Computer Network

Date: 2/8/24

Text Book — Forouzan

Why computer network?
- sharing resource
- real time data transfer

Definition: Network is a set of devices (also known as nodes) connected by communication links. A node can be a computer, printer or any other device capable of sending and receiving data. The primary goal of a network is to share the information in realtime and reduce the transmission cost.

Criteria of Good Network:—

1. Performance (Speed)
2. Reliability (Consistency)
3. Security

(*) A network is classified as a good network if it satisfies the criteria.

1. **Performance:** Performance can be measured in different ways including transit time (speed). The performance highly depends on the hardware and the transmission medium.
   e.g. Optical fiber
2. **Reliability:** Reliability depends on the following factors—
   - accuracy of delivery,
   - frequency of failure,
   - time of recovery / Robustness of the network → exception situation handling capacity
3. **Security:** Network security includes protecting the data from unauthorized access.

Physical Structure:

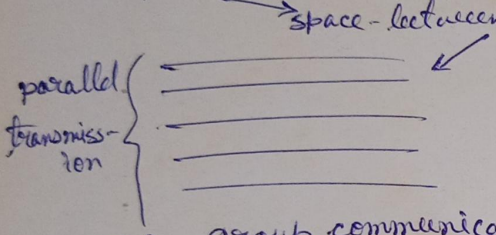
Types of Connection

1. Point to Point
2. Multipoint / Multidrop

① The point to point connection provides a dedicated link between the sender and receiver. It uses the entire capacity of the network for a single communication.

e.g. Keyboard, mouse, TV remote, mobile phones

② In this communication more than two specific devices share a single communication thing. The capacity of the channel is shared. The sharing can be spacial or time shared.



e.g. group communication etc.

Types of transmission:

① Simplex,
② Half duplex,
③ Duplex / Full duplex

① In simplex communication, there is a permanent sender and a permanent receiver. The communication flows in one direction only.

e.g. keyboard, mouse, monitor, printer etc.

② Here the communication occures in both direction but not at the same time. When one transmit the other receives and vice-versa.

e.g. Waki-Toki

③ Duplex: Here the transmission occurs in both direction simultaneously. Both the nodes can transmit and receive at the same time.

e.g. Mobile Phone

Message Transmission:

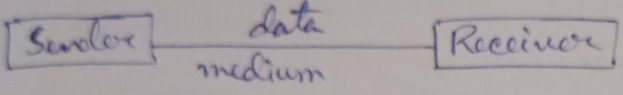
① Unicast, ② Multicast, ③ Broadcast

① The unicast messages are one to one, ie there is only one receiver of that message.

② The Transmission is one to some. i.e. there is a group of receiver for the message.

③ This type of transmission is one to all, i.e. every receiver receives a copy of the message.

Component of Network



Protocol

① **Sender**: There must be a sender that will send the data.

② **Receiver**: There must be a receiver that will receive the data.

③ **Medium**: Sender and receiver must be connected via a communication medium. This medium can be wired / wireless.

④ **Data**: This is the information which is exchanged between the sender and receiver.

⑤ **Protocol**: The protocol is a set of rules among the communication parties. The protocol specifies many aspects such as packet size, transmission rate, bandwidth etc.

Protocol consist of the following three things—

① Syntax → grammer

② Semantics → meaning

③ Timing

(1) The syntax determines the parameters for data transmission such as packet size, transmission states, medium to be used, format of each packet etc.

(2) The semantics deals with the meaning of field. (It can use any syntax)

(3) Timing:

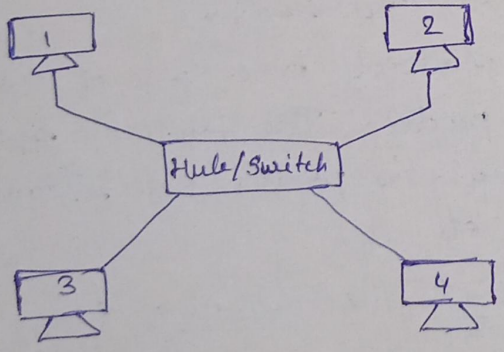
Convoy Effect

The timing controls the synchronization issues between the sender and receiver so that there should not be any mismatch of speed.

Lab:
packettracer
Heading: Connecting two nodes directly using packet tracing

8/8/24

Star topology



In this topology, it divides as a dedicated point to point link. Only to the central controller known as hub/switch. The devices are not directly linked with one another. All the

traffic first comes to the hub and then they are distributed.

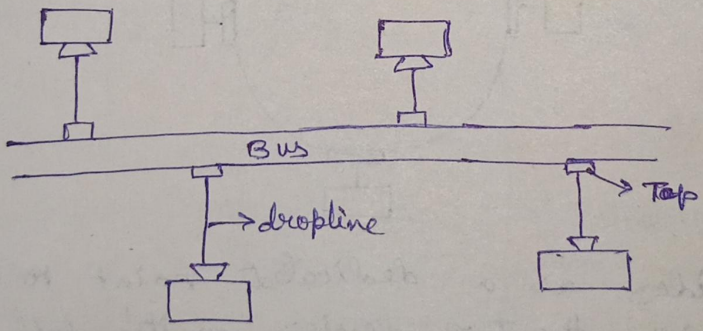
Advantages:

(1) Less cabling compared to mesh.
(2) Every connection is dedicated and point to point. So, both privacy and security is preserved.
(3) If one link fails it does not break down the entire network.

Disadvantages:

(1) If the central hub fails, the entire network is down.
(2) If a link fails, that node becomes unreachable.
(3) There are other topologies that requires less cabling.

Bus Topology



It is a multipoint connection. One long cable is used as a backbone to link all the devices in a network. The nodes are connected to the bus cable by droplines and taps. Tap is the connection point between the backbone and the device. The dropline is a cable between the backbone and the device.

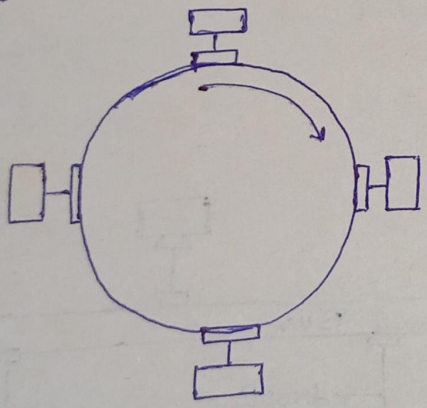
Advantages:

1. More stable than star.
2. Less cabling compared to star or mesh.
3. Cheaper than star or mesh.

Disadvantages:

1. Difficult to install and maintain.
2. Due to the multipoint connection, the privacy and security is less.
3. Since there is a signal loss at every tap, so there is a limit on the no. of nodes that can be connected within a given distance.
4. The breakage of the backbone cable (due to earth quake, fire or similar incidents) make break down the entire network.

Ring Topology



It devides as a dedicated point to point link. Only with the two devices on its' left and right. The signal is passed along the ring in one direction from device to device until it reaches its' destination. When a device receives a signal intended for another device, it simply passes it warm.

Advantages:

(1) Easy to install and reconfigure
(2) Privacy and security are implement to the point to point connection.
(3) Cabling is less and so the architecture is cheap.

Disadvantages:

(1) One way data transform, so the effective bandwidth is half.
(2) Maximum ring length is fixed.

Date: 10/8/24

(3) Comparison between LAN, MAN, WAN —

LAN	MAN	WAN
1) Full form: Local Area Network	1) Metropolitan Area Network	1) Wide Area Network.
2) Ownership: Private	2) Private / Public	2) Public (mainly) Private is also possible
3) Connection type: Primarily wire	3) Wired but may be wireless at some point	3) Mainly through satellite and OFC.
4) Topology: Star, Ring, Bus	4) Bus, Ring	4) Bus
~~5) Cabling~~		
5) Distance: within few kilometers	5) Within a city or country	5) Wide geographical area.
6) Cabling: Copper wire (Twisted pair)	~~Coaxial cable~~ 6) Coaxial cable	6) OFC
7) Speed: Gbps	7) Mbps	8) Kbps
8) Use: Small office/ laboratories	8) Different ~~bo~~ branches of the same office	8) Intercontinental communication
9) Cost: Cheap	9) Costlier	9) Costly

LAN	MAN	WAN
10) Installation & Maintanance: Easy	10) Difficult	10) Very difficult
11) Environment: Homogeneous (same type of h/w & s/w)	11) May or may not be homogeneous	11) Heterogeneous (h/w & s/w are different)
12) Protocol: Same	12) Same	12) Different
13) Governing body: single	13) single / multiple	13) multiple
14) Cyber Law: Same	14) Same	14) Different cyber law at different countries

Topology

Date: 7/8/24

Definition: The term topology refers to the method in which a network is arranged that is geometrical representation of link and nodes.

Two or more devices are connected by links and two or more links formed a topology.

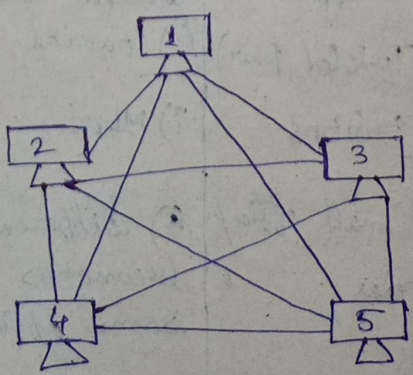
∴ The following are imp Topology available in CN

1) Mesh Topology

∴ No of nodes = $n = 5$

$$\frac{n(n-1)}{2}$$

∴ Total link = $\frac{5(5-1)}{2}$



This architecture every device has dedicated point to point link other devices. A dedicated link carry traffic only between the two devices. So, n devices will requires total $\frac{n(n-1)}{2}$ links and each device has (n-1) takes.

Advantages:

1. Since, if each connection point to point there is no sharing and hence, no conjunction is less.
2. It is very stable. Since, if one link become unusable, the node can be still reached using alternative path. Since each link is dedicated so both privacy and security are preserved.
3. Fault identification is easy so maintanance is easy.

Disadvantages:

1. Huge amount of cabeling, space availability problem.
2. Complex architecture so installation and reconnection difficult.
3. Costly Architecture
4. Change in Architecture, one install is difficult.

Date: 14/8/2024

Layered Approach

Most networks are organized as a back of layered, each one build on the one below it. The number of layers, name of each layer, the content of each layer and their functions varries from network to network. The basic idea is to distribute the total job among the different layers. The purpose of each layer is to provide some services to the upper layer.

Layer n of one machine will communicate with layer n of another machine. The layers at the same level are called peers.

Services: Layers can offer 2 different types of services to the layers above them.

① Connection oriented service
② Connectionless service
} No relation with wired/wireless

① **Connection Oriented Service**: This service is designed after the telephone system. To use a connection oriented service, the service user first establish a connection, uses the connection & then release the connection when it is no longer needed.

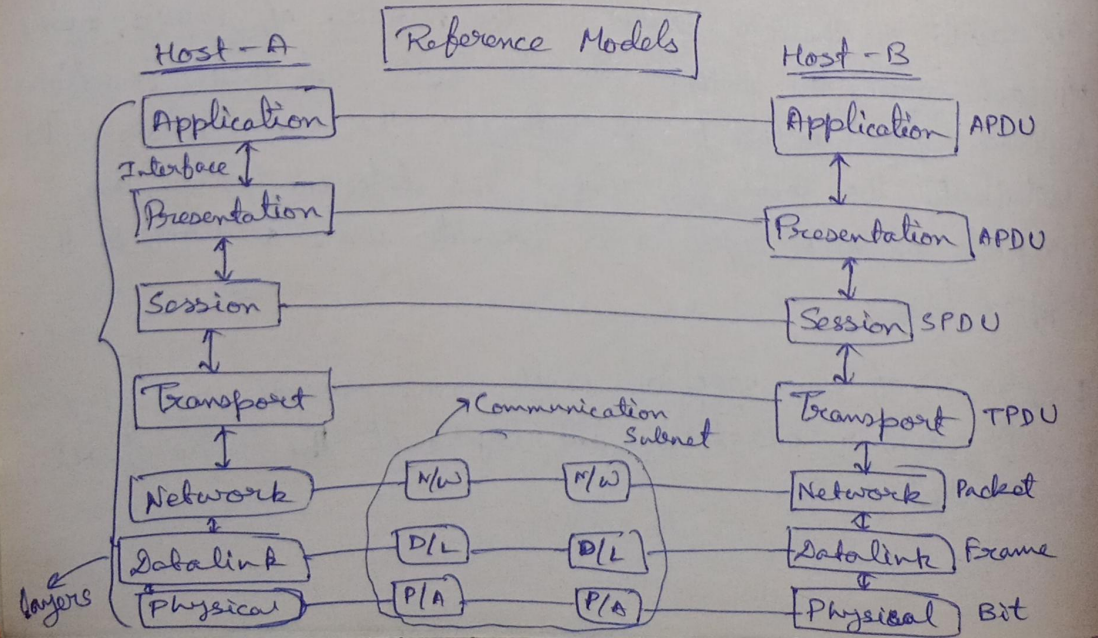
The packets arrived in the same ordered as they were sent. e.g. Cell phone.

② **Connectionless Service**: This service is designed after the postal system. The pre-establishment of connection is not required. Each packet carries the full destination address and may or may not arrive in the same order as they were sent. e.g. Email, sms.

(*) Each service is further characterised by the quality of service (QOS). Which may be either reliable (sents acknowledgement) or unreliable. e.g. Email

OSI Model

Date: 21/8/2024



PDU = Protocol Data Unit

The OSI model is based on a proposal developed by International Standard Organisation (ISO). The complete model is known as ISO. OSI (Open System Interconnection).

The OSI Model has 7 layers as shown in the figure.

① Physical Layer:

It is concerned with conversion of signals to bit or bit to signal. It makes sure that

(i) '1' is received as '1' not '0'.

The design issue deals with mechanical, electrical and timing parameters. It also takes care about the transmission medium to be used.

② Data link Layer:

The main task of DLL is to breakup the input data into data frames and transmit the frames sequentially over and error free line. If the service is reliable, the receiver sends an acknowledgement. Another job of DLL is to control the flow of traffic and keep the sender and receiver synchronized. The access to a shared channel is also controlled by this layer.

③ Network Layer:

It controls the operation of subnet. The key design issue involves running different routing protocols to find the best path between the source and destination.

Routing can be static or dynamic. Network layer is also responsible for conjestion control.

④ Transport Layer:

The basic function of transport layer is to accept the data from above, split it into small units and pass them to the network layer. It also determines what types of service to provide to the session

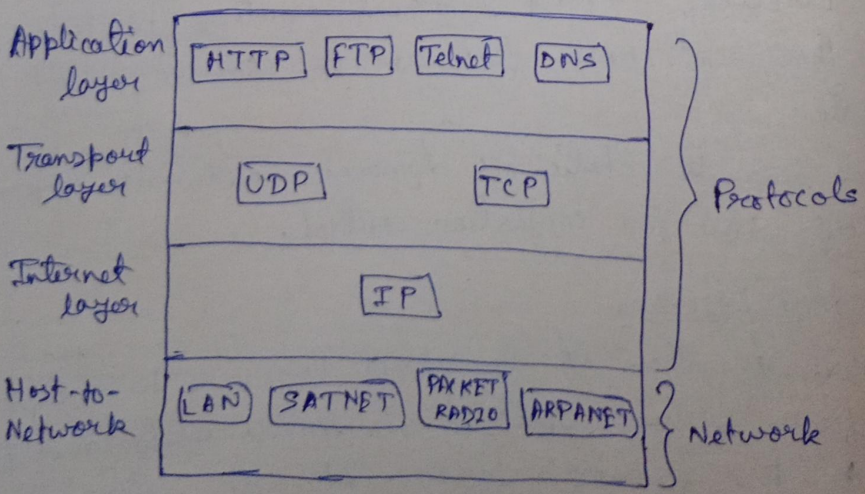
layer. The transport layer is called end-to-end layer.

Session: Display and allows the user on different machines to establish session among them. Session offers various services including dialogue control (who will transmit), token management (prevent simultaneous transmission) and synchronization (allow them to continue where they were after a crash).

This layer is responsible for all data comparison and cryptography operation. The data security is the major concern here. It helps the data with different representation to communicate with one another.

Application: This layer contains a no. of high level protocol that are commonly needed by the user. Few of such protocols are —
Http (Browsery), FTP (use to transfer file), SMTP (Simple File Transfer Protocol), (use for email), Tell net (use for remote login), (terminat network)

TCP/IP



TCP/IP is the successor of ARPANET project (Advance Research Project Association Network). That context 4 layers as shown in the figure.

Application Layer: It is the top-most layer above the transport layer. It contains all the high level protocols. The following are some of them —
HTTP, FTP, Telnet, DNS
This layer is responsible for accepting high level data & interact with the user's application.

Transport layer: This layer is designed to allow peer entities. From the source and destination to exchange data. To end-to-end transport protocols have been defined here. The first one — TCP (Transmission Control Protocol) is a reliable connection oriented protocol. That allows the data from one machine to be delivered on another machine without error. It divides the incoming data into discrete messages and pass each one through the internet layer. TCP also ensures the synchronisation issues. The destination, the receiving process reassembles the received message. The second protocol is UDP (User Datagram Protocol), connectionless and unreliable for those applications where faster delivery is more important than accurated.
e.g. video streaming.

Internet layer: Internet layer holds the entire architecture together. Its job is to permit the host to inject packet in any network and have them travel independently of to the architecture. They may even have in the different order than they were sent. It is the job of the higher layer

to rearrange them. The internet layer defines the packet format on IP (Internet Protocol). The job of the Internet layer is to deliver the IP packets where they are supposed to go. Packet routing and congestion control are the main issues here.

Host-to-Network layer: Below the internet layer is a great void. The TCP/IP model does not really specify what happens here except to point out that the host must connect to the network using some protocol so that it can send IP packets to it. This protocol is not defined here and may vary from host to host and network to network.

Compare b/w OSI & TCP/IP

(1) Both the TCP/IP & OSI models are based on the layered architecture. Both the models (2) support independent protocols. Both the layers provide end-to-end independent transport services to the parties wish to communicate. Both the model supports high level protocols at the Application layer.	But inspite of fundamental similarities the two models also have many differences.

OSI	TCP/IP
(i) 7 layer architecture.	
(ii) The services, protocols, interfaces are distinct.	(ii) It does not clearly distinguish among them.
(iii) The protocols are hidden and can be replaced as and when necessarily.	(iii) Protocols are visible & replacement is difficult.
(iv) This model came first. before the corresponding protocols were designed.	(iv) Here the protocol came first before the model was proposed so there was no problems for the protocols to feed in the model.
(v) No thought was given for internet working of different devices. So when internet growed the model failed.	(v) The main idea was to connect heterogeneous architecture together. So, it was success for internet and its still continue.
(vi) It provides only connection oriented services at the transport layer, giving no choice to the user.	(vi) User can choose between connection oriented (TCP) or connectionless (UDP) as per the application requirement.

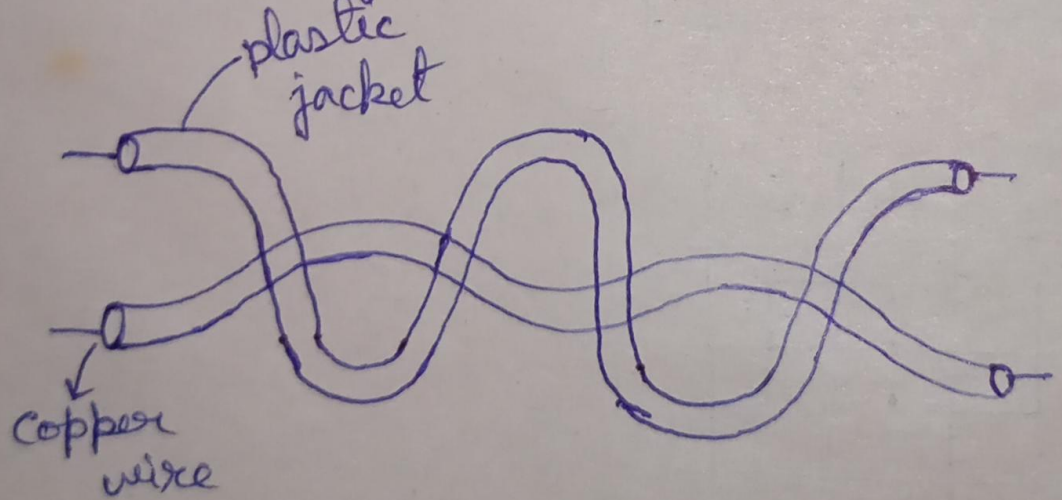
23/8/2024

Physical Layer :

- Transmission medium
  - Guided (wired)
    - Twisted Pair
    - Coaxial (Coax)
    - OFC
  - Unguided (wireless)
    - Radio Wave
    - Microwave
    - Infrared wave

29/8/2024

① Twisted Pair Calele :



Twisted pair consist of 2 conductors / normally copper. Each with its plastic insulator twisted together as shown in the diagram.

One of the wire is used to carry signals to the receiver and the other is used only as ground interference. The receiver uses the between these two levels.

The twisting reduce the noise equally for these 2 wires.

The twisted wire can be divided into —

(i) UTP (Unshielded Twisted Pair): The UTP is the most common type of twisted pairs.

There are 7 categories (CAT 1 to CAT-7)

- Among which CAT 6 and CAT 5 are most common. Categories are determines by the cables with 1 as the lowest and 7 as the highest.
- The standard data transmission speed varies between 100 mbps to 1 gbps.
- The connector tools for such cables are called RJ-45 (Registered Jack)

(ii) STP (Shielded Twisted Pair): This is the standard used by IBM.

- It has a metal foil or mess cover / shield that contains each pair of insulated conductor. The metal used to improve the quality of the cable by preventing the noise or crosstalk. However it is heavy and So, mostly used only within IBM.

Advantages:

(a) Cheapest among all the guided medium
(b) Easy to configure.
(c) Light weight
(d) Good data transfer speed

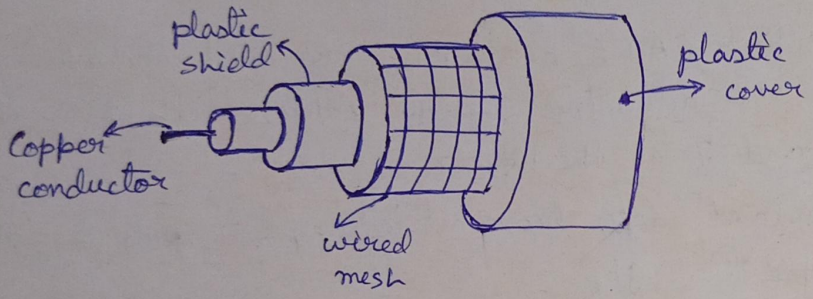
Disadvantages:

(a) Durability is less as it uses thin wires.
(b) The thin wires, can't carry signals to long distance without amplifier due to their high resistance.
(c) Data transmission speed is lower compare to other guided medium.

Application:

(i) The twisted pair are used in LAN (Local Area Network).

(2) Coaxial Cable (Coax):



It carries signals of higher frequency ranges than the Twisted pair (Faster than twisted pair). The coax cable as a central core conductor of solid copper wire. Enclosed within insulating copper, which in term engaged in the outer conductor of metal foil. The outer metalic wrap is used both as a sheild against noise and as a 2nd conductor which completes the circuit. This outer conductor is also covered by an insulator and the entire cable is protected by a plastic copper.

Cable standard:

The wires are standarised by RG standard. (Radio Govt.)
This standard specifies the physical structure of the cable. The popular categories are RG-49. RG58 ethernet and LAN.

The connector for this cable is called BNC (Bayone-Neil-Caneel mann)

Application:

Coaxis used in cable TV & LAN.

Advantage:

(i) Stronger than twisted pair so, more reliable.
(ii) Data transfer speed is more compared to twisted pair.
(iii) Installation & maintainance is easy.

Disadvantage:

(i) Costlier & heavier than twisted pair.
(ii) The signal goes down rapidly due to resistance and frequently used by users.

(3) OFC (Optical Fiber Cable):

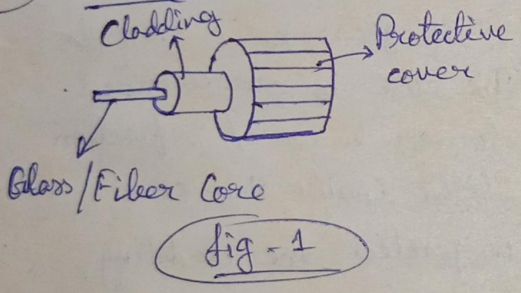
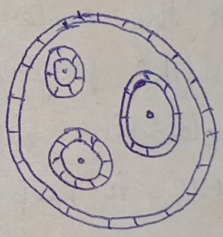


fig - 1



Cross section of a fiber cable

fig - 2

Fiber Optic cable is made of glass of plastic fiber. It transmit the signal in form of light. The OFC uses the special property of light known as total internal inference.

Propagation models:

Present technology support 2 mode of propagating light along the optical cable. Each requiring the fiber with different characteristics.

(i) Multimode: Since any light ray insident on a boundary above the critical angle will be reflected internally, it is possible to have many different range bouncing around

at different angles. Each ray is say to have a different mode at the fiber having this property is called multimode fiber.

- It is divided into two —
  (a) Step index
  (b) Graded index

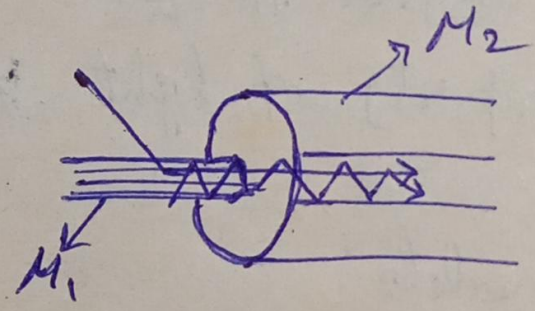
(2) Single Mode: With a fiber diameter is reduced to a few wave length of the light. The fiber behaves like a wave guide and the light propagates only in straight line without bouncing.
It is known as single mode in which only one signal can be passed through a wire.

4/9/24

Optical fiber cable is shown in figure 1 and figure 2. At the center, there is a glass core through which the light propagates. The core is surrounded by glass cladding with a lower index of refraction than the core, to keep all the light inside the core. Thin plastic packet is used to protect the cladding. The connector for optical fiber are known as MT-RJ. Two kind of light sources are used for signalling — LEDs & semiconductor lasers.

Advantages:

(i) Light weight
(ii) High speed
(iii) No signal loss
(iv) Can travel long distances without amplifier.



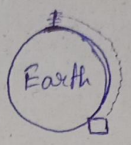
$M_1 > M_2$

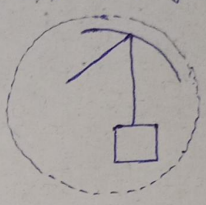
Disadvantages:

(i) Costly
(ii) Required specialized training & instruments for connection and maintainance.

Unguided or wireless Medium:

Unguided medium usage electromagnetic waves without using a physical conductor. This type of communication is also referred as wireless communication. Signals are normally broadcasted through air and is available to anyone who has a compatible The unguided signals can travel from source to destination using ground propagation.





Line of sight propagation
↓
one to one
↓
e.g. TV remote

- The unguided media is divided into 3 categories:

(1) Radio Waves:

The electro-magnetic waves having frequency between 3KHz – 1GHz are known as radiowave.
They are omni-directional.
(Propagates in all possible direction).
Sender or receiver need not have to maintain any kind of alignment. Radio waves can pass through walls. However omni-directional property is not suitable for secure transmission. The data rate for digital communication is low. This frequency bound is controlled by FCC (Federal Communication Commision)
Radio wave are transmitted using omni-directional antennas. It uses multi-casting. The propagation is route & sky.

Application: (i) Radio waves are used by AM and FM radioes.
(ii) Bluetooth devices use radio waves for communication.

Date: 5/9/24

Microwave

The electromagnetic spectrum ranging from 1 GHz to 300 GHz are known as microwaves. The microwaves are transmitted using the dish antenna and horn antenna. It uses sky and light of sight propagation. Microwaves cannot pass through walls. Periodic installation of microwave tower is required for long distance communicator. Microwaves

can carry large amount of data and supports secure communication. Microwaves are used in cellular phone, wifi (both 2.4 GHz and 5 GHz), satellite communication.

Advantages —

1. High bandwidth so can carry more data.
2. Secure transmission
3. Availability of devices

Disadvantages —

1. Cannot travel long distances without transmission towers.
2. Cannot pass through walls

Infrared waves

Infrared wave having the range in between 300 GHz to 400 TeraHz are called infrared wave. Infrared follows the line of sight propagations only that is sender and receiver must be able to see one another. ~~Example of infrared~~ is Infrared communication can not pass through the walls. The overlapping between the devices is very less due to its' high bandwidth support.

~~Applications~~

The infrared spectrum is controlled by IrDA (Infrared Data Association)

Application —

1. Infrared is used in remote control devices such as TV.

Advantages:

1. No overlapping due to high bandwidth.
2. Secure and unicast communication.
3. Huge availability of compatable devices.

Disadvantages:

1. Very short communication.
2. Slow data transfer rate.
3. Cannot pass through wall.

6/9/2024

Encoding

Digital to Analog

1. Polar encoding
   - NRZ
   - RZ
   - Manchester
   - Differential Manchester.

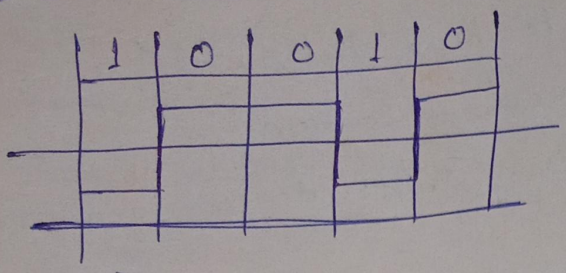
Polar encoding — It is uses 2 voltage levels, one +ve and one -ve. Polar encoding can be divided into following categories —

(i) NRZ (Non-Return to Zero) — In this encoding the value of the signal is always either +ve or -ve. There are two types of NRZ encoding —

a) NRZ-L (NRZ Level encoding) — In this encoding the level of the signal is dependent on the state of the bit. A +ve voltage usually means the bit is 0 (zero), while the -ve voltage means the bit is 1.

0 = +ve voltage
1 = -ve voltage

Bit pattern



left to right

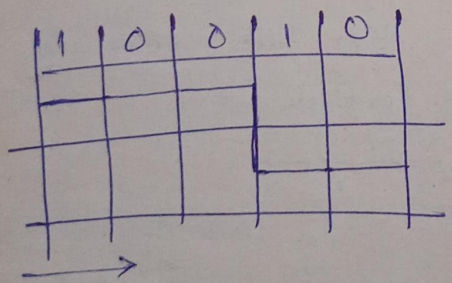
Drawback:

If there is a series of 0's or series of 1's in the incoming data, then there will be no change of levels for a long time. So, the sender and receiver may lose out of synchronization.

b) NRZ-I (NRZ Invert encoding) — In NRZ invert, and inversion (flip) represents binary one (1). Binary zero (0) is represented by no change in the signal level. The synchronisation is easy in this case as compared to NRZ-L.

0 = No change
1 = Flip the signal

Bit pattern



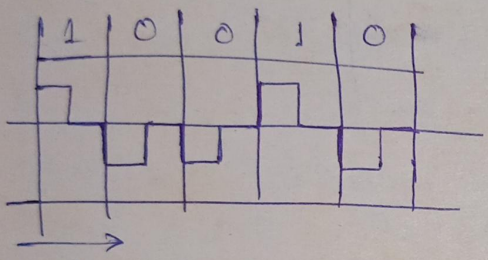
Drawback:

The synchronization problem for continuous 1's is solved by alternate flip. However the problem for continuous 0's still remain.

(ii) RZ (Return to Zero) — In RZ encoding, 3 values : +ve, -ve and 0 (zero) are used for each bit. Binary one (1) is represented by starting in +ve region and ending at zero. Binary zero (0) starts in the -ve region and ends at zero. The transition is half wave.

0 = -ve to zero (½ -ve, ½ zero)
1 = +ve to zero

Bit pattern



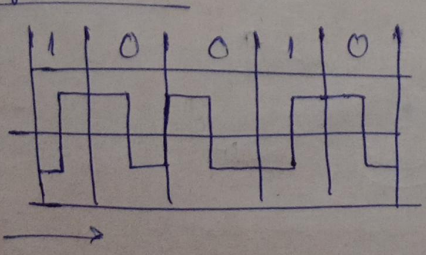
Disadvantage :

The main disadvantage of RZ encoding is that, it requires two signal change for each bit and hence occupies more bandwidth.

(iii) Manchester encoding — The manchester encoding uses and invertion (flip) at the middle of each bit interval. The -ve to +ve transition represents binary one (1) and the +ve to -ve transition represents binary zero (0). Manchester encoding achieve the same level of as RZ but with only 2 levels encoding

0 = +ve to -ve
1 = -ve to +ve

Bit pattern :

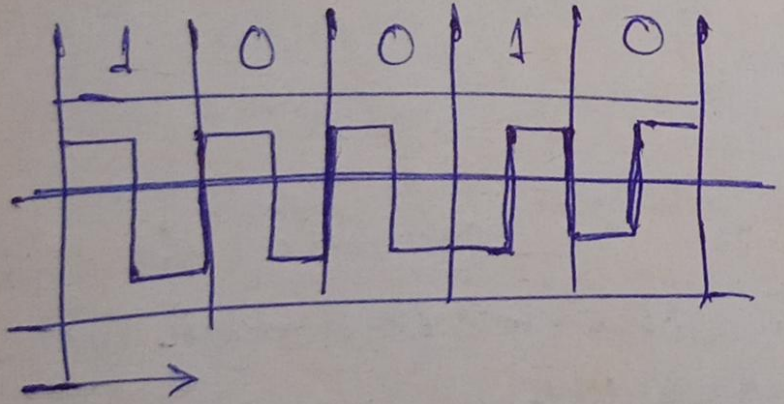


~~Disadvantage~~

(iv) Differential manchester — This is a variation of pure manchester encoding. In this encoding the presence and absence of a transition at the beginning of the bit interval is used to identify the bit (0 or 1). A transition means zero (0) and no transition means of one (1). Differential manchester encoding requires two signal changes to represent zero (0) but only one (1) to represent no change.

0 = change of start point
1 = NO change, starts from the same point

Bit pattern



12/9/2024

Message switching is applied in SMS and other messaging services.

Packet Switching—

For large message block, the message switching suffers from long transmission delays. The packet switching can limits the length of the message to a fixed sized by spliting the message into fixed sized packets. It is not necessary that all the packets must be transmitted through the same route. Packets belonging to the single message can be transmitted through different routes depending on the availability of the channels. Packets switching supports two modes for transmission.

i) Datagraph & ii) Virtual circuits

Advantages—

1) It is the most popular switching technique that is used in all modern transmission irrespective of the type of data.

2) Packet switching technique is much faster than message switching technique & its also effective for interactive traffic.

3) Since there is an upper limits on packet sized, no packets can occupy the channels for more than a fixed amount of time.

4) Each node can forward any packet as soon as it is received without waiting for the remaining packets.

5) It can be used for voiced data also.

Difference b/w —

Circuits	Messages	Packets
1) Dedicated transmission paths.	1) No fixed path.	1) No fixed path.
2) Continuous transfer of data.	2) Continuous transfer of message.	2) Continuous transfer of packets.
3) Information is not stored.	3) Informations are stored before they are forwarded.	3) Packet's are stored before they are forwarded.
4) Fixed rule for entire transfer.	4) The path is established for each message.	4) The path is established for packets.
5) Initial call setup delayed.	5) No call setup is required.	5) No call setup is required.
6) User is responsible for information loss.	6) Network is responsible for information loss.	6) Network is responsible for information loss.
7) Fixed bandwidth.	7) Dynamically vary bandwidth.	7) Dynamically vary bandwidth.
8) Error control bits are not required.	8) Error control bits for each message.	8) Error control bits for each packets.

Data Link Layer —

Introduction : The role of data link layer is to break the data into frames & send them to a channel free of error. So error detection & correction is necessary at this layer. The transmitted data may be corrupted & need to be transmitted. For reliable communication, errors must be detected & corrected (if possible)

Transmission modes

① Parallel transmission
② Serial transmission → Asynchronous transmission
② Serial transmission → Synchronous transmission

The transmission modes is an important factor to sent the data from sender to receiver is divided into following types.

1) Parallel transmission —

In parallel transmission n wires are used to send n bits at a time. As a computer usually consumes data in groups, this method is very useful.

The advantage of parallel transmission is the speed. But its main disadvantage is the cost. So, parallel transmission is used for very short distances only (usually less than a meter).

2) Serial transmission —

In serial transmission, a single pipeline is used to deliver the data. In this transmission, one bit follows another, so only one communication channel is needed. So it reduces the transmission cost & can be used for long distance transmission. It may be any one of the following.

i) Asynchronous Transmission Modes (ATM)

In ATM, the timing of a signal is not important. The information flows by a commonly agreed pattern & as long as the pattern is follows, the transmission can continue. In radiant, the bit boundary is denoted by 0 (start bit) & 1 (stop bit). There may be a gap between each byte or synchronization. So the total data consists of

Data bit + boundary bits.

ii) Synchronous Transmission Modes (STM) –

In this transmission the sender & receiver clock is synchronized & the data is sent as a stream of bits without any start/stop bits or gap. It is the responsibility of the receiver group the bits. Timing is the main criteria here, because the accuracy of the information is completely dependent on that. This mode is useful for high speed data transfer as no. extra bit or gap is required.

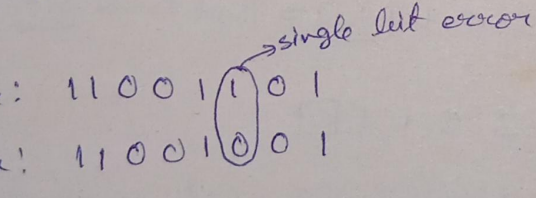
13/9/24

Mid Sem
26/9
1:00 – 2:00
B-209

Types of errors! –

(1) Single bit error – In a single bit error, only one bit in the data unit is changed (from 0 to 1 or 1 to 0). A single bit error usually occurs in parallal transmission. For example, if 8 wires are used to send one byte of data (each wire carry 1 bit) at the same time and one of the wires is noisy, one bit will be corrupted in every byte.

i.e.



(2) Burst error / Multiple bit error — A burst error indicates two or more bits in a data unit are corrupted. The burst error however does'nt mean that the error will occur in the consicutive bits. The length of the burst is measured from the first corrupted bit to the last corrupted bit. Some bits in between may or may not be corrupted. The burst error occurs in serial transmission.

All the bits within the burst length are discarded irrespective of ~~whether~~ whether the bits are good or bad.

i.e.

Sender: 1 1 0 0 1 1 0 1

Receiver: 1 1 1 0 1 0 0 1

Burst length

Error Detection Techniques

① Single bit error detection —

ⓐ Redundancy: Each data is sent twice one after another the receiver's device compare the two data bit by bit. If there is any mismatch then both the data is discarded. This method is accurate but requires more bandwidth and transmission time. So it is impractical for large amount of data.

ⓑ Parity bit method:

↳ Even parity

Odd Parity

i.e. Even Parity

Data: 1 1 0 1 0 0 1 1

Sender: 1 1 0 1 0 0 1 1 [1] ⇒ Total 1's should be even

odd Parity

1 1 0 1 0 0 1 1 [0]

Parity bit method can check single bit error by adding 1 bit with the data bit

Even Parity / odd Parity

In parity bit method one extra bit called parity bit is added to every data unit so that the total no. of 1's in the encoded unit (including the parity bit) is even (even parity) or ~~(odd parity)~~. the total no. of 1's in the encoded unit is odd (odd parity).

The choice to use even or odd depends on the user.

Even Parity

Data: 1 1 0 1 0 0 1 1

Sender: 1 1 0 1 0 0 1 1 [1] ⇒ Total 1's should be even

Odd Parity

1 1 0 1 0 0 1 1 [0] ⇒ Total 1's should be odd

9/9/2024

Checksum

Checksum method is used to detect both single bit and burst error. In this method the data unit is divided into equal segments. The operation is done as follows.

Step ①: The data is divided into K sections each with size 'm' bits.

Step ②: All sections are added using 1's compliment method to get the sum.

Step ③: If there is a carry in the final addition result, the wrapped sum is found by cutting and adding the carry with the sum.

Step ④: The sum is complimented and becomes the checksum

Step ⑤: The checksum is appended at the end of the data and ~~sent to the~~ is set to the receiver side.

~~The da~~ Receiver Side :—

The data receives with checksum is again taken as data by the receiver. The receiver again calculate the checksum. If the answer is zero then the data is good.

Example

Calculate the checksum for the data 11011011 using 4-bit checksum method. Also validate the data at receiver side.

Soln:

```
          1 1 0 1
        + 1 0 1 1
        ---------
 sum  [1] 1 0 0 0
wrapped +       1
sum     ---------
          1 0 0 1     = 0 1 1 0 → check sum (compliment)
```

Sender: 1 1 0 1 1 0 1 1 0 1 1 0

Receiver:

```
      1 1 1
      1 1 0 1
      1 0 1 1
    + 0 1 1 0
    ---------
   [1] 1 1 1 0
     \-------> 1
wrapped  +
    ---------
sum ---> 1 1 1 1   = 0 0 0 0 -> check sum (compliment)
```

So, the data is good / errorfree.

Drawback

Suppose we have ~~dataset arrays~~ data segments 1001 and 1111. Then the calculated checksum will be same as 1101 and 1011. However the data are different. So the checksum method fails when the bits are altered at the same position.

Application of checksum:

Checksum is applied in check the hardware errors in storage devices or data.

Cyclic Redundancy Check (CRC)

CRC is a powerful ~~method~~ that can be used to detect both single and multibit errors. It does not suffer from the problems that checksum faces. CRC is based on binary division. It is done as follows —

① Extract the binary digits from the given polynomial.

e.g. $x^3 + x^2 + 1$

Rewrite including the missing terms

$1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 1 \cdot x^0$

1 1 0 1

Pull down the coefficients

(2) Append the string of $(n-1)$ zeros with the data where n is the no. of bits in the divisor extracted from the polynomial. For the above example $n=4$ so $(4-1)=3$ zeros will be appended at the end of the data.

(3) The total data unit (original + added zero) is divided by the divisor using XOR operation.

(4) One bit from RHS of the data unit is pull down and appended at the RHS of the result of the XOR operation. If the result even after the pull down operation becomes less than the divisor, then instead of original divisor, the zeros are XOR in the next operation.

(5) When the division is finished, the remainder will become the CRC which will substitute the $(n-1)$ dummy zeroes that were padded with the original data earlier.

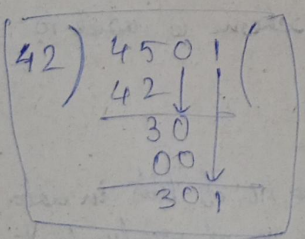
(6) At the receiver end, the data + CRC is again divided by the same divisor. If the calculated CRC is now zero then the data is good.

Example:

$$x^4 + x^2 + 1$$

$$1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 1 \cdot x^0 = 10101$$

Calculate the CRC for the data : 100100 with the polynomial : $x^3 + x^2 + 1$. Also validate the data at the receiver side.

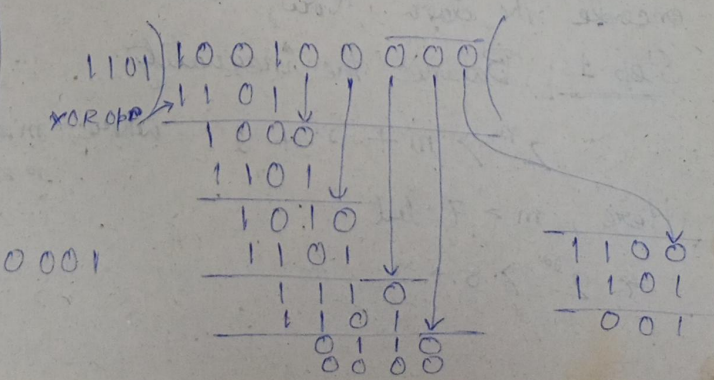


So, CRC = 001

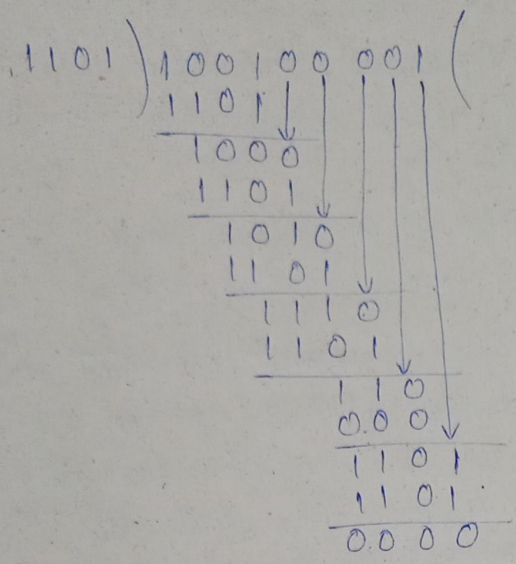
encoded data : 100100001

$$x^3 + x^2 + 1$$

$$\Rightarrow 1101$$



Validate:



Remainder is zero. So, the data is error-free.

error detection (2 to 1 for 7 marks mid-sem = 2 marks)

Hamming Code (Single bit error correction code)

Hamming distance

Two methods are there — (i) Computer Science Method (CSE)
(ii) Electronics Method (E)

2 for binary no. → 2 for changed digit

Count '1' after XOR operation

e.g.:

```
  1 1 0 1 0 1 1
XOR
  1 0 1 1 0 1 1
  ---------------
  1 1 0 0 1 0
```

H.D. = 3 (CSE)

H.D. = 3 (E)

The hamming code is proposed by E. H. Hamming. This method is used to correct the received data where retransmission is not possible.

Let, the data bit 1001101 has to be set using hamming code. The even parity scheme is used to encode the data. Now,

Step 1: Balance the inequality

$$2^r > m + r + 1$$

where, m = no. of bits in data
r = no. of redundant bit required

Here, m = 7 bit

$\Rightarrow 2^r > 8 + r$

~~The above condition~~

True for $r=4$, Suppose, r_1, r_2, r_4, r_8

So total = 7+4 = 11 bits will be transmitted

			2^3				2^2	2^1	2^0
11	10	9	8	7	6	5	4	3	2	1
1	0	0	r_8	1	1	0	r_4	1	r_2	r_1

Find the rooms that are power of 2.

r_1: All room numbers with first bit (LSB)

1, 3, 5, 7, 9, 11

Even parity of 3, 5, 7, 9, 11 as r_1 is not available

1 0 1 0 1
11 9 7 5 3 ⇒ Even parity 1

r_2: 2nd bit (LSB)

2, 3, 6, 7, 10, 11

Even parity of 3, 6, 7, 10, 11 as r_2 is not available

1 1 1 0 1 ⇒ Even parity 0

r_4: 4th bit (LSB)

4, 5, 6, 7

Even parity of 5, 6, 7 as r_4 is not available

0 1 1 ⇒ Even parity 0

r_8: 8th bit

8, 9, 10, 11

r_8 0 0 1 ⇒ Even parity = 1

8	4	2	1	
0	0	0	1	→ 1
0	0	1	0	→ 2
0	0	1	1	→ 3
0	1	0	0	→ 4
		⋮		
1	0	1	1	→ 11

Now, the data is: 1 0 0 1 1 1 0 0 1 0 1

CSMA/CD

CSMA (Carrier Sense Multiple Access with Collision Detection):

In this method any station can send the frame. The station then monitors the medium to see if the transmission was successful. If not (due to collision or some other cause), the frame need to be retransmitted to reduce the probability of collision again during retransmission. The station must wait. This waiting time must be different for each station. It performs the operations as follows—

CSMA/CD Algorithm

Step 1: Before beginning the transmission, the station senses the medium to see if anyone else is transmitting.

Step 2: If the medium is idle, the station starts transmission and goes to step 4. Otherwise, it goes to step 3.

Step 3: If the medium is busy, it continuously listens until the channel become idle. Then it starts immediately.

Step 4: If collision is detected during the transmission, a brief jamming signal is transmitted to inform all other stations to stop transmission immediately.

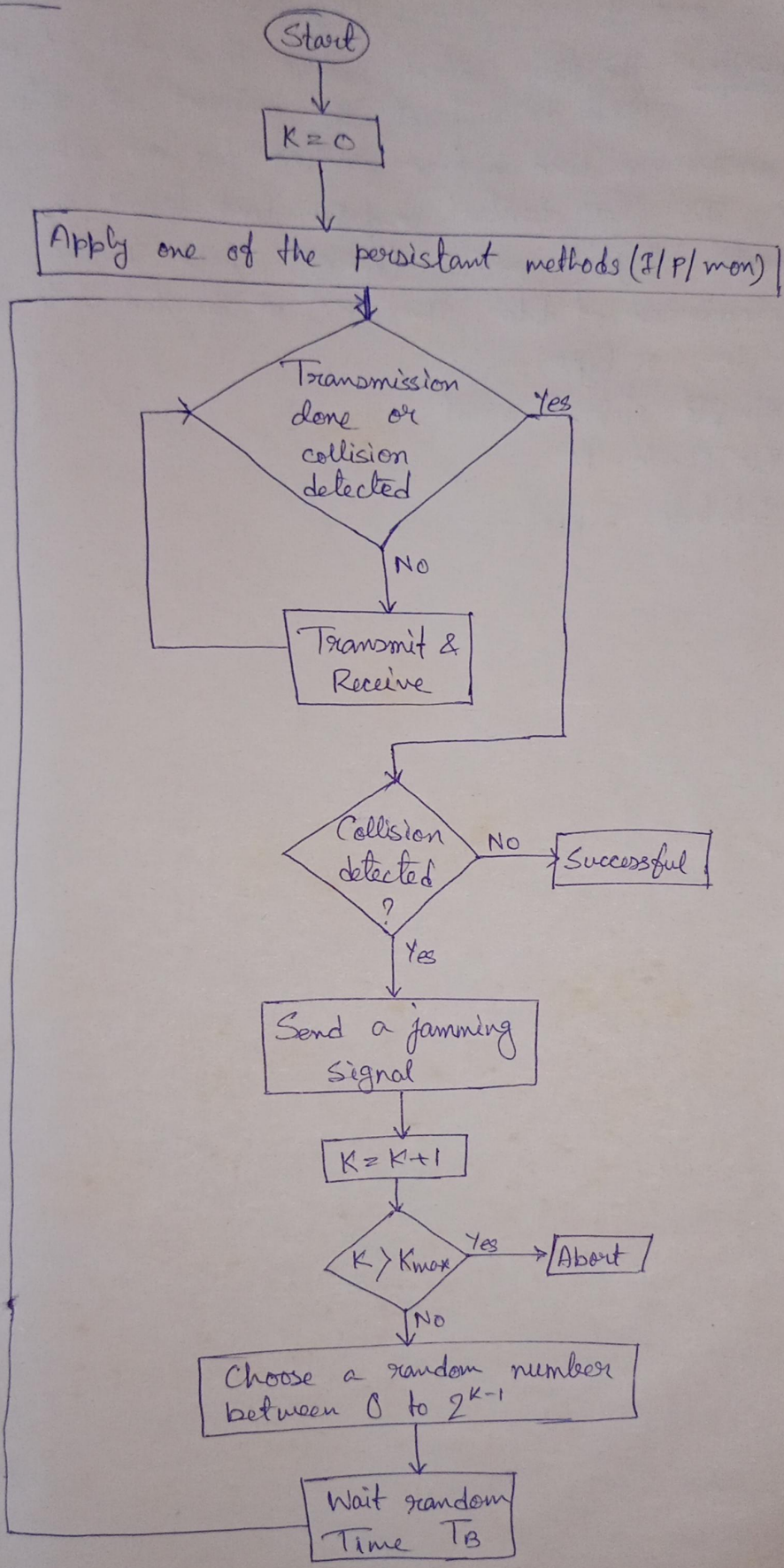
Step 5: After transmitting the jamming signal, the station waits for random amount of time using exponential back off method and starts from step 1 again.

- CSMA/CD is used in Ethernet protocol and few other LAN protocol.

CSMA/CA (Collision Avoidance)

CSMA/CA is the version of CSMA/CD, i.e. used for wireless transmission. CSMA/CD can not be used in wireless medium.

Flowchart:


Start
K=0
Apply one of the persistant methods (1/P/non)
Transmission done or collision detected
Yes
No
Transmit & Receive
Collision detected ?
No
Successful
Yes
Send a jamming signal
K=K+1
K > Kmax
Yes
Abort
No
Choose a random number between 0 to 2^K-1
Wait random Time TB

(A) Flow and Error Control Mechanism:

Definition: The flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for an acknowledgement. The flow control in data link layer is based on Automatic Repeat request (ARQ) which is the retransmission of data. The ARQ is divided into the following 3 types —

(i) Simple stop & wait
(ii) Go Back - N
(iii) Selective Repeat.

6/10/2024

Network Layer

1. IP Address
2. MAC address

IP Address is an unique address which is logically assign to a device in a network. It is also known as Logical Address or Software Address. The IP Address may be changed from time to time accross different networks. However two devices can not have same IP Address under the same network.

MAC (Media Access Control) / Physical Address

Each device connected to the network must have an unique hardware address that is assigned by the device manufacturer. This address is unique and cannot be changed. This address is refeerced as Hardware or Machine Address with size 6 bytes.

Classification of IP

IPv4 consists of 4 bytes of (32 bits) address.

→ 8 bits

X . X . X . X

↓

0 - 255

= 36 values

Min. 0 0 0

Max 1 1 1

$2^8 = 256$

Minimum IP address 0.0.0.0

Maximum " " 255.255.255.255

Total no. of IP address available in the world -

$2^8 \times 2^8 \times 2^8 \times 2^8 = 2^{32}$

This technique is known as Classful Addressing

Class A ← x.x.x.x

0|0000000 min — 0|1111111 max

0 - 127 — $2^7 = 128$

Class B

10|000000 — 10|111111

128 - 191

Class C

110|00000 (2^3) — 110|11111

192 - 223

Class D $2^4 = 16$

1110|0000 — 1110|1111

224 - 239

Class E

240 - 255

Net id & Host id

Class A - x.x.x.x

x → Net id; x.x.x → Host id

Net id

$2^8 = 256$ networks

Class B -

→ Net id - 16 bit x.x

→ Host id - 16 bit .x.x

network/host → 2^{16}

Net ⇒ 2^{16}

host/network

$2^8 \times 2^8 \times 2^8 = 2^{24}$ no. of machine in one n/w

Class C -

→ Net id - 24 bit x.x.x

→ Host id - 8 bit .x

2^{24} → net

2^8 → host/network

(1) 5.34.200.85 – Belongs from which class?

→ Class A

Class D ⇒ Defense

Class E ⇒ Special purpose

(2) 228.57.56.98 – "

→ Class D

(3) 198.168.0.1 – "

→ Class C

(4) 169.45.17.10 – "

→ Class B

Net id & Host id

Class A – X . XXX

X → Net id

XXX → host id

Subnetting & Supernetting

- If all the ip addresses in the network are not used, subnetting allowse the address to be divided among various organizations by creating smaller networks. Subnetting is done by using a portion of host id as network id. It is to be remembered as subnetting does not increase the total no. of IPs. However, it saves the wastage of IP.
- Supernetting was proposed to combine multiple class C blocks in the large block for those organizations who require more than 256 addresses of using class C.

CIDR (Classless Inter Domain Routing)

In this method variable length block are used that belong to no class. The prefix of any address defines the Net ID & the suffix defines the host. According to CIDR, the prefix is denoted at the end of the address with the front slash.

Ex: 12.12.12.13/8 → prefix

132.16.50.5/16

192.168.1.1/24

Rules

1) Total no. of addresses in a block

$N = 2^{32 - \text{prefix}}$

Class C

$N = 2^{32-24} = 2^8$

2) The first address in the block can be found by keeping the prefix bits fixed at the left side & 32- prefix bits to all 0's.

3) Last address of the block can be found by keeping the prefix bits fixed the left side & 32- prefix bits to all 1's.

Example — The classless address is given by 167.199.170.82/27. Find the total no. of address in the.

block, the first address & the last address of the block.

→ Lock = 27 bit

167 199 170 62
X . X . X . X
010|10010

62 ⇒ 01010010

167.199.170.010|00000 → 64

167.199.170.010|11111 → 95

Total = 2^{32-27} = 32

7/11/2024

Block Allocation

① Prefix length in each subnet
= 32 − $\log_2$ (total allocated address in power of 2)

② Allocated address must be power of 2.

Example: An organisation is granted block of address with the starting address 14.24.74.0/24. You need to design a network that have

i) One subblock of 10 addresses.
ii) One subblock of 60 addresses.
iii) One subblock of 120 addresses.

How many addresses will still be free?

⇒ Total address = 2^{32} prefix = 2^{32-24} = 2^8 = 256

Let us start with 120 addresses.

120 → 128

120 can not be allocated as it is not power of 2 so nearest power of 2 is that is 128 is allocated.

So, Free IP in this block will be 8.

128, convert in power of 2 ⇒ 2^7

Prefix of this block = 32 − $\log_2(2^7)$ = 32 − 7 = 25

First IP: 14.24.74.0/25

Last IP: 14.24.74.127/25

Let us start with 60 addresses

$60 \rightarrow 64$

∴ Free IP in this block will be 4.

∴ 64, convert in power of 2 $\Rightarrow 2^6$

∴ prefix of this block $= 32 - \log_2(2^6) = 32 - 6 = 26$

∴ First IP: 14.24.74.128/26

Last IP: 14.24.74.191/26

Let no. start with 10 addresses.

$10 \rightarrow 16$

∴ Free IP in this block will be 6.

∴ 16, convert in power of 2 $\Rightarrow 2^4$

∴ prefix of this block $= 32 - \log_2(2^4) = 32 - 4 = 28$

∴ First IP: 14.24.74.192/28

∴ Last IP: 14.24.74.207/28

∴ 208 address is used out of 256 address.

∴ $256 - 208 = 48$ addresses will be free.

∴ Total allocated address = 25

∴ Total used address = 208

∴ Total free address = 48

9) An ISP is granted the block 16.12.64.0/20. The ISP is to allocate addresses for 4 organization each with 256 addresses.

a) Find the number and range of addresses in each block.

b) Find the number of unallocated addresses.

Total address $= 2^{32 - \text{prefix}} = 2^{32-20} = 2^{12} = 4096$

Address given

Prefix of each block $= 32 - \log_2(2^8) = 32 - 8 = 24$

First org.) First IP: 16.12.64.0/24

Last IP: 16.12.64.255/24

Second org.) First IP: 16.12.65.0/24

Last IP: 16.12.65.255/24

Third org. First IP: 16.12.66.0/24
Last IP: 16.12.66.255/24

Forth org. First IP: 16.12.67.0/24
Last IP: 16.12.67.255/24

∴ Total allocated = 4096
∴ Total used = 1024
∴ Total Free = 4096 - 1024 = 3072

Q) An organisation is granted the block 130.56.0.0/16. The admin wants to create 1024 subnets.

i) Find the number of addresses in each subnet.
ii) Find the first and last addresses of the first subnet.
iii) Find the first and last address of the last subnet.

Address given = $2^{32-16} = 2^{16}$
∴ machine/subnet = $2^{16}/2^{10} = 2^6 = 64$
∴ prefix of each subnet = $32 - \log_2(2^6) = 32 - 6 = 26$

First block: First IP: 130.56.0.0/26
Last IP: 130.56.0.63/26

Last block: First IP: 130.56.255.191/26
Last IP: 130.56.255.254/26

64 × 4 = 256

4) 1023 (255
3 (rotation)

126
8 16 24
X. X. X. X
255.255.255.192
11000000

Q) An ISP is granted a block of addresses starting with 190.100.0.0/16
The ISP needs to distribute the addresses three group of customer as follows ——

i) First group has 64 customers each need 256 addresses.
ii) The second group has 128 customers each need 128 addresses.
iii) The third group has 128 customers each need 64 addresses.

Design the subblocks and find out how many address are still available after this allocation.