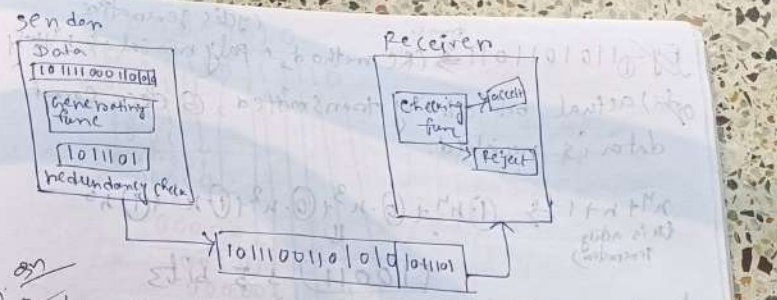
corrupted bits

0 1 0 1 1 0 1 1 1 0 1 0 0 1 1]

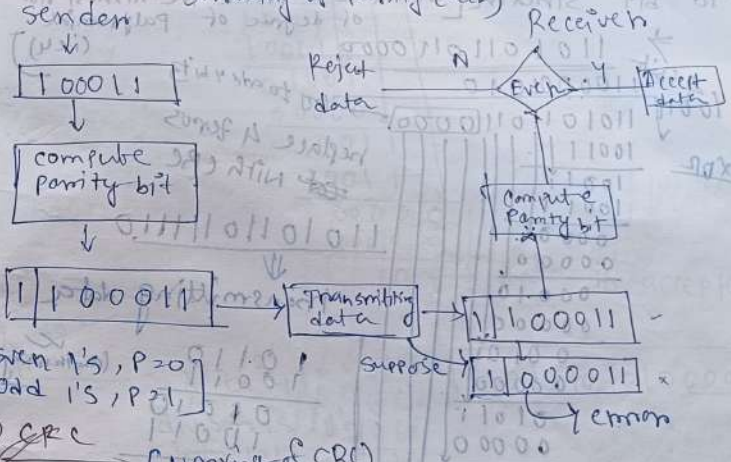
(*) Error detection method) the base is

Redundancy & correction — It is the main base of error detection technique. Redundancy means group of bits adding to end of data unit. If we can send the full 8-bit/16 bit then there is no chance of error, but as we can't do that, we always have to send redundancy bits

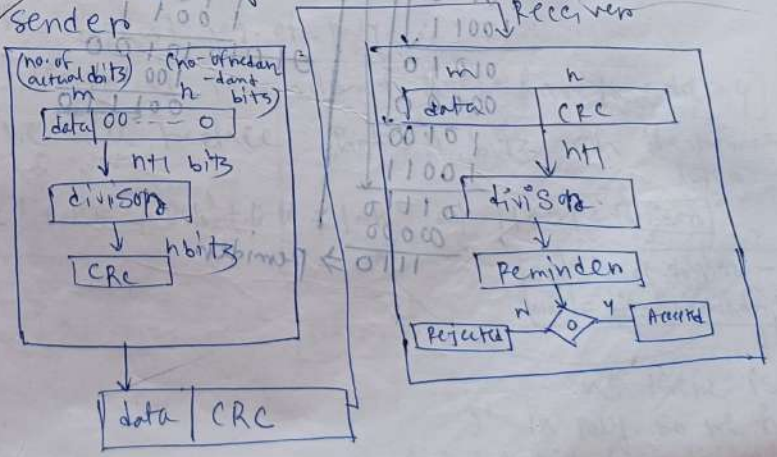
error occurs.



① Parity check — (working of parity check)



② CRC — (working of CRC)



Eg - (1) 1101011011 ⇒ trans. by CRC method, cyclic generative polynomial ⇒ x^4+x+1

Q(a) actual bit string transmitted, (b) check correct data is received.

$x^4+x+1 \Rightarrow (1)x^4 + (0)\cdot x^3 + (0)\cdot x^2 + (1)x^1 + (1)x^0$ (it is actual generator)

⇓

10011 → 5 bits

⇒ So, a string of 4 zeros is appended to bit stream [we have append the highest no. of degree of polynomial (i.e 4)]

⇒ 11010110110000

```
       1100001010
10011 ) 1101011011 0000   → try to add 4 bits
XOR     10011
         10011
         10011
          00001
          00000
           00010
           00000
            00101
            00000
             01011
             00000
              10110
              10011
               01010
               00000
                10100
                10011
                 01110
                 00000
                  1110 ⇒ remainder
```

replace 4 zeros with CRC

11010110111110

⇓

transmitting data

```
10110
10011
01010
10011
11001
10011
0101010100
 100 ...
 001110
```

```
       1100001010
10011 ) 11010110111110
        10011
         10011
         10011
          00001
          00000
           00010
           00000
            00101
            00000
             01011
             00000
              10111
              10011
               01001
               00000
                10011
                10011
                 00000
                 00000
                     0 → data is accepted
```

(2) Q2

Polynomial - x^4+x^3+1 ; 11001) 1010101010 0000

division is lying into this polynomial

The highest deg. of poly = 4

∴ The no. of redundant bits we have to add = 4

[we will replace that 4 bits with the remainder later]

$1\cdot x^4 + 1\cdot x^3 + 0\cdot x^2 + 0\cdot x + 1\cdot x^0 \Rightarrow 11001$ ← divisor

No. of bits of divisor − 1 = no. of redundant bits to add

as there is a '1' in poly. So we have to '−' 1 bit from divisor to get no. of r. b.

Other way,

```
1001 ) 1010101010000
       1001
       ------
        0111000
         1001
        ------
        00001101 0
             1001
        ------
             1100 1
             1001
        ------
             00011000
                 1001
        ------
             000010   (from LSB 4 bits)
```

↳ (As 4 redundant bits, so taking 4 bits for replacement)

⇓

```
1100 ) 10101010101 0010  ← valid data code word
       1100 1
       ------
       011000
        1100 1
       ------
        0000110 10
            1100 1
       ------
            000110 01
                1100 1
       ------
            00000 0  → rem 0 (no error in data is accepted)
```

[If any error then rem will not be 0, then we need to understand there is an error & data will be rejected]

[efficiency = $\frac{10}{14} \times 100$ → actual data bits; 14 → full data (wrtn)

↳ or channel utilization for sending message]

Not needed

Q5

Hamming code (working of hamming code with eg)

If hamming code is of 7 bits, then 4 bits are for data & 3 bits are for parity

Position	7	6	5	4	3	2	1
bit	d_3	d_2	d_1	P_2	d_0	P_1	P_0

→ 7 bit data: 3 - P, 4 - d

the pos. of parity bits 2^n is calculated by

2^n where $n = 0, 1, 2$ ($2^0 = 1$, $2^1 = 2$, $2^2 = 4$)

For eg, 11 bit data

11	10	9	8	7	6	5	4	3	2	1
d_6	d_5	d_4	P_3	d_3	d_2	d_1	P_2	d_0	P_1	P_0

4 – P, 7 – d

⇓ can also represent it by like this

d	d	d	r8	d	d	d	r4	d	r2	r1

For more than 7 bit this is the for.

- P_0 | r_1 = 1, 3, 5, 7 … → 1 pick, 1 leave
- P_1 | r_2 = 2, 3, 6, 7, 10, 11 → 2 pick, 2 leave
- P_2 | r_4 = 4, 5, 6, 7 → 4 pick, 4 leave
- P_3 | r_8 = 8, 9, 10, 11, 12, 13, 14, 15, 16

→ 4b data, 1010 ($d_3\ d_2\ d_1\ d_0$)

for this,

1	0	1	0	0	1	0

$P_2 = d_3 \oplus d_2 \oplus d_1$

$P_1 = d_3 \oplus d_2 \oplus d_0$

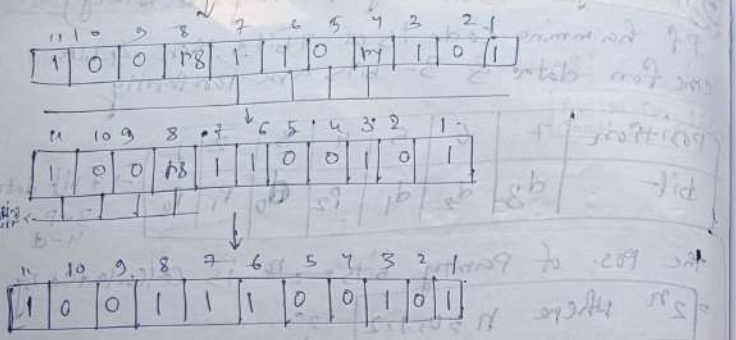
$P_0 = d_3 \oplus d_1 \oplus d_0$

→ 7 bits, data = 1001 1011 1

for this,

11	10	9	8	7	6	5	4	3	2	1
1	0	0	r8	1	1	0	r4	1	r2	r1

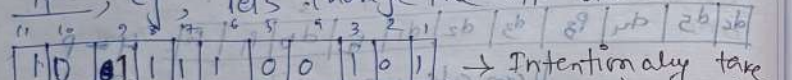
11	10	9	8	7	6	5	4	3	2	1
1	0	0	r8	1	1	0	r4	1	r2	1



O/P data = 10011100101

Error detection & Correction through hamming code

Now if, there is an error it will detect it; eg, lets change the o/p bit-



→ Intentionally take 1 instead of 0.

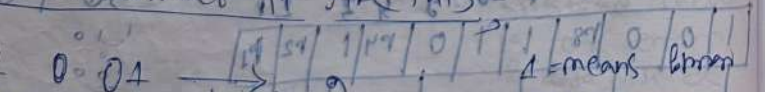
Now calculate r_1,

$r_1 = 1$

Now, 1110 (1) → no of 1's 5 (odd parity), but we are working on even parity so the LSB should be '0' not 1, so there is an error

[or [my method] → only by without counting it self) see we are getting 0, but at o/p the r1 is '1' so there is an error]

Now it will correct it like this-



1 0 01 → decimal 9

1 = means Error
0 = No Error

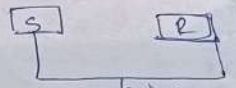
It means there is 9th error in the bit. And we know the 9th bit should consist 0, but we intentionally changed it into 1.

So, after recognizing the errored bit it will correct by either by converting it 1 → to 0 or 0 → 1. Here we know, at 9th bit we have 1 that is an error. so it will convert it into 0. So, the correct o/p now = 10011100101

(2)

15|3|24

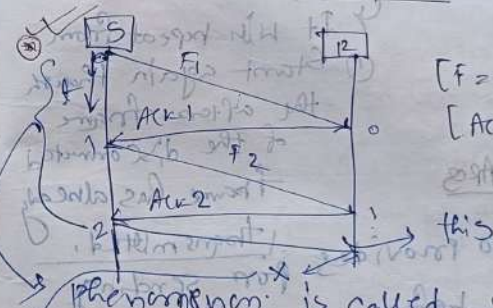
Flow control - It is design issue at D.L. It is a technique that generally observes the proper flow of data from sender to receiver.



(wire has capacity)

D.D.L. → device → frame

Flow control mechanism

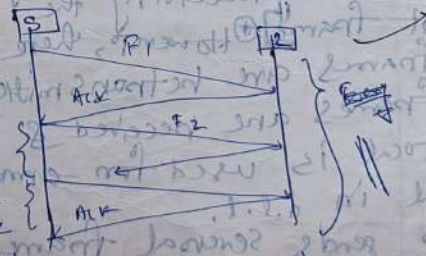


[F = Frame]
[ACK = Acknowledgement]

this is a quite good method.

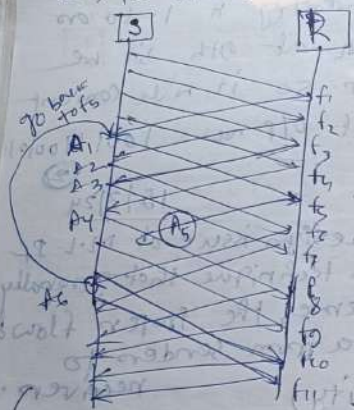
phenomenon is called - **Stop & wait ARQ**

(Advantages & disadvantages & incurtetheat)



Until & unless it receive the ack it will continue the frame at next time (Stop & Wait ARQ). [But we can't waste our time]

So, to overcome the problem,



→ communication is bidirectional ⇄ 2 way

→ Go back N ARQ

(Advantage & disadvantage)

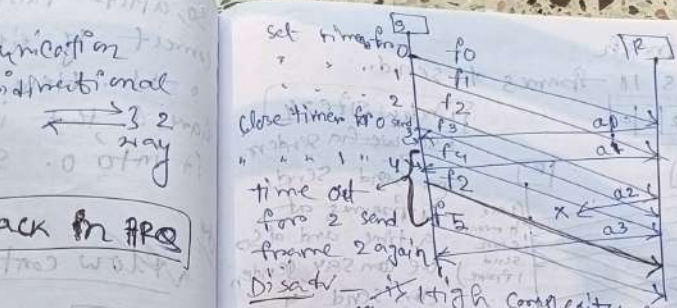
① It isn't waiting

② It will repeat from the after frame of the disconnected frame has already transmitted.

Selective repeat ARQ

This protocol also provides for sending multiple frames before receiving the ack for the first frame. However, there only the lost frames are retransmitted while the good frames are received & buffered. This protocol is used for error detection & control in d.l.l.

* Here, the senders sends several frames specified by a window size even without the need to wait for individual ack from the receiver as in Go-Back-N ARQ. Here, the retransmitted frame is received out of sequence.



Adv — i) Efficient retransmission of lost packets.
ii) Helps in reducing network delay (fast process)
iii) Provides high throughput

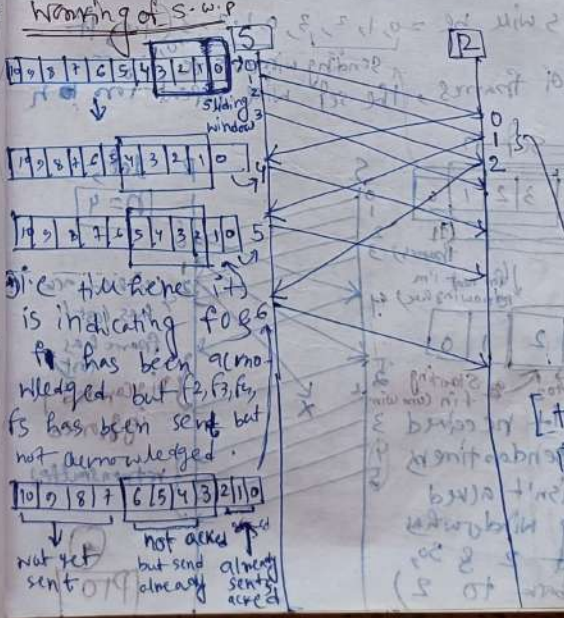
Disadv — i) High complexity & difficult to implement.
ii) May increase packet waiting time.
iii) Requires more buffering on both the senders & receiver sides.

Sliding window protocol

Go Back N ARQ
Selective Repeat ARQ

Here, the sender can send multiple frames at a time.
i) No. of frames to be sent is based on window size.
ii) Each frame is numbered → sequence number. which we call as

Window size = 4
(i.e, 4 frames can be sent at a time & can be sent before expecting an ack)



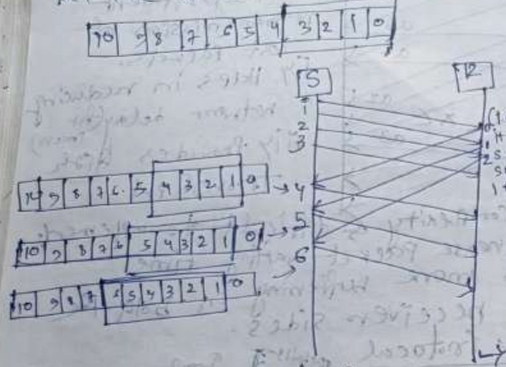
i.e till here it is indicating f0 has been acknowledged, but f2, f3, f4, f5 has been sent but not acknowledged.

not yet sent
not acked but send already
already sent & acked

* this sentence is the same as * is indicating 0, 1 has been received but 2, 3, 4, 5 has not been acknowledged, but they have been sent

that sliding window is basically marking the unacked & acked frames

Let the sender has 11 (↓ fresh) frames to send.



Window size = 4 (so we the sender can send 4 frames at a time, and also we can say sender can send 4 frames before expecting an ack)

like that
↳ to be continued ||

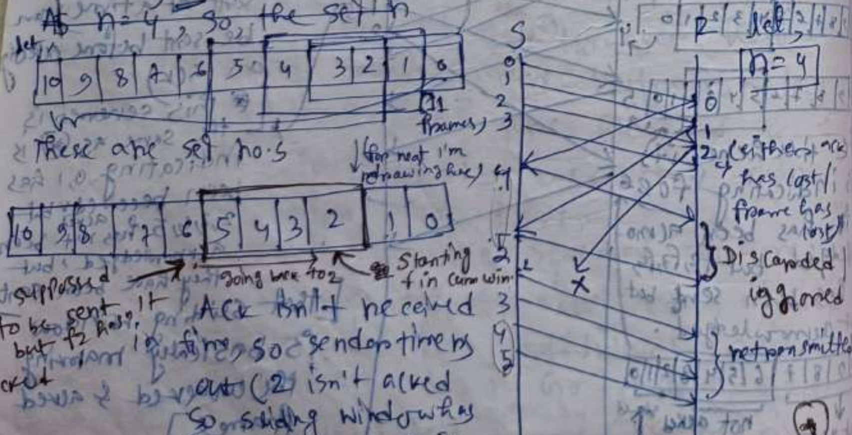
GO-BACK-N ARQ Protocol

'N' is the senders window size (i.e., N frames can be sent at a time before expecting an ack from the receiver)

For eg, if sending window size is 4 (2^2), then 2 will be the no. of bits in the sequence number (i.e., 00, 01, 10, 11) → 0, 1, 2, 3 (in decimal)

∴ the set of no.s will be = 0, 1, 2, 3, 0, 1, 2, 3 (i.e. if sending window size is 4, & we have N no. of frames, the set will repeat for n times) ||

As n = 4, so the set is



[suppose 2 sent to be sent but 2 hasn't acked] It ACK isn't received in time, so sender's timer out (2 isn't acked)

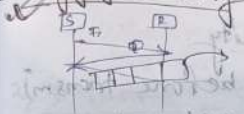
[So sliding window has stucked at 2 & so, the sender is now going back to 2)

PTO

• ACK contains a number that is 2 [it implies that 1 is successfully received & I'm waiting for 2] ↓ But is the real. [if one 50% or another percentage (i.e. some data has been lost in way)

Here a replication of acked frame is also sent to the sender to know that no data has been lost on the way

Piggy-backing ← to overcome this problem

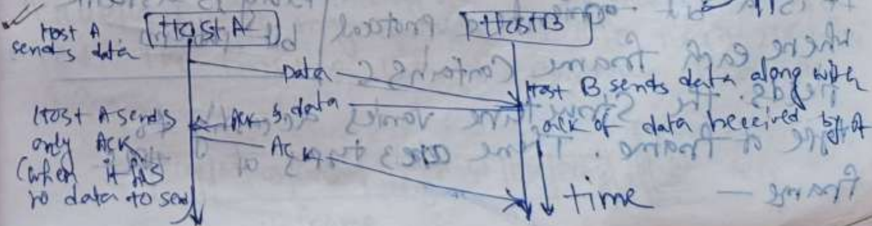


copy from the receiver to make ensure that all the data has been successfully received.

[It is a cybersecurity term that describes using a wireless network without the authorization of its administrators.

1 way to achieve full-duplex transmission is to have 2 separate channels with 1 forwarding data transmission & the other for reverse data transfer (to accept). But this will almost completely waste the bandwidth of the reverse channel. ||

[to overcome this, a preferable solution would be to use each channel to transmit the frame both ways, with both channels having the same capacity. Assume that A & B are interconnected with the ack from A to B & can be identified as a data frame / ack by checking the sort field in the header of the received frame.] ||



Adv - 1) The major adv of it is the better use of available channel bandwidth (B.W). [This happens because an ack frame needs not be sent seperately].
2) Usage cost reduction
3) Improves latency of data transfer.
4) To avoid the delay & rebroadcast of frame transmission, it uses a very short duration timer.

Disadv - 1) Additional complexity
2) If the d.l.l waits long before transmitting the ack, the frame will rebroadcast.
3) Blocks Ack for some time.

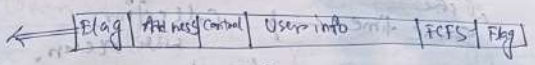
HDLC (High level data link control)

Bit oriented protocol
Has 3 types of frames (S, U, I frame)
Briefly describe about various types of frame in HDLC,
S → Supervising frame (used for only for transmit/retransmit purpose)
I → Information frame (used for user data & control info)
U → Unnumbered frame (Used for system management or reserved for)

HDLC Stands for High level data link control.
It is a bit-oriented protocol where each frame contains 6 fields. The structure varies according to type of frame. There are 3 types of HDLC frame —

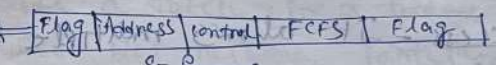
Flag is a specific bit pattern.

1) I-frame - I-frames / Information frames carry users data from the network layer. They also include flow & error control information [that is piggybacked on user data]!! the first bit of control field of I-frame is 0.



I-frame

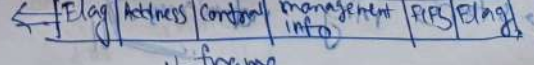
2) S-frame - S-frame stands for supervising frames. These frames are basically referred & essential for error control & flow control. They also provide control info. It contains / includes only ack no. number. First 2 bit of this frame of control field is 10. It doesn't have any information fields. It contains send & receive sequence no.s.



S-frame

Eg - Receive Ready (RR), Receive Not Ready (RNR), Reject on frame N(R) (REJ), selective reject on N(R) (SREJ) etc.]

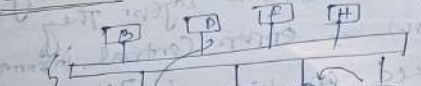
3) U-frame - U frames or Un-numbered frames are used for control purposes & they aren't sequenced. It may contain an info field, if required. The first 2 bits of control field of U-frame is 11.



U-frame

Eg - SNRM, UP etc

Channel - It means where it is the medium through which the data flows between transmitter & receiver i.e data transmission happens.



at the same time → Collection with accn.

(It is case of multiple access)

It is very essential problem in CN.

[It is a model for interprocess communication & synchronization via message passing, on a specific frequency or band of frequencies used for communication. channels can vary in size, such as 5m Hz, 10m Hz, 20 m Hz] the wider the channel, the more data it can carry.

multiple access - It allows multiple terminals to share a communication medium such as a wired cable / wireless spectrum. this allows the terminals to transmit over the medium & share its capacity. It is essential for maintaining successful communication among multiple devices. [It is based on multiplexing, that is provided in the physical layer. the shared communication medium can be Bus networks, wireless networks etc, & token ring networks.]

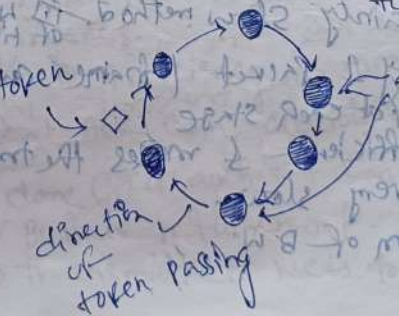
Ex Eg - ALOHA, CSMA/CD etc.

Write short note on token ring

All short notes with diagram.

It will capture the NIC & connect with it. token, it is traveling through the network.

A token ring is a computer n/w configuration that connects each computers to the next one in a closed ring, also known as a star topology & pass one or more tokens from host to host. A token is a frame of data transmitted b/w network points. [only a host that holds a token, is a frame of data transmitted b/w network points] only a host that holds a token can send data, & tokens are released when receipt of the data is confirmed. IBM developed token ring technology in 1980s as an alternative to ethernet.



Flow control mechanisms

Stop & wait ARQ - It provides unreliable and data transmission with flow control & error control mechanisms, appropriate for noisy channels. The sender keeps a copy of the sent frame. It then waits for a finite time to receive a positive ack from receiver. If the time expires the frame is retransmitted. If a positive ack is received then next frame is sent.

Here, the sender waits for an ack after every frame it sends.

When ack is received then only next frame is sent. The process of alternately sending & waiting frame continues until the sender transmits the EoT (End of transmission) frame.

Adv - i) It is very easy & simple & each of frames is received & acknowledged well.
ii) It is also very accurate.

Disadv - i) this is fairly slow method. It waste of time.
ii) In this only 1 packet frame can be sent at a time at each stage.
iii) It is very inefficient & makes the transmission process very slow.
iv) poor utilization of B.W.

Go-Back-N ARQ - It is a type of ARQ (Automatic repeat request) protocol that allows a senders to send multiple frames to a receivers without receiving an ack packet from the receiver first. It uses the concept of sliding windows, & so is also called Sliding window protocol. The frames are sequentially numbered & a finite no. of frames are sent. If the ack of a frame is not received within the time period, all frames starting from that frame are retransmitted.

Working - i) The sender sends a no. of frames specified by a window size.
ii) The sender goes back N places from the (last transmitted packet in the unacknowledged window)
iii) The sender continues to send frames without receiving an ack packet from the receiver.

Adv
- i) It doesn't wait for receiving the ack.
- ii) The sender can send many frames at a time.
- iii) Timer can be set for a group of frames.
- iv) Efficiency is more.
- v) 1 Ack can acknowledge more than 1 frame.

Disadv
- i) done if an ack hasn't been received for 1 frame the good frames are ignored & retransmitted again that's wastage of b/w/frames.
- ii) Buffers requirement.
- iii) transmitter needs to store the last N packets.

S.W.P
Selective Repeat ARQ

In Go Back N ARQ the sender sends the all frames in the current window, if the ack of a frame isn't received within an agreed upon time period. (the 1st frame of the curr. wdw. is the un-acked but sent frame, as while sliding the curr. wdw has stucked at the un starting from the un-acked frame & it got stucked as that frame hasn't acked) ||

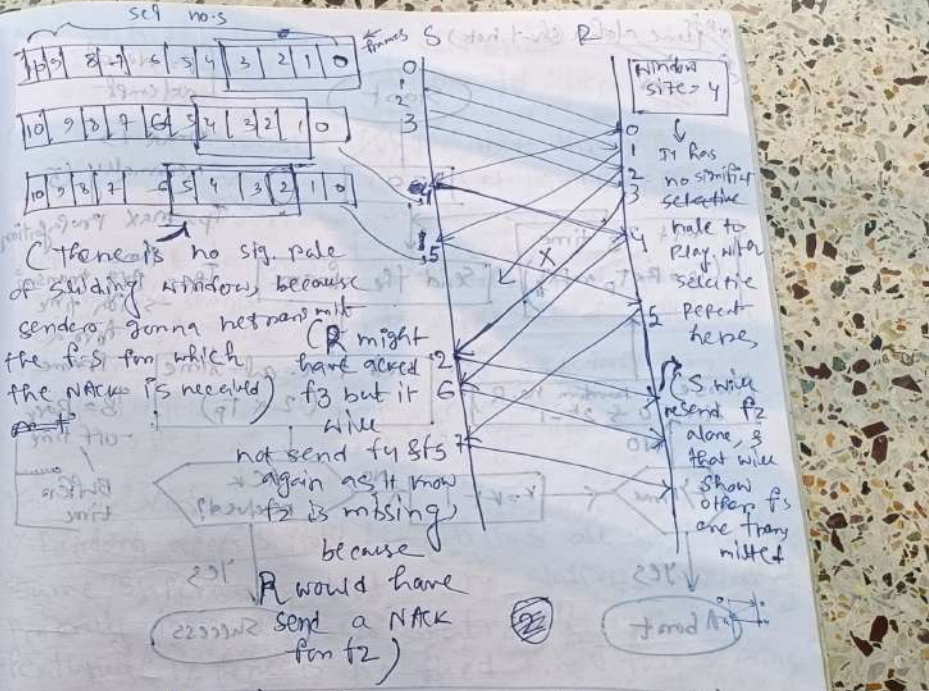
I.e. if a frame/ack has lost all the frames of current window are retransmitted in Go-Back-N ARQ, whereas,

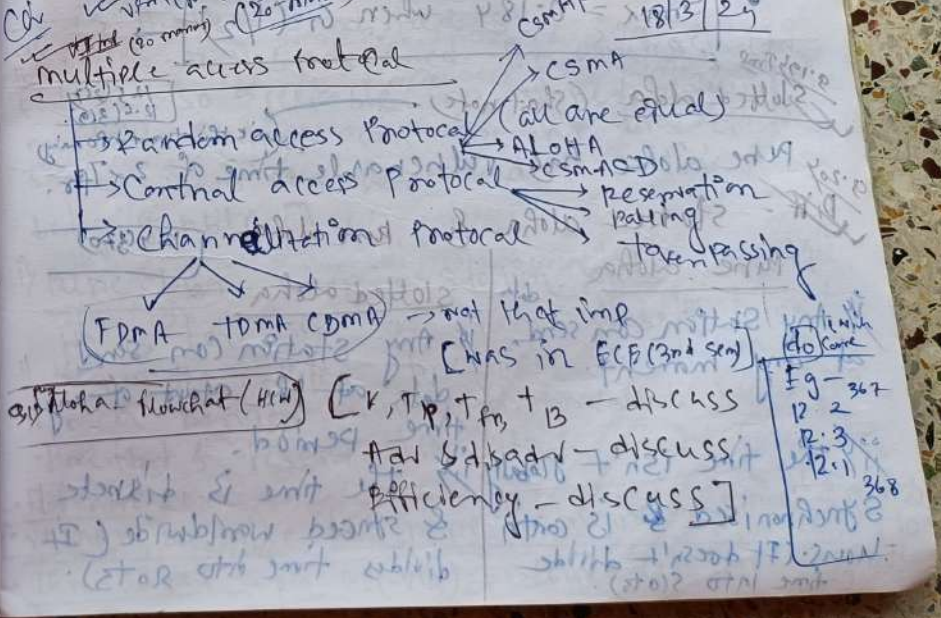
i) In selective Repeat ARQ only the lost ~~(stucked frame)~~ erroneous (lost acked frame) are retransmitted, while correct frames are received & buffered.

ii) the receiver while keeping track of seq no.s, buffers the frames in memory & sends NACK (neg Ack) for only frame that is missing / damaged.

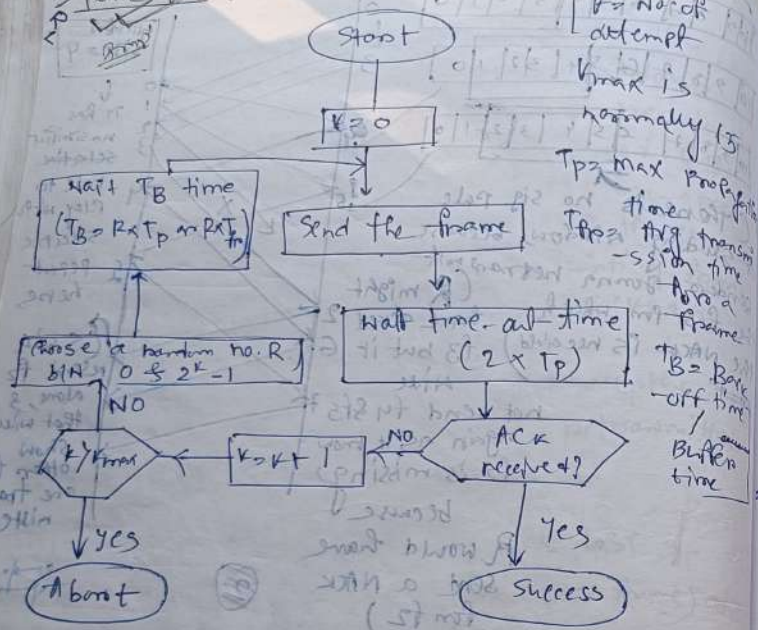
∴ no of retransmission < no of retransmission in selective repeat ARQ in G.B.N

iii) The sender will send/retransmit Packet/Frame for which NACK is received.





Pure aloha (short note)



K = No. of attempt
K max is normally 15
T_p = max Propagation time
T_{fr} = Avg transmission time for a frame
T_B = Back-off time
Buffer time

- $S_{max} = 0.184$ when $G = (1/2)$

Slotted aloha (short note)

Pure aloha has vulnerable time of $2 \times T_{fr}$.

Diff - slotted aloha & pure aloha

Pure aloha	slotted aloha
any station can send data at any moment.	any station can send data at the start of any time period.
time isn't globally synchronised & is continuous (It doesn't divide time into slots).	the time is discrete & synced worldwide (It divides time into slots).

vulnerable time for collision to occur = $2 * T_t$

the max throughput occurs at $G = 1/2$ & is 18.39%.

At light load, there will be no chance of collisions in pure aloha.

more collisions.

less efficient than slotted a.

vulnerable time for collision to occur = T_t

The max throughput occurs at $G = 1$, & is 36.79%.

At light load, there will be a chance of collisions.

Less collisions than pure aloha.

more efficient than p a.

multiple access

Random access protocol - In this all stations have same superiority that is no station has more priority than another station. It has 2 features. i) there is no fixed time for sending data ii) no fixed sequence of sending data. It is further to subdivided as:

a) Aloha - It was designed for wireless LAN but is also applicable for shared medium (Here multiple stations can transmit data at the same time & can hence lead to collision & data being garbled).

i) Pure aloha - when a station sends data it waits for an ack. If ack doesn't come within the alloted time then the station waits for a random amt of time called back-off time (T_b) & resends the data.

- Flowchart - done
- vulnerable time - $2 * T_t$ (Frame transmission time)
- Throughput - $G e^{-2G}$ -> (efficiency)

G = no. of stations willing to transmit data

• max throughput - 0.184 for G=0.5

Adv - i) simple protocol, ii) minimal overhead, iii) simple n/w, iv) immediate data transmission, v) low latency requirements.

Disadv - i) inefficient, ii) high probability of collisions iii) data frame hitting, iv) data frame can be lost.

Efficiency - $S = G \cdot e^{-2G}$

ii) slotted aloha - It's similar to Pure aloha, except that we divide time into slots & sending of data is allowed only at the beginning of these time slots. If a station misses the allowed time, it must wait for the next slot. This reduces the probability of collision.

• Vulnerable time - Frame transmission time

Throughput $S = G \cdot e^{-G}$ → (efficiency)]

• max throughput - 0.368 for G=1

Adv - i) simple protocol, ii) single active node can continuously transmit at full rate of channel, iii) highly decentralized (only slots in nodes need to be sync) iv) less collision than pure aloha.

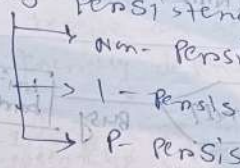
Disadv - i) collisions, wasting slots, ii) Idle slots, iii) clock synchronization, iv) nodes may be able to detect collision in less than time to transmit packet.

t_p - the time taken by the last bit in a frame to reach frame 1 side to the other.

t_{fr} - the time taken to send a frame. It is generally 2056 bits / 200 kbps / 1ms. [min frame transmission time = $2 \times t_p$ = 51.2 µs]

b) CSMA (Carrier sense multiple access)

• It has persistence methods

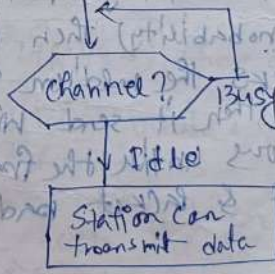


1-persistent - It stands for carrier sense multiple access. It ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However, there is still chance of collision in CSMA due to propagation delay.]

Adv - i) Helps to prevent data collisions, ii) thanks to feedback, no data is unnoticeably lost, iii) Avoids unnecessary data traffic, iv) It is flexible, v) cost effective

Disadv - i) It has limited scalability, ii) It has high power consumption, iii) not suitable for long distances etc.

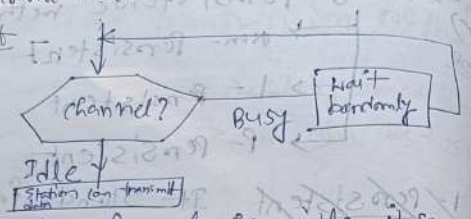
Briefly describe i) Non, P-Persistent methods with 1-Persistent



Here stations nodes senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle & transmits unconditi-

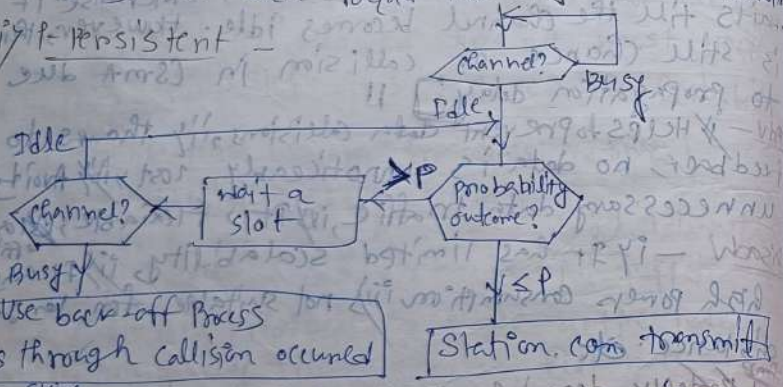
onally (with 1 probability) as soon as the channel gets idle. Eg - Ethernet network

i) Non-Persistent



Here stations the node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) & transmits when found idle. Eg - Home automation

ii) P-Persistent -



- The stations node senses the medium, if idle it sends the data with p probability. If the data isn't transmitted ((1-p) probability) then it waits for some time & checks the medium again, now if it is found idle then it send with p probability this repeat continuous until the frame is sent. It is used in wifi & packet radio systems.

Eg - wifi network

• TB — It is the random amount of time a station waits before resending a frame after it doesn't receive an ack within the specified time. It generally depends on ki

Imp (Exam - In either this) (Wired network) 12.10 (3+2)

CSMA (CD - Carrier sense multiple access with collision detection stations can terminate transmission of data if collision is detected.

• Efficiency — suppose, station A transmitting data but collision & the worst-case time wasted is $2T_p$ & then some station B found out a way to transmit the data so it took - [Tp (Propagation delay) + Tt (transmission time)]

$$\text{Efficiency} = T_t / (C * 2 * T_p + T_t + T_p)$$

[considering the worst case to be of n contention slots]

T_t → transmission time

T_p → propagation time

C → no. of collision

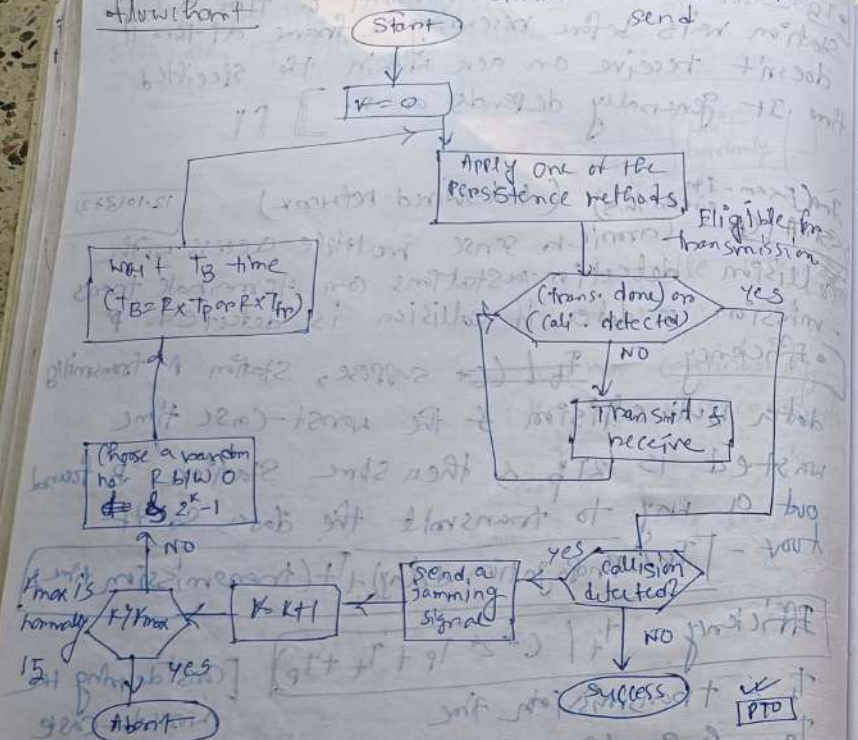
Condition to detect collision = [Transmission delay ≥ 2 * Propagation delay]

$$\text{Efficiency} = 1 / (1 + 6.44a) \quad \text{where } a = T_p / T_t$$

Now - Less collision occured compared to CSMA/CD Transmission on demand.

• Disadv - Unknown delay when more nodes are connected Wasted time exists due to collisions, [but better performance & wasted time compared to CSMA.]

flowchart



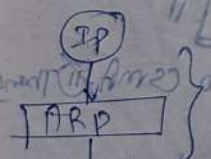
14/4/20

ARP shortcut

when IP known, mac = unknown then ARP.

[IP = Real name (eg), MAC = Nickname (eg)]

ARP = Address resolution protocol.



mapping

ARP request = Broadcasting
ARP response = Unicasting

RARP (Reverse ARP) → Reverse of ARP

chart note

Icmp (Internet control message protocol)

↓

Indicates the status of the h/w.

see ping

Igmp (Internet group message protocol)

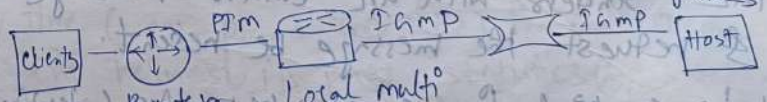
Internet group management protocol is a network layer protocol that allows multiple devices to share an IP address & receive the same data. Igmp is used to set up multicasting on h/ws that use the internet protocol version 4 (IPv4).

Igmp runs b/w a router & a node enabling the following actions-

i) Igmp query: Routers ask nodes if they need a particular multicast system.

ii) Igmp reports: Nodes respond to the router if they are seeing a particular multicast stream.

It can be used for one-to-many networking applications such as online streaming video, etc games

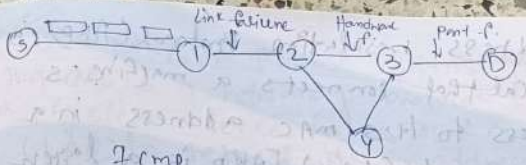


Igmp protocol

ICMP – The internet control message protocol (ICMP) is a n/w layer protocol that allows devices to communicate data transmission errors in a network. ICMP is mainly used to determine whether data is reaching its intended destination in a timely manner. [For eg, if a message is too long, or data packets arrive out of order, the receiver uses ICMP to inform the sender with an error message & request the message be resent.

It is crutial for error reporting & testing, but it can also be used in DDOS (distributed denial-of-service) etc.

Some egs of ICMP message includes:
i) Port Unreachable, ii) No route to host, iii) Lifetime expired, iv) Administratively prohibited

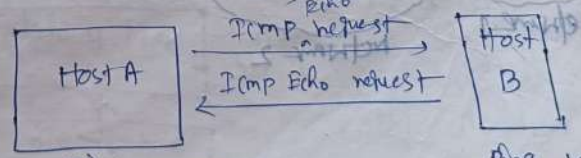


ICMP

Ping – Ping is a network utility used to test the reachability & responsiveness of a host or a n/w device over an IP network.

[When we run the "ping" command (ICMP Echo) followed by an IP address / a domain name in a command prompt / terminal, it sends request packets to the target host.

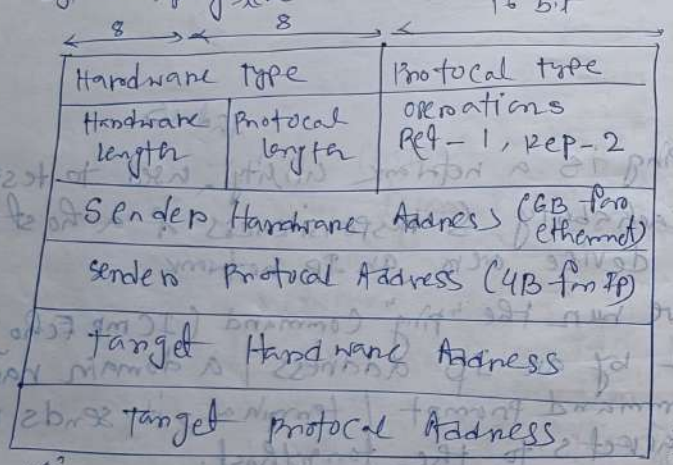
The o/p of a ping command is presented in a series of text lines including information such as:
i) Time (RTT - Round-Trip Time) for each ICMP echo request, ii) ping statistics (A summary of command's result).]



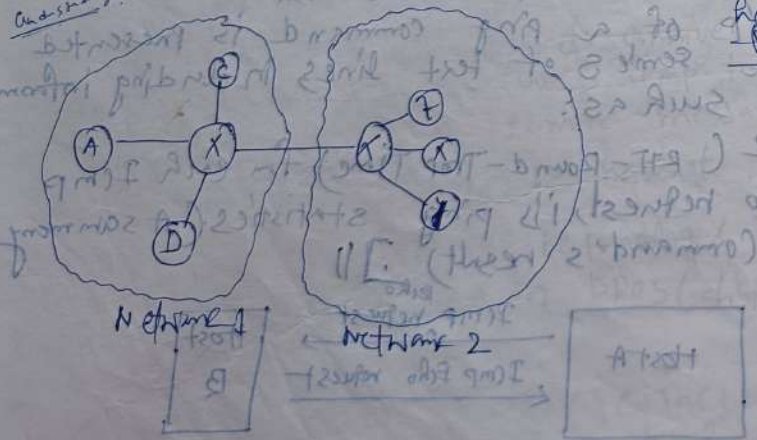
Ping Command

ARP - Address resolution Protocol (ARP) is a protocal that connects a machine's IP address to it's MAC address in a local area n/w (LAN). [ARP is a layer 2 protocal that translates 32-bit addresses to 48-bit addresses & vice versa].

i.e,
ARP: IP → MAC
Logical → physical



ARP header format

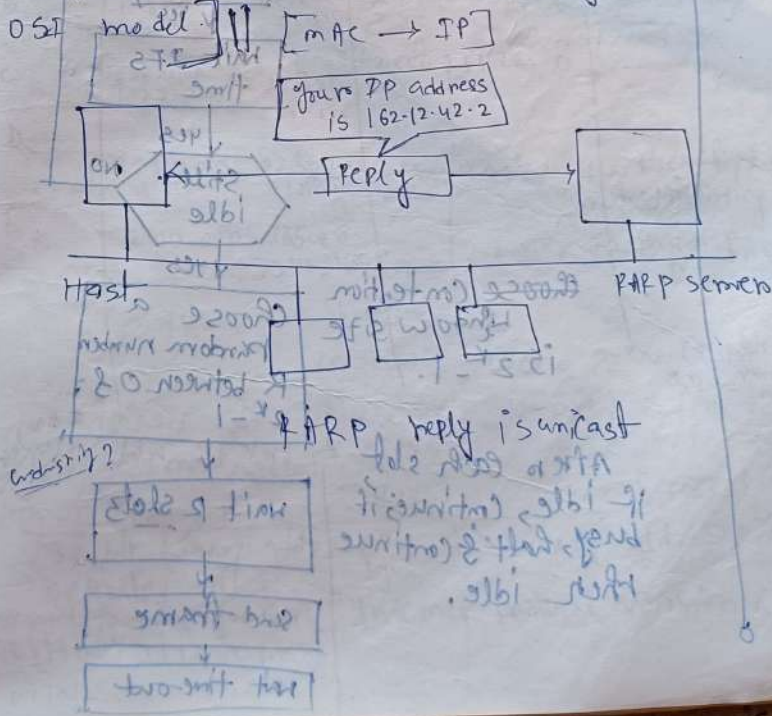


RARP - RARP, or Reverse Address Resolution Protocal, is a networking protocal that allows a physical device in a local area network (LAN) to request it's IP address.

[It works by sending the device's physical address to a RARP server on the same LAN, which then returns an IP address for the device to use. RARP was originally developed to assign IP addresses to diskless workstations / other devices that lack the storage capacity to store their IP addresses.]

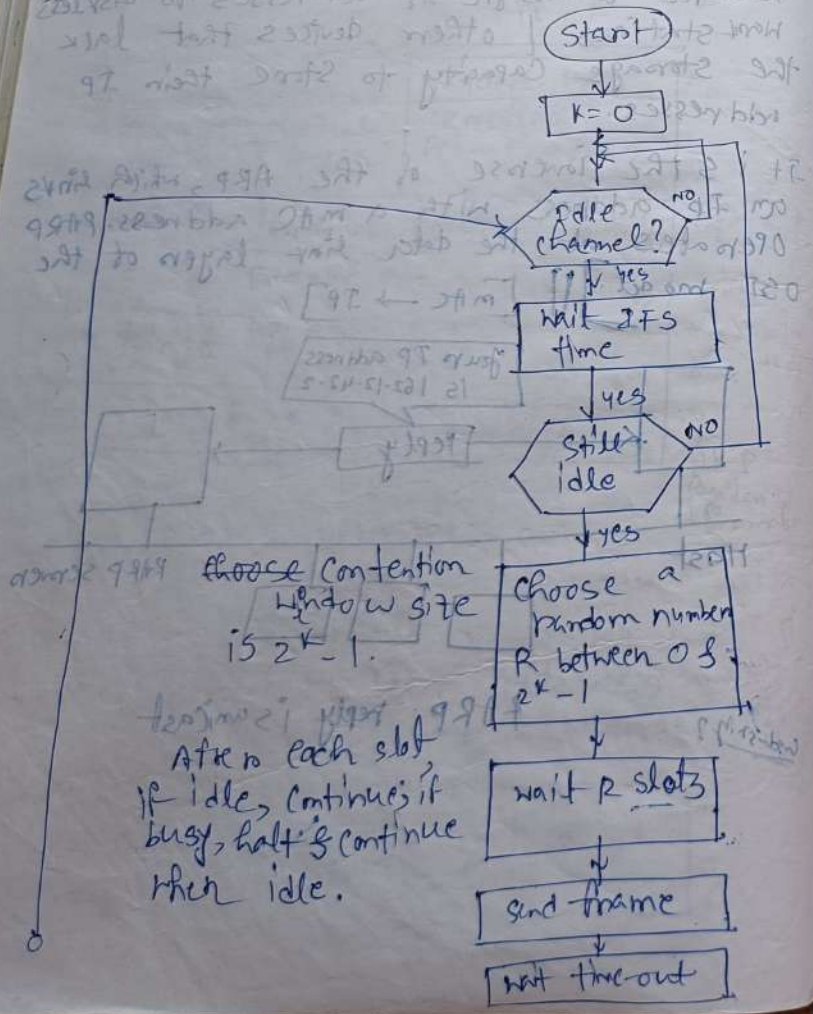
It is the inverse of the ARP, which links an IP address with a MAC address. RARP operates at the data link layer of the OSI model.

[MAC → IP]



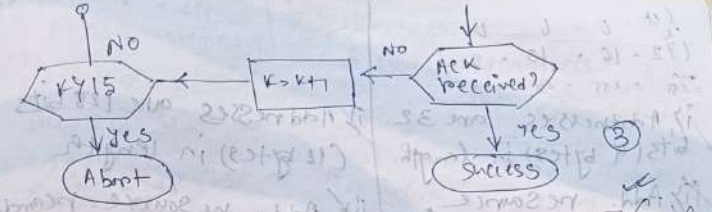
22/4/24

CSMA/CA – Carrier sense multiple access / Collision avoidance. It uses wireless network always.



Choose contention window size is $2^K - 1$.

After each slot if idle, continue; if busy, halt & continue when idle.



Pg - 395 eg (2.3 (numerical - Imp) [4 marks] (with changed values)

Imp - CSMA/CA, CD, pure aloha, slotted aloha, all types of persistence, upper math (imp for exam)

↳ 20 marks

20/4/24

IPv4 has 5 classes (Briefly explain about ranges of IPv4)

class	ranges	default subnet mask	remarks
A	0.0.0.0 – 127.255.255.255	255.0.0.0	① 0.0.0.0 → default route ② 127.0.0.0 → loop back address
B	128.0.0.0 – 191.255.255.255	255.255.0.0	
C	192.0.0.0 – 223.255.255.255	255.255.255.0	
D	224.0.0.0 – 239.255.255.255	~~255.255.255.255~~	Used for multicasting
E	240.0.0.0 – 255.255.255.255		Used for R & D

(Public IP addresses)

IPv4	IPv6
32 bit binary add. seperated by '.'	128 bit binary add. seperated by ':'
Internet Protocol version 4	Internet Protocol version 6
10011100.011000 1.10001100	
octate	

let

172 . 16 . 10 . 9

=255 = 255 = 255 = 255

IPv4	IPv6
i) Addresses are 32 bits (4 bytes) in length.	i) Addresses are 128 bits (16 bytes) in length.
ii) Add. resource records in DNS to map host names to IPv4 adds.]||	ii) Add. resource records in ~~DNS to map~~ IPC [ARPA DNS domain to map IPv6 adds. to hot name.]||
iii) IPSec is optional & should be supported externally.	iii) IPsec support is not optional
iv) Header doesn't identify packet flow for QoS handeling by routers.]||	iv) Header contains flow Labled field, [which identifies packet flow for QoS handeling by router.] ||
v) Header includes a checksum.	v) Header doesn't include a checksum
vi) Header includes options	vi) IPv6 optional data is supported as extention headers.
vii) ARP uses broadcast ARP request to resolve IP to MAC / Hardware add.	vii) multicast neighbour solicitation messages resolve IP addresses to MAC add's

(IPv6 not IPv5)

{network address / Host address}

• { network address / Host address} | Subnet mask — 32-bit binary address.

192 . 168 . 5 . 2
Net ID — Host

255 . 00 . 0
network ID (8-bit) — Host ID (24-bit)

• Disadvantage of classfull address?

• public (global) & Private IP?

Ranges of Private IP

→ class A → range 10.0.0.0 – 10.255.255.255

→ " B → 172.16.0.0 – 172.31.255.255

→ " C → 192.168.0.0 – 192.168.255.255

Q. 23) Briefly describe about various ranges of private IP?

→ class A – 10.0.0.0 to 10.255.255.255, used for large networks with 8 bits for the n/w & 24 bits for hosts.

class B – 172.16.0.0 – 172.31.255.255, used for medium n/ws with 16bits for the n/w & 16 bits for host.

class C – 192.168.0.0 – 192.168.255.255 used for smaller n/ws with 24 bits for the n/w & 8 bits for hosts.

NAT/PAT —

Network address translation (NAT) is a networking technique that allows multiple devices to use a single public IP add. NAT is typically implemented on a router, which intercepts data from a device on a private n/w & replaces the source IP add. with its own public add. The router then sends the data to the destination device.

Imp	Imp			
A	10.5.5.5	—	255.0.0.0 →	10.0.0.0
B	171.5.5.7	—	255.255.0.0 →	171.5.0.0
C	192.168.10.7	—	255.255.255.0 →	192.168.10.0

← network address calc

Ip of incoming pkts of same class (imp for exam)

10.5.5.5 + 255.0.0.0 → NW add. 10.0.0.0

00001010 + 11111111 → 00001010

Subnetting — In computer networking, subnetting is the process of dividing an IP network into 2 or more smaller networks, known as subnets. It improves n/w performance & security by making n/w routing more efficient.

Public & Private IP — A public IP add. is a unique IP add. assigned to your n/w router by your internet service provider & can be accessed directly over the internet.

A private IP add. is a unique add. that your n/w router assigns to your device. It is used within a private n/w to connect securely to other devices.

CSMA/CA — Carrier sense multiple access with collision avoidance is a network protocol for carrier transmission that operates in the medium access control (MAC) layer. In contrast to CSMA/CD that deals with collisions after their occurrence, CSMA/CA prevents collisions prior to their occurrence.

Vulnerable time — Propagation time (T_p)

Adv — CSMA/CA prevents collision
Due to acks, data is not lost unnecessarily.
It avoids wasteful transmission.
It is very much suited for wireless transmissions.

disadv — The algo calls for long waiting times.
It has high power consumption.

Flowchart —

Eg 12.5 — A n/w using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time (including the delays in the device etc) is 23.6 μs, what is the min size of the frame?

The frame transmission time is $T_{fr} = 2 \times T_p = 51.2$ μs. This means in the worst case a station needs to transmit for a period of 51.2 μs to detect the collision, the min. size of the frame is 10 Mbps × 51.2 μs = 512 bits / 64 bytes. This is actually the min. size of frame for standard ethernet

Network address – A network add. is a unique identifier for a device / network node on a computer n/w. It can be numeric / symbolic, & can take several forms, including

i) IP address (A 32-bit no. that uniquely identifies a device on an IP network)
ii) MAC add (A n/w add.)
iii) Host add. (A n/w add.)

Host address – The host (or node) add. is used to identify a particular device attached to the n/w. [The IP add. is generally represented with dotted ~~domain~~ decimal notation, where 32-bits are divided into 4 octets can be rep. in a decimal format, seperated by decimal points.]

Subnet mask – It is a 32 bit no. created by setting host bits to all 0s & setting network bits to all 1s. In this way, it seperates the IP add. into the n/w & host add.

Disadvs of classfull add.

i) ~~IANA has~~ too few network addresses for large networks
ii) Two-layer hierarchy isn't appropriate for large n/w's with class A & class B addresses
iii) Growth rate exhausted the IP add. space

iv) Now only /C add. were available which increases the routing table sizes in gate-ways.

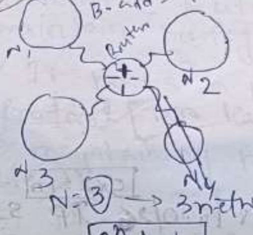
Subnetting

Q) Imp (exam)

Private IP 192.168.10.0] → in exam I am giving this (& how)
N add = 192.168.10.0
B-add = 192.168.10.63

29/4/24

add. == id



192.168.10.0/24 ← subnet mask (n)

8+8+8 = 24 → 255.255.255.0

N = 3 → 3 networks

$2^n \geq N$

if $2^n \geq 3$

then n = 2 (min) should be

∴ n = 2

net bit ← → Host bit

192	168	10	00	000000	192.168.10.0
192	168	10	01	000000	192.168.10.64
192	168	10	10	000000	192.168.10.128
192	168	10	11	000000	192.168.10.192
11111111	11111111	11111111	11	000000	

← 255.255.255.(n=2)·192 new subnet mask

borrow from host bit

192.168.10.0 → 192.168.10.0/26
24

upto
63
127
191
255

Broadcast add. of a network

When the all bits in host bit will be 1, then it is called broadcast add. 11111111.11111111

Broadcast add
192.168.10.63
192.168.127
192.168.191
192.168.255

• From 64 add, 1 add. will be deducted for N. add, 1 will be deducted for B. add, Therefore,

in N₁ we can assign this no. of systems / PCs

192.168.10.1 → 1st machine / 1st IP
10.2
10.3
—
10.62] total 62

→ subnetting

Benifits of subnetting

① security issue
② Broadcast storm
③ smoothness of transmission

Eg (Prov - Sath) – ① You are given 192.168.10.0/26 IP slot. [5x2=10]
You have to divide it into 3 subnetwork. what
is i) new subnet mask? → ~~192.168.10.192~~ 255.255.255.192
ii) what is network add. of 2nd network?
iii) what is broadcast address of 2nd network?

192.168.10.0/26 (Class C)
└→ class C

Default subnet mask = 255.255.255.0

as 26 we have to borrow 2 bits from HID.

∴ 11111111.11111111.11111111.11000000 (borrowed)

i) 255.255.255.192 → new subnet mask

[n = total no. of bits borrowed from the host] → to find no. of n/ws

[h = total no. of host bits] → (to find the no. of IP add. on each n/w)

(ii) n/w add. of 2nd n/w = 192.168.10.64 (from prev chart)

(iii) Broadcast = 192.168.10.127

Q-24) Diff. b/w Routed & Routing protocol & it's eg.

Routing P.	Routed P.
① used b/w layer 3 devices to learn & advertise routes & maintain routing tables.	① Used b/w routers to direct users traffic. It is also called n/w protocols
② It routs a routed protocol [for learning & maintaining routing table.]	② Routed protocols are routed by routing protocols
③ This are not available in a normal computer or a printer.	③ A routed protocol in an int part of n/w p. suit & it is available in every device which is participating in n/w communication.
④ It's just concerned about the router	④ It is just concern about the mode of data transfer & also include the source & destination add.
⑤ It is about path	⑤ It's about the data.
Eg – ~~IP, IPX, Appletalks~~ RIP, OSPF BGP etc.	Eg – IP, IPX, Appletalk etc.

Q-25) Header format of IP.

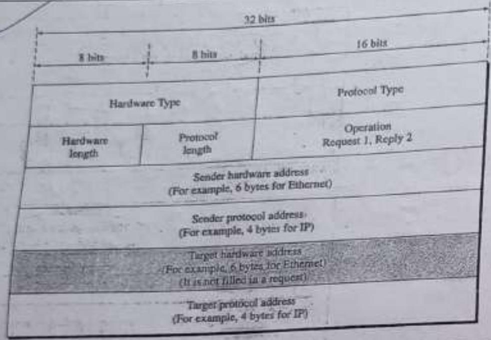
IP's data units = datagram

The IP header is 20-24 bytes long & contains the IP addresses of the source & destination, along with other fields that help route the packet. It is divided into 4 sections – i) version – the IP ver. is used ii) IHL (Internet Header length) – the length of the IP in 32-bit increments. iii) TOS (Type of services) – low delay, high throughput / reliability. iv) Total length – The length of header & data in bytes.

PTO

Q26) Briefly describe about [7 marks]
ARP packet / ARP header format / ARP datagram format
diagram (table) [Pg - 614]
(Ans)

Figure 21.2 *ARP packet*



The fields are as follows:

- **Hardware type.** This is a 16-bit field defining the type of the network on which ARP is running. Each LAN has been assigned an integer based on its type. For example, Ethernet is given type 1. ARP can be used on any physical network.
- **Protocol type.** This is a 16-bit field defining the protocol. For example, the value of this field for the IPv4 protocol is 0800_{16}. ARP can be used with any higher-level protocol.
- **Hardware length.** This is an 8-bit field defining the length of the physical address in bytes. For example, for Ethernet the value is 6.
- **Protocol length.** This is an 8-bit field defining the length of the logical address in bytes. For example, for the IPv4 protocol the value is 4.
- **Operation.** This is a 16-bit field defining the type of packet. Two packet types are defined: ARP request (1) and ARP reply (2).
- **Sender hardware address.** This is a variable-length field defining the physical address of the sender. For example, for Ethernet this field is 6 bytes long.
- **Sender protocol address.** This is a variable-length field defining the logical (for example, IP) address of the sender. For the IP protocol, this field is 4 bytes long.
- **Target hardware address.** This is a variable-length field defining the physical address of the target. For example, for Ethernet this field is 6 bytes long. For an ARP request message, this field is all 0s because the sender does not know the physical address of the target.
- **Target protocol address.** This is a variable-length field defining the logical (for example, IP) address of the target. For the IPv4 protocol, this field is 4 bytes long.

Q27) TCP header format, UDP header format, IP datagram format, HDLC header format (any 1 of them)

Assignment [10 marks (in exam)]

① You are given 172.16.0.0. You have to divide it into 14 subnetwork. i) What will be new subnet mask? ii) What will be network add./NId of 5th network. iii) What will be broadcast add. of 5th network? iv) What will be the IP add. of 11th PC of 5th network? (class B)

NID | HID
172.16.0.0 → class B

Default subnet mask = 255.255.0.0

How many bits to borrow = not given, but they wanted the new subnet mask that means bits are borrowed from HID.
How many bits are borrowed we can get it from this formula $2^n \geq N$

N = no. of n/w in which the n/w is divided (subnetworks)
n = total no. of borrowed bits.

$2^n \geq 14$
$\Rightarrow 2^4 \geq 14$
$\Rightarrow 16 \geq 14$
$\therefore n = 4 \rightarrow$ 172.16.0.0/28

i) New subnet mask = 11111111.11111111.00000000.11110000 = 255.255.0.240

NID	HID		Network add.	B.A.
1 172.168.0	0000	0000	172.168.0.0	15
2 172.168.0	0001	0000	172.168.0.16	31
3 172.168.0	0010	0000	172.168.0.32	47
4 172.168.0	0011	0000	172.168.0.48	63
5 172.168.0	0100	0000	172.168.0.64	79
6 172.168.0	0101	0000	172.168.0.80	95
7 172.168.0	0110	0000	172.168.0.96	111
8 172.168.0	0111	0000	172.168.0.112	127
9 172.168.0	1000	0000	172.168.0.128	143
10 172.168.0	1001	0000	172.168.0.144	159
11 172.168.0	1010	0000	172.168.0.160	175
12 172.168.0	1011	0000	172.168.0.176	191

1. 172.168.0.0
2. 172.168.0.64
3. 172.168.0.96
4. 172.168.0.112

1100	00000	172.168.0.192	207
1101	00000	172.168.0.208	223
1110	00000	172.168.0.224	239
1111	00000	172.168.0.240	255

Broad. Add	5th n/w's PCs
172.168.0.15	1. 172.168.0.129
172.168.0.31	2. 172.168.0.130
172.168.0.47	3. 172.168.0.131
172.168.0.63	4. 172.168.0.132
172.168.0.79	5. 172.168.0.133
172.168.0.95	6. 172.168.0.134
172.168.0.111	7. 172.168.0.135
172.168.0.127	8. 172.168.0.136
172.168.0.143	9. 172.168.0.137
172.168.0.159	10. 172.168.0.138
172.168.0.175	11. 172.168.0.139
172.168.0.191	12. 172.168.0.140
172.168.0.207	13. 172.168.0.141
172.168.0.223	14. 172.168.0.142
172.168.0.239	
172.168.0.225	

172.168.0.64 = NID of 5th n/w

172.168.0.79 = B.ID = 5th

IP add. of 11th PC of 5th network

∴ IP add. of 11th PC of 5th n/w = 172.168.0.139

Broadcast address of a n/w — It is a special IP address that allows you to send a message / packet to all devices on a network. [It's the highest numeric value of the add. format being used] & it enables transmission to every node in a local n/w.

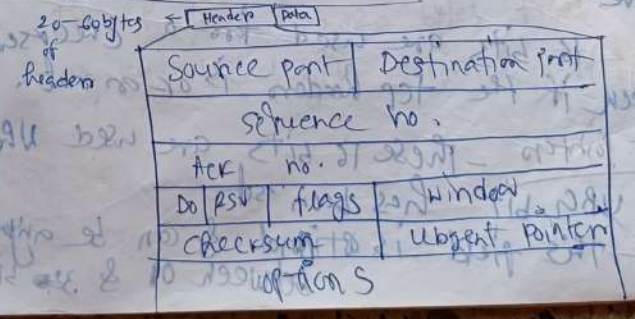
Benifits of subnetting

1. Reduce n/w traffic (Broadcast storm)
2. Optimized n/w performence
3. Simplified management.
4. Facilitated spanning of large geographical distance.
5. Bandwidth utilization will increase.
6. Smoothen the transmission.
7. Reduce security issues

(7m) TCP header format — It is a reliable transfer protocol as it establishes a connection before sending any data & everything that it sends is acknowledged by the receiver.

TCP header format —

20 - 60 bytes of header



Source port - this is a 16 bit field that specifies the port no. of the sender.

Destination port - this is a 16 bit field that specifies the port no. of the receiver.

Sequence no. - It is a 32-bit field (variable length) that indicates how much data is sent during TCP session.

ACKnowledgment no. - It is a 32 bit field, is used by the receiver to request the next TCP segment.

DO - This is a 4 bit data offset field also known as the header length. [It indicates the length of the TCP header so that we know where the actual data begins.]

RSV - these are 3 bits for the reserved field. They are unused & are always set to 0.

Flags - there are 9 bit flags, we also call them control bits.

Window - the 16 bit window field specifies how many bytes the receiver is willing to receive.

Checksum - 16 bits are used for a checksum to check if the tcp header is ok or not.

Urgent pointer - these 16 bits are used when the URG bit has been set.

Options - this field is optional & can be anywhere between 0 & 320 bits

4) UDP header format - It is an 8-byte packet that contains 4 fields -

Source port - the port no. of the device sending the data

Destination port - the port no. of the destination computer.

Packet length - the length of the segment in bytes.

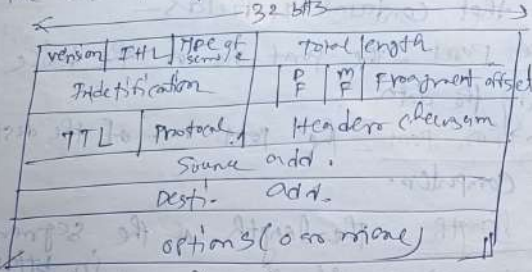
Checksum - A 16-bit field used by the sender & receiver to check for data corruption.

The 1st 4 bytes of the UDP header store the port no.s, the next 2 bytes store the segment length & the final 2 bytes store the checksum.

5) IP datagram format

- The format of data that can be recognized by IP is called IP datagram.
- It consists of 2 components, namely, the header & data, which need to be transmitted.
- Every field in the IP datagram has a fixed size except for the IP options field which can be 20-60 bytes in length.
- the header has 20 bytes fixed part & a variable length optional part.

The IP datagram Headers format



HDLC Header format — (Connected with PPP)

[the Header of HDLC (High level Data Link control) frame contains info about sender, receiver & user data. the Header is followed by user data & a CRC.]

the Header info of an HDLC frame contains the following fields —

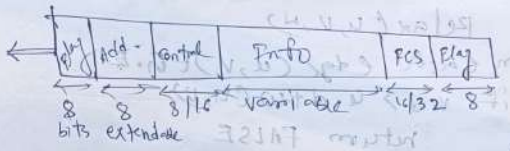
Flag - An 8-bit sequence that marks the beginning & end of the frame.

Address - contains the add. of the receiver. [If the frame is sent by the primary station it contains the add. of the secondary station.]

Control - contains flow & error control info in 1/2 bytes, identifies the frame type etc.

Information - can be an arbitrary binary bit set with a max length of 1000 to 2000 bits.

Frame check sequence (FCS) - 16 bit CRC that checks the content of the frame.

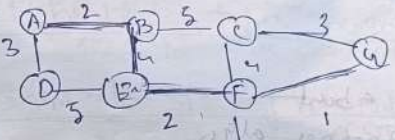


Basic frame structure of HDLC

CN

(3) 6/5/24

Routing → static Routing
→ Dynamic "



optimized

Autonomous system = Intra domain

It is a set of routers under single administration / more than one or more

Inter domain - 2 or more autonomous system's comm.

Intra domain - 1 autonomous system's comm.

Distance vector routing (Bellman ford algo)

Linked State routing (Dijkstra algo)

Bellman ford algo

Bellmanford (G, w, s)

1. Initialize - single - source (G, s)
2. for i = 1 to |G.V| - 1
3. for each edge (u, v) ∈ G.E

4. Relax(u,v,w)
5. for each edge(u,v) ∈ G.E
6. if v.d > u.d + w(u,v)
7. return FALSE
8. Return TRUE

Q. 2nd
Briefly describe about
Distance vector routing algo

It is actually bellman ford algo. It is
Iterative - it continues until no node exchange info
self-terminating. no 'signal' to stop
Asynchronous - Nodes need not exchange info/ iterate in lock step
Distributed - Each node communicates only with directly attached neighbours (adjacent nodes)

Distance table structure

$D^x(y,z)$ = distance from x to y, via z as next hop

$= c(x,z) + \min_w \{D^z(y,w)\}$

z = neighbours

Q. 3rd short note - Spanning tree Protocol (STP)

Q. 4th
Split horizon & Poison reverse

path vector routing - not imp (just read) (not in exam)

RIP

metric, metric of RIP (hopcount), OSPF (metric (OSPF cost)), OSPF metric

Border gateway protocol (BGP) Version 4 (BGP4)

Transport layer with sublayers

Socket - (combination of IP add. & port add.)
IP add + port add = Process id (PID)

- Port add is a 16 bit address
  - Registered port add. (1024 - 49151)
  - Unregistered → (49152 - 65535)
  - Well known → (0 - 1023) (start - end)

Q. 5th Briefly describe about various types of port add.s with their ranges?

Port add. Done (pmv)

types of ports -
i) Well known port
ii) Registered port
iii) Dynamic port

Well known Port

i) It is from the range 0 - 1023
ii) It is reserved for common & specifically used service.
iii) It is used by some widely adopted protocals & services like http etc.

Registered port

i) It's from range 1024 to 49151
ii) These are used by applications / services that are not as common.
iii) But it's used by those applications / services which requires its specific port.
iv) organizations can ask IANA (Internet assigned number authority) for any specific port no. with this range.

Dynamic ports

i) It is from range 49152 to 65535
ii) It is also known as Private port.
iii) It is used for those connections that are temporary / short-lived.
iv) It is not registered / assigned & can be used by any process.

Autonomous System - An autonomous system (AS) is a very large n/w or group of n/ws with a single routing policy. Each AS is assigned a unique ASN, which is a no. that identifies the AS. Eg - Driverless cars, autonomous mobile robots etc.

Split Horizon & Poison reverse

Split horizon - Distance vector protocals employ the split horizon technique to avoid network routing loops. The fundamental rule is straightforward; never transmit routing info back in the direction it came from.

Poison reverse - An implemented algo called poison reverse is frequently used in distance-vector routing to solve the count-to-infinity problem, employ poison reverse. It is the opposite of split horizon. The main goal of poison reverse is to prevent paths from reversing into the same node when a network cost changes.

Spanning tree protocal / STP - It is also known as STP. It is a protocal that monitors the overall performance of the network. The main task of the spanning tree protocal is to remove the redundant links. This protocal uses the spanning tree algo (STA)

, that's used to detect the redundant link

Steps of STP

i) This p. selects 1 switch as a root bridge (where the root bridge is a central point as when the message is sent: then it always passes through the bridge.)

ii) It selects the shortest path from a switch to the root bridge.

iii) It blocks the links that cause the loop on a n/w, & all the blocked links are maintained as backups. It can also activate the blocked links whenever the active link fails. Therefore, we can say that it also provides fault tolerance on a n/w.

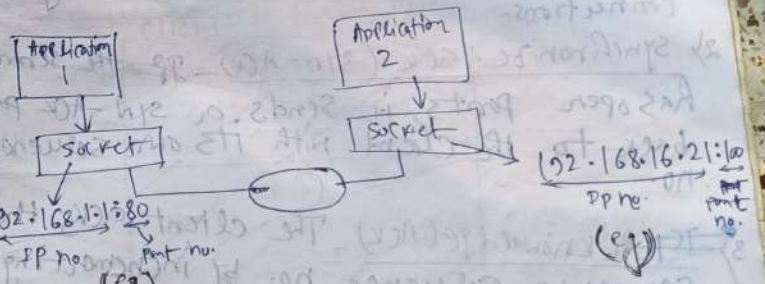
RIP — It stands for routing information protocol. It is a dynamic routing protocol that uses hop count as a routing metric to find the best path b/w the source & distance destination n/w.

Hop count — It is the no. of routers occurring in b/w the source & destination network. The path with the lowest hop count is considered as the best route to reach a n/w & therefore placed in the routing table. RIP prevents routing loops by limiting the no. of hops allowed in a path from source & destination (max h.c = 15, h.c = 16 → N/w unreachable).

OSPF — It stands for open shortest path first. It is an IP routing protocol that uses a mathematical algo to determine the most efficient path for traffic on IP networks.

BGP v4 — It's an eg of path vector routing protocol & is described as the needle & thread which binds the Internet together (Border gateway protocol)

Socket — These are seen as the end of the 2-way communication b/w 2 processes. It is created by concatenating the IP no. of a system & a software port no. This allows the process to know the add. of the system (the IP add.) & the port no. the IP & port no.s are seperated by ':'.



(eg)

(eg)

CN

Diff b/w leaky & token bucket algo.

Leaky B	Token B
i) Token independent.	i) Token dependent.
ii) It doesn't save any token.	ii) It saves token for the burst of packet transmission.

10/5/24

i) Sends packets at constant rate.	i) It can send large burst of packets at faster rate.
ii) Packets are transmitted continuously.	ii) Packets can only transmit when there is enough token.
iii) More restrictive as compared to token bucket algo	iii) Less restrictive as compared to leaky bucket algo

3-way handshaking process (with diagram)

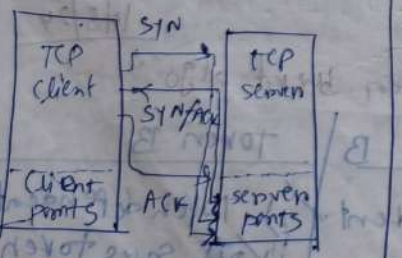
It is a process that establishes a reliable connection b/w 2 devices.

It involves 3 steps -

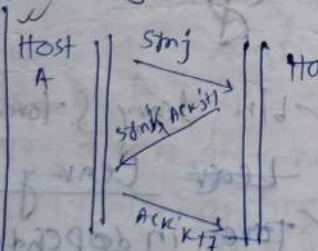
1) Synchronize (SYN) - the client sends a SYN packet to the server with an arbitrary sequence no. to ask if there are any open connections.

2) Synchronize-ACK (SYN-ACK) - If the server has open ports, it sends a SYN-ACK packet back to the client with its own sequence no.

3) ~~If~~ ACKnowledge (ACK) - The client acks the server's sequence no. by incrementing it.



(1)



(2)

TCP connection establish = 3-way handshaking
terminate = 4-way handshaking

Q. 3-way handshaking process (connection termination) with diagram?

It involves exchanging messages b/w an access point (authenticator) & a client device (supplicant) to generate encryption keys. The messages are -

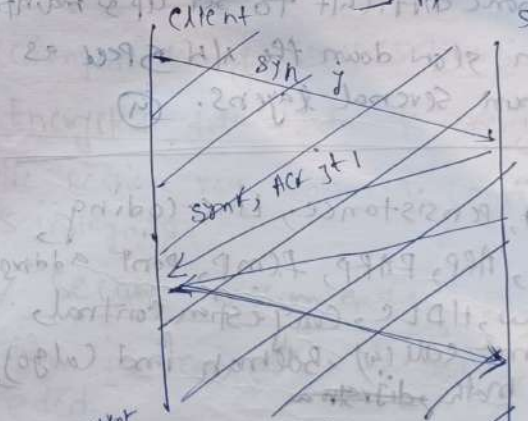
1) The WAP (wireless access point) sends an EAPOL-key frame with a nonce value & connection info to the client.

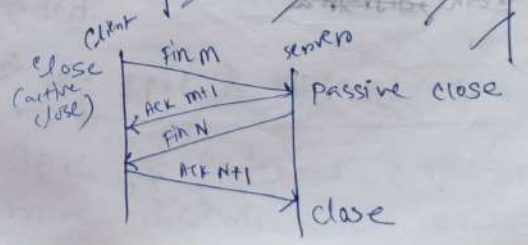
2) The client derives / calculates its own shuts.

3) The authenticator uses the shuts as an authenticators no.

4) The client & authenticator exchange their MAC addresses.

FIN= finish message





Q.33) ~~Adv~~ & dis adv of TCP

Adv – i) It ensures that data is transferred reliably.

ii) It reduces the sender's transmission rate if the destination can't process it quickly. (Flow control)

iii) It controls congestion.

iv) It provides error checking mechanism & recovery.

v) It gives ~~us-st~~ scalability.

Disadv – i) It can introduce latency.

ii) It can introduce a lot of overhead.

iii) TCP is more complex than UDP.

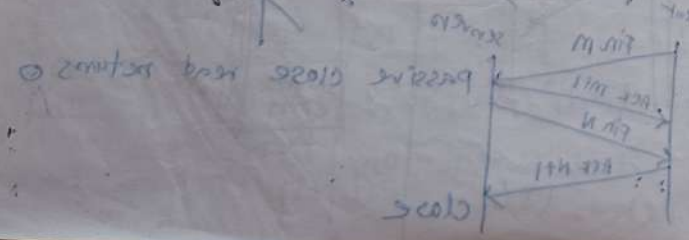
iv) TCP requires more resources than UDP.

v) It is more difficult to set up & maintain.

vi) It can slow down the N/W speed as it can run several layers. (4)

Sugg

① Aloha(all), persistance, Line coding, IP'S math, ARP, RARP, ICMP, Port address, sliding window, HDLC, Congestion control, headers format call (4), Bellman ford (algo), subnetting's math, ~~dijkstra~~



Q.34) Working of https – HTTPS stands for hypertext transfer protocol secure. It is the most common protocol for sending data b/w a web browsers & a website.

working

i) Client request – The browsers initiates a connection to the servers via "https://".

ii) Server sends certificate – The servers provides an SSL/TLS certificate containing its public key.

iii) Browsers verifies – The browsers checks if the certificate is valid & trusted.

iv) Key exchange – A secure session key is exchanged using server's public key.

v) Encrypted data – Data is encrypted using the session key, ensuring confidentiality & integrity.

vi) Secure session ends – once communication is complete, the session key is discarded.

Q.35) Why IPv6 is preferred over IPv4?

IPv6 is Preferred over IPv4 as, it's more efficient, secure & has a longer

address spaces that helps to support the growing numbers of internet users & devices.